Errore di aggiornamento download automatico in un centro di gestione Firepower

Sommario

Introduzione

In questo documento vengono illustrati i motivi per cui un'attività pianificata per l'aggiornamento di un Centro gestione Cisco Firepower potrebbe non riuscire. È possibile aggiornare Cisco Firepower Management Center manualmente o automaticamente. Per eseguire un aggiornamento software automatico, è possibile creare un'attività di pianificazione sul centro di gestione per l'esecuzione in un momento successivo.

Possibili cause dell'errore

Un centro Firepower Management potrebbe non riuscire a scaricare un file di aggiornamento dall'infrastruttura Cisco Download Update quando nella rete si verifica una delle seguenti azioni:

- I criteri di sicurezza della società bloccano il traffico DNS (Domain Name System).
- La configurazione esterna al centro di gestione influisce sul download. Ad esempio, una regola del firewall può consentire un solo indirizzo IP per support.sourcefire.com.

  Attenzione: Cisco utilizza il DNS round robin per il bilanciamento del carico, la tolleranza di errore e l'uptime. È pertanto possibile che gli indirizzi IP dei server DNS vengano modificati.

Conseguenze

Se Si Utilizza Questo Metodo...	Azione
Configurazione predefinita di sistema per il download automatico	Nessuna azione richiesta
Scaricare il file di aggiornamento manualmente e caricarlo in Firepower Management Center	Nessuna azione richiesta
Regole del firewall per filtrare l'accesso all'infrastruttura di aggiornamento download gestita da Cisco	Segui la soluzio

- Gli errori vengono parzialmente risolti dai tre tentativi e dalla successiva esecuzione pianificata. I guasti ripetuti possono indicare un fattore esterno, ad esempio un firewall, o

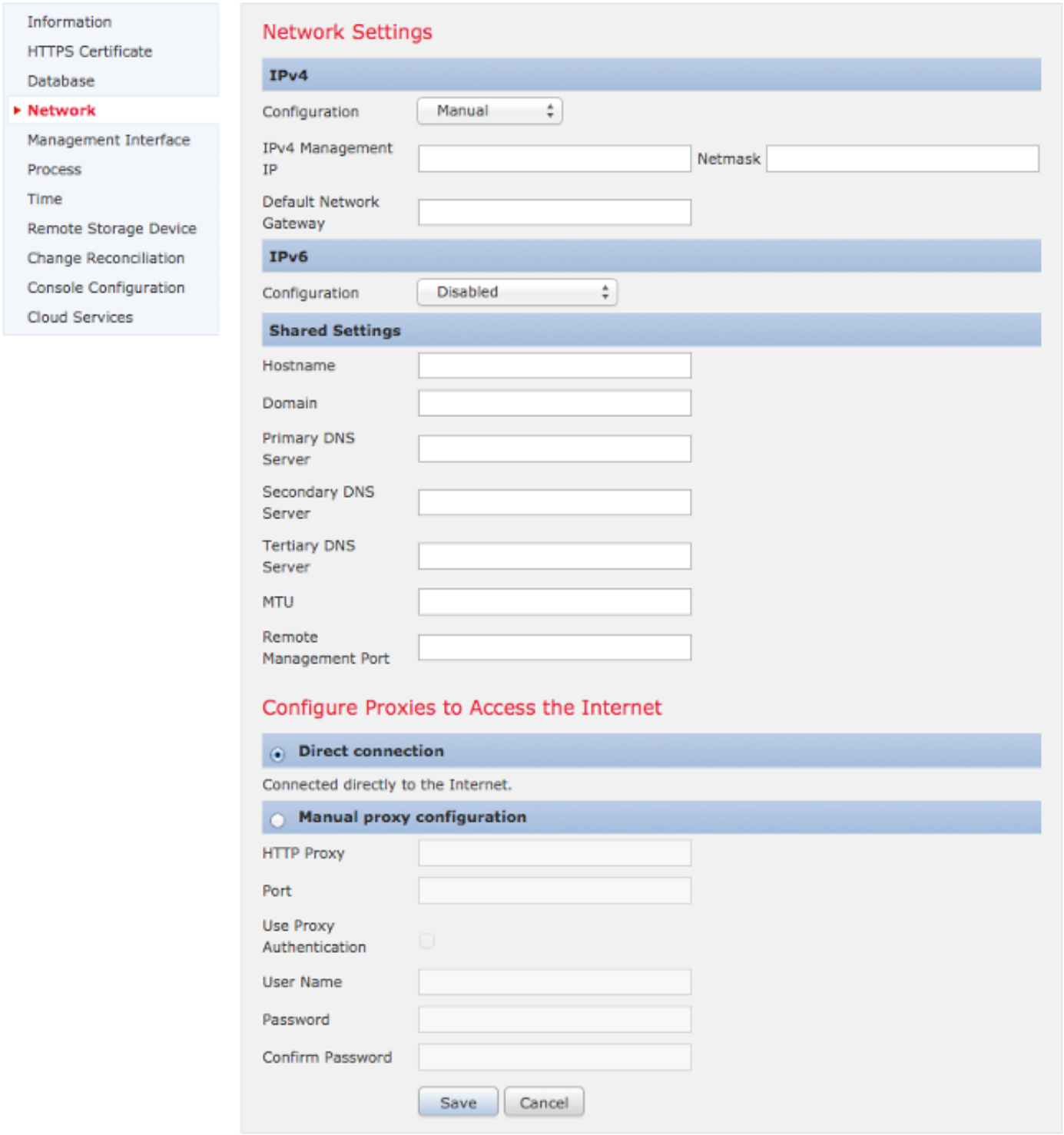
un'interruzione dell'alimentazione con l'infrastruttura.
- Poiché il DNS round robin è incluso nel nome di dominio, è necessario adottare le misure necessarie per garantire che non si verifichino errori di download intermittenti.

Verifica

Verifica impostazioni DNS

Verificare che Firepower Management Center sia configurato per l'utilizzo del server DNS.

> **Attenzione:** Cisco consiglia di mantenere le impostazioni predefinite.



Èpossibile configurare le impostazioni DNS in **Sistema > Locale > Configurazione**, nella sezione **Rete**. Nella sezione **Impostazioni condivise** è possibile specificare fino a tre server DNS.

> **Nota:** Se è stato selezionato **DHCP** nell'elenco a discesa **Configuration** (Configurazione), non è possibile specificare manualmente le **impostazioni condivise**.

Verifica connessione

Èpossibile utilizzare vari comandi, ad esempio telnet, nslookup o dig per determinare lo stato del server DNS e le impostazioni DNS nel centro di gestione Firepower. Ad esempio:

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

> **Nota:** Il ping su support.sourcefire.com non funziona. Pertanto, non deve essere utilizzato come test di connettività.

Per verificare la connessione al sito di supporto da un accessorio (per scaricare gli aggiornamenti, ecc.), è possibile accedere all'accessorio tramite SSH o l'accesso diretto alla console e usare questo comando:

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

Questo comando mostra la negoziazione dei certificati e fornisce un equivalente di una sessione telnet a un server Web della porta 80. Di seguito è riportato un esempio dell'output del comando:

```
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 44A18130176C9171F50F33A367B55F5CFD10AA0FE87F9C5C1D8A7A7E519C695B
Session-ID-ctx:
Master-Key:
D406C5944B9462F1D6CB15D370E884B96B82049300D50E74F9B8332F84786F05C35BF3FD806672630BE26C2218AE5BDE
Key-Arg : None
Start Time: 1398171146
Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

A questo punto non dovrebbe esserci alcuna richiesta. Tuttavia, poiché la sessione è in attesa di input, è possibile immettere il comando:

```
GET /
```

Dovrebbe essere visualizzato codice HTML non elaborato, ovvero la pagina di accesso del sito di supporto.

Risoluzione dei problemi

Opzione 1: Sostituire l'indirizzo IP statico con il nome di dominio support.sourcefire.com nei firewall. Se è necessario utilizzare un indirizzo IP statico, verificare che sia corretto. Di seguito sono riportate informazioni dettagliate sul server di download utilizzato da un sistema Firepower:

- **Dominio**: support.sourcefire.com

- **Port:** 443/tcp (bidirezionale)
- **Indirizzo IP:** 50.19.123.95, 50.16.210.129

Gli indirizzi IP aggiuntivi utilizzati anche da support.sourcefire.com (metodo round robin) sono:

```
54.221.210.248
54.221.211.1
54.221.212.60
54.221.212.170
54.221.212.241
54.221.213.96
54.221.213.209
54.221.214.25
54.221.214.81
```

Opzione 2: È possibile scaricare gli aggiornamenti manualmente con un browser Web e quindi installarli manualmente durante l'intervento di manutenzione.

Opzione 3: Aggiungere un record A per support.sourcefire.com nel server DNS.

Documenti correlati

- Tipi di aggiornamenti che possono essere installati in un sistema Firepower
- Indirizzi server richiesti per le operazioni Advanced Malware Protection (AMP)
- Porte di comunicazione necessarie per il funzionamento del sistema Firepower
- Documentazione e supporto tecnico – Cisco Systems