Cisco FindIT Network Management Häufig gestellte Fragen

Ziel

Cisco FindIT Network Management ist eine Software, mit der Sie Ihr gesamtes Netzwerk einschließlich Ihrer Cisco Geräte über Ihren Webbrowser einfach verwalten können. Er erkennt, überwacht und konfiguriert automatisch alle unterstützten Cisco Geräte in Ihrem Netzwerk. Diese Software sendet Ihnen auch Benachrichtigungen über Firmware-Updates und Informationen über Geräte in Ihrem Netzwerk, für die keine Garantie mehr besteht.

Das Cisco FindIT Network Management besteht aus zwei Komponenten: einen einzelnen Manager, den FindIT Network Manager, und eine oder mehrere Probes, die FindIT Network Probes, genannt FindIT Network Probe.

Dieser Artikel enthält die häufig gestellten Fragen zur Einrichtung, Konfiguration und Fehlerbehebung des Cisco FindIT Network Management und deren Antworten.

Häufig gestellte Fragen

Inhaltsverzeichnis

Remote-Zugriff

Software-Update

Allgemeines

FindIT Network Management wird in die folgenden Sprachen übersetzt:

- Chinesisch
- Englisch
- Französisch
- Deutsch
- Japanisch
- Spanisch

Erkennung

FindIT verwendet verschiedene Protokolle, um das Netzwerk zu erkennen und zu verwalten. Das genaue Protokoll, das für ein bestimmtes Gerät verwendet wird, hängt vom Gerätetyp ab. Zu diesen Protokollen gehören:

- Multicast Domain Name System (mDNS) und DNS Service Discovery - Dieses Protokoll

wird auch als Bonjour bezeichnet. Sie sucht Geräte wie Drucker, andere Computer und die Dienste, die diese Geräte in einem lokalen Netzwerk anbieten. Weitere Informationen zu mDNS erhalten Sie hier. Weitere Informationen zur DNS Service Discovery erhalten Sie hier.

- Cisco Discovery Protocol (CDP) - Ein proprietäres Protokoll von Cisco, das verwendet wird, um Informationen über andere direkt verbundene Cisco Geräte auszutauschen, z. B. die Betriebssystemversion und die IP-Adresse.
- Link Layer Discovery Protocol (LLDP) - Ein herstellerneutrales Protokoll, das verwendet wird, um Informationen über andere direkt verbundene Geräte auszutauschen, z. B. die Betriebssystemversion und die IP-Adresse.
- Simple Network Management Protocol (SNMP) - Ein Netzwerkverwaltungsprotokoll, das zum Erfassen von Informationen und zum Konfigurieren von Netzwerkgeräten wie Servern, Druckern, Hubs, Switches und Routern in einem IP-Netzwerk (Internet Protocol) verwendet wird.
- RESTCONF - Ein Entwurf einer Internet Engineering Task Force (IETF), in dem beschrieben wird, wie eine weitere YANG-Datenmodellspezifikation (Next Generation Data Model) einer RESTful-Schnittstelle zugeordnet wird. Weitere Informationen erhalten Sie hier.

3. Wie erkennt FindIT mein Netzwerk?

Die FindIT Network Probe erstellt eine erste Liste von Geräten im Netzwerk, die CDP-, LLDP- und mDNS-Meldungen überwachen. Die Anfrage stellt dann über ein unterstütztes Protokoll eine Verbindung zu jedem Gerät her und sammelt zusätzliche Informationen wie CDP- und LLDP-Adjacency-Tabellen, MAC-Adresstabellen (Media Access Control) und zugeordnete Gerätelisten. Diese Informationen werden verwendet, um zusätzliche Geräte im Netzwerk zu identifizieren. Der Prozess wiederholt sich, bis alle Geräte erkannt wurden.

4. Führt FindIT Netzwerkprüfungen durch?

FindIT überprüft die Netzwerkadressenbereiche nicht aktiv. Dabei wird eine Kombination aus passiver Überwachung bestimmter Netzwerkprotokolle und aktiver Abfrage von Netzwerkgeräten nach Informationen verwendet.

Port-Management

5. Warum zeigt die Portverwaltung keine Stack-Ports an?

Die Abbildungen zur Portverwaltung basieren auf der Liste der Ports, die vom Gerät über die Verwaltungsprotokolle bereitgestellt werden. Im Stacking-Modus werden die Stack-Ports als interne Verbindung innerhalb des Stacks betrachtet, sodass diese Ports nicht in den Listen der Verwaltungsprotokolle enthalten sind.

Konfiguration

6. Was geschieht, wenn ein neues Gerät erkannt wird? Wird die Konfiguration geändert?

Neue Geräte werden der standardmäßigen Gerätegruppe hinzugefügt. Wenn Konfigurationsprofile der Standardgerätegruppe zugewiesen wurden, wird diese Konfiguration auch auf neu erkannte Geräte angewendet.

7. Was passiert, wenn ich ein Gerät von einer Gerätegruppe in eine andere verschiebe?

Alle Konfigurationen für Virtual Local Area Network (VLAN) oder Wireless Local Area Network (WLAN), die Profilen zugeordnet sind, die derzeit auf die ursprüngliche Gerätegruppe angewendet werden und nicht auf die neue Gerätegruppe angewendet werden, werden entfernt, und dem Gerät wird die VLAN- oder WLAN-Konfiguration hinzugefügt, die Profilen zugeordnet ist, die auf die neue Gruppe angewendet werden und nicht auf die ursprüngliche Gruppe angewendet werden. Die Systemkonfigurationseinstellungen werden durch Profile überschrieben, die auf die neue Gruppe angewendet werden. Wenn für die neue Gruppe keine Systemkonfigurationsprofile definiert sind, ändert sich die Systemkonfiguration für das Gerät nicht.

Überlegungen zur Sicherheit

8. Welche Port-Bereiche und Protokolle sind für FindIT Network Manager erforderlich?

Die folgende Tabelle enthält die Protokolle und Ports, die vom FindIT Network Manager verwendet werden:

Port	Richtung	Protokoll	Verwendung
TCP 22	Eingehend	SSH	Befehlszeilenzugriff auf den Manager
TCP 80	Eingehend	HTTP	Webzugriff auf Manager. Umleitung zum sicheren Webserver (Port 443)
TCP	Eingehend	HTTPS	Sicherer Internetzugriff für Manager
TCP	Eingehend	NETCONF/TLS	Kommunikation zwischen Probe und Manager
TCP	Eingehend	HTTPS	Remote-Zugriff auf die Sonde-GUI
TCP	Eingehend	Geräteabhängig	Remote-Zugriff auf Geräte
UDP 53	Ausgehend	DNS	Auflösung von Domänennamen
UDP 123	Ausgehend	NTP	Zeitsynchronisierung
UDP 5353	Ausgehend	mDNS	Multicast-DNS-Service-Werbung für das lokale Netzwerk, die den Manager informiert

9. Welche Port-Bereiche und Protokolle werden von FindIT Network Probe benötigt?

In der folgenden Tabelle sind die Protokolle und Ports aufgeführt, die von FindIT Network Probe verwendet werden:

Port	Richtung	Protokoll	Verwendung
TCP 22	Eingehend	SSH	Befehlszeilenzugriff auf die Anfrage
TCP 80	Eingehend	HTTP	Webzugriff auf Manager. Umleitung zum sicheren Webserver (Port 443)
TCP	Eingehend	HTTPS	Sicherer Internetzugriff für Manager
UDP 5353	Eingehend	mDNS	Multicast-DNS-Service-Meldungen aus dem lokalen Netzwerk. Wird für die Geräteerkennung verwendet.
TCP	Eingehend	Geräteabhängig	Remote-Zugriff auf Geräte

UDP 53	Ausgehend	DNS	Auflösung von Domänennamen
UDP 123	Ausgehend	NTP	Zeitsynchronisierung
TCP 80	Ausgehend	HTTP	Verwaltung von Geräten ohne Aktivierung sicherer Web-Services
UDP 161	Ausgehend	SNMP	Verwaltung von Netzwerkgeräten
TCP	Ausgehend	HTTPS	Verwaltung von Geräten mit aktivierten sicheren Web-Services Zugriff auf Cisco Web Services für Informationen wie Software-Updates, Support, Status und Hinweise zum Ende des Lebenszyklus
TCP	Ausgehend	NETCONF/TLS	Kommunikation zwischen Probe und Manager
UDP 5353	Ausgehend	mDNS	Multicast-DNS-Service-Anzeigen für das lokale Netzwerk, die die Anfrage senden

10. Wie sicher ist die Kommunikation zwischen FindIT Network Manager und FindIT Network Probe?

Die gesamte Kommunikation zwischen Manager und Probe wird mithilfe einer mit Client- und Serverzertifikaten authentifizierten Transport Layer Security (TLS) 1.2-Sitzung verschlüsselt. Die Sitzung wird von der Probe zum Manager initiiert. Bei der ersten Herstellung der Verbindung zwischen Manager und Probe muss sich der Benutzer von der Probe aus beim Manager anmelden. An dieser Stelle tauschen der Manager und die Probe Zertifikate aus, um zukünftige Kommunikation zu authentifizieren.

11. Verfügt FindIT über "Backdoor"-Zugriff auf meine Geräte?

Nein. Wenn FindIT ein unterstütztes Cisco Gerät erkennt, versucht es, mithilfe der werkseitigen Standardanmeldeinformationen für dieses Gerät mit dem Standardbenutzernamen und -kennwort auf das Gerät zuzugreifen: cisco oder die Standard-SNMP-Community: öffentlich. Wenn die Gerätekonfiguration von der Standardkonfiguration geändert wurde, muss der Benutzer FindIT die richtigen Anmeldeinformationen zuweisen.

12. Wie sicher sind die Anmeldeinformationen in FindIT gespeichert?

Anmeldeinformationen für den Zugriff auf FindIT werden mit dem SHA512-Algorithmus unwiderruflich gehasht. Anmeldeinformationen für Geräte und andere Services, z. B. den **Cisco Active Advisor**, werden mit dem AES-128-Algorithmus reversibel verschlüsselt.

13. Wie stelle ich ein verlorenes Kennwort für die Administrations-GUI wieder her?

Wenn Sie das Kennwort für alle Admin-Konten in der Verwaltungs-GUI verloren haben, können Sie das Kennwort zurücksetzen, indem Sie sich in der Konsole der Probe oder des Managers anmelden und das **Wiederherstellungs-Kennwort**-Tool ausführen. Dieses Tool setzt das Kennwort für das Cisco Konto auf den Standardwert von cisco zurück. Wenn das Cisco Konto entfernt wurde, wird das Konto mit dem Standardkennwort neu erstellt. Das nachfolgende Beispiel zeigt die Befehle, die bereitgestellt werden müssen, um das Kennwort mit diesem Tool zurückzusetzen.

```
cisco@FindITProbe:~# Wiederherstellungs-Kennwort
```

```
Sind Sie sicher? (J/N) y

Zurücksetzen des Cisco Kontos auf das Standardkennwort

cisco@FindITProbe:~#
```

Remote-Zugriff

14. Ist die Sitzung sicher, wenn ich über FindIT Network Management eine Verbindung zur Administration-GUI eines Geräts herstellen kann?

FindIT Network Management tunnelt die Remote-Zugriffssitzung zwischen dem Gerät und dem Benutzer. Das verwendete Protokoll hängt von der Endgerätekonfiguration ab, aber FindIT richtet die Sitzung immer mithilfe eines sicheren Protokolls ein, wenn ein Protokoll aktiviert ist (z. B. wird HTTPS gegenüber HTTP bevorzugt). Wenn der Benutzer über den Manager eine Verbindung zum Gerät herstellt, durchläuft die Sitzung einen verschlüsselten Tunnel, der zwischen dem Manager und der Probe verläuft, unabhängig von den Protokollen, die auf dem Gerät aktiviert sind.

15. Warum meldet sich meine Remote-Zugriffssitzung mit einem Gerät sofort ab, wenn ich eine Remotezugriffssitzung mit einem anderen Gerät öffne?

Wenn Sie über FindIT Network Management auf ein Gerät zugreifen, erkennt der Browser jede Verbindung als mit demselben Webserver (FindIT) und zeigt daher Cookies von jedem Gerät an jedes andere Gerät an. Wenn mehrere Geräte denselben Cookie-Namen verwenden, besteht die Möglichkeit, dass ein Gerätecookie von einem anderen Gerät überschrieben wird. Dies wird häufig bei Session-Cookies beobachtet, und das Ergebnis ist, dass das Cookie nur für das zuletzt besuchte Gerät gültig ist. Alle anderen Geräte, die denselben Cookie-Namen verwenden, sehen das Cookie als ungültig und melden sich an.

16. Warum schlägt meine Remote-Zugriffssitzung mit einem Fehler wie dem folgenden fehl: Zugriffsfehler: Anforderungseinheit zu groß, HTTP-Headerfeld überschreitet unterstützte Größe?

Nachdem Sie viele Remote-Zugriffssitzungen mit verschiedenen Geräten durchgeführt haben, werden im Browser eine große Anzahl von Cookies für die Testdomäne gespeichert. Um dieses Problem zu umgehen, verwenden Sie die Browsersteuerelemente, um Cookies für die Domäne zu löschen und anschließend die Seite neu zu laden.

Software-Update

17. Wie halte ich das Betriebssystem Manager auf dem neuesten Stand?

Der Manager verwendet die CentOS Linux-Distribution für ein Betriebssystem. Die Pakete und der Kernel können mit den standardmäßigen CentOS-Prozessen aktualisiert werden. Um beispielsweise eine manuelle Aktualisierung durchzuführen, melden Sie sich als Cisco Benutzer bei der Konsole an, und geben Sie den Befehl *sudo yum -y* update ein. Das System sollte nicht auf eine neue CentOS-Version aktualisiert werden, und es sollten keine zusätzlichen Pakete installiert werden, die über die Pakete hinausgehen, die im Virtual Machine Image von Cisco enthalten sind.

18. Wie aktualisiere ich Java im Manager?

Java-Updates sollten von Oracle heruntergeladen und manuell mithilfe der folgenden Befehle installiert werden:

So laden Sie ein neues Java-Paket direkt auf den Manager herunter:

```
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
```

Im Folgenden sehen Sie ein Beispiel:

```
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"
```

So installieren Sie die aktualisierte Java-Version:

Schritt 1: Entfernen Sie die alte Version mit dem Befehl *sudo yum -y remove jre1.8.0_102.*

Schritt 2: Installieren Sie die neue Version mit dem Befehl *sudo yum -y localinstall jre-<version>-linux-x64.rpm*

19. Wie erhalte ich das Testbetriebssystem auf dem neuesten Stand?

Die Probe verwendet OpenWRT für ein Betriebssystem. Enthaltene Pakete können mit dem **opkg-**Tool aktualisiert werden. Um beispielsweise alle Pakete auf dem System zu aktualisieren, melden Sie sich als cisco-Benutzer bei der Konsole an, und geben Sie den Befehl update-packages ein. Bei Bedarf werden Kernel-Updates von Cisco als Teil einer neuen Version der Probe bereitgestellt. Es sollten keine zusätzlichen Pakete installiert werden, die über die Pakete hinausgehen, die im Virtual Machine Image von Cisco enthalten sind.

20. Was ist das Cisco FindIT Kaseya Plugin?

Das Cisco FindIT Kaseya Plugin wurde entwickelt, um die Betriebseffizienz durch die enge Integration von Cisco FindIT Network Manager und Kaseya Virtual System Administrator (VSA) zu steigern. Das Cisco FindIT Kaseya Plugin bietet leistungsstarke Funktionen wie Aktionsmanagement, Dashboards, Geräteerkennung, Netzwerktopologie, Remote-Gerätemanagement, aussagekräftige Warnmeldungen und Ereignisprotokolle.

Das Plugin ist so konzipiert, dass es sehr einfach zu installieren ist, und nur wenige Klicks erforderlich. Es erfüllt alle Integrationsanforderungen von Drittanbietern für Kaseya VSA Version 9.3 und 9.4 vor Ort. Weitere Informationen erhalten Sie hier.