Domande frequenti su Cisco FindIT Network Management

Obiettivo

Cisco FindIT Network Management è un software che consente di gestire facilmente l'intera rete, inclusi i dispositivi Cisco, tramite il browser Web. Individua, controlla e configura automaticamente tutti i dispositivi Cisco supportati nella rete. Il software invia inoltre notifiche relative agli aggiornamenti del firmware e alle informazioni sui dispositivi della rete non più supportati dalla garanzia.

Cisco FindIT Network Management ha due componenti separati: un singolo manager noto come FindIT Network Manager e una o più sonde note come FindIT Network Probe.

Questo articolo contiene le domande frequenti su configurazione, configurazione e risoluzione dei problemi di Cisco FindIT Network Management e le relative risposte.

Domande frequenti

Sommario

Accesso remoto

Aggiornamento software

Generale

1. Quali lingue sono supportate da FindIT Network Management?

FindIT Network Management è tradotto nelle seguenti lingue:

- Cinese
- Inglese
- Francese
- Tedesco
- Giapponese
- Spagnolo

Individuazione

2. Quali protocolli utilizza FindIT per gestire i dispositivi?

FindIT utilizza diversi protocolli per individuare e gestire la rete. Il protocollo esatto utilizzato per un determinato dispositivo varia a seconda del tipo di dispositivo. Tali protocolli includono:

- Multicast Domain Name System (mDNS) e individuazione servizio DNS: questo

protocollo è noto anche come Bonjour. Consente di individuare dispositivi quali stampanti, altri computer e i servizi offerti da tali dispositivi in una rete locale. Per ulteriori informazioni su mDNS, fare clic qui. Per ulteriori informazioni sull'individuazione dei servizi DNS, fare clic qui.

- Cisco Discovery Protocol (CDP): protocollo proprietario di Cisco utilizzato per condividere informazioni su altre apparecchiature Cisco a connessione diretta, come la versione del sistema operativo e l'indirizzo IP.
- LLDP (Link Layer Discovery Protocol): protocollo indipendente dal fornitore utilizzato per condividere informazioni su altre apparecchiature collegate direttamente, ad esempio la versione del sistema operativo e l'indirizzo IP.
- SNMP (Simple Network Management Protocol): protocollo di gestione di rete utilizzato per la raccolta di informazioni e la configurazione di dispositivi di rete quali server, stampanti, hub, switch e router in una rete IP (Internet Protocol).
- RESTCONF — Bozza di IETF (Internet Engineering Task Force) che descrive come mappare una specifica del linguaggio di modellazione dei dati YANG (Another Next Generation) a un'interfaccia RESTful. Per ulteriori informazioni, fare clic qui.

3. In che modo FindIT rileva la rete?

FindIT Network Probe crea un elenco iniziale di dispositivi nella rete dall'ascolto di annunci CDP, LLDP e mDNS. La sonda si connette quindi a ciascun dispositivo utilizzando un protocollo supportato e raccoglie informazioni aggiuntive quali tabelle adiacenti CDP e LLDP, tabelle indirizzi MAC (Media Access Control) ed elenchi di dispositivi associati. Queste informazioni vengono utilizzate per identificare ulteriori dispositivi nella rete e il processo si ripete finché non vengono individuati tutti i dispositivi.

4. FindIT esegue scansioni di rete?

FindIT non esegue una scansione attiva degli intervalli di indirizzi di rete. Utilizza una combinazione di monitoraggio passivo di alcuni protocolli di rete e interroga attivamente i dispositivi di rete per ottenere informazioni.

Gestione delle porte

5. Perché Gestione porte non visualizza le porte dello stack?

Le illustrazioni di Gestione porte sono basate sull'elenco di porte fornite dal dispositivo tramite i protocolli di gestione. In modalità stack, le porte sono considerate una connessione interna allo stack e il dispositivo non le include negli elenchi forniti tramite i protocolli di gestione.

Configurazione

6. Cosa succede quando viene individuato un nuovo dispositivo? La configurazione verrà modificata?

Le nuove periferiche verranno aggiunte al gruppo di periferiche predefinito. Se i profili di configurazione sono stati assegnati al gruppo di dispositivi predefinito, la configurazione verrà applicata anche ai nuovi dispositivi individuati.

7. Cosa succede quando si sposta un dispositivo da un gruppo di dispositivi a un altro?

Qualsiasi configurazione di VLAN (Virtual Local Area Network) o WLAN (Wireless Local Area Network) associata ai profili attualmente applicati al gruppo di dispositivi originale e non al nuovo gruppo di dispositivi verrà rimossa e la configurazione VLAN o WLAN associata ai profili applicati al nuovo gruppo e non al gruppo originale verrà aggiunta al dispositivo. Le impostazioni di configurazione del sistema verranno sovrascritte dai profili applicati al nuovo gruppo. Se per il nuovo gruppo non sono stati definiti profili di configurazione del sistema, la configurazione del sistema per il dispositivo non verrà modificata.

Considerazioni sulla sicurezza

[8. Quali intervalli di porte e protocolli sono richiesti da FindIT Network Manager?]

Nella tabella seguente sono riportati i protocolli e le porte utilizzati da FindIT Network Manager:

Port	Direzione	Protocollo	Utilizzo
TCP 22	In entrata	SSH	Accesso da riga di comando a Manager
TCP 80	In entrata	HTTP	Accesso Web a Manager. Reindirizzamento a un server Web protetto (porta 443)
TCP 443	In entrata	HTTPS	Accesso Web sicuro a Manager
TCP 1069	In entrata	NETCONF/TLS	Comunicazione tra Probe e Manager
TCP 9443	In entrata	HTTPS	Accesso remoto all'interfaccia utente probe
TCP 5000-5100	In entrata	Dipendente dal dispositivo	Accesso remoto ai dispositivi
UDP 53	In uscita	DNS	Risoluzione dei nomi di dominio
UDP 123	In uscita	NTP	Sincronizzazione ora
UDP 5353	In uscita	mDNS	Annunci del servizio DNS multicast alla rete locale per l'annuncio di Manager

[9. Quali intervalli di porte e protocolli sono richiesti da FindIT Network Probe?]

Nella tabella seguente vengono elencati i protocolli e le porte utilizzati da FindIT Network Probe:

Port	Direzione	Protocollo	Utilizzo
TCP 22	In entrata	SSH	Accesso della riga di comando al probe
TCP 80	In entrata	HTTP	Accesso Web a Manager. Reindirizzamento a un server Web protetto (porta 443)
TCP 443	In entrata	HTTPS	Accesso Web sicuro a Manager
UDP 5353	In entrata	mDNS	Annunci servizio DNS multicast dalla rete locale. Utilizzato per l'individuazione dei dispositivi.
TCP 1000-10100	In entrata	Dipendente dal dispositivo	Accesso remoto ai dispositivi
UDP 53	In uscita	DNS	Risoluzione dei nomi di dominio
UDP 123	In uscita	NTP	Sincronizzazione ora

TCP 80	In uscita	HTTP	Gestione dei dispositivi senza servizi Web sicuri
UDP 161	In uscita	SNMP	Gestione dei dispositivi di rete
TCP 443	In uscita	HTTPS	Gestione dei dispositivi con servizi Web protetti abilitati. Accedi ai servizi Web Cisco per informazioni come aggiornamenti software, supporto, stato e notifiche di fine ciclo di vita
TCP 1069	In uscita	NETCONF/TLS	Comunicazione tra Probe e Manager
UDP 5353	In uscita	mDNS	Annunci del servizio DNS multicast alla rete locale che annunciano la sonda

10. Quanto è sicura la comunicazione tra FindIT Network Manager e FindIT Network Probe?

Tutte le comunicazioni tra Manager e la sonda vengono crittografate utilizzando una sessione TLS (Transport Layer Security) 1.2 autenticata con certificati client e server. La sessione viene avviata dalla sonda al manager. Quando viene stabilita l'associazione tra il manager e il probe, l'utente deve accedere al manager dal probe. A questo punto, il manager e il probe scambiano i certificati per autenticare le comunicazioni future.

11. FindIT ha accesso tramite 'backdoor' ai miei dispositivi?

No. Quando FindIT rileva un dispositivo Cisco supportato, tenterà di accedere al dispositivo utilizzando le credenziali predefinite di fabbrica per il dispositivo con il nome utente e la password predefiniti: cisco o la community SNMP predefinita: public. Se la configurazione del dispositivo è stata modificata rispetto a quella predefinita, sarà necessario che l'utente fornisca le credenziali corrette per FindIT.

12. Quanto sono sicure le credenziali archiviate in FindIT?

L'hash delle credenziali per l'accesso a FindIT viene eseguito in modo irreversibile utilizzando l'algoritmo SHA512. Le credenziali dei dispositivi e di altri servizi, ad esempio **Cisco Active Advisor**, vengono crittografate in modo reversibile utilizzando l'algoritmo AES-128.

13. Come è possibile recuperare una password persa per l'interfaccia utente grafica (GUI) di amministrazione?

Se si è persa la password di tutti gli account admin nell'interfaccia utente grafica di amministrazione, è possibile reimpostarla accedendo alla console di Probe o Manager ed eseguendo lo strumento **recoverpassword**. Questo strumento reimposta la password predefinita dell'account cisco o, se l'account cisco è stato rimosso, lo ricreerà con la password predefinita. Di seguito è riportato un esempio dei comandi da fornire per reimpostare la password utilizzando questo strumento.

```
cisco@FindITProbe:~# recoverpassword

Sei sicuro? (s/n) s

Reimposta l'account cisco sulla password predefinita
```

```
cisco@FindITProbe:~#
```

Accesso remoto

14. La sessione è sicura quando ci si connette alla GUI di amministrazione di un dispositivo da FindIT Network Management?

FindIT Network Management esegue il tunneling della sessione di accesso remoto tra il dispositivo e l'utente. Il protocollo utilizzato dipenderà dalla configurazione del dispositivo terminale, ma FindIT stabilirà sempre la sessione utilizzando un protocollo sicuro, se abilitato (ad esempio, HTTPS verrà preferito a HTTP). Se l'utente si connette al dispositivo tramite Manager, la sessione passerà attraverso un tunnel crittografato mentre passa da Manager alla sonda, indipendentemente dai protocolli abilitati sul dispositivo.

15. Perché la sessione di accesso remoto con un dispositivo si disconnette immediatamente quando si apre una sessione di accesso remoto su un altro dispositivo?

Quando si accede a un dispositivo tramite FindIT Network Management, il browser vede ogni connessione come se fosse con lo stesso server Web (FindIT) e quindi presenta cookie da ogni dispositivo a ogni altro dispositivo. Se più dispositivi utilizzano lo stesso nome cookie, è possibile che un cookie di dispositivo venga sovrascritto da un altro dispositivo. Ciò si verifica più spesso con i cookie di sessione e il risultato è che il cookie è valido solo per il dispositivo visitato più di recente. Tutti gli altri dispositivi che utilizzano lo stesso nome cookie vedranno il cookie come non valido e chiuderanno la sessione.

16. Perché la sessione di accesso remoto non riesce con un errore simile al seguente: Errore di accesso: Entità richiesta troppo grande. Il campo dell'intestazione HTTP supera le dimensioni supportate.

Dopo aver eseguito molte sessioni di accesso remoto con dispositivi diversi, il browser avrà un gran numero di cookie memorizzati per il dominio Probe. Per risolvere il problema, utilizzare i controlli del browser per cancellare i cookie per il dominio e quindi ricaricare la pagina.

Aggiornamento software

17. Come è possibile mantenere aggiornato il sistema operativo Manager?

Manager utilizza la distribuzione CentOS Linux per un sistema operativo. I pacchetti e il kernel possono essere aggiornati utilizzando i processi CentOS standard. Ad esempio, per eseguire un aggiornamento manuale, accedere alla console come utente cisco e immettere il comando *sudo yum -y* update. Non aggiornare il sistema a una nuova versione di CentOS e non installare pacchetti aggiuntivi oltre a quelli inclusi nell'immagine della macchina virtuale fornita da Cisco.

18. Come posso aggiornare Java sul Manager?

Gli aggiornamenti a Java devono essere scaricati da Oracle e installati manualmente utilizzando i seguenti comandi:

Per scaricare un nuovo pacchetto Java direttamente in Manager:

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie" -k
```

```
http://download.oracle.com/otn-pub/java/jdk/<versione>-<build>/jre-<versione>-linux-x64.rpm
```

Di seguito è riportato un esempio:

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie" -k
"http://download.oracle.com/otn-pub/java/jdk/8u102-b14/jre-8u102-linux-x64.rpm"
```

Per installare la versione Java aggiornata:

Passaggio 1. Rimuovere la versione precedente con il comando *sudo yum -y remove jre1.8.0_102*

Passaggio 2. Installare la nuova versione con il comando *sudo yum -y localinstall jre-<version>-linux-x64.rpm*

19. Come è possibile mantenere aggiornato il sistema operativo Probe?

La sonda utilizza OpenWRT per un sistema operativo. I pacchetti inclusi possono essere aggiornati utilizzando lo strumento **opkg**. Ad esempio, per aggiornare tutti i pacchetti del sistema, accedere alla console come utente cisco e immettere il comando update-packages. Se necessario, gli aggiornamenti del kernel verranno forniti da Cisco come parte di una nuova versione della sonda. Non installare pacchetti aggiuntivi oltre a quelli inclusi nell'immagine della macchina virtuale fornita da Cisco.

20. Cos'è il plug-in Cisco FindIT Kaseya?

Il plug-in FindIT Kaseya di Cisco è progettato per aumentare l'efficienza operativa integrando strettamente Cisco FindIT Network Manager con Kaseya Virtual System Administrator (VSA). Il plug-in FindIT Kaseya di Cisco offre potenti funzionalità, tra cui gestione delle azioni, dashboard, rilevamento dei dispositivi, topologia di rete, gestione remota dei dispositivi, avvisi attivabili e cronologia degli eventi.

Il plug-in è progettato per essere estremamente facile da installare e richiede solo pochi clic. È conforme a tutti i requisiti di integrazione di terze parti per le versioni VSA locali 9.3 e 9.4 di Kaseya. Per ulteriori informazioni, fare clic qui.