

# Risoluzione dei problemi relativi all'integrazione con ISE

## Sommario

---

[Introduzione](#)

[Panoramica delle procedure ottimali](#)

[CCV-ISE - Diagramma di flusso ad alto livello](#)

[Linee guida per la risoluzione dei problemi](#)

[Dati da raccogliere](#)

[Messaggi di log previsti](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'integrazione di CyberVision Center con ISE.

## Panoramica delle procedure ottimali

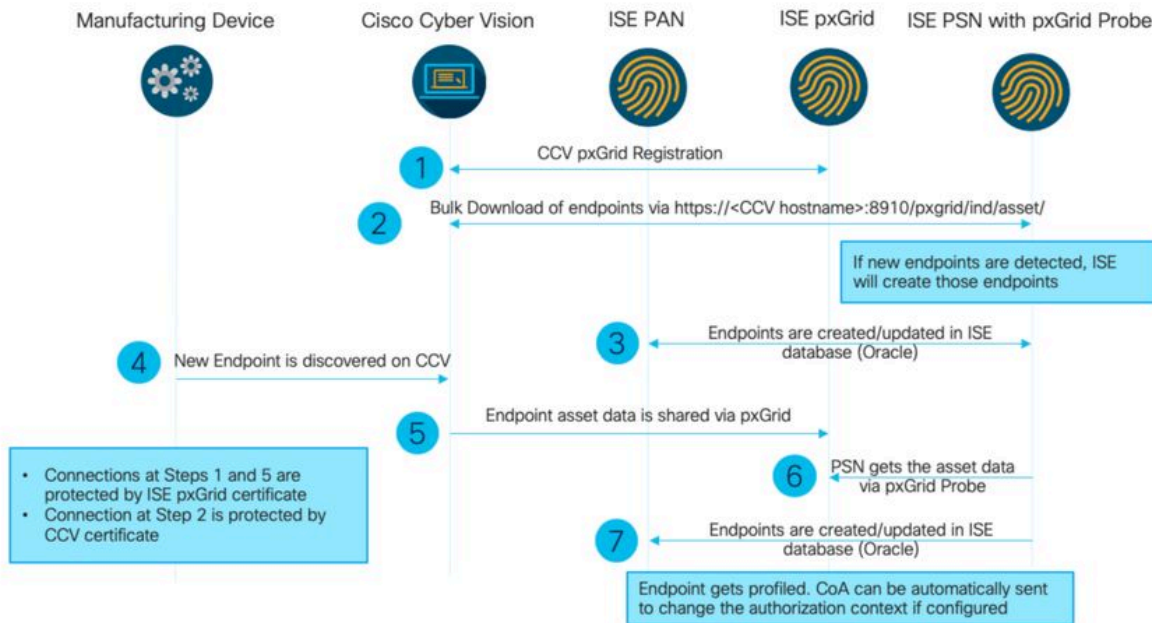
Le procedure ottimali sono i passi consigliati che è necessario prendere in considerazione per garantire il corretto funzionamento della configurazione del sistema. Consigli:

- Per le funzionalità, le linee guida, le limitazioni e le avvertenze più recenti, consultare le note di rilascio di Cisco Cyber Vision e le note di rilascio di Cisco Identity Services Engine (ISE)
- Verifica e risoluzione dei problemi relativi alle nuove modifiche alla configurazione dopo l'implementazione

## Diagramma di flusso ad alto livello CCV-ISE

## Configure

### High-Level Flow Diagram



## Linee guida per la risoluzione dei problemi

Rispondendo alle domande successive, è possibile determinare il percorso per la risoluzione dei problemi e i componenti che richiedono un'ulteriore analisi. Rispondere alle domande successive per determinare lo stato dell'installazione:

- Si tratta di un sistema appena installato o di un'installazione esistente?
- CyberVision ha mai visto l'ISE?

Controllare lo stato dei servizi di pxGrid utilizzando il comando `systemctl status pxgrid-agent`.

```
root@center:~# systemctl status pxgrid-agent
● pxgrid-agent.service - Agent for interfacing with pxGrid
   Loaded: loaded (/lib/systemd/system/pxgrid-agent.service; enabled)
   Active: active (running) since Wed 2021-03-17 20:12:15 UTC; 17min ago
     Process: 28434 ExecStop=/usr/bin/lxc-stop -n pxgrid-agent (code=exited, status=0/SUCCESS)
    Main PID: 28447 (lxc-start)
      CGroup: /system.slice/pxgrid-agent.service
              └─28447 /usr/bin/lxc-start -F -n pxgrid-agent

Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: create_path_for_hierarchy: 1306 Path "/sys/fs/cgroup/pids//lxc/pxgrid-agent-6" already existed.
Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: cgfsng_create: 1363 File exists - Failed to create /sys/fs/cgroup/pids//lxc/pxgrid-agent-6: File exists
Mar 17 20:12:15 center lxc-start[28447]: pxgrid-agent Center type: standalone [caller=postgres.go:290]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [caller=main.go:135]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock' [caller=main.go:102]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Account activated [caller=pxgrid.go:81]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Service registered, ID: 3d7bee0f-3840-4dc7-a121-a8740f86fa06 [caller=pxgrid.go:99]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent Cyber Vision is in sync with ISE [caller=assets.go:67]
Mar 17 20:23:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
```

- ISE esegue pxGrid in ambienti ad alta disponibilità?
- Che cosa è cambiato nella configurazione o nell'infrastruttura complessiva immediatamente prima che le applicazioni iniziassero ad avere problemi?

Per individuare un problema di rete, eseguire le operazioni generali di risoluzione dei problemi di rete:

Passaggio 1. È possibile eseguire il ping tra CyberVision Center Hostname e ISE?

```

ESCISE2/admin# ping center
PING center (10.2.3.138) 56(84) bytes of data.
64 bytes from 10.2.3.138: icmp_seq=1 ttl=64 time=1.53 ms
64 bytes from 10.2.3.138: icmp_seq=2 ttl=64 time=1.73 ms
64 bytes from 10.2.3.138: icmp_seq=3 ttl=64 time=1.87 ms
64 bytes from 10.2.3.138: icmp_seq=4 ttl=64 time=1.80 ms

--- center ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.539/1.737/1.878/0.125 ms

```

Se non è possibile eseguire il ping, connettersi a ISE CLI usando Secure Shell (SSH) e aggiungere il nome host.

```

ESCISE2/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ESCISE2/admin(config)# ip host 10.2.3.138 center
Add Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes

```

Passaggio 2. È possibile eseguire il ping tra ISE Hostname e CyberVision Center?

```

root@center:~# ping ESCISE2.ccv.local
PING ESCISE2.ccv.local (10.2.3.118) 56(84) bytes of data.
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=1 ttl=64 time=2.04 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=2 ttl=64 time=1.88 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=3 ttl=64 time=1.75 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=4 ttl=64 time=1.98 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=5 ttl=64 time=2.02 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=6 ttl=64 time=1.97 ms
^C
--- ESCISE2.ccv.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.754/1.945/2.045/0.109 ms

```

In caso contrario, provare ad aggiungere il nome host ISE al /data/etc/hosts file in Center.

```

root@Center:~# cat /data/etc/hosts
127.0.0.1        localhost.localdomain        localhost

# The following lines are desirable for IPv6 capable hosts
::1            localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.1.1 center
10.48.60.131 ise31-tm2.cisco.com

```

Passaggio 3. Individuazione dei problemi relativi ai certificati.

Immettere il comando `openssl s_client -connect YourISEHostname:8910` da CyberVision Center.

```
root@center:~# openssl s_client -connect ESCISE2.ccv.local:8910
CONNECTED(00000003)
depth=3 CN = Certificate Services Root CA - ESCISE2
verify error:num=19:self signed certificate in certificate chain
verify return:1
depth=3 CN = Certificate Services Root CA - ESCISE2
verify return:1
depth=2 CN = Certificate Services Node CA - ESCISE2
verify return:1
depth=1 CN = Certificate Services Endpoint Sub CA - ESCISE2
verify return:1
depth=0 OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
verify return:1
```

---
Certificate chain

```
0 s:OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
  i:CN = Certificate Services Endpoint Sub CA - ESCISE2
1 s:CN = Certificate Services Endpoint Sub CA - ESCISE2
  i:CN = Certificate Services Node CA - ESCISE2
2 s:CN = Certificate Services Node CA - ESCISE2
  i:CN = Certificate Services Root CA - ESCISE2
3 s:CN = Certificate Services Root CA - ESCISE2
  i:CN = Certificate Services Root CA - ESCISE2
```

Server certificate

-----BEGIN CERTIFICATE-----

```
MIIF3jCCA8agAwIBAgIQUKVBBihpQhWBK5cZEJFpeDANBqkqhkiG9w0BAQsFADA5
MTcwNQYDVQQDDDC5DZXJ0aWZpY2F0ZSBVTXJ2aWNlcyBFbmRwb2ludCBTdWl0eGQ0Eg
LSBFU0NlU0UyMB4XDTEwMTEyMTEzMDEwMTcwTjEwMjE2MDEzMDEwMTcwTjEwMjE2
A1UECwwnQ2VydG1maWNhdGUuU2VydmljZXMgU3lzdGVtIENlcnRzZmljYXRlMR0w
GAYDVQQDBBFU0NlU0UyLmNjdjdi5sb2NhbDCCAiIwdQYJKoZIhvcNAQEBBQADggIP
ADCCAg0CggIBANE1Ukx/7QnUdrCIXJLUXg0XWTV0FTNme4L16yDFsLvytGjFqYfR
RCRM/kzRVjDk8f/cSSP9T+5pR/JA+PbOZqkAWWDJVAqH1ndqL0kX7UaCCodKUWon
DafVimPjKqV1RSCd8bwVDxAr7gYou3S4BcCe00s1x5pL1WyZw6F6MPze2F388kSR
GuSRsn40ZM4JjDDeaxSBrs789f7zACw4eMZIfRDk0RL9qzMtoghIU089/1VuacUb
WYrF0e0mThUWg7wk7dFv4bozyWeHjdqsbEt0Geme8ZWPX5ZYddSKjWhOrNUXeQV
NvDBUXhb5NpSsKYMocqnvIv+JYzkIV6ukksX9xqI5bL3/vik/CyPVMexIOJo64dK
S0vmjrcnmpNznoLzEv3mgvgp9mJhcTROg86wlyOrOzjOoMCGGLrhpgxuLeVatFKv
GLWjsmrWcLk/FOAe4H+tb6/+yO7KNXTSX+nP1z5epDA8stzvLxm1ylw65XdeEBho
m0qgGEKr5y/I/2b+myi24ZYrqsV64KpohCisIvZxbCG/2q77SP7ml8v8+BidpMaW
Lzr20tD2XRJeyhPypRBYwV4QDBWPn+mCAFgpNd3KC36zAn138c2WW1Hs0PKhReMX
vNn+SwtKmyIbM09Oeww5zRSdMU90zPcFkY0qvrBUD31Gf5fAiWqlmkVAgMBAAGj
gcwgckwaAYDVR0jBGEwX4AUxz+SV+KtR/CpwGiyNg+mp/xxiAqhNaQzMDExLzAt
BgNVBAMMJkNlcnRzZmljYXRlIFNlcnRzZmljYXRlIE5vZGUgQ0EgLSBFU0NlU0Uy
ghAx1cB30YJL0Kwj6XolaV7SMB0GA1UdDgQWBRRigvgT63FOqKmS9m9COhW3ahdv8jAO
BgNVHQ8BAf8EBAMCBeAwIAYDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMC
MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggIBADwnDKtdHj/y3Pj4ADDV
57RrdHsiU/EkkWGLzmp/aMKJ9rY7f6eUDlig6b6gpJ8B0MnTPi9VfVduc++oZDEt
CrIMMwFexnbnhPWJfzjSNJPnAMIgFUeiPuoxBJYkjFzhiXtat0fOmdm5RbEu5W1a
f7EEBd/XOIRTMyIxqubXQCT6pE61y9gBPuQU9Hvd5QpcLX77LSfEroJhkD4dmuRs
o4uj0wWKFtXW+yLWhwjkiieoBuREEU8Gvtk+iq+11mThfpeP32fV2IO/WIo4SKh0
ILkzS206rbSxxatKDQ6jZds3a5YKyFtR55r7VndmX0I4sqXI9dFQjTPVfW7TEbK
GPds+vMe4J9g4c1KGRhiXNiNzfbS5S3eWzOL/2o9ZgWS1u7R7GVXK1YrvSHMieL3t
n/p+ov8cogr00o6jXFItZ+Rsnp11Kbq+DrsoCE/i26QgkTKBruMfhz6P8k/2aLqQ
MwJp0dhH1SFmkWCAQbGQpapoX3lpK36FUta3sZL2mdN/XyK5UutLbLJx87elwunp
w6Cxz5MA97NXOUZIUqThnTG7Ibu8pzw11XZyt1f1T50luCoY2CkVbU93rqfD4zyr
WyK2a0BmizcKXD+F8Yti4fm4Kv10bpWihUNPPMTmgwJMUOW+zdC7b7g13j5rnE9X
lyFJ3uHTohidxEtXi4XsiCn5
```

-----END CERTIFICATE-----

subject=OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local

Dati da raccogliere

Per i problemi di rete:

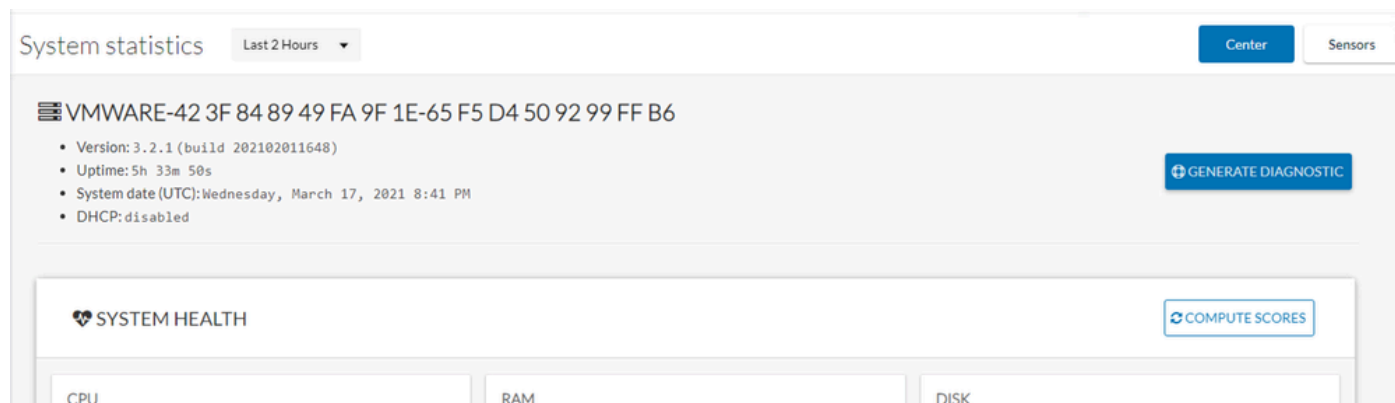
- Architettura:

Uno schema che mostra questi dettagli tra il centro e ISE è utile:

- Regole firewall
- Route statiche
- Configurazione del gateway
- Configurazioni VLAN

- Log da raccogliere per tutti i problemi ISE:

È possibile iniziare raccogliendo un file di diagnostica di Center per evitare la perdita di dati.



System statistics Last 2 Hours ▾ Center Sensors

VMWARE-42 3F 84 89 49 FA 9F 1E-65 F5 D4 50 92 99 FF B6

- Version: 3.2.1 (build 202102011648)
- Uptime: 5h 33m 50s
- System date (UTC): Wednesday, March 17, 2021 8:41 PM
- DHCP: disabled

GENERATE DIAGNOSTIC

SYSTEM HEALTH COMPUTE SCORES

CPU RAM DISK

Quindi attivare i log avanzati sul centro utilizzando la seguente procedura:

Creare due file nella cartella /data/etc/sbs.

Il primo file deve avere un nome listener.conf e contenere il contenuto:

Notare lo spazio iniziale davanti al livello di log.

```
root@Center:~# cat /data/etc/sbs/listener.conf
configlog:
 loglevel: debug
root@Center:~#
```

Il secondo file deve essere denominato pxgrid-agent.conf e contenere il contenuto:

Notare lo spazio iniziale davanti al livello di log.

```
root@Center:~# cat /data/etc/sbs/pxgrid-agent.conf
configlog:
 loglevel: debug
```

Una volta creati entrambi i file, riavviare il Centro o i servizi sbs-burrow epxgrid-agent.

Restart service using the command:

```
#systemctl restart sbs-burrow
#systemctl restart pxgrid-agent
```

Raccogliere quindi i log di pxGrid (utilizzare gli strumenti di trasferimento dei file per esportare i log dal centro).

```
root@Center:~# journalctl -u pxgrid-agent > /data/tmp/pxgridLogs.log
```

Raccogliere le clip tcpdump per analizzare il flusso di comunicazione tra il Center e ISE.

```
root@Center:~# tcpdump -i eth0 -n host CCV_IP and host ISE_IP -w /data/tmp/ccv_ise.pcap
```

- Abilitare Debug su ISE e raccogliere il bundle di supporto.

Per abilitare i debug su ISE, selezionare Administration > System > Logging > Debug Log Configuration. Impostare i seguenti livelli di log:

Persona	Nome componente	Livello log	File da controllare	
PAN (opzionale)	profiler	DEBUG	profiler.log	
PSN con probe pxGrid abilitato	profiler	DEBUG	profiler.log	

PxGrid	pxgrid	TRACCIA	pxgrid-server.log	
--------	--------	---------	-------------------	--

Messaggi di log previsti

I log di debug dell'agente pxGrid al centro mostrano l'agente che viene avviato, il servizio registrato, Cisco Cyber Vision (CCV) che stabilisce una connessione STOMP (Text Oriented Messaging Protocol) semplice (o streaming) con ISE e invia un'operazione di aggiornamento per un asset/componente:

<#root>

Jul 11 13:05:02 center systemd[1]:

**Started Agent**

for interfacing with pxGrid.

```
Jul 11 13:05:02 center pxgrid-agent[5404]: pxgrid-agent Center type: standalone [caller=postgres.go:543]
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock'
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccountActivate body=
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent
```

**Account activated**

[caller=pxgrid.go:58]

```
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceRegister body=
```

"assetTopic":"/topic/com.cisco.endpoint.asset"

, "restBaseUrl": "https://Center:8910/"

```
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent
```

**Service registered**

, ID: c514c790-2361-47b5-976d-4a1b5ccfa8b7 [caller=pxgrid.go:76]

```
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceLookup body=
Jul 11 13:05:05 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccessSecret body=
Jul 11 13:05:06 center pxgrid-agent[5404]: pxgrid-agent
```

**Websocket connect url**

=wss://labise.aaalab.com:

8910

/pxgrid/ise/pubsub [caller=endpoint.go:129]

```
Jul 11 13:05:07 center pxgrid-agent[5404]: pxgrid-agent
```

**STOMP CONNECT host**

=10.48.78.177 [caller=endpoint.go:138]

```
Jul 11 13:06:59 center pxgrid-agent[5404]: pxgrid-agent
```

**STOMP SEND destination**

=/topic/com.cisco.endpoint.asset body={

"opType": "UPDATE"

, "asset": {"assetId": "01:80:c2:00:00:00", "assetName": "LLDP/STP bridges Multicast 0:0:0", "assetIpAddress"}



Jul 11 13:10:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceReregister

Il formato del messaggio previsto dopo l'integrazione riuscita e l'attributo assetGroup viene pubblicato senza un valore, come mostrato di seguito:

<#root>

Jan 25 11:05:49 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endpoint.asset body={"opType":"UPDATE","a

```
{"key": "assetGroup", "value": ""}
```

```
, {"key": "assetCustomName", "value": "test"}, {"key": "assetGroupPath", "value": ""}], "assetConnectedLinks": []
```

Formato previsto del messaggio (assetGroup con un valore, come mostrato). Ciò conferma che CyberVision Center sta inviando gli attributi e se la stessa condizione non viene riflessa ulteriormente sul lato ISE, è necessario indagare ulteriormente con ISE.

<#root>

Jan 25 11:09:28 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endpoint.asset body={"opType":"UPDATE","a

```
{"key": "assetGroup", "value": "test group"}
```

```
, {"key": "assetCustomName", "value": "test"}, {"key": "assetGroupPath", "value": "test group"}], "assetConnecte
```

Informazioni correlate

- [Solution Brief su CCV e ISE](#)
- [Demo Lab: Uso di Cisco Cyber Vision per fornire una microsegmentazione dinamica con Cisco ISE](#)
- [Demo ISE e CCV](#)
- [Guida all'integrazione ISE](#)
- [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).