Intégrer ISE à Prime Infrastructure pour une visibilité sur les terminaux

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configurations
    - Configuration du commutateur
    - Configuration de l'infrastructure Cisco Prime
    - Configuration des terminaux
- Vérifier
  - Vérifier ISE
  - Vérification du NAD
  - Vérification de l'infrastructure Prime
- Dépannage

Introduction

Ce document décrit comment intégrer ISE à Prime Infrastructure pour obtenir une visibilité sur les terminaux authentifiés.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE.
- Infrastructure Cisco Prime.
- Flux AAA filaire ou sans fil pour les terminaux authentifiés par rapport à ISE.
- Configuration SNMP sur les NAD (Network Access Devices) tels que les commutateurs et les WLC.

Composants utilisés

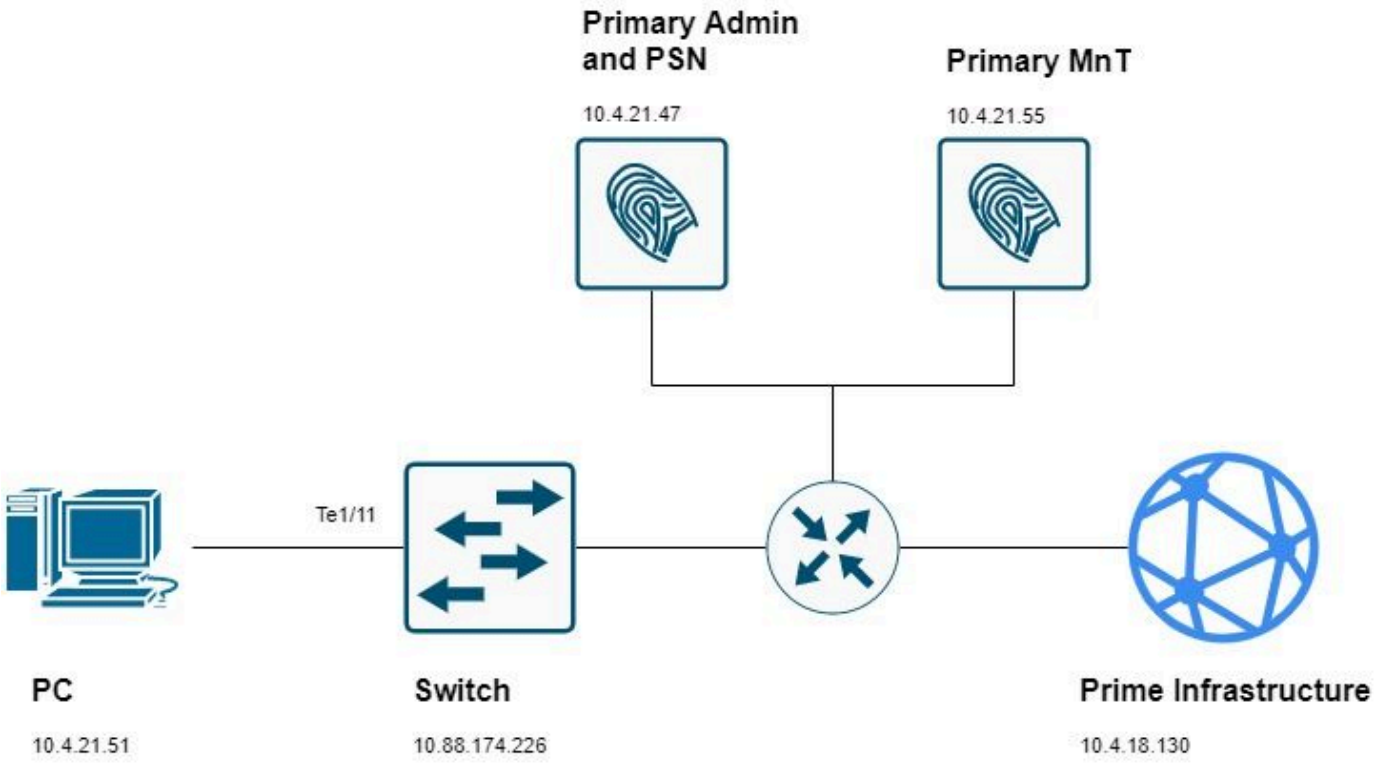
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- déploiement ISE 3.1.
- Infrastructure Cisco Prime 3.8.
- C6816-X-LE exécutant Cisco IOS® 15.5.
- Ordinateur Windows 10.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Configurations

Configuration du commutateur

1. Configurez le périphérique d'accès réseau (NAD) pour l'authentification AAA par rapport à ISE. Dans ce guide, vous utilisez cette configuration :

```
aaa new-model

radius server ise31
 address ipv4 10.4.21.47 auth-port 1812 acct-port 1813
 key Cisc0123

aaa server radius dynamic-author
```

```
 client 10.4.21.47 server-key Cisc0123

aaa group server radius ISE
 server name ise31

aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

dot1x system-auth-control
```

2. Configurez le suivi des périphériques dans le commutateur :

```
device-tracking policy DT1
 tracking enable

device-tracking tracking auto-source
```

3. Configurez le port de commutation pour l'authentification dot1x et associez-y la stratégie de suivi du périphérique :

```
interface TenGigabitEthernet1/11
 device-tracking attach-policy DT1
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 mab
 dot1x pae authenticator
```

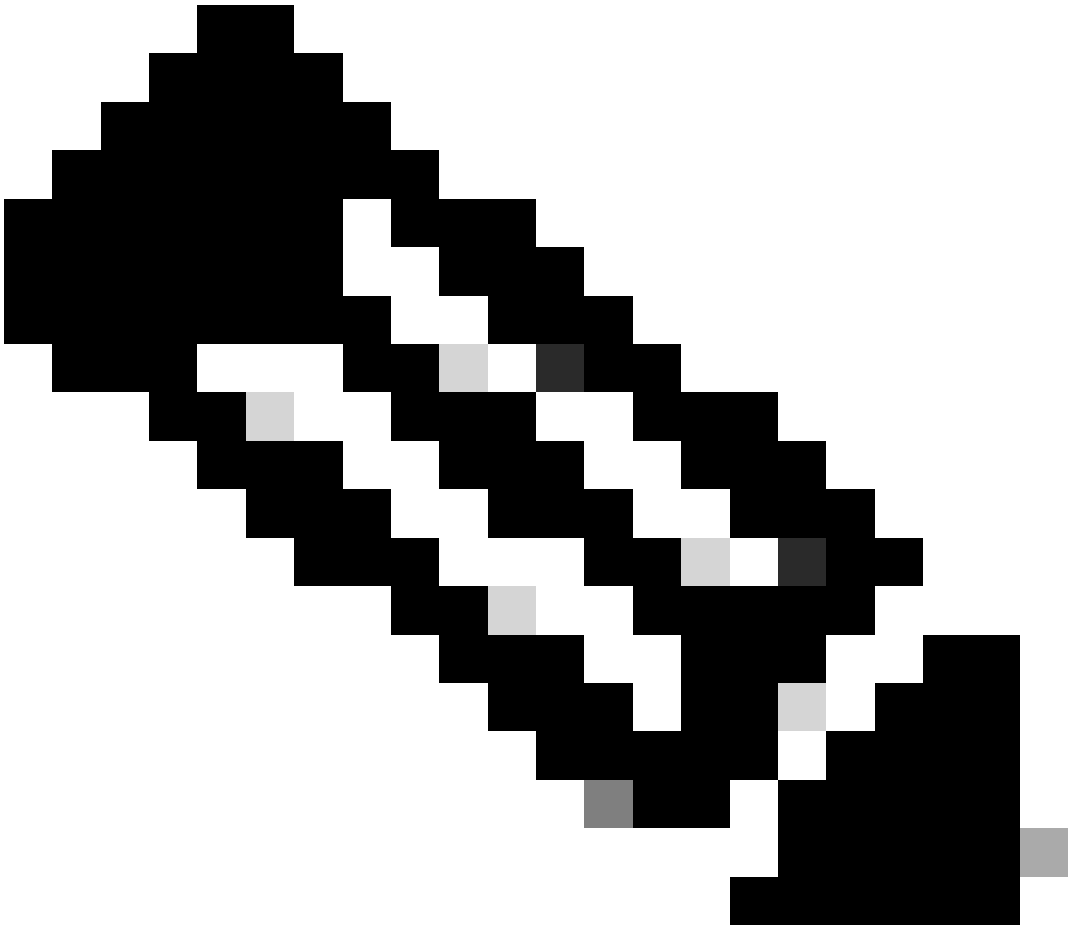
4. Configurez la communauté RW SNMP et les déroutements SNMP pour répondre aux exigences de votre réseau (vous pouvez éventuellement configurer la communauté RW) :

```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server enable traps trustsec authz-file-error
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps port-security
snmp-server enable traps event-manager
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.4.18.130 version 2c public udp-port 161
```

5. Configurez un accès Telnet ou SSH afin que Prime puisse gérer le périphérique :

```
username admin password 0 cisco!123
aaa authentication login default local

line vty 0 4
 transport input ssh
 login authentication default
```

6. (Facultatif) Pour les connexions SSH, une clé RSA est requise. Si le NAD n'en a pas, procédez comme suit pour le générer.

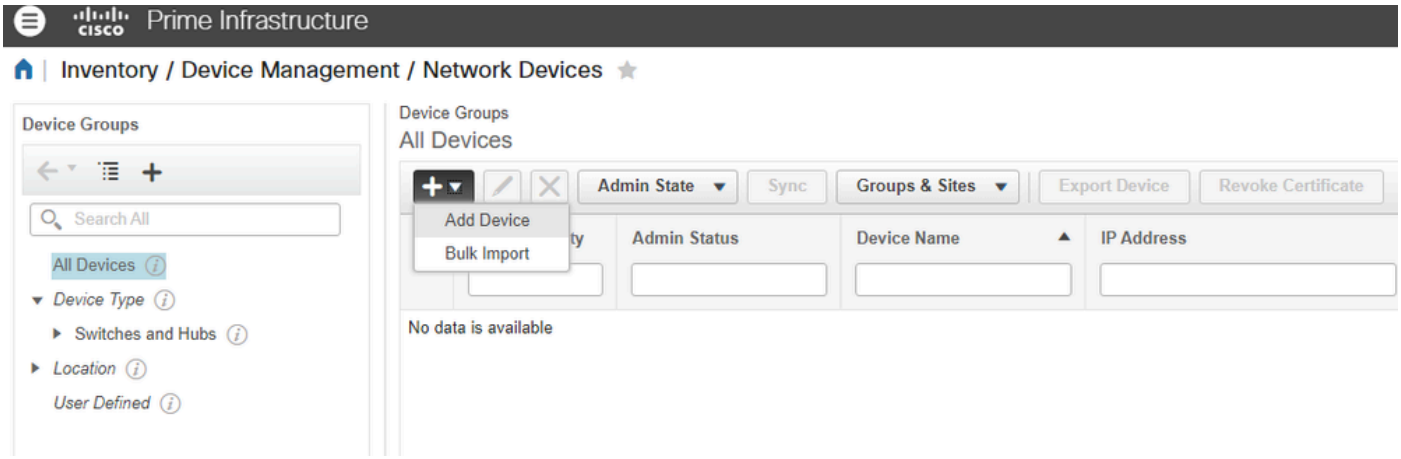


Remarque : Certains périphériques nécessitent un domaine configuré avant de générer le RSA. Vérifiez si un domaine est configuré sur votre périphérique afin de ne pas remplacer le domaine existant.

```
ip domain-name cisco.com
crypto key generate rsa
```

Configuration de l'infrastructure Cisco Prime

7. Ajoutez le périphérique réseau dans Inventaire > Gestion des périphériques > Périphériques réseau > Signe plus (+) > Ajouter un périphérique :



Les champs obligatoires pour obtenir l'inventaire sont les suivants :

Pour les périphériques filaires :

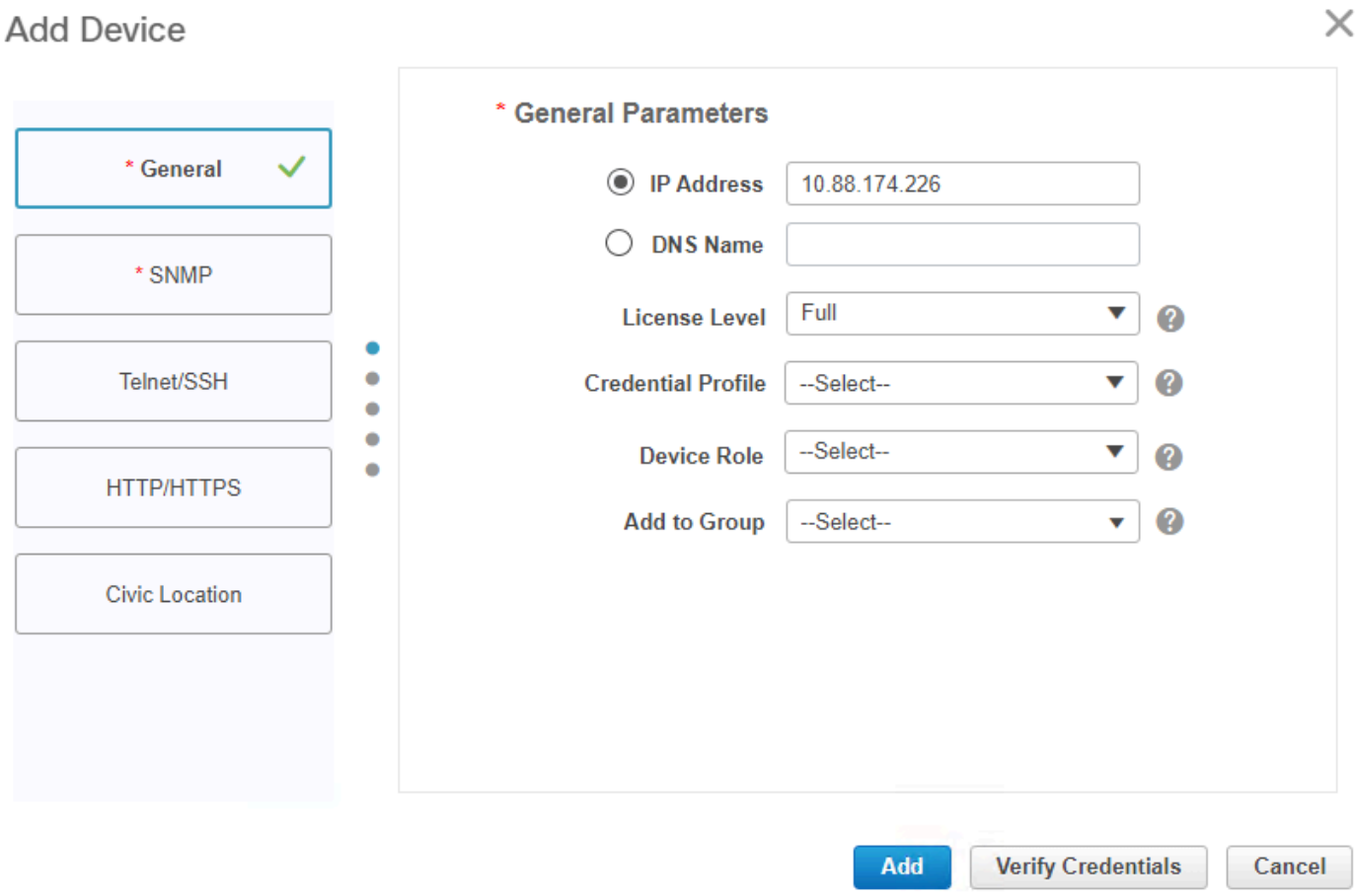
- Généralités: IP ou DNS.
- SNMP : La communauté RO est requise - assurez-vous de la configurer également dans le commutateur/WLC.
- Telnet/SSH : Informations d'identification du mode d'exécution et du mode actif.

Pour WLC :

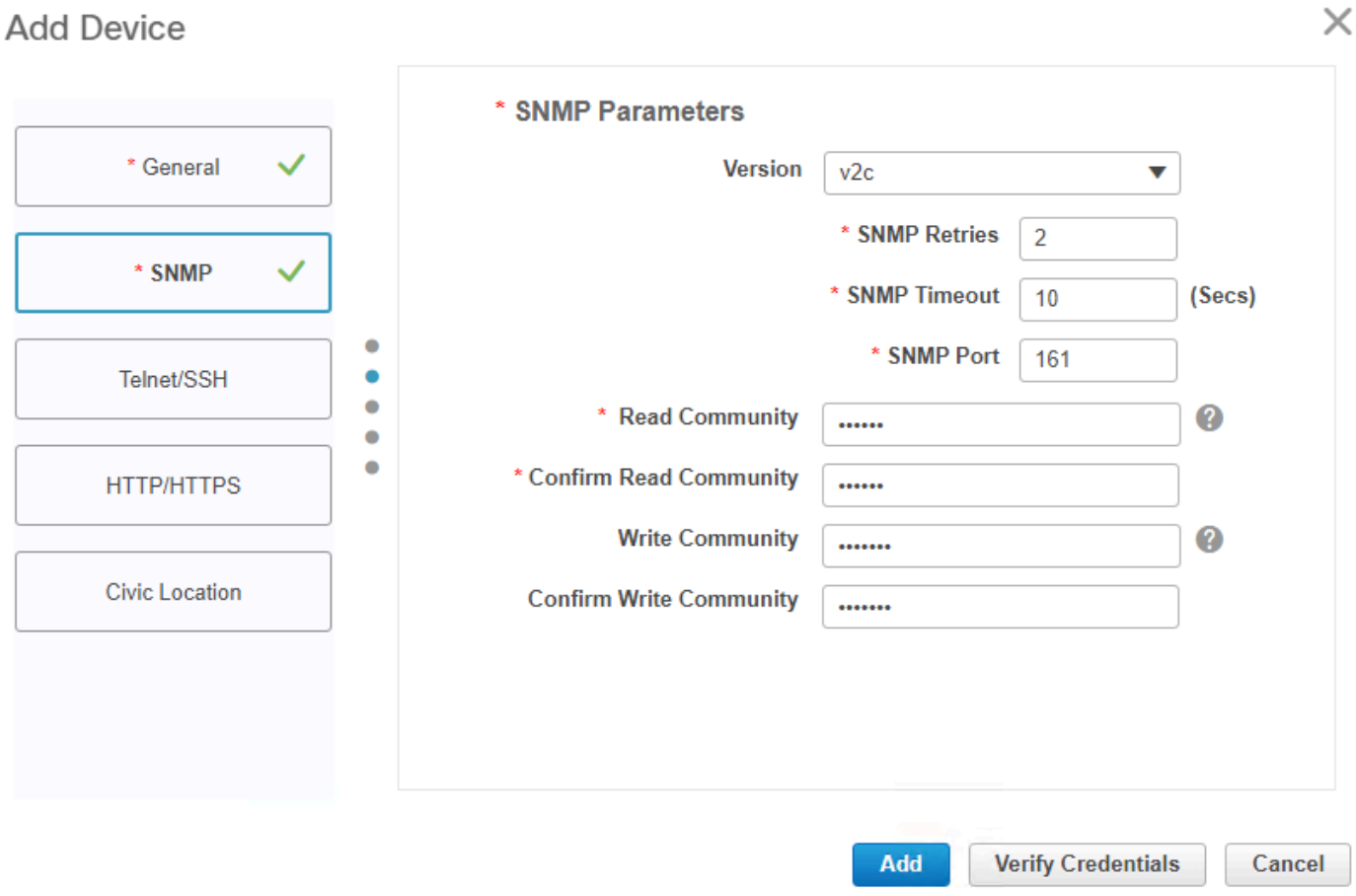
- Généralités: IP ou DNS.
- SNMP : La communauté RO est requise - assurez-vous de la configurer également dans le commutateur/WLC.

Dans ce guide, vous utilisez un commutateur Cisco :

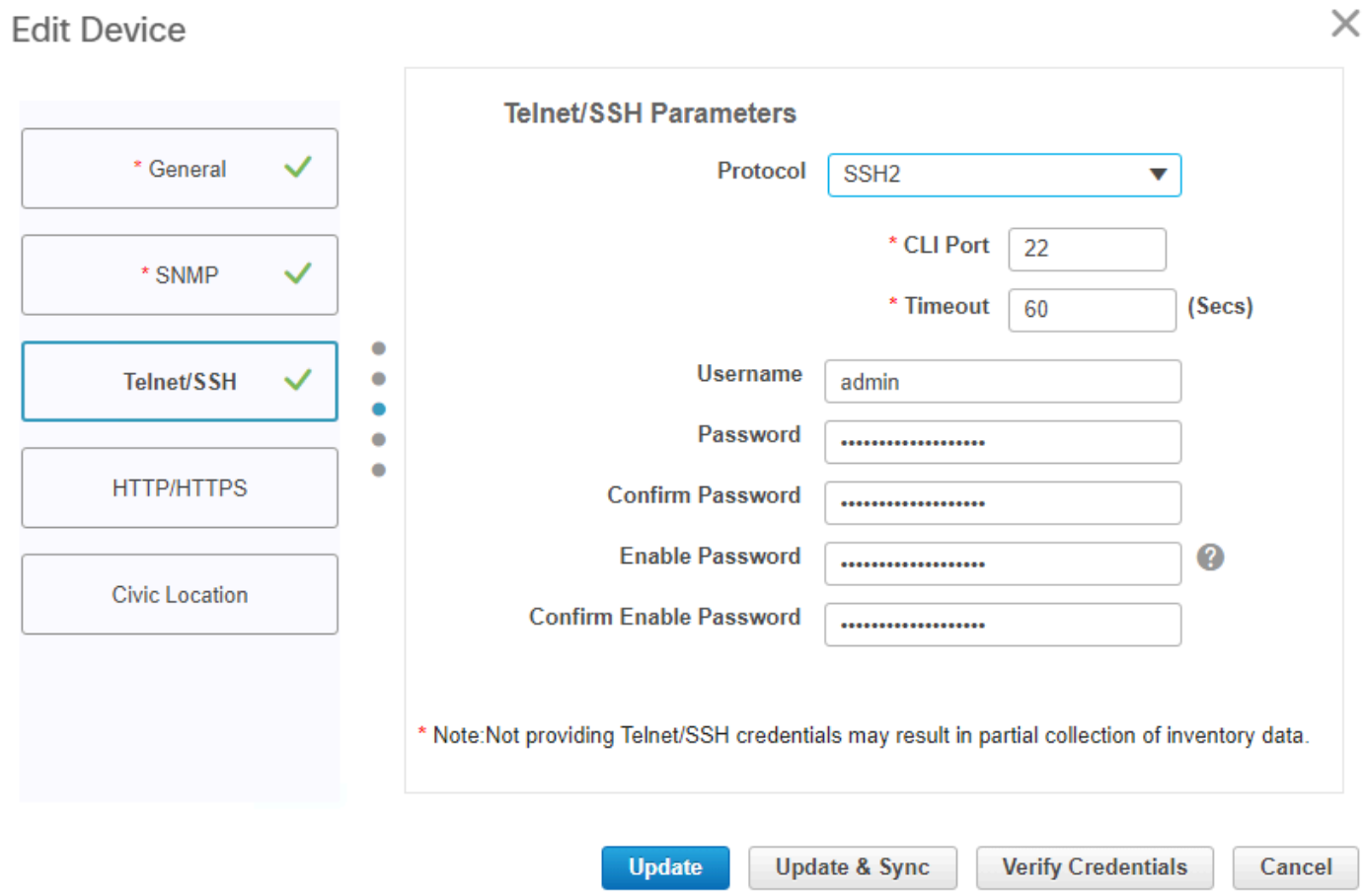
i. Section Général :



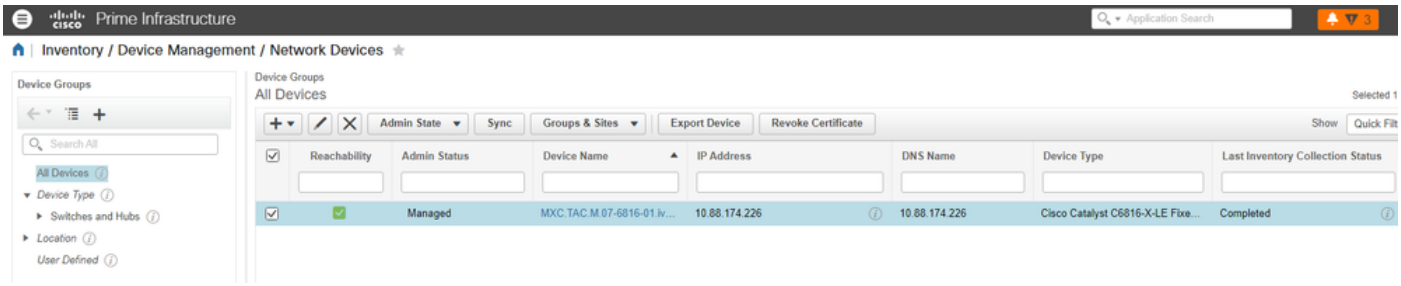
ii. Section SNMP:



iii. Section Telnet/SSH :



8. Une fois que tous les champs obligatoires sont renseignés, assurez-vous que l'accessibilité et l'état de collecte sont verts et terminés respectivement :

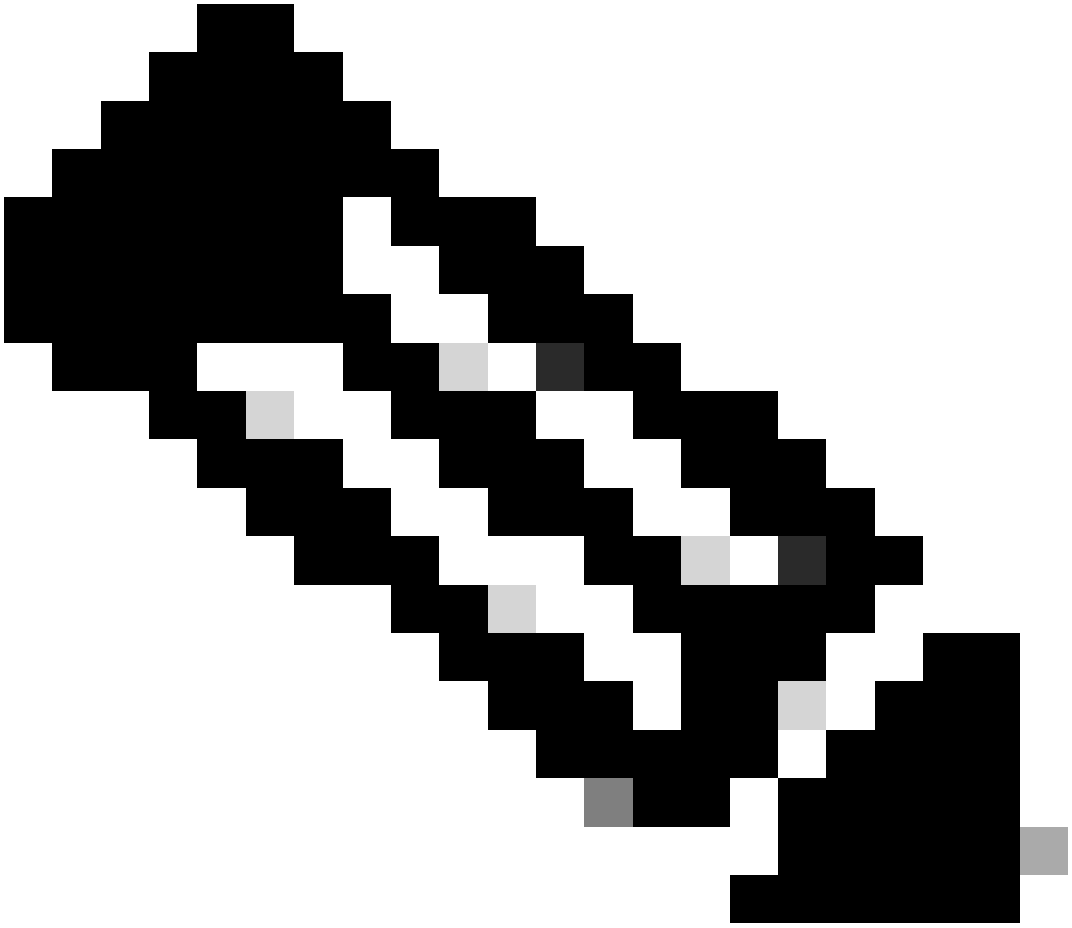


9. Intégrer Prime à ISE.

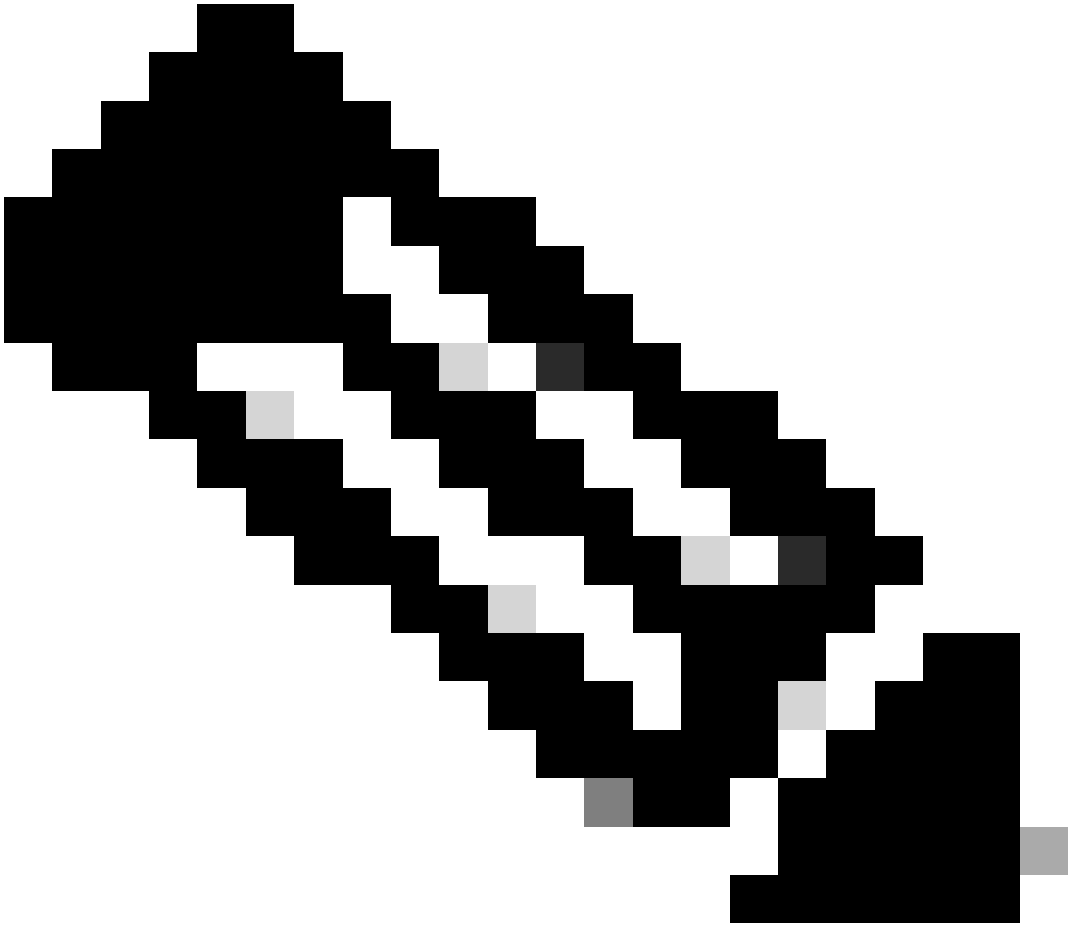
i. Accédez à Administration > Servers > ISE Servers.

ii. Dans le menu déroulant, sélectionnez Add ISE Server, puis cliquez sur Go :

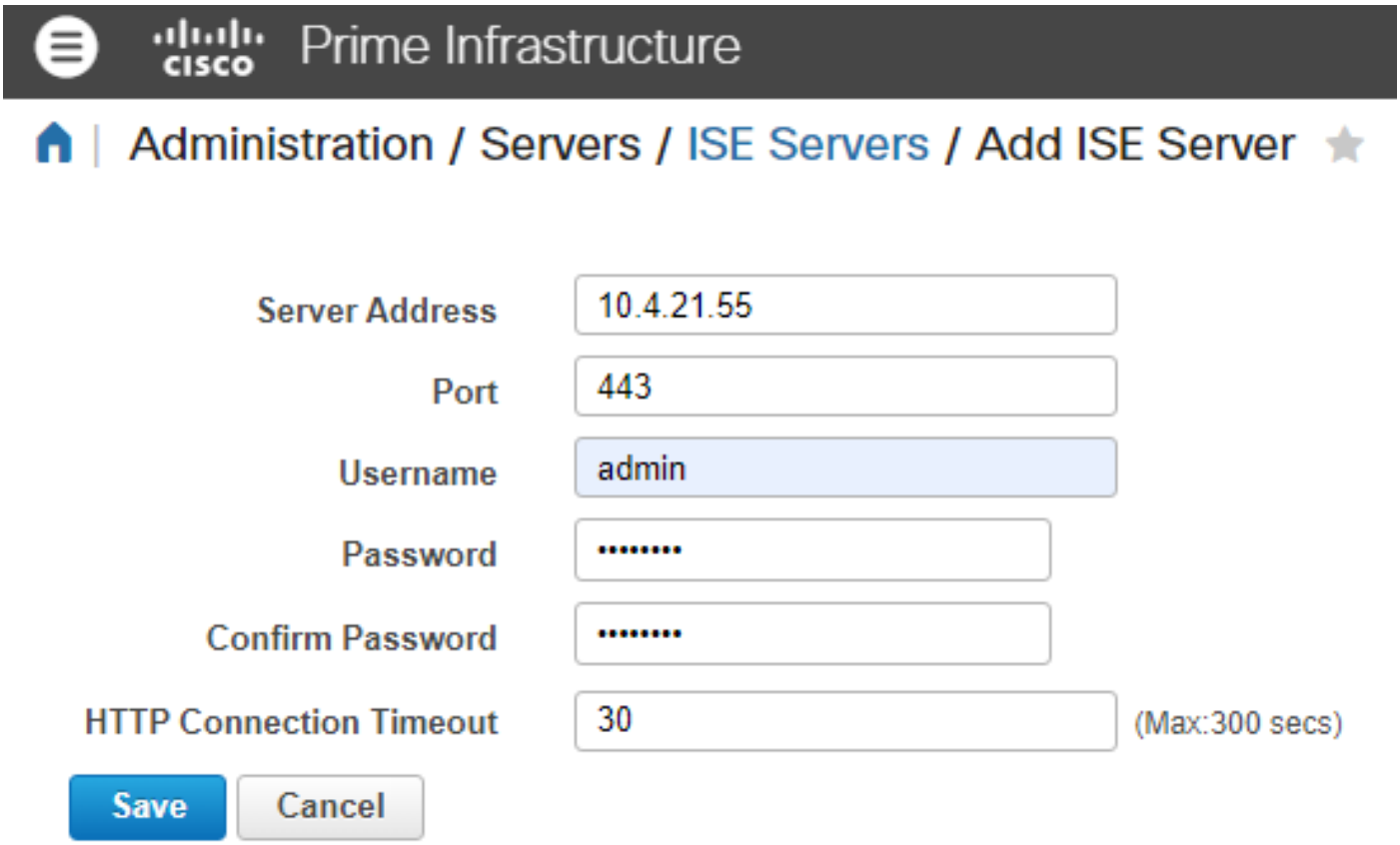
iii. Remplissez tous les champs et cliquez sur Enregistrer.



Remarque : La connexion doit être établie par rapport aux noeuds ISE de surveillance principal et secondaire (le cas échéant).



Remarque : Le port par défaut est défini sur 443, mais vous pouvez utiliser n'importe quel autre port ouvert dans ISE pour établir la connexion.



iv. Revenez à la page ISE Server. L'état du serveur indique Accessible et le rôle s'affiche (Autonome, Principal [MnT] ou Secondaire [MnT]) :

Configuration des terminaux

10. Le point de terminaison doit être configuré pour effectuer l'authentification dot1x (RFC 3850). Pour ce faire, vous pouvez configurer Cisco Network Access Manager (NAM) ou utiliser le demandeur natif du système d'exploitation. Comme il existe de nombreux guides relatifs à cette configuration, nous n'incluons pas ces étapes dans ce guide.

Vérifier

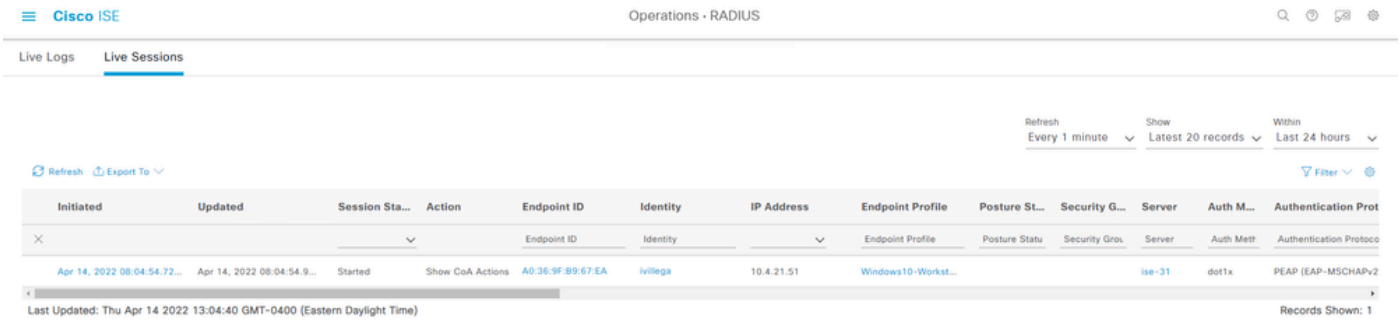
Vérifier ISE

ISE reçoit la requête RADIUS du NAD et authentifie l'utilisateur avec succès.

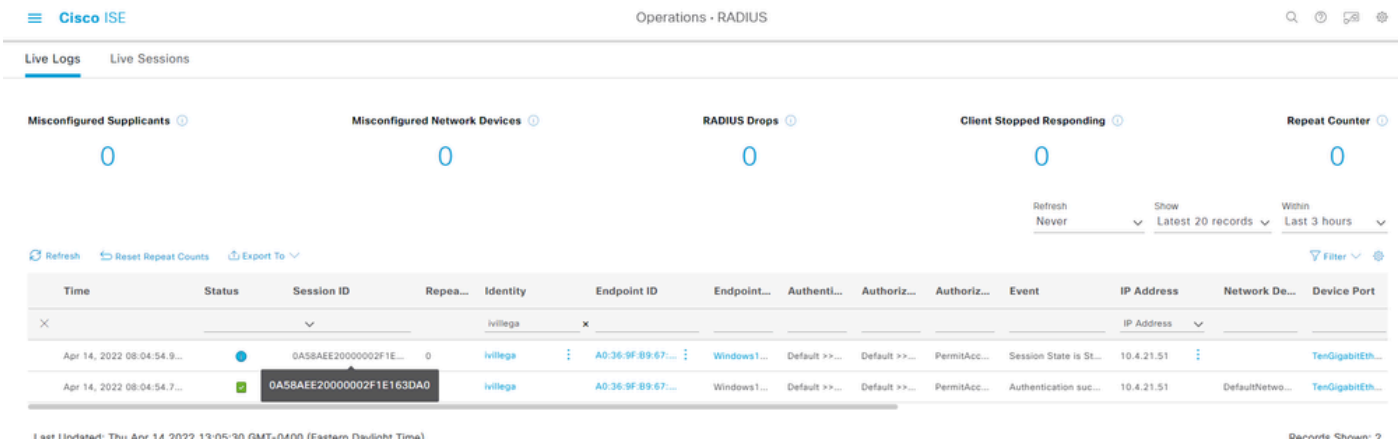
Le NAD est ajouté et configuré pour RADIUS dans ISE > Administration > Network Resources > Network Devices.

1. Accédez à Operations > RADIUS > Live Sessions.

Assurez-vous que la session utilisateur en direct est répertoriée dans cette page. Les informations de session sont partagées avec Prime Infrastructure.



2. Vérifiez l'ID de session dans Operations > RADIUS > Live Logs :



Vérification du NAD

3. Vérifiez les détails de la session dans le NAD. L'ID de session correspond à l'ID de session dans ISE :

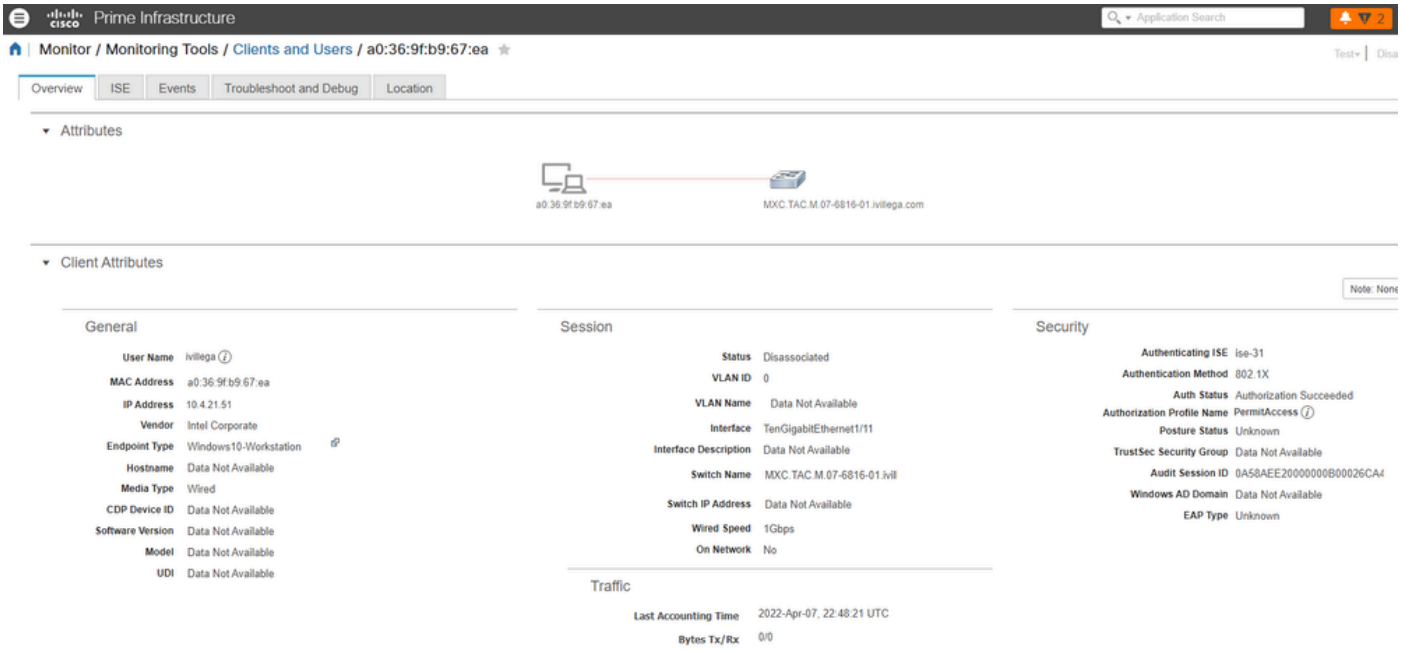
```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
        Interface: TenGigabitEthernet1/11
      MAC Address: a036.9fb9.67ea
     IPv6 Address: Unknown
     IPv4 Address: 10.4.21.51
        User-Name: ivillega
           Status: Authorized
           Domain: DATA
   Oper host mode: multi-domain
 Oper control dir: both
  Session timeout: N/A
Common Session ID: 0A58AEE20000002F1E163DA0
  Acct Session ID: 0x00000023
           Handle: 0xD9000001
   Current Policy: POLICY_Te1/11

Method status list:
        Method     State
```

```
dot1x      Authc Success
```

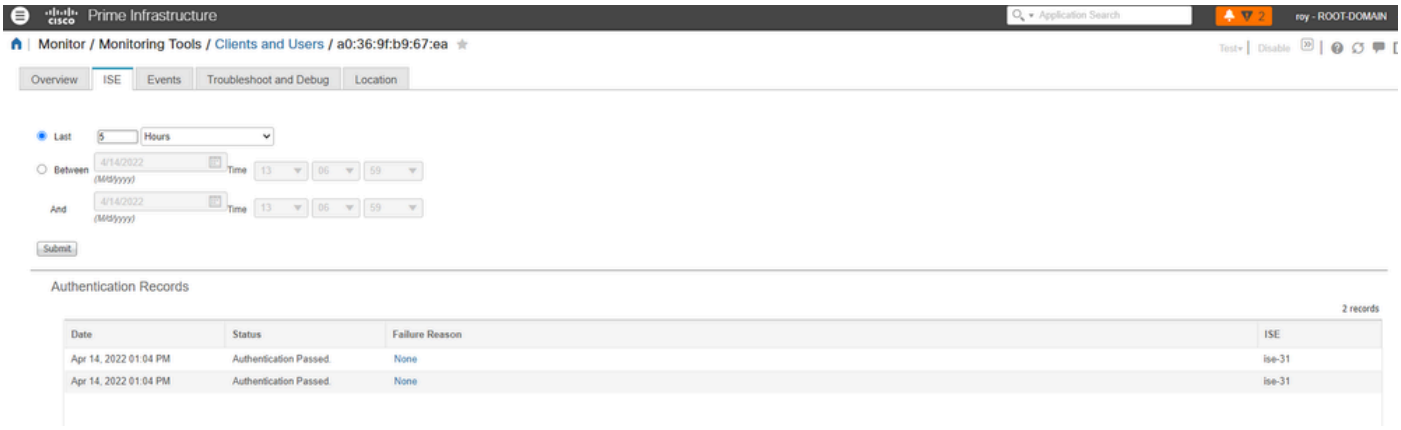
Vérification de l'infrastructure Prime

4. Accédez à Monitor > Monitoring Tools > Clients and Users. L'adresse MAC du point d'extrémité s'affiche :

5. Si vous cliquez dessus, vous voyez les détails de la session utilisateur et les informations du serveur ISE :



6. Il existe également un onglet intitulé ISE pour récupérer les événements de session pour ce point de terminaison particulier. Vous pouvez sélectionner une période que Prime Infrastructure utilise pour récupérer des événements à partir d'ISE :



Dépannage

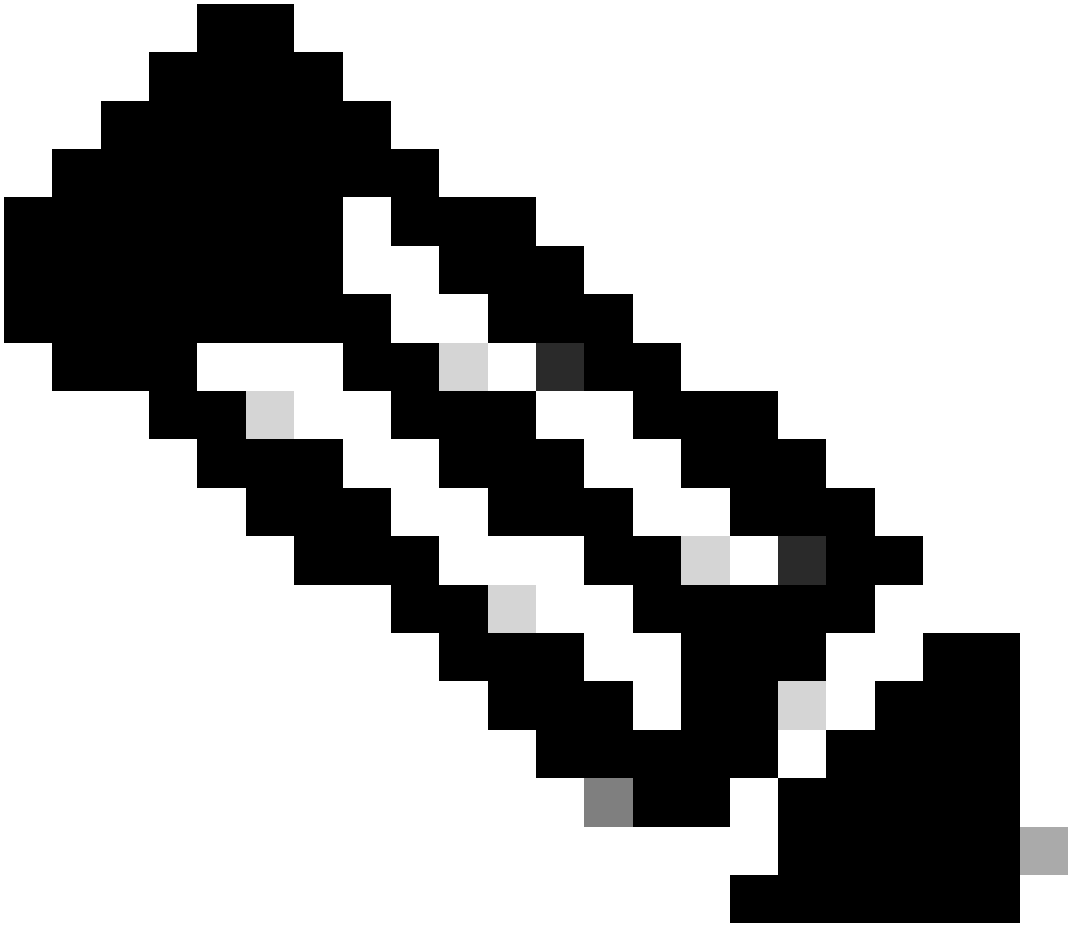
1. Testez la connectivité entre ISE et Prime Infrastructure avec des requêtes ping. S'il n'y a pas de connectivité, vous pouvez utiliser les routes de suivi depuis ISE ou PI pour localiser le problème.

2. Vérifiez que le port configuré à l'étape 9 est ouvert dans le noeud MnT ISE (le port par défaut est 443) :

```
ise-31-1/admin# show ports | include :443
     tcp: 0.0.0.0:80, 0.0.0.0:19444, 0.0.0.0:19001, 0.0.0.0:443
```

Si le port est répertorié dans le résultat, cela signifie que le port est ouvert pour ISE MnT.

S'il n'y a pas de sortie ou si le port n'est pas répertorié, cela signifie que le MnT ISE a fermé ce port. Dans ce cas, vous pouvez essayer avec un autre port ou ouvrir un dossier TAC avec l'équipe ISE pour vérifier pourquoi le port n'est pas ouvert.



Remarque : Le noeud MnT ISE utilise uniquement certains ports. Il est impossible d'ouvrir des ports dans le noeud MnT ISE qui ne sont pas répertoriés dans le guide d'installation d'ISE, section Référence de port.

3. Testez le port configuré à l’étape 9 avec Telnet à partir de l’infrastructure Prime :

```
prime-testcom/admin# telnet 10.4.21.55 port 443
Trying 10.4.21.55...
Connected to 10.4.21.55.
```

Si le résultat du test telnet est Connected to <ISE MnT IP/FQDN>, cela signifie que le test a réussi.

Si le résultat du test Telnet est bloqué à l’état Trying <ISE MnT IP/FQDN>, cela signifie que le test a échoué. Cela peut être lié aux listes de contrôle d'accès de vos périphériques réseau

intermédiaires ou aux règles de pare-feu.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.