Configurazione della restrizione di accesso IP in ISE

Sommario

Introduzione

In questo documento vengono descritte le opzioni disponibili per configurare la limitazione dell'accesso IP in ISE 3.1, 3.2 e 3.3.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Identity Service Engine (ISE).

Componenti usati

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

- Cisco ISE versione 3.1
- Cisco ISE versione 3.2
- Cisco ISE versione 3.3

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.

Premesse

La funzione di restrizione dell'accesso IP consente agli amministratori di controllare gli indirizzi IP o gli intervalli di indirizzi IP che possono accedere al portale di amministrazione e ai servizi ISE.

Questa caratteristica si applica a diverse interfacce e servizi ISE, tra cui:

- Accesso al portale di amministrazione e CLI
- Accesso API ERS
- Accesso al portale per gli ospiti e gli sponsor
- Accesso al portale I miei dispositivi

Se abilitata, ISE consente solo le connessioni dagli indirizzi IP o dagli intervalli specificati. Qualsiasi tentativo di accedere alle interfacce di amministrazione ISE da indirizzi IP non specificati viene bloccato.

In caso di blocco accidentale, ISE offre un'opzione di avvio in modalità provvisoria che può ignorare le restrizioni di accesso IP. Ciò consente agli amministratori di riottenere l'accesso e correggere eventuali configurazioni errate.

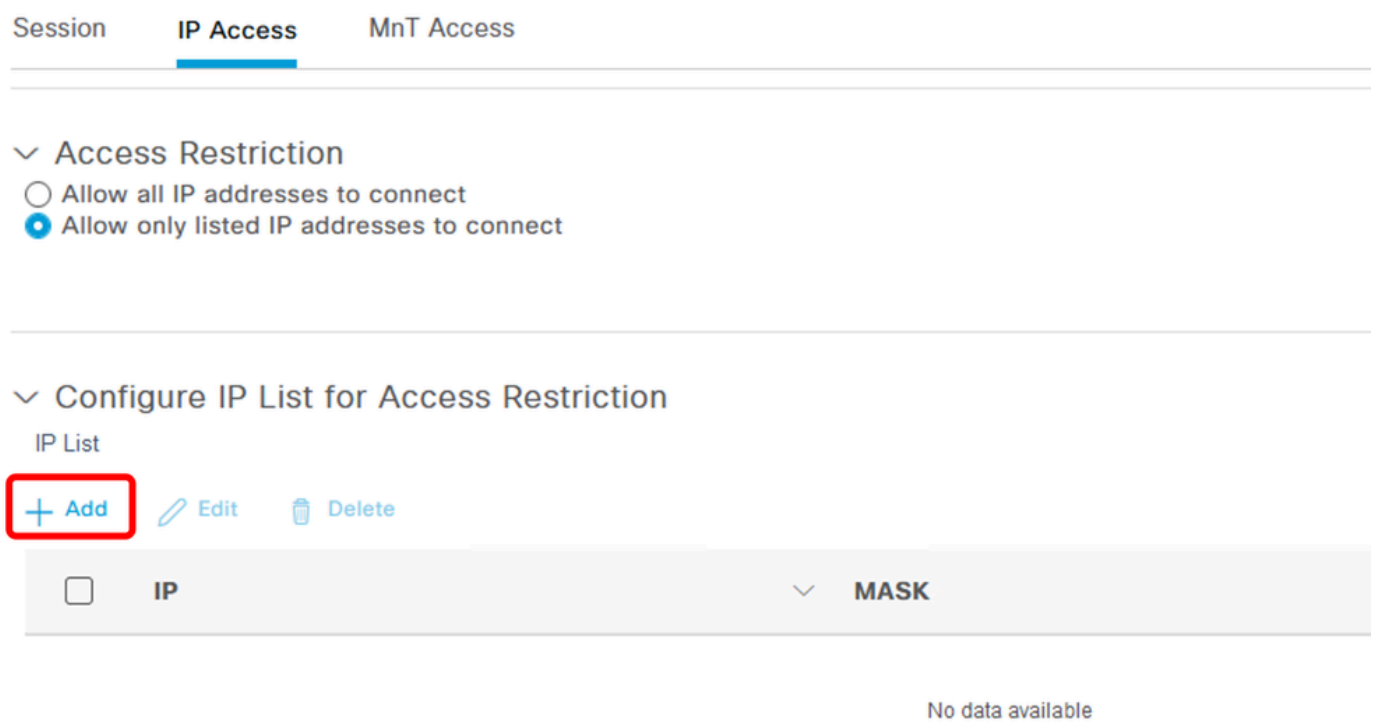
Comportamento in ISE 3.1 e versioni precedenti

Passare a Administration > Admin Access > Settings > Access . Sono disponibili le opzioni seguenti:

- Sessione
- Accesso IP
- Accesso MnT

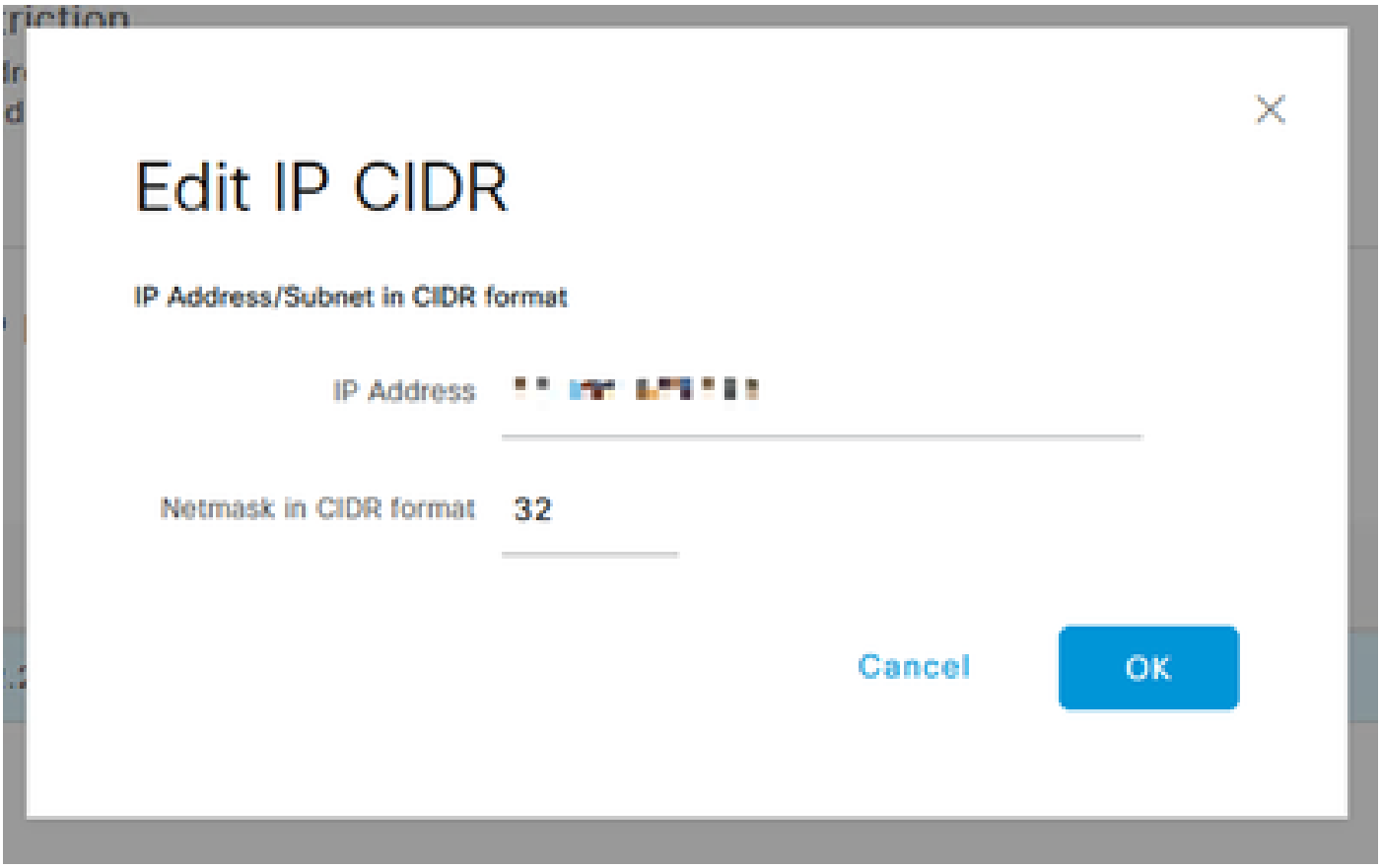
Configurazione

- Selezionare **Allow only listed IP addresses to connect** .
- Fare clic su .Add

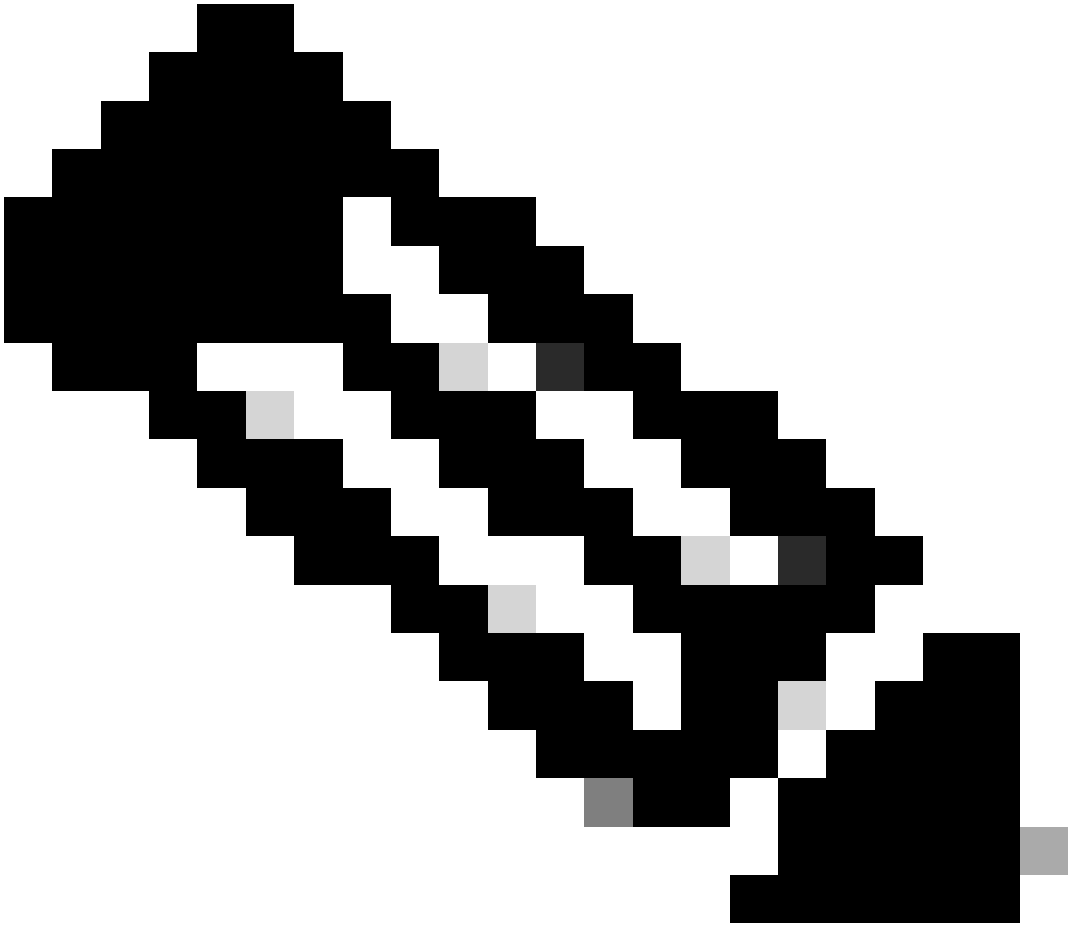


Configurazione accesso IP

- In ISE 3.1 non è disponibile un'opzione per selezionare tra Admin e **User** servizi, abilitando la limitazione dell'accesso IP le connessioni a:
  - GUI
  - CLI
  - SNMP
  - SSH
- Verrà visualizzata una finestra di dialogo in cui è possibile immettere gli indirizzi IP, IPv4 o IPv6, in formato CIDR.
- Una volta configurato l'IP, impostare la maschera in formato CIDR.



Modifica CIDR IP

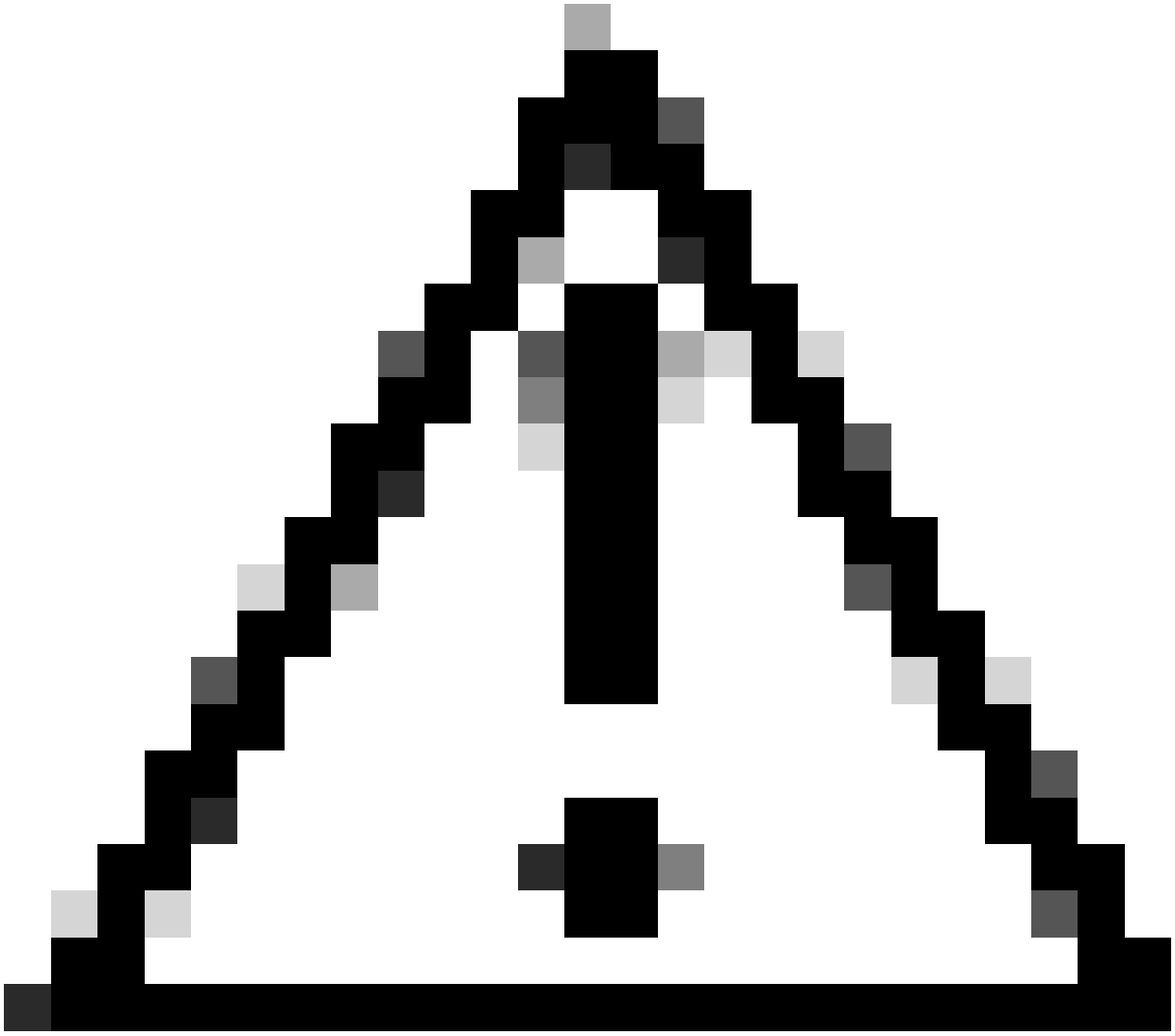


Nota: il formato CIDR (IP Classless Inter-Domain Routing) è un metodo per rappresentare gli indirizzi IP e il prefisso di routing associato.

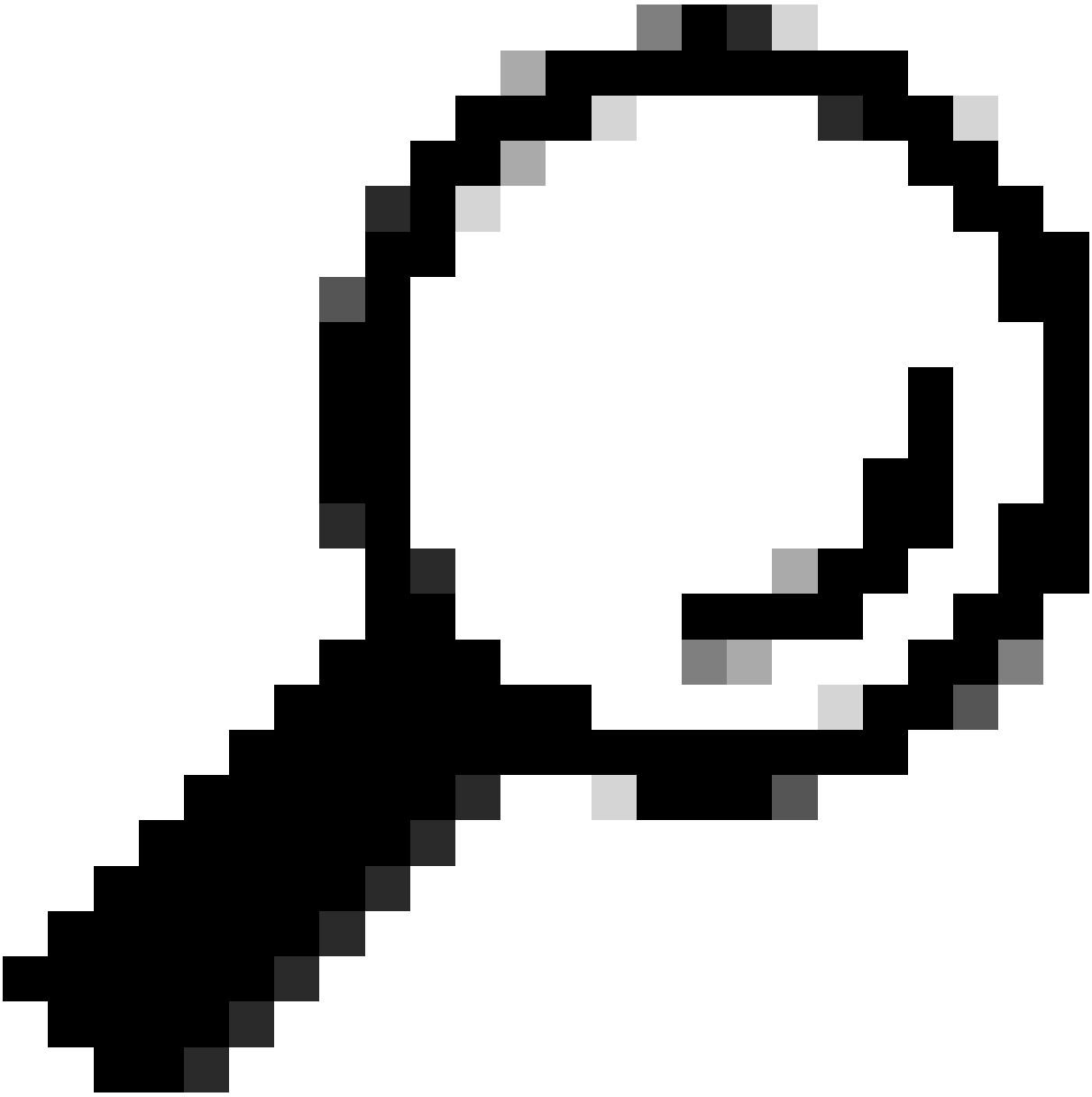
Esempio:

IP: 10.8.16.32

Maschera: /32



Attenzione: prestare attenzione quando si configurano le restrizioni IP per evitare di bloccare accidentalmente l'accesso degli amministratori autorizzati. Cisco consiglia di testare accuratamente qualsiasi configurazione con restrizioni IP prima di implementarla completamente.



Suggerimento: per indirizzi IPv4:

- Utilizzare /32 per indirizzi IP specifici.
- Per le subnet, utilizzate qualsiasi altra opzione. Esempio: 10.26.192.0/18

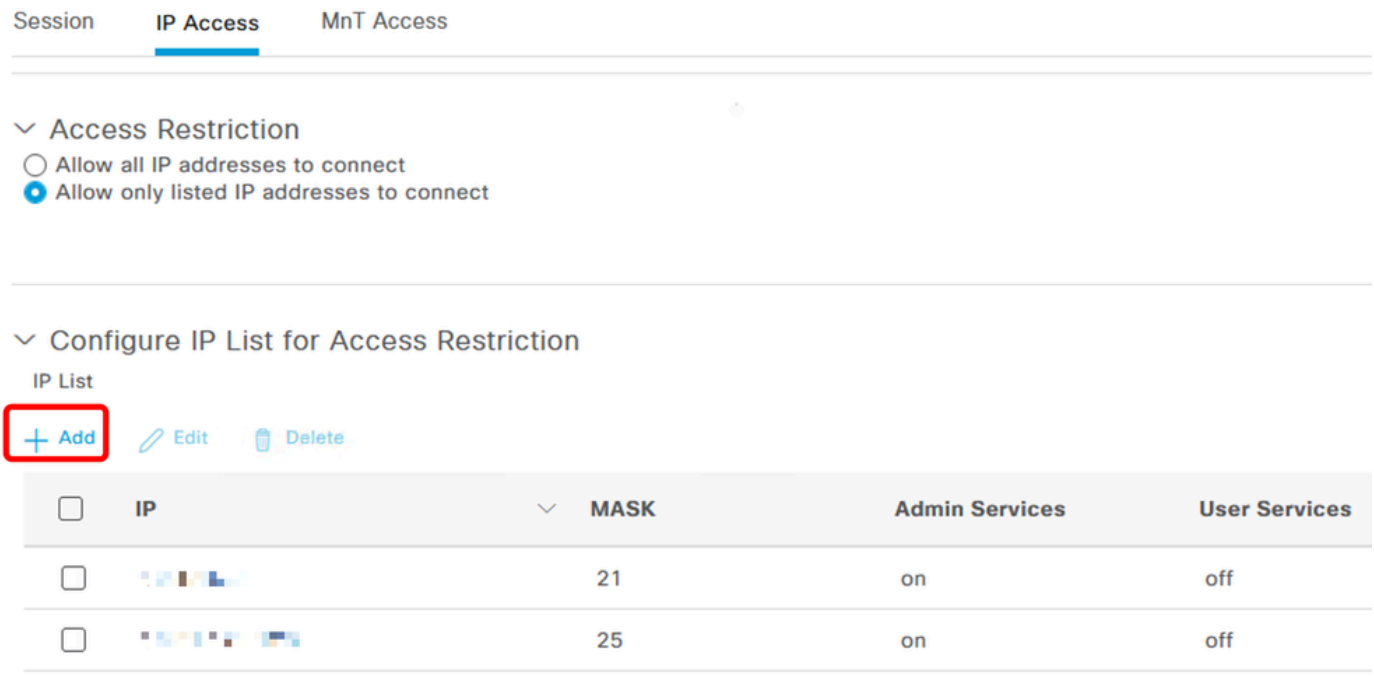
Comportamento in ISE 3.2

Passare a Sono Administration > Admin Access > Settings > Access. disponibili le seguenti opzioni:

- Sessione
- Accesso IP
- Accesso MnT

Configurazione

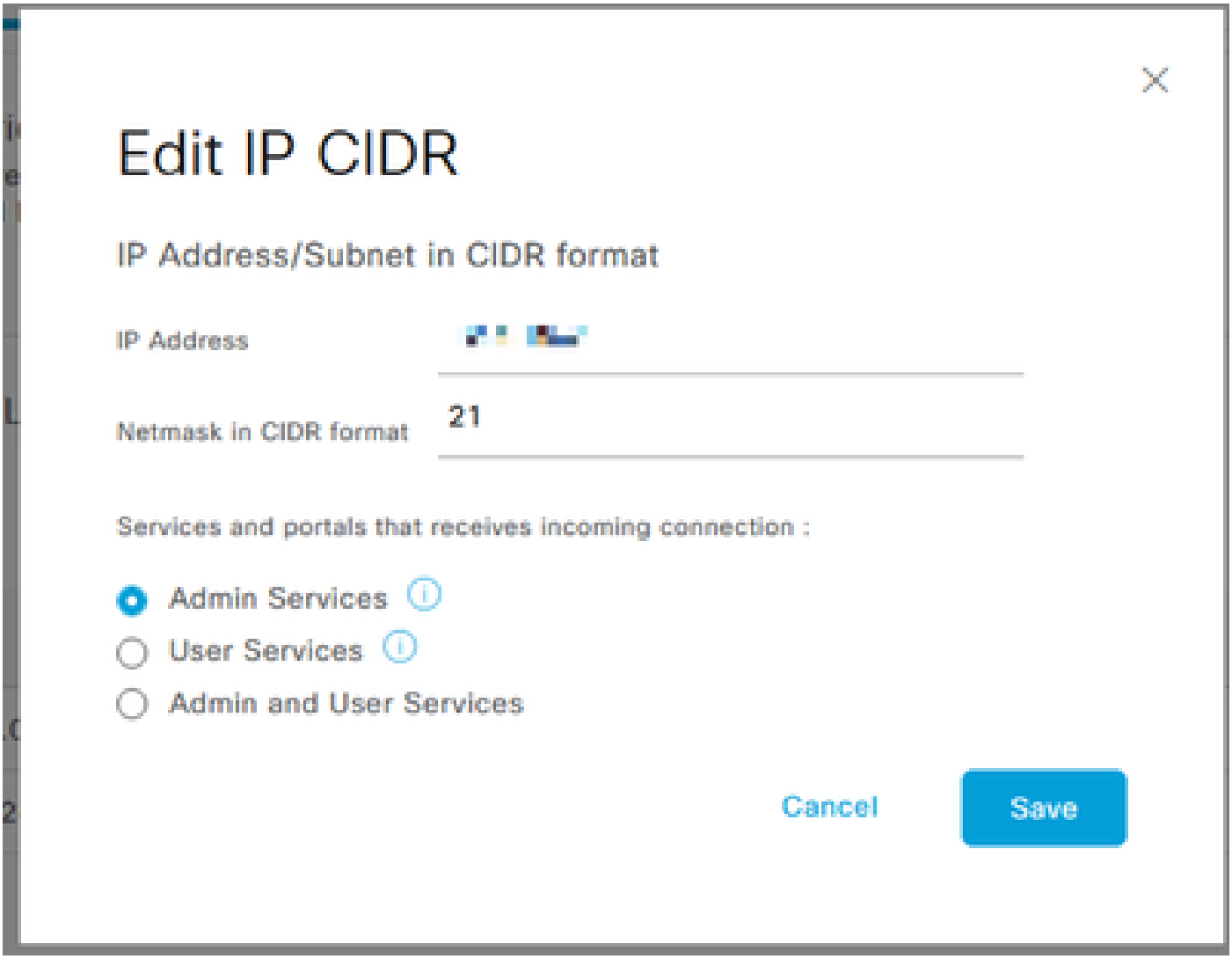
- Seleziona **Allow only listed IP addresses to connect**.
- Fare clic su .Add



Configurazione dell'accesso IP

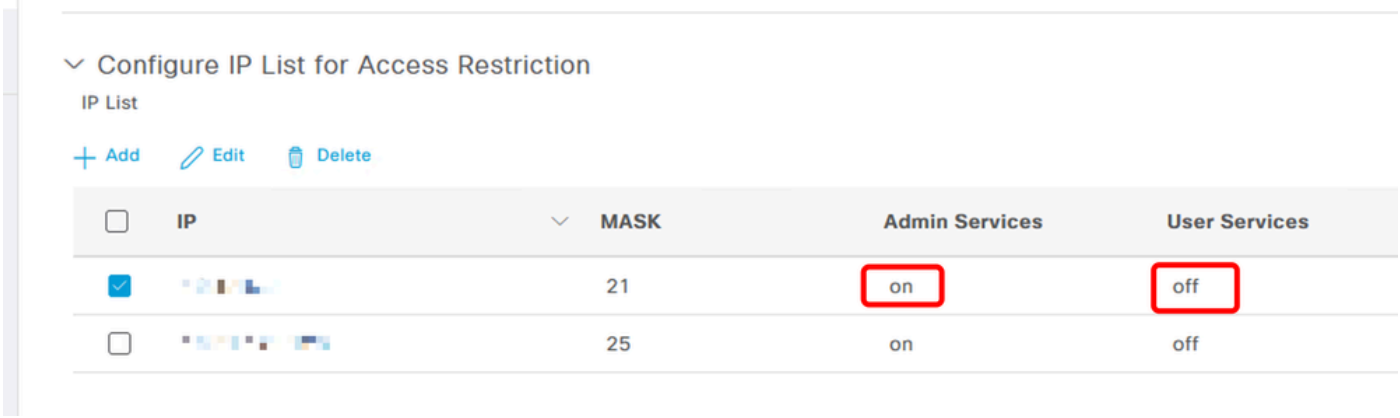
- Verrà visualizzata una finestra di dialogo in cui è possibile immettere gli indirizzi IP, IPv4 o IPv6, in formato CIDR.
- Una volta configurato l'IP, impostare la maschera in formato CIDR.
- Le seguenti opzioni sono disponibili per le restrizioni di accesso IP:

- Servizi di amministrazione: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (disabilitato nella patch 2), MnT Analytics
- Servizi utente: Guest, BYOD, Postura, Profiling
- Servizi per l'amministratore e gli utenti



Modifica CIDR IP

- Fare clic sul Save pulsante.
- ON indica che i servizi di amministrazione sono abilitati, OFF indica che i servizi utente sono disabilitati.

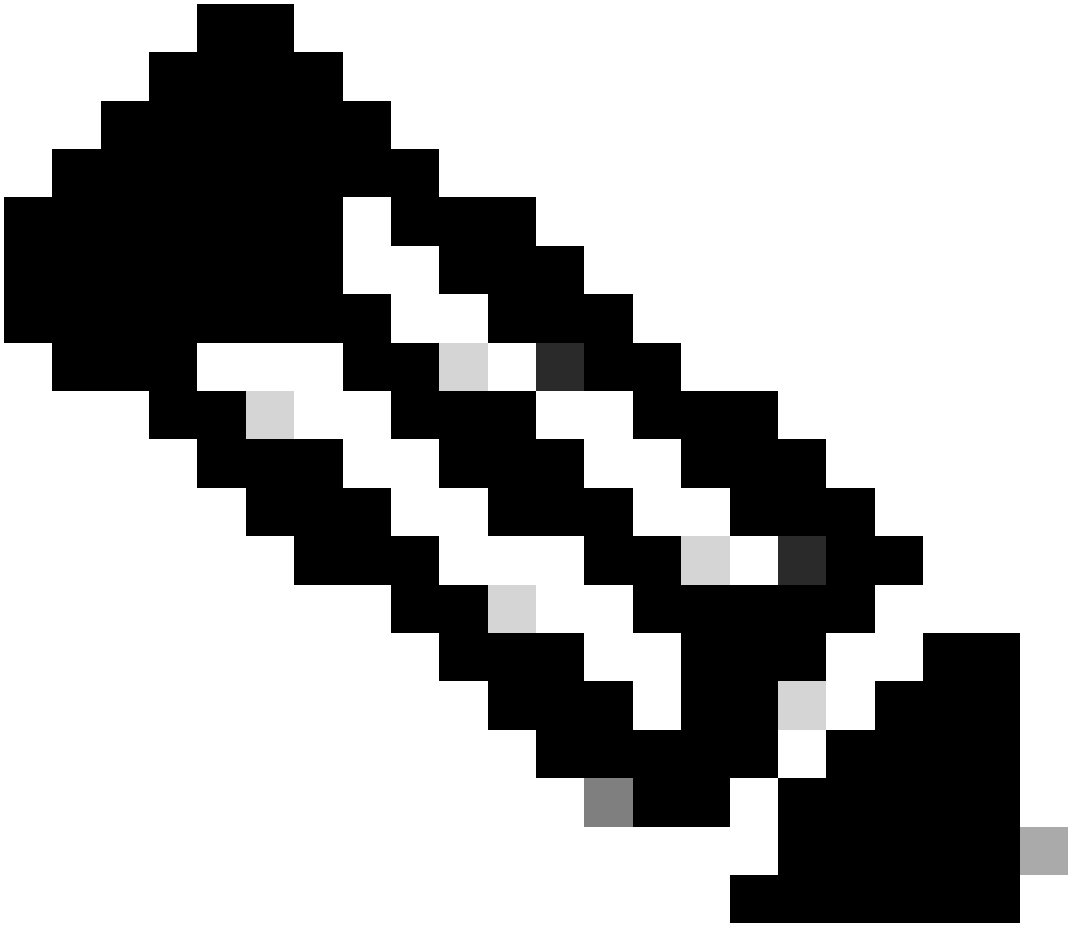


Configurazione dell'accesso IP in 3.2

Caratteristiche di ISE 3.2 P4 e successive

Passare a Administration > Admin Access > Settings > Access . Sono disponibili le seguenti opzioni:

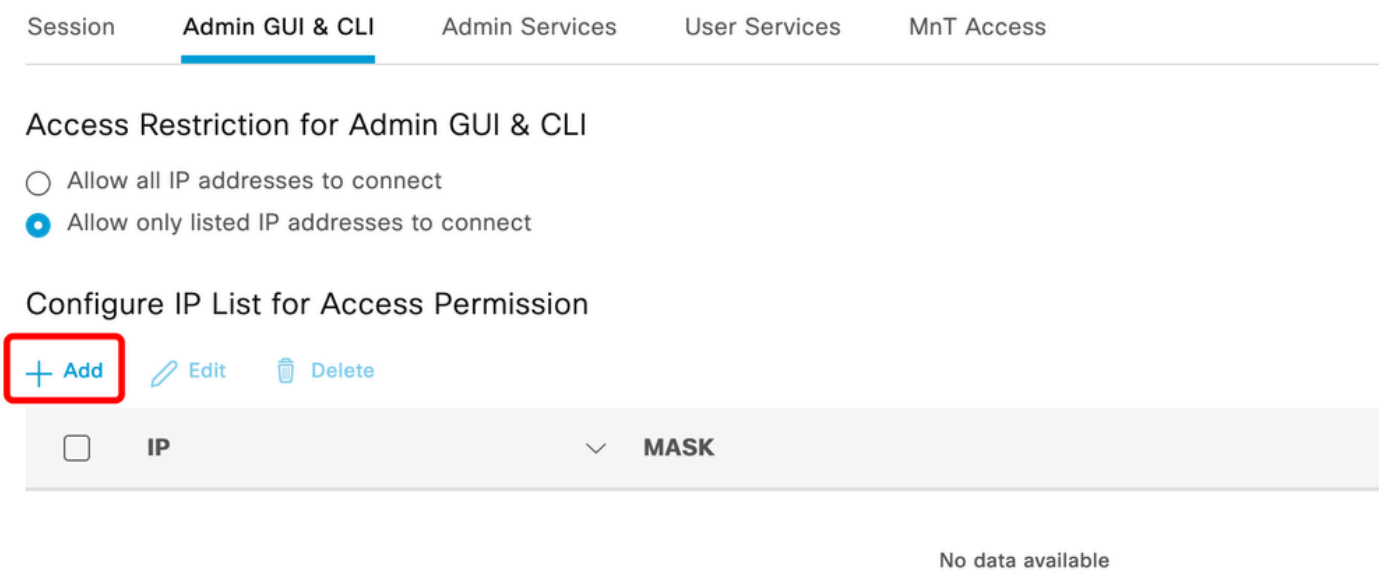
- Sessione
- GUI e CLI di amministrazione: ISE GUI (TCP 443), ISE CLI (SSH TCP22) e SNMP.
- Servizi di amministrazione: API ERS, Open API, pxGrid, DataConnect.
- Servizi per gli utenti: Guest, BYOD, Posture.
- Accesso MNT: Con questa opzione, ISE non utilizza i messaggi Syslog inviati da fonti esterne.



Nota: la restrizione di accesso a pxGrid e Data Connect è valida per ISE 3.3+, ma non per ISE 3.2 P4+.

Configurazione

- Seleziona Allow only listed IP addresses to connect.
- Fare clic su **Add**.



Configurazione dell'accesso IP in 3.3

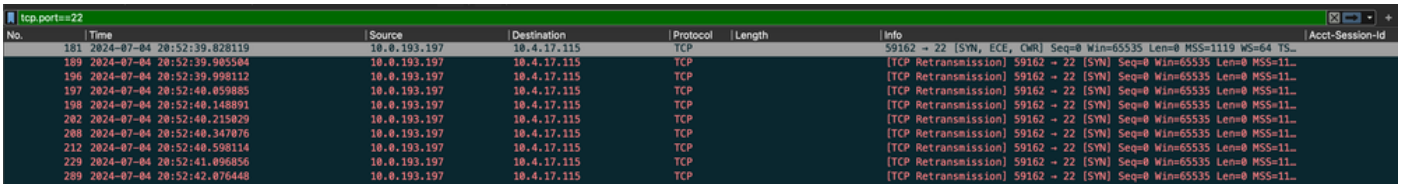
- Verrà visualizzata una finestra di dialogo in cui è possibile immettere gli indirizzi IP, IPv4 o IPv6, in formato CIDR.
- Una volta configurato l'IP, impostare la maschera in formato CIDR.
- Fare clic su .Add

Ripristino della GUI/CLI di ISE

- Accedere con la console.
- Arrestare i servizi ISE utilizzando application stop ise
- Avviare i servizi ISE utilizzando application start ise safe
- Rimuovere la restrizione di accesso IP dalla GUI.

Risoluzione dei problemi

Eseguire l'acquisizione di un pacchetto per verificare se ISE non risponde o se sta eliminando il traffico.



Verifica le regole di ISE Firewall

- Per la versione 3.1 e precedenti, è possibile controllare questa opzione solo nel programma show tech.

    - Puoi prendere uno show tech e memorizzarlo sul disco locale usando show tech-support file <filename>

        - È quindi possibile trasferire il file in un repository utilizzando copy disk:/<filename> ftp://<ip_address>/path. L'URL del repository cambia a seconda del tipo di repository utilizzato.
        - È possibile scaricare il file nel computer in modo da poterlo leggere e cercare **Running iptables -nvL**.
        - Le regole iniziali nello show tech non sono incluse qui. In altre parole, qui è possibile trovare le ultime regole aggiunte alla funzione di restrizione 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
```

- Per la versione 3.2 e successive è possibile utilizzare il comando show firewall per controllare le regole del firewall.
- La versione 3.2 e successive offrono un maggiore controllo sui servizi che vengono bloccati dalla restrizione di accesso 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

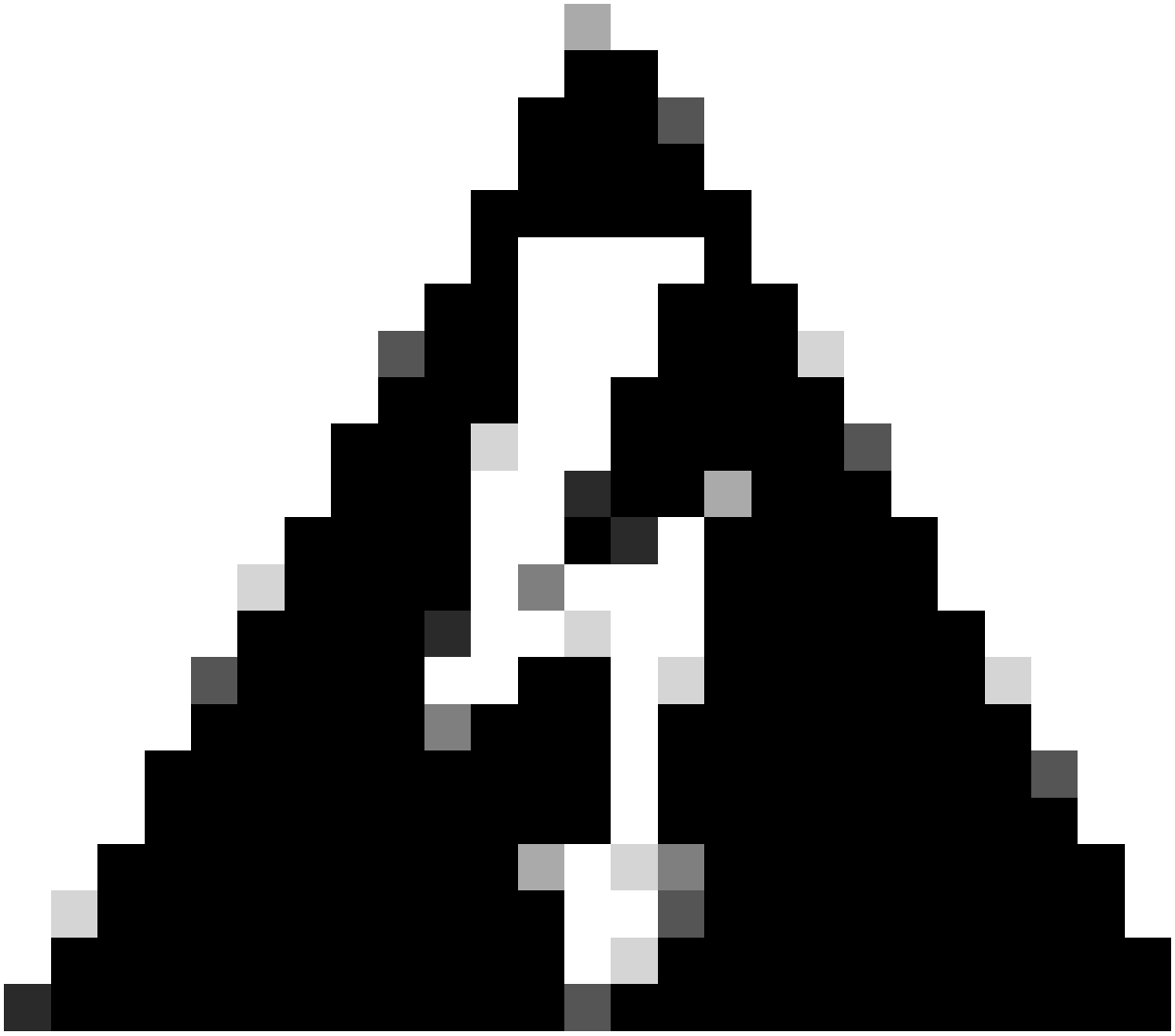
Chain ACCEPT_8910_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8910 Firewall rule permitting the PxGrid traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
90 5400 DROP all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

Controllo dei log di debug



Avviso: non tutto il traffico genera registri. La restrizione di accesso IP può bloccare il traffico a livello di applicazione e utilizzando il firewall interno di Linux. SNMP, CLI e SSH sono bloccati a livello di firewall, quindi non viene generato alcun log.

- Abilitare il DEBUG dei Infrastructure componenti dalla GUI.
- Abilitare il **Admin-infra** componente per il DEBUG dalla GUI.
- Abilitare il **NSF** componente per il DEBUG dalla GUI.
- Utilizzare il comando show logging application ise-psc.log tail.

Le voci del log di esempio possono essere visualizzate quando l'accesso webUI dell'amministratore ISE è limitato, dove la subnet consentita è 198.18.133.0/24, mentre l'accesso dell'amministratore ISE è limitato da 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
```

Informazioni correlate

- Guida per l'amministratore di ISE 3.1
- Guida per l'amministratore di ISE 3.2
- Guida per l'amministratore di ISE 3.3
- Supporto tecnico Cisco e download

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).