Configuration de la restriction d'accès IP dans ISE

Table des matières

Introduction

Ce document décrit les options disponibles pour configurer la restriction d'accès IP dans ISE 3.1, 3.2 et 3.3.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de Cisco Identity Service Engine (ISE).

Composants utilisés

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

- Cisco ISE version 3.1
- Cisco ISE version 3.2
- Cisco ISE version 3.3

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.

Informations générales

La fonctionnalité de restriction d'accès IP permet aux administrateurs de contrôler les adresses IP ou les plages qui peuvent accéder au portail et aux services d'administration ISE.

Cette fonctionnalité s'applique à divers services et interfaces ISE, notamment :

- Accès au portail admin et CLI
- Accès à l'API ERS
- Accès au portail invité et sponsor
- Accès au portail Mes périphériques

Lorsqu'elle est activée, ISE autorise uniquement les connexions à partir des plages ou adresses IP spécifiées. Toute tentative d'accès aux interfaces d'administration ISE à partir d'IP non spécifiées est bloquée.

En cas de verrouillage accidentel, ISE fournit une option de démarrage « en mode sans échec » qui peut contourner les restrictions d'accès IP. Cela permet aux administrateurs de récupérer l'accès et de corriger les erreurs de configuration.

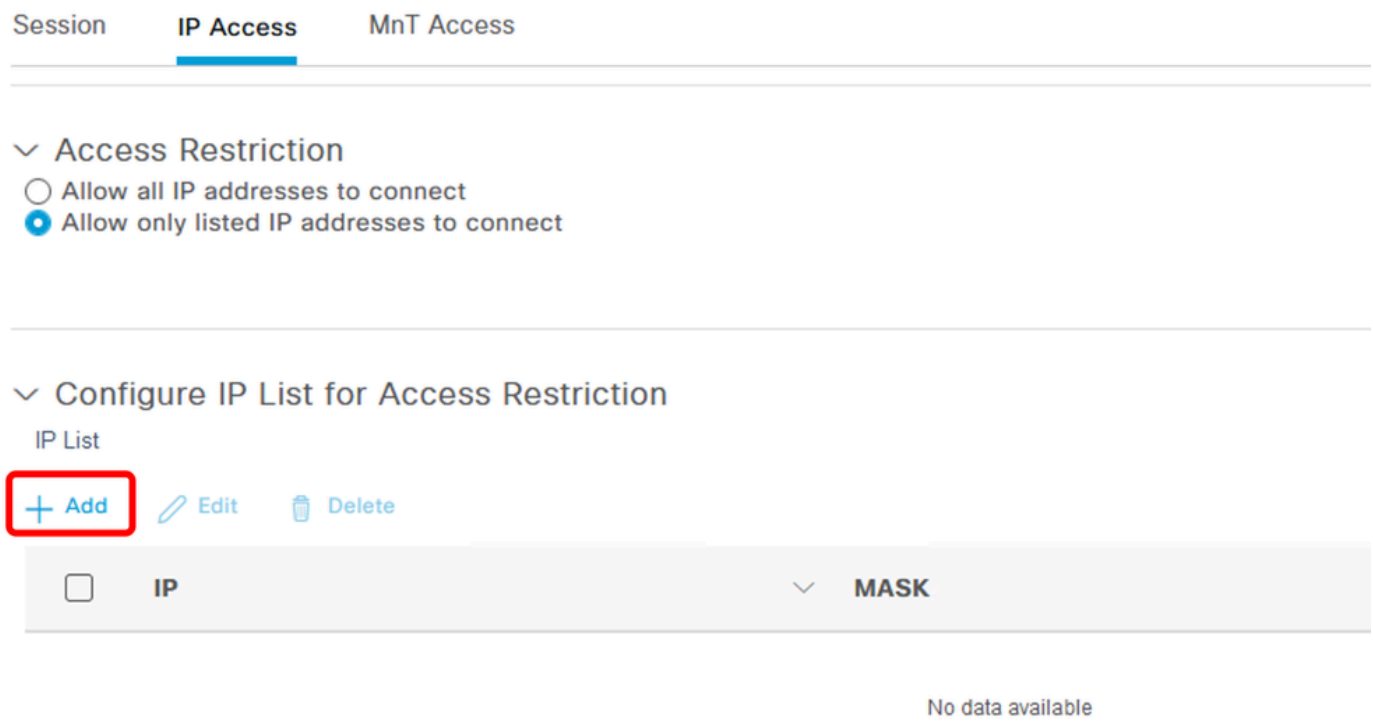
Comportement dans ISE 3.1 et versions antérieures

Accédez à Administration > Admin Access > Settings > Access . Vous disposez des options suivantes :

- Session
- Accès IP
- Accès MnT

Configurer

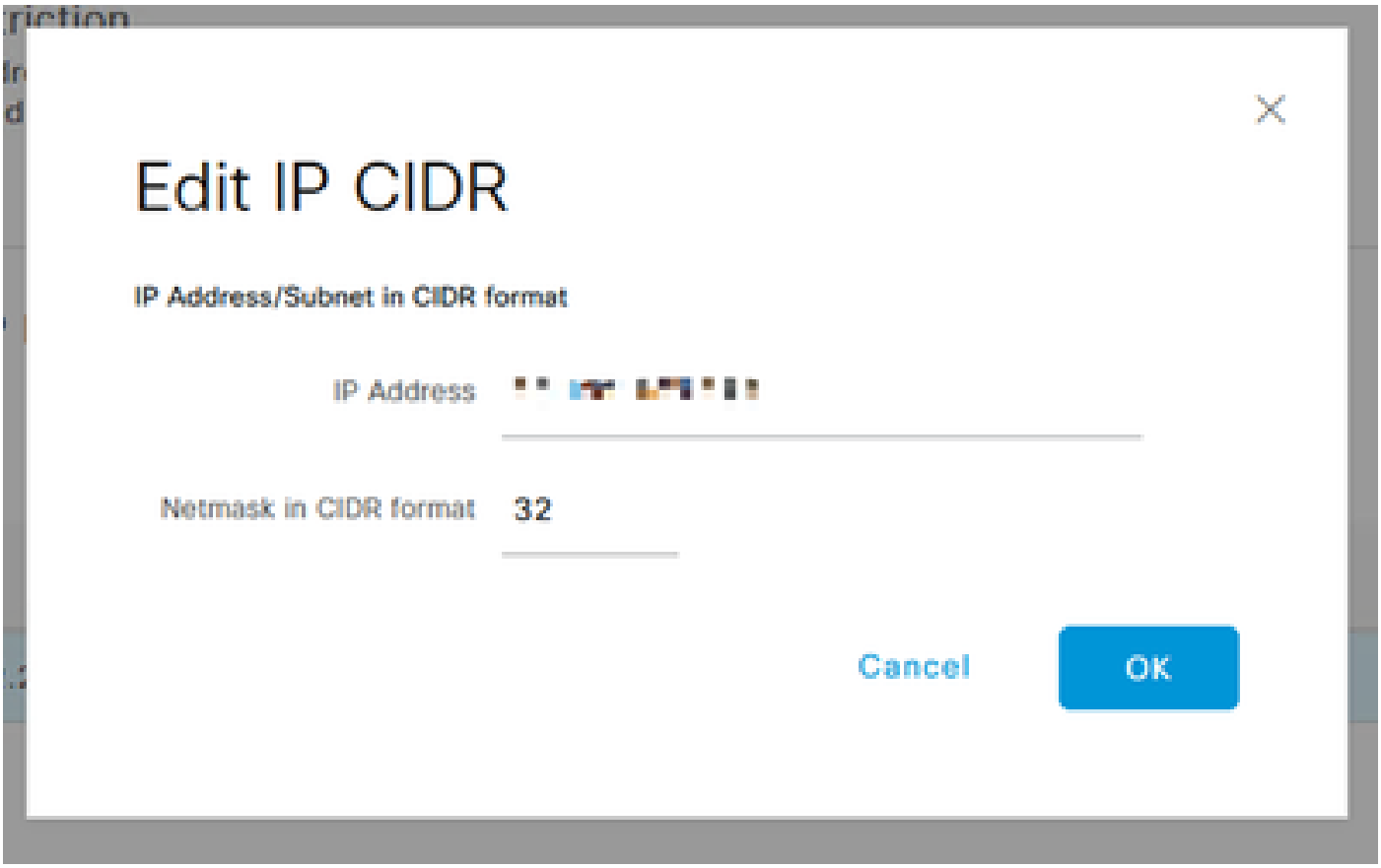
- Sélectionnez **Allow only listed IP addresses to connect** .
- Cliquez sur Add.



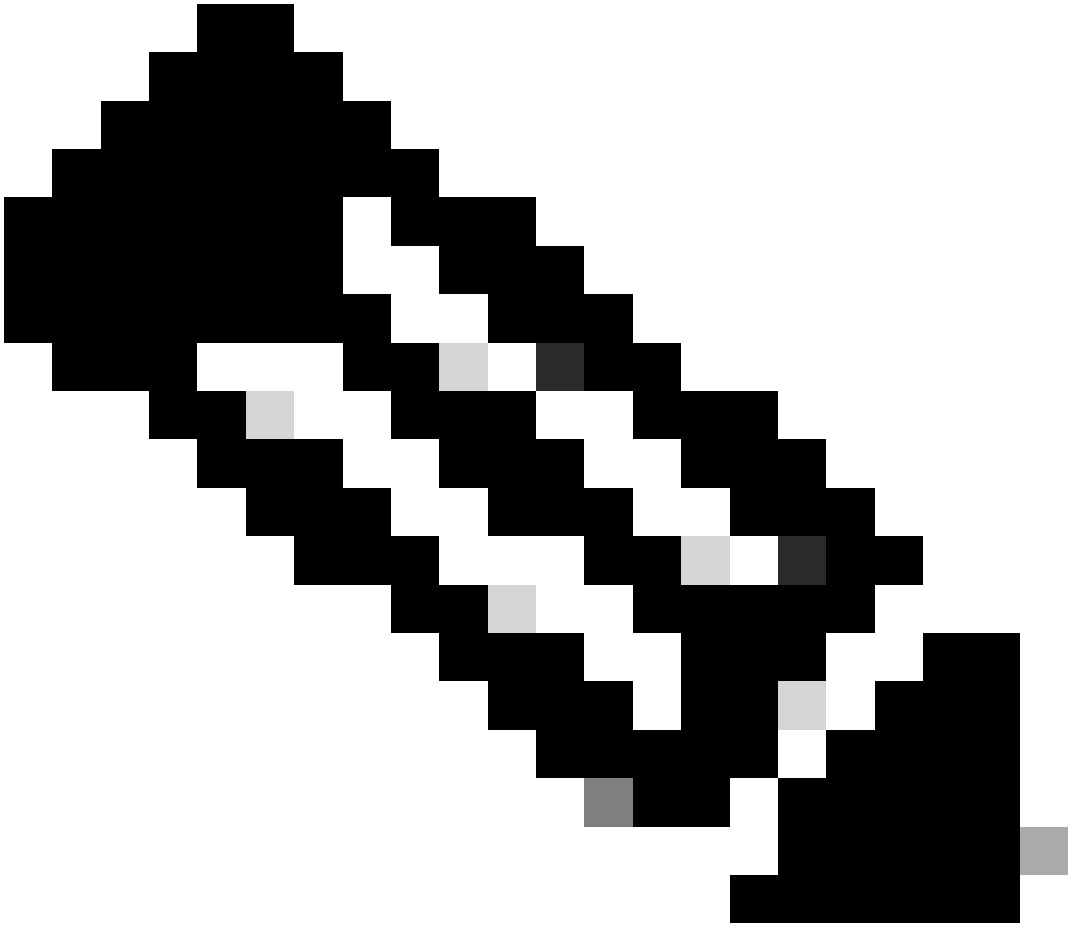
Configuration d'accès IP

- Dans ISE 3.1, vous n'avez pas la possibilité de sélectionner entre Admin et les **User** services, ce qui permet à la restriction d'accès IP de bloquer les connexions pour :
  - IUG
  - CLI
  - SNMP
  - SSH

- Une boîte de dialogue s'ouvre et vous permet d'entrer les adresses IP, IPv4 ou IPv6, au format CIDR.
- Une fois l'adresse IP configurée, définissez le masque au format CIDR.



Modifier le CIDR IP

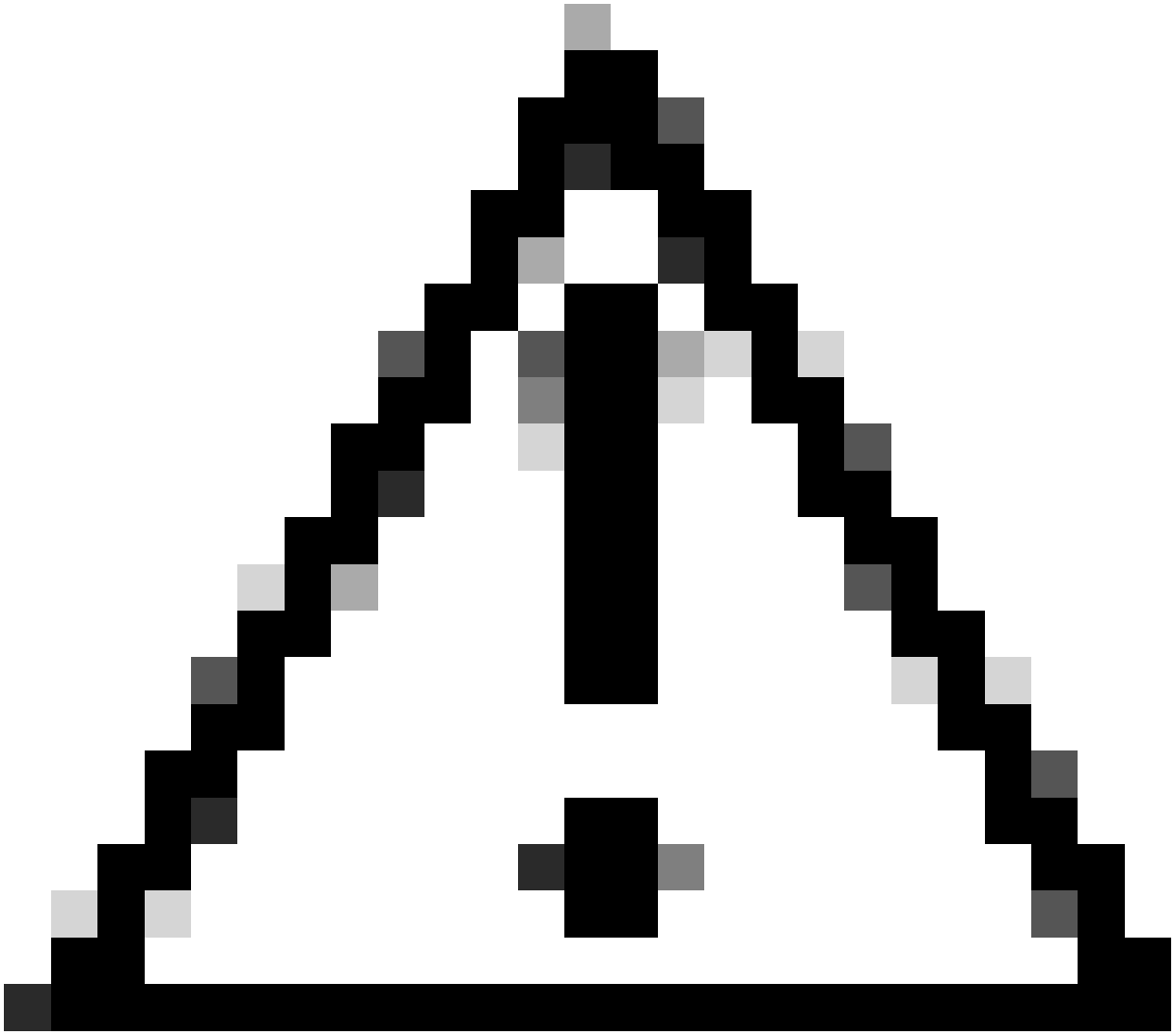


Remarque : le format CIDR (Classless Inter-Domain Routing) IP est une méthode de représentation des adresses IP et de leur préfixe de routage associé.

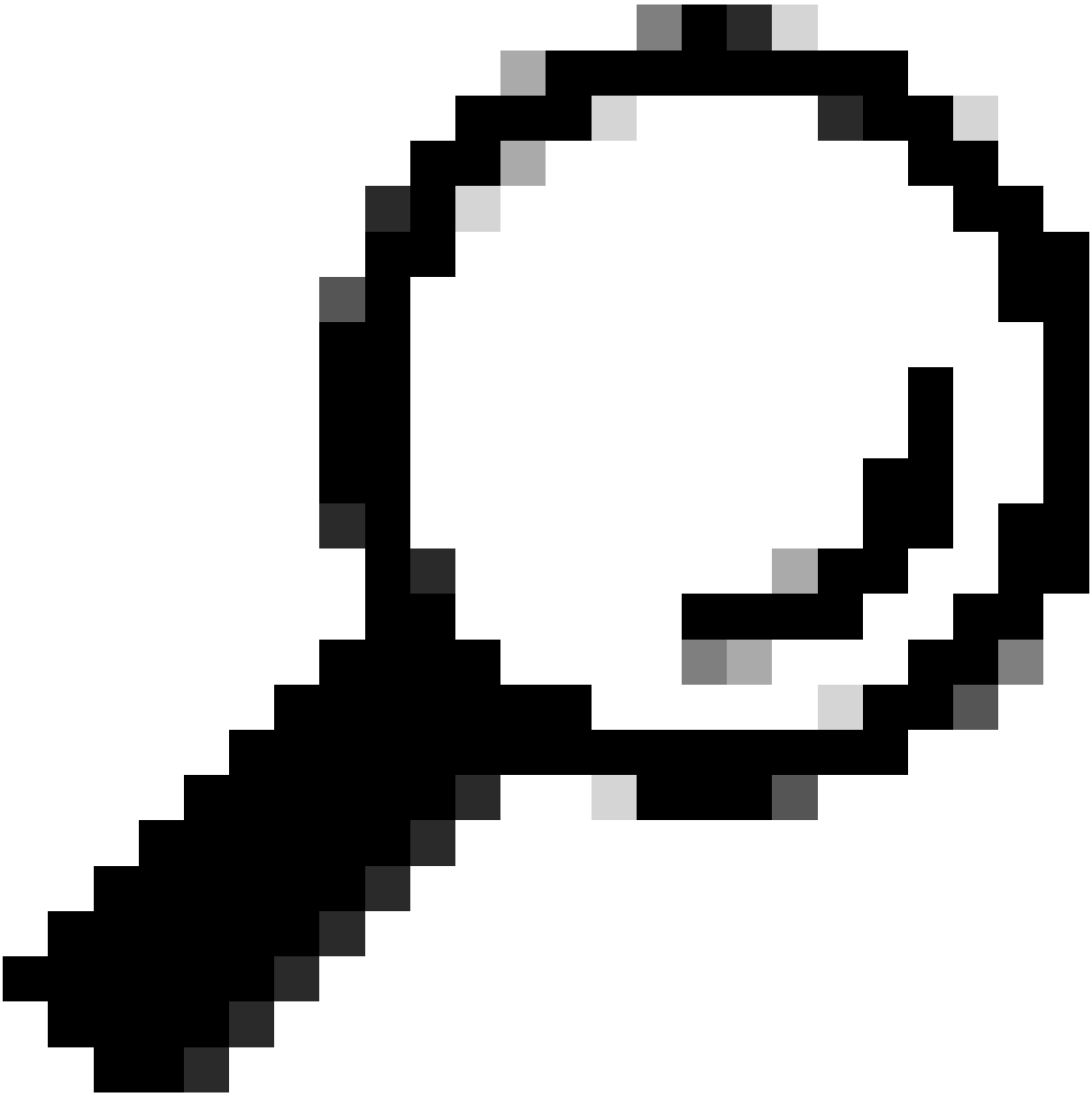
Exemple :

IP : 10.8.16.32

Masque : /32



Attention : vous devez être prudent lors de la configuration des restrictions IP afin d'éviter de verrouiller accidentellement l'accès administrateur légitime. Cisco recommande de tester minutieusement toute configuration de restriction IP avant de l'implémenter complètement.



Conseil : pour les adresses IPv4 :

- Utilisez /32 pour des adresses IP spécifiques.
- Pour les sous-réseaux, utilisez une autre option. Exemple : 10.26.192.0/18

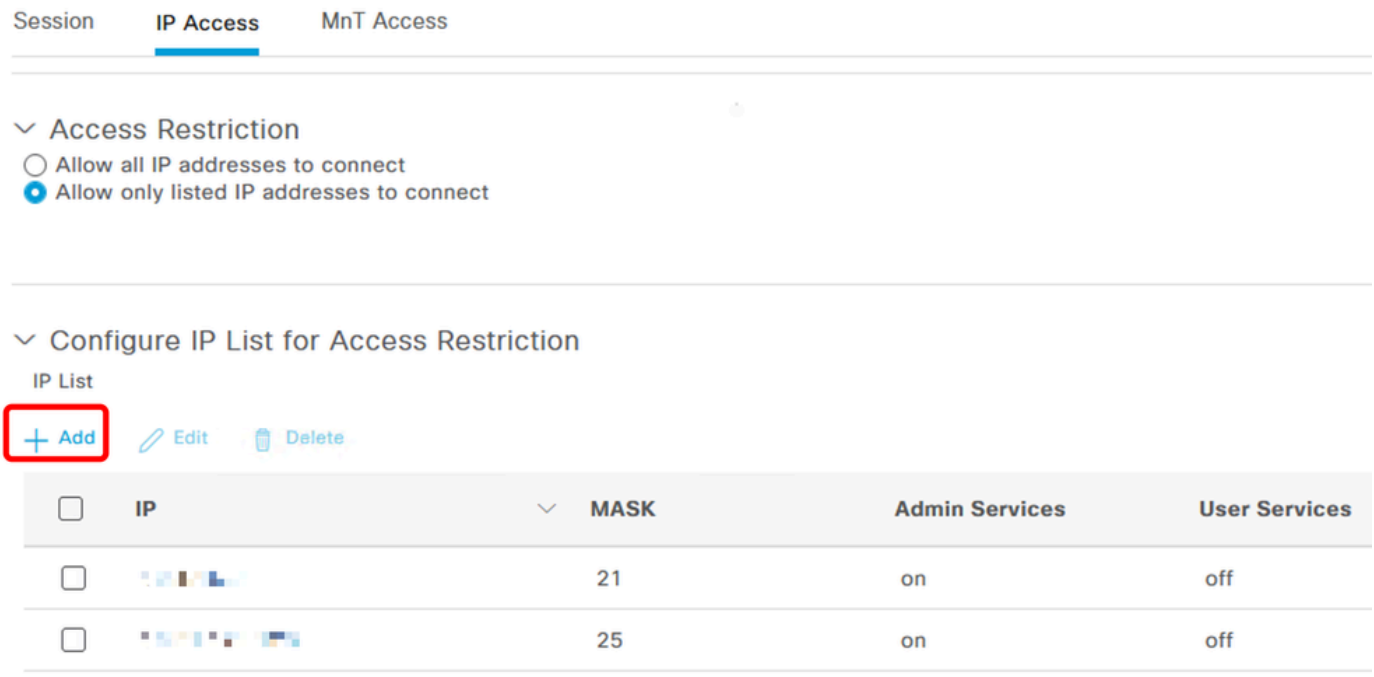
Comportement dans ISE 3.2

Accédez à Administration > Admin Access > Settings > Access. Vous disposez des options suivantes :

- Session
- Accès IP
- Accès MnT

Configurer

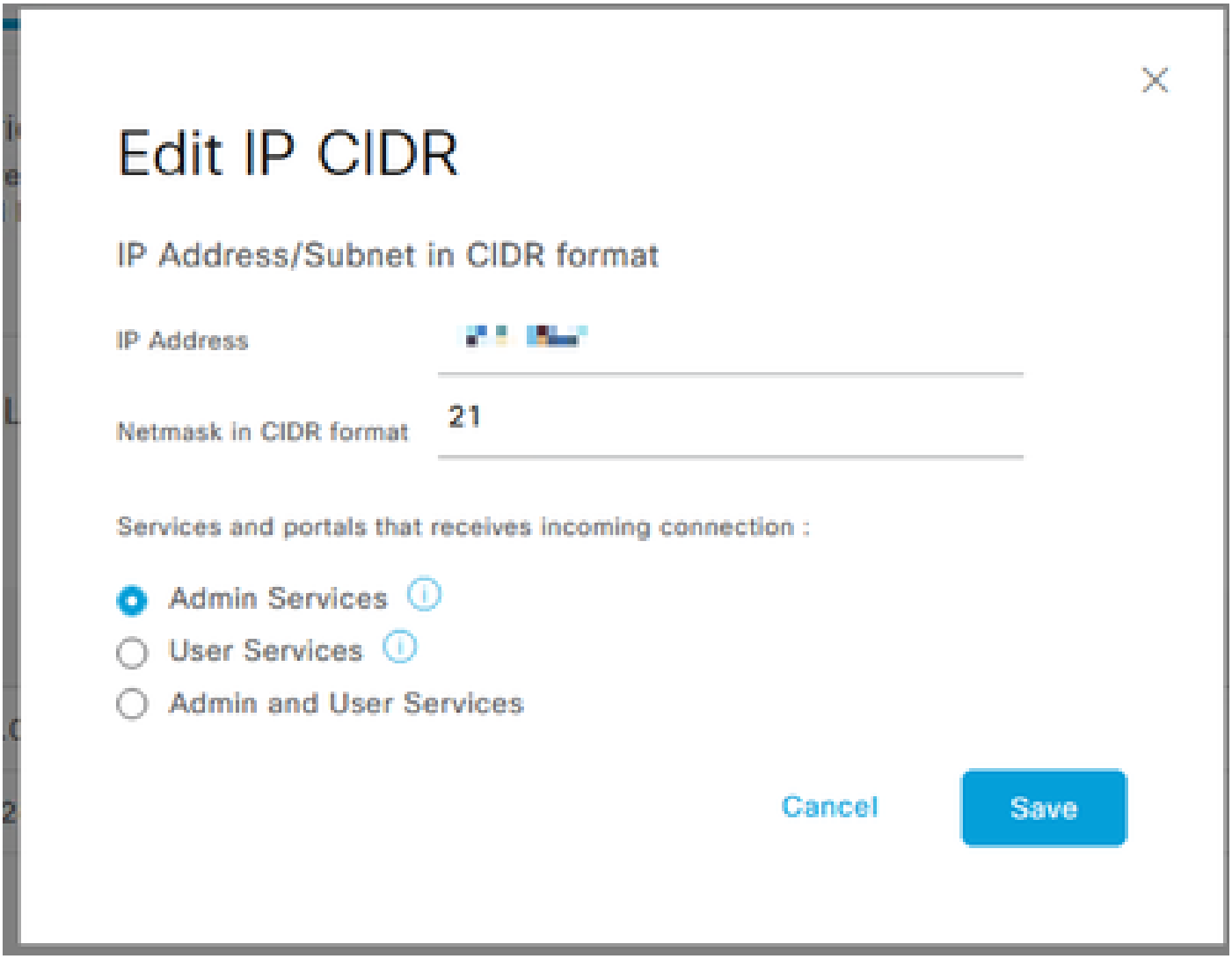
- Sélectionner **Allow only listed IP addresses to connect**.
- Cliquez sur Add.



Configuration de l'accès IP

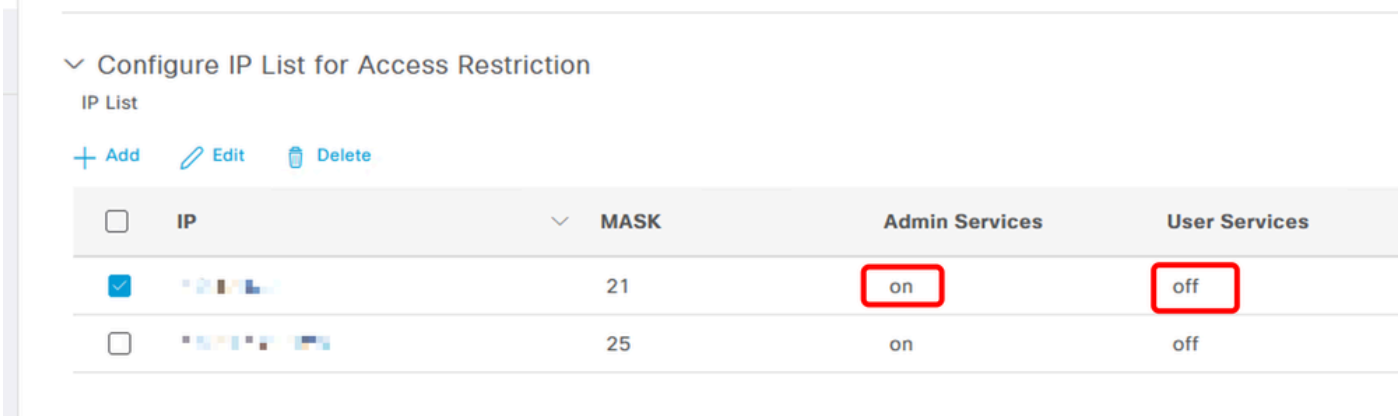
- Une boîte de dialogue s'ouvre et vous permet d'entrer les adresses IP, IPv4 ou IPv6, au format CIDR.
- Une fois l’adresse IP configurée, définissez le masque au format CIDR.
- Ces options sont disponibles pour la restriction d'accès IP :

- Services d'administration : GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (désactivé dans le patch 2), MnT Analytics
- Services utilisateur : invité, BYOD, posture, profilage
- Services administrateur et utilisateur



Modifier le CIDR IP

- Cliquez sur le boutonSave.
- ON signifie que les services Admin sont activés, OFF que les services utilisateur sont désactivés.

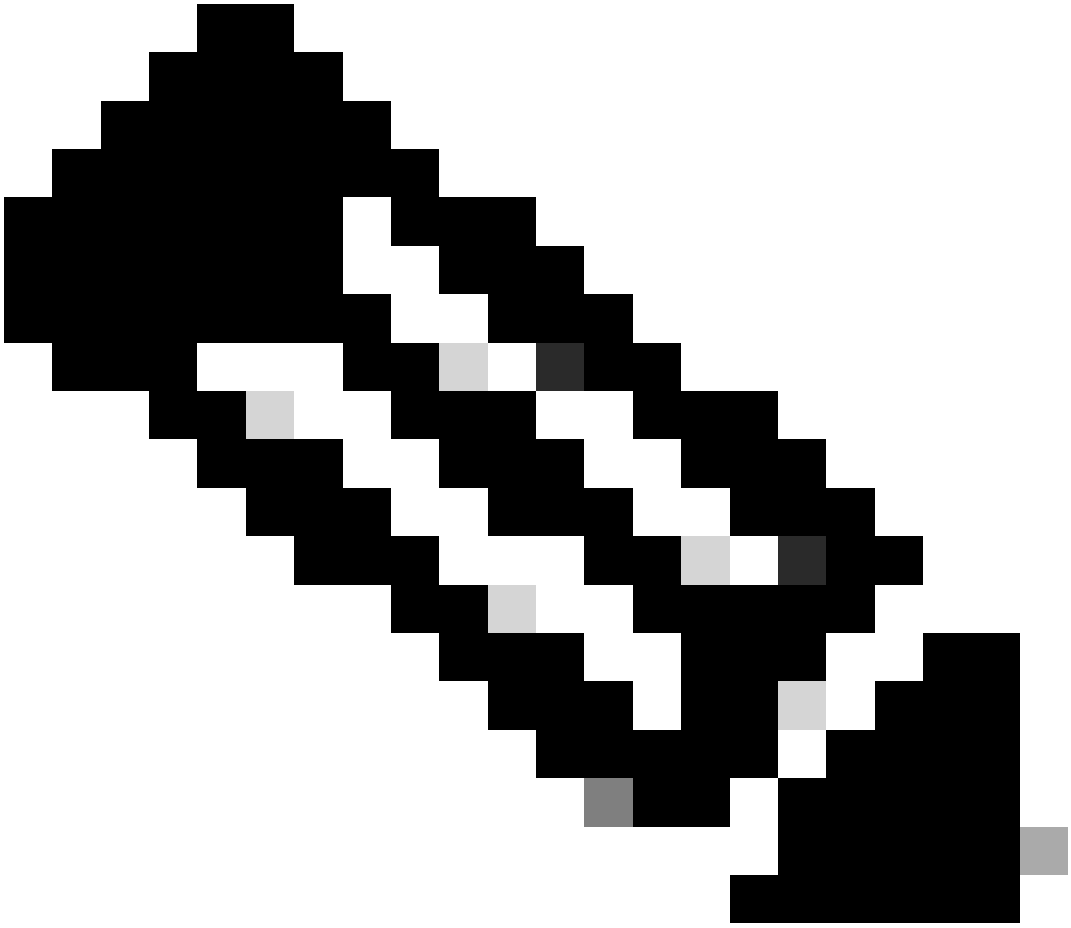


Configuration de l'accès IP dans 3.2

Comportement dans ISE 3.2 P4 et versions ultérieures

Accédez à Administration > Admin Access > Settings > Access . Vous disposez des options suivantes :

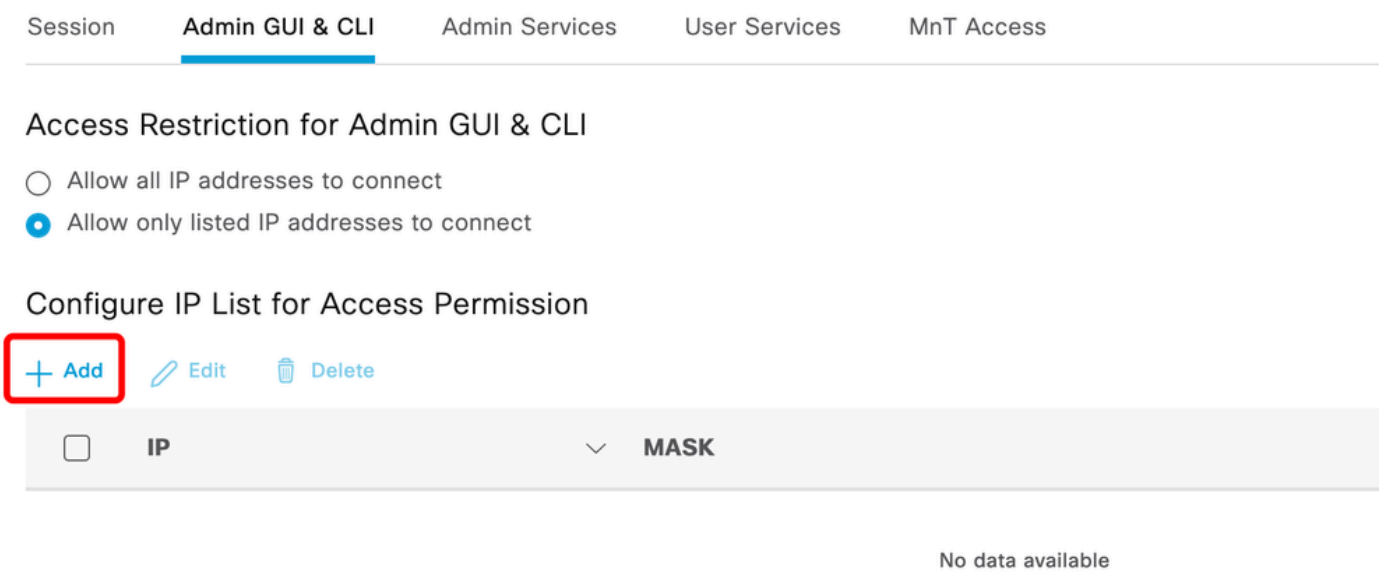
- Session
- Interface utilisateur graphique et interface de ligne de commande d'administration : interface utilisateur graphique ISE (TCP 443), interface de ligne de commande ISE (SSH TCP22) et SNMP.
- Services d'administration : API ERS, API ouverte, pxGrid, DataConnect.
- Services utilisateur : invité, BYOD, posture.
- Accès MNT : avec cette option, ISE n'utilise pas les messages Syslog envoyés depuis des sources externes.



Remarque : la restriction d'accès pxGrid et Data Connect concerne ISE 3.3+, mais pas ISE 3.2 P4+.

Configurer

- Sélectionner Allow only listed IP addresses to connect.
- Cliquer **Add**.



Configuration de l'accès IP dans 3.3

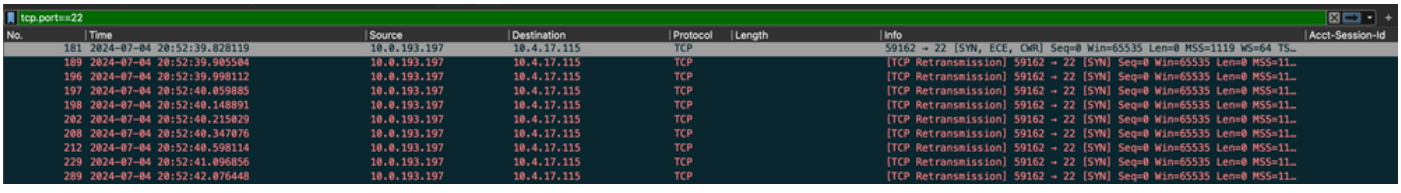
- Une boîte de dialogue s'ouvre et vous permet d'entrer les adresses IP, IPv4 ou IPv6, au format CIDR.
- Une fois l'adresse IP configurée, définissez le masque au format CIDR.
- Cliquez sur Add.

Récupérer l'interface utilisateur graphique/CLI ISE

- Connectez-vous avec la console.
- Arrêter les services ISE en utilisant application stop ise
- Démarrer les services ISE en utilisant application start ise safe
- Supprimez la restriction d'accès IP de l'interface utilisateur graphique.

Dépannage

Effectuez une capture de paquets pour vérifier si ISE ne répond pas ou s'il abandonne le trafic.



Vérifier les règles du pare-feu ISE

- Pour les versions 3.1 et inférieures, vous pouvez vérifier cela uniquement dans le show tech.

    - Vous pouvez prendre un show tech et le stocker sur le disque local en utilisant show tech-support file <filename>

        - Vous pouvez ensuite transférer le fichier vers un référentiel à l'aide de copy disk:/<filename> ftp://<ip_address>/path. L'URL du référentiel change en fonction du type de référentiel que vous utilisez.
        - Vous pouvez télécharger le fichier sur votre ordinateur pour le lire et le rechercher **Running iptables -nvL**.
        - Les règles initiales du show tech ne sont pas incluses ici. En d'autres termes, vous trouverez ici les dernières règles ajoutées à la fonctionnalité de restriction show tech by IP Access.

```
****************************************
Running iptables -nvL...
****************************************
.
.
Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0 tcp dpt:22 Firewall rule permitting the SSH traffic from segment x.x.x.x/x
461 32052 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
65 4048 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0 udp dpt:161 Firewall rule permitting the SNMP traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

- Pour les versions 3.2 et ultérieures, vous pouvez utiliser la commande show firewall pour vérifier les règles de pare-feu.
- Les versions 3.2 et ultérieures offrent un meilleur contrôle sur les services bloqués par la restriction d'accès IP.

```
gjuarezo-311/admin#show firewall
.
.

Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
170 13492 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0 tcp dpt:22 Firewall rule permitting the SSH traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
13 784 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0 udp dpt:161 Firewall rule permitting the SNMP traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

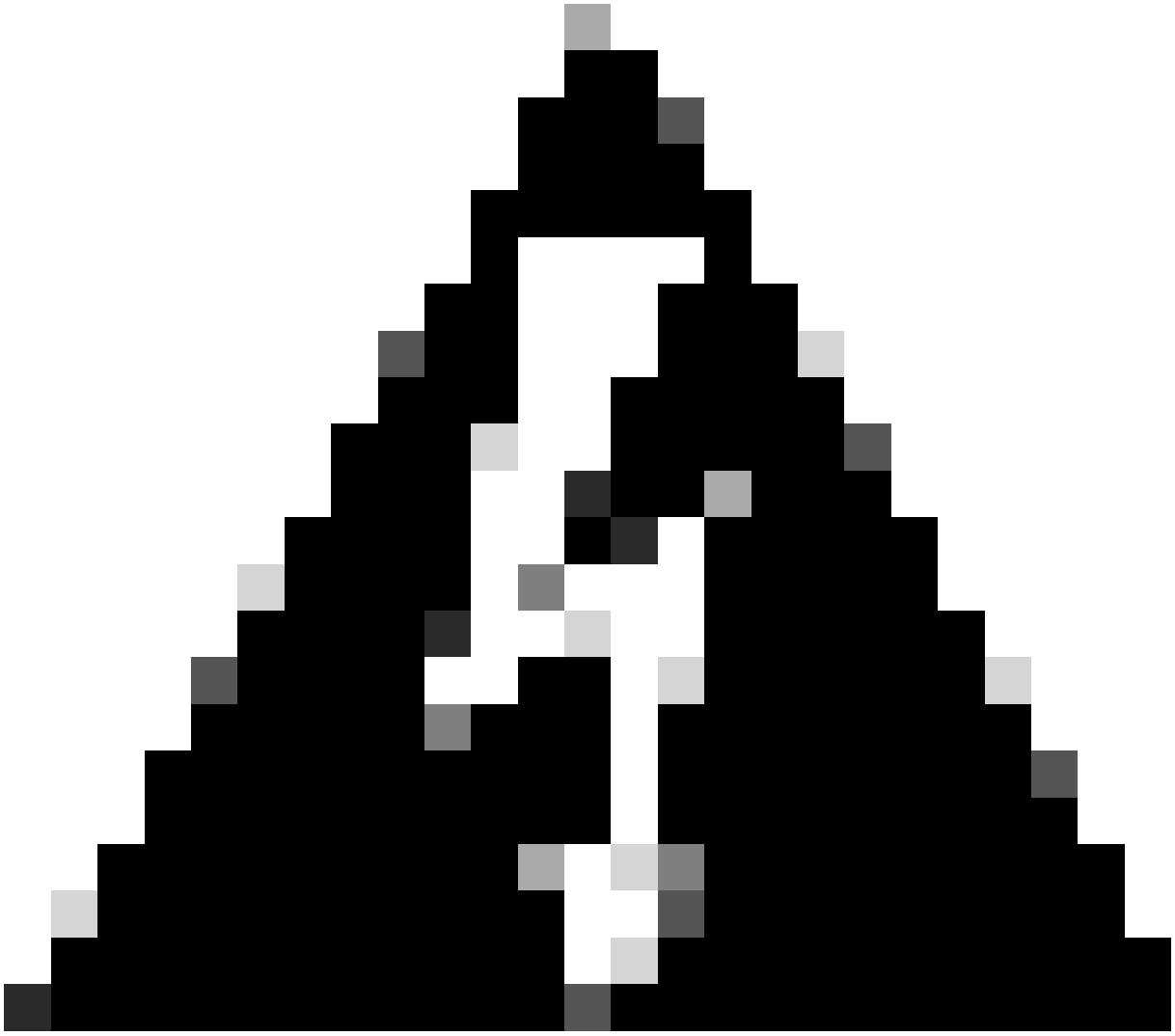
Chain ACCEPT_8910_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8910 Firewall rule permitting the PxGrid traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
90 5400 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8443_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8443 Firewall rule permitting the HTTPS traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8444_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8444 Firewall rule permitting the Block List Portal traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8445_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8445 Firewall rule permitting the Sponsor Portal traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Vérifier les journaux de débogage



Avertissement : tout le trafic ne génère pas de journaux. La restriction d'accès IP peut bloquer le trafic au niveau de l'application et à l'aide du pare-feu interne Linux. SNMP, CLI et SSH sont bloqués au niveau du pare-feu, de sorte qu'aucun journal n'est généré.

- Activer le Infrastructure composant pour DEBUG à partir de l'interface utilisateur graphique.
- Activez le **Admin-infra** composant pour DEBUG depuis l'interface utilisateur graphique.
- Activez le **NSF** composant pour DEBUG depuis l'interface utilisateur graphique.
- Utilisez show logging application ise-psc.log tail.

Les exemples d'entrées de journal peuvent être vus lorsque l'accès à l'interface utilisateur Web de l'administrateur ISE est restreint, où le sous-réseau autorisé est 198.18.133.0/24 tandis que l'administrateur ISE provient de 198.18.134.28.

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- IpList -> 198.18.133.0/24/basicS
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- Low ip address198.18.133.0
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- High ip address198.18.133.255
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.nsf.impl.NetworkElement -:::::- The ip address to check is v4 198.18.134.28
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- Checkin Ip In ipList returned Fin
```

Informations connexes

- Guide d'administration ISE 3.1
- Guide d'administration ISE 3.2
- Guide d'administration ISE 3.3
- Assistance technique de Cisco et téléchargements

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.