Bereitstellung der Identity Services Engine (ISE) Version 3.4 auf AWS

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Cisco ISE auf AWS mithilfe der folgenden Funktionen beschrieben:

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

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesen Themen verfügen, bevor Sie mit der Bereitstellung fortfahren:

- Cisco Identity Services Engine (ISE)
- AWS EC2 Instanzmanagement und Netzwerk

- Generierung und Verwendung von SSH-Schlüsselpaaren
- Grundlegendes Verständnis von VPCs, Sicherheitsgruppen und DNS-/NTP-Konfiguration in AWS

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

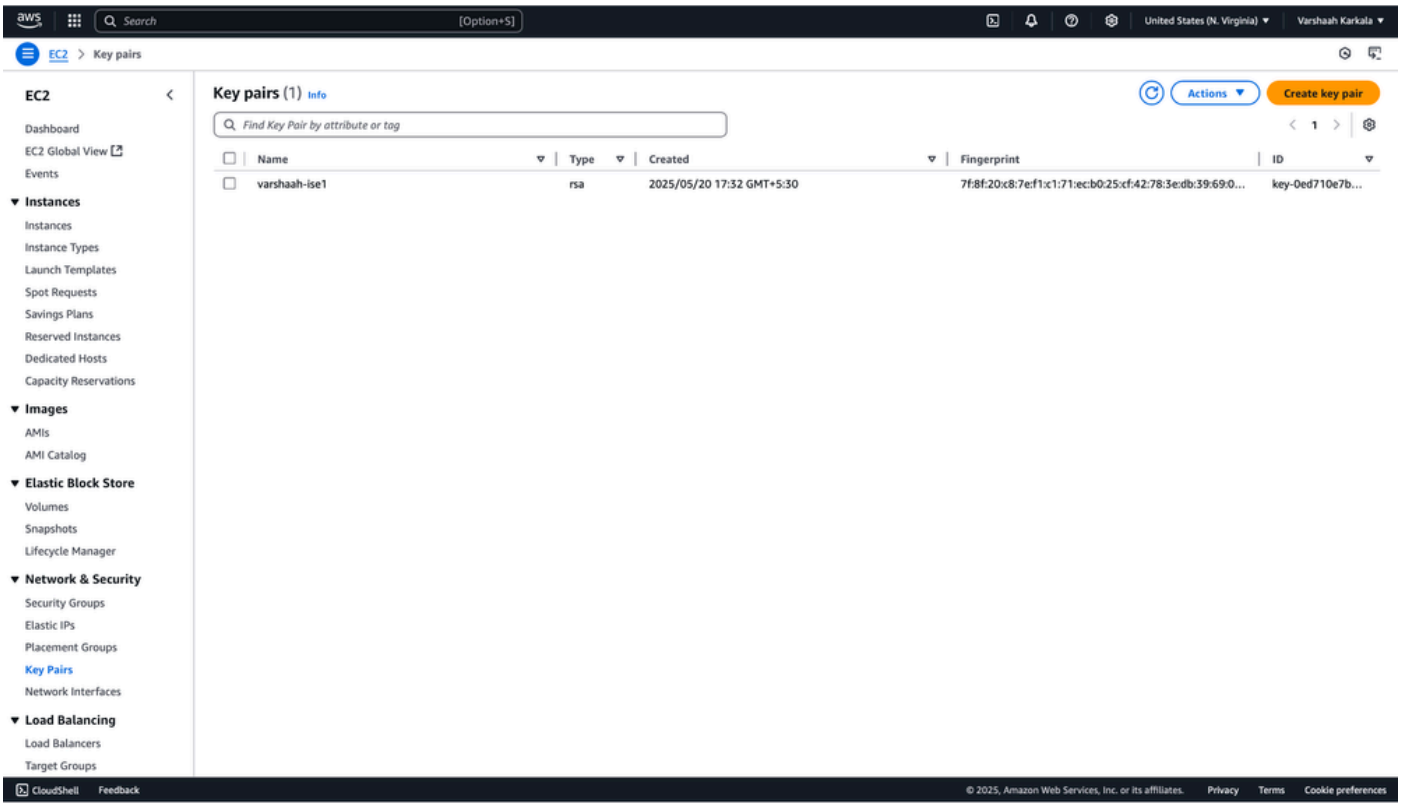
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

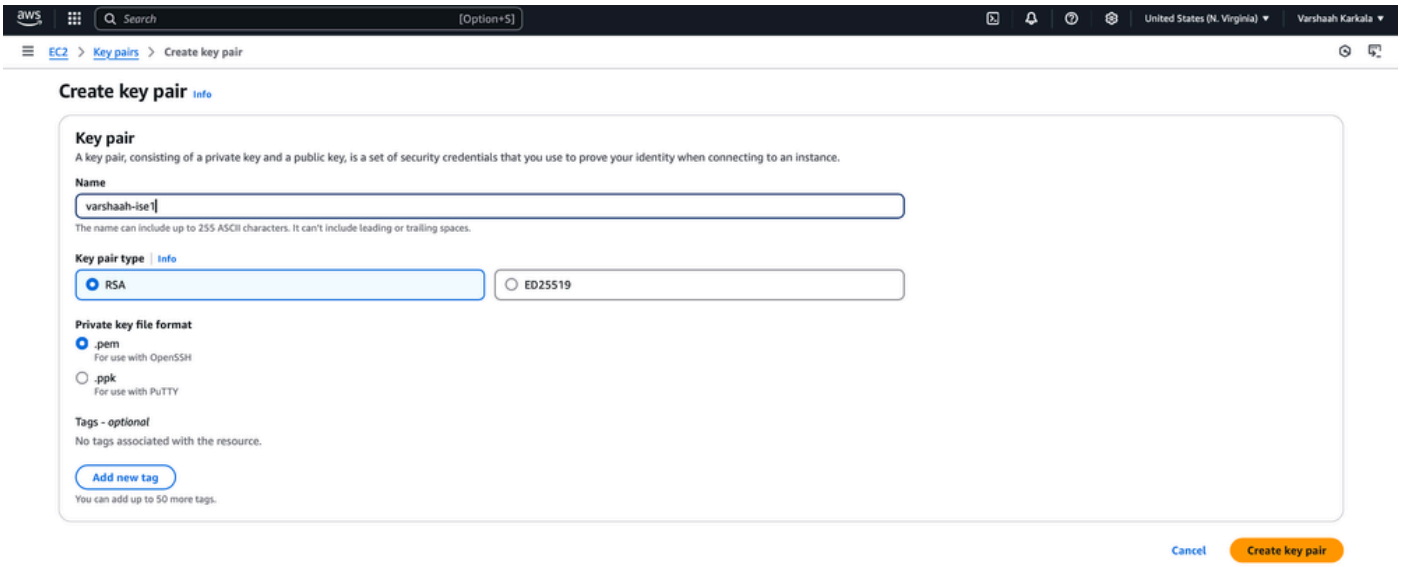
Teil 1: Generieren eines SSH-Schlüsselpaares

1. Für diese Bereitstellung können Sie entweder ein bereits vorhandenes Schlüsselpaar verwenden oder ein neues erstellen.

2. Um ein neues Paar zu erstellen, navigieren Sie zu EC2 > Network and Security > Key Pairs und klicken Sie auf Create Key Pair.



3. Geben Sie den Schlüsselpaarnamen ein, und klicken Sie auf Schlüsselpaar erstellen.

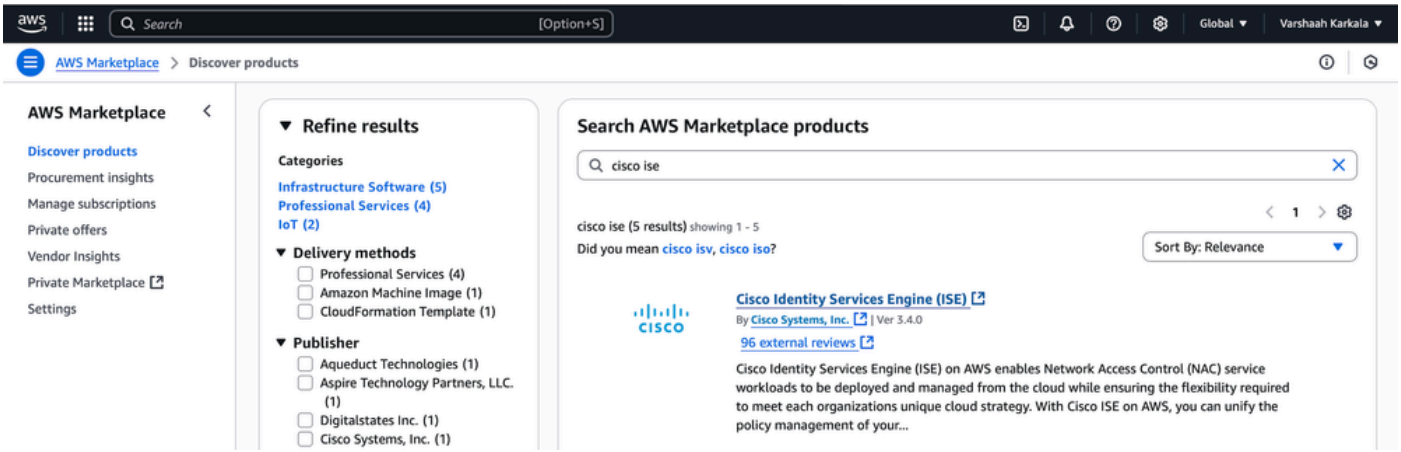


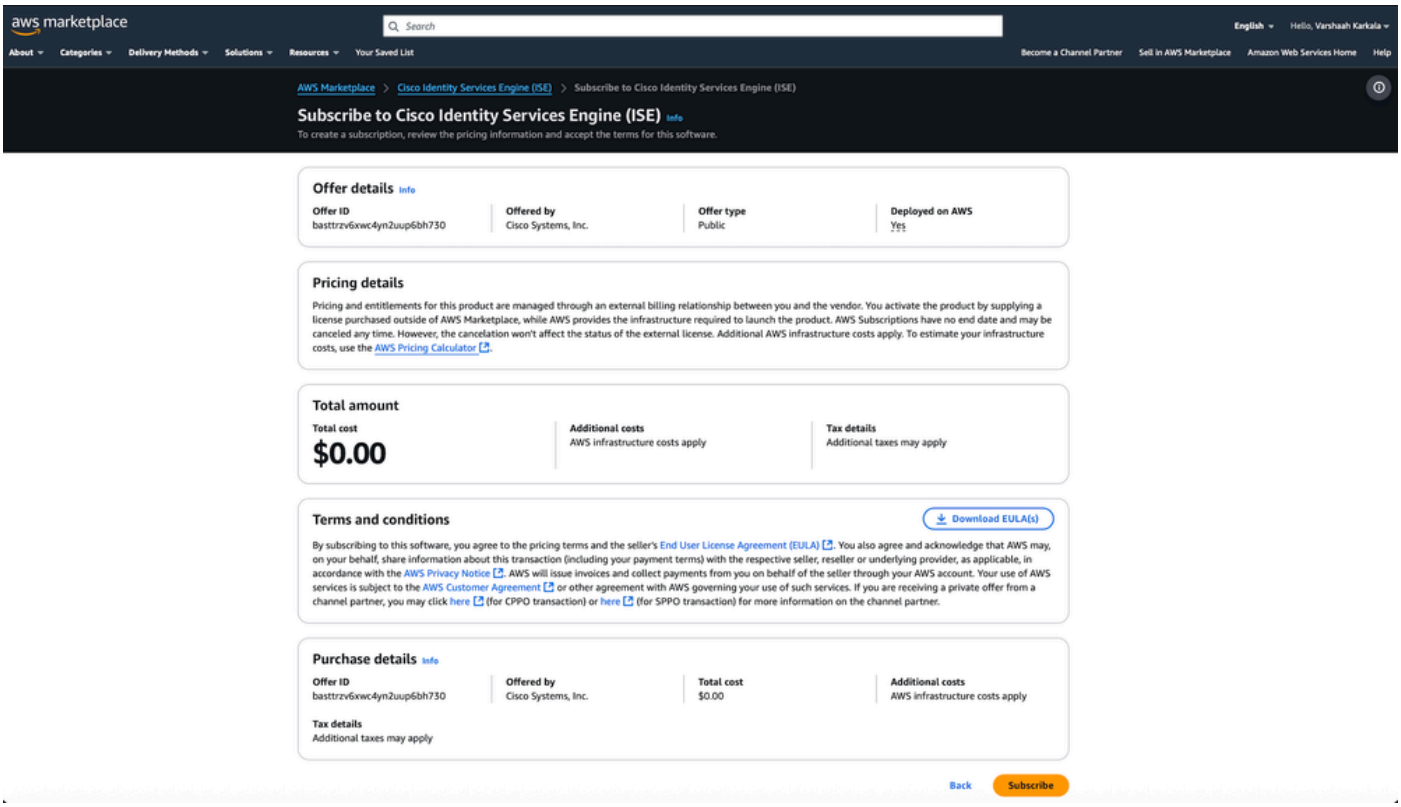
Die Schlüsselpaardatei (.pem) wird auf Ihren lokalen Computer heruntergeladen. Stellen Sie sicher, dass Sie diese Datei sicher aufbewahren, da dies die einzige Möglichkeit ist, auf Ihre EC2-Instanz zuzugreifen, sobald diese gestartet wurde.

Teil 2: Konfigurieren der ISE mithilfe der CloudFormation-Vorlage (CFT)

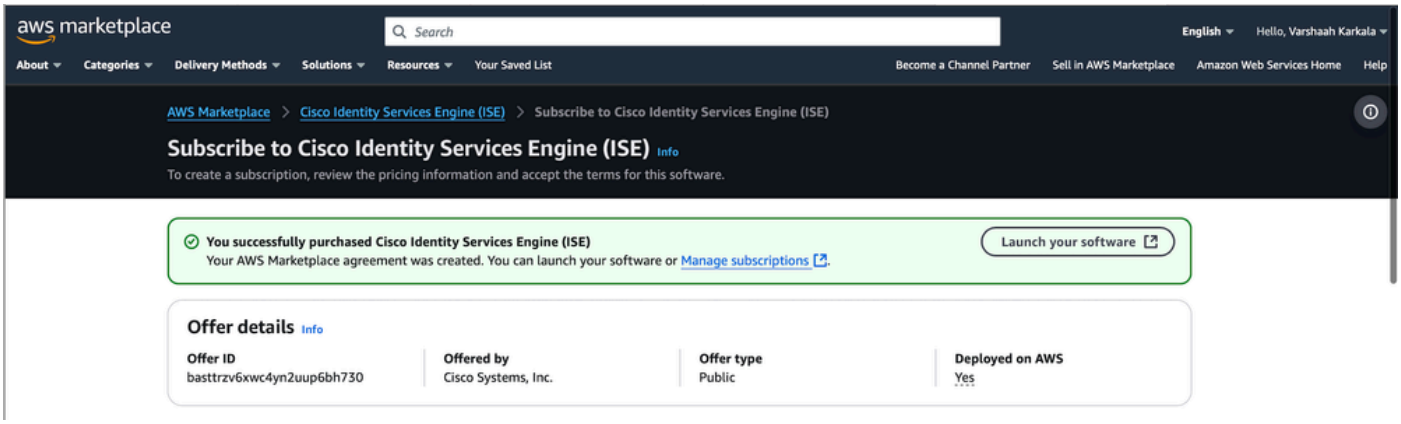
1. Melden Sie sich bei der AWS Management Console an, und suchen Sie nach AWS Marketplace Subscriptions.

2. Geben Sie in der Suchleiste "cisco ise" ein, und wählen Sie Cisco Identity Services Engine (ISE) aus den Ergebnissen aus. Klicken Sie auf Abonnieren.

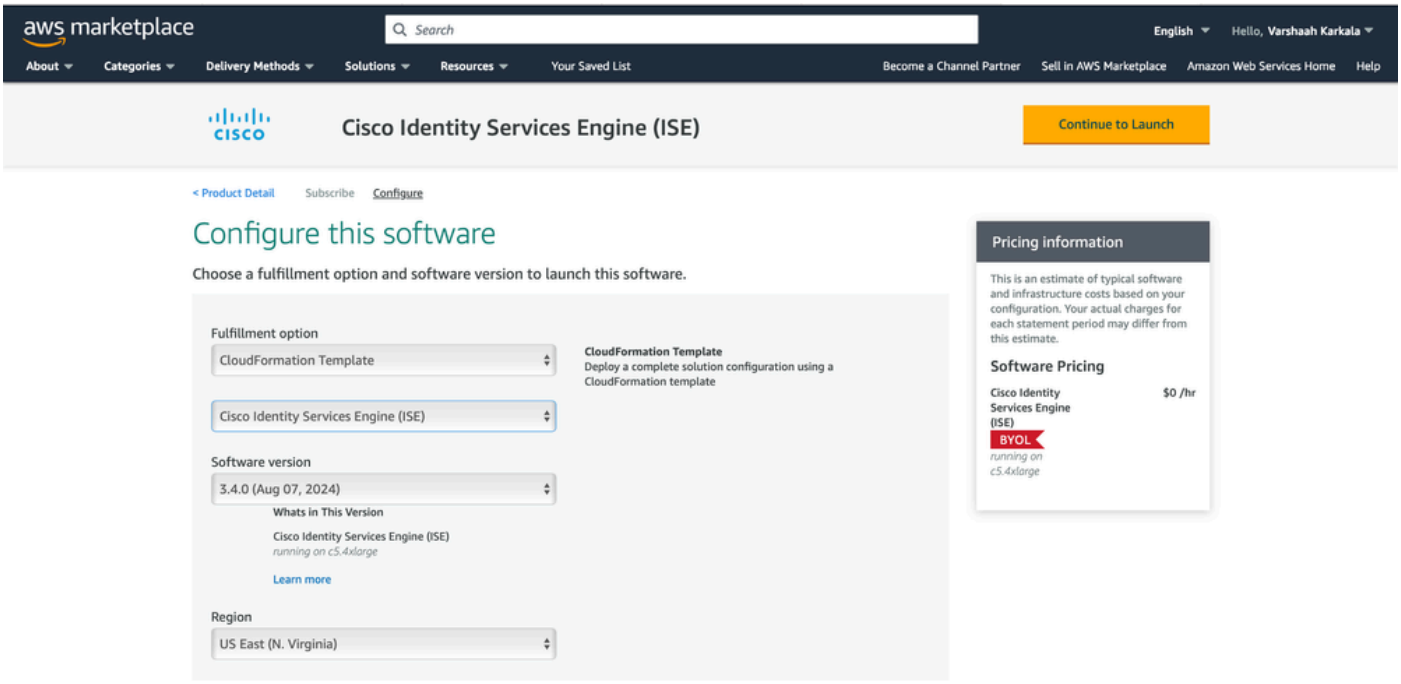




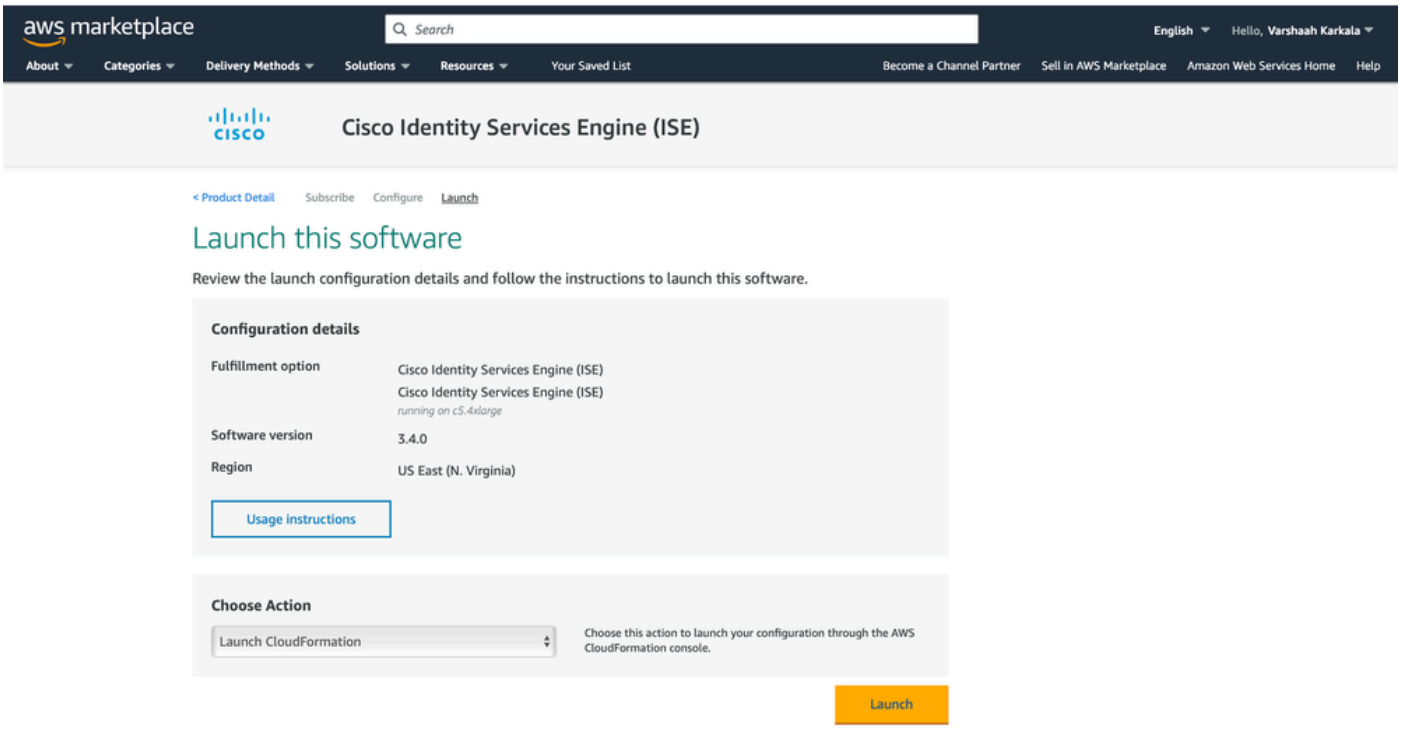
3. Wählen Sie nach dem Abonnement Launch Your Software (Software starten).



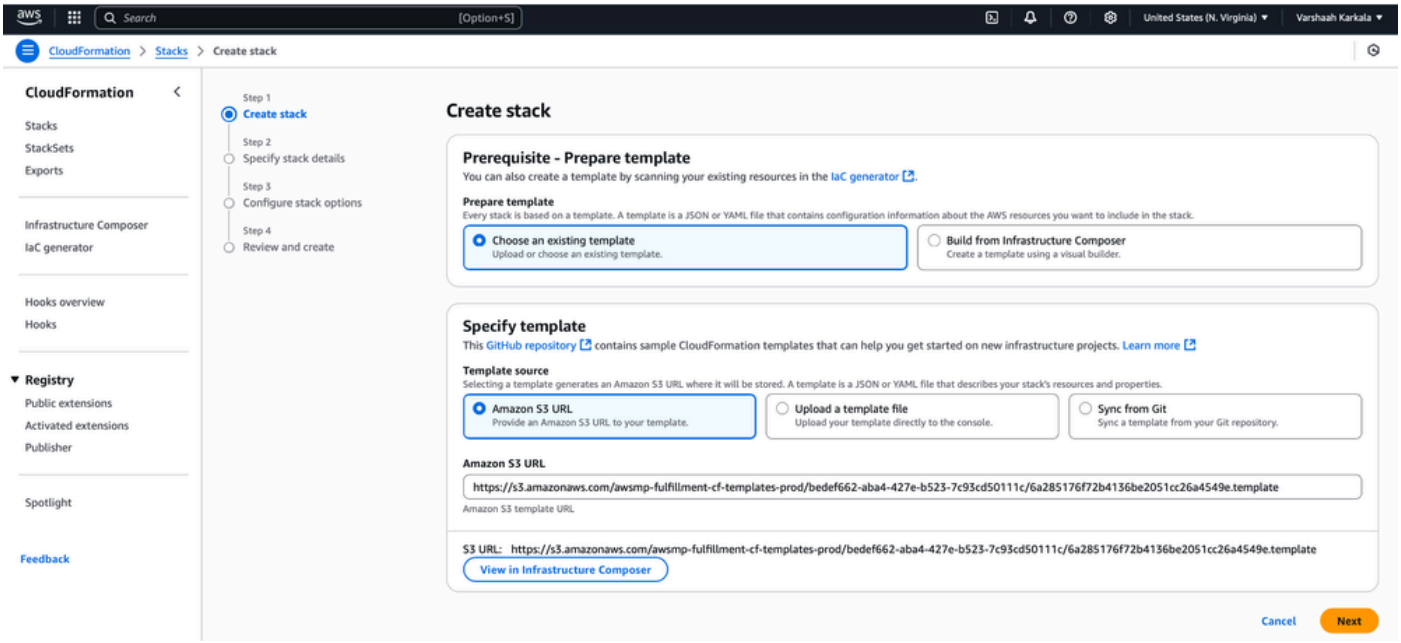
4. Wählen Sie unter Fulfillment Option die Option CloudFormation Template. Wählen Sie die Softwareversion (ISE-Version) und die Region aus, in der Sie die Instanz bereitstellen möchten, und klicken Sie auf Continue to Launch (Weiter zum Starten).



5. Wählen Sie auf der nächsten Seite CloudFormation starten als Aktion.

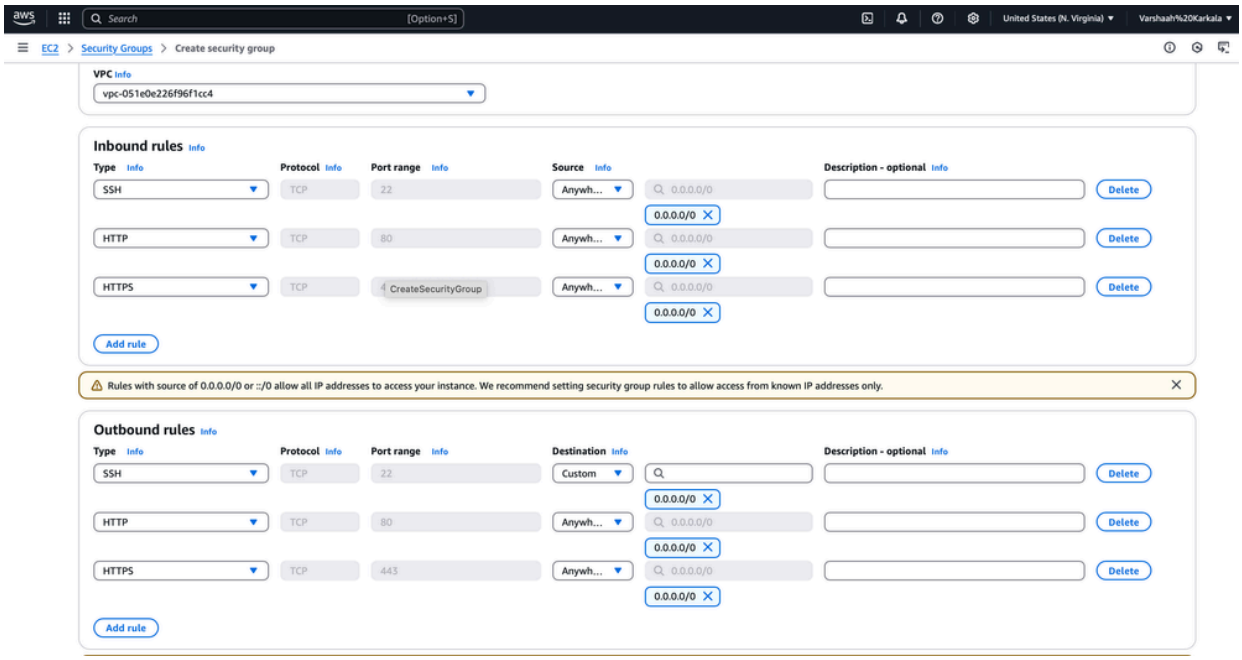


6. Behalten Sie unter den Stapeleinstellungen die Standardeinstellungen bei, und klicken Sie auf Weiter.



7. Geben Sie die erforderlichen Parameter ein:

- Stapelname: Geben Sie einen eindeutigen Namen für Ihren Stack an.
- Hostname: Weisen Sie den Hostnamen für den ISE-Knoten zu.
- Schlüsselpaar: Wählen Sie das generierte oder bereits vorhandene Schlüsselpaar aus, um später auf die EC2-Instanz zuzugreifen.
- Management-Sicherheitsgruppe:
    - Verwenden Sie entweder die standardmäßige Sicherheitsgruppe (wie unten gezeigt), oder erstellen Sie eine benutzerdefinierte Gruppe über das EC2-Dashboard.
    - Um eine neue Sicherheitsgruppe zu erstellen, navigieren Sie zum EC2 Dashboard, und gehen Sie zu Network and Security > Security Groups, um eine neue Sicherheitsgruppe zu erstellen.
    - Klicken Sie auf Sicherheitsgruppe erstellen, und geben Sie die erforderlichen Details ein.
    - Stellen Sie sicher, dass die Sicherheitsgruppe so konfiguriert ist, dass der erforderliche ein- und ausgehende Datenverkehr zugelassen wird. Aktivieren Sie beispielsweise den SSH-Zugriff (Port 22) über Ihre IP-Adresse für den CLI-Zugriff.

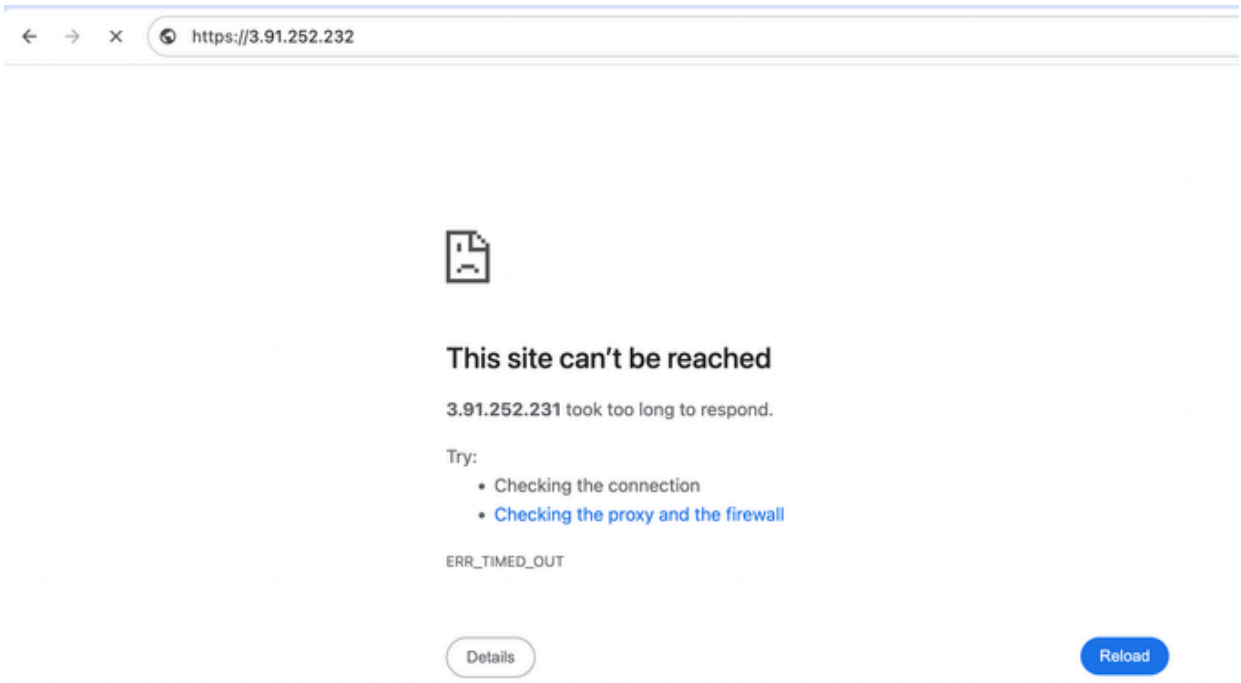


- Wenn der SSH-Zugriff nicht richtig konfiguriert ist, tritt beim Versuch, eine Verbindung über SSH herzustellen, möglicherweise ein Timeout beim Vorgang auf.

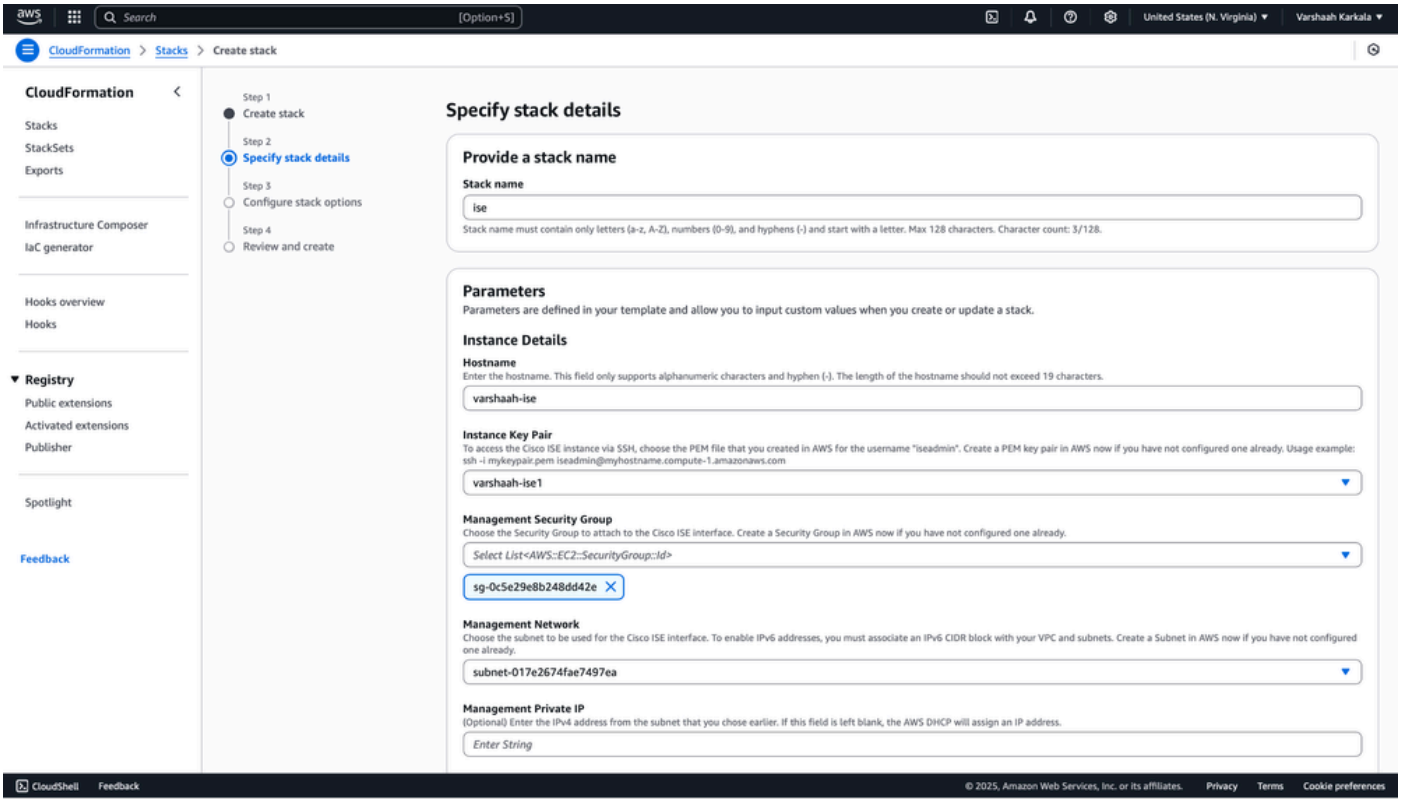
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

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

- Wenn der HTTP-/HTTPS-Zugriff nicht konfiguriert ist, wird beim Versuch, auf die GUI zuzugreifen, möglicherweise der Fehler "Diese Site kann nicht erreicht werden" angezeigt.



- Managementnetzwerk: Eines der vorhandenen Subnetze wurde ausgewählt.



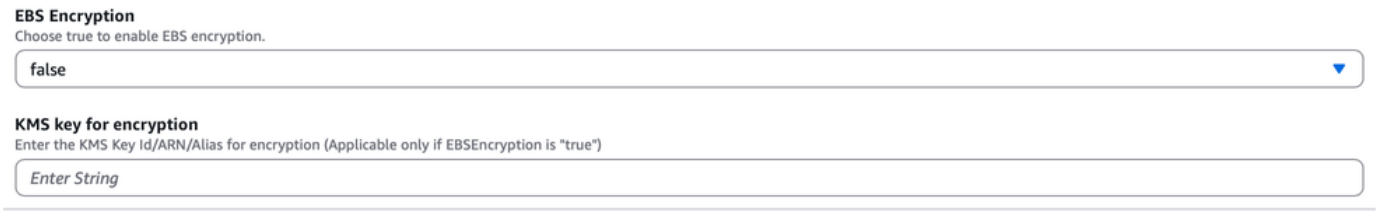
Wenn Ihr Design eine verteilte Bereitstellung mit einigen in AWS gehosteten Knoten und anderen lokalen Knoten erfordert, konfigurieren Sie eine dedizierte VPC mit einem privaten Subnetz und richten einen VPN-Tunnel zum lokalen VPN-Headend-Gerät ein, um die Konnektivität zwischen AWS-gehosteten und standortbasierten ISE-Knoten zu ermöglichen.

Ausführliche Informationen zur Konfiguration des VPN-Headend-Geräts finden Sie in diesem

Handbuch.

8. EBS-Verschlüsselung

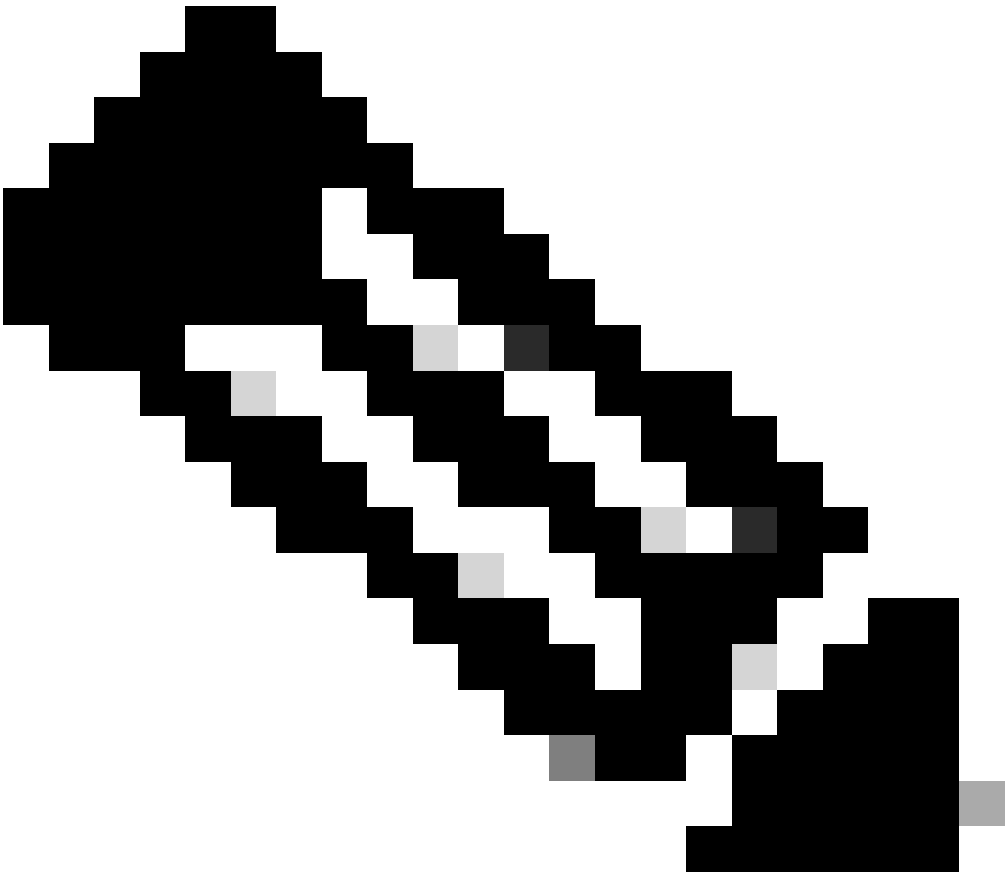
- Blättern Sie nach unten, um die EBS-Verschlüsselungseinstellungen zu finden.
- Legen Sie EBS Encryption (EBS-Verschlüsselung) auf False fest, es sei denn, Sie haben bestimmte Verschlüsselungsanforderungen.



9. Netzwerkkonfiguration:

- Blättern Sie nach unten, um Zugriffsoptionen für die Konfiguration von Netzwerkeinstellungen wie die DNS-Domäne, den primären Namenserver und den primären NTP-Server anzuzeigen.

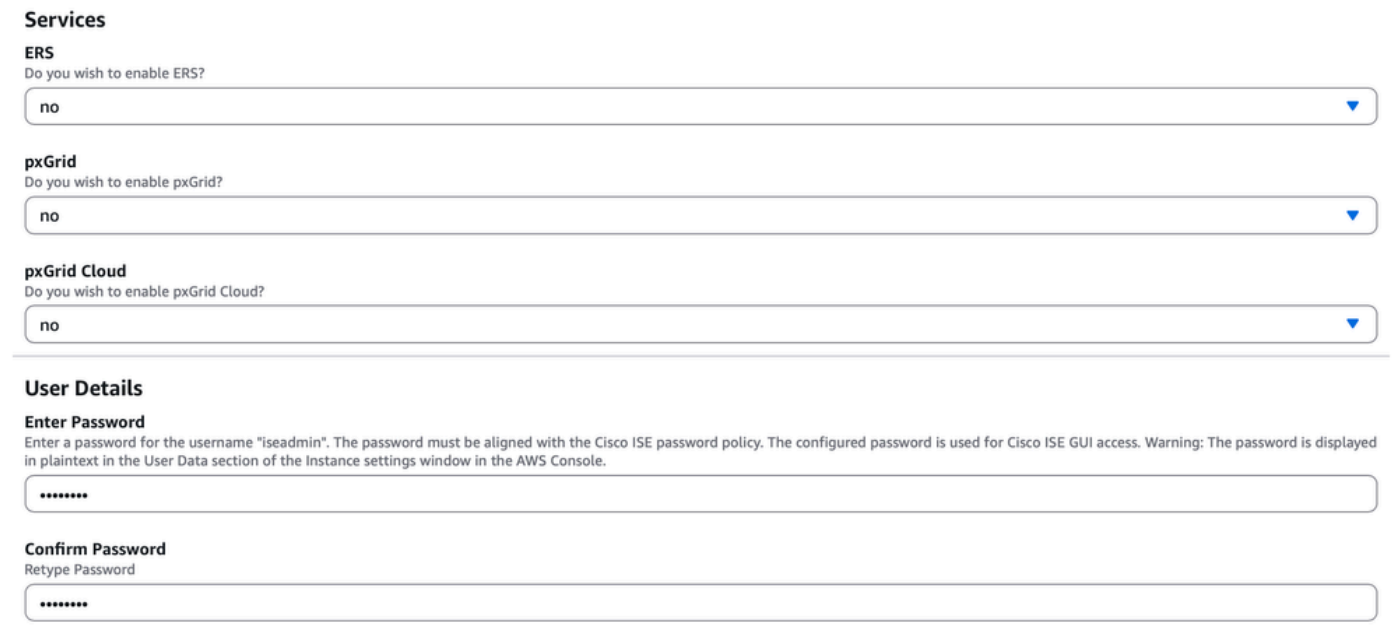
  Stellen Sie sicher, dass diese Werte korrekt eingegeben wurden.



Anmerkung: Eine falsche Syntax hier kann verhindern, dass ISE-Services nach der Bereitstellung ordnungsgemäß gestartet werden.

10. Service- und Benutzerdetails:

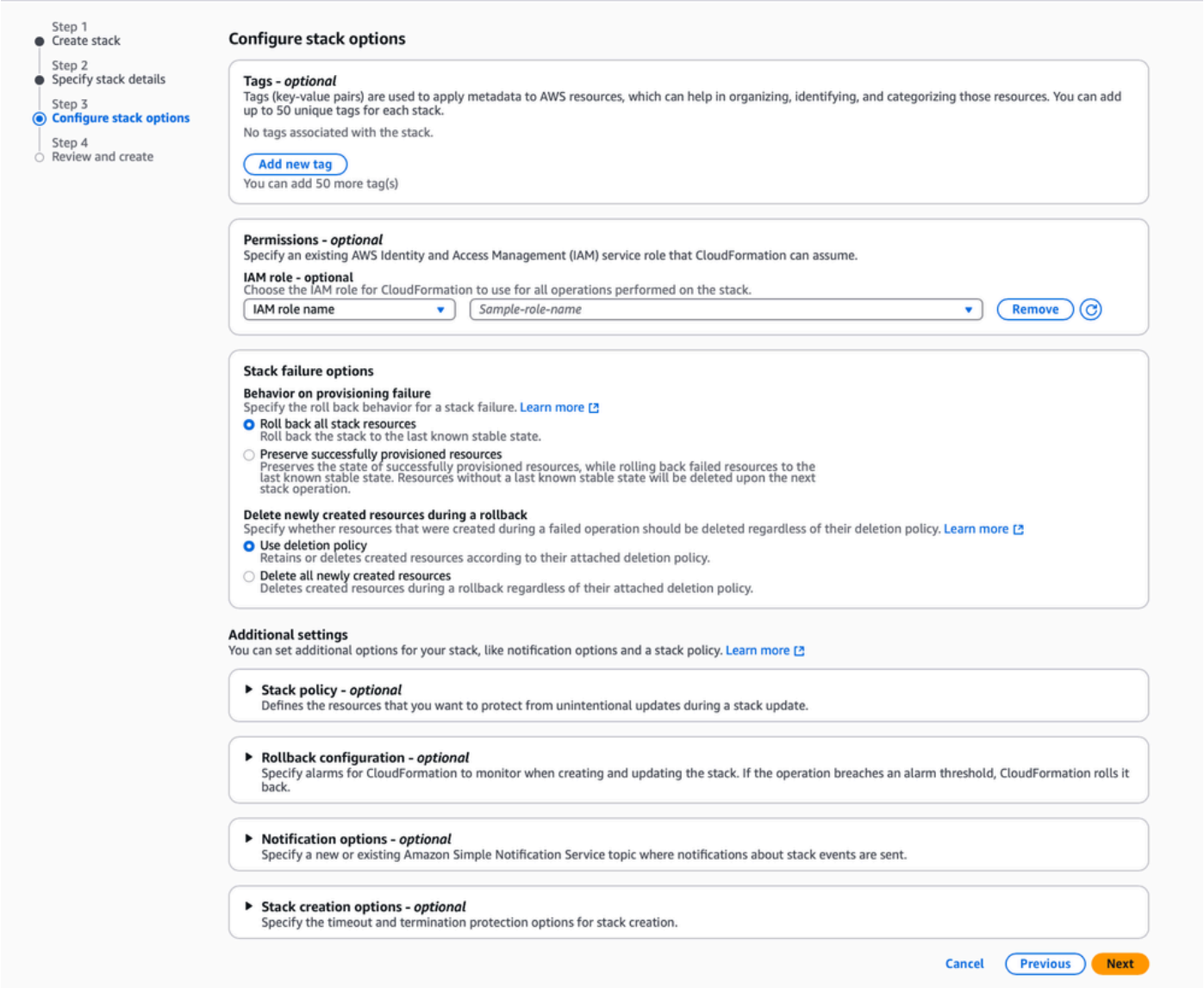
- Blättern Sie nach unten, um die Option zum Aktivieren von ERS- und pxGrid-Services zu finden.
- Wählen Sie aus, ob ERS- und pxGrid-Dienste aktiviert werden sollen, indem Sie ja oder nein auswählen.
- Legen Sie unter Benutzerdetails das Kennwort für den Administrator-Standardbenutzer fest.



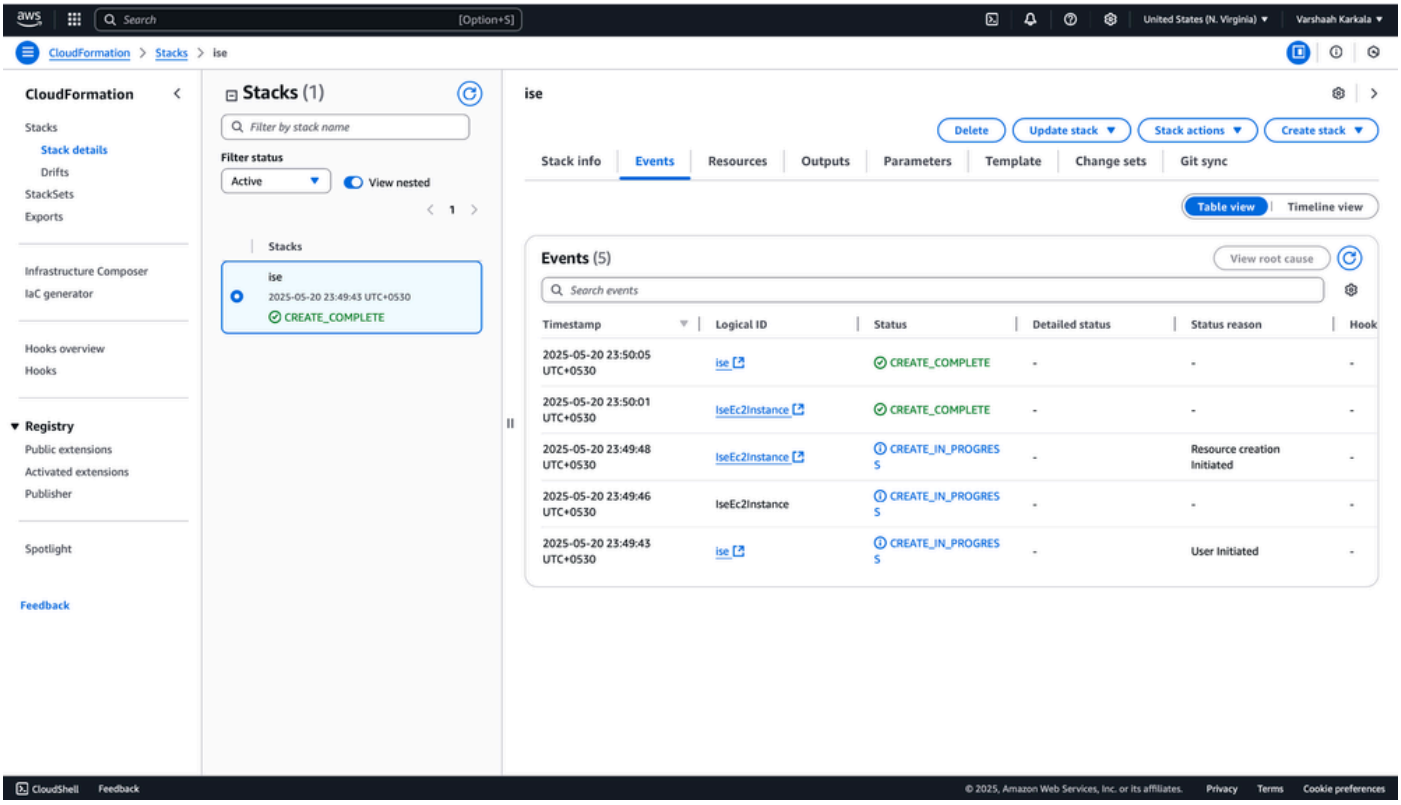
- Klicken Sie auf Next (Weiter).

11. Stapeloptionen konfigurieren:

- Belassen Sie alle Standardoptionen unverändert, und klicken Sie auf Weiter.



12. Überprüfen Sie die Vorlage, um sicherzustellen, dass alle Konfigurationen korrekt sind, und klicken Sie dann auf Senden. Sobald die Vorlage erstellt wurde, ähnelt sie dem unten gezeigten Beispiel:



13. Zugriff auf die Stapeldetails:
Navigieren Sie zum CloudFormation-Dienst in der AWS-Verwaltungskonsole, und gehen Sie zum Abschnitt Stacks. Suchen Sie den bereitgestellten Stack aus der Liste.

14. Registerkarte "Ausgabe anzeigen":

Wählen Sie Ihren Stapel aus, und öffnen Sie die Registerkarte Ausgänge. Hier finden Sie wichtige Informationen, die während des Bereitstellungsprozesses generiert wurden, z. B.:

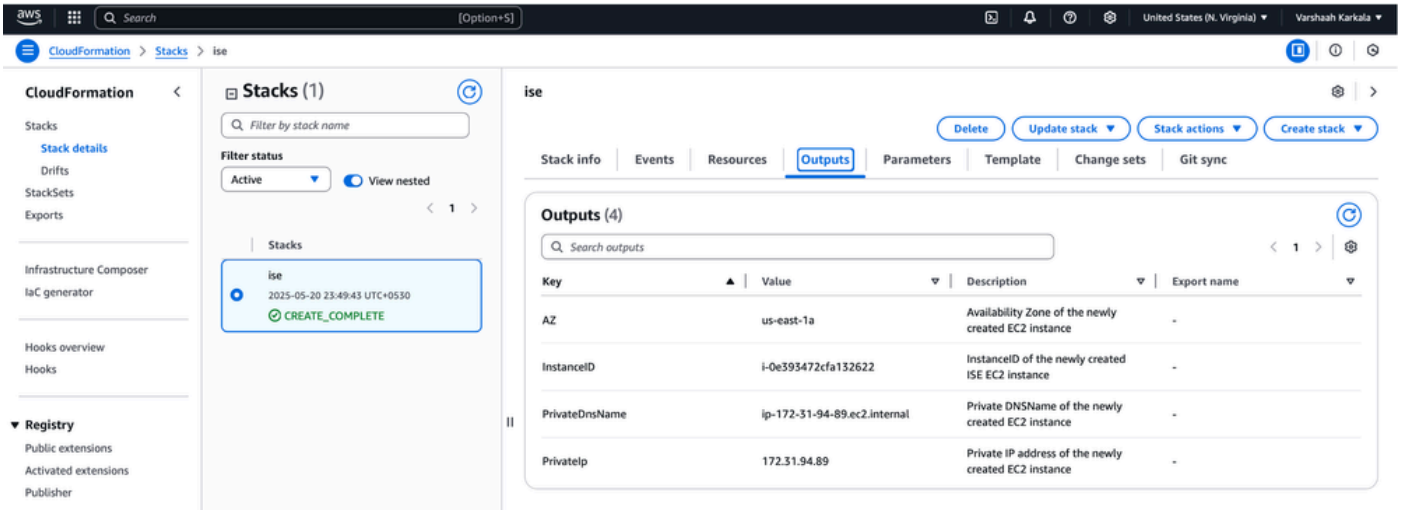
- Verfügbarkeitszone: Die Region, in der die Ressourcen eingesetzt werden.

- Instanz-ID: Der eindeutige Bezeichner der bereitgestellten Instanz

- DNS-Name: Der private DNS-Name der Instanz, der für den Remotezugriff verwendet werden kann.

•IP-Adresse: Die öffentliche oder private IP-Adresse der Instanz, je nach Konfiguration.

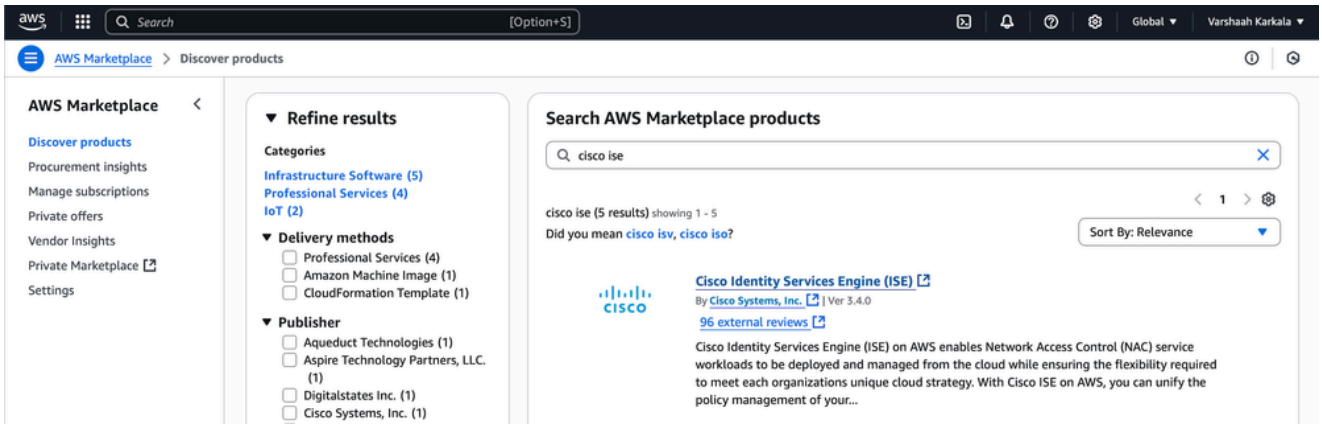
Diese Informationen helfen Ihnen, eine Verbindung mit der Instanz herzustellen und deren Verfügbarkeit zu überprüfen. Die Registerkarte Ausgaben ähnelt diesem Beispiel:



Teil 3: Konfigurieren der ISE mit Amazon Machine Image (AMI)

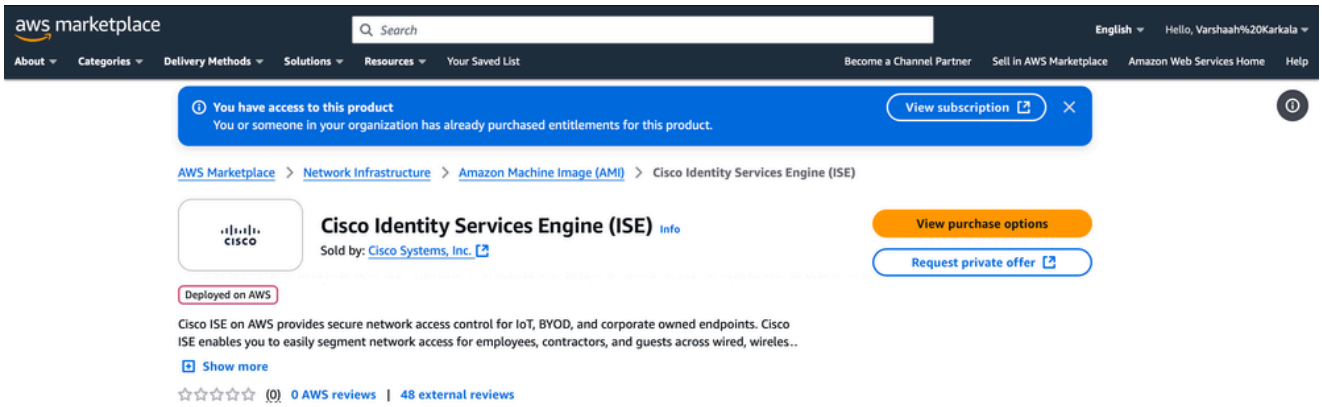
1. Melden Sie sich bei der AWS Management Console an, und suchen Sie nach AWS Marketplace Subscriptions.

2. Geben Sie in der Suchleiste "cisco ise" ein, und wählen Sie Cisco Identity Services Engine (ISE) aus den Ergebnissen aus.

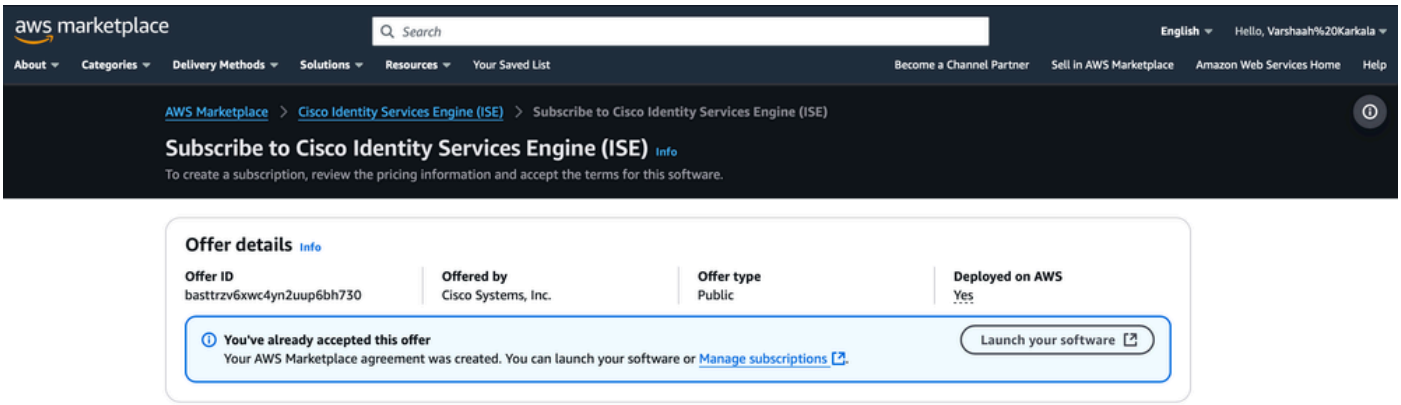


ISE auf dem AWS-Marktplatz

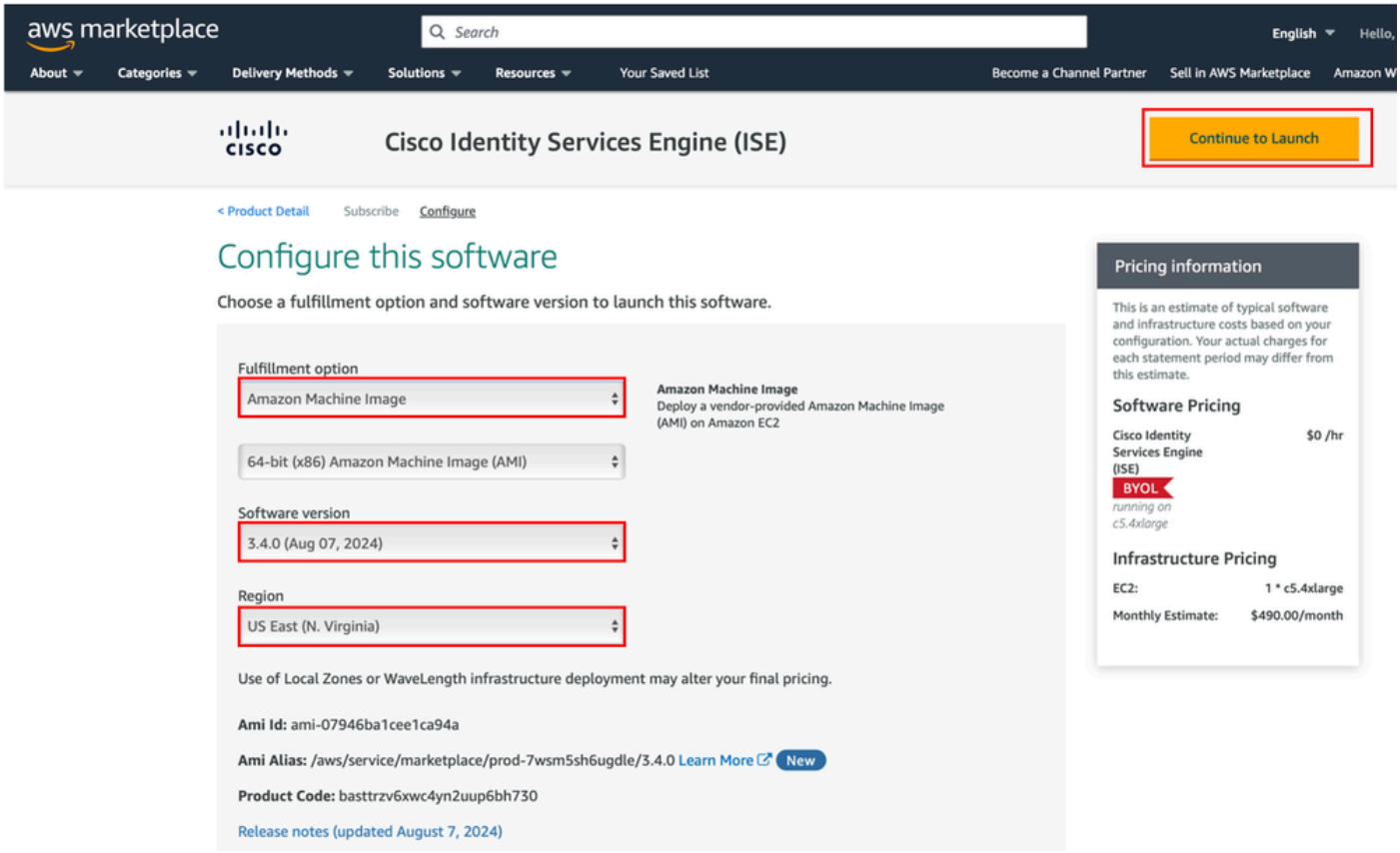
3. Klicken Sie auf Kaufoptionen anzeigen.



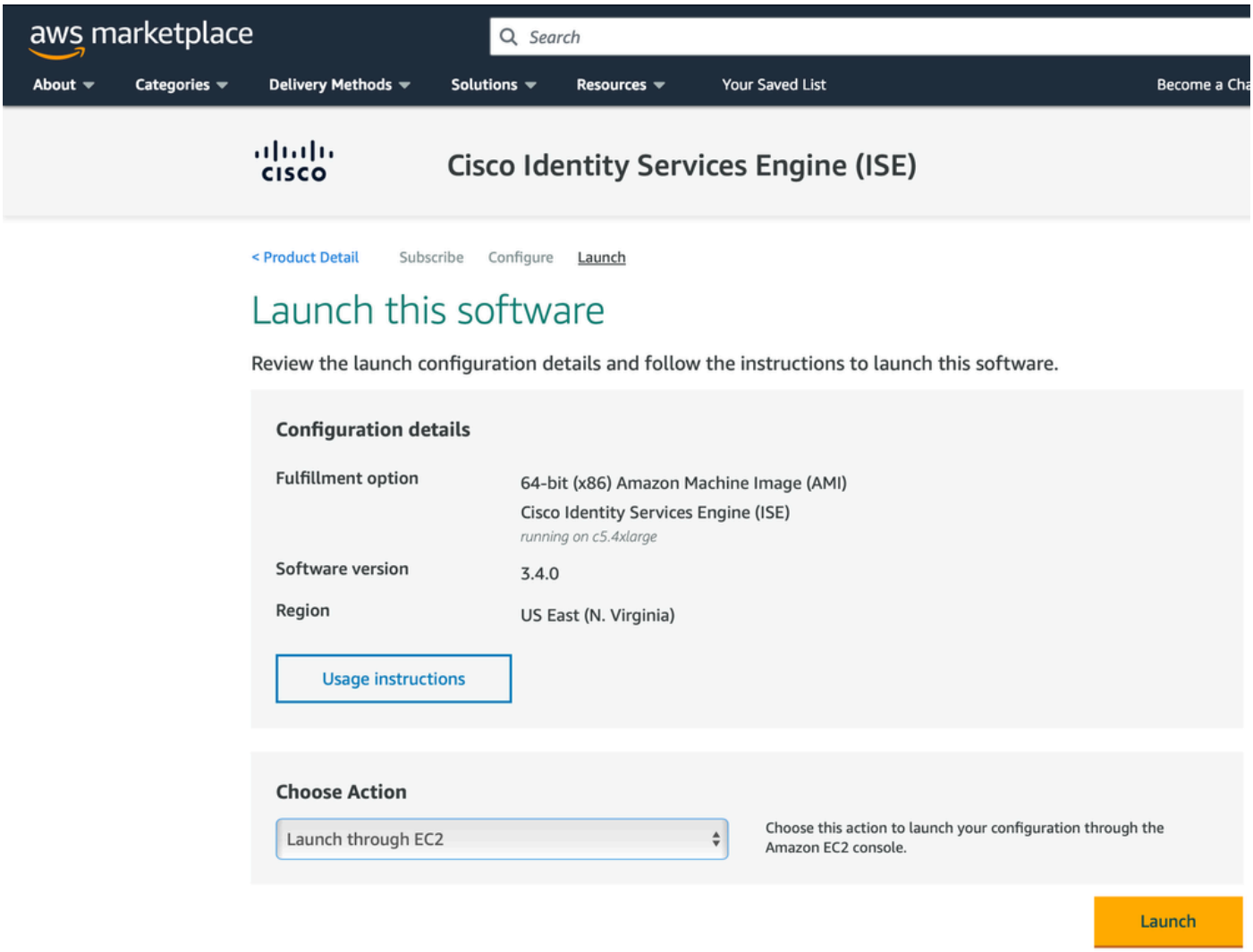
4. Klicken Sie auf Software starten.



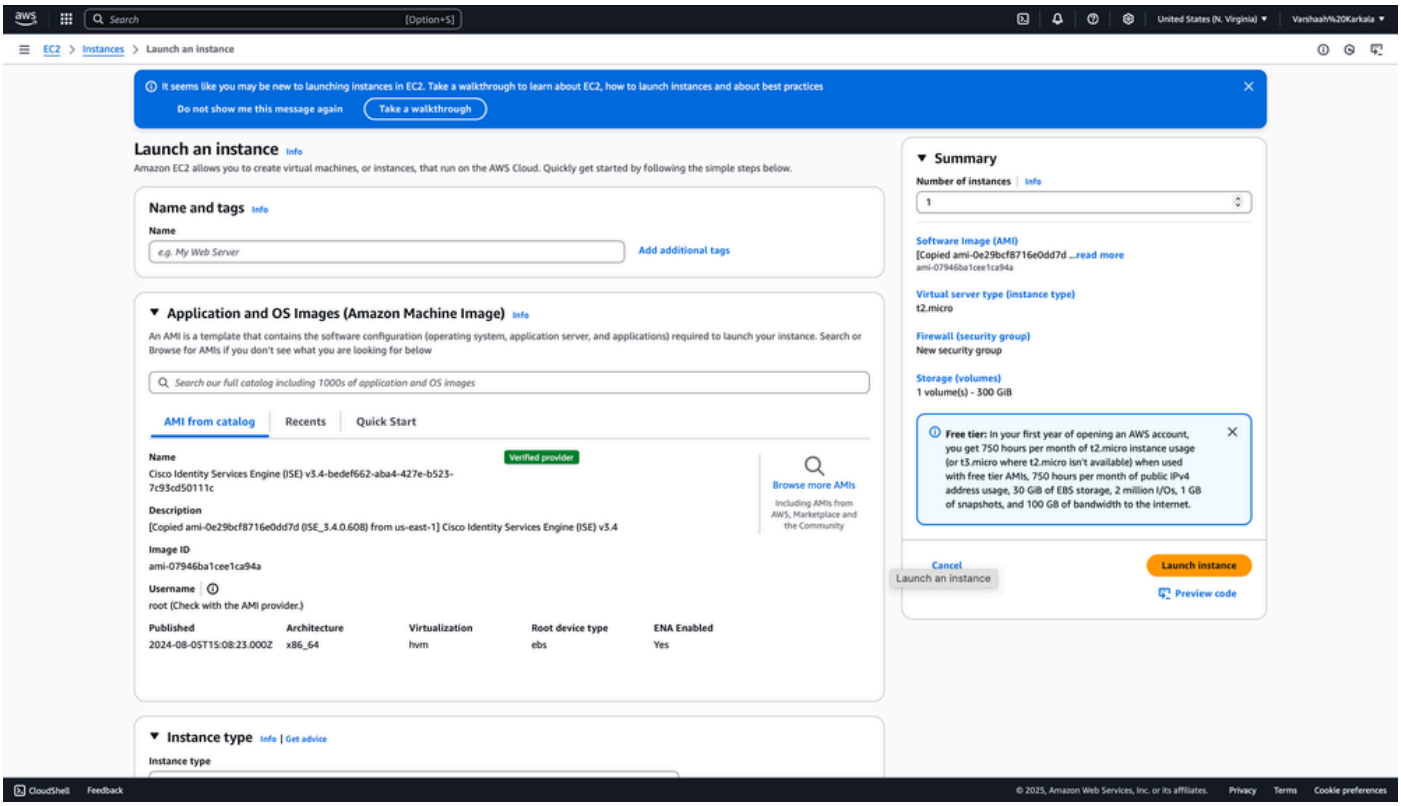
5. Wählen Sie unter der Erfüllungsoption Amazon Machine Image aus. Wählen Sie die gewünschte Softwareversion und den AWS-Bereich aus, und klicken Sie dann auf Weiter, um zu starten.



6. Wählen Sie im Dropdown-Menü Aktion auswählen die Option Über EC2 starten, und klicken Sie dann auf Starten, um fortzufahren.



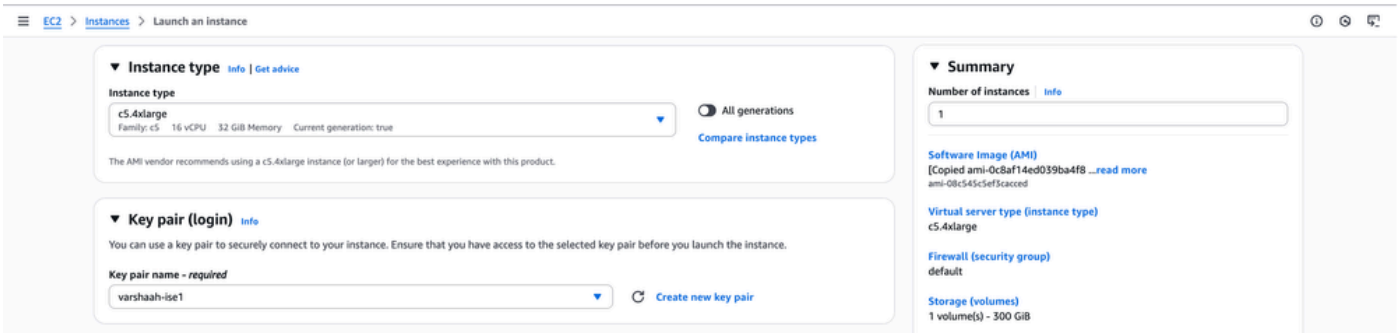
7. Sie werden auf die Seite EC2 Launch an Instance umgeleitet, um Ihre Instanzeinstellungen zu konfigurieren.



8. Blättern Sie nach unten zum Abschnitt Instanztyp, und wählen Sie einen geeigneten Instanztyp basierend auf Ihren Bereitstellungsanforderungen aus.

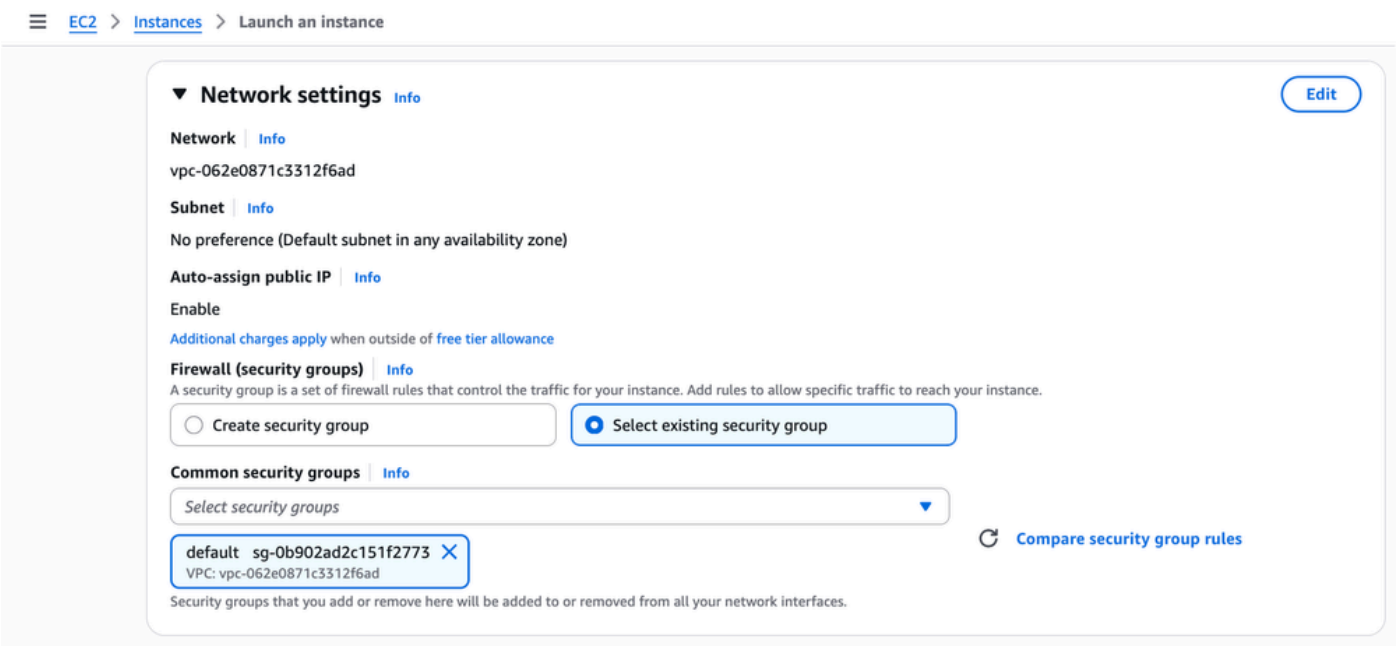
Wählen Sie unter Schlüsselpaar (Anmeldung) das zuvor generierte Schlüsselpaar aus, oder erstellen Sie ein neues (siehe die zuvor bereitgestellten Schritte zum Erstellen von Schlüsselpaaren).

Legen Sie die Anzahl der Instanzen auf 1 fest.



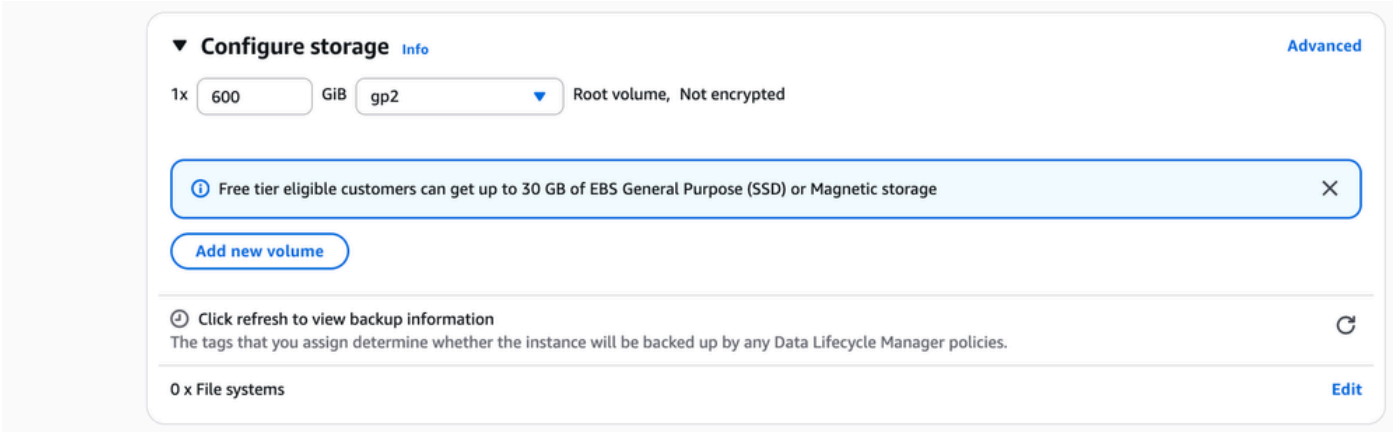
9. Im Abschnitt Netzwerkeinstellungen:

- Konfigurieren Sie VPC und Subnetz nach Bedarf.
- Wählen Sie für die Sicherheitsgruppe entweder eine vorhandene aus, oder erstellen Sie eine neue Gruppe (wie im Beispiel gezeigt).



10. Konfigurieren Sie im Abschnitt Storage konfigurieren die gewünschte Volume-Größe.

Beispiel: 600 GiB bei Verwendung des Volumentyps gp2



11. Konfigurieren Sie im Abschnitt Erweiterte Details alle zusätzlichen Einstellungen, die für Ihre Bereitstellung erforderlich sind, wie IAM-Instanzprofil, Benutzerdaten oder Abschaltverhalten.

▼ **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 ▼

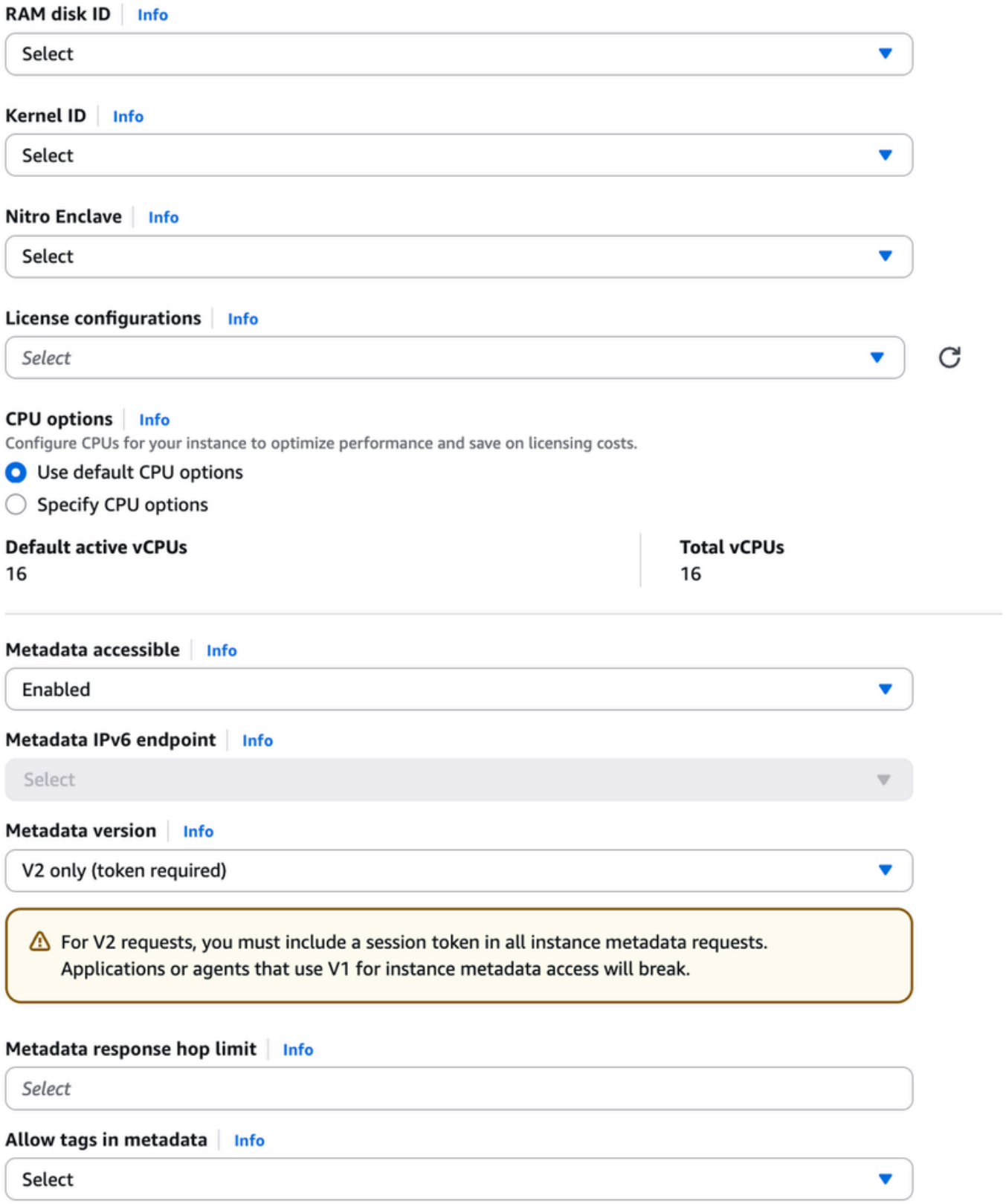
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12. Im Abschnitt Metadatenversion:

- Wählen Sie für ISE Version 3.4 und höher die Option "Nur V2" (Token erforderlich) aus. Dies ist die empfohlene Option.
- Für ISE-Versionen vor 3.4 wählen Sie V1 und V2 (Token optional), um die Kompatibilität sicherzustellen.



13. Geben Sie im Feld Benutzerdaten die Parameter für die Erstkonfiguration der ISE-Instanz an, einschließlich Hostname, DNS, NTP-Server, Zeitzone, ERS und Admin-Anmeldedaten.

Beispiel:
hostname=varshaahise2

primarynameserver=x.x.x.x

dnsdomain=varshaah.local

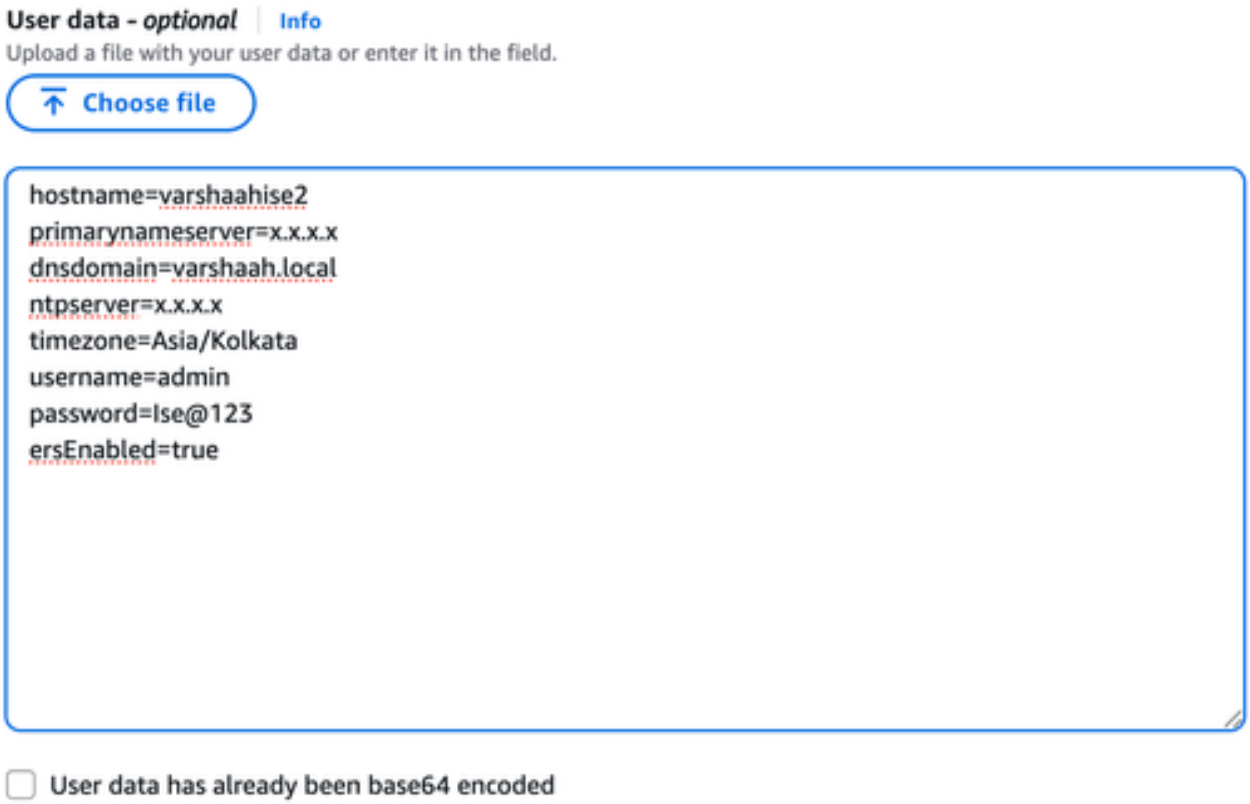
ntpserver=x.x.x.x

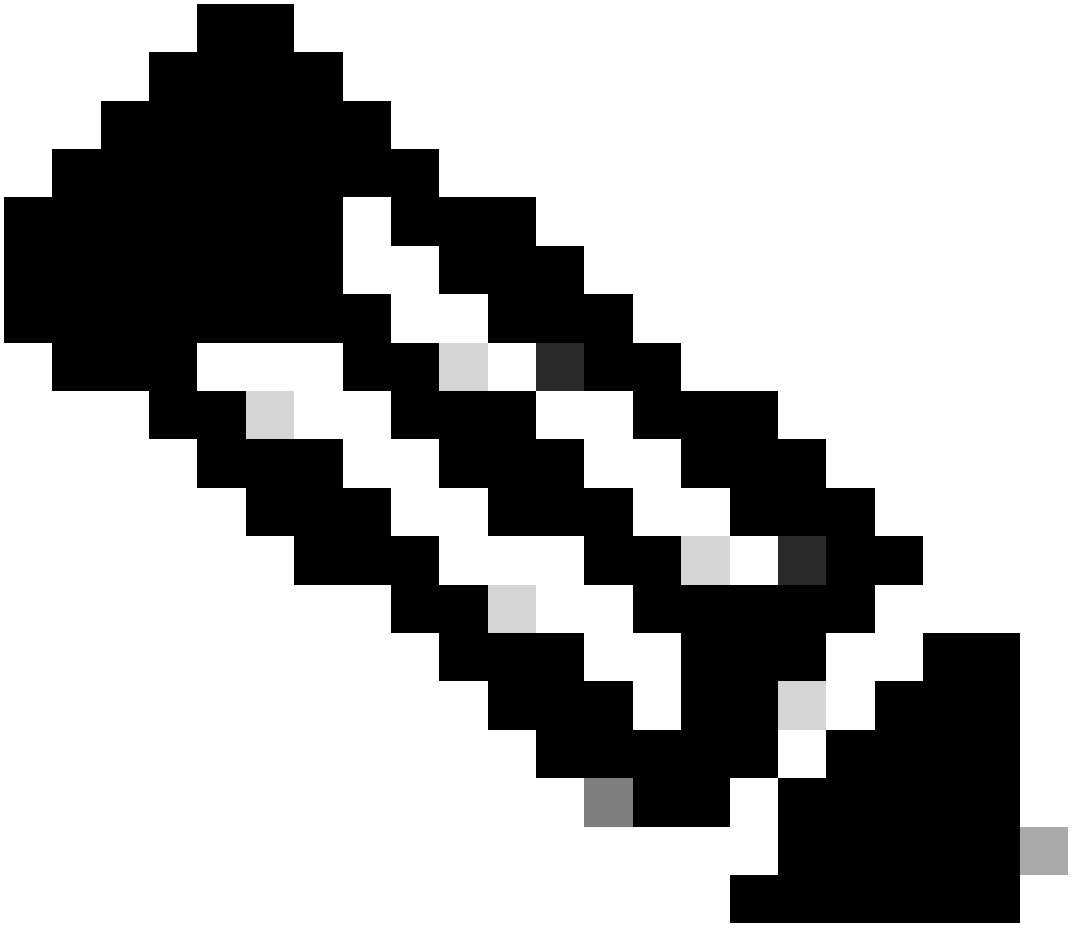
timezone=Asien/Kolkata

username=admin

password=Ise@123

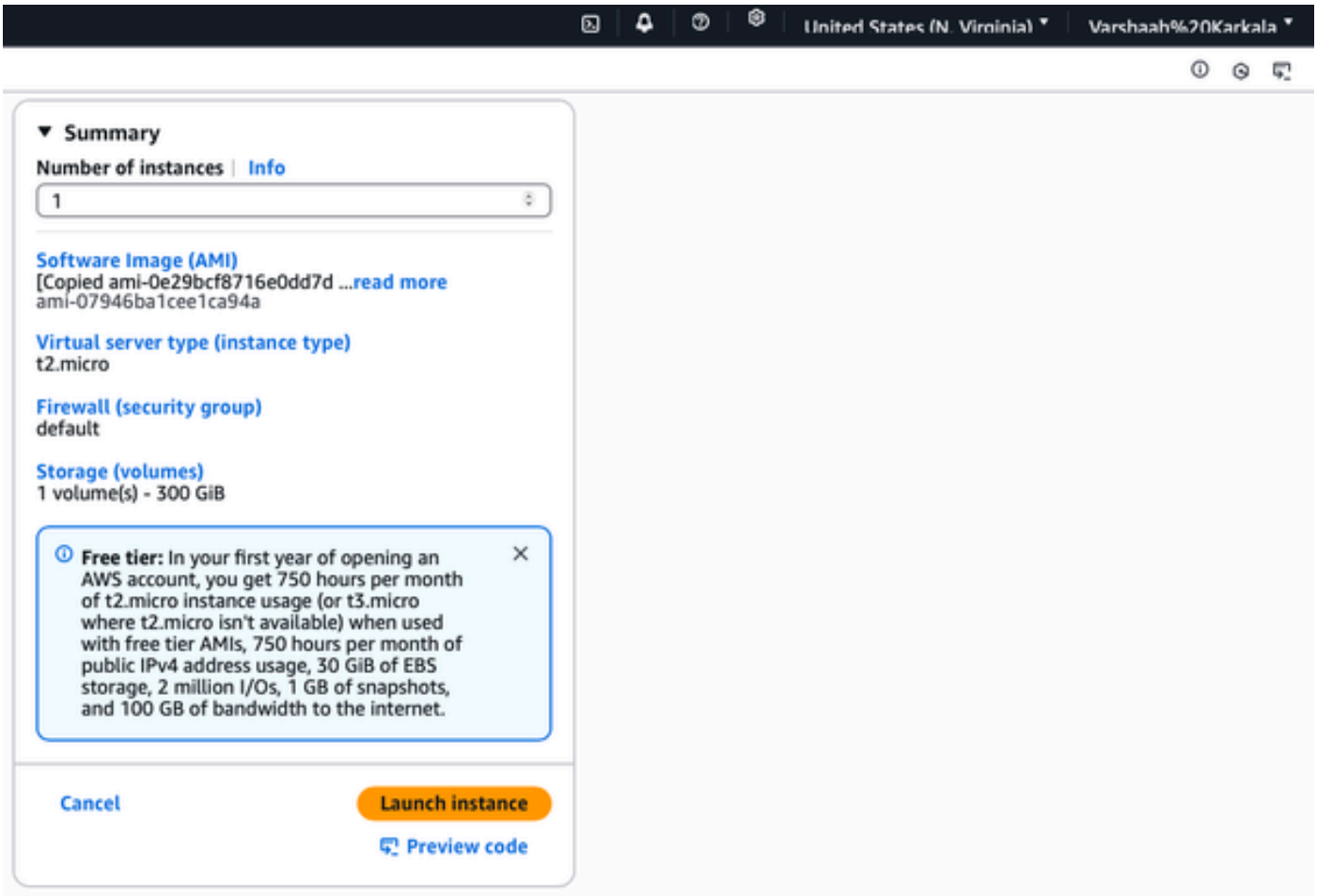
ersEnabled=true



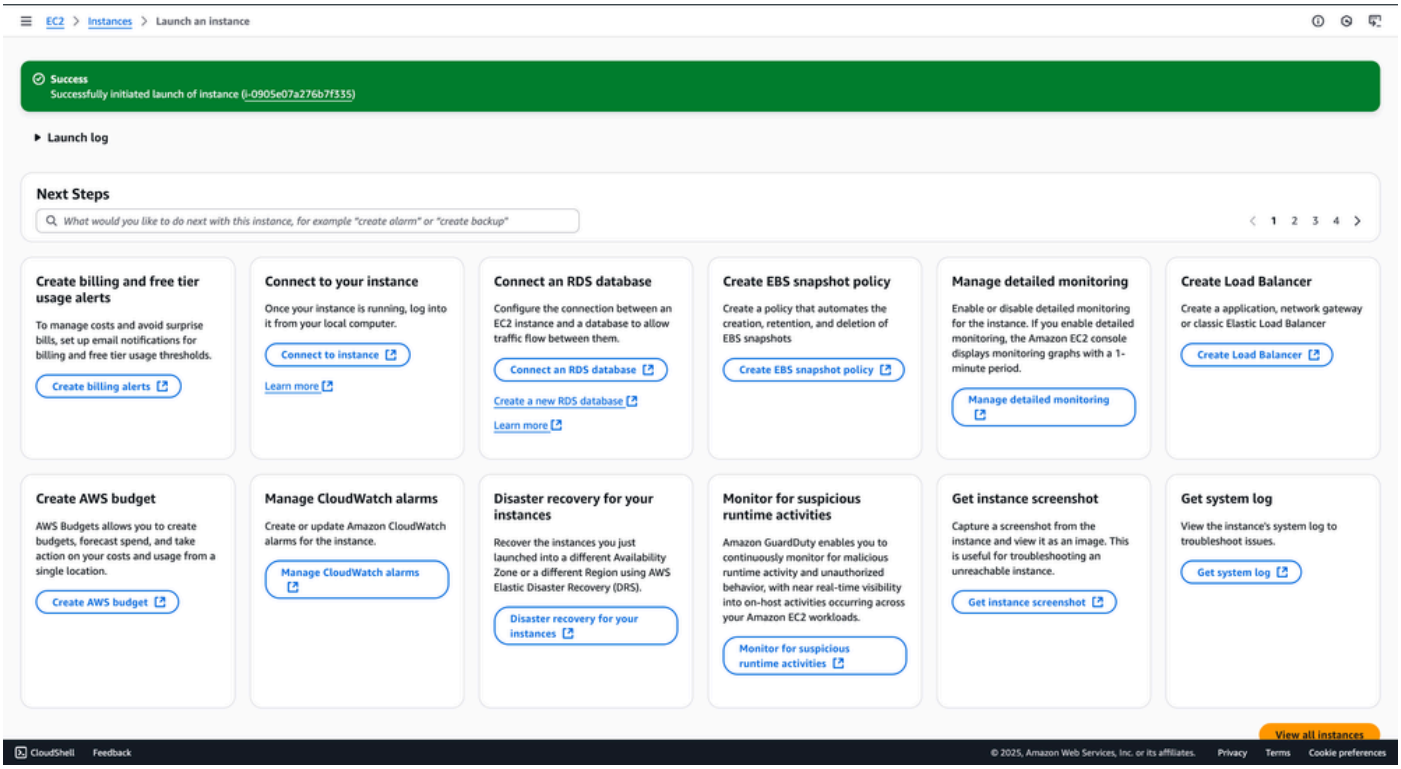


Anmerkung: Stellen Sie sicher, dass das Kennwort mit der Cisco ISE-Kennwortrichtlinie übereinstimmt.

Nachdem Sie die Benutzerdaten eingegeben und die Konfiguration abgeschlossen haben, klicken Sie auf Instanz starten.



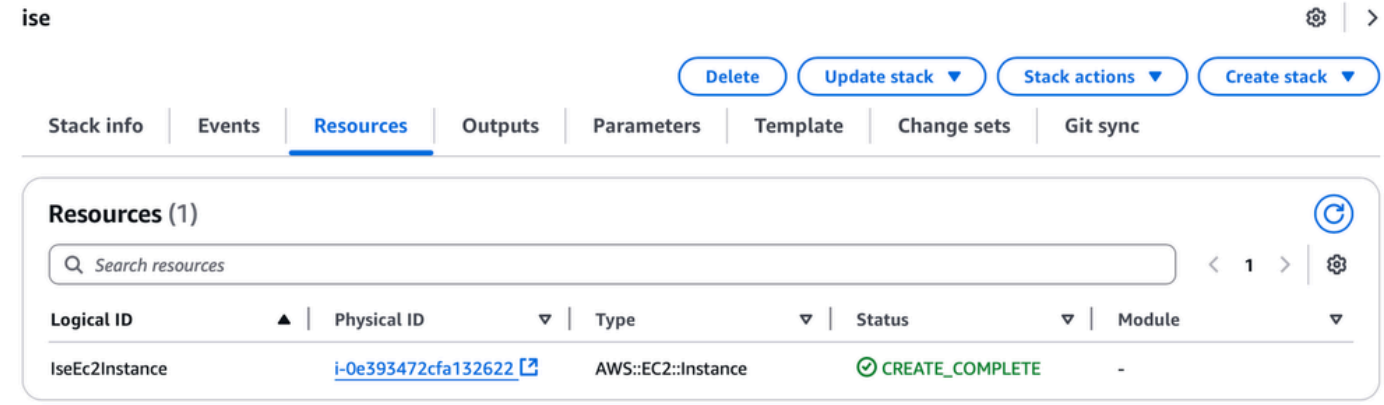
14. Nachdem die Instanz gestartet wurde, erscheint eine Bestätigungsmeldung mit folgendem Hinweis: 'Der Start der Instanz <Instanzname> wurde erfolgreich initiiert.' Dies zeigt an, dass der Startvorgang erfolgreich gestartet wurde.

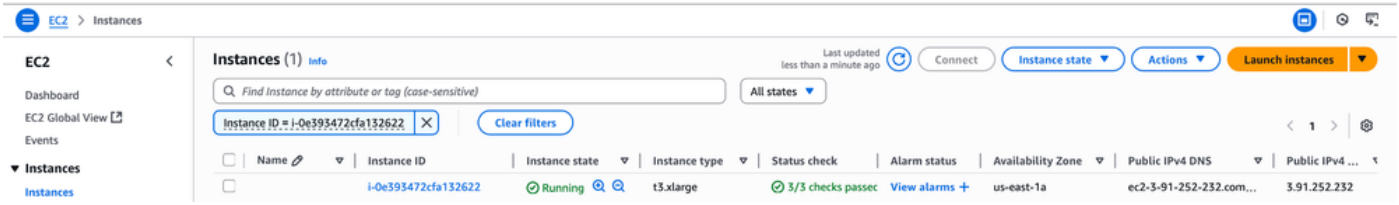


Überprüfung

Zugriff auf die mit CFT erstellte ISE-Instanz

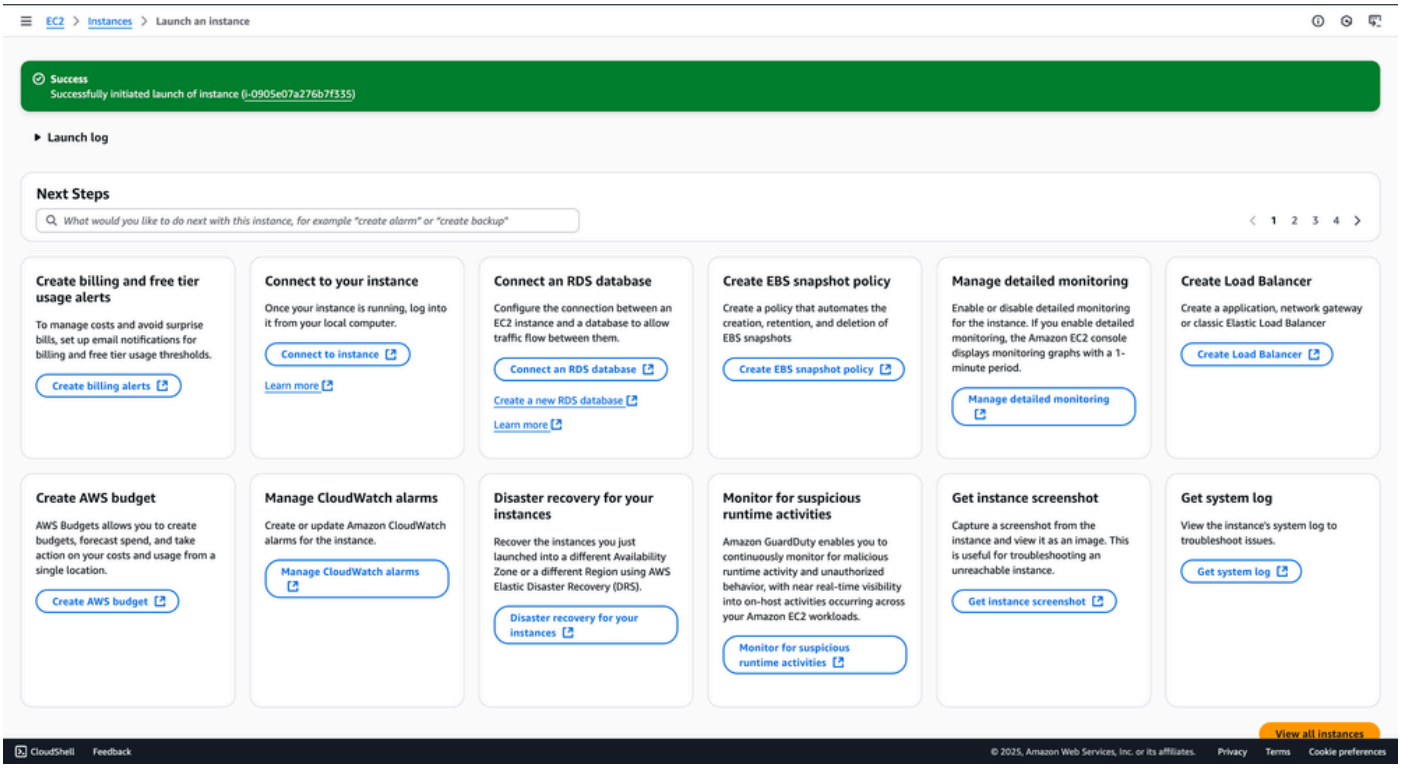
Wechseln Sie zur Registerkarte Ressourcen in Ihrem CloudFormation-Stack, und klicken Sie auf die physische ID. Sie werden zum EC2-Dashboard weitergeleitet, wo Sie die Instanz sehen können.

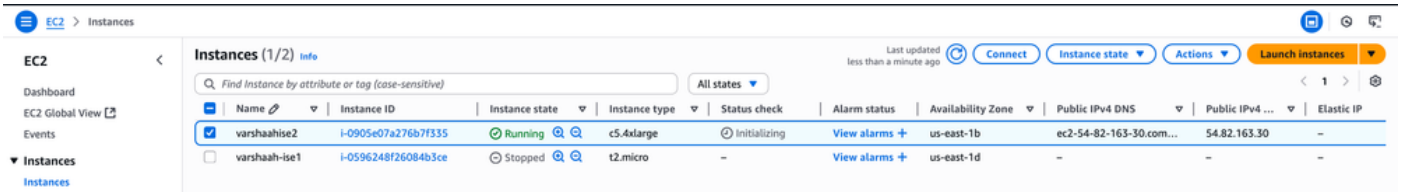




Zugriff auf die mit AMI erstellte ISE-Instanz

Klicken Sie auf "Alle Instanzen anzeigen", um zur Seite "EC2-Instanzen" zu navigieren. Überprüfen Sie auf dieser Seite, ob die Statusüberprüfung als 3/3-Prüfung angezeigt wird, die anzeigt, dass die Instanz aktiv und fehlerfrei ist.





Zugriff auf die ISE-GUI

Der ISE-Server wurde erfolgreich bereitgestellt.

Um auf die ISE-GUI zuzugreifen, müssen Sie die IP-Adresse der Instanz in Ihrem Browser verwenden. Da die Standard-IP-Adresse privat ist, kann nicht direkt über das Internet auf sie zugegriffen werden.

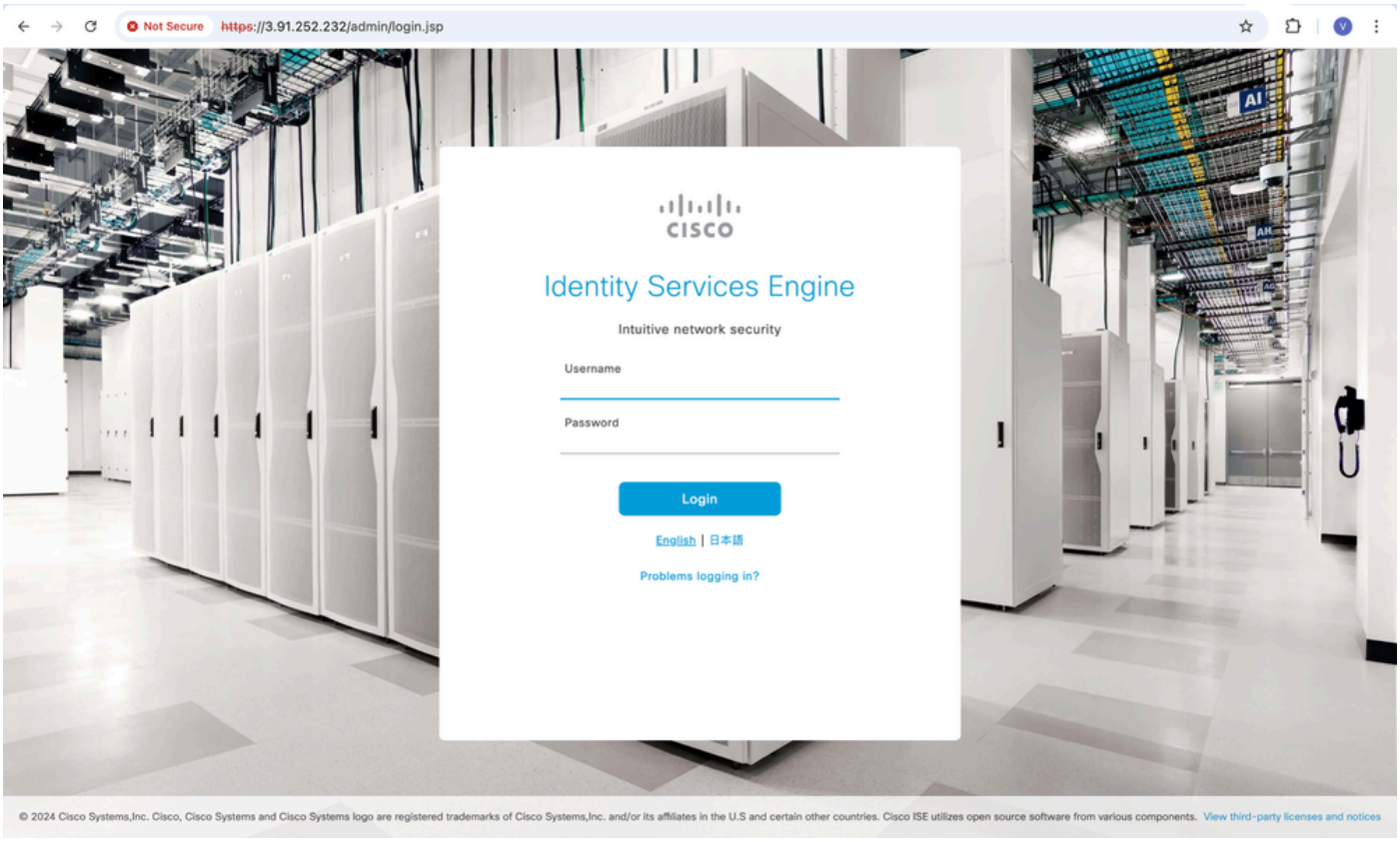
Überprüfen Sie, ob eine öffentliche IP mit der Instanz verknüpft ist:

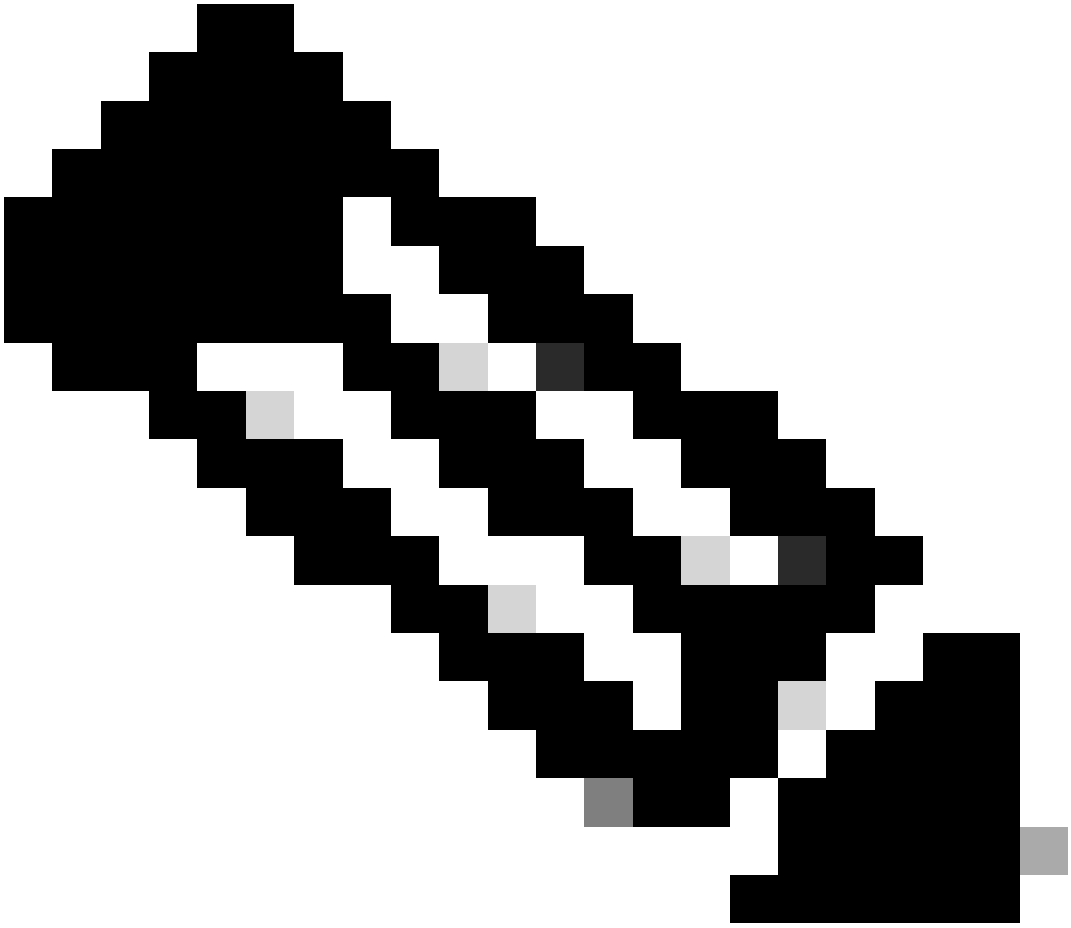
- Navigieren Sie zu EC2 > Instances und wählen Sie Ihre Instanz aus.
- Suchen Sie nach dem Feld für die öffentliche IPv4-Adresse.

Hier sehen Sie eine öffentliche IP-Adresse, über die Sie auf die ISE-GUI zugreifen können.

Öffnen Sie einen unterstützten Browser (z. B. Chrome oder Firefox), und geben Sie die öffentliche IP-Adresse ein.

Die Anmeldeseite der ISE-GUI wird angezeigt.





Anmerkung: Sobald der SSH-Zugriff verfügbar ist, dauert es in der Regel weitere 10 bis 15 Minuten, bis die ISE-Services vollständig in den Betriebszustand übergehen.

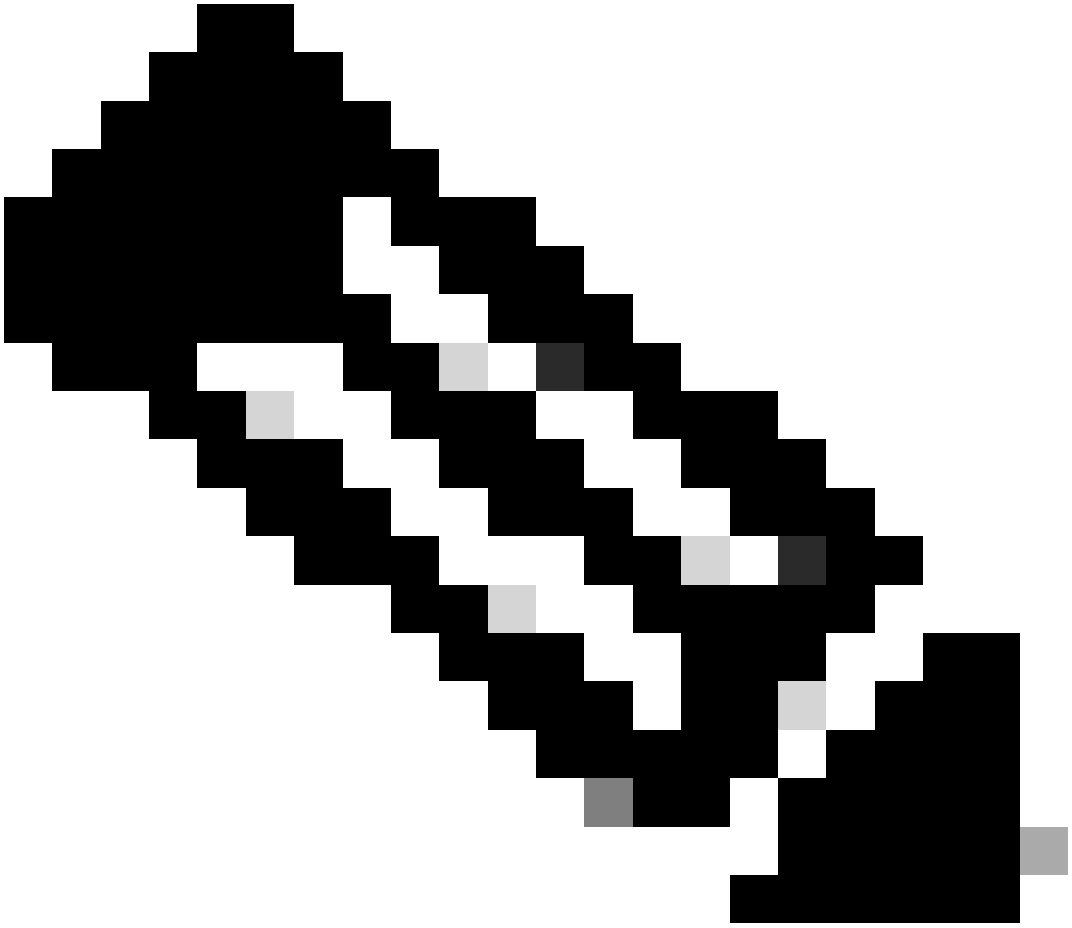
Zugriff auf CLI über SSH vom Terminal

Wählen Sie in der EC2-Konsole Ihre Instanz aus, und klicken Sie auf Verbinden.

Führen Sie auf der Registerkarte SSH-Client die folgenden Schritte aus:

- Navigieren Sie zu dem Ordner, der Ihre heruntergeladene .pem-Schlüsseldatei enthält.
- Führen Sie folgende Befehle aus:

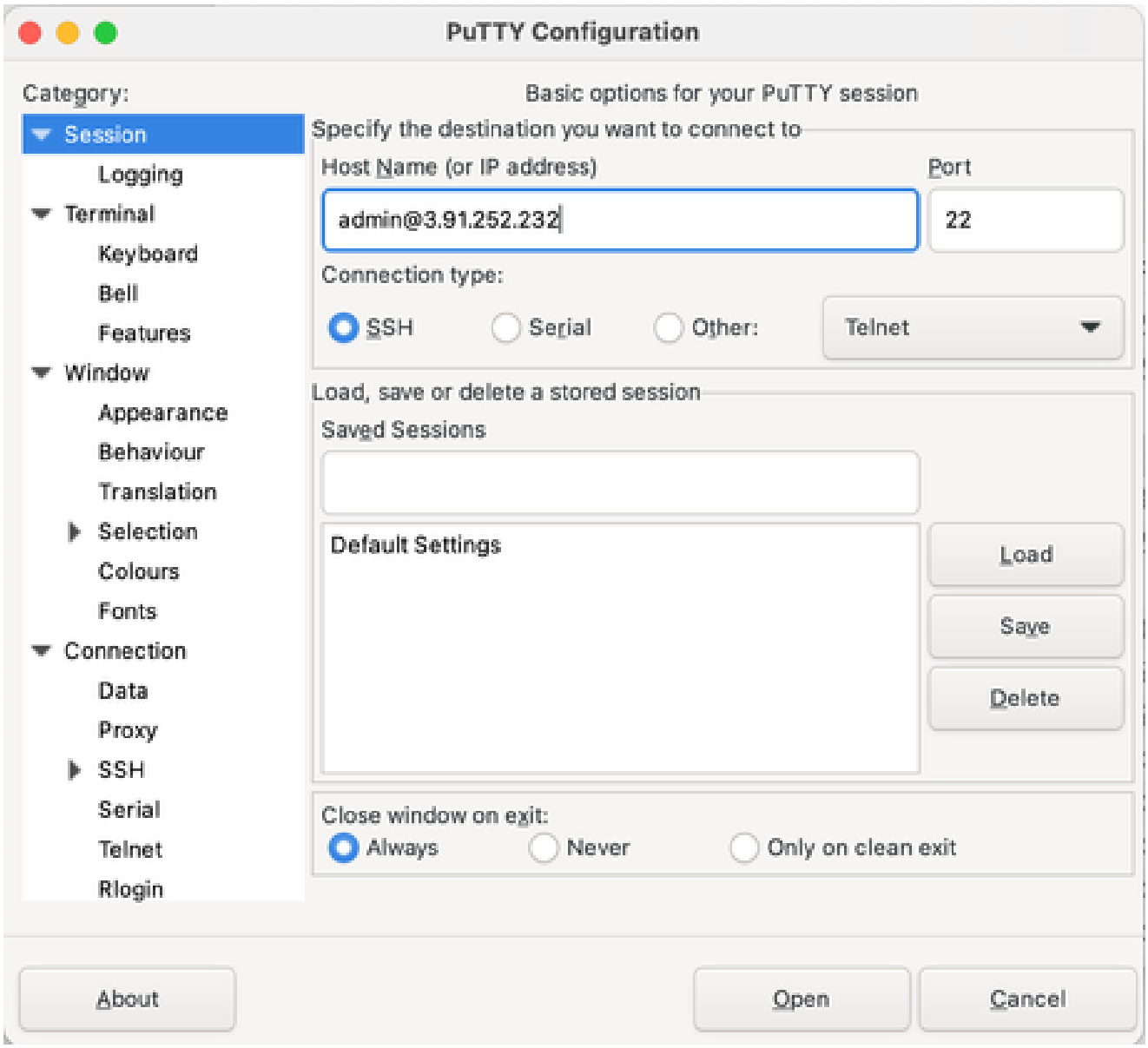
- cd <Pfad zur Schlüsseldatei>
- chmod 400 <Ihr-Schlüsselpaar-Name>.pem
- ssh -i "<Name des Schlüsselpaars>.pem" admin@<öffentliche-IP-Adresse>



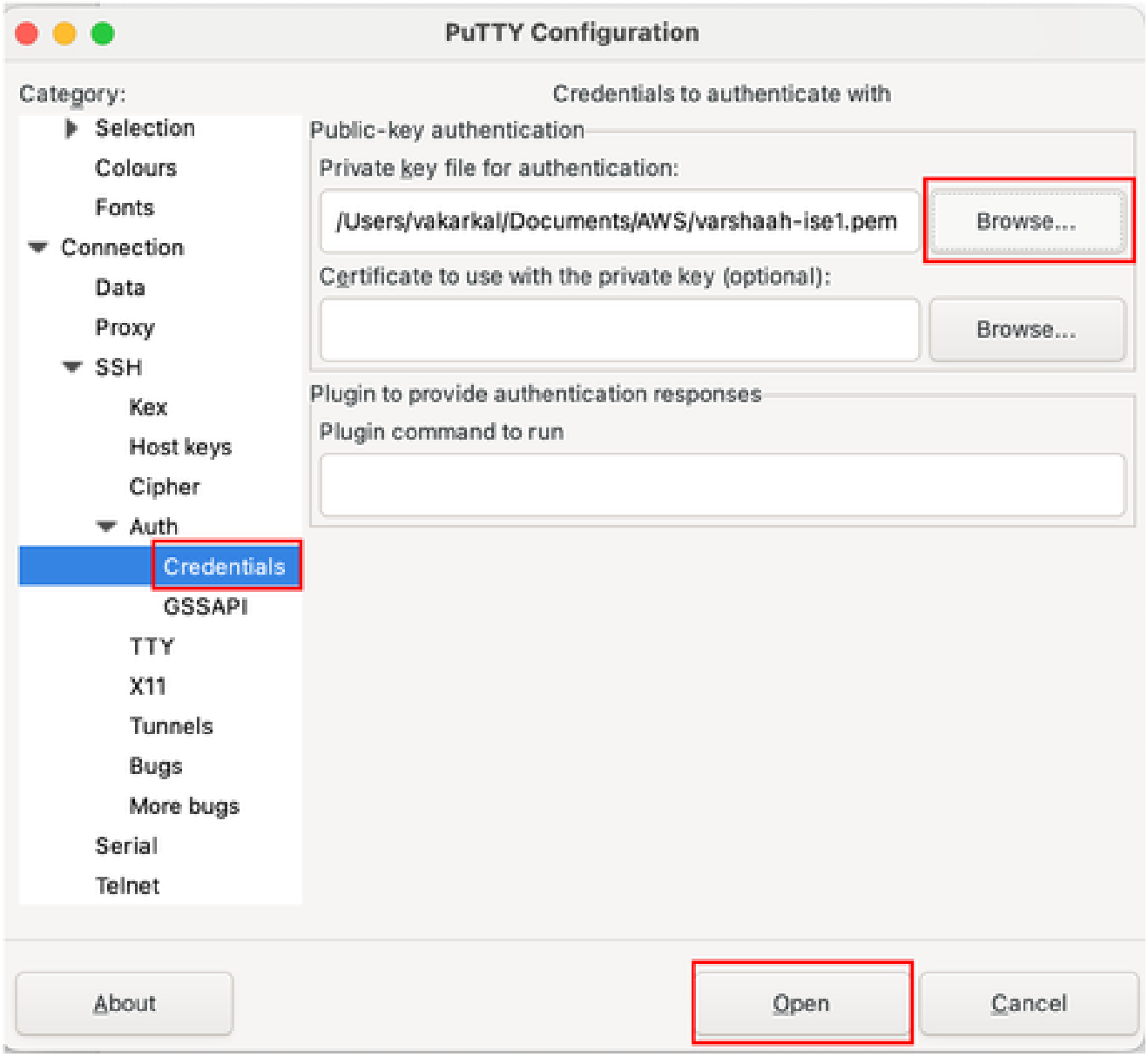
Anmerkung: Verwenden Sie admin als SSH-Benutzer, da die Cisco ISE die Root-Anmeldung über SSH deaktiviert.

Zugriff auf CLI über SSH mit PuTy

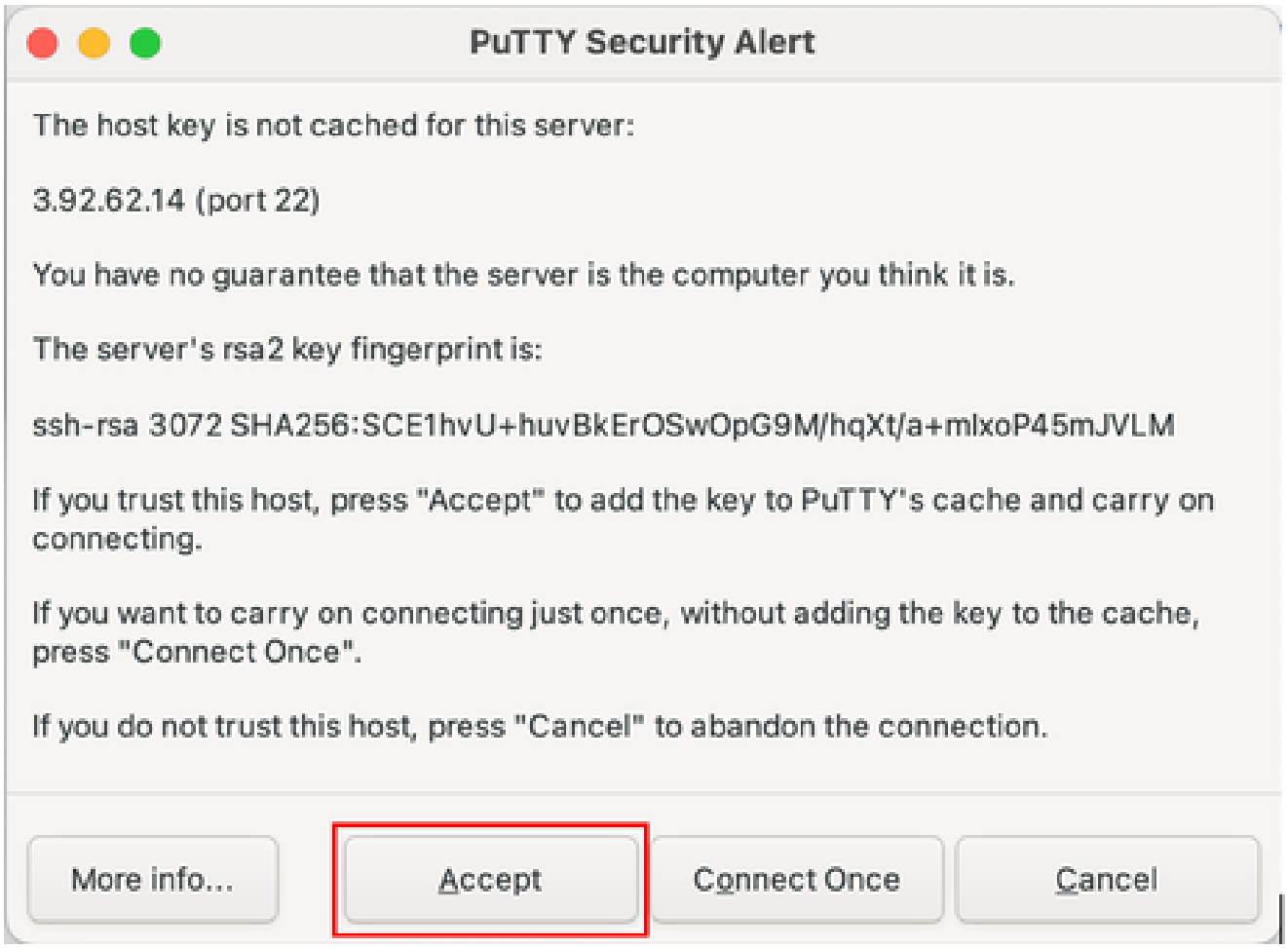
- Öffnen Sie PuTTY.
- Geben Sie im Feld Hostname Folgendes ein: admin@<öffentliche-IP-Adresse>



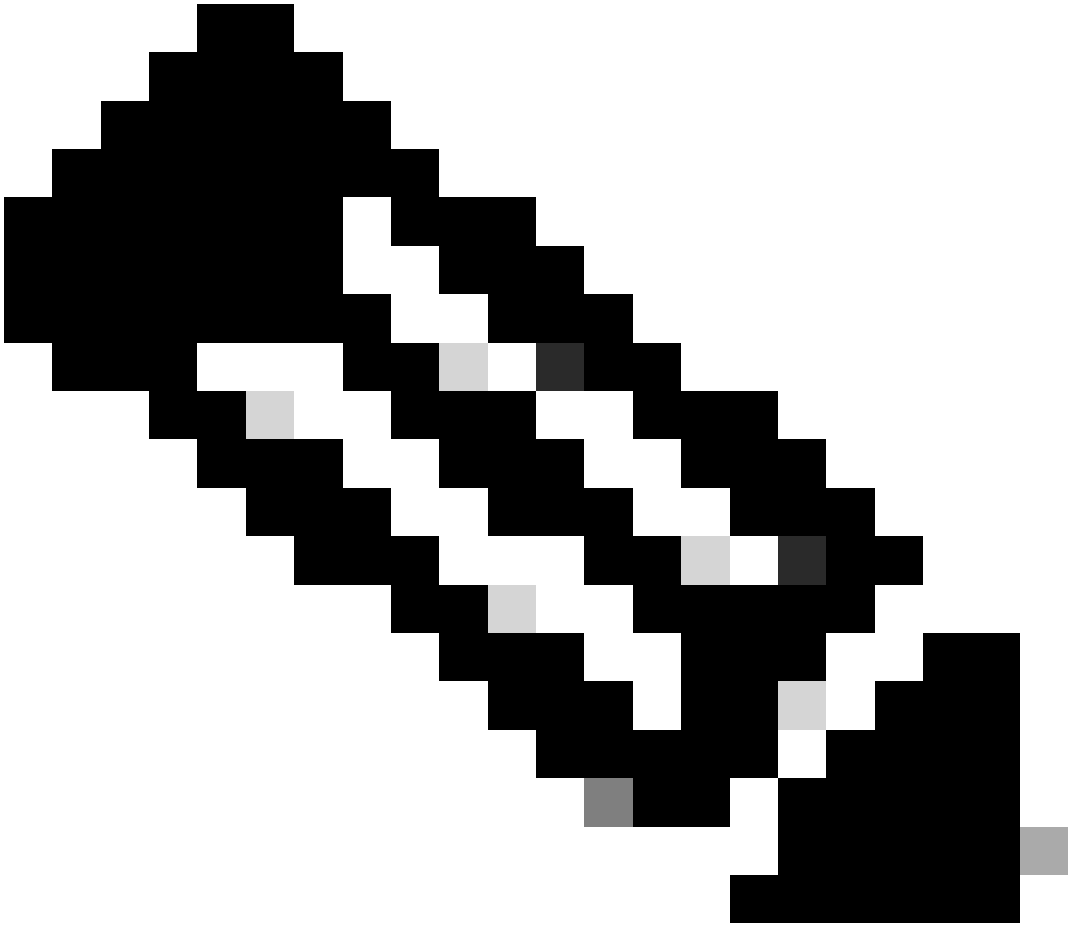
- Navigieren Sie im linken Bereich zu Connection > SSH > Auth > Credentials (Verbindung > SSH > Authentifizierung > Anmeldedaten).
- Klicken Sie neben Private Key File (Datei mit privatem Schlüssel) auf Browse (Durchsuchen), um die Authentifizierung durchzuführen, und wählen Sie die Datei mit dem privaten SSH-Schlüssel aus.
- Klicken Sie auf Öffnen, um die Sitzung zu starten.



- Wenn Sie dazu aufgefordert werden, klicken Sie auf Akzeptieren, um den SSH-Schlüssel zu bestätigen.



- Ihre PuTTY-Sitzung wird nun mit der ISE-CLI verbunden.

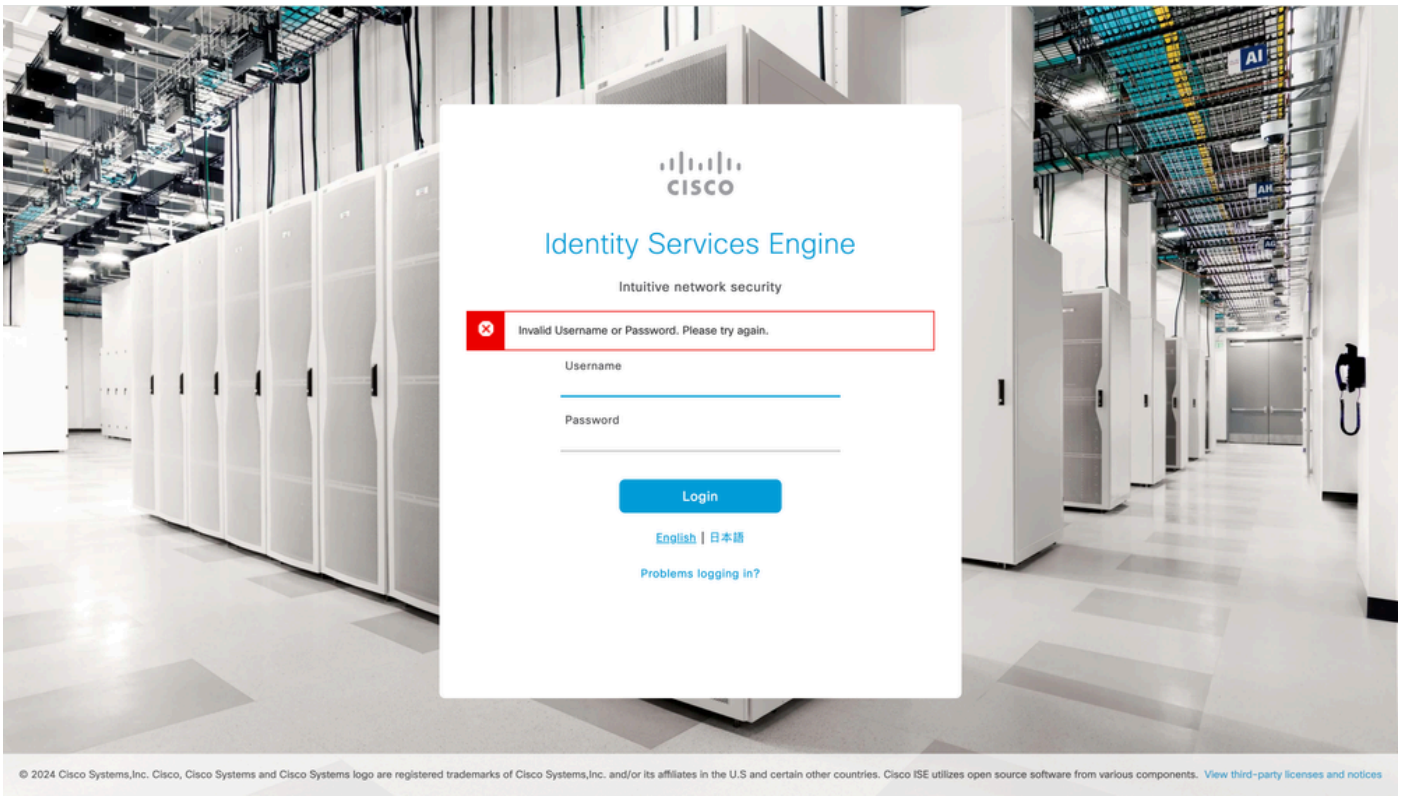


Anmerkung: Es kann bis zu 20 Minuten dauern, bis ISE über SSH erreichbar ist. Während dieser Zeit können Verbindungsversuche fehlschlagen, und zwar mit folgendem Fehler: "Berechtigung verweigert (publickey)."

Fehlerbehebung

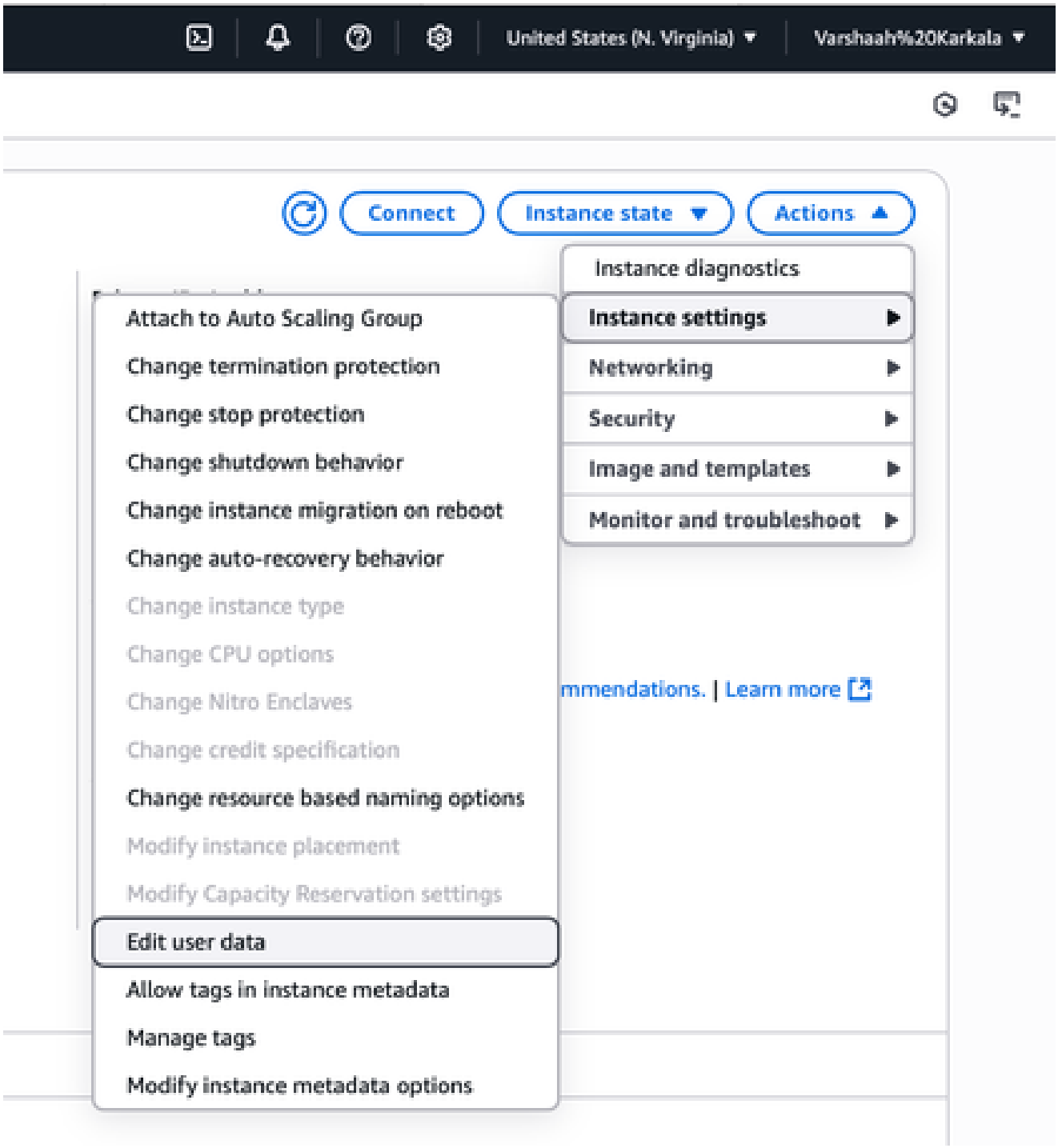
Ungültiger Benutzername oder ungültiges Kennwort

Authentifizierungsprobleme werden häufig durch falsche Benutzereingaben während der Instanzerstellung verursacht. Dies führt zu einer Fehlermeldung wie "Ungültiger Benutzername oder ungültiges Kennwort. Bitte versuchen Sie es erneut." Fehler, wenn versucht wird, sich bei der GUI anzumelden.

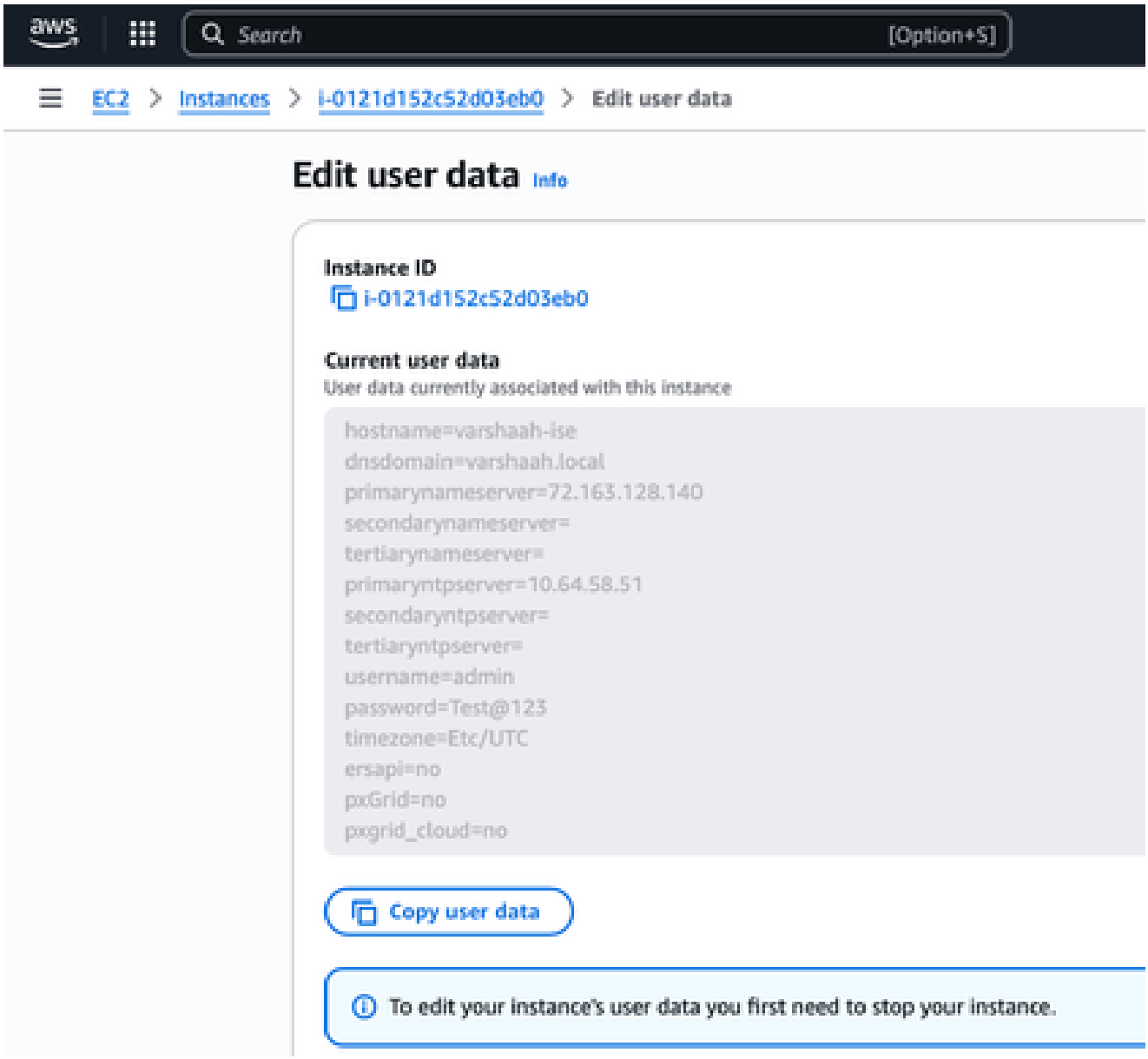


Lösung

- Navigieren Sie in der AWS EC2-Konsole zu EC2 > Instances > your_instance_id.
- Klicken Sie Aktionen > Instanzeinstellungen > Benutzerdaten bearbeiten.



- Hier finden Sie den spezifischen Benutzernamen und das Passwort, die während des Instanzstarts festgelegt wurden. Mit diesen Anmeldeinformationen können Sie sich bei der ISE-GUI anmelden.



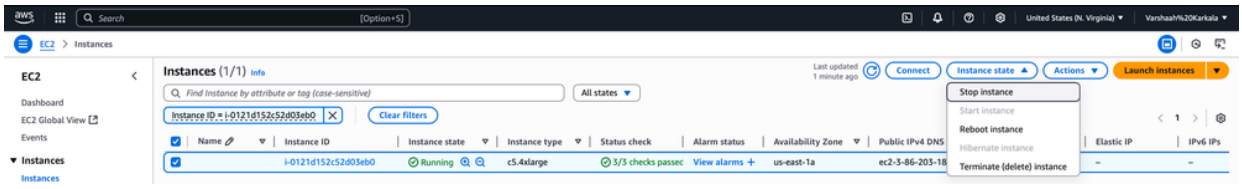
- Überprüfen Sie den Hostnamen und das Kennwort, wenn Sie den Hostnamen und das Kennwort einrichten:
    - Hostname
        - Nur alphanumerische Zeichen und Bindestriche (-) sind zulässig.
        - Die Länge darf 19 Zeichen nicht überschreiten.
    - Kennwort
        - Muss die Cisco ISE-Kennwortrichtlinie erfüllen.
        - Weitere Informationen finden Sie im offiziellen ISE-Administratorhandbuch: ISE 3.4 Kennwortrichtlinie - Cisco Administratorhandbuch

- Wenn das konfigurierte Kennwort nicht der ISE-Kennwortrichtlinie entspricht, schlagen die Anmeldeversuche fehl. auch mit den richtigen Anmeldeinformationen.

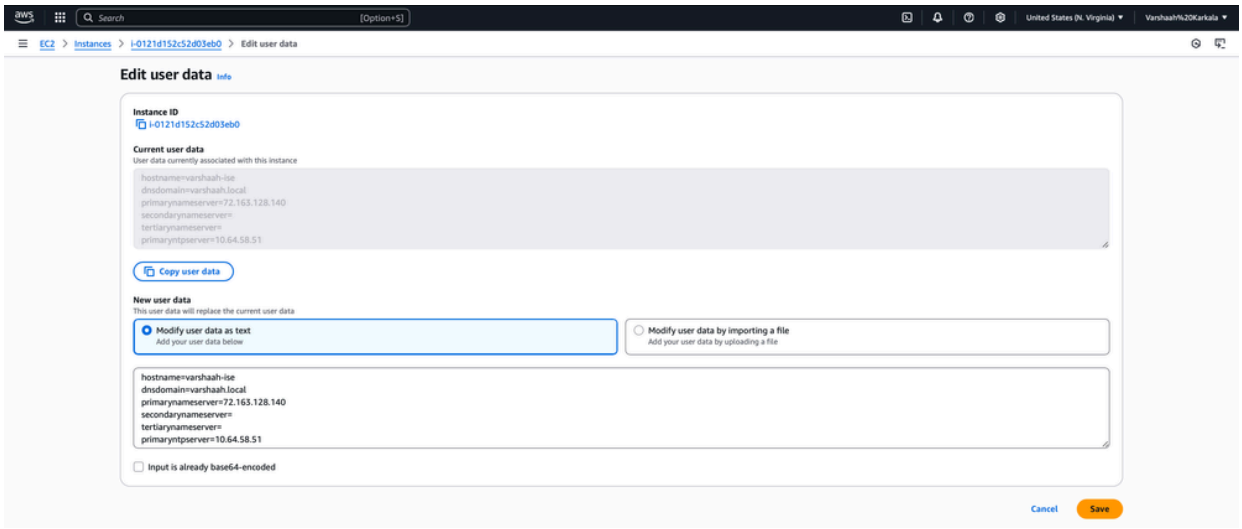
- Wenn Sie vermuten, dass das Kennwort falsch konfiguriert wurde, führen Sie die folgenden Schritte aus, um es zu aktualisieren:

    1. Gehen Sie in der EC2-Konsole zu EC2 > Instances > your_instance_id

    2. Klicken Sie auf Instanzstatus > Instanz beenden.



    3. Nachdem die Instanz beendet wurde, klicken Sie auf Aktionen > Instanzeinstellungen > Benutzerdaten bearbeiten.



    4. Ändern Sie das Benutzerdatenskript, um das Kennwort entsprechend zu aktualisieren.

    5. Speichern Sie die Änderungen, und starten Sie die Instanz über Instance state > Start instance neu.

Bekannte Fehler

Bug-ID	Beschreibung
Cisco Bug-ID: 41693	ISE auf AWS kann keine Benutzerdaten abrufen, wenn die Metadatenversion auf "Nur V2" festgelegt ist. Nur IMDSv1 wird in Versionen

	vor ISE 3.4 unterstützt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.