Identity Services Engine (ISE) versie 3.4 implementeren op AWS

Inhoud

Inleiding

In dit document wordt beschreven hoe u Cisco ISE op AWS kunt configureren met:

- CloudFormation-sjabloon (CFT)
- Amazon Machine Image (AMI)

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen voordat u doorgaat met deze implementatie:

- Cisco Identity Services Engine (ISE)
- Beheer en netwerken van AWS EC2-instanties
- Generatie en gebruik van SSH-sleutelparen

- Basiskennis van VPC's, beveiligingsgroepen en DNS/NTP-configuratie in AWS

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine (ISE)
- Amazon Web Services (AWS) Cloud Console

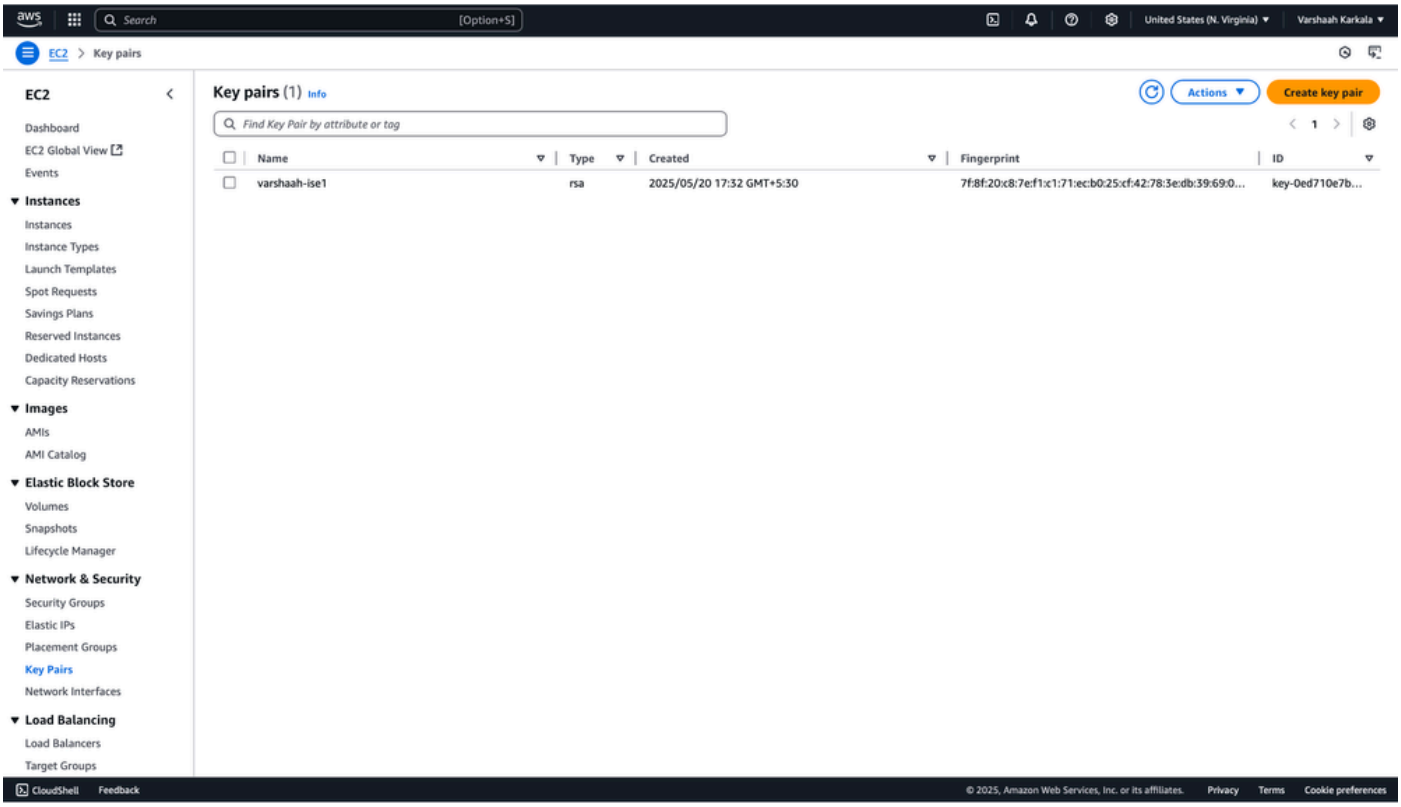
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

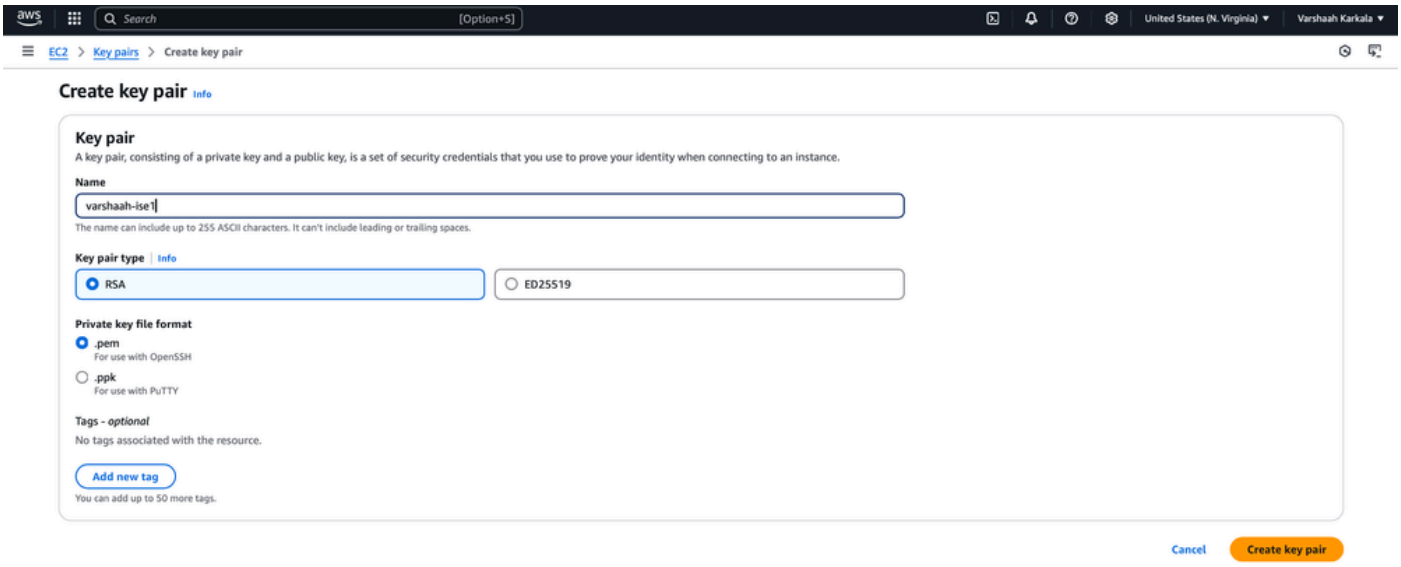
Deel 1: Een set SSH-sleutelparen genereren

1. Voor deze implementatie kunt u een reeds bestaand sleutelpaar gebruiken of een nieuw sleutelpaar maken.

2. Als u een nieuw paar wilt maken, gaat u naar EC2 > Netwerk en beveiliging > Sleutelparen en klikt u op Sleutelpaar maken.



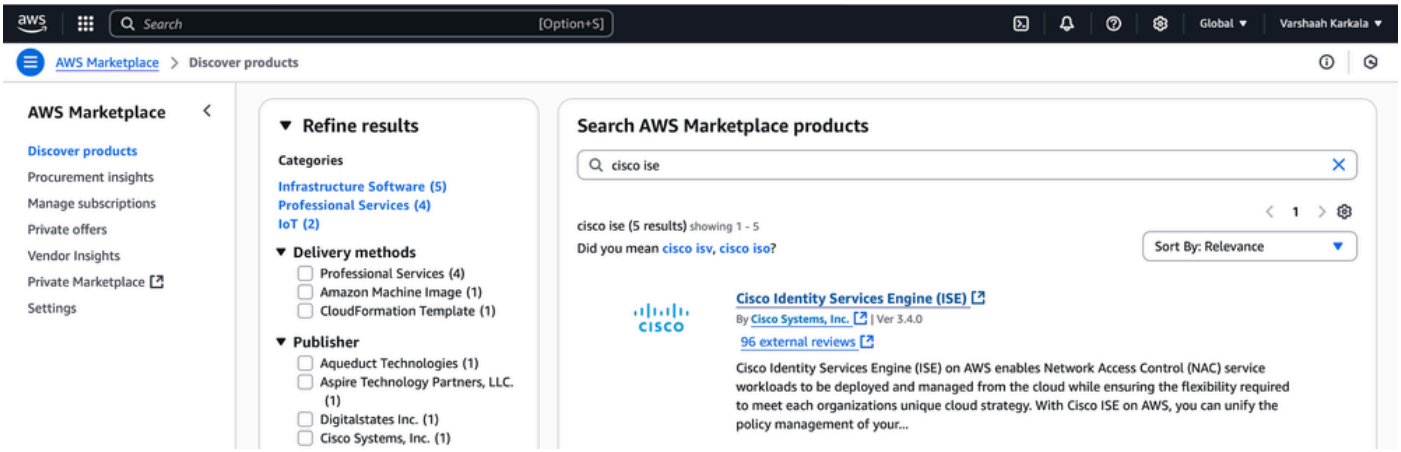
3. Voer de naam van het sleutelpaar in en klik op sleutelpaar maken.

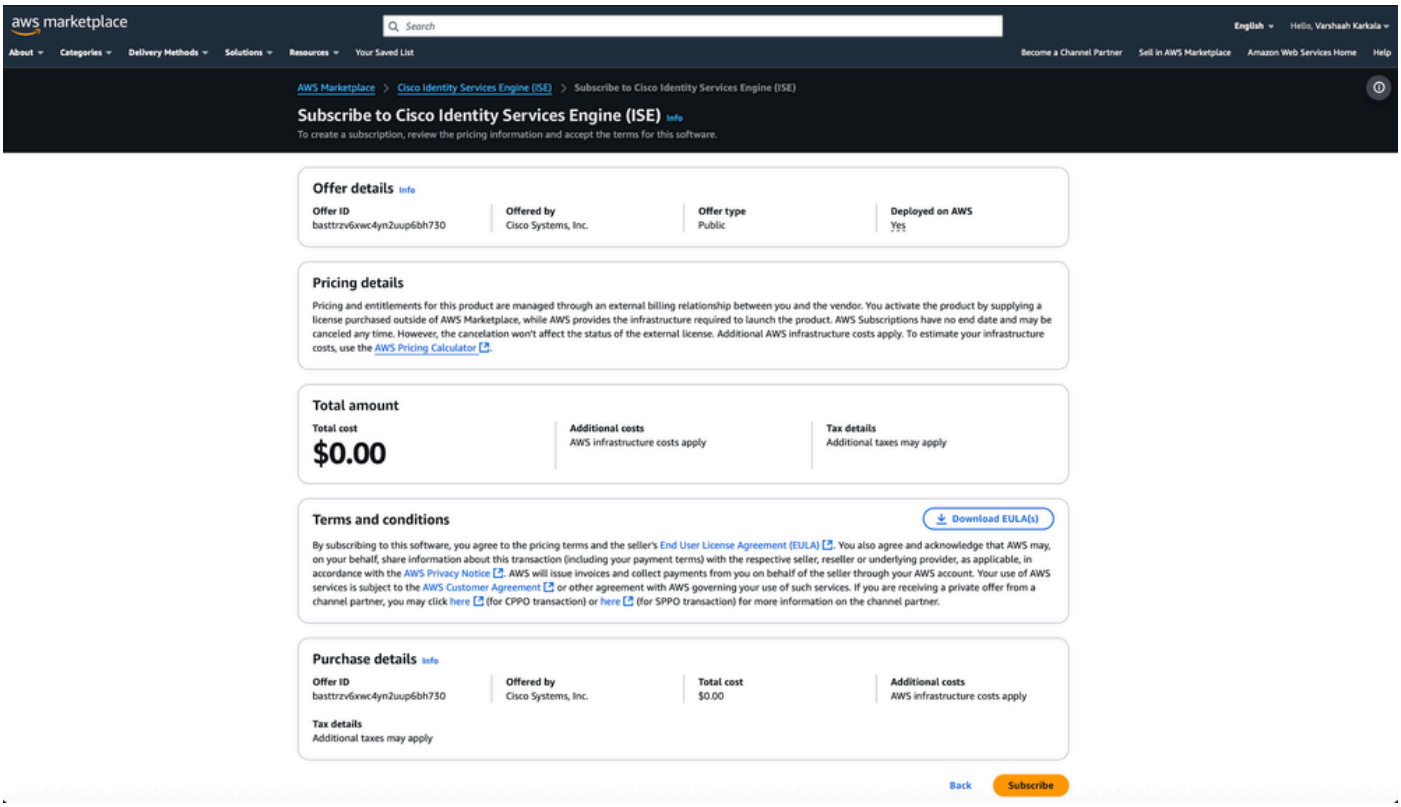


Het sleutelpaarbestand (.pem) wordt gedownload op uw lokale computer. Zorg ervoor dat u dit bestand veilig bewaart, want dit is de enige manier waarop u toegang kunt krijgen tot uw EC2-exemplaar zodra het wordt gestart.

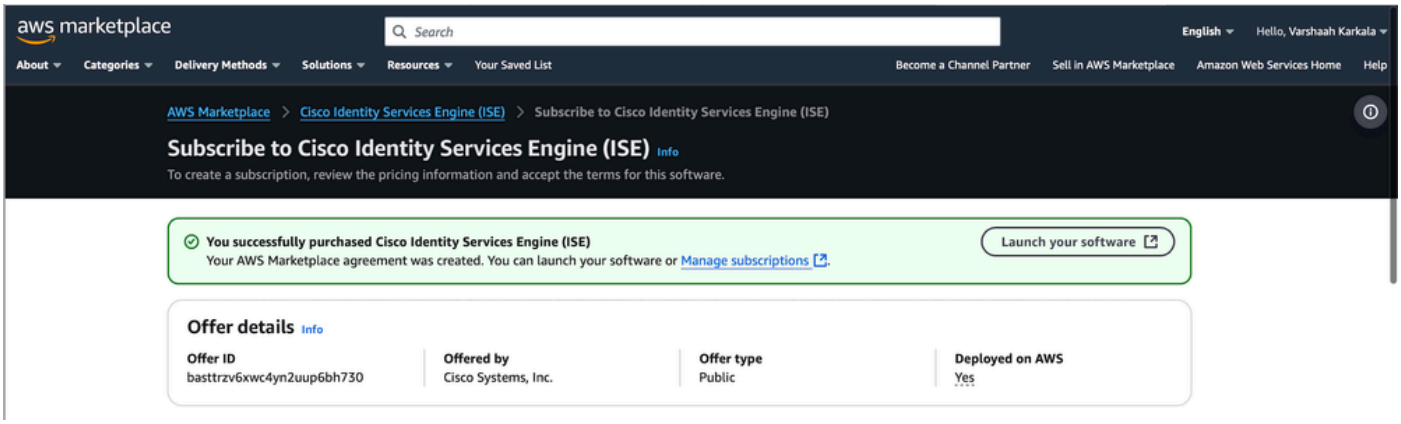
Deel 2: ISE configureren met behulp van CloudFormation Template (CFT)

1. Log in op de AWS Management Console en zoek naar AWS Marketplace-abonnementen.
2. Typ in de zoekbalk "cisco ise" en selecteer Cisco Identity Services Engine (ISE) uit de resultaten. Klik op abonneren.

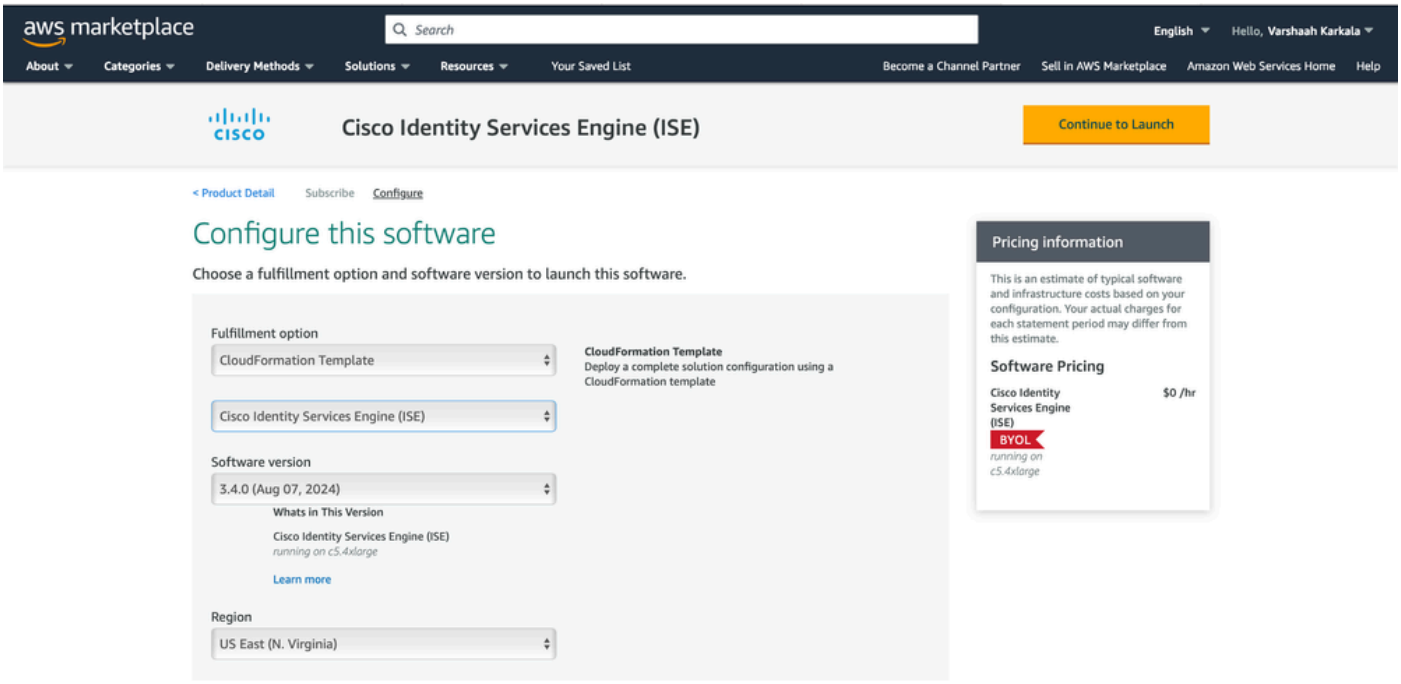




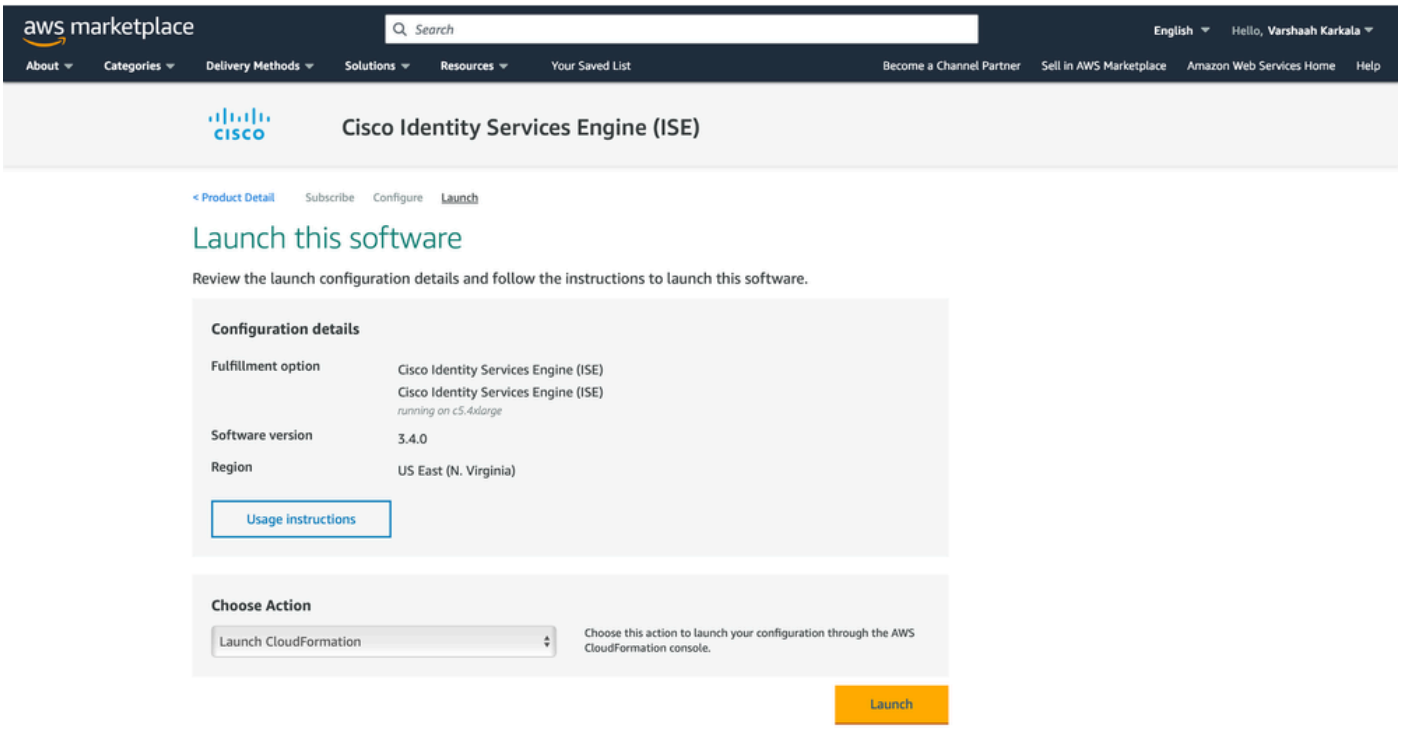
3. Selecteer Software starten nadat u zich hebt geabonneerd.



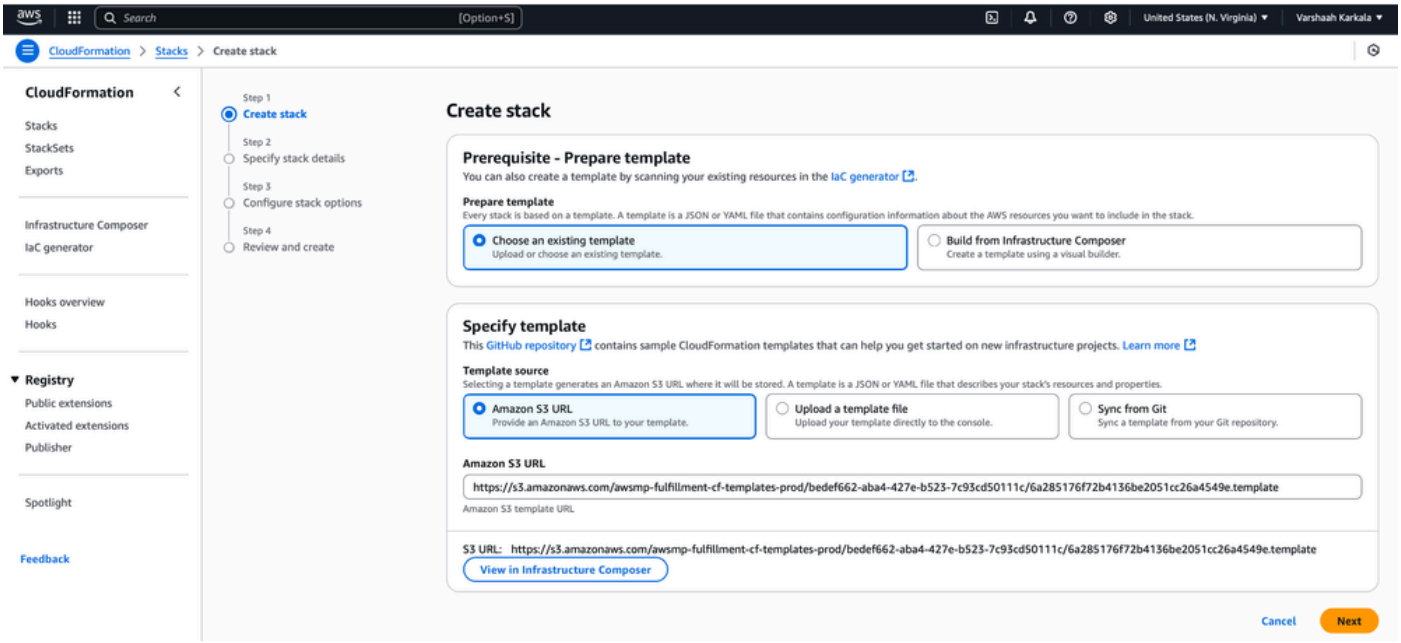
4. Kies onder Fulfillment Option CloudFormation Template. Kies de softwareversie (ISE-versie), de regio waar u de installatie wilt implementeren en klik op Doorgaan om te starten.



5. Selecteer op de volgende pagina CloudFormation starten als actie.

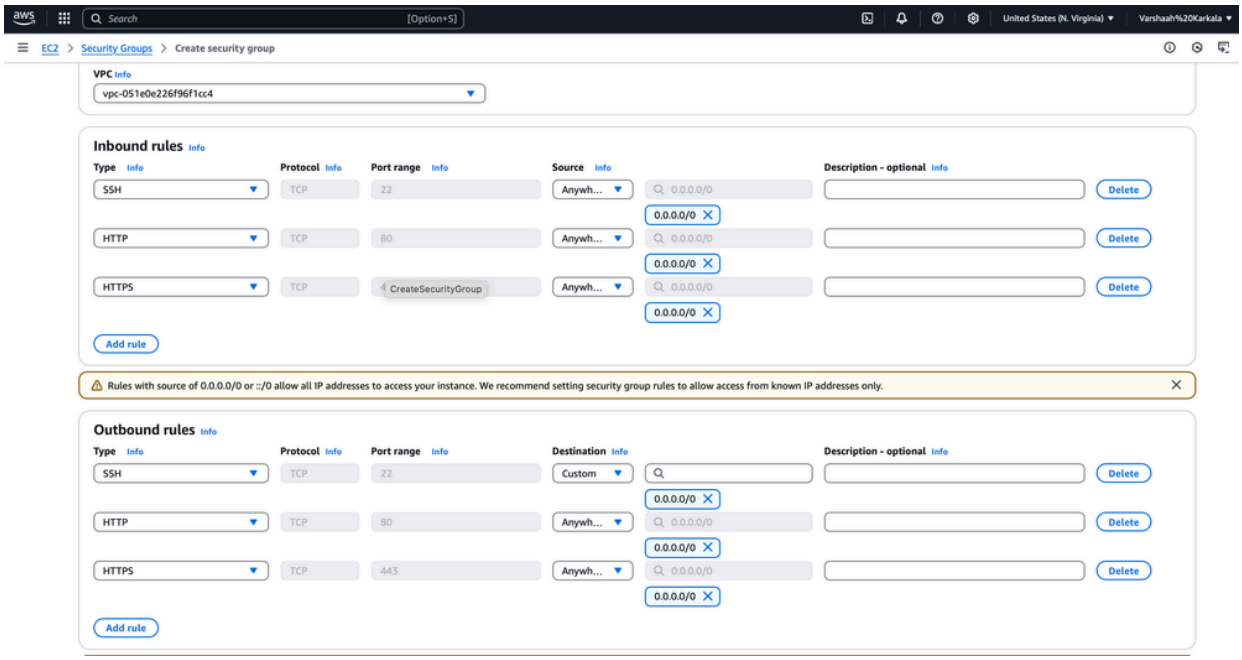


6. Bewaar de standaardinstellingen onder de stapelinstellingen en klik op Volgende.



7. Voer de vereiste parameters in:

- Stapelnaam: geef een unieke naam op voor uw stapel.
- Hostname: Wijs de hostnaam toe voor de ISE-node.
- Sleutelpaar: Selecteer het sleutelpaar dat is gegenereerd of reeds bestaat om later toegang te krijgen tot de EC2-instantie.
- Management Security Group:
    - Gebruik de standaardbeveiligingsgroep (zoals hieronder wordt weergegeven) of maak een aangepaste groep via het EC2-dashboard.
    - Als u een nieuwe beveiligingsgroep wilt maken, gaat u naar het EC2-dashboard en gaat u naar Netwerk en beveiliging > Beveiligingsgroepen om een nieuwe beveiligingsgroep te maken.
    - Klik op Beveiligingsgroep maken en voer de gewenste gegevens in.
    - Zorg ervoor dat de beveiligingsgroep is geconfigureerd om het vereiste inkomende en uitgaande verkeer toe te staan. Schakel bijvoorbeeld SSH-toegang (poort 22) in vanaf uw IP-adres voor CLI-toegang.

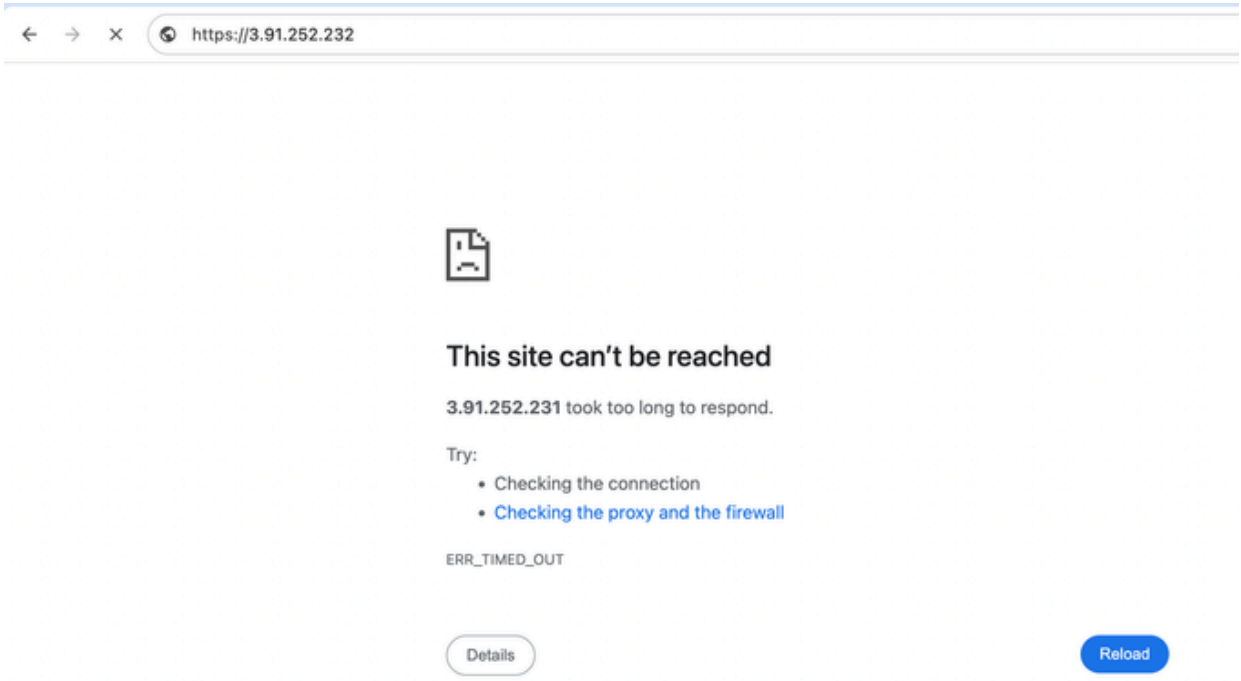


- Als de SSH-toegang niet goed is geconfigureerd, kan er een "Operation timed out" fout optreden wanneer u probeert verbinding te maken via SSH.

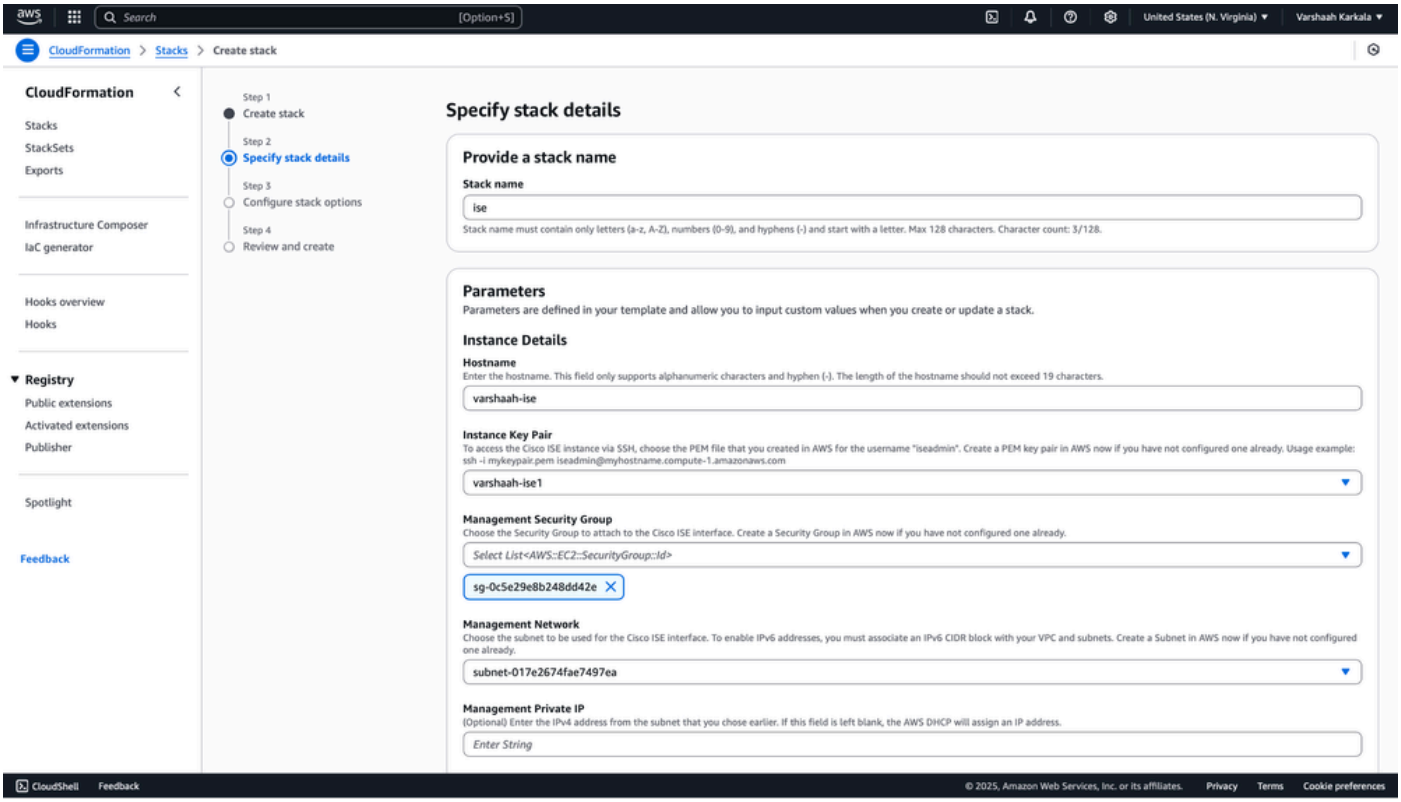
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

ssh: connect to host 3.91.252.232 port 22: Operation timed out
```

- Als HTTP/HTTPS-toegang niet is geconfigureerd, kan er een fout "Deze site kan niet worden bereikt" worden weergegeven wanneer u probeert toegang te krijgen tot de GUI.



- Beheernetwerk: een van de reeds bestaande subnetten is geselecteerd.



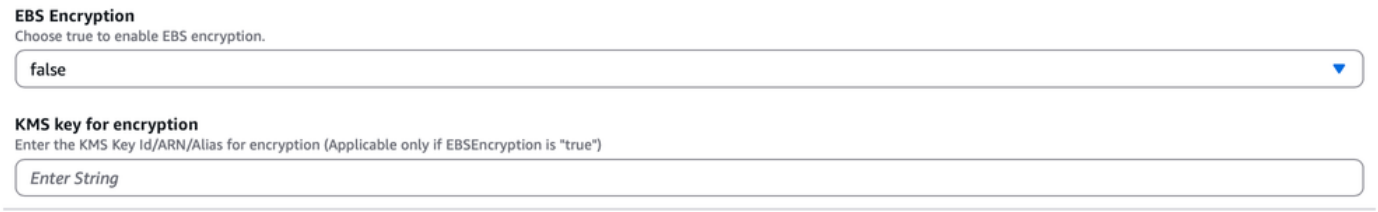
Als uw ontwerp een gedistribueerde implementatie vereist met sommige knooppunten die in AWS en andere on-premises worden gehost, configureert u een speciale VPC met een privé-subnet en stelt u een VPN-tunnel in naar het On-Prem VPN Headend Device om connectiviteit tussen AWS-gehoste en on-premises ISE-knooppunten mogelijk te maken.

Raadpleeg deze handleiding voor gedetailleerde stappen voor het configureren van het VPN

Headend Device.

8. EBS-codering

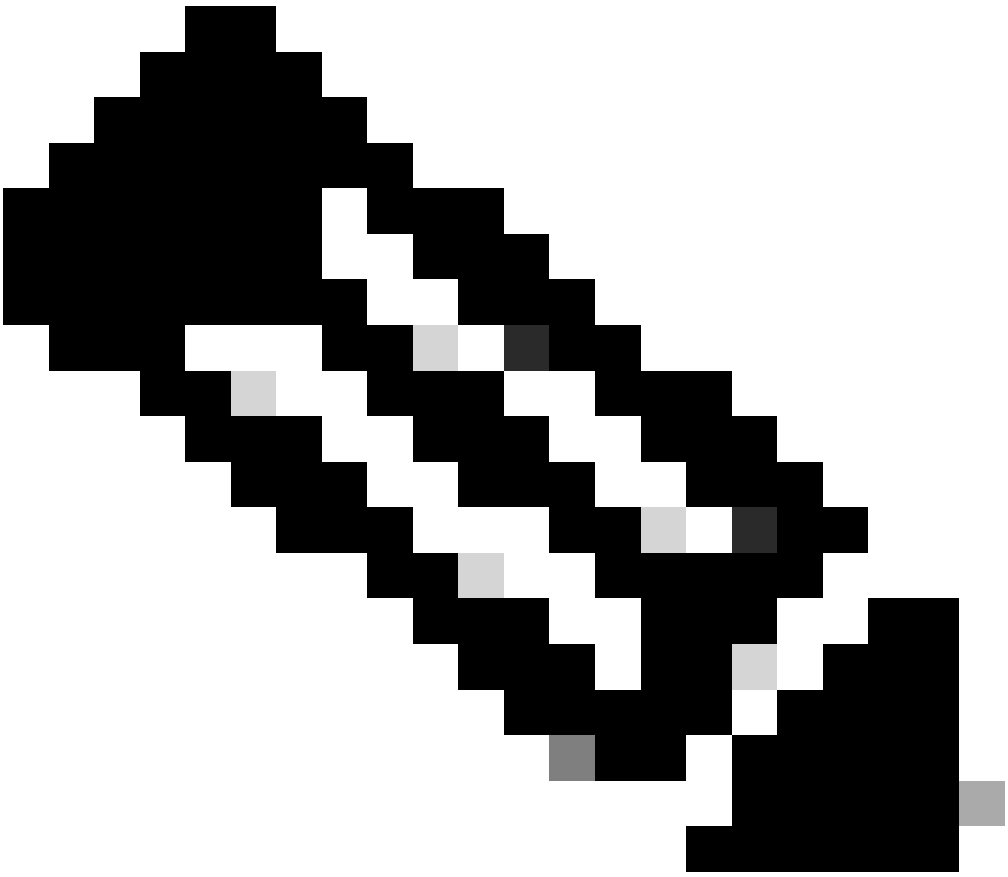
- Blader omlaag om de EBS-coderingsinstellingen te vinden.
- Stel EBS-codering in op Onwaar, tenzij u specifieke coderingsbehoeften hebt.



9. Netwerkconfiguratie:

- Scroll naar beneden om toegang te krijgen tot opties voor het configureren van netwerkinstellingen, zoals het DNS-domein, de primaire naamserver en de primaire NTP-server.

  Zorg ervoor dat deze waarden nauwkeurig worden ingevoerd.



Opmerking: onjuiste syntaxis kan voorkomen dat ISE-services na implementatie goed worden gestart.

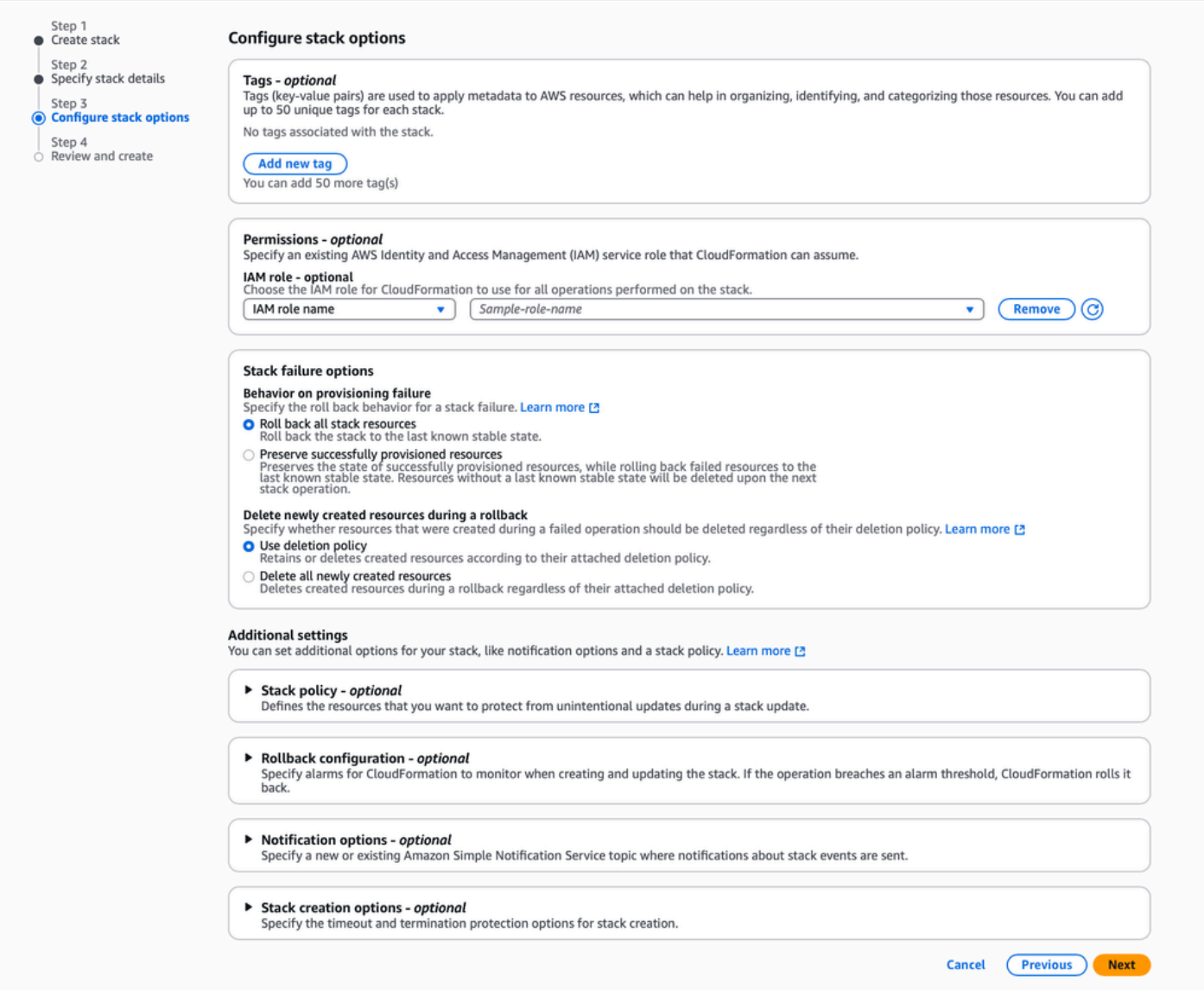
10. Service- en gebruikersdetails:

- Blader omlaag om de optie voor het inschakelen van ERS- en pxGrid-services te vinden
- Kies of u ERS- en pxGrid-services wilt inschakelen door ja of nee te selecteren.
- Stel onder Gebruikersgegevens het wachtwoord in voor de standaard admin-gebruiker.

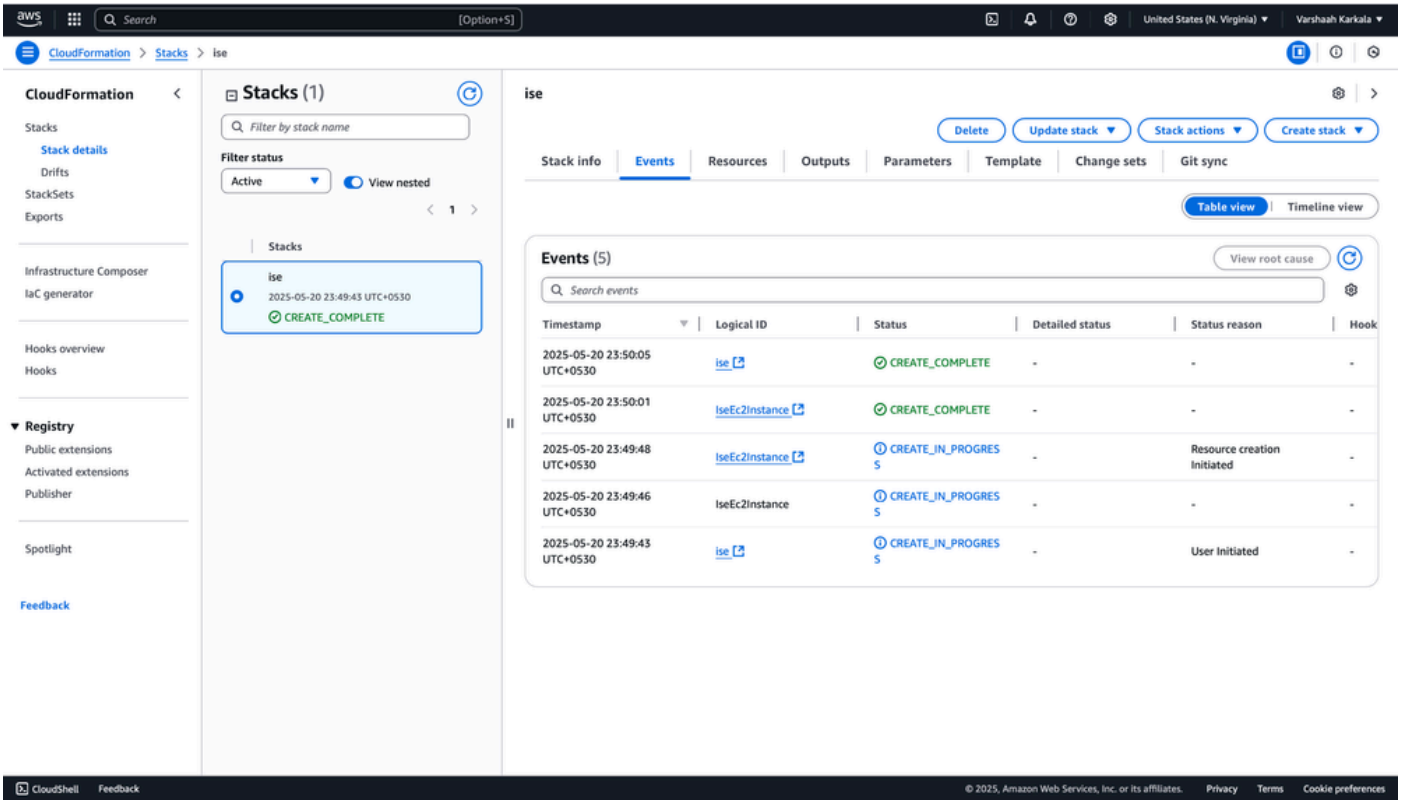
- Klik op Next (Volgende).

11. Stapelopties configureren:

- Laat alle standaardopties zoals ze zijn en klik op Volgende.



12. Controleer de template om te controleren of alle configuraties correct zijn en klik vervolgens op Indienen. Zodra de sjabloon is gebouwd, lijkt deze op het onderstaande voorbeeld:



13. Toegang tot de stapelgegevens:
Navigeer naar de CloudFormation-service in de AWS Management Console en ga naar de sectie Stacks. Zoek uw geïmplementeerde stapel in de lijst.

14. Tabblad Uitgangen weergeven:

Selecteer uw stapel en open het tabblad Uitgangen. Hier vindt u belangrijke informatie die tijdens het implementatieproces is gegenereerd, zoals:

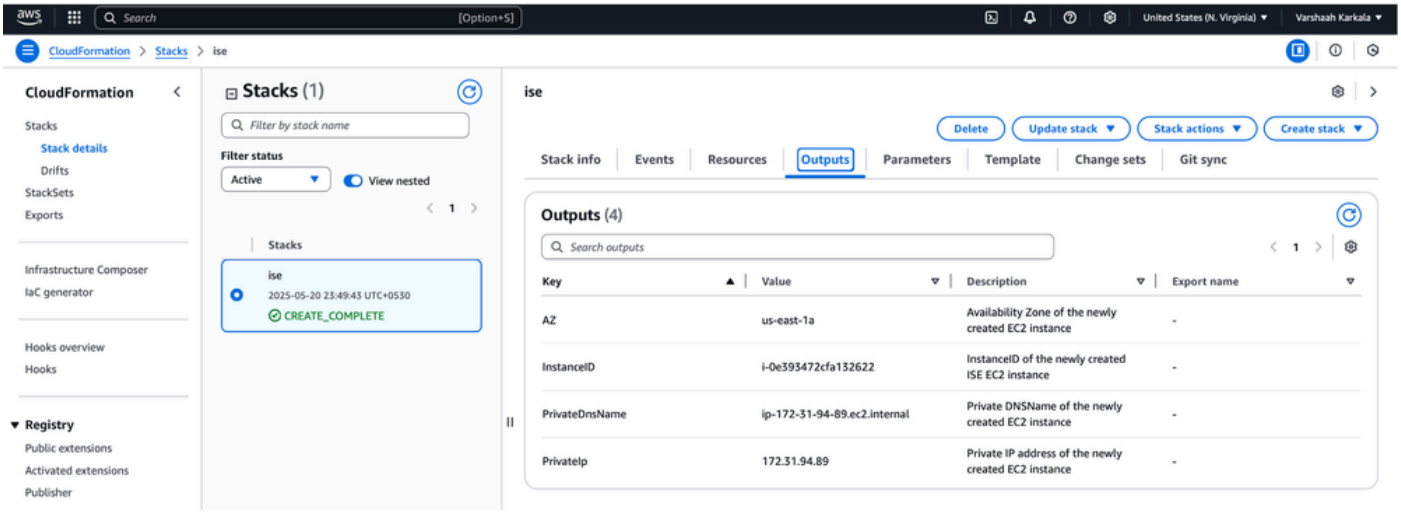
· Beschikbaarheidszone: de regio waar de middelen worden ingezet.

· Instantie-ID: de unieke id van de geïmplementeerde instantie.

· DNS-naam: De private DNS-naam van de instantie, die kan worden gebruikt voor toegang op afstand.

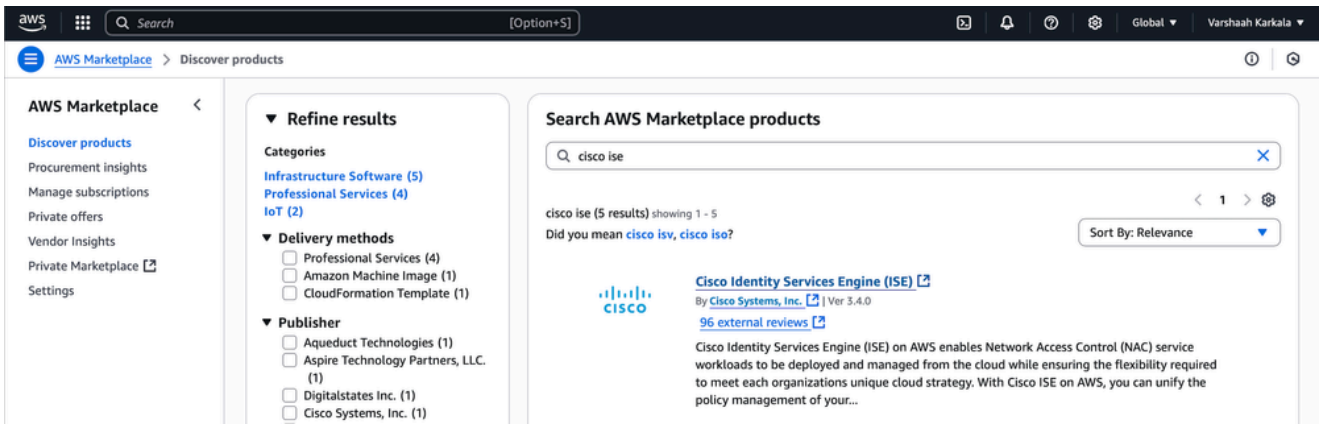
· IP-adres: het publieke of private IP-adres van de instantie, afhankelijk van uw configuratie.

Deze informatie helpt u verbinding te maken met de instantie en de beschikbaarheid ervan te verifiëren. Het tabblad Uitgangen lijkt op dit voorbeeld:



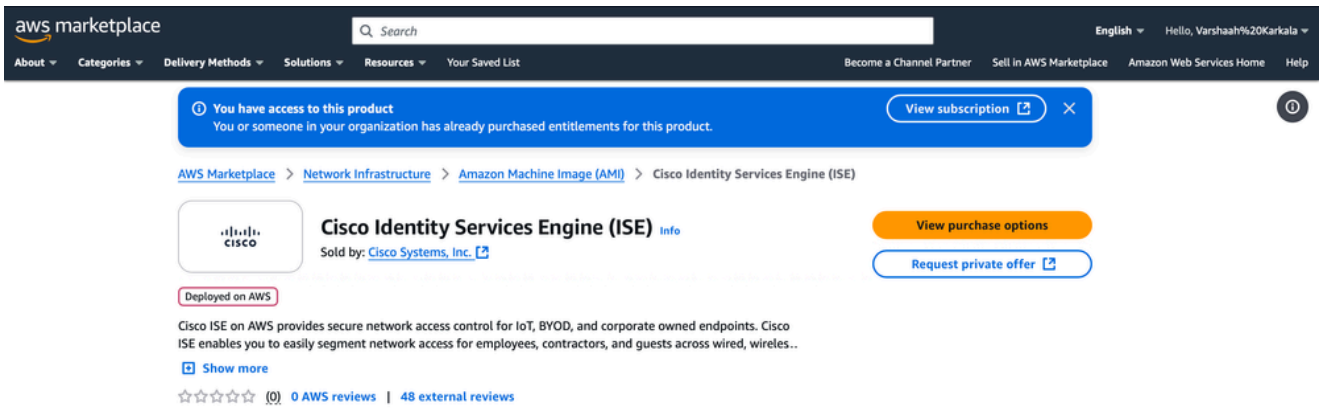
Deel 3: ISE configureren met Amazon Machine Image (AMI)

1. Log in op de AWS Management Console en zoek naar AWS Marketplace-abonnementen.
2. Typ in de zoekbalk "cisco ise" en selecteer Cisco Identity Services Engine (ISE) uit de resultaten.

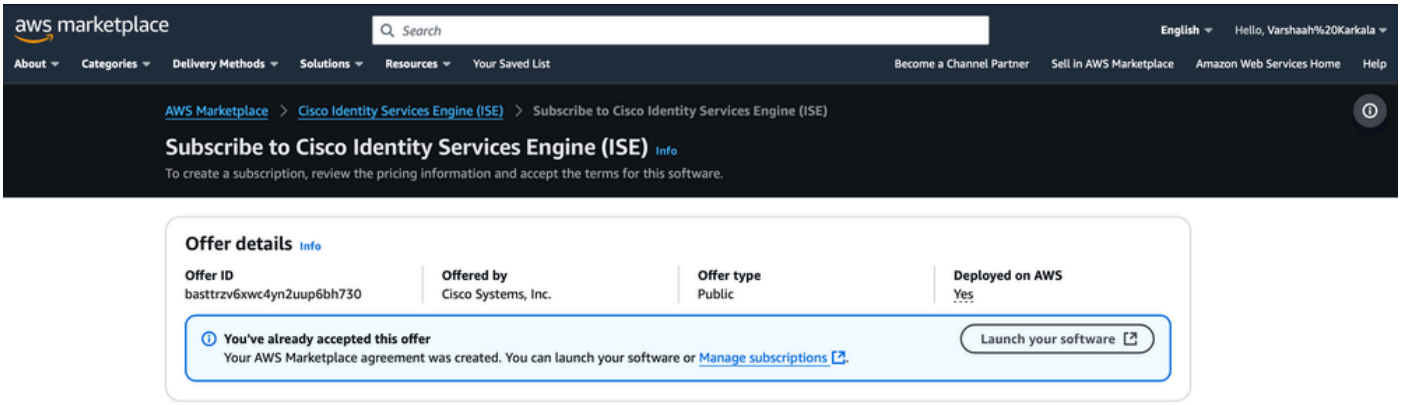


ISE op AWS Marktplaats

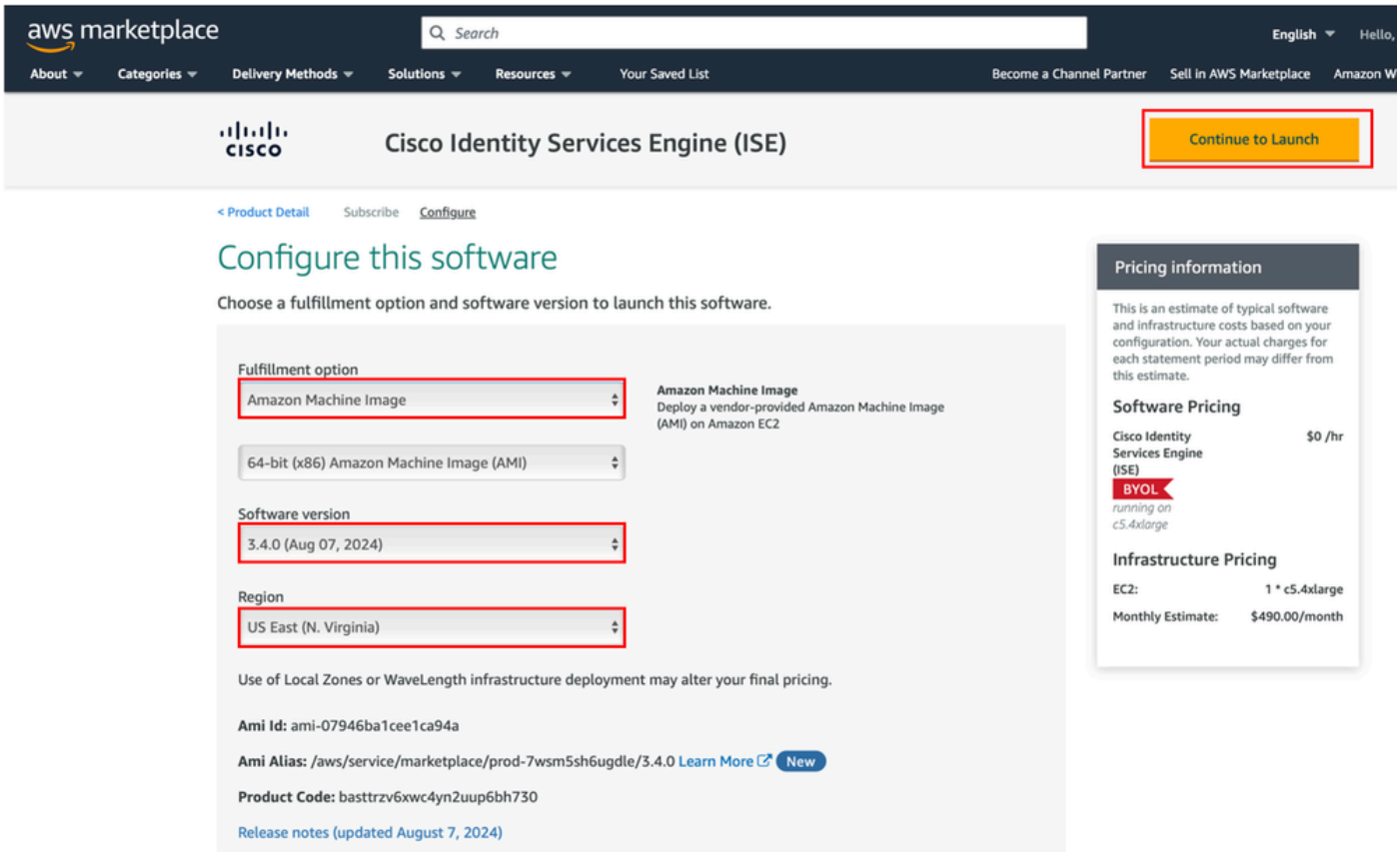
3. Klik op Aankoopopties bekijken.



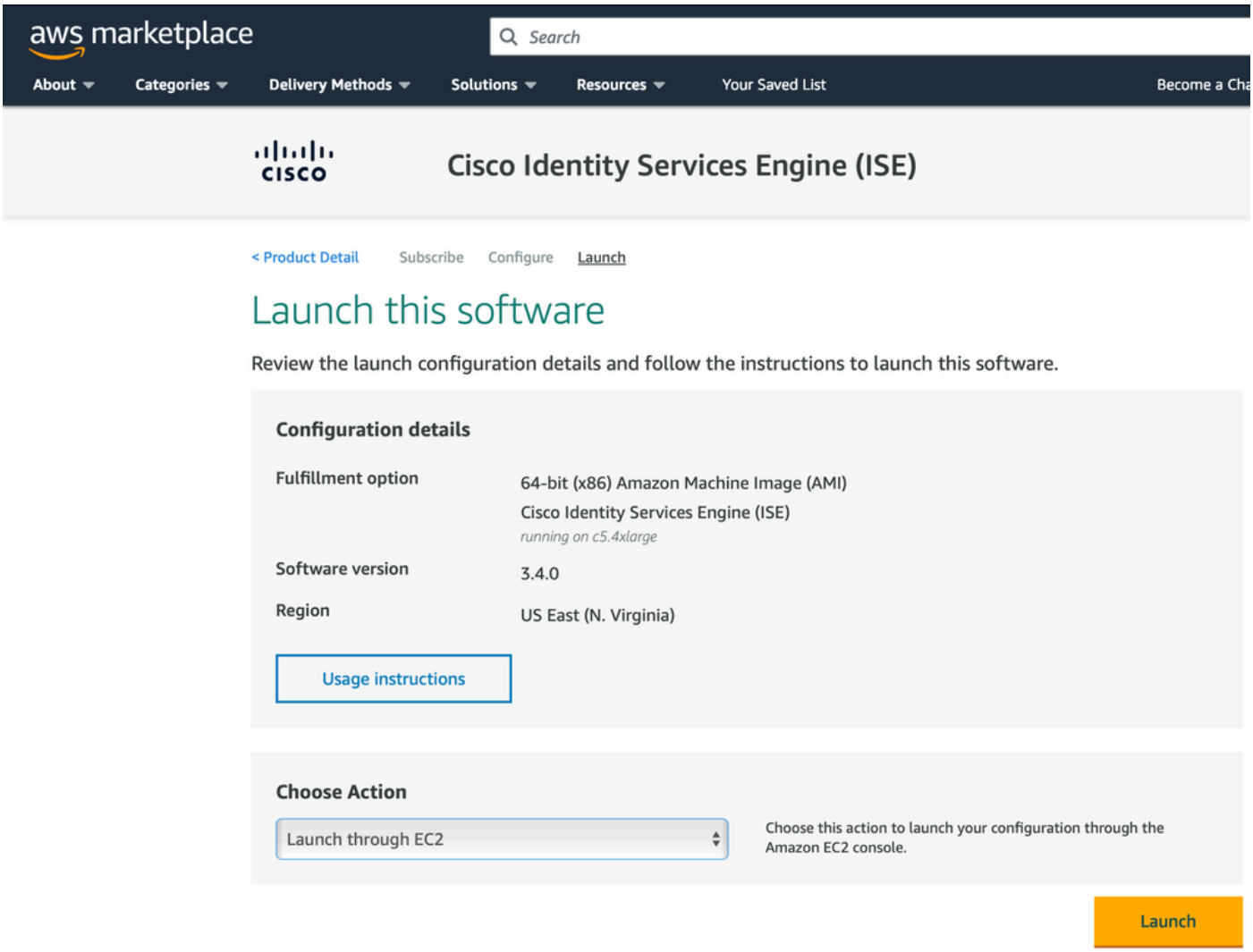
4. Klik op Software starten.



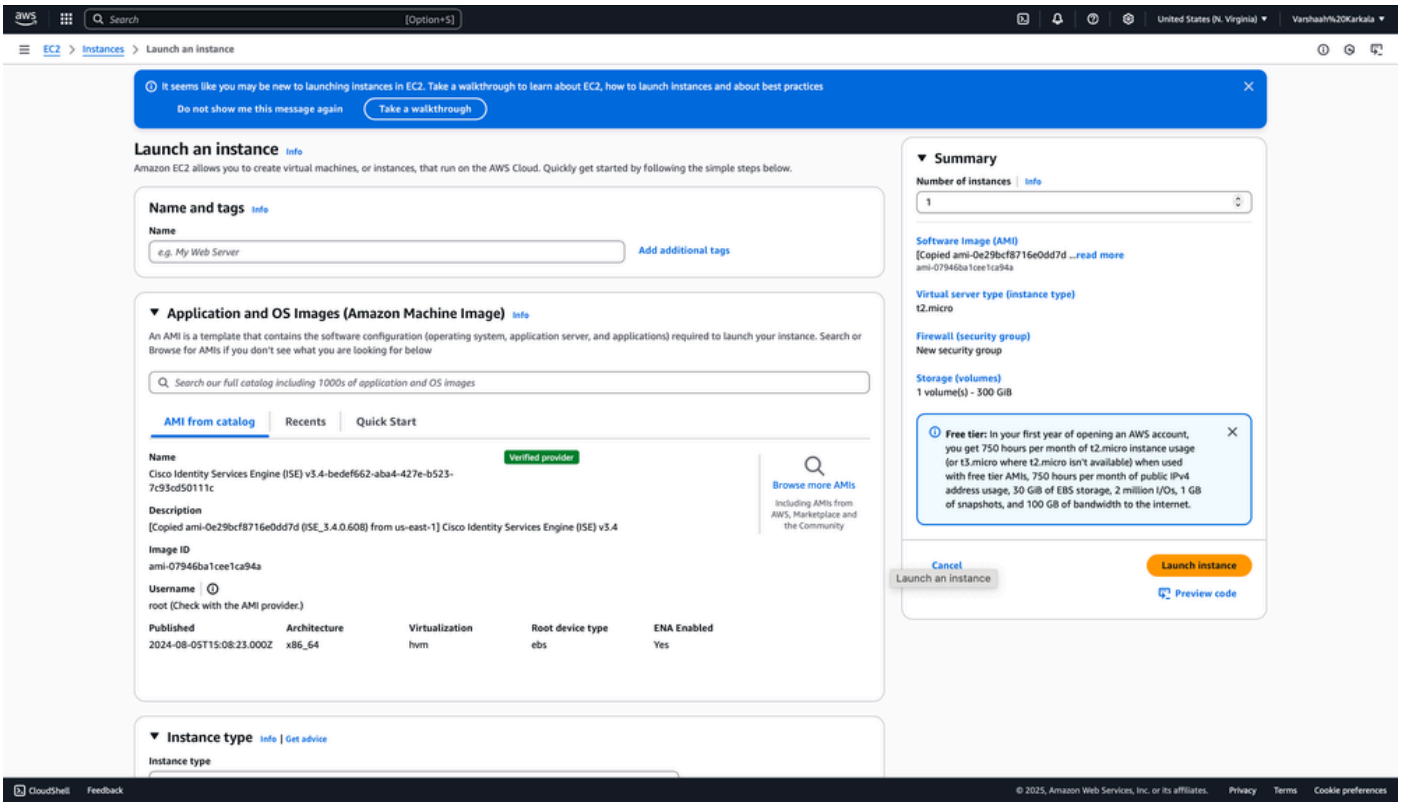
5. Kies onder de Fulfillment Option de optie Amazon Machine Image. Selecteer de gewenste softwareversie en AWS-regio en klik op Doorgaan om te starten.



6. Selecteer in de vervolgkeuzelijst Kies actie de optie Starten via EC2 en klik vervolgens op Starten om door te gaan.



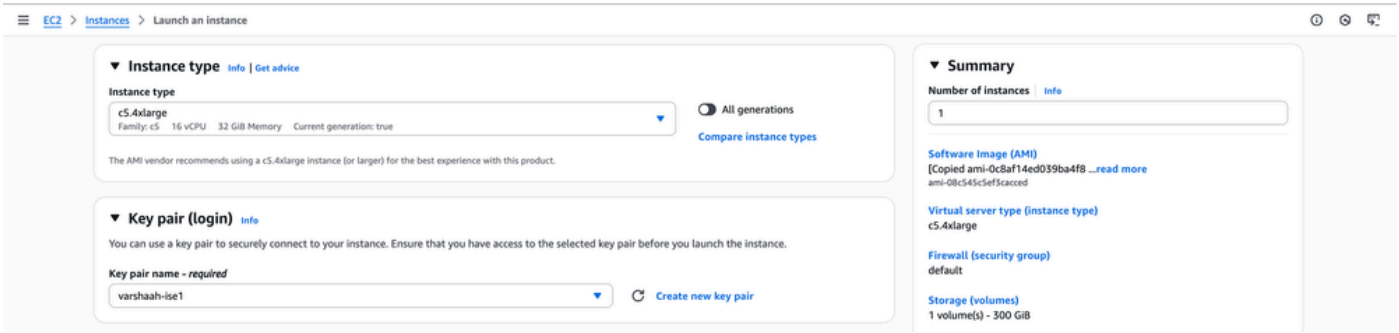
7. U wordt doorgestuurd naar de pagina EC2 Een instantie starten om uw instellingen voor de instantie te configureren.



8. Blader omlaag naar het gedeelte Instantietype en kies een geschikt instantietype op basis van uw implementatievereisten.

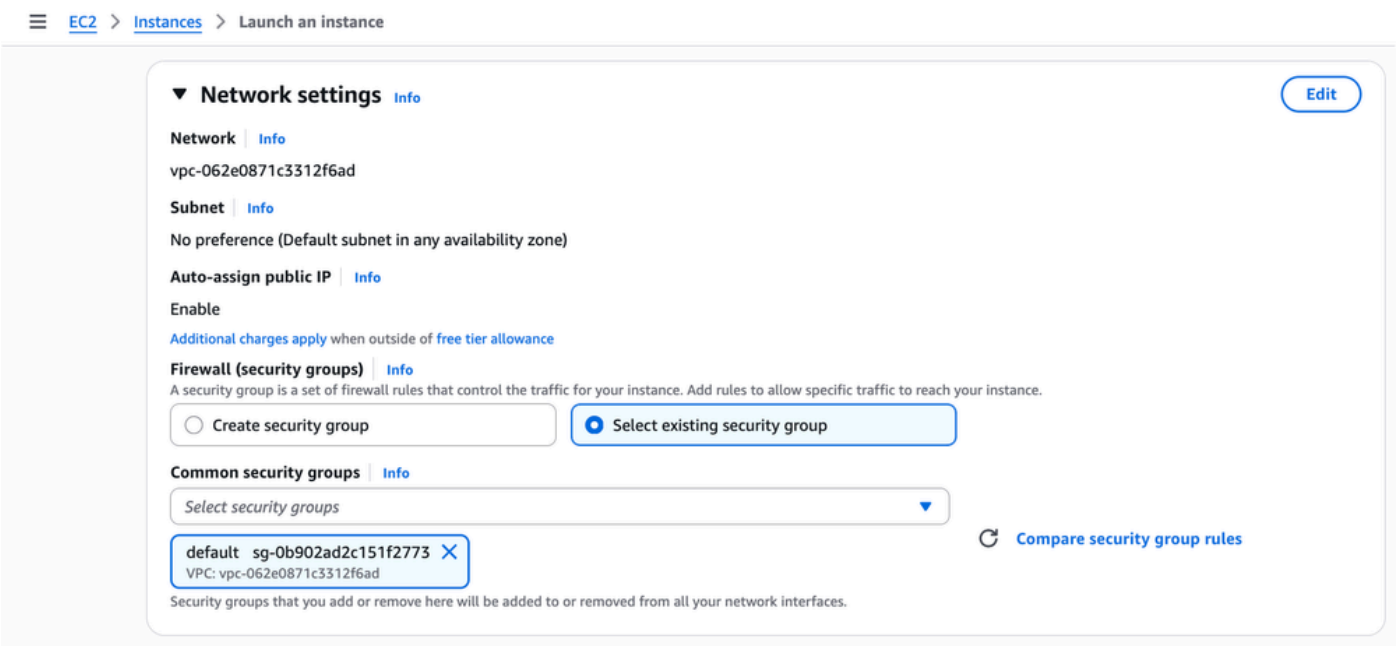
Selecteer onder Sleutelpaar (inloggen) het sleutelpaar dat eerder is gegenereerd of maak een nieuw paar (raadpleeg de eerder verstrekte stappen voor het maken van sleutelparen).

Stel het aantal instanties in op 1.



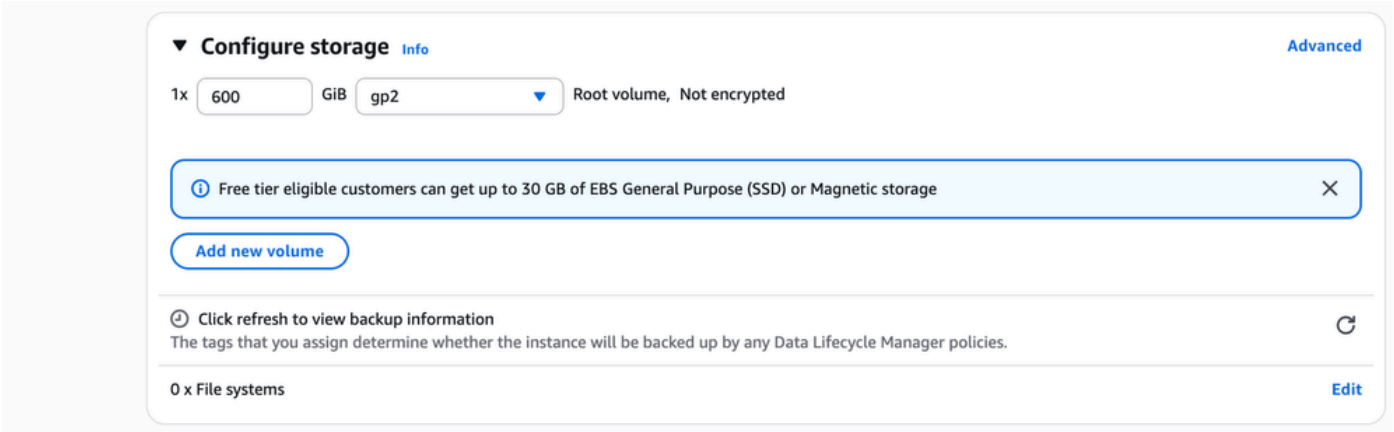
9. In het gedeelte Netwerkinstellingen:

- Configureer uw VPC en subnet indien nodig.
- Voor de beveiligingsgroep selecteert u een bestaande groep of maakt u een nieuwe groep (zoals in het voorbeeld wordt getoond).



10. Configureer in het gedeelte Opslag configureren de gewenste volumegrootte.

Voorbeeld: 600 GiB met gp2-volumetype.



11. Configureer in het gedeelte Geavanceerde details eventuele aanvullende instellingen die nodig zijn voor uw implementatie, zoals IAM-instantieprofiel, gebruikersgegevens of afsluitgedrag.

▼ **Advanced details** Info

Domain join directory | Info

Select ▼ Create new directory

IAM instance profile | Info

Select ▼ Create new IAM profile

Hostname type | Info

IP name ▼

DNS Hostname | Info

- Enable IP name IPv4 (A record) DNS requests
- Enable resource-based IPv4 (A record) DNS requests
- Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | Info

Default ▼

Shutdown behavior | Info

Stop ▼

Stop - Hibernate behavior | Info

Disable ▼

Termination protection | Info

Disable ▼

Stop protection | Info

Select ▼

Detailed CloudWatch monitoring | Info

Disable ▼

Credit specification | Info

Standard ▼

Placement group | Info

Select ▼ Create new placement group

EBS-optimized instance | Info

Disable ▼

Instance bandwidth configuration | Info

Default ▼

Purchasing option | Info

- (●) None
- ( ) Capacity Blocks
  Launch instances for your active capacity blocks
- ( ) Spot instances
  Request Spot Instances at the Spot price, capped at the On-Demand price

Capacity reservation | Info

None ▼

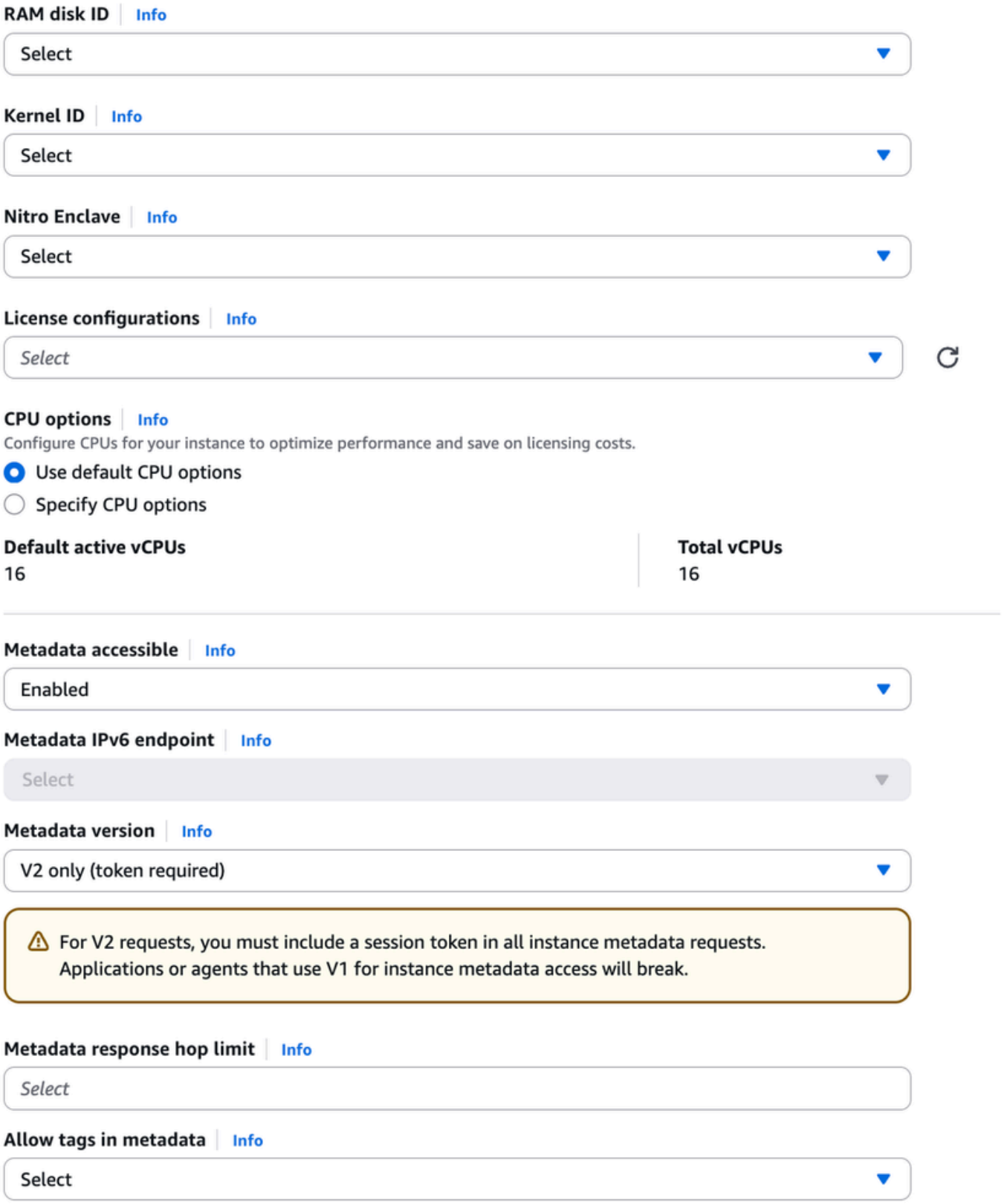
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12. In de sectie Metagegevensversie:

- Voor ISE versie 3.4 en hoger selecteert u alleen V2 (token vereist) — dit is de aanbevolen optie.
- Voor ISE-versies die ouder zijn dan 3.4, kiest u V1 en V2 (token optioneel) om compatibiliteit te garanderen.



13. Geef in het veld Gebruikersgegevens de initiële configuratieparameters voor de ISE-instantie op, waaronder hostnaam, DNS, NTP-server, tijdzone, ERS en beheerdersreferenties.

Voorbeeld:
hostnaam=varshahise2

Primaire naamserver=x.x.x.x

DNSdomain=varshaah.local

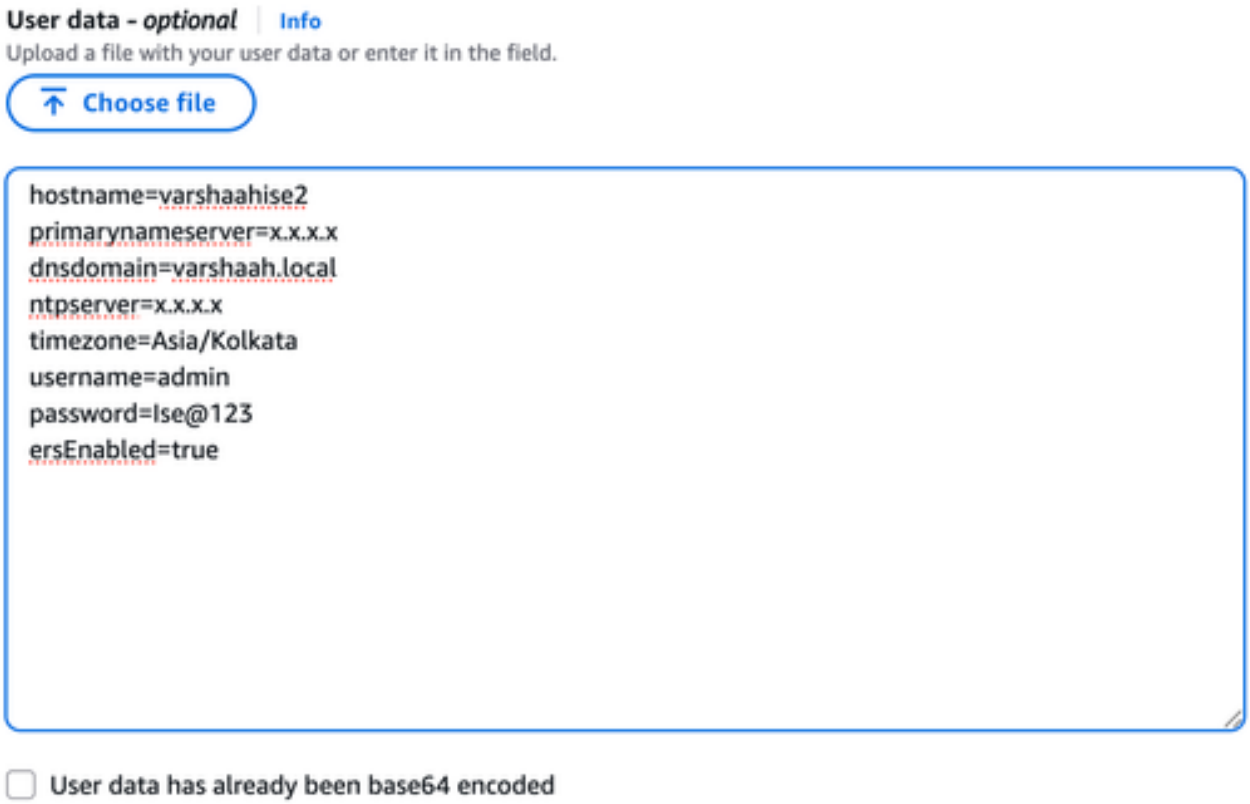
NTPserver=x.x.x.x

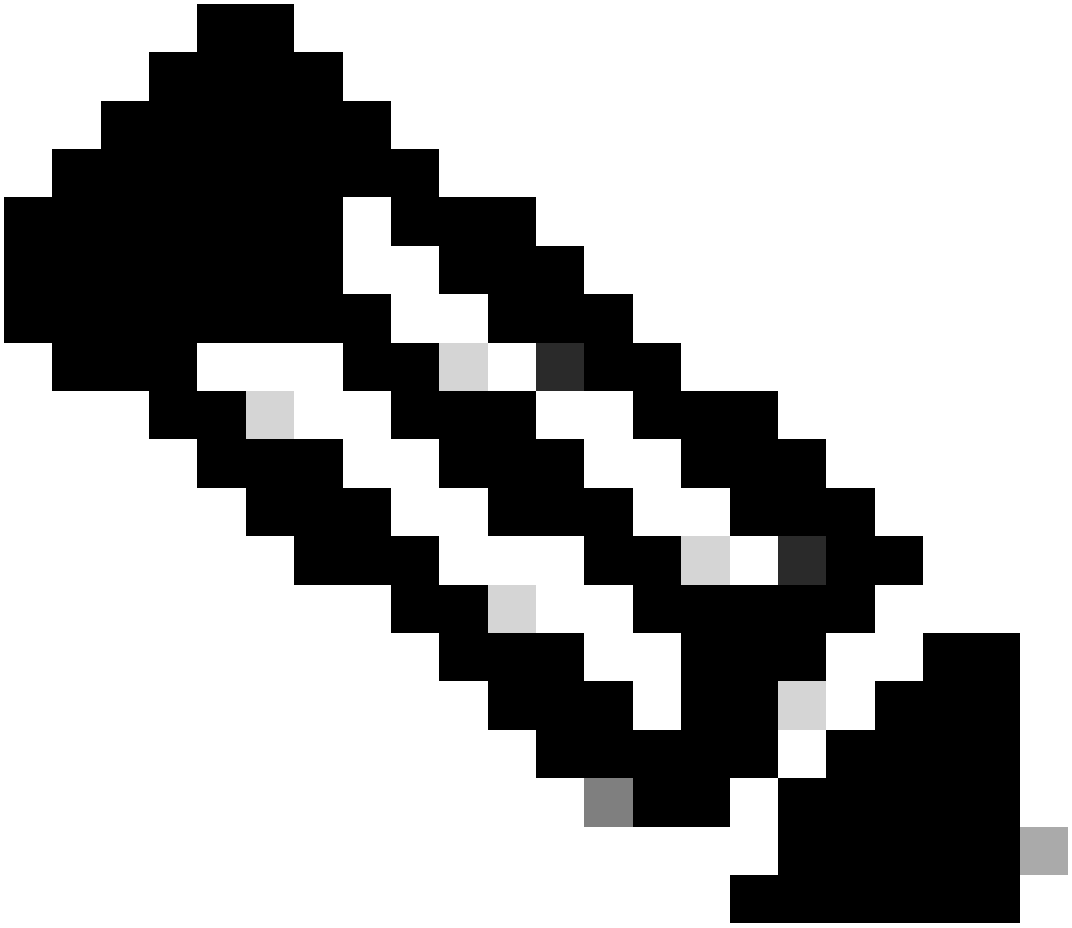
tijdzone=Azië/Kolkata

Gebruikersnaam=beheerder

Wachtwoord=Ise@123

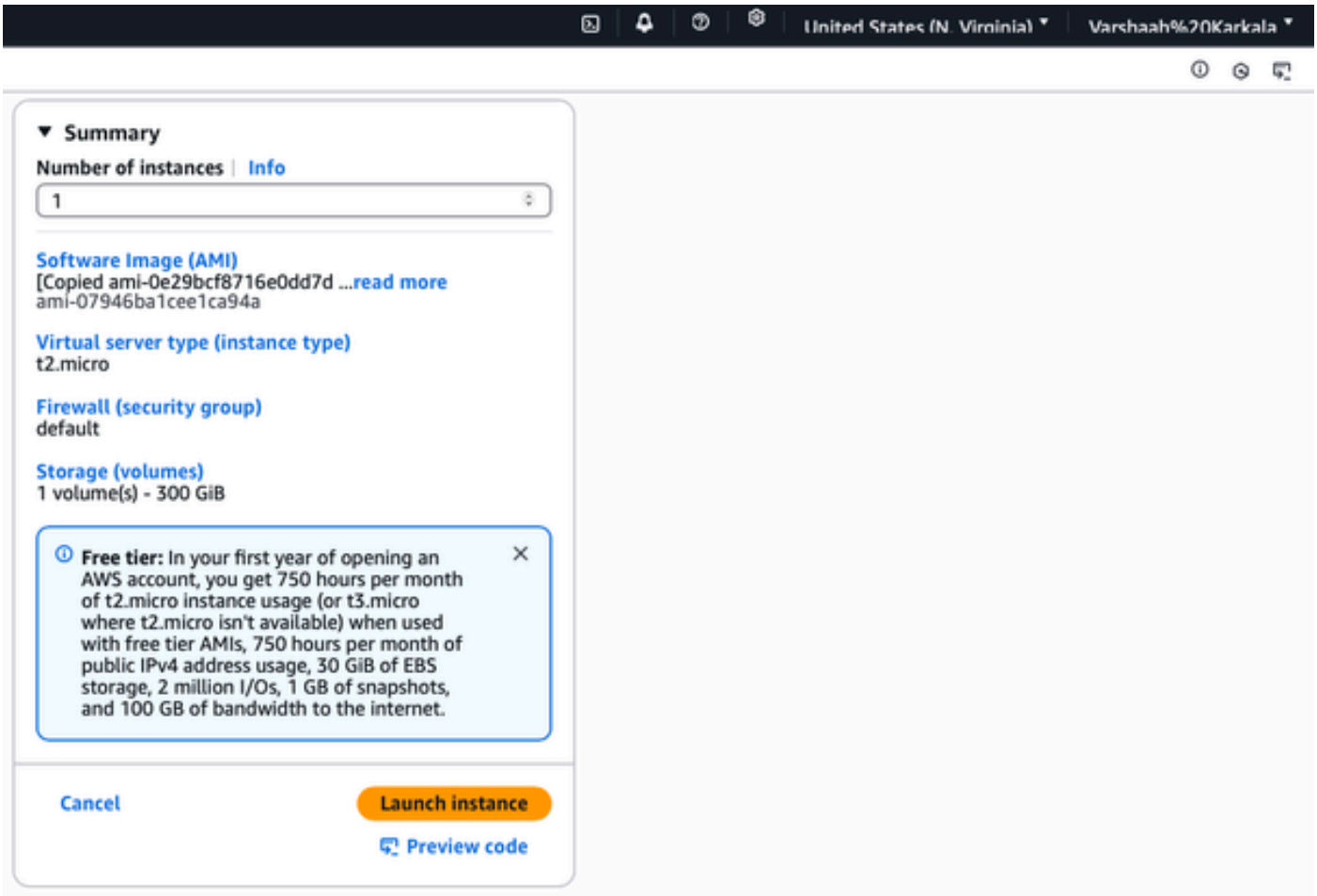
ersEnabled=true



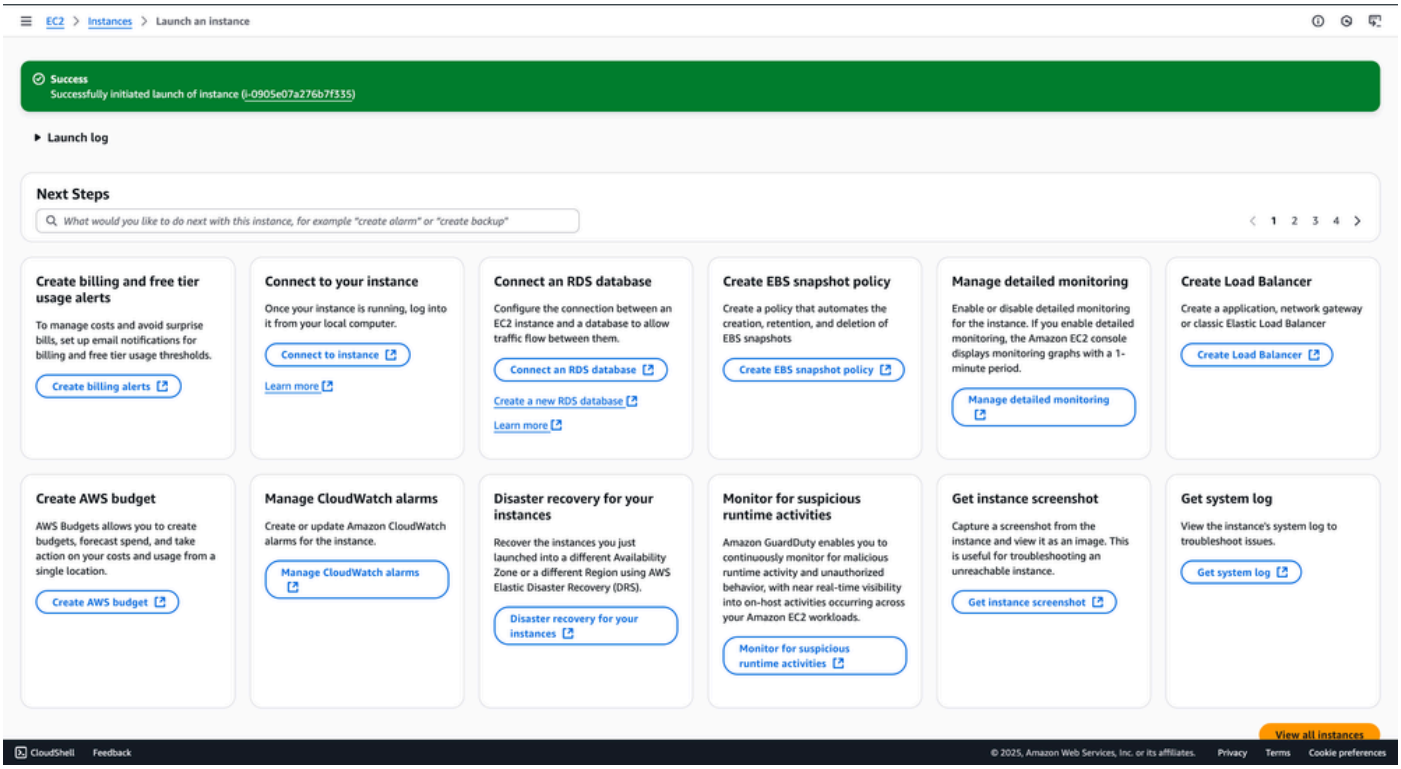


Opmerking: Controleer of het wachtwoord voldoet aan het Cisco ISE-wachtwoordbeleid.

Nadat u de gebruikersgegevens hebt ingevoerd en de configuratie hebt voltooid, klikt u op Installatie starten.



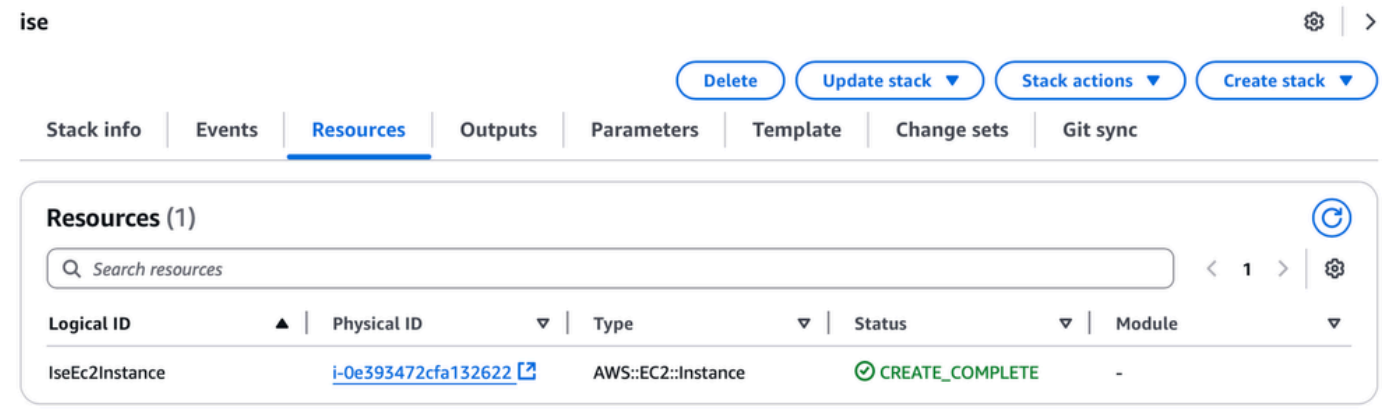
14. Nadat de instantie is gestart, wordt een bevestigingsbericht weergegeven met de vermelding: 'Opstarten van instantie <instance_name> is met succes gestart'. Dit geeft aan dat het opstartproces met succes is gestart.

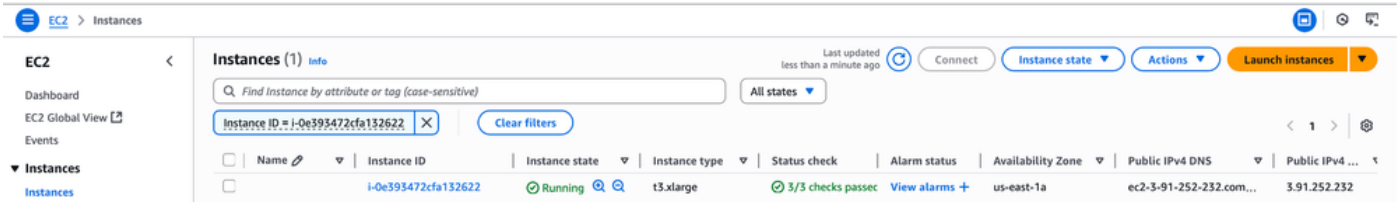


Verifiëren

Toegang tot de ISE-instantie die met CFT is gebouwd

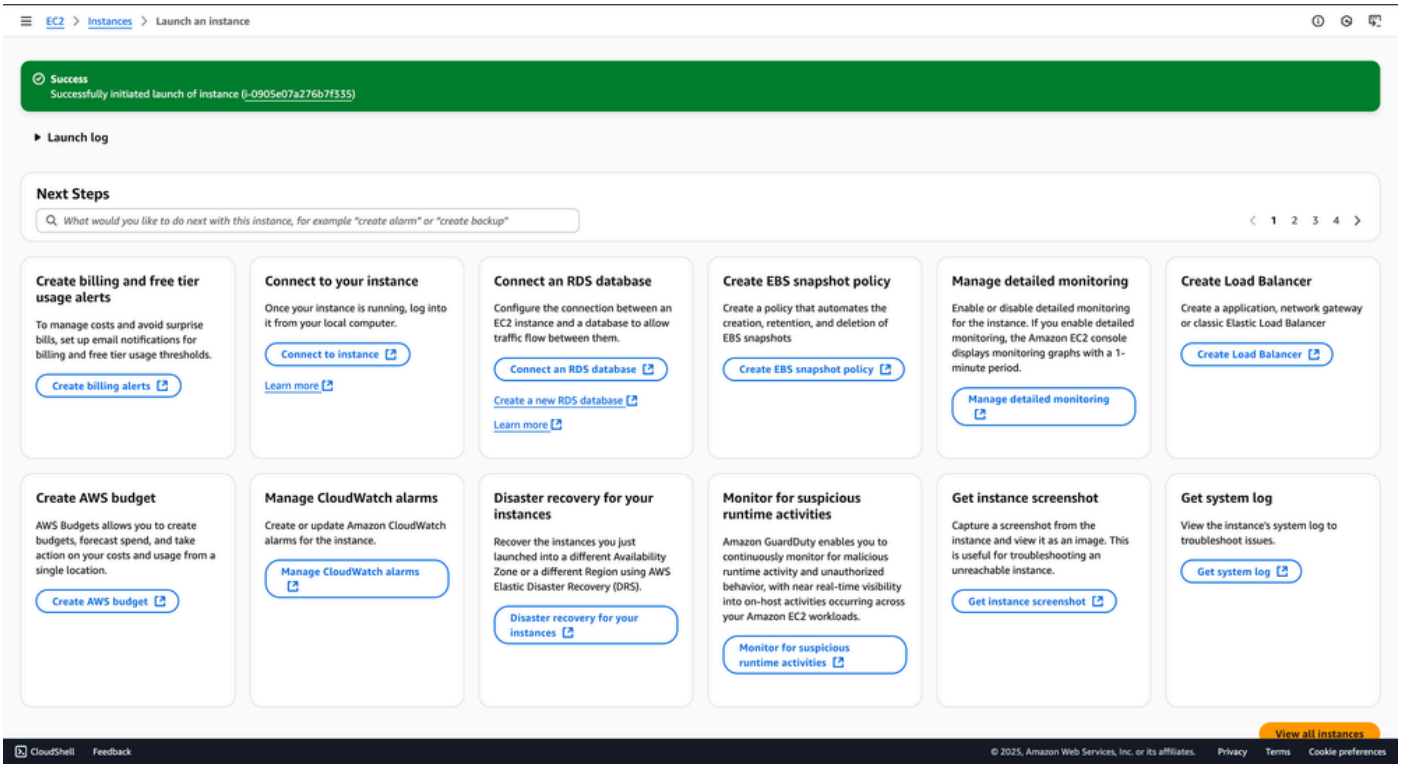
Ga naar het tabblad Bronnen in uw CloudFormation-stapel en klik op de fysieke ID. Het leidt u naar het EC2-dashboard waar u de instantie kunt zien.

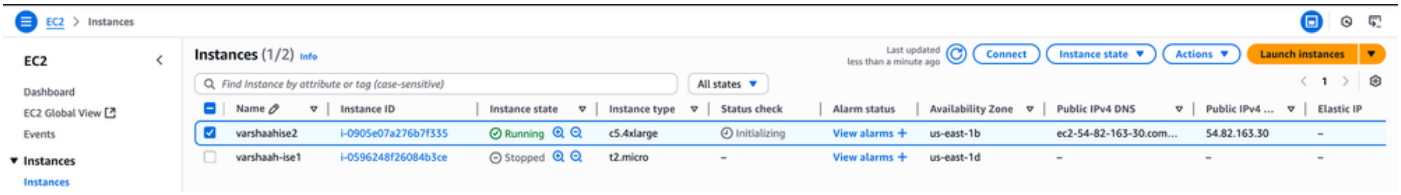




Toegang tot de ISE-instantie die is gebouwd met AMI

Klik op Alle instanties weergeven om naar de pagina EC2-instanties te gaan. Controleer op deze pagina of de statuscontrole wordt weergegeven als 3/3-controles zijn geslaagd, wat aangeeft dat de instantie up en healthy is.





Toegang tot de ISE GUI

De ISE-server is nu met succes geïmplementeerd.

Om toegang te krijgen tot de ISE GUI, moet u het IP-adres van de instantie in uw browser gebruiken. Aangezien het standaard IP-adres privé is, kan het niet rechtstreeks vanaf internet worden geopend.

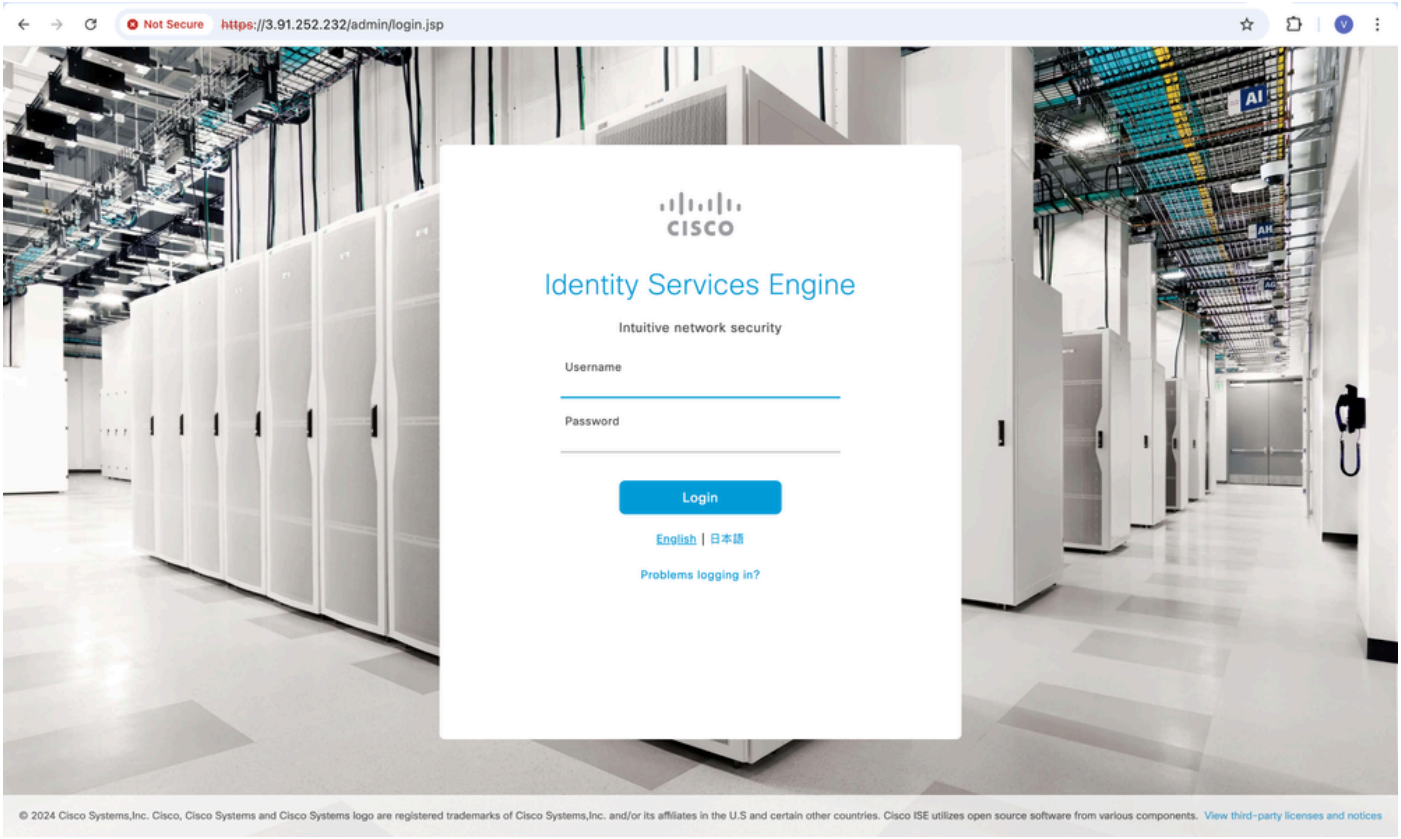
Controleer of een openbaar IP-adres aan de instantie is gekoppeld:

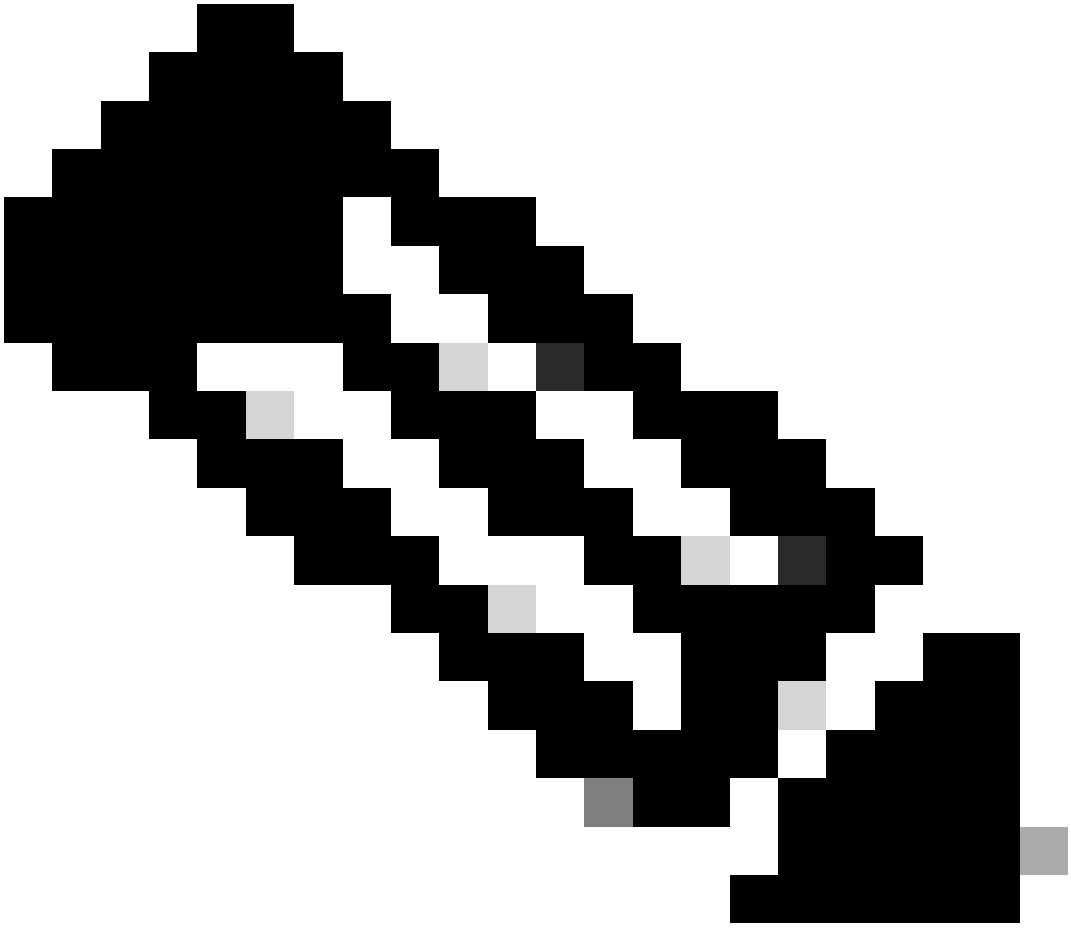
- Navigeer naar EC2 > Instanties en selecteer uw instantie.
- Zoek het veld Openbaar IPv4-adres.

Hier kunnen we een openbaar IP-adres zien dat u kunt gebruiken om toegang te krijgen tot de ISE GUI.

Open een ondersteunde browser (bijvoorbeeld Chrome of Firefox) en voer het openbare IP-adres in.

De ISE GUI-aanmeldingspagina wordt weergegeven.





Opmerking: Nadat SSH-toegang beschikbaar is, duurt het doorgaans 10-15 minuten extra voordat ISE-services volledig zijn overgeschakeld naar een actieve status.

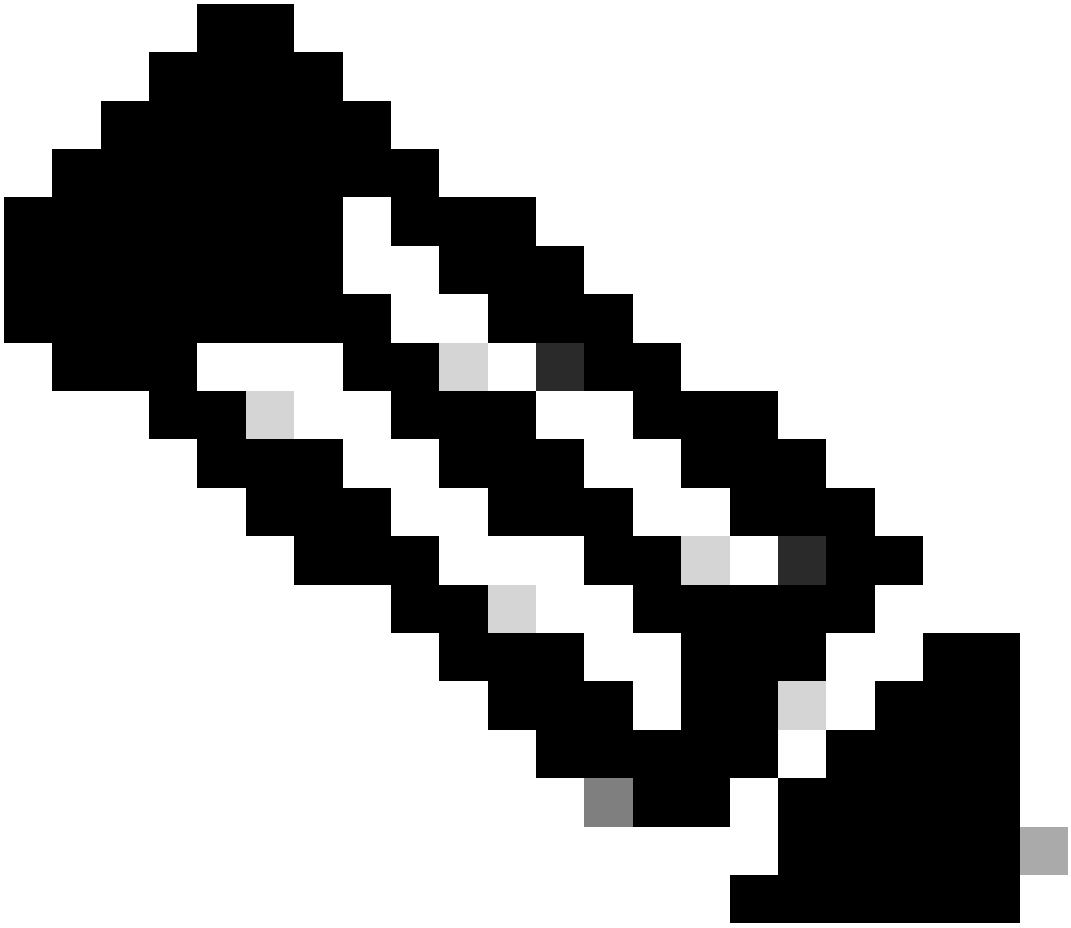
Toegang tot CLI via SSH vanaf terminal

Selecteer in de EC2-console uw exemplaar en klik op Verbinden.

Volg de volgende stappen op het tabblad SSH-client:

- Navigeer naar de map met uw gedownloade .pem-sleutelbestand.
- Voer de volgende opdrachten uit:

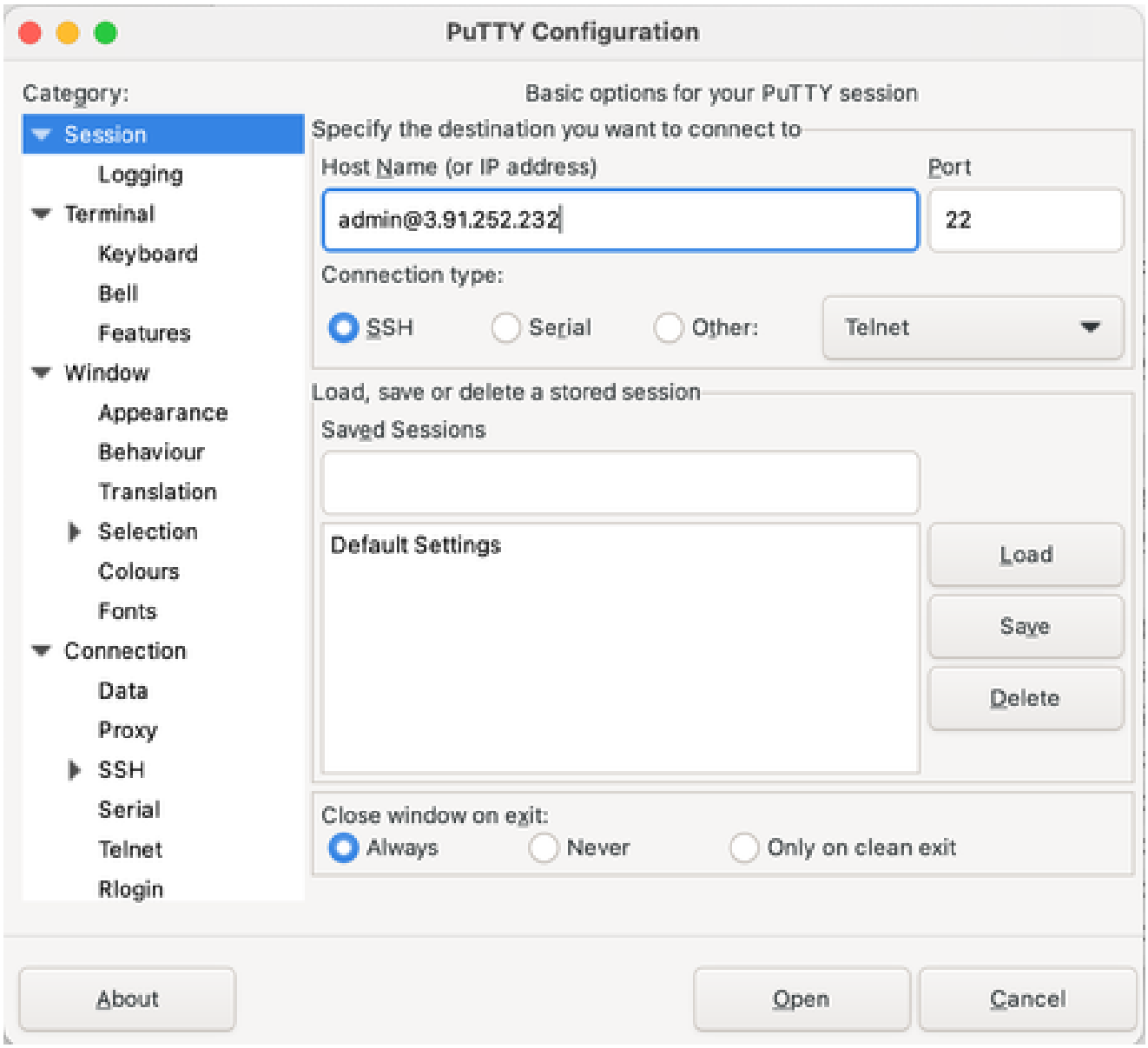
- cd <path-to-key-file>
- chmod 400 <your-key-pair-name>.pem
- ssh -i "<your-key-pair-name>.pem" admin@<public-ip-address>



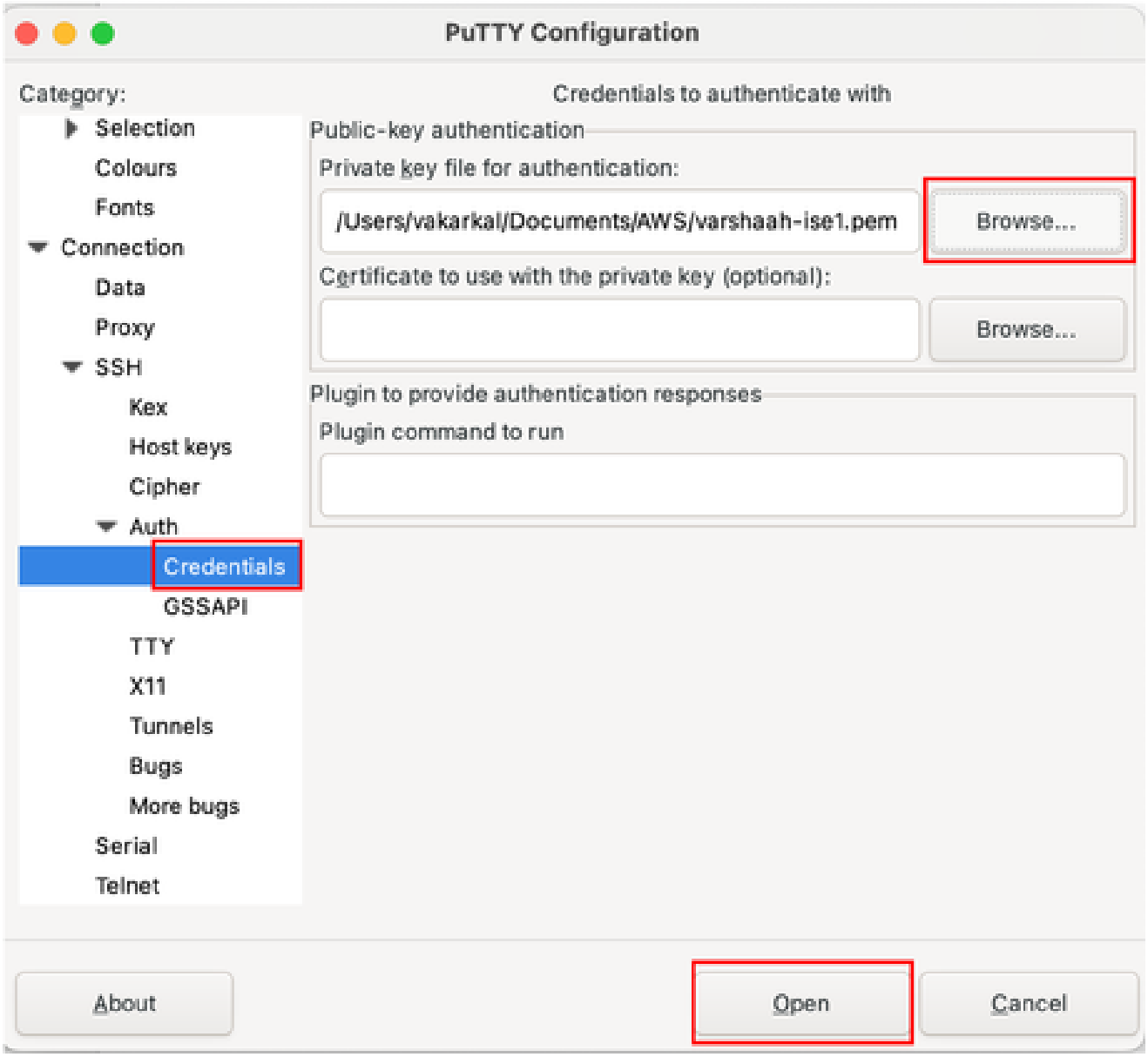
Opmerking: gebruik admin als de SSH-gebruiker, omdat Cisco ISE root login via SSH uitschakelt.

CLI openen via SSH met PuTTy

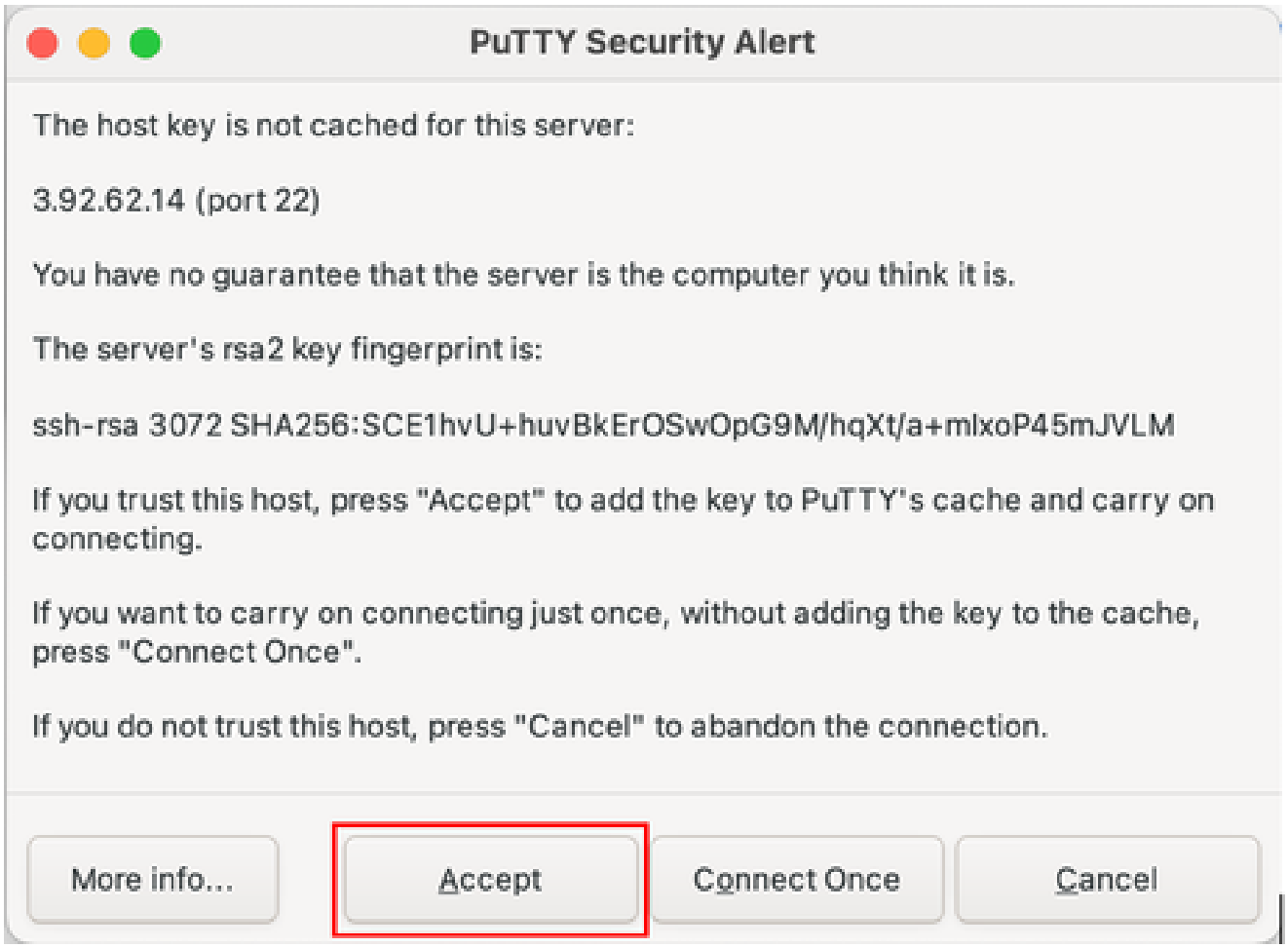
- Open PuTTY.
- Voer in het veld Hostnaam het volgende in: admin@<public-ip-address>



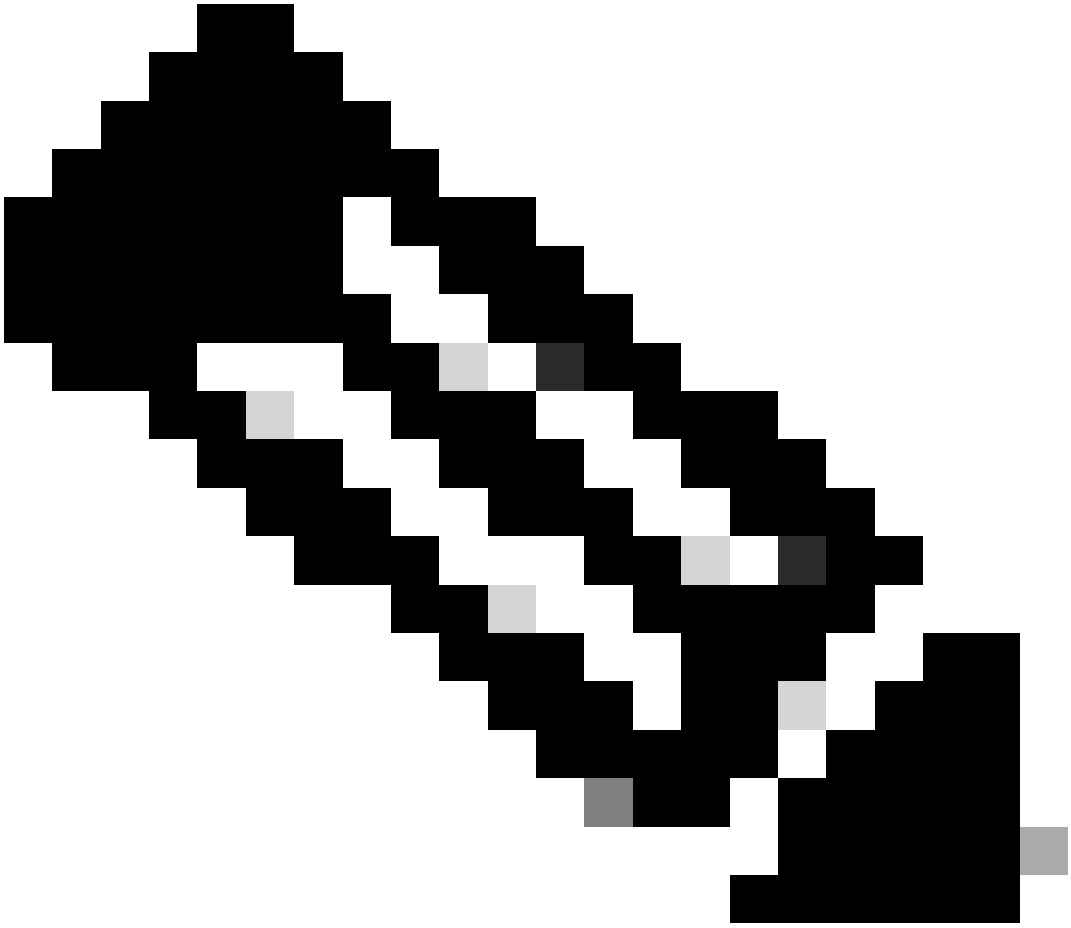
- Navigeer in het linkerdeelvenster naar Verbinding > SSH > Auth > Credentials.
- Klik op Bladeren naast Privésleutelbestand voor verificatie en selecteer het bestand met uw SSH-privésleutel.
- Klik op Openen om de sessie te starten.



- Klik op Accepteren om de SSH-sleutel te bevestigen.



- Uw PuTTY-sessie maakt nu verbinding met de ISE CLI.

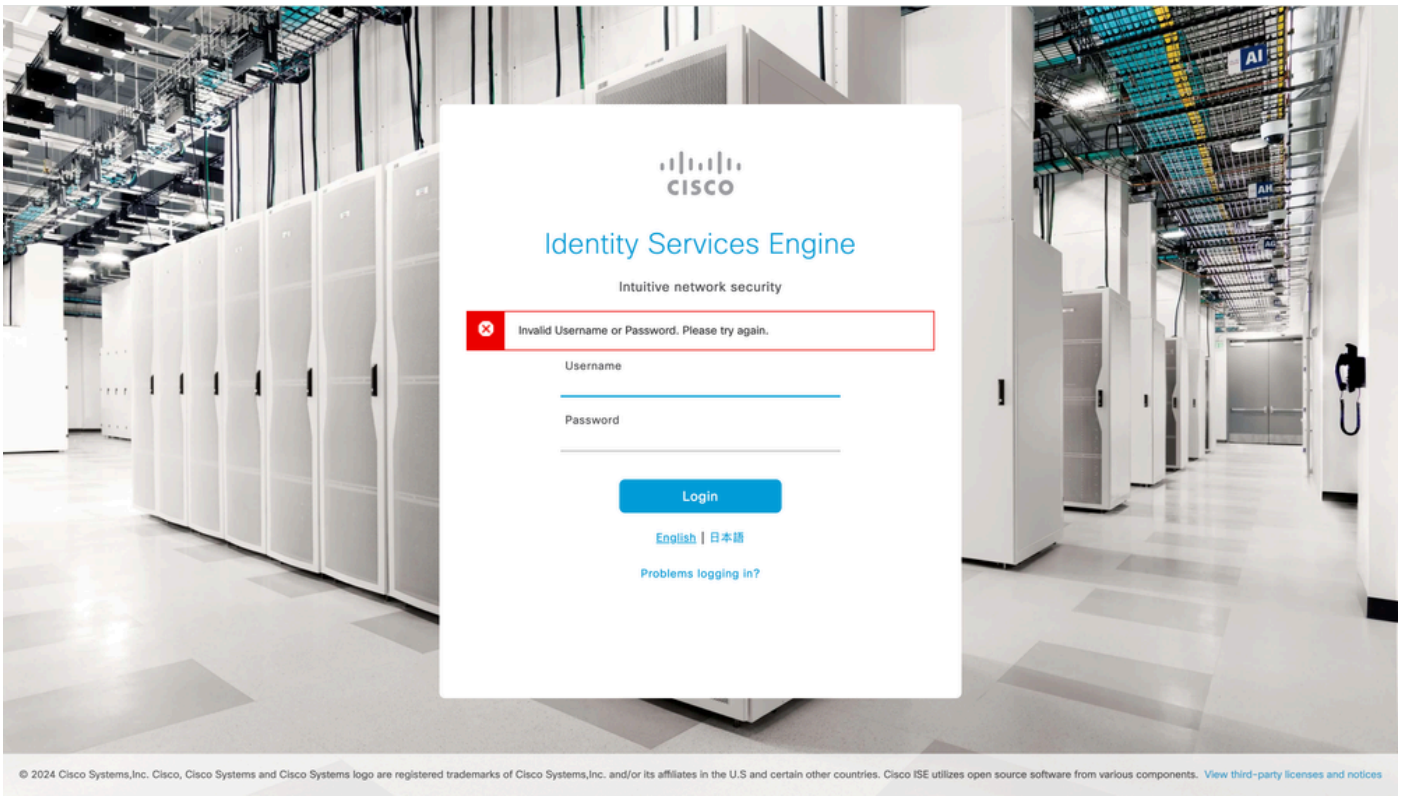


Opmerking: het kan tot 20 minuten duren voordat ISE via SSH toegankelijk is. Gedurende deze tijd kunnen verbindingspogingen mislukken met de fout: "Toestemming geweigerd (public key)."

Problemen oplossen

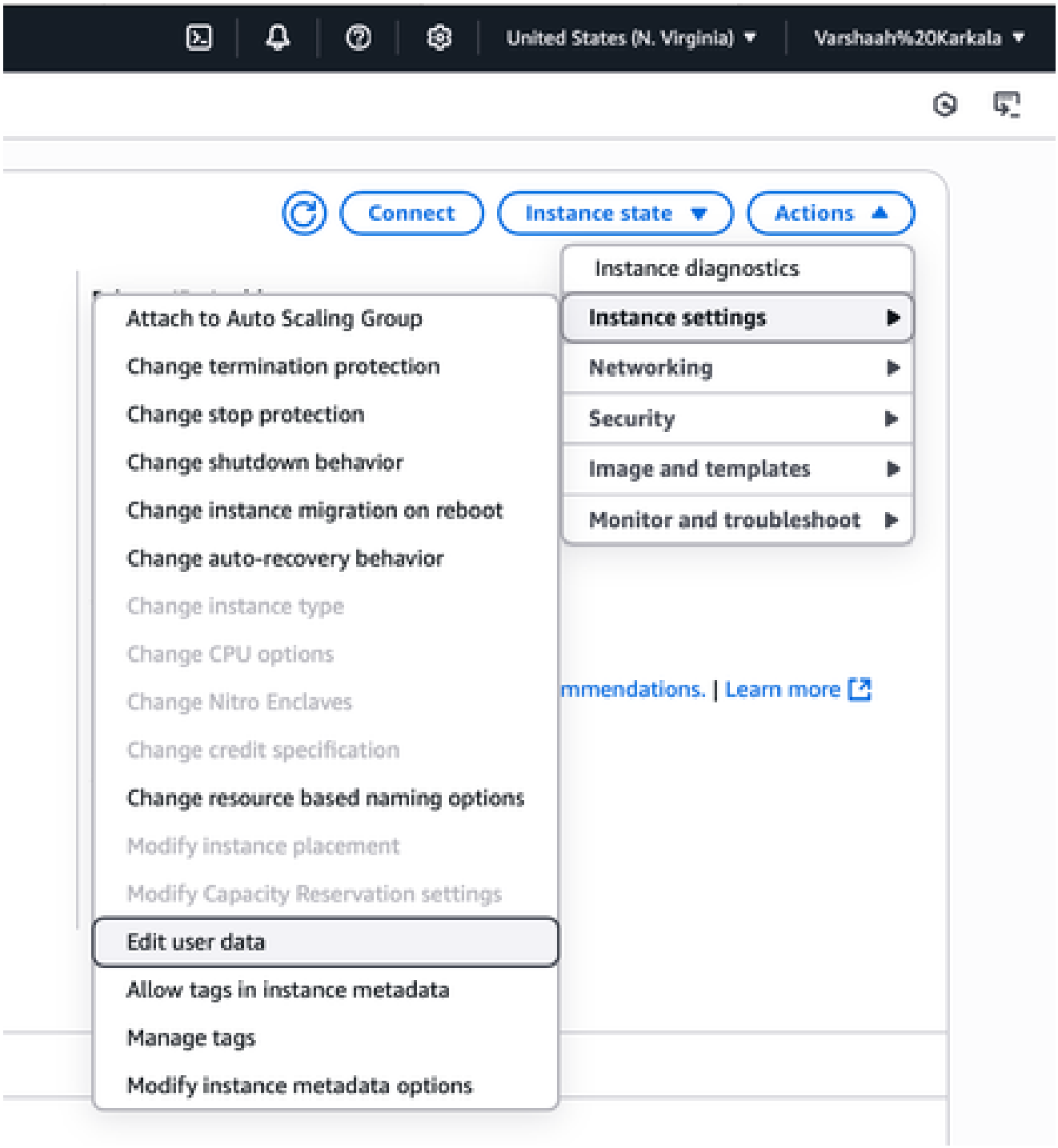
Ongeldige gebruikersnaam of wachtwoord

Authenticatieproblemen worden vaak veroorzaakt door onjuiste gebruikersinvoer tijdens het maken van de instantie. Dit resulteert in een foutmelding als "Ongeldige gebruikersnaam of wachtwoord. Probeer het opnieuw." fout bij het aanmelden bij de GUI.

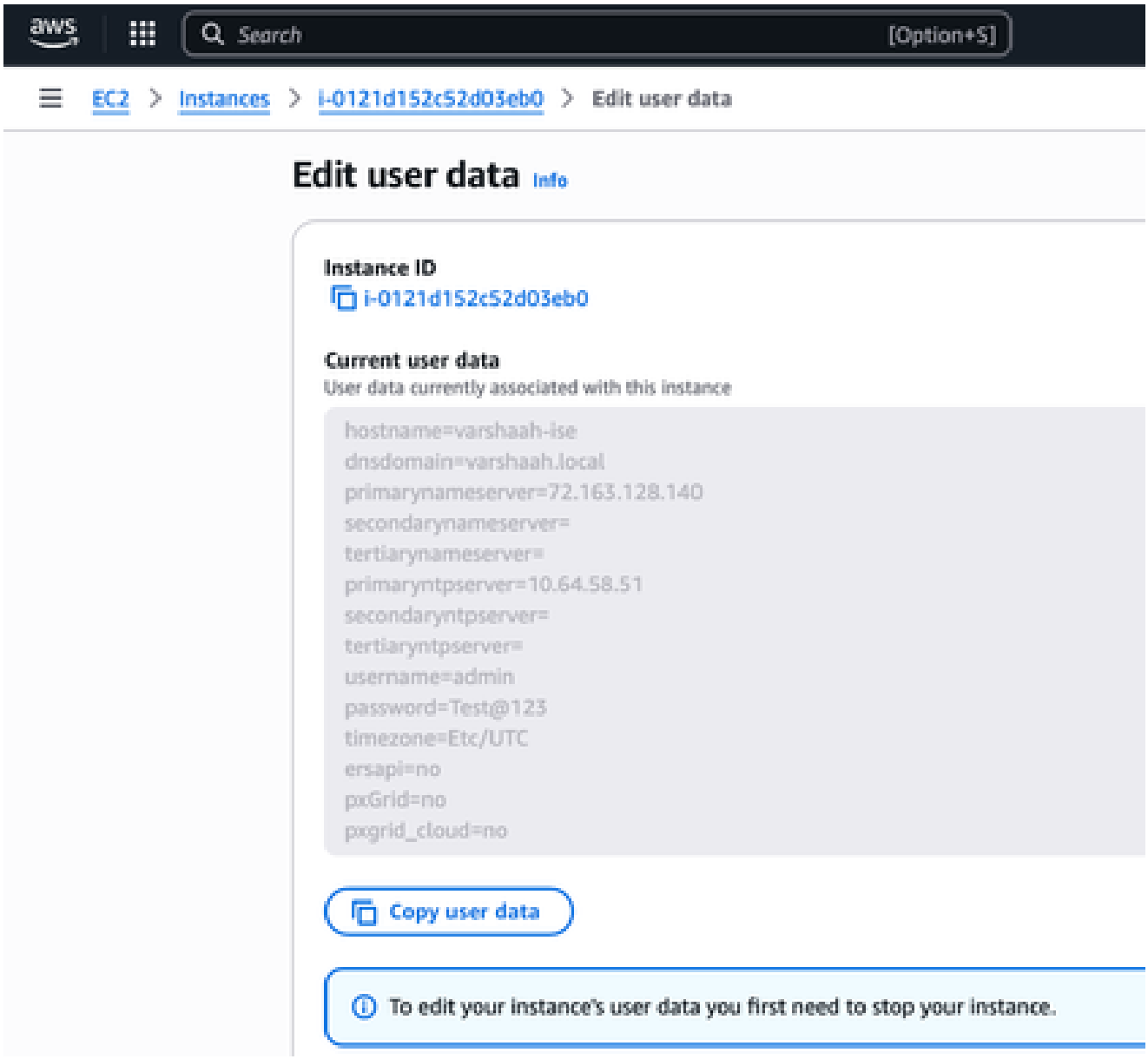


Oplossing

- Navigeer in de AWS EC2-console naar EC2 > Instanties > your_instance_id
- Klik op Acties > Instellingen instantie > Gebruikersgegevens bewerken.



- U kunt hier de specifieke gebruikersnaam en het wachtwoord vinden die zijn ingesteld tijdens het starten van de instantie. Deze referenties kunnen worden gebruikt om in te loggen op de ISE GUI.



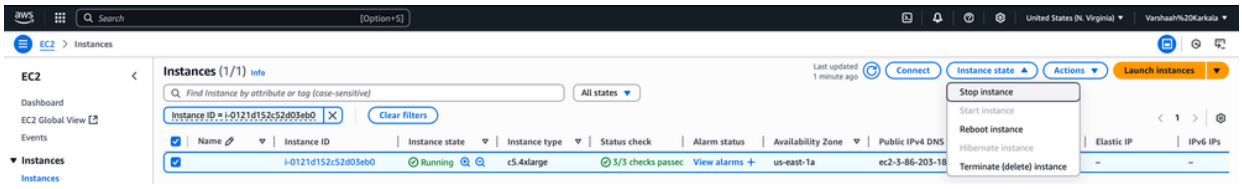
- Controleer Hostnaam en wachtwoord bij het instellen van de hostnaam en het wachtwoord:
  - Hostnaam
    - Alleen alfanumerieke tekens en koppeltekens (-) zijn toegestaan.
    - De lengte mag niet meer dan 19 tekens bedragen.
  - wachtwoord
    - Moet voldoen aan het Cisco ISE-wachtwoordbeleid.
    - Raadpleeg de officiële ISE Admin Guide: ISE 3.4 Password Policy – Cisco Admin Guide

- Als het geconfigureerde wachtwoord niet voldoet aan het ISE-wachtwoordbeleid, mislukken de aanmeldingspogingen; zelfs met de juiste referenties.

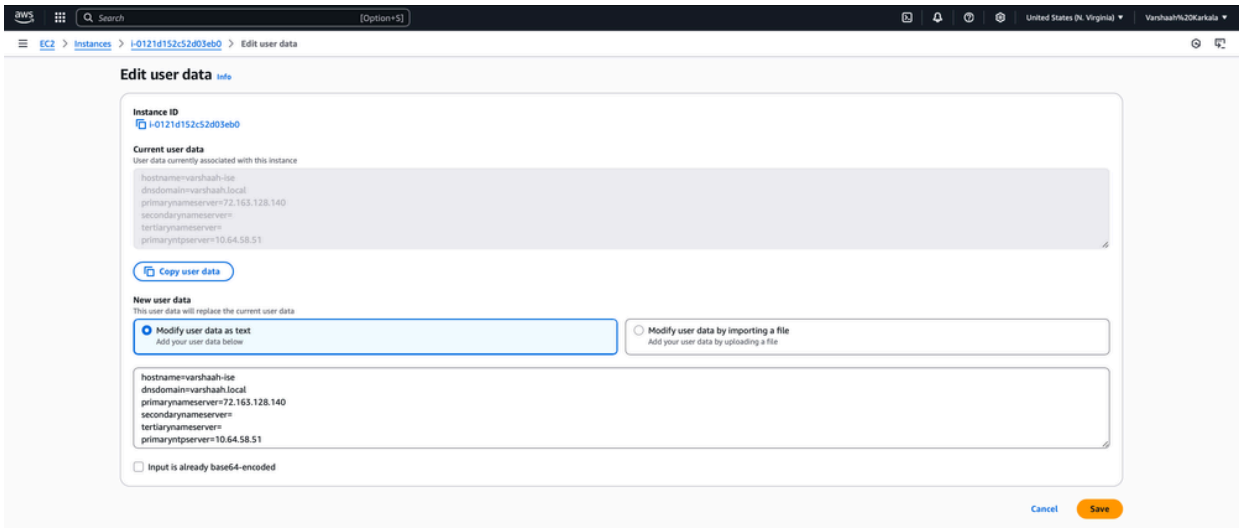
- Als u vermoedt dat het wachtwoord verkeerd is geconfigureerd, volgt u deze stappen om het bij te werken:

    1. Ga in de EC2-console naar EC2 > Instanties > your_instance_id

    2. Klik op Instantietoestand > Stopinstantie.



    3. Nadat de instantie is gestopt, klikt u op Acties > Instellingen instantie > Gebruikersgegevens bewerken.



    4. Wijzig het gebruikersgegevensscript om het wachtwoord dienovereenkomstig bij te werken.

    5. Sla uw wijzigingen op en start de instantie vervolgens opnieuw op via Instantiestaat > Start.

Bekende gebreken

Bug-ID	Beschrijving
Cisco Bug ID 41693	ISE op AWS kan geen gebruikersgegevens ophalen als de metagegevensversie is ingesteld

	op "Alleen V2". Alleen IMDSv1 wordt ondersteund in versies voorafgaand aan ISE 3.4.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.