Cisco FindIT Network Management - Forum aux questions

Objectif

Cisco FindIT Network Management est un logiciel qui vous permet de gérer facilement l'ensemble de votre réseau, y compris vos périphériques Cisco, via votre navigateur Web. Il détecte, surveille et configure automatiquement tous les périphériques Cisco pris en charge sur votre réseau. Ce logiciel vous envoie également des notifications sur les mises à jour du micrologiciel et les informations sur les périphériques de votre réseau qui ne sont plus pris en charge par la garantie.

Cisco FindIT Network Management comporte deux composants distincts : un gestionnaire unique appelé FindIT Network Manager et un ou plusieurs sondes appelés FindIT Network Probe.

Cet article contient les questions fréquemment posées lors de la configuration, de la configuration et du dépannage de Cisco FindIT Network Management et leurs réponses.

Forum aux questions

Table des matières

Accès à distance

Mise à jour logicielle

Généralités

1. Quelles langues sont prises en charge par FindIT Network Management ?

FindIT Network Management est traduit dans les langues suivantes :

- Chinois
- Anglais
- Français
- Allemand
- Japonais
- Espagnol

Découverte

2. Quels protocoles FindIT utilise-t-il pour gérer mes périphériques ?

FindIT utilise divers protocoles pour détecter et gérer le réseau. Le protocole exact utilisé

pour un périphérique particulier varie selon le type de périphérique. Ces protocoles incluent :

- Multicast Domain Name System (mDNS) and DNS Service Discovery : ce protocole est également appelé Bonjour. Il localise des périphériques tels que des imprimantes, d'autres ordinateurs et les services que ces périphériques offrent sur un réseau local. Pour en savoir plus sur mDNS, cliquez ici. Pour plus d'informations sur la découverte de service DNS, cliquez ici.
- CDP (Cisco Discovery Protocol) : protocole propriétaire de Cisco utilisé pour partager des informations sur d'autres équipements Cisco directement connectés, tels que la version du système d'exploitation et l'adresse IP.
- Protocole LLDP (Link Layer Discovery Protocol) : protocole indépendant du fournisseur utilisé pour partager des informations sur d'autres équipements directement connectés, tels que la version du système d'exploitation et l'adresse IP.
- SNMP (Simple Network Management Protocol) : protocole de gestion de réseau utilisé pour collecter des informations et configurer des périphériques réseau tels que des serveurs, des imprimantes, des concentrateurs, des commutateurs et des routeurs sur un réseau IP (Internet Protocol).
- RESTCONF — Version préliminaire de l'IETF (Internet Engineering Task Force) qui décrit comment mapper une spécification de langage de modélisation de données YANG (Encore une nouvelle génération) à une interface RESTful. Pour en savoir plus, cliquez ici.

3. Comment FindIT découvre-t-il mon réseau ?

La sonde FindIT Network crée une première liste de périphériques du réseau à partir de l'écoute des annonces CDP, LLDP et mDNS. La sonde se connecte ensuite à chaque périphérique à l'aide d'un protocole pris en charge et collecte des informations supplémentaires telles que les tables de contiguïté CDP et LLDP, les tables d'adresses MAC (Media Access Control) et les listes de périphériques associées. Ces informations sont utilisées pour identifier des périphériques supplémentaires dans le réseau et le processus se répète jusqu'à ce que tous les périphériques aient été découverts.

4. FindIT analyse-t-il le réseau ?

FindIT n'analyse pas activement les plages d'adresses réseau. Il utilise une combinaison de surveillance passive de certains protocoles réseau et d'interrogation active des périphériques réseau pour obtenir des informations.

Gestion des ports

5. Pourquoi la gestion des ports n'affiche-t-elle pas les ports de pile ?

Les illustrations de la gestion des ports sont basées sur la liste des ports fournis par le périphérique via les protocoles de gestion. En mode empilage, les ports de pile sont considérés comme une connexion interne au sein de la pile, de sorte que le périphérique n'inclut pas ces ports dans les listes fournies via les protocoles de gestion.

Configuration

6. Que se passe-t-il lorsqu'un nouveau périphérique est détecté ? Sa configuration sera-t-elle modifiée ?

De nouveaux périphériques seront ajoutés au groupe de périphériques par défaut. Si des profils de configuration ont été attribués au groupe de périphériques par défaut, cette configuration sera également appliquée aux périphériques nouvellement découverts.

7. Que se passe-t-il lorsque je déplace un périphérique d'un groupe de périphériques à un autre ?

Toute configuration de réseau local virtuel (VLAN) ou de réseau local sans fil (WLAN) associée à des profils qui sont actuellement appliqués au groupe de périphériques d'origine et qui ne sont pas appliqués au nouveau groupe de périphériques sera supprimée, et la configuration de réseau local virtuel ou de réseau local sans fil associée aux profils qui sont appliqués au nouveau groupe et qui ne sont pas appliqués au groupe d'origine sera ajoutée au périphérique. Les paramètres de configuration système seront remplacés par des profils appliqués au nouveau groupe. Si aucun profil de configuration système n'est défini pour le nouveau groupe, la configuration système du périphérique ne changera pas.

Examen de la sécurité

8. Quelles plages de ports et quels protocoles sont requis par FindIT Network Manager ?

Le tableau suivant contient les protocoles et les ports utilisés par FindIT Network Manager :

Port	Direction	Protocol	Utilisation
TCP 22	Entrant	SSH	Accès en ligne de commande à Manager
TCP 80	Entrant	HTTP	Accès Web au gestionnaire. Redirige vers le serveur Web sécurisé (port 443)
TCP 443	Entrant	HTTPS	Accès Web sécurisé à Manager
TCP 1069	Entrant	NETCONF/TLS	Communication entre Probe et Manager
TCP 9443	Entrant	HTTPS	Accès à distance à l'interface utilisateur de Probe
TCP 50000-51000	Entrant	Dépendance du périphérique	Accès à distance aux périphériques
UDP 53	Sortant	DNS	Résolution des noms de domaine
UDP 123	Sortant	NTP	Synchronisation temporelle
UDP 5353	Sortant	mDNS	Annonces de service DNS multidiffusion vers le réseau local annonçant le gestionnaire

9. Quelles plages de ports et quels protocoles sont requis par FindIT Network Probe ?

Le tableau suivant répertorie les protocoles et les ports utilisés par FindIT Network Probe :

Port	Direction	Protocol	Utilisation
TCP 22	Entrant	SSH	Accès en ligne de commande à Probe
TCP 80	Entrant	HTTP	Accès Web au gestionnaire. Redirige vers le serveur Web sécurisé (port 443)

TCP 443	Entrant	HTTPS	Accès Web sécurisé à Manager
UDP 5353	Entrant	mDNS	Annonces de service DNS multidiffusion à partir du réseau local. Utilisé pour la détection de périphériques.
TCP 10000-10100	Entrant	Dépendance du périphérique	Accès à distance aux périphériques
UDP 53	Sortant	DNS	Résolution des noms de domaine
UDP 123	Sortant	NTP	Synchronisation temporelle
TCP 80	Sortant	HTTP	Gestion des périphériques sans services Web sécurisés activés
UDP 161	Sortant	SNMP	Gestion des périphériques réseau
TCP 443	Sortant	HTTPS	Gestion des périphériques avec services Web sécurisés activés. Accédez aux services Web Cisco pour obtenir des informations telles que les mises à jour logicielles, l'assistance, l'état et les avis de fin de vie
TCP 1069	Sortant	NETCONF/TLS	Communication entre Probe et Manager
UDP 5353	Sortant	mDNS	Annonces de service DNS multidiffusion vers le réseau local annonçant la sonde

[10. Quelle est la sécurité de la communication entre FindIT Network Manager et FindIT Network Probe ?]

Toute communication entre le gestionnaire et la sonde est chiffrée à l'aide d'une session TLS (Transport Layer Security) 1.2 authentifiée avec des certificats client et serveur. La session est initiée de la sonde au gestionnaire. Au moment de l'établissement de l'association entre le gestionnaire et la sonde, l'utilisateur doit se connecter au gestionnaire à partir de la sonde, à partir de laquelle le gestionnaire et les certificats d'échange de la sonde doivent être utilisés pour authentifier les communications futures.

[11. FindIT dispose-t-il d'un accès 'backdoor' à mes périphériques ?]

Non. Lorsque FindIT détecte un périphérique Cisco pris en charge, il tente d'accéder au périphérique à l'aide des informations d'identification par défaut d'usine de ce périphérique avec le nom d'utilisateur et le mot de passe par défaut : cisco ou communauté SNMP par défaut : public. Si la configuration du périphérique a été modifiée par défaut, il sera nécessaire que l'utilisateur fournisse les informations d'identification correctes à FindIT.

[12. Quelle est la sécurité des informations d'identification stockées dans FindIT ?]

Les informations d'identification permettant d'accéder à FindIT sont irréversiblement hachées à l'aide de l'algorithme SHA512. Les informations d'identification des périphériques et autres services, tels que **Cisco Active Advisor**, sont chiffrées de manière réversible à l'aide de l'algorithme AES-128.

[13. Comment récupérer un mot de passe perdu pour l'interface utilisateur d'administration ?]

Si vous avez perdu le mot de passe de tous les comptes admin de l'interface utilisateur graphique d'administration, vous pouvez réinitialiser le mot de passe en vous connectant sur la console du Probe ou du Manager et en exécutant l'outil **de mot de passe restauré**. Cet outil réinitialise le mot de passe par défaut du compte cisco ou, si le compte cisco a été supprimé, recrée le compte avec le mot de passe par défaut. Voici un exemple des commandes à fournir pour réinitialiser le mot de passe à l'aide de cet outil.

```
cisco@FindITProbe :~# mot de passe de récupération

En es-tu sûr ? (y/n) y

Rétablir le mot de passe par défaut du compte cisco

cisco@FindITProbe:~#
```

Accès à distance

14. Lorsque je me connecte à l'interface utilisateur graphique d'administration d'un périphérique à partir de FindIT Network Management, la session est-elle sécurisée ?

FindIT Network Management effectue un tunnel de la session d'accès à distance entre le périphérique et l'utilisateur. Le protocole utilisé dépend de la configuration du périphérique final, mais FindIT établit toujours la session à l'aide d'un protocole sécurisé si l'un d'eux est activé (par exemple, HTTPS sera préféré à HTTP). Si l'utilisateur se connecte au périphérique via le gestionnaire, la session passe par un tunnel chiffré lorsqu'elle passe entre le gestionnaire et la sonde, quels que soient les protocoles activés sur le périphérique.

15. Pourquoi ma session d'accès à distance avec un périphérique se déconnecte-t-elle immédiatement lorsque j'ouvre une session d'accès à distance à un autre périphérique ?

Lorsque vous accédez à un périphérique via FindIT Network Management, le navigateur voit chaque connexion comme étant avec le même serveur Web (FindIT) et présente donc des cookies de chaque périphérique à chaque autre périphérique. Si plusieurs périphériques utilisent le même nom de cookie, il est possible qu'un cookie de périphérique soit remplacé par un autre périphérique. Ceci est le plus souvent vu avec les cookies de session, et le résultat est que le cookie n'est valide que pour le périphérique visité le plus récemment. Tous les autres périphériques qui utilisent le même nom de cookie voient le cookie comme non valide et déconnectent la session.

16. Pourquoi ma session d'accès à distance échoue-t-elle avec une erreur comme celle-ci : Erreur d'accès : L'entité de demande est trop grande, le champ d'en-tête HTTP dépasse la taille prise en charge ?

Après avoir effectué de nombreuses sessions d'accès à distance avec différents périphériques, le navigateur aura un grand nombre de cookies stockés pour le domaine Probe. Pour contourner ce problème, utilisez les contrôles du navigateur pour effacer les cookies du domaine, puis rechargez la page.

Mise à jour logicielle

17. Comment puis-je maintenir le système d'exploitation Manager à jour ?

Le gestionnaire utilise la distribution CentOS Linux pour un système d'exploitation. Les

paquets et le noyau peuvent être mis à jour à l'aide des processus CentOS standard. Par exemple, pour effectuer une mise à jour manuelle, connectez-vous à la console en tant qu'utilisateur cisco et entrez la commande *sudo yum -y* update. Le système ne doit pas être mis à niveau vers une nouvelle version de CentOS et aucun package supplémentaire ne doit être installé au-delà de ceux inclus dans l'image de machine virtuelle fournie par Cisco.

18. Comment mettre à jour Java sur le gestionnaire ?

Les mises à jour Java doivent être téléchargées à partir d'Oracle et installées manuellement à l'aide des commandes suivantes :

Pour télécharger un nouveau package Java directement au gestionnaire :

```
curl -L -O -H « Cookie : oraclelicense=accept-securebackup-cookie » -k
http://download.oracle.com/otn-pub/java/jdk/<version>-<build>/jre-<version>-linux-x64.rpm
```

Voici un exemple :

```
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"
```

Pour installer la version Java mise à jour :

Étape 1. Supprimez l'ancienne version avec la commande *sudo yum -y remove jre1.8.0_102*

Étape 2. Installez la nouvelle version avec la commande *sudo yum -y localinstall jre-<version>-linux-x64.rpm*

19. Comment puis-je maintenir le système d'exploitation Probe à jour ?

La sonde utilise OpenWRT pour un système d'exploitation. Les paquets inclus peuvent être mis à jour à l'aide de l'outil **opkg**. Par exemple, pour mettre à jour tous les packages du système, connectez-vous à la console en tant qu'utilisateur cisco et entrez la commande update-packages. Si nécessaire, les mises à jour du noyau seront fournies par Cisco dans le cadre d'une nouvelle version du Probe. Aucun package supplémentaire ne doit être installé au-delà de ceux inclus dans l'image de machine virtuelle fournie par Cisco.

20. Qu'est-ce que le plug-in Cisco FindIT Kaseya ?

Le plug-in Cisco FindIT Kaseya est conçu pour augmenter l'efficacité opérationnelle en intégrant étroitement Cisco FindIT Network Manager à l'administrateur système virtuel (VSA) de Kaseya. Le plug-in Cisco FindIT Kaseya offre des fonctionnalités puissantes, notamment la gestion des actions, les tableaux de bord, la détection des périphériques, la topologie du réseau, la gestion des périphériques distants, les alertes exploitables et l'historique des événements.

Le plug-in est conçu pour être extrêmement facile à installer, ne nécessitant que quelques clics. Il est conforme à toutes les exigences d'intégration tierce pour les versions 9.3 et 9.4 de la VSA sur site de Kaseya. Pour en savoir plus, cliquez ici.