Distribuire Identity Services Engine (ISE) versione 3.4 su AWS

Sommario

Introduzione

Questo documento descrive come configurare Cisco ISE su AWS utilizzando il modello CloudFormation (CFT) e Amazon Machine Image (AMI).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di procedere con questa distribuzione:

- Cisco Identity Services Engine (ISE)
- Gestione e rete di istanze AWS EC2
- Generazione e uso della coppia di chiavi SSH
- Conoscenze base di VPC, gruppi di sicurezza e configurazione DNS/NTP in AWS

Componenti usati

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

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

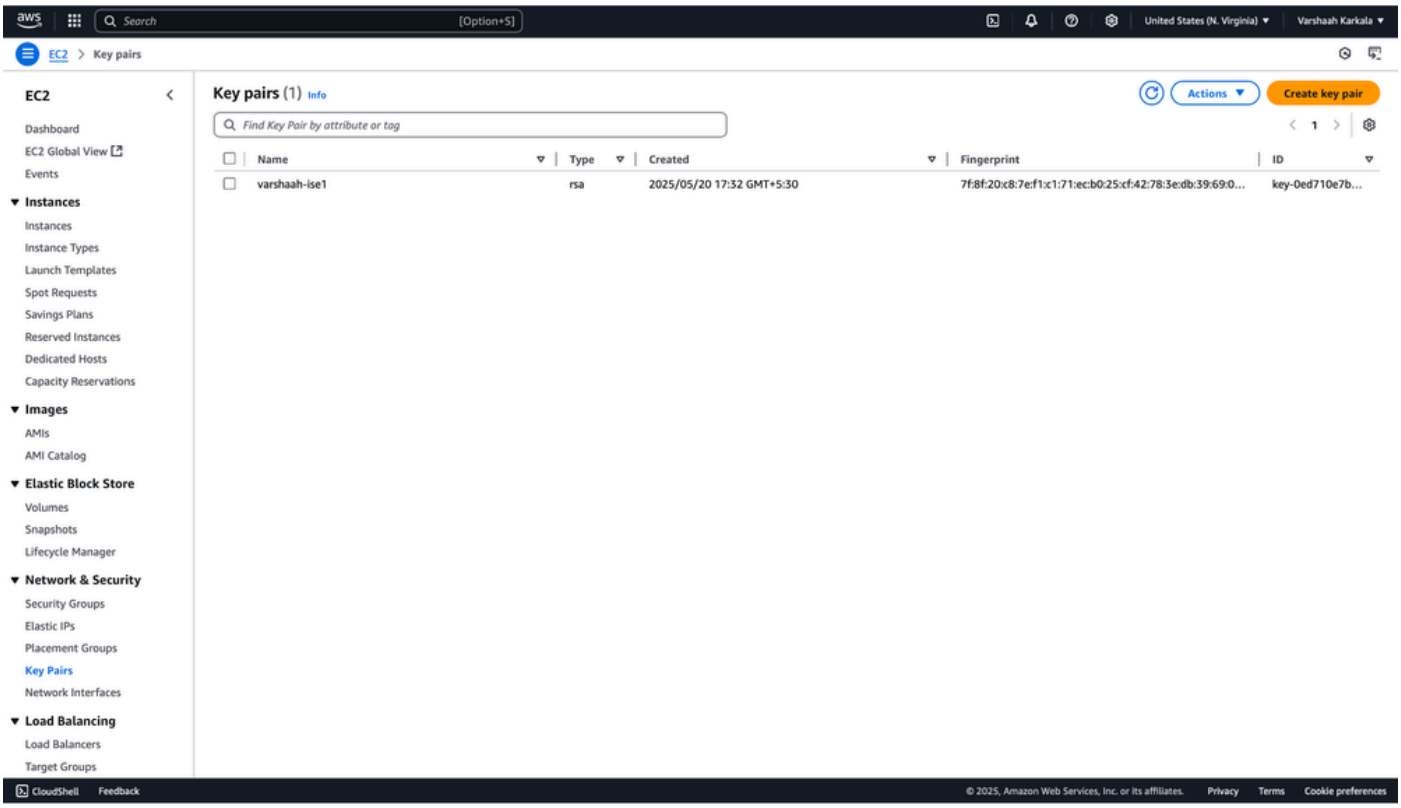
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

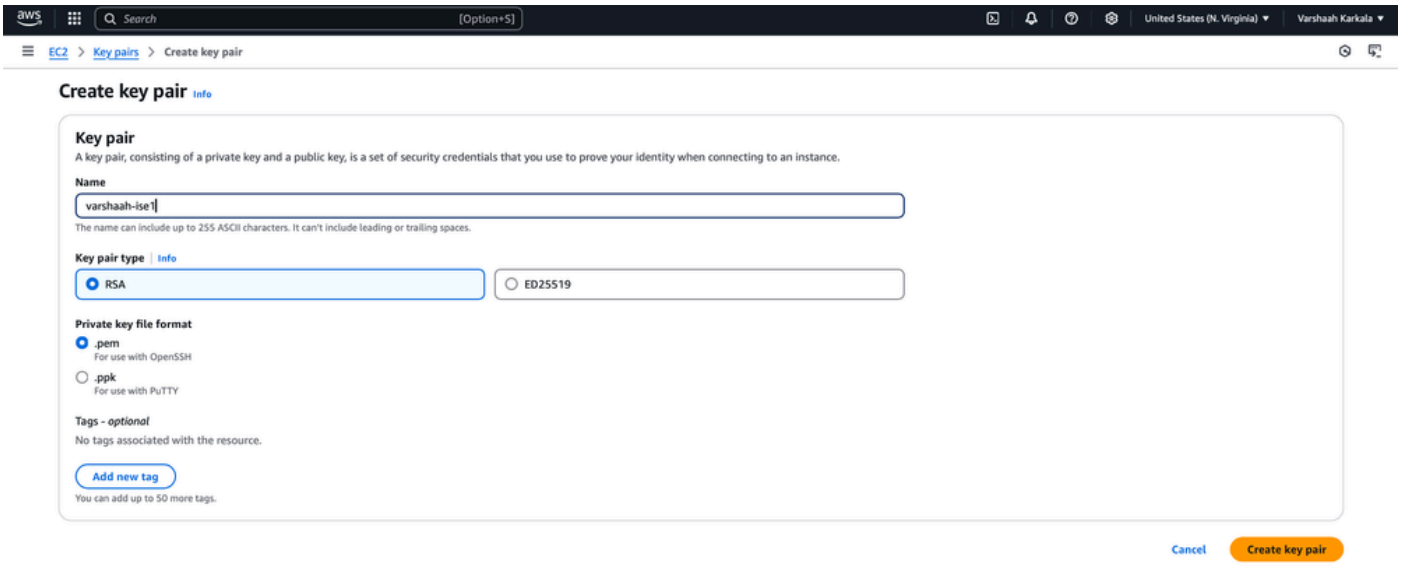
Parte 1: Generazione di una coppia di chiavi SSH

1. Per questa distribuzione è possibile utilizzare una coppia di chiavi preesistente oppure crearne una nuova.

2. Per creare una nuova coppia, selezionare EC2 > Rete e sicurezza > Coppie di chiavi e fare clic su Crea coppia di chiavi.



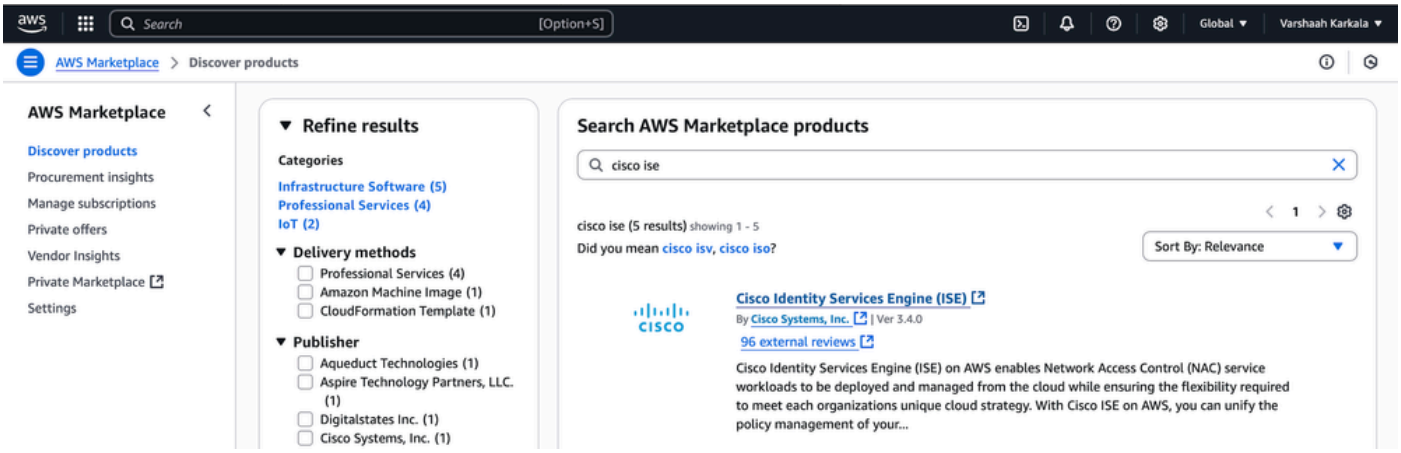
3. Immettere il nome della coppia di chiavi e fare clic su Crea coppia di chiavi.

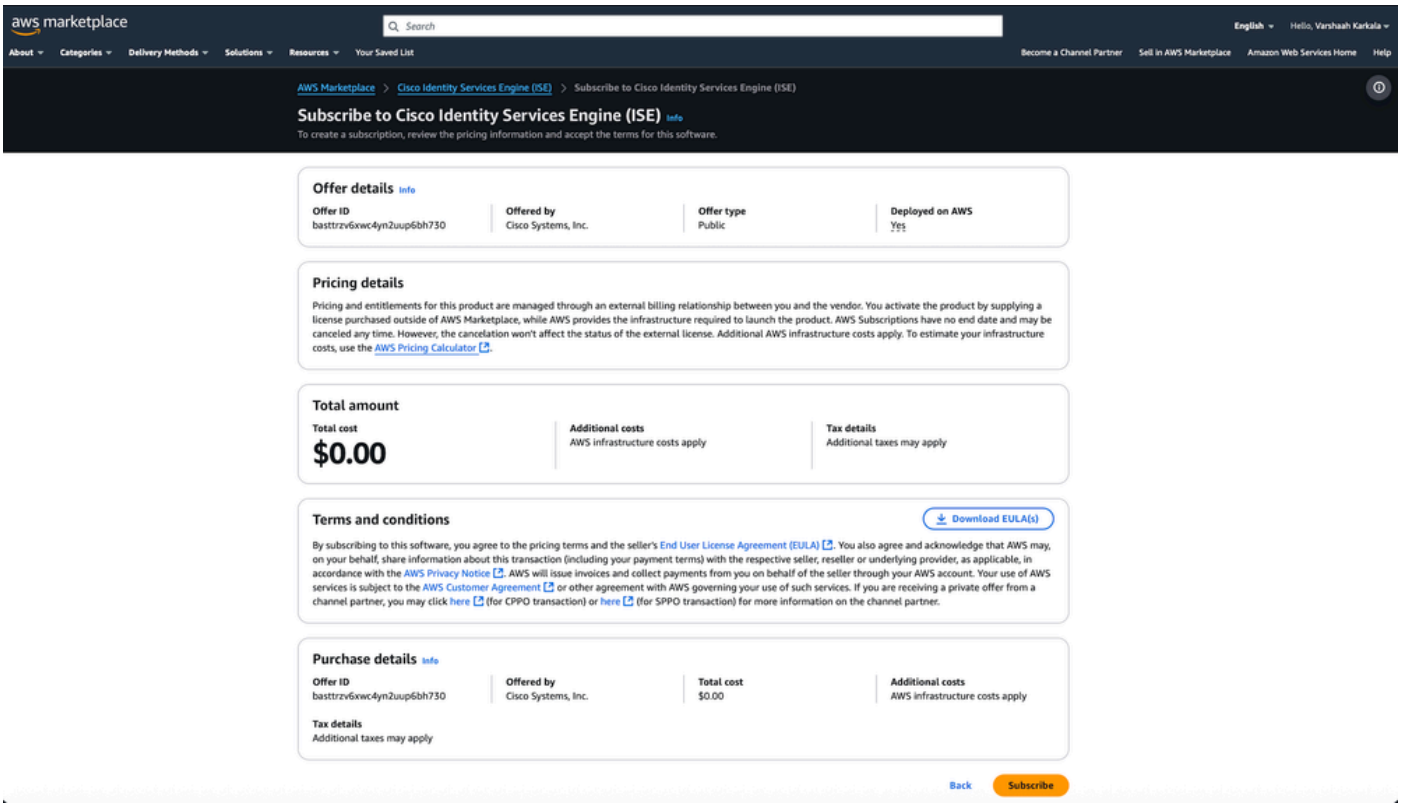


Il file della coppia di chiavi (.pem) viene scaricato nel computer locale. Accertarsi di conservare il file in modo sicuro, poiché questo è l'unico modo per accedere all'istanza EC2 una volta avviata.

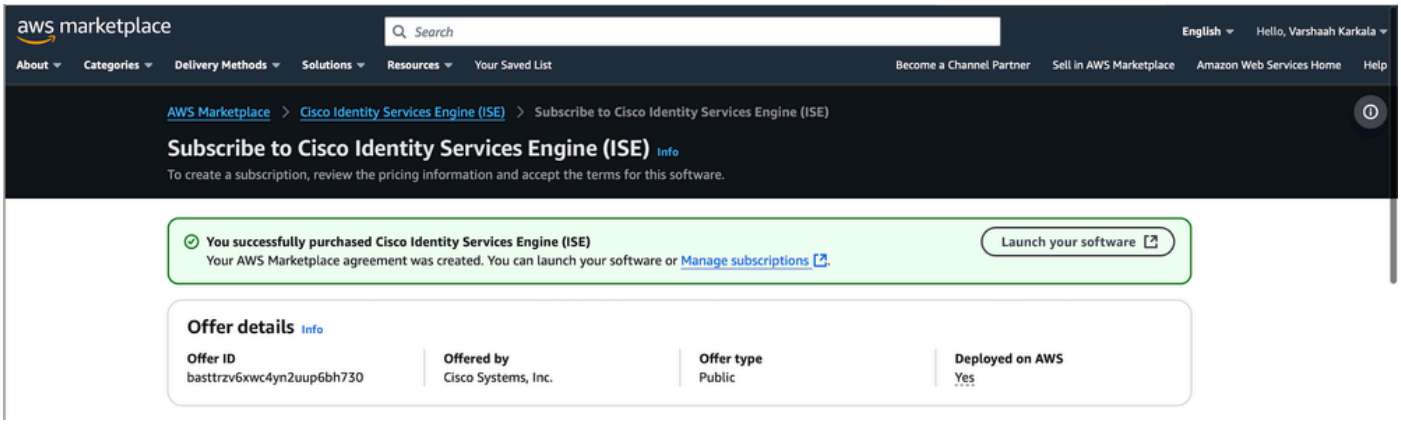
Parte 2: Configurazione di ISE con un modello CloudFormation (CFT)

1. Accedere alla console di gestione AWS e cercare sottoscrizioni AWS Marketplace.
2. Nella barra di ricerca, digitare cisco ISE e fare clic su Cisco Identity Services Engine (ISE) dai risultati. Fare clic su Sottoscrivi.

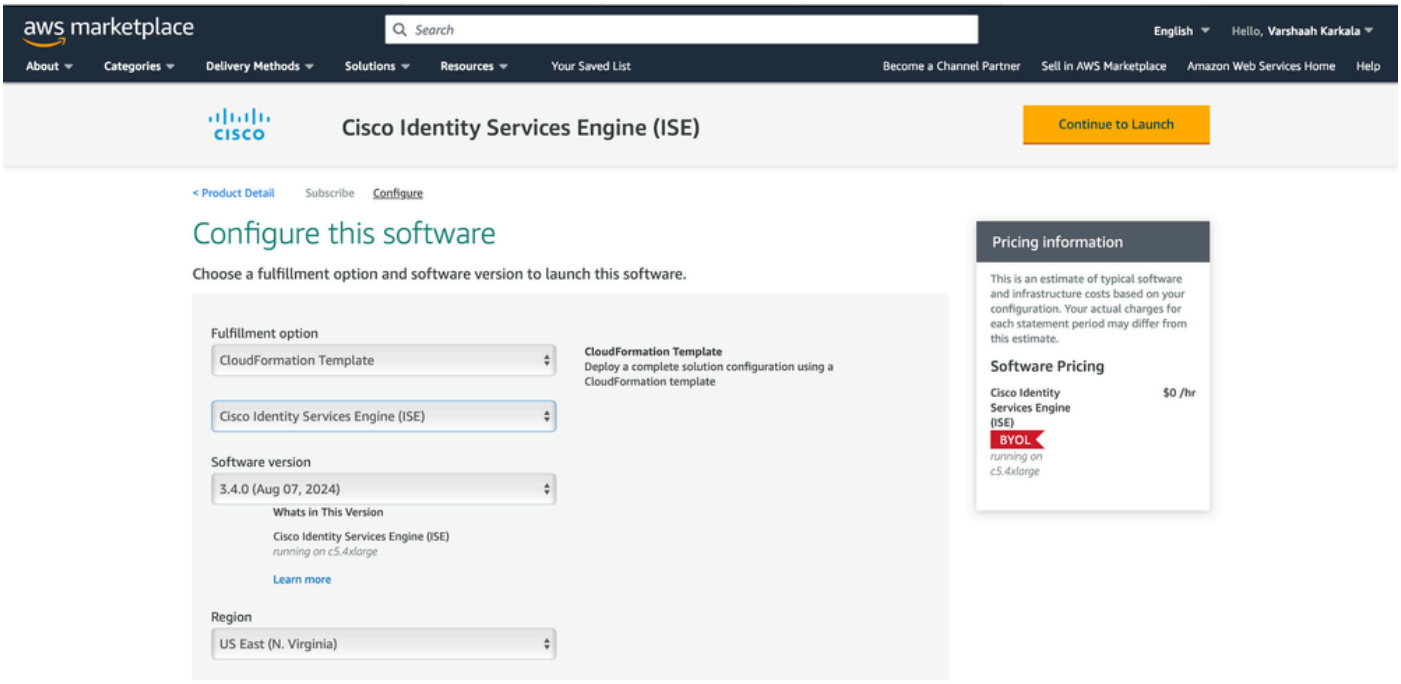




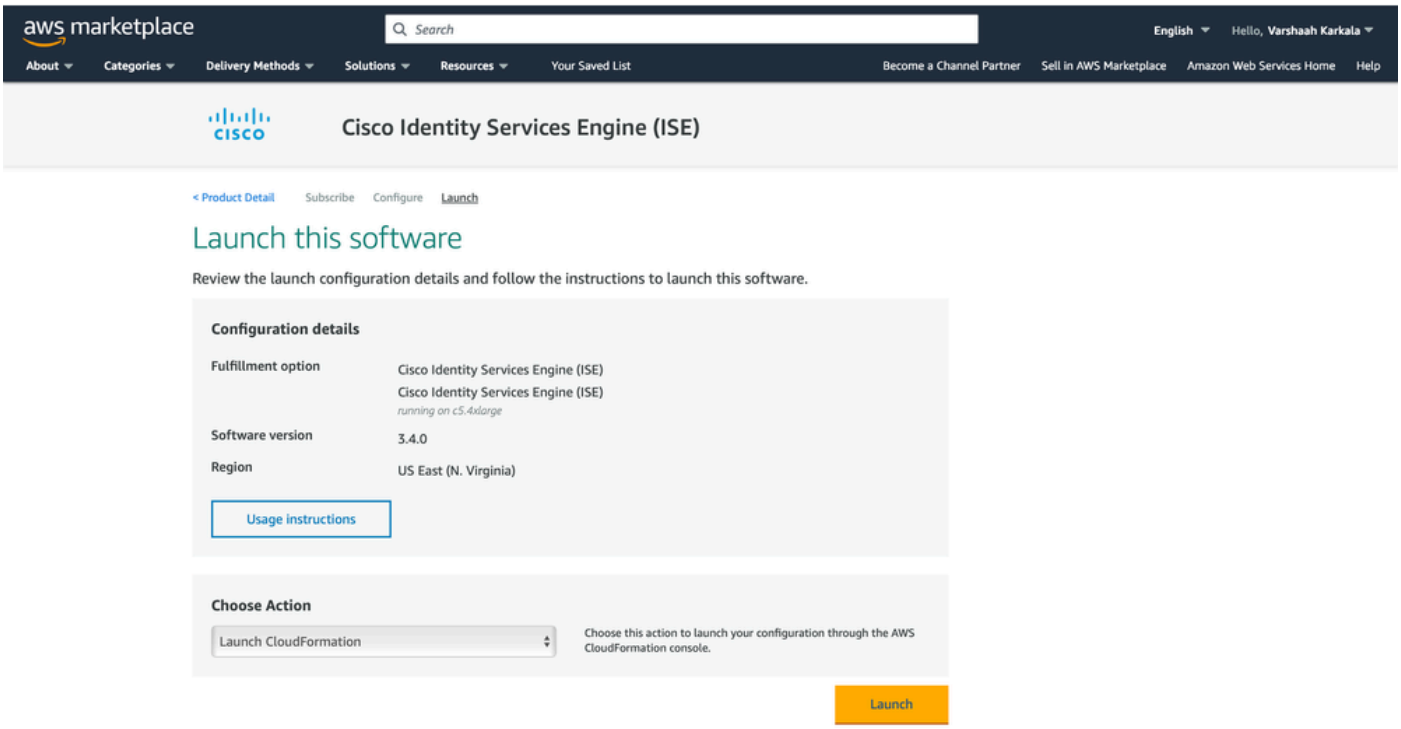
3. Dopo aver effettuato l'abbonamento, fare clic su Avvia il software.



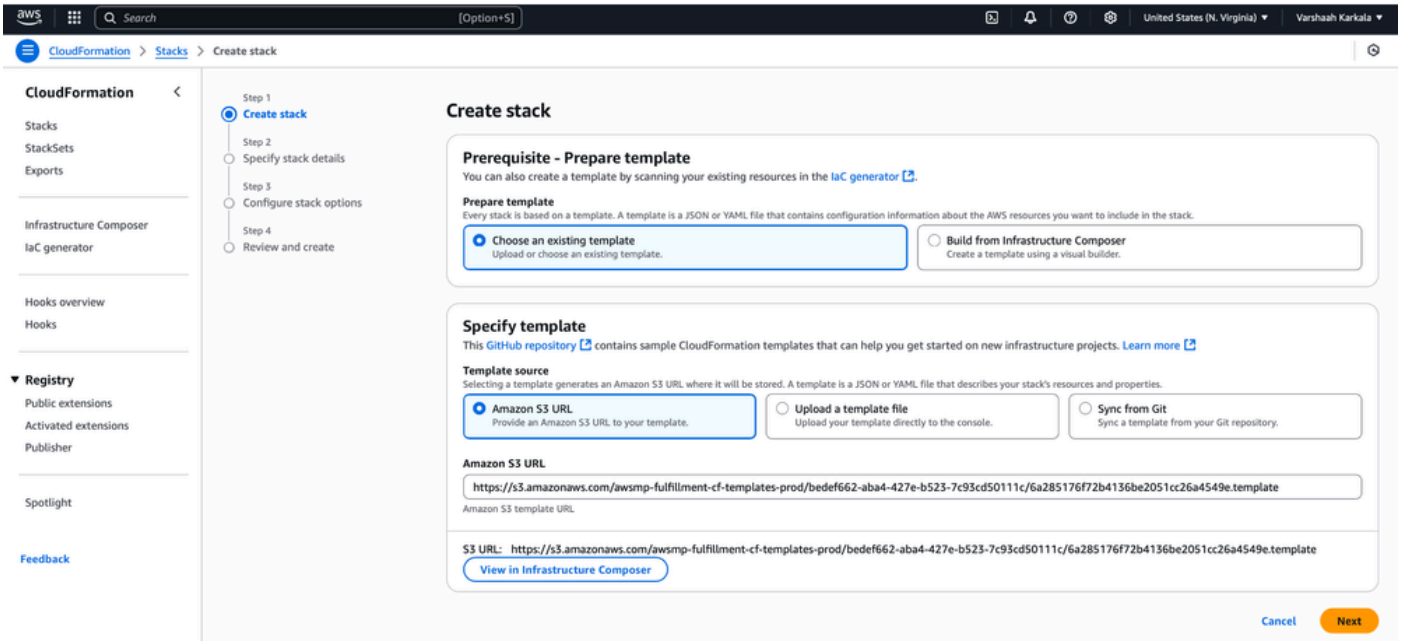
4. In Opzione di evasione, scegliere Modello di formazione cloud. Scegliere la versione del software (versione ISE) e la regione in cui si desidera distribuire l'istanza. Fare clic su Continua per avviare.



5. Nella pagina successiva, scegliere Launch CloudFormation come azione e fare clic su Launch (Avvia).

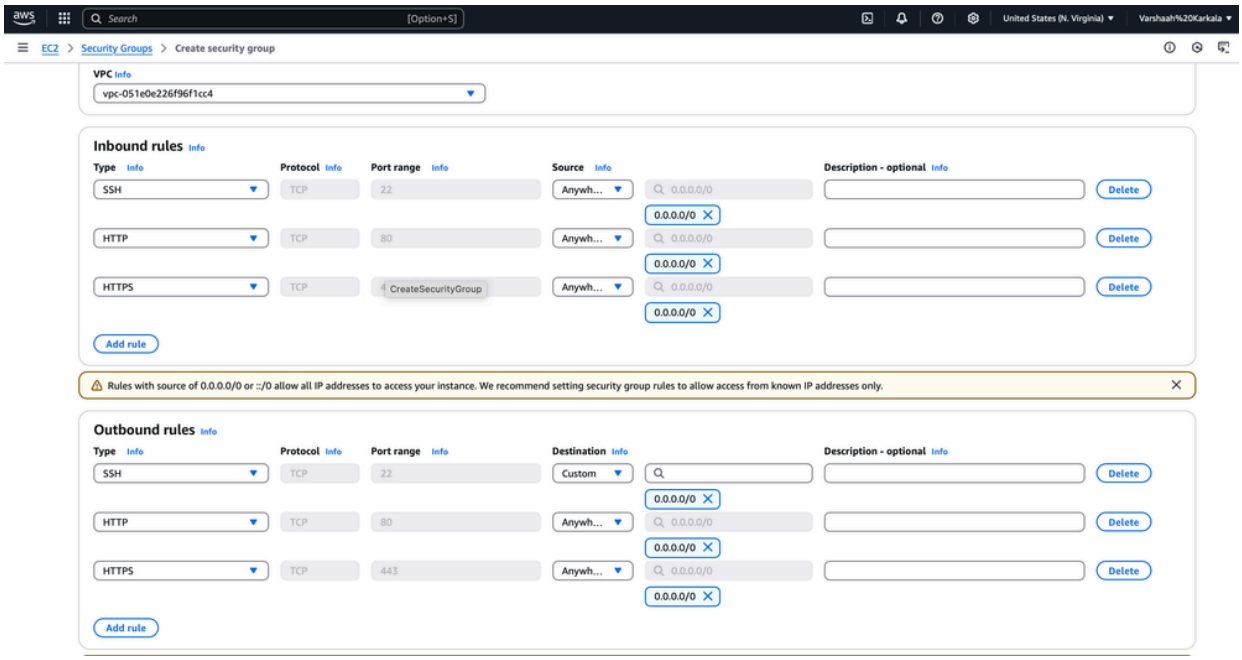


6. Sotto le impostazioni dello stack, mantenere le impostazioni predefinite e fare clic su Avanti.



7. Inserire i parametri obbligatori:

- Nome stack: Assegnare un nome univoco allo stack.
- Nome host: Assegnare il nome host per il nodo ISE.
- Coppia di tasti: Selezionare la coppia di chiavi generata o preesistente per accedere all'istanza EC2 in un secondo momento.
- Gruppo di sicurezza di gestione:
    - Utilizzare il gruppo di sicurezza predefinito (come illustrato) oppure crearne uno personalizzato tramite il dashboard EC2.
    - Per creare un nuovo gruppo di sicurezza, passare al Dashboard EC2 e selezionare Rete e sicurezza > Gruppi di sicurezza per creare un nuovo gruppo di sicurezza.
    - Fare clic su Crea gruppo di sicurezza e immettere i dettagli richiesti.
    - Verificare che il gruppo di sicurezza sia configurato in modo da consentire il traffico in entrata e in uscita richiesto. Ad esempio, abilitare l'accesso SSH (porta 22) dall'indirizzo IP per l'accesso alla CLI.

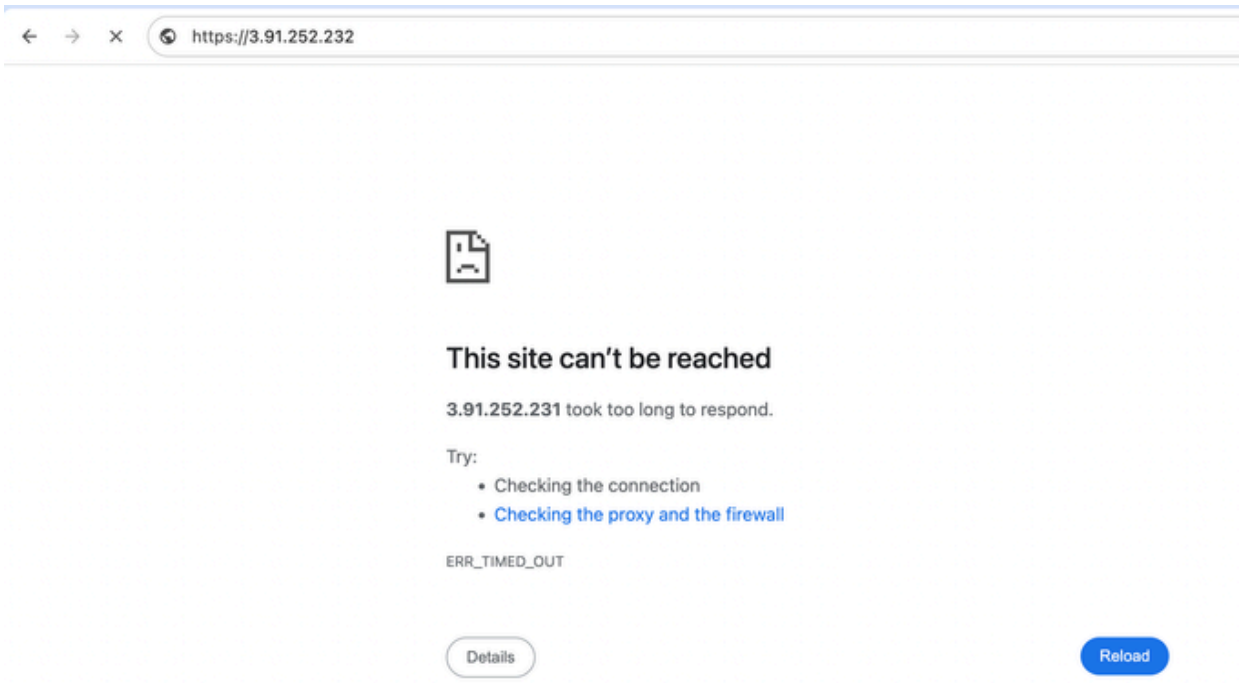


- Se l'accesso SSH non è configurato correttamente, potrebbe essere visualizzato un errore di "Timeout dell'operazione" quando si cerca di connettersi tramite SSH.

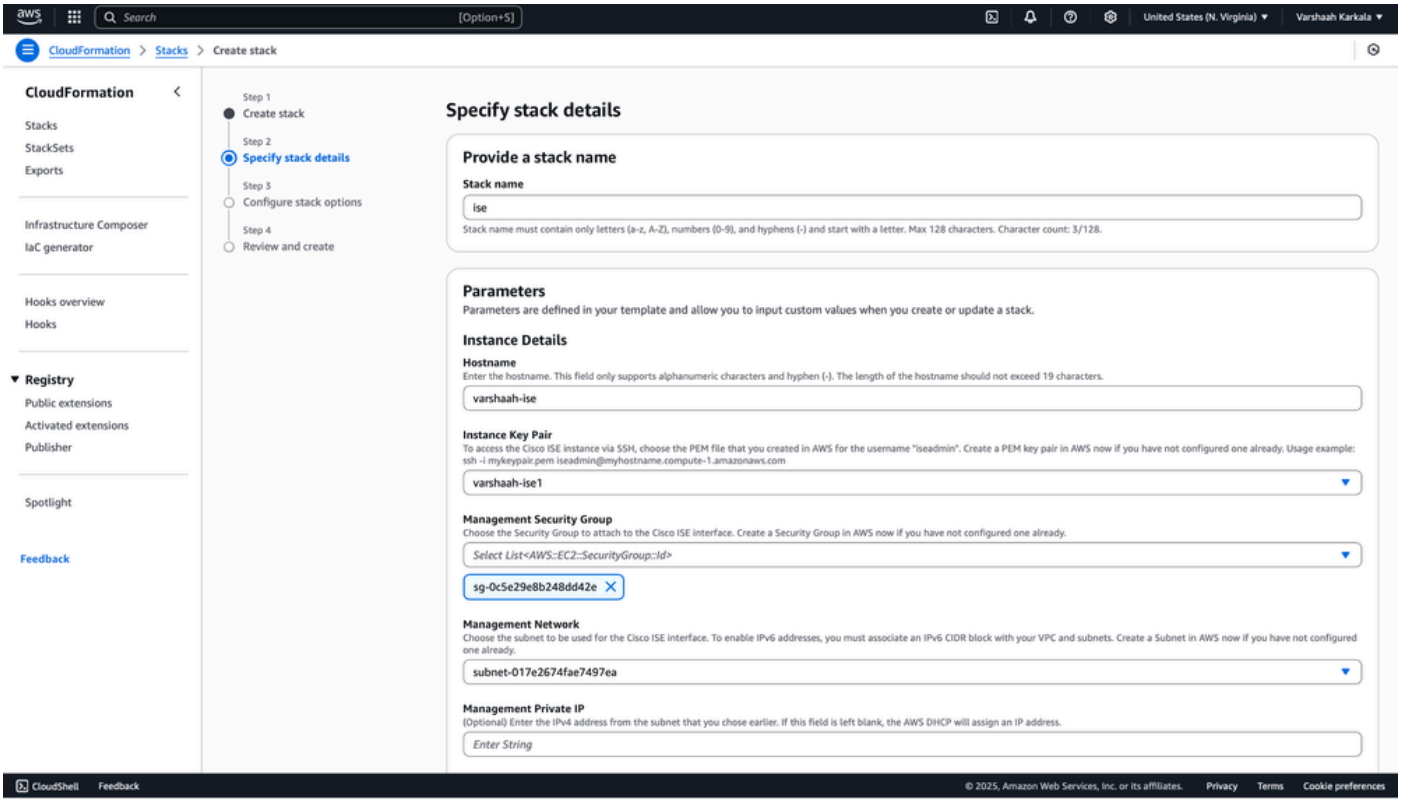
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

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

- Se l'accesso HTTP/HTTPS non è configurato, è possibile che venga visualizzato l'errore "Impossibile raggiungere questo sito" quando si tenta di accedere alla GUI.



- Rete di gestione: viene selezionata una delle subnet preesistenti.



Se la progettazione richiede una distribuzione distribuita con alcuni nodi ospitati in AWS e altri in locale, configurare un VPC dedicato con una subnet privata e stabilire un tunnel VPN per il dispositivo headend VPN in locale per abilitare la connettività tra i nodi ISE ospitati e locali.

Per i dettagli sulla configurazione del dispositivo headend VPN, consultare questa guida.

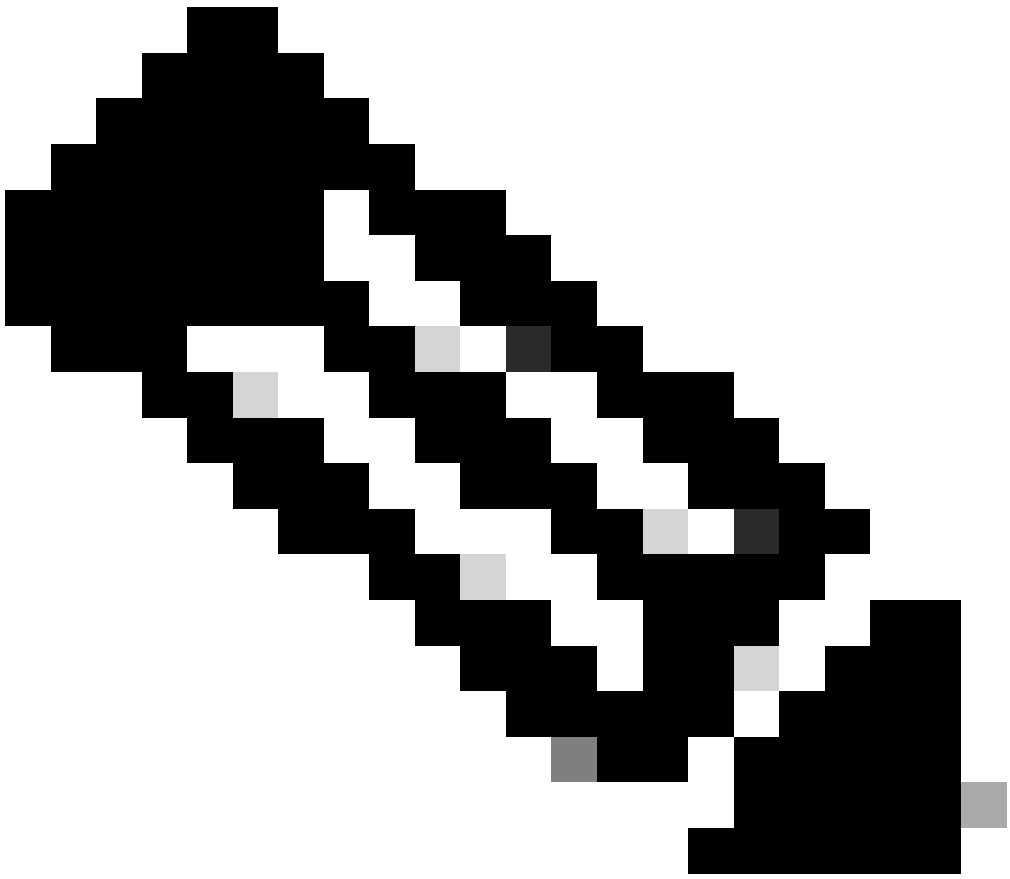
8. Crittografia EBS

- Scorrere verso il basso per individuare le impostazioni di crittografia EBS.
- Impostare EBS Encryption su False a meno che non si abbiano esigenze di crittografia specifiche.

9. Configurazione della rete:

- Scorrere verso il basso per accedere alle opzioni per la configurazione delle impostazioni di rete, ad esempio il dominio DNS, il server dei nomi primario e il server NTP primario.

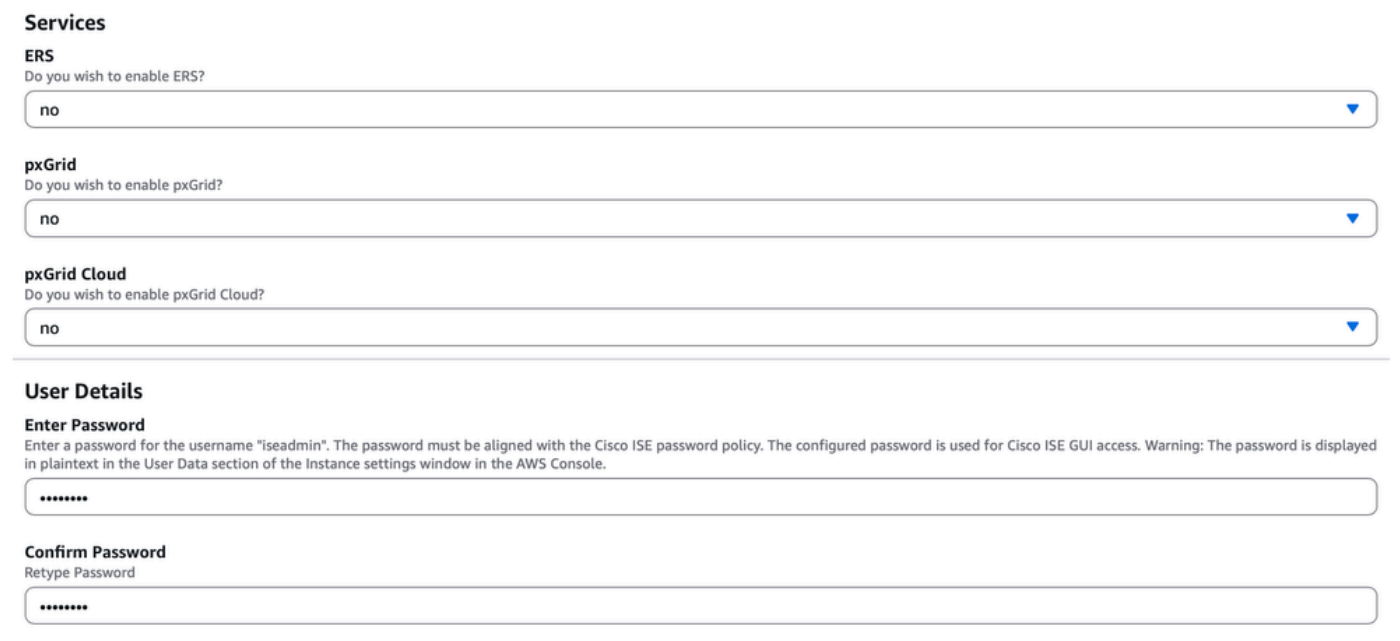
  Accertarsi che questi valori vengano immessi accuratamente.



Nota: Una sintassi errata può impedire il corretto avvio dei servizi ISE dopo l'implementazione.

10. Dettagli utente e servizio:

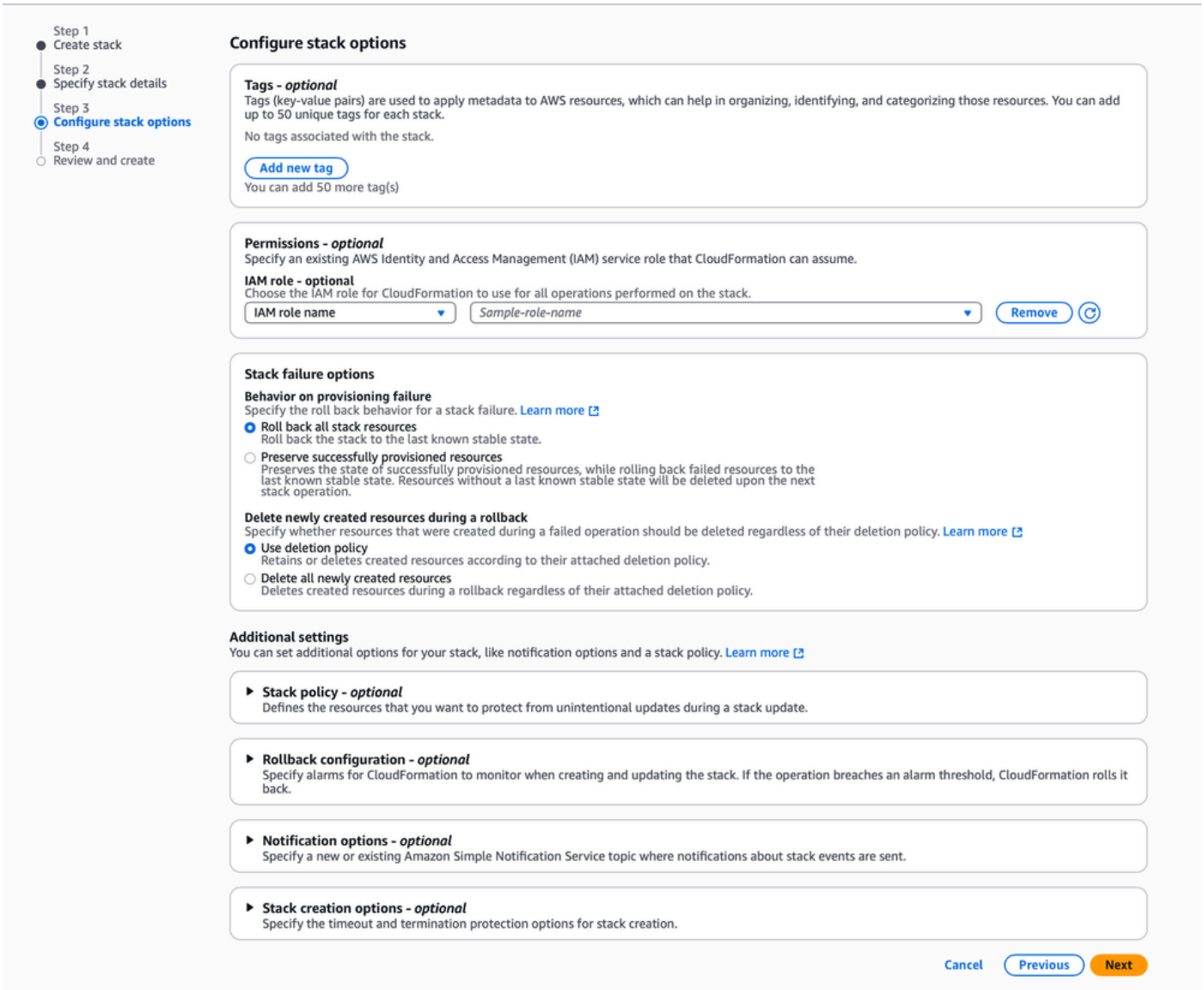
- Scorrere verso il basso per individuare l'opzione di abilitazione dei servizi ERS e pxGrid
- Scegliere se abilitare i servizi ERS e pxGrid selezionando sì o no.
- In Dettagli utente, impostare la password per l'utente amministratore predefinito.



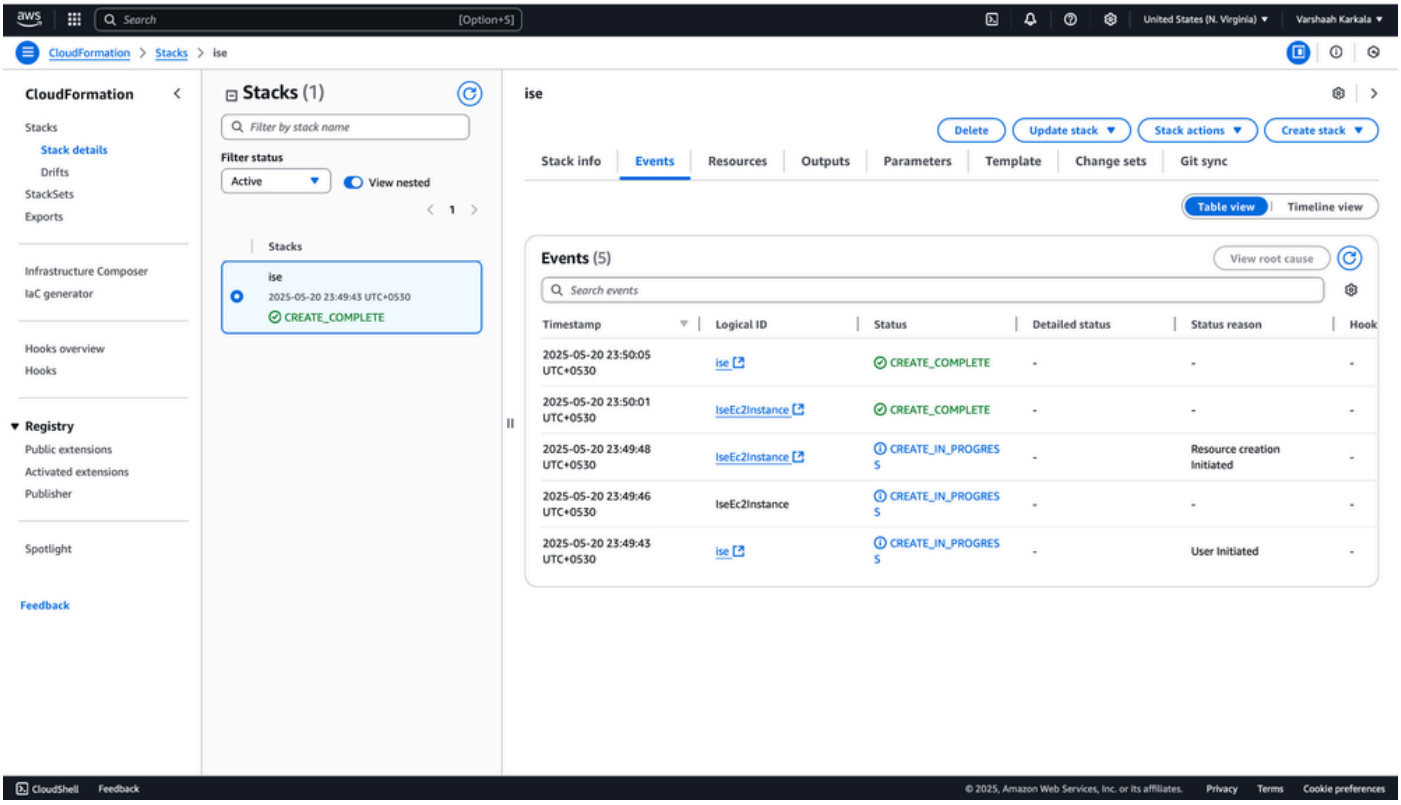
- Fare clic su Next (Avanti).

11. Configurare le opzioni dello stack:

- Lasciare invariate tutte le opzioni predefinite e fare clic su Avanti.



12. Esaminare il modello per verificare che tutte le configurazioni siano corrette, quindi fare clic su Invia. Una volta creato, il modello è simile all'esempio riportato di seguito:



13. Accedere ai dettagli dello stack:
Passare a CloudFormazione > Stack e individuare lo stack distribuito.

14. Scheda Output vista:

Selezionare lo stack e aprire la scheda Output. Qui sono disponibili importanti informazioni generate durante il processo di distribuzione, ad esempio:

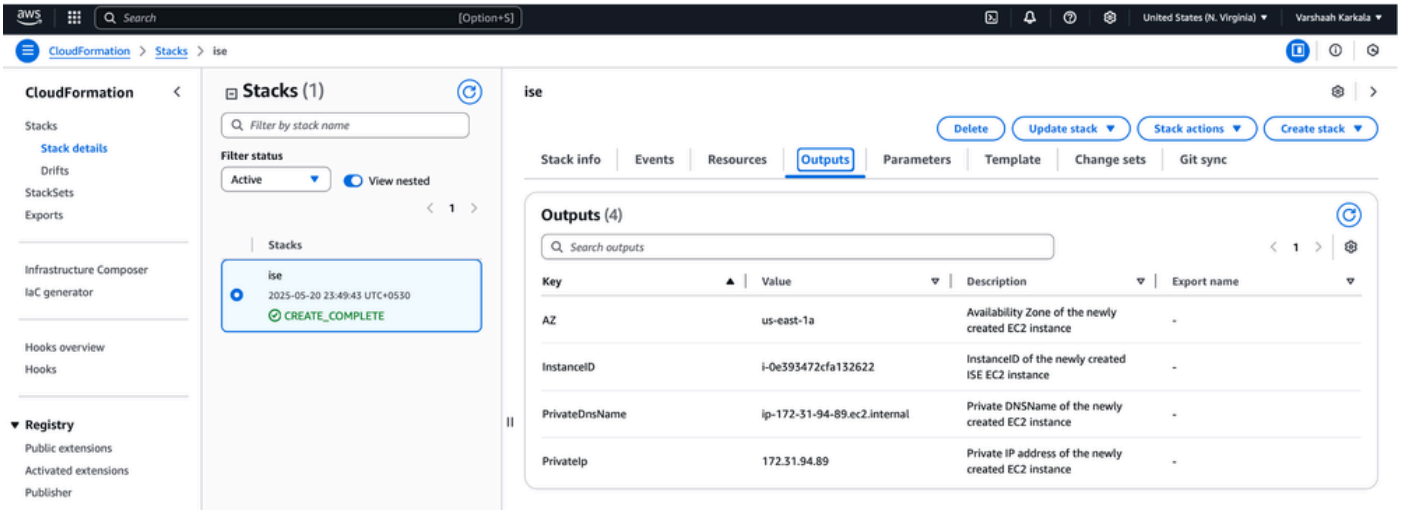
· Zona di disponibilità: Regione in cui vengono distribuite le risorse.

· ID istanza: Identificatore univoco dell'istanza distribuita.

· Nome DNS: Nome DNS privato dell'istanza, che può essere utilizzato per l'accesso remoto.

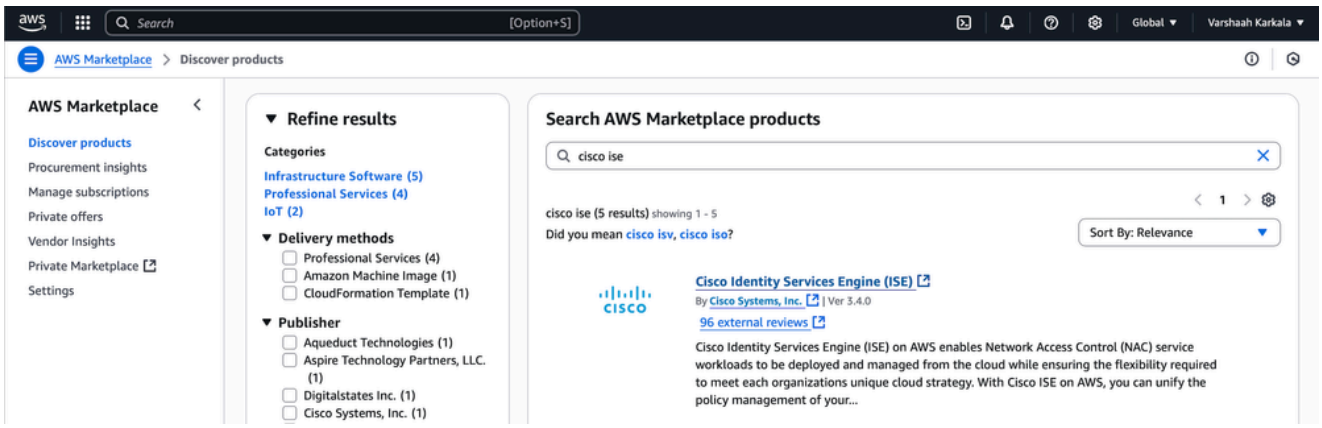
•Indirizzo IP: L'indirizzo IP pubblico o privato dell'istanza, a seconda della configurazione.

Queste informazioni consentono di connettersi all'istanza e verificarne la disponibilità. La scheda Output è simile all'esempio seguente:



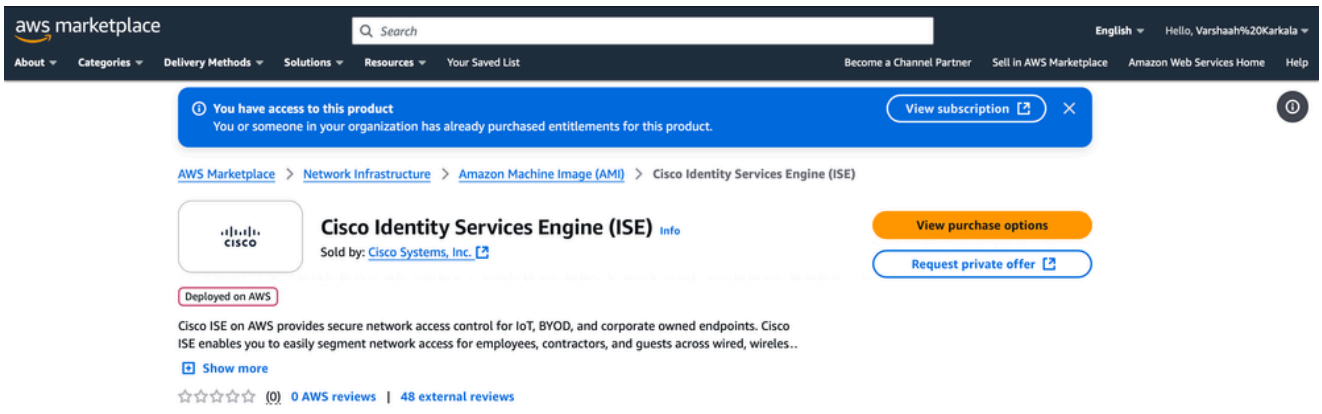
Parte 3: Configurazione di ISE con un Amazon Machine Image (AMI)

1. Accedere alla console di gestione AWS e cercare sottoscrizioni AWS Marketplace.
2. Nella barra di ricerca, digitare cisco ISE e fare clic su Cisco Identity Services Engine (ISE) dai risultati.

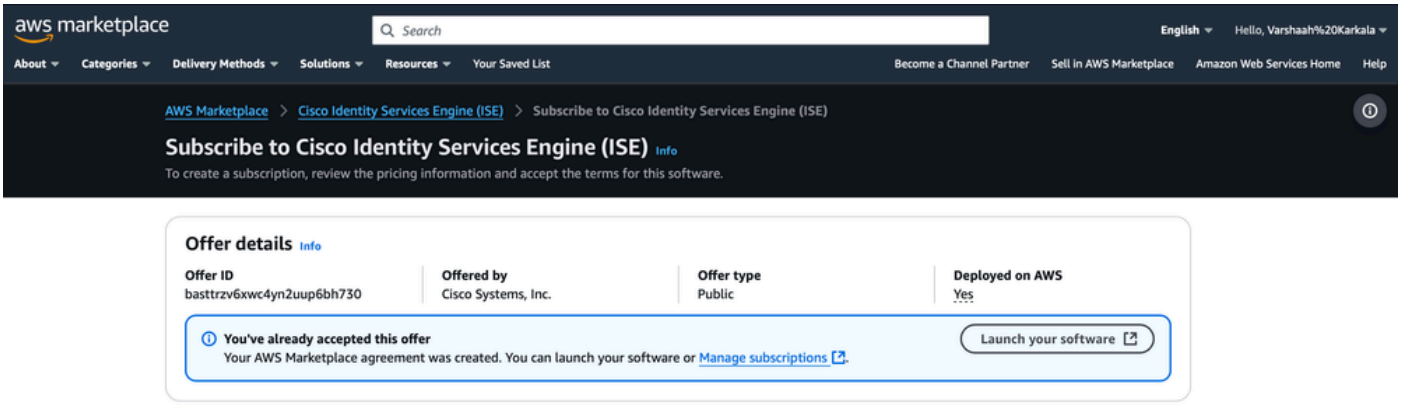


ISE - AWS Markeplace

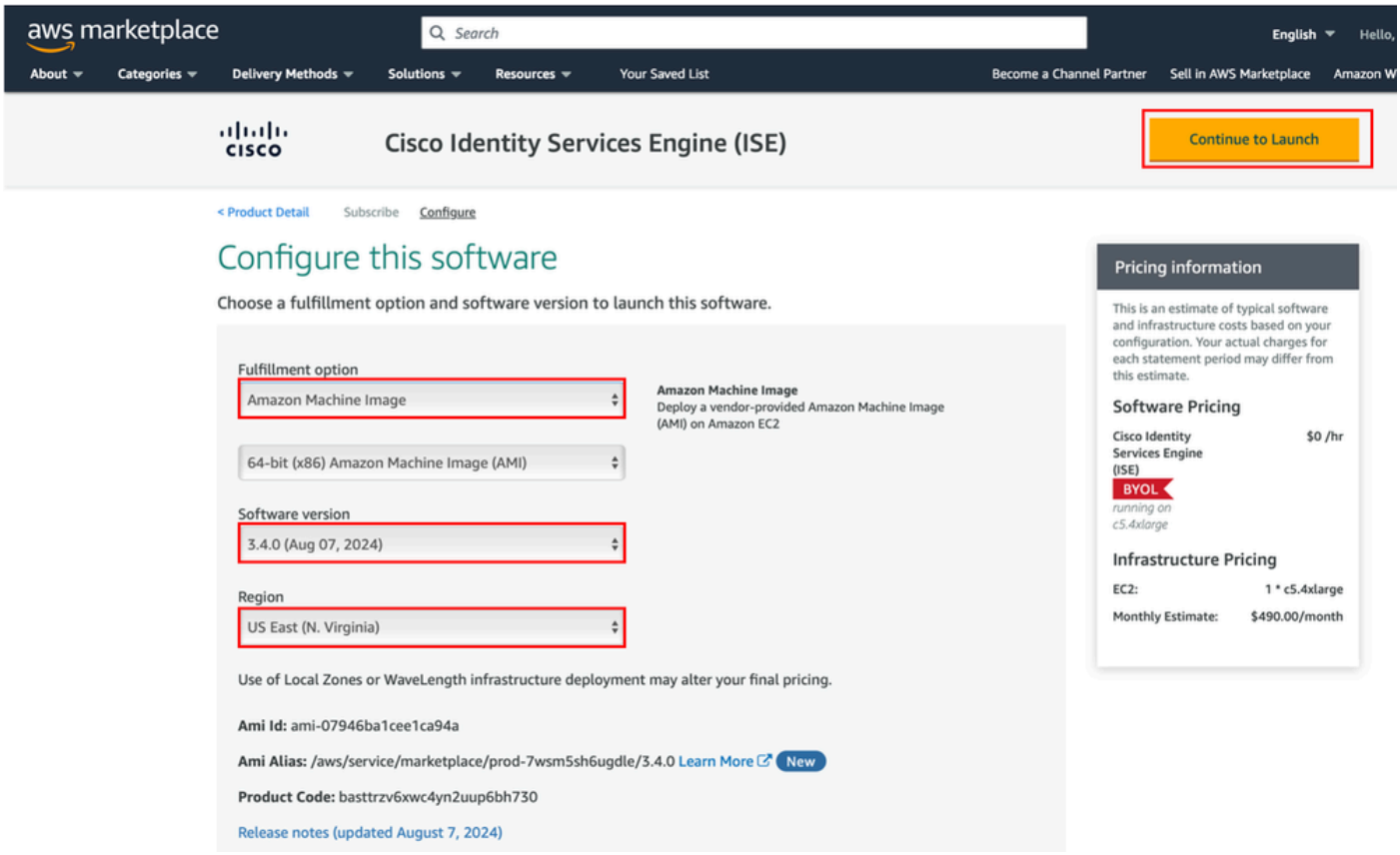
3. Fare clic su Visualizza opzioni di acquisto.



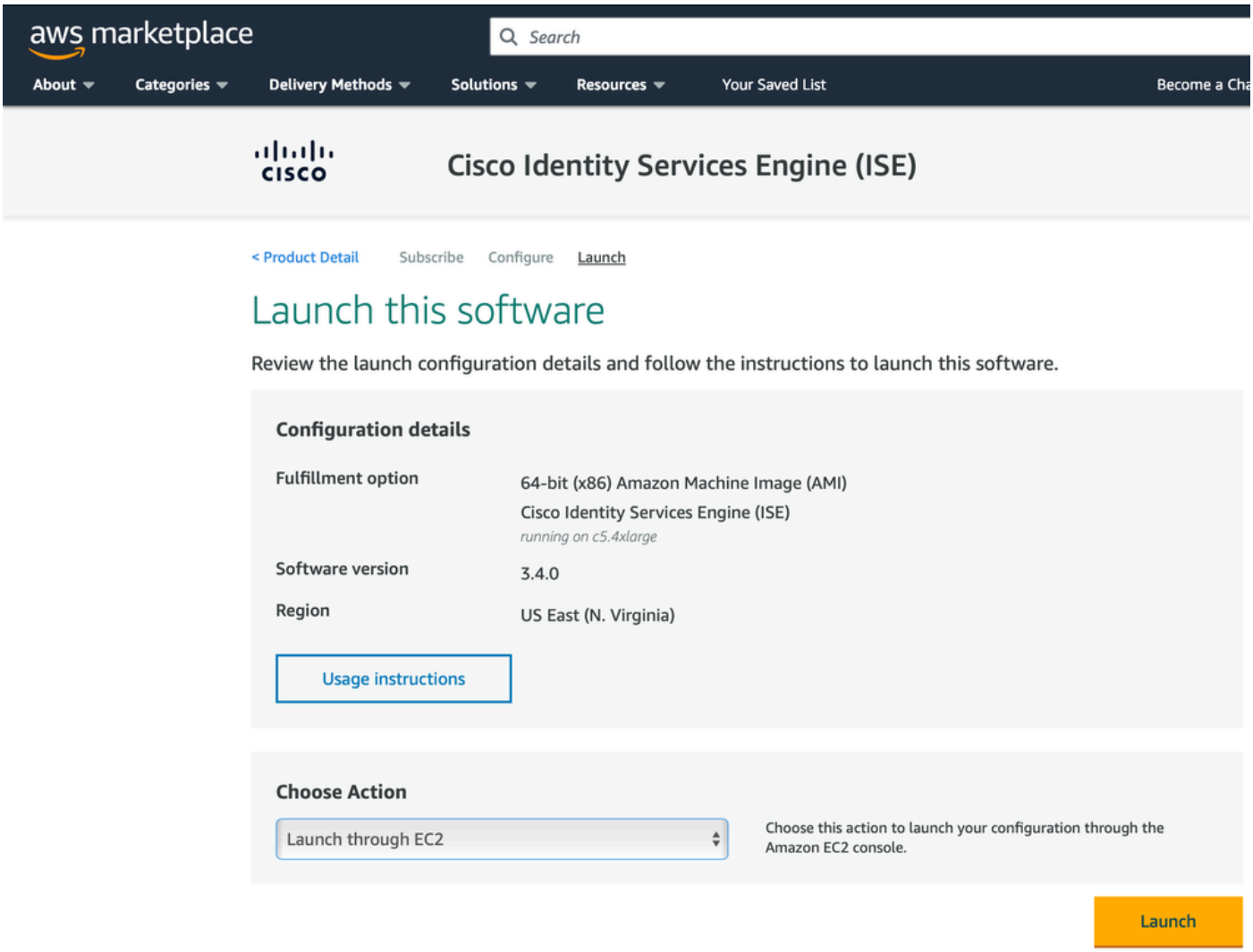
4. Fare clic su Avvia il software.



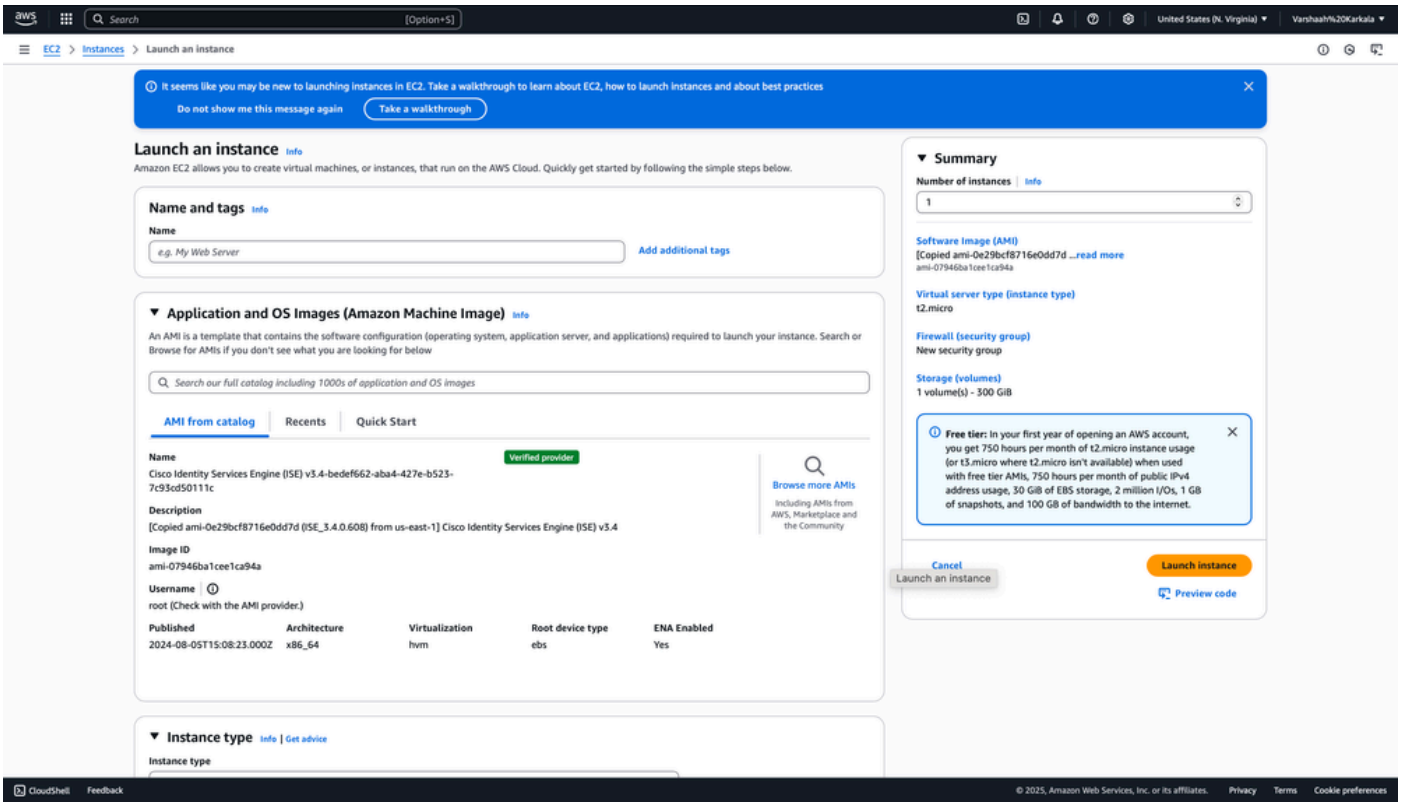
5. In Fulfillment Option, scegliere Amazon Machine Image. Scegliere la versione software e l'area desiderate. Fare clic su Continua per avviare.



6. In Scegli azione, scegliere Avvia tramite EC2. Fare clic su Avvia per continuare.



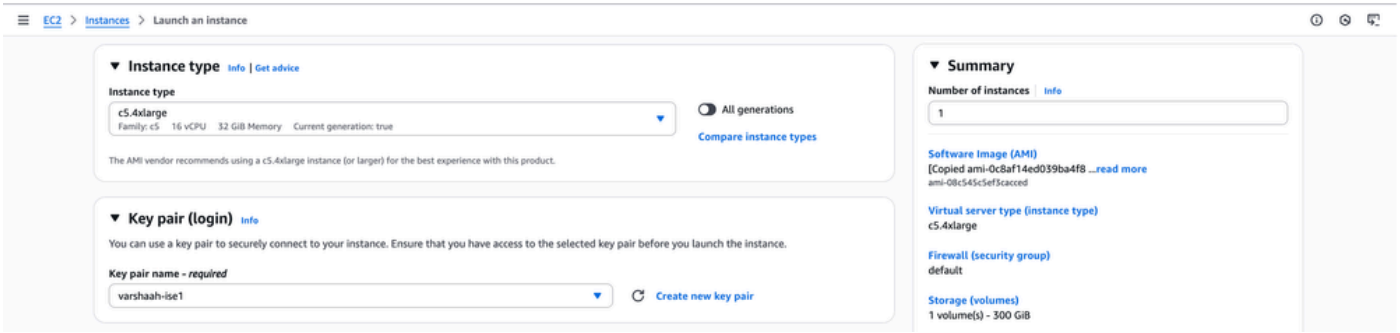
7. Viene visualizzata la pagina Avvia istanza EC2 per configurare le impostazioni dell'istanza.



8. Scorrere fino alla sezione Tipo di istanza e scegliere un tipo di istanza appropriato in base ai requisiti di distribuzione.

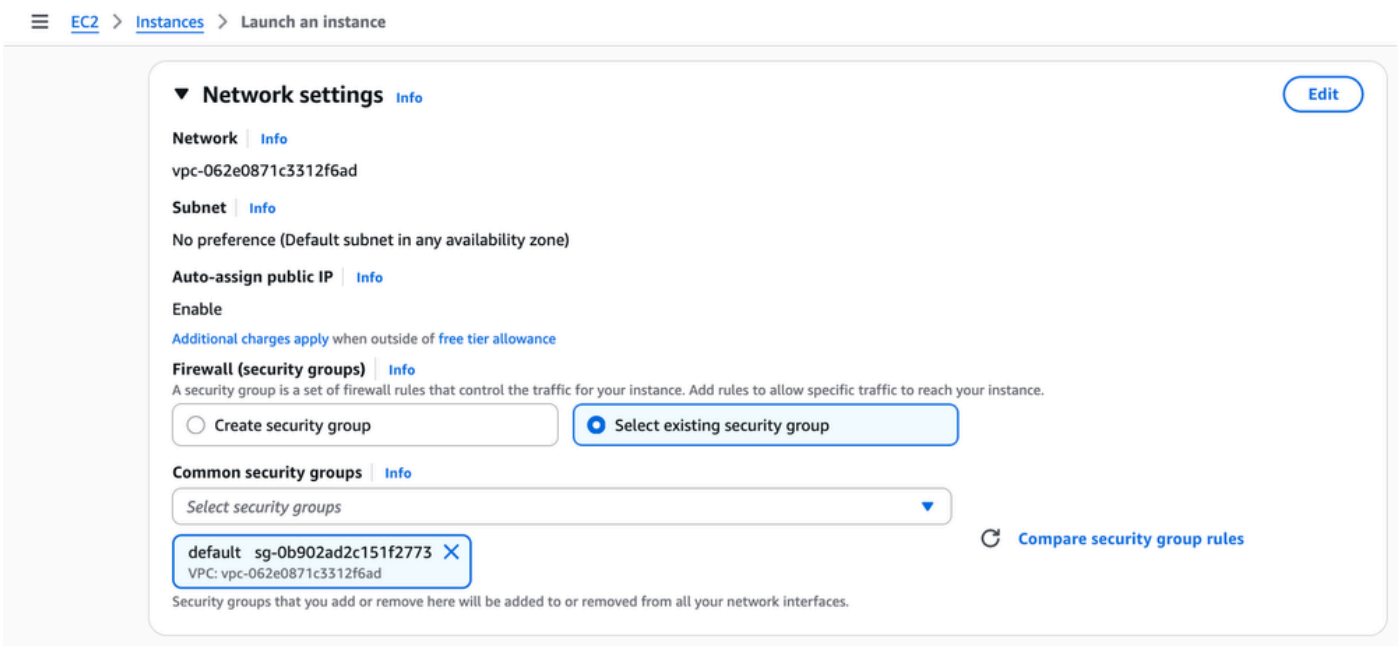
In Coppia di chiavi (login), selezionare la coppia di chiavi generata in precedenza o crearne una nuova (fare riferimento ai passaggi per la creazione della coppia di chiavi forniti in precedenza).

Impostate il numero di varianti a 1.



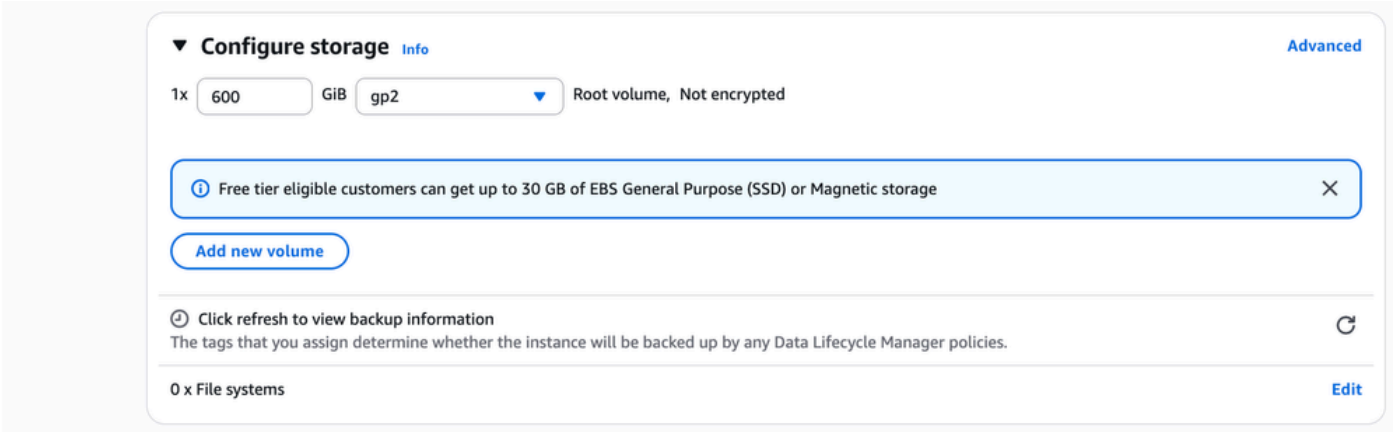
9. Nella sezione Impostazioni di rete:

- Configurare il VPC e la subnet in base alle esigenze.
- Per il gruppo di sicurezza, selezionare un gruppo esistente o creare un nuovo gruppo (come mostrato nell'esempio).



10. Nella sezione Configura archiviazione, configurare le dimensioni del volume desiderate.

Esempio: 600 GiB usando il tipo di volume gp2.



11. Nella sezione Dettagli avanzati configurare eventuali impostazioni aggiuntive necessarie per la distribuzione, ad esempio il profilo dell'istanza IAM, i dati utente o il comportamento di arresto.

▼ **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 ▼

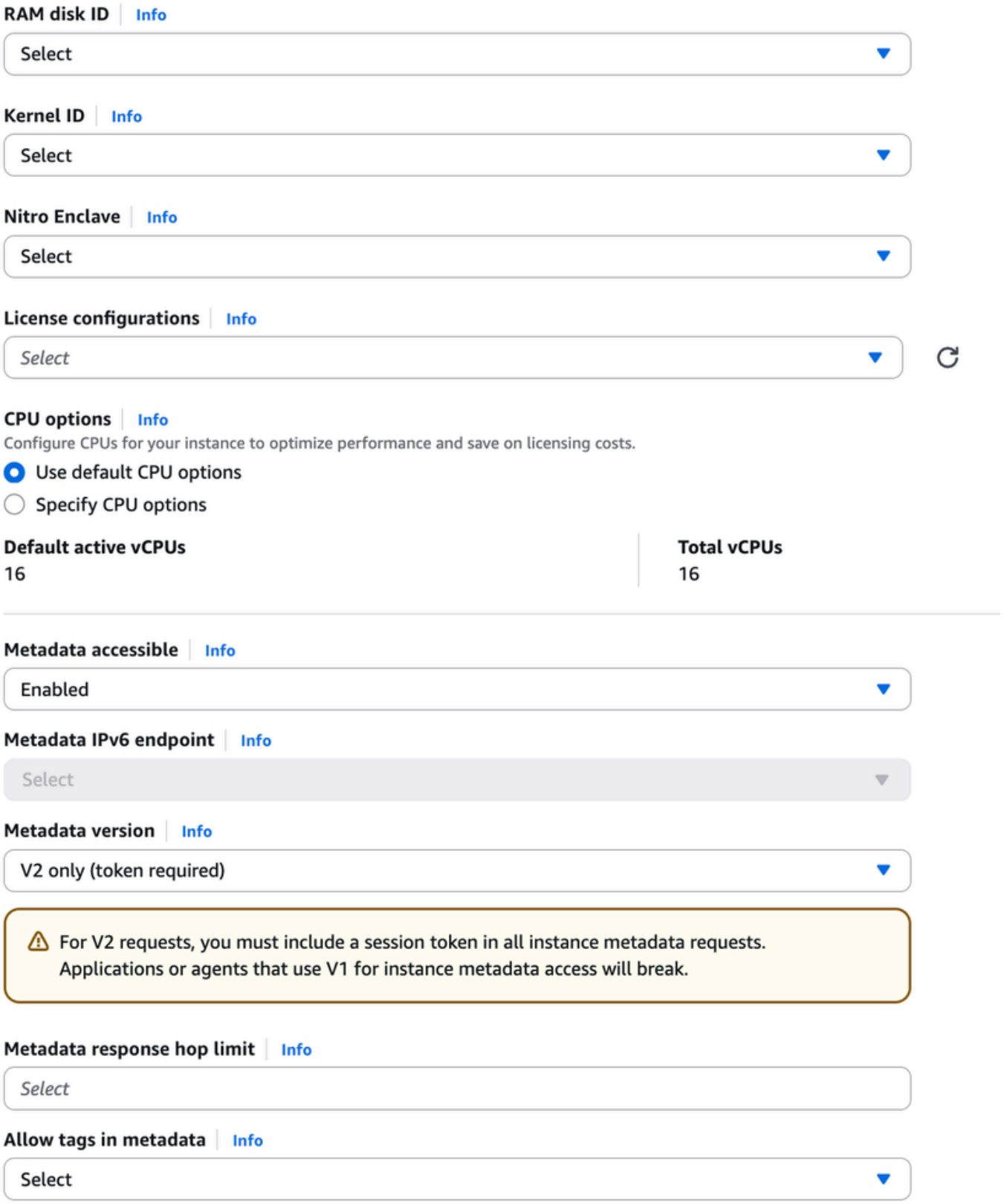
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12. Nella sezione Versione metadati:

- Per ISE versione 3.4 e successive, scegliere solo V2 (token richiesto) - questa è l'opzione consigliata.
- Per le versioni ISE precedenti alla 3.4, scegliere V1 e V2 (token facoltativo) per garantire la compatibilità.



13. Nel campo Dati utente, fornire i parametri di configurazione iniziale per l'istanza ISE, inclusi hostname, DNS, NTP server, timezone, ERS e admin credentials.

Esempio:
nomehost=varshaahise2

primarynameserver=x.x.x.x

dnsdomain=varshaah.local

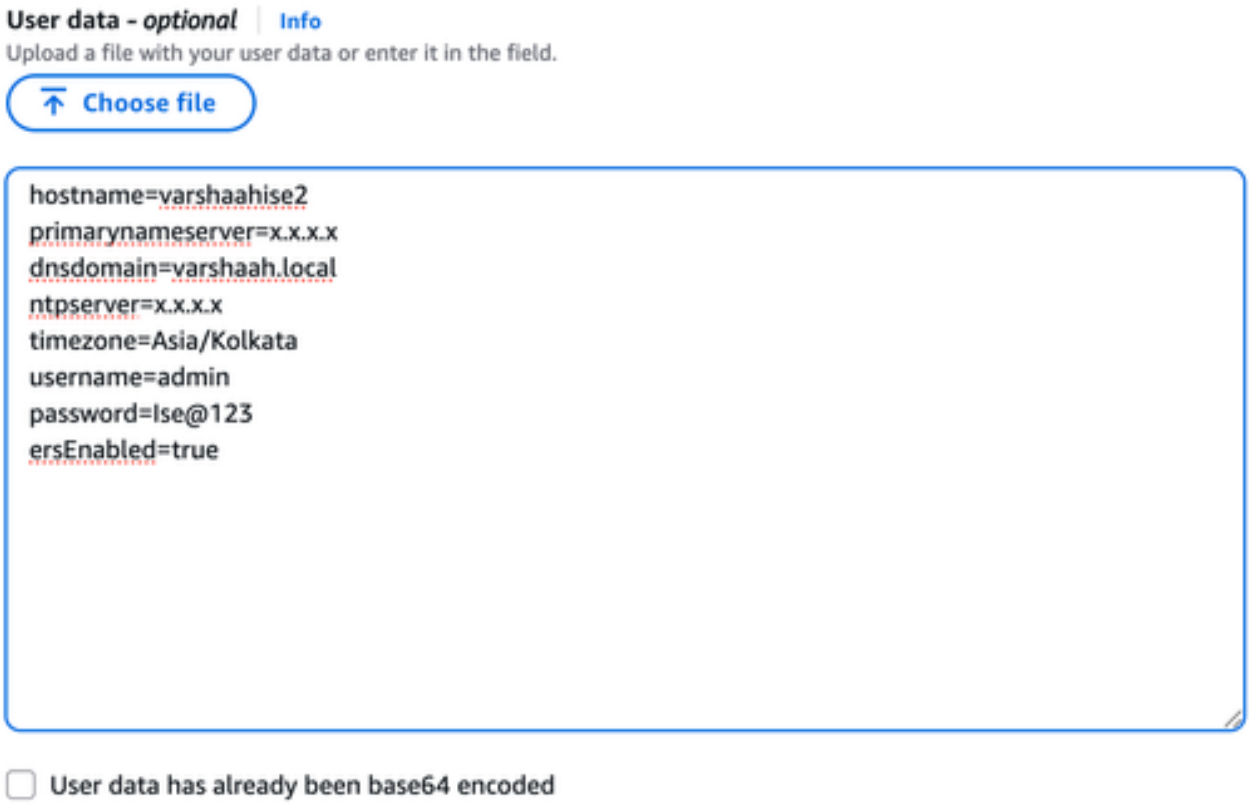
ntpserver=x.x.x

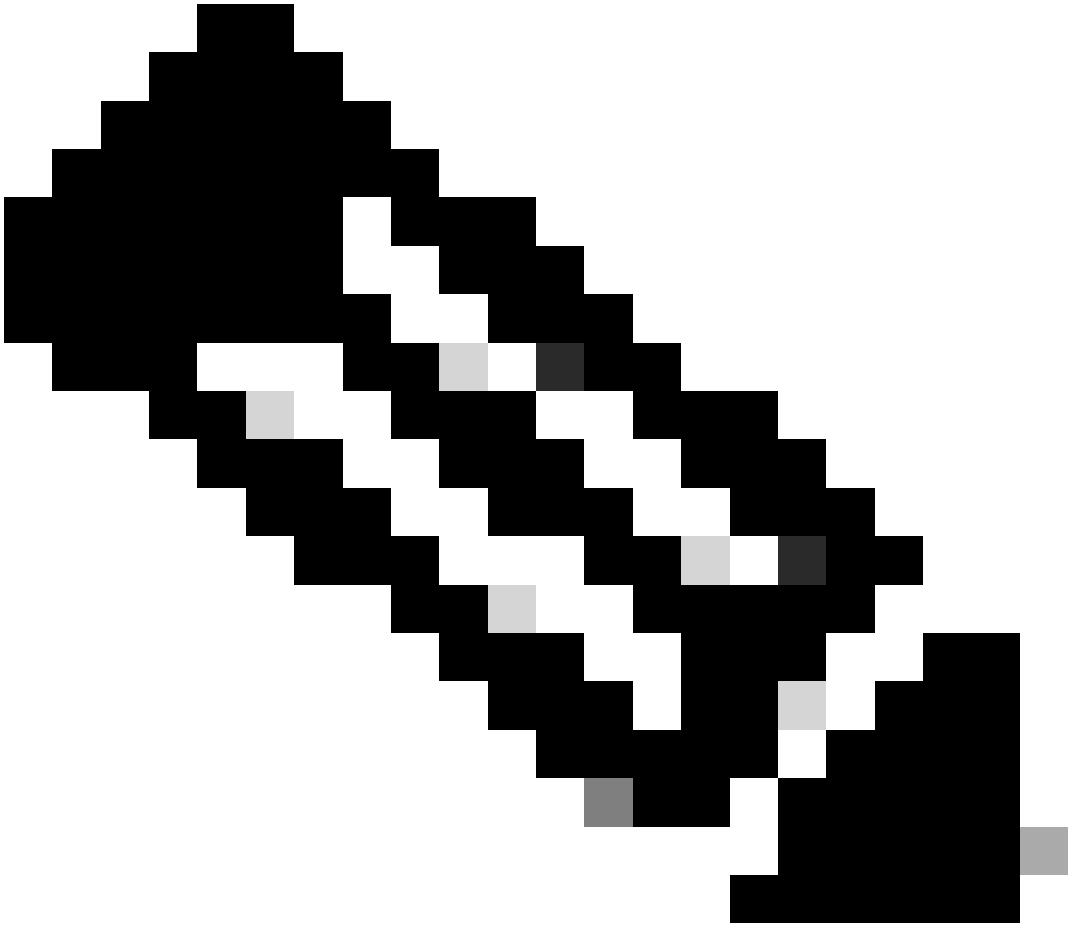
timezone=Asia/Calcutta

username=admin

password=Ise@123

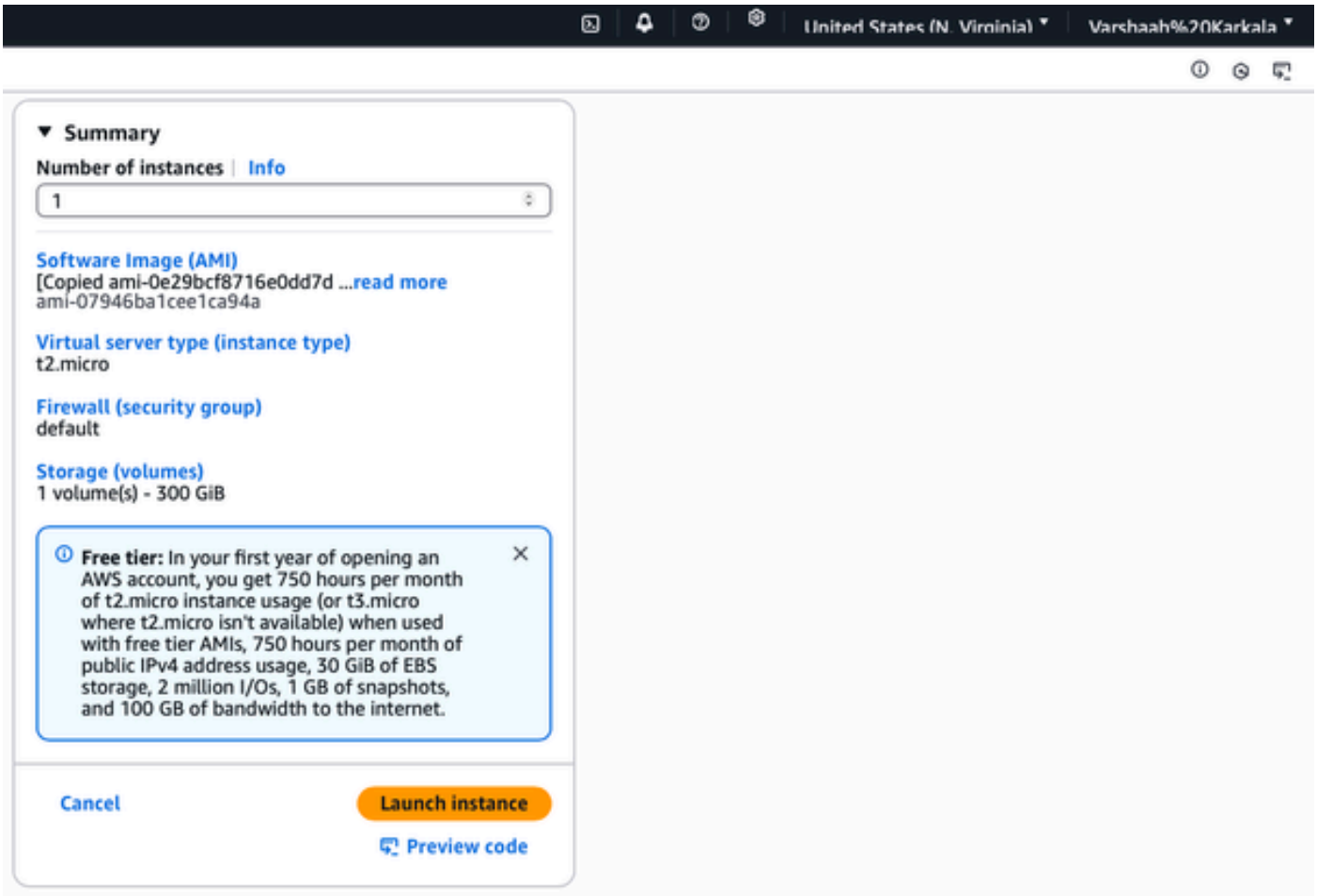
ersEnabled=true



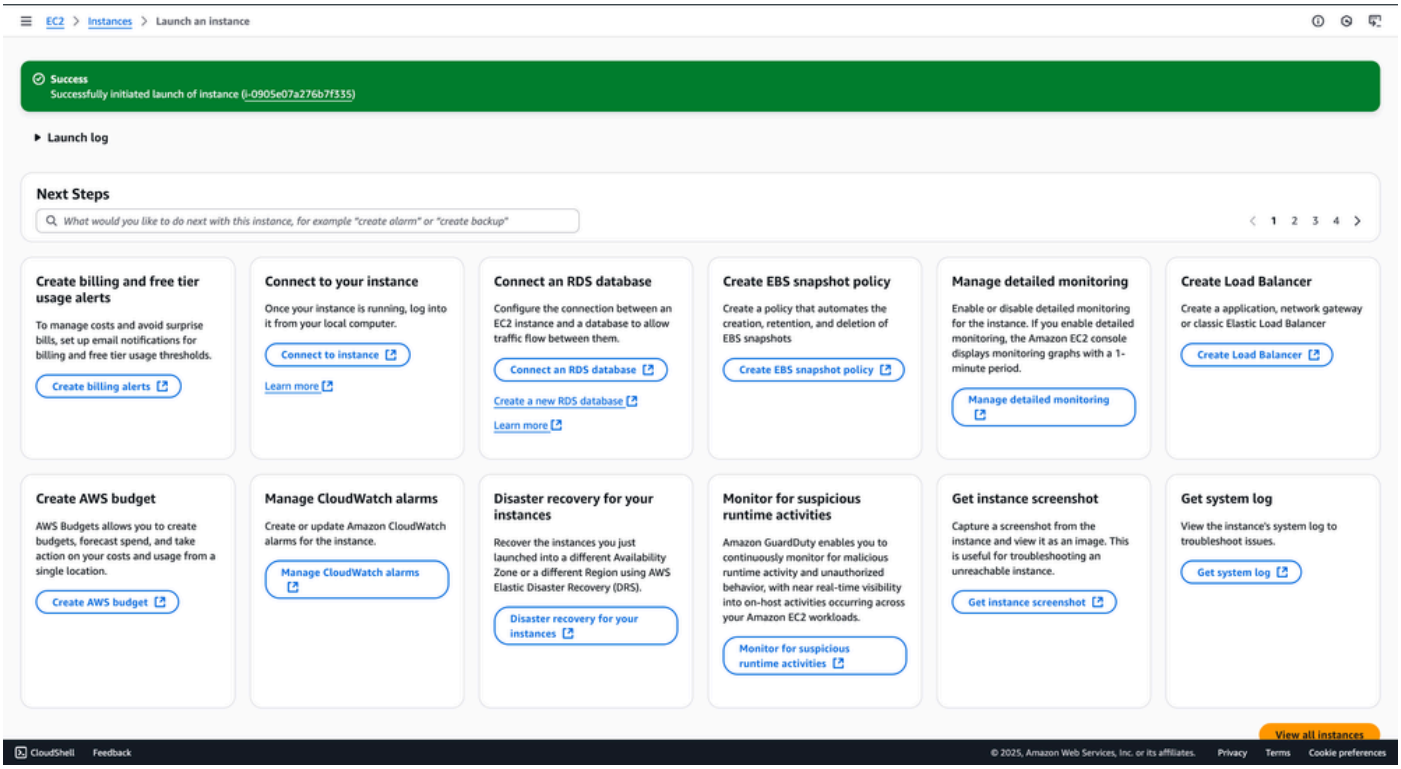


Nota: Verificare che la password sia conforme alle policy sulle password di Cisco ISE.

Dopo aver immesso i dati utente e completato la configurazione, fare clic su Avvia istanza.



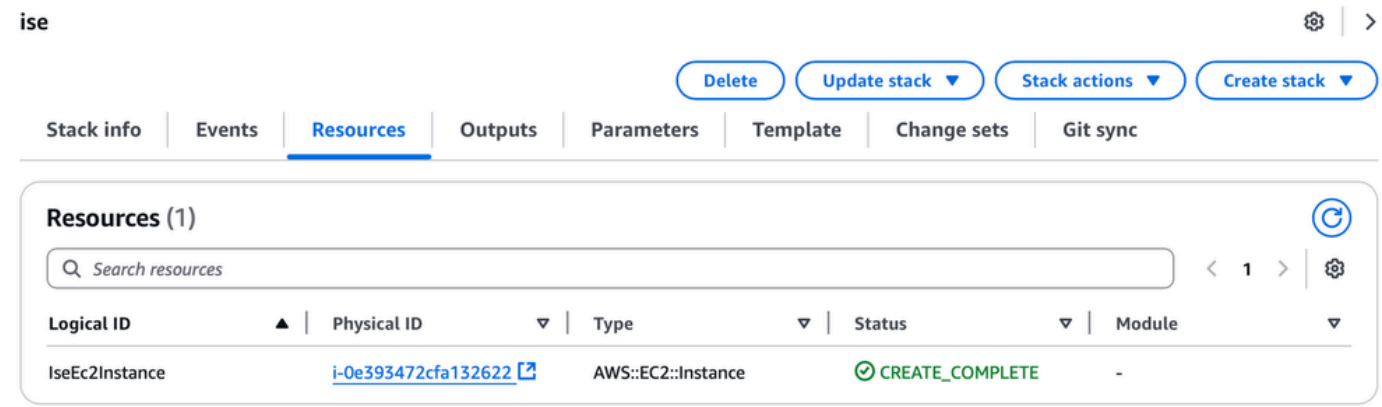
14. Dopo l'avvio dell'istanza, viene visualizzato un messaggio di conferma che indica: 'Avvio dell'istanza <nome_istanza>' avviato. Ciò indica che il processo di avvio è stato avviato correttamente.

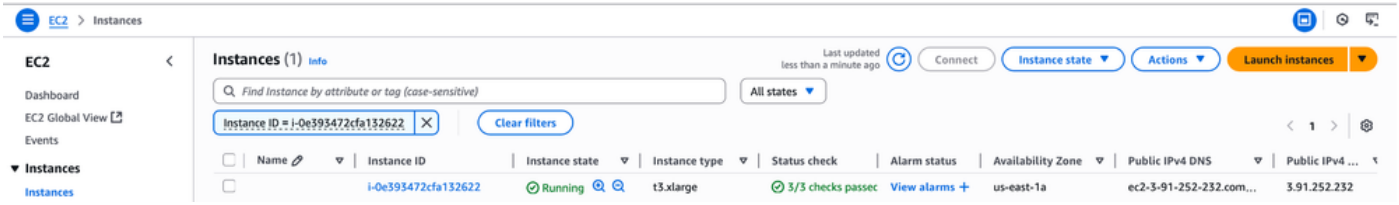


Verifica

Accesso all'istanza ISE creata con CFT

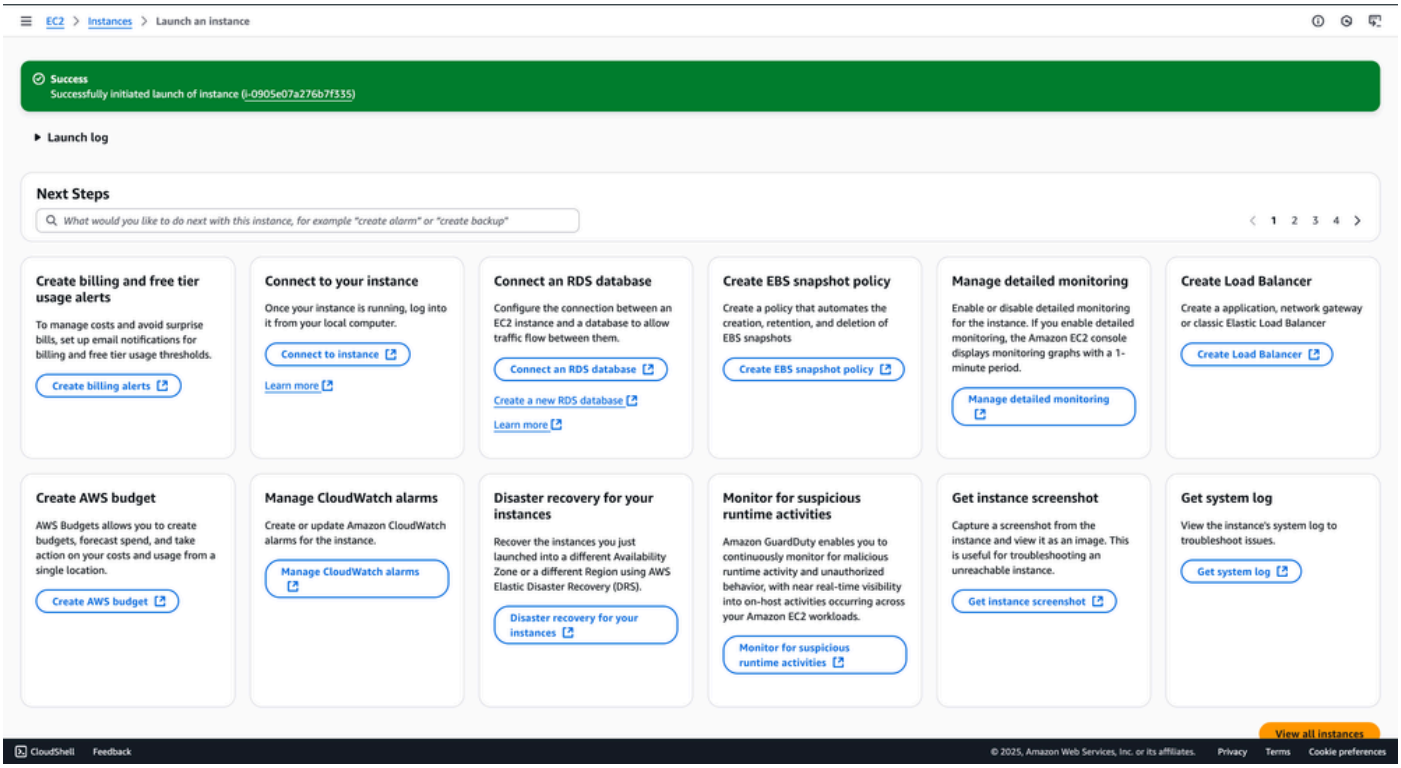
Passare alla scheda Resources nello stack CloudFormation e fare clic sull'ID fisico. Viene reindirizzato al dashboard EC2 in cui è possibile visualizzare l'istanza.

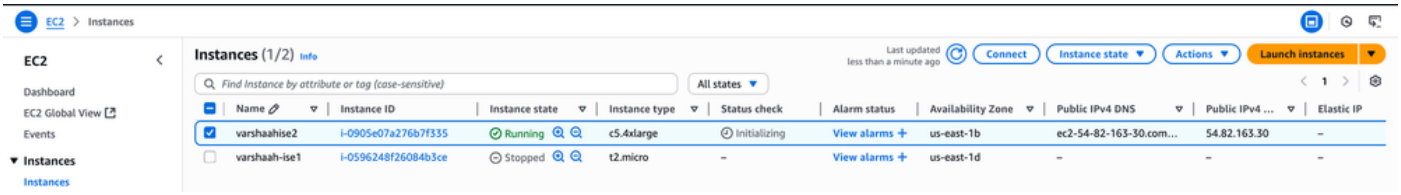




Accesso all'istanza ISE creata con AMI

Fare clic su Visualizza tutte le istanze per passare alla pagina Istanze EC2. In questa pagina verificare che il controllo dello stato venga visualizzato come controlli 3/3 superati, a indicare che l'istanza è attiva e integra.





Accesso all'interfaccia grafica di ISE

Il server ISE è stato implementato correttamente.

Per accedere all'interfaccia utente di ISE, è necessario usare l'indirizzo IP dell'istanza nel browser. Poiché l'indirizzo IP predefinito è privato, non è possibile accedervi direttamente da Internet.

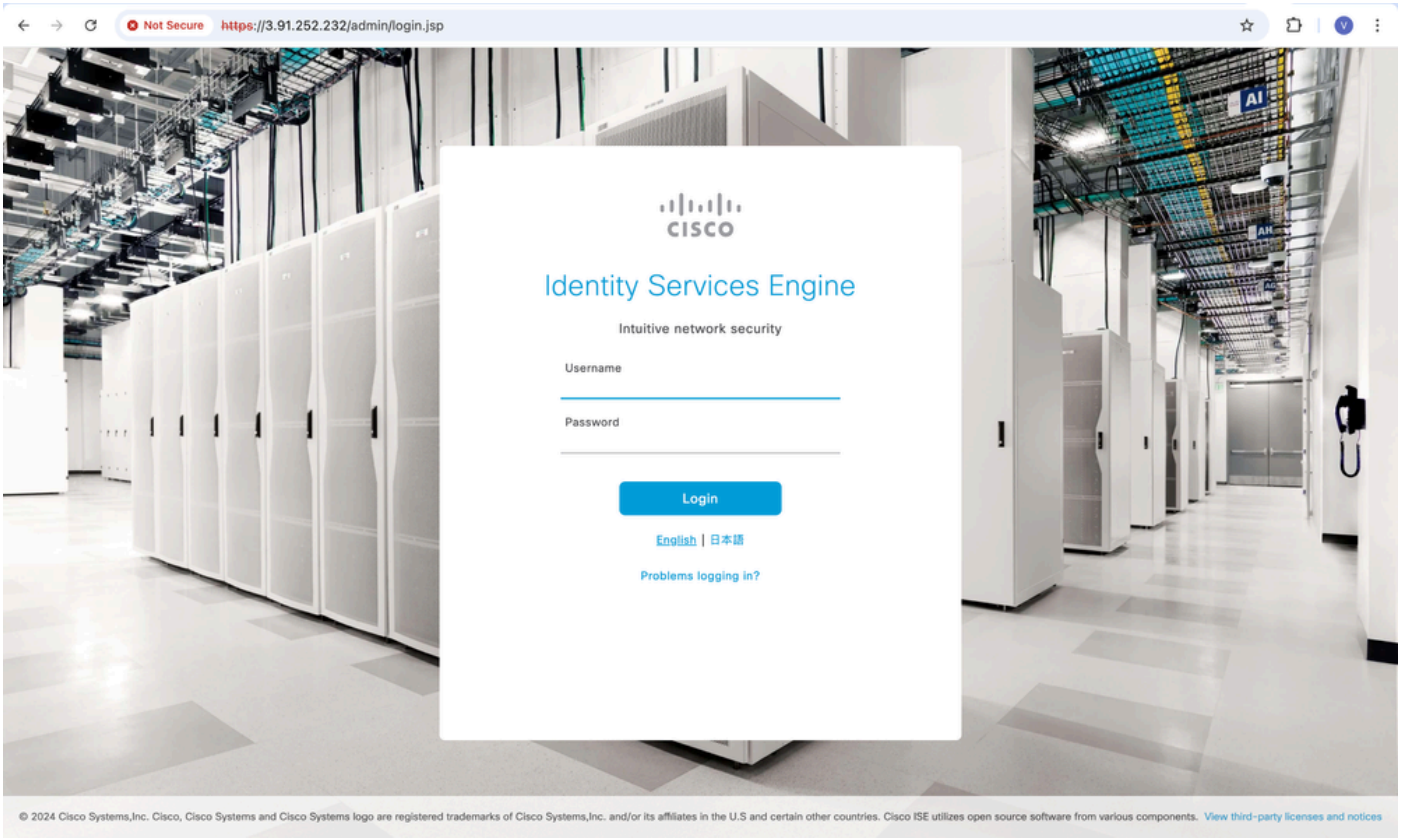
Verificare se all'istanza è associato un indirizzo IP pubblico:

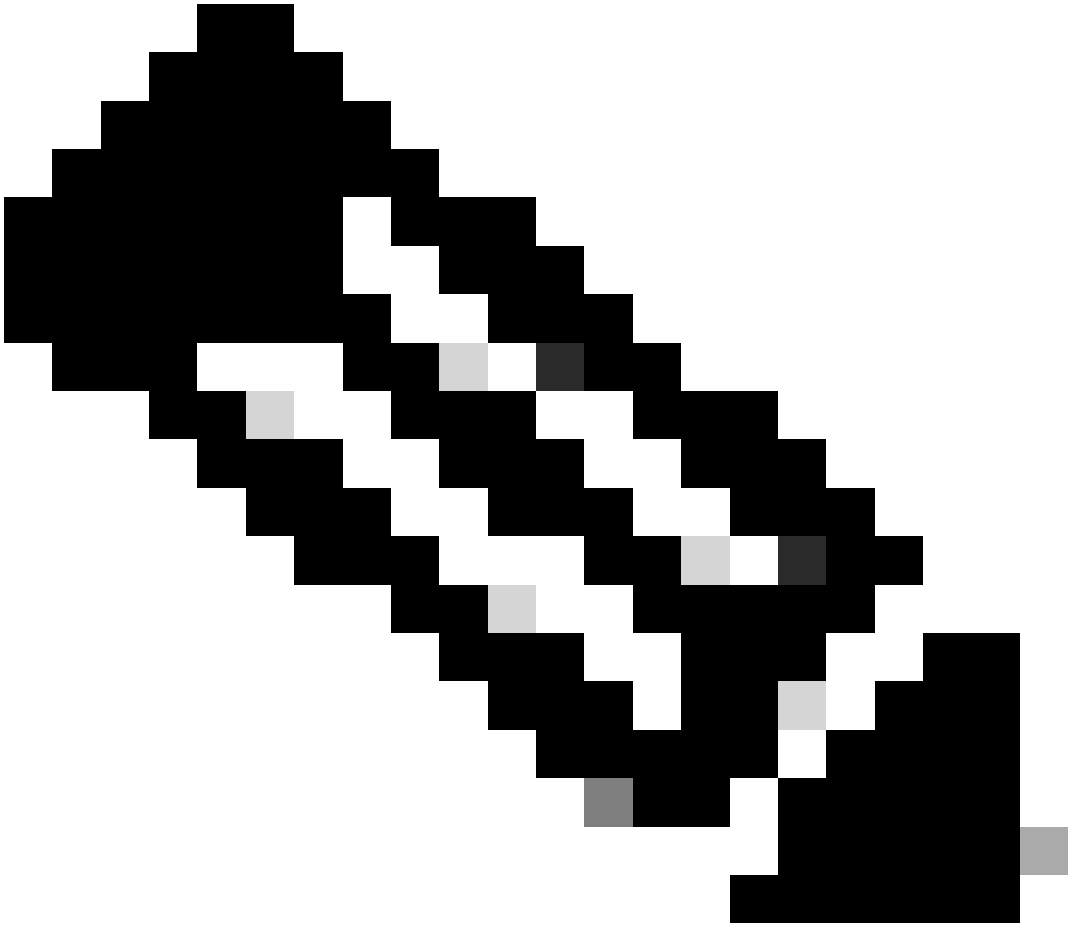
- Passare a EC2 > Istanze e selezionare la propria istanza.
- Cercare il campo Indirizzo IPv4 pubblico.

Qui è possibile vedere un indirizzo IP pubblico da utilizzare per accedere all'interfaccia grafica di ISE.

Aprire un browser supportato (ad esempio, Chrome o Firefox) e immettere l'indirizzo IP pubblico.

Viene visualizzata la pagina di accesso all'interfaccia grafica di ISE.





Nota: Quando l'accesso SSH è disponibile, in genere sono necessari altri 10-15 minuti prima che i servizi ISE passino completamente a uno stato di esecuzione.

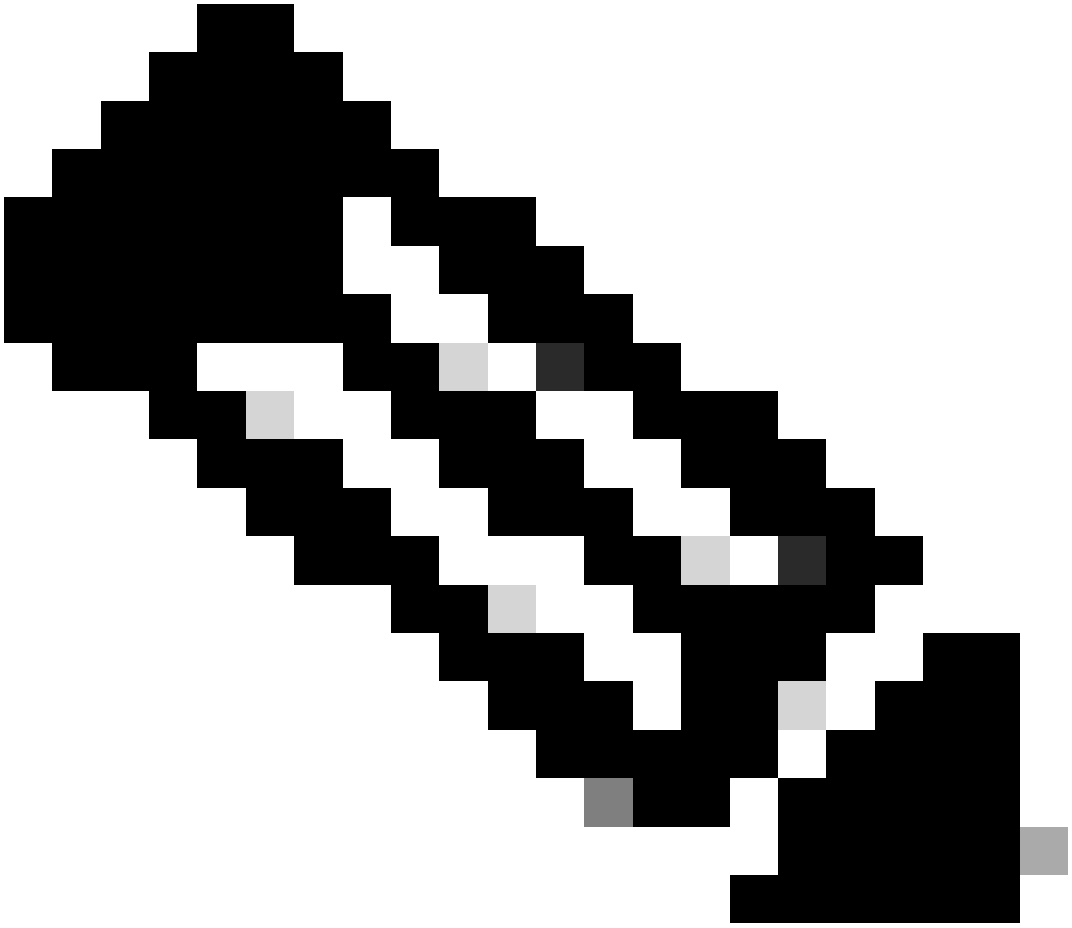
Accesso a CLI tramite SSH dal terminale

Nella console EC2, selezionare la propria istanza e fare clic su Connetti.

Nella scheda Client SSH, attenersi alla seguente procedura:

- Passare alla cartella contenente il file di chiave .pem scaricato.
- Eseguire i seguenti comandi:

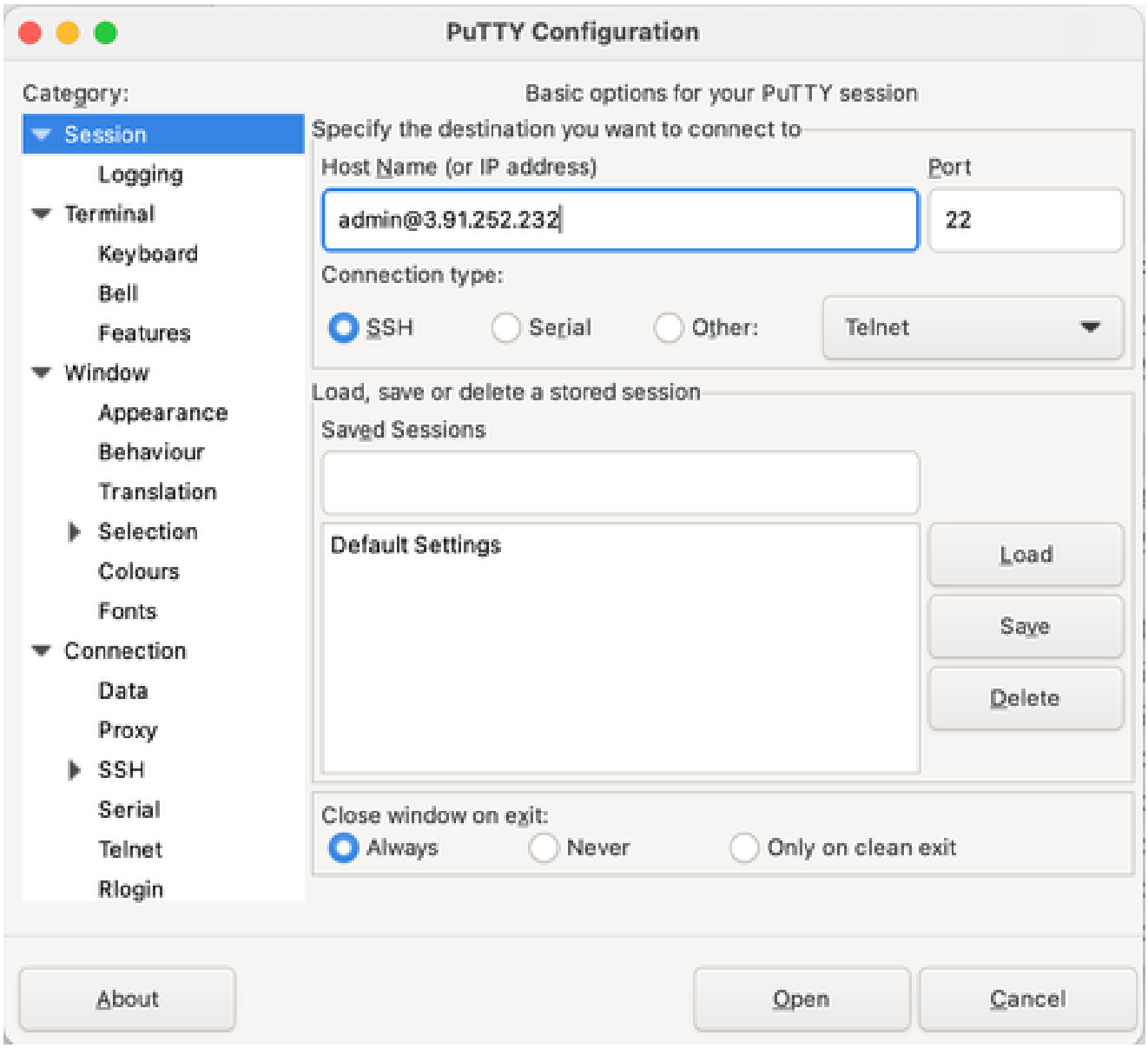
- cd <percorso-file-chiave>
- chmod 400 <nome-coppia-chiavi>.pem
- ssh -i "<nome-coppia-chiavi>.pem" admin@<indirizzo-ip-pubblico>



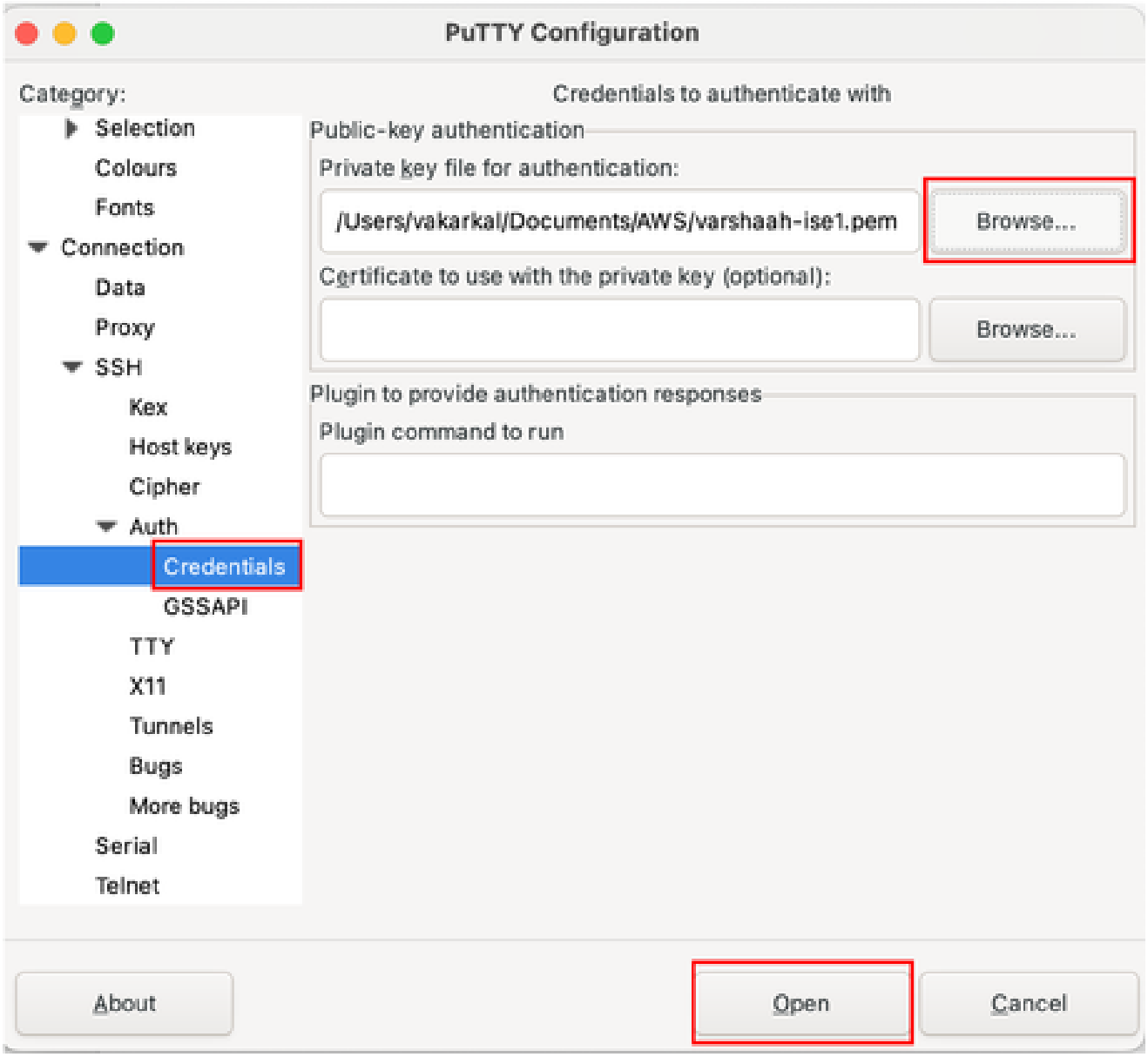
Nota: Usare admin come utente SSH, poiché Cisco ISE disabilita l'accesso root tramite SSH.

Accesso a CLI tramite SSH con PuTTy

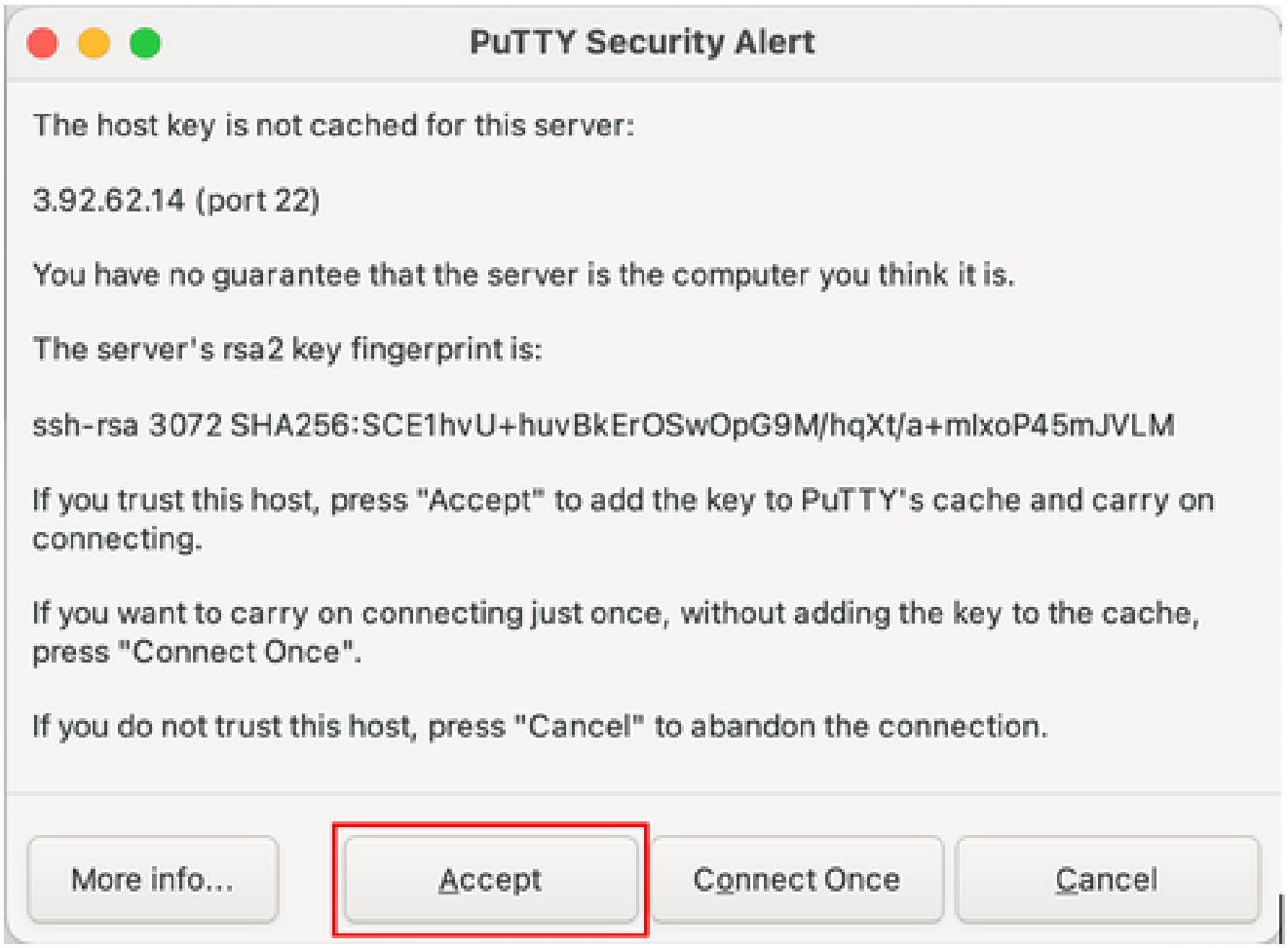
- Aprire PuTTY.
- Nel campo Host Name (Nome host), immettere: admin@<indirizzo-ip-pubblico>



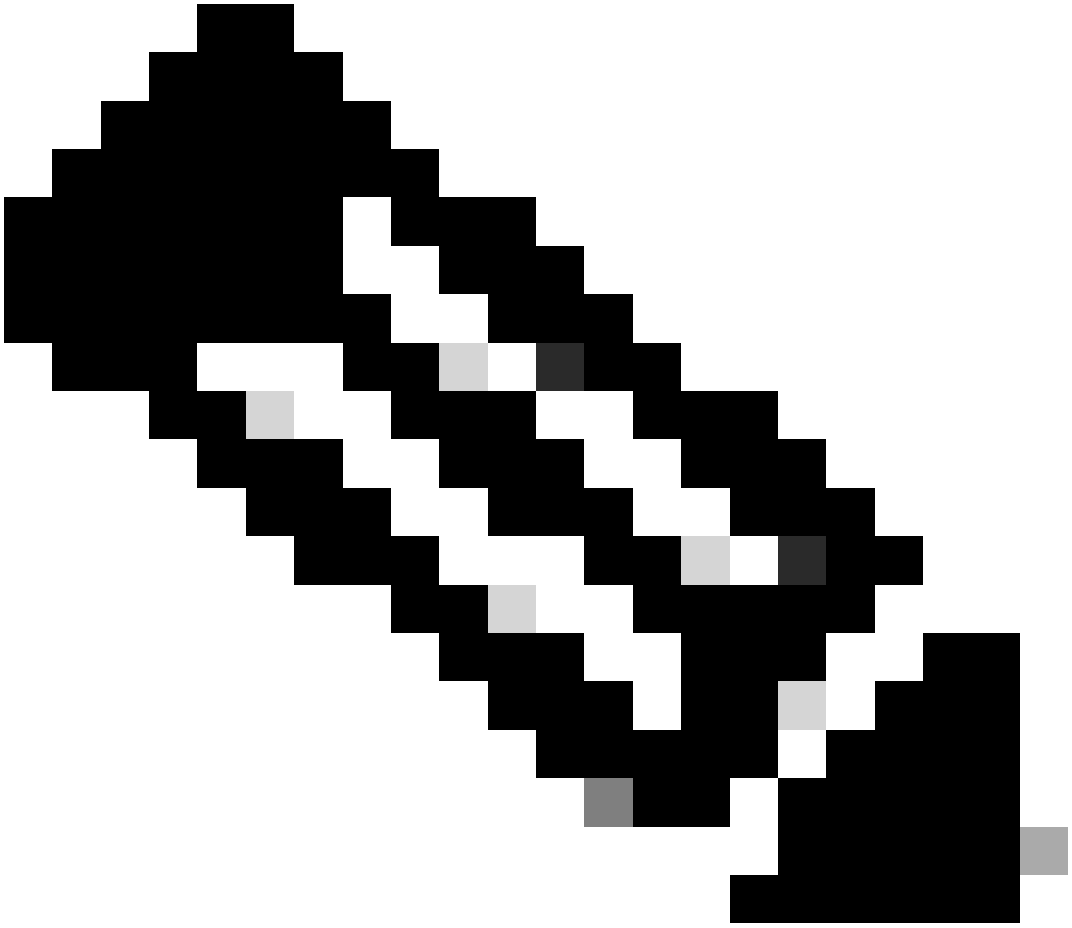
- Nel riquadro di sinistra, selezionare Connessione > SSH > Auth > Credentials.
- Fare clic su Sfoglia accanto a File della chiave privata per l'autenticazione, quindi selezionare il file della chiave privata SSH.
- Fare clic su Apri per avviare la sessione.



- Quando richiesto, fare clic su Accept (Accetto) per confermare la chiave SSH.



- La sessione PuTTy si connette ora alla CLI di ISE.

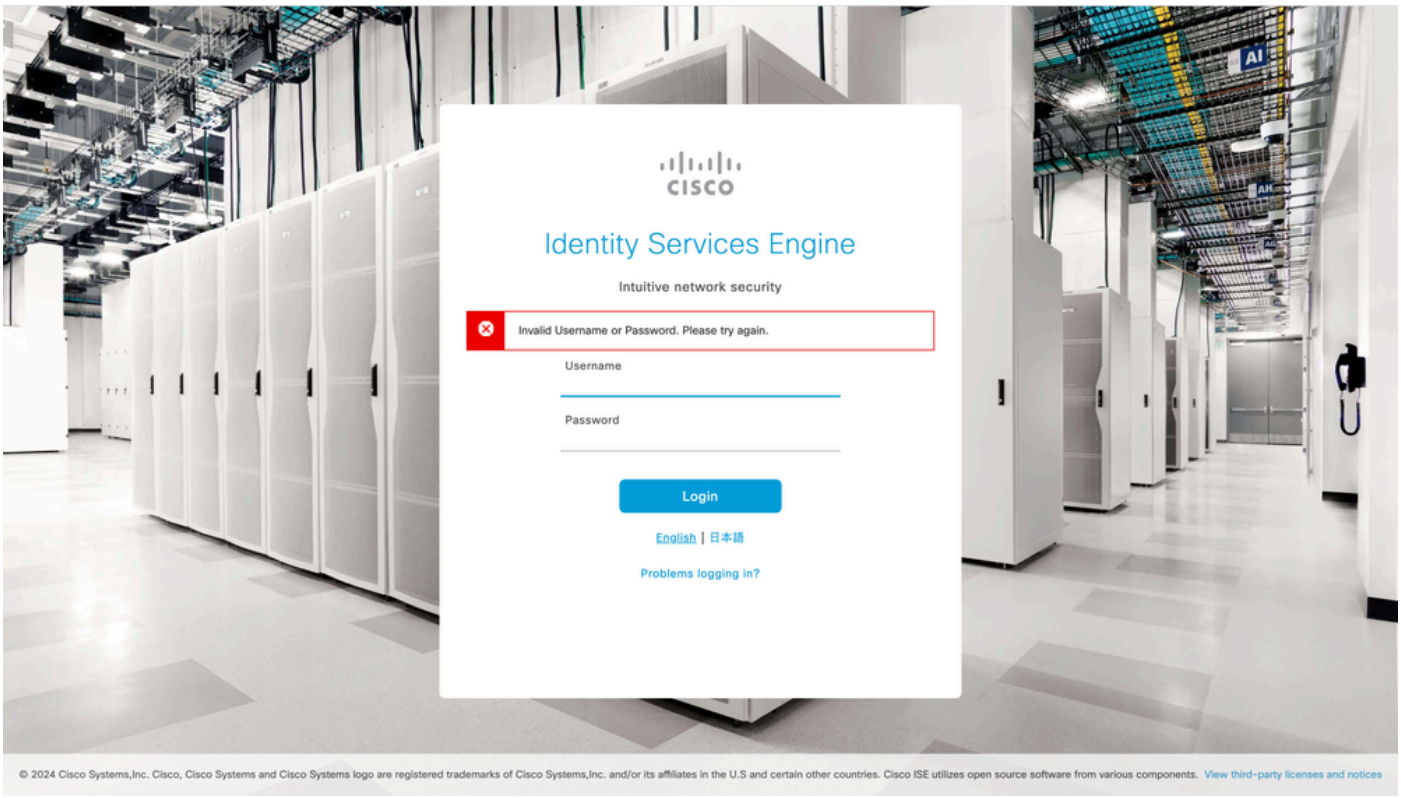


Nota: Per diventare accessibile via SSH, ISE potrebbe impiegare fino a 20 minuti. Durante questo periodo, i tentativi di connessione potrebbero non riuscire con l'errore: "Autorizzazione negata (chiave pubblica)."

Risoluzione dei problemi

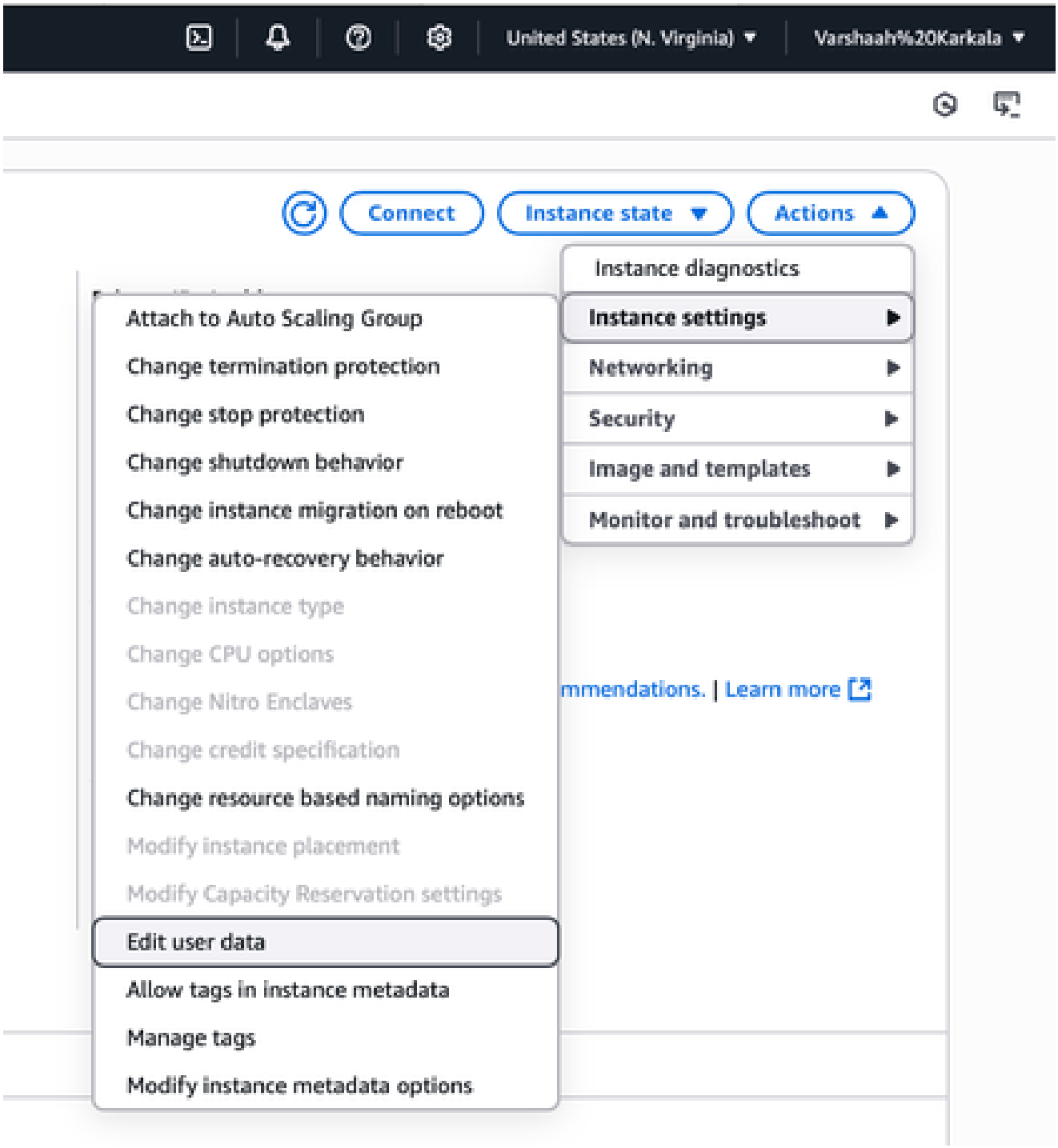
Nome utente o password non validi

I problemi di autenticazione sono spesso causati da un input utente non corretto durante la creazione dell'istanza. Ciò genera un messaggio di errore come "Nome utente o password non valida". Riprova." errore durante il tentativo di accesso alla GUI.

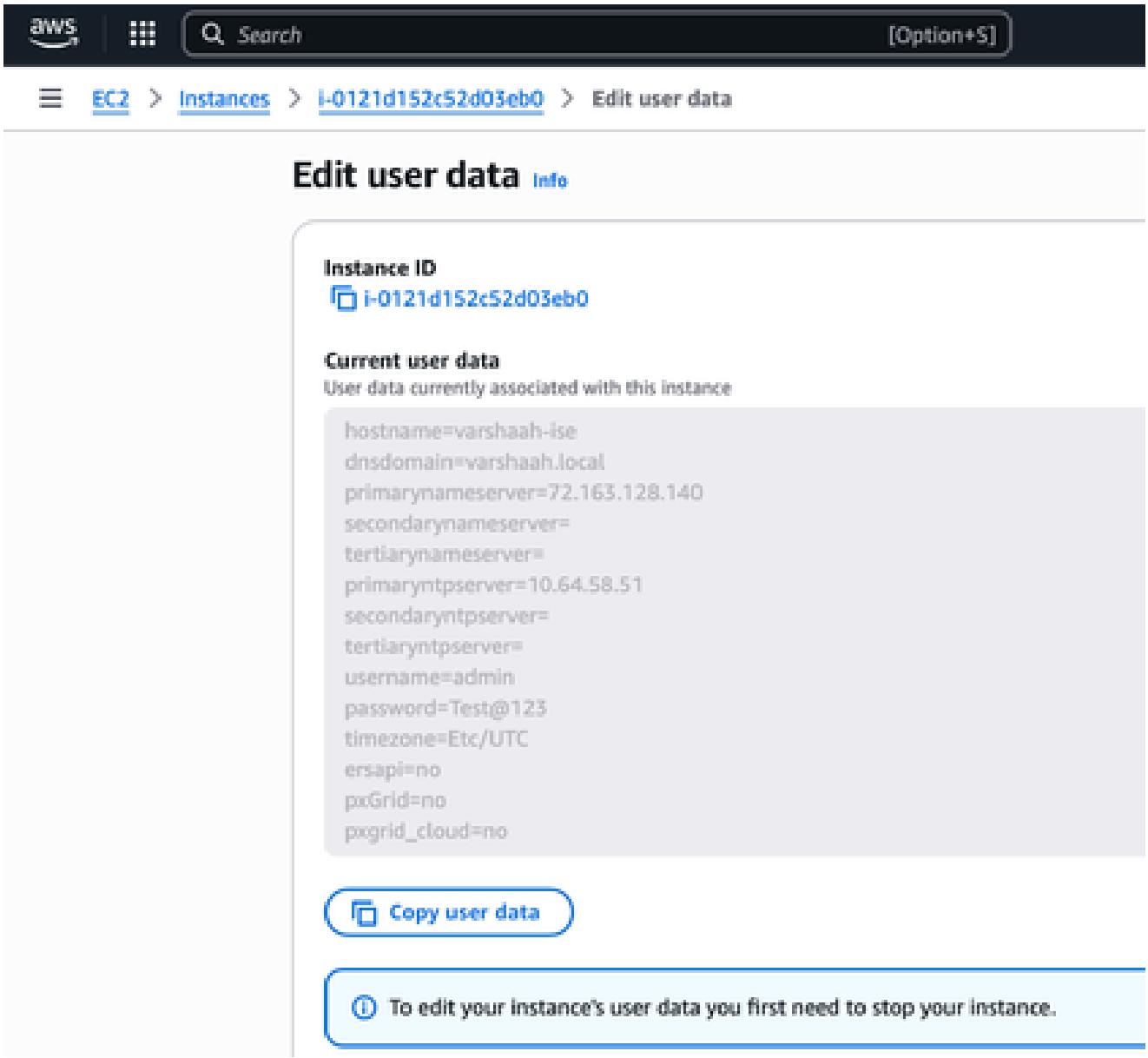


Soluzione

- Nella console AWS EC2, selezionare EC2 > Instances > your_instance_id.
- Fare clic su Azioni e scegliere Impostazioni istanza > Modifica dati utente.



- In questa sezione è possibile trovare il nome utente e la password specifici impostati durante l'avvio dell'istanza. Queste credenziali possono essere usate per accedere all'interfaccia grafica di ISE.



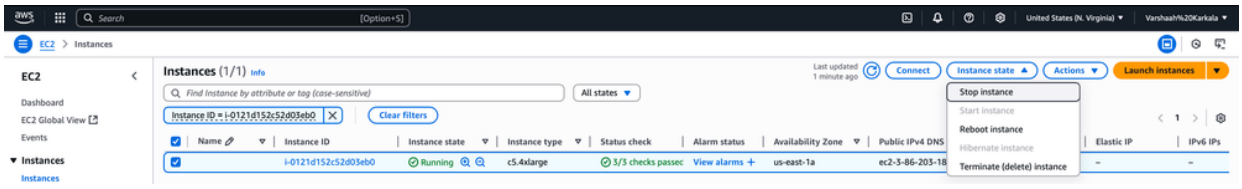
- Verificare il nome host e la password durante la configurazione del nome host e della password:
  - Nome host
    - Sono consentiti solo caratteri alfanumerici e trattini (-).
    - La lunghezza non deve superare i 19 caratteri.
  - Password
    - Deve essere conforme alle policy sulle password di Cisco ISE.
    - Per ulteriori informazioni, fare riferimento al manuale ISE Admin Guide: Policy per la password di ISE 3.4 - Guida per l'amministratore di Cisco

- Se la password configurata non soddisfa i criteri ISE per la password, i tentativi di accesso non riusciranno; anche con le credenziali corrette.

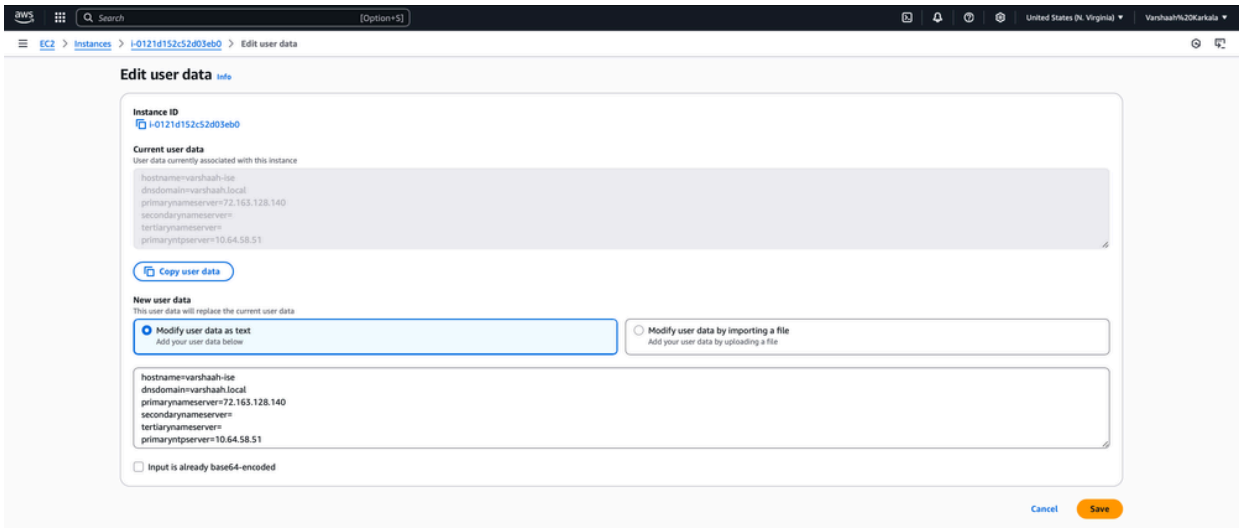
- Se si sospetta che la password non sia stata configurata correttamente, eseguire la procedura seguente per aggiornarla:

    1. Nella console EC2, selezionare EC2 > Instances > your_instance_id

    2. Selezionate Stato variante (Instance state) > Arresta variante (Stop instance).



    3. Una volta arrestata l'istanza, fare clic su Azioni > Impostazioni istanza > Modifica dati utente.



    4. Modificare lo script dei dati utente per aggiornare la password di conseguenza.

    5. Fare clic su Salva per salvare le modifiche. Fate clic su Stato variante (Instance state) > Avvia variante (Start instance) per riavviare l'istanza.

Difetti noti

ID bug	Descrizione
Cisco, ID bug 41693	ISE su AWS non riesce a recuperare i dati utente se la versione dei metadati è impostata solo su V2. Nelle versioni precedenti a ISE 3.4,

	è supportato solo il software IMDSv1.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).