Cisco FindIT-netwerkbeheer vaak gestelde vragen

Doel

Het Cisco FindIT-netwerkbeheer is een software waarmee u uw gehele netwerk, inclusief uw Cisco-apparaten, eenvoudig kunt beheren via uw webbrowser. Het ontdekt, controleert, en vormt automatisch alle ondersteunde apparaten van Cisco in uw netwerk. Deze software stuurt u ook een melding van de updates van de firmware en informatie over de apparaten in uw netwerk die niet langer door garantie worden ondersteund.

Cisco FindIT-netwerkbeheer heeft twee afzonderlijke onderdelen: één enkele Manager bekend als de FindIT Network Manager en één of meer tests bekend als de FindIT Network Probe.

Dit artikel bevat de vaak gestelde vragen bij het opzetten, configureren en oplossen van het Cisco FindIT-netwerkbeheer en hun antwoorden.

Veelgestelde vragen

Inhoud

Algemeen

1. Welke talen worden door het FindIT-netwerkbeheer ondersteund?

ontdekking

2. Welke protocollen gebruikt FindIT om mijn apparaten te beheren?
3. Hoe ontdekt FindIT mijn netwerk?
4. Werkt FindIT netwerkscans?

Poortbeheer

5. Waarom toont Port Management geen stapelpoorten?

Configuratie

6. Wat gebeurt er wanneer een nieuw apparaat wordt ontdekt? Zal de configuratie worden gewijzigd?
7. Wat gebeurt er als ik een apparaat van de ene naar de andere apparaatgroep verplaats?

Veiligheidsoverweging

8. Welke poortbereik en -protocollen worden door FindIT Network Manager vereist?
9. Welke poortbereiken en protocollen worden door FindIT-netwerkmodule vereist?

Externe toegang

Software update

Algemeen

1. Welke talen worden ondersteund door het FindIT-netwerkbeheer?

FindIT-netwerkbeheer wordt vertaald in de volgende talen:

- Chinees
- Engels
- Frans
- Duits
- Japans
- Spaans

ontdekking

2. Welke protocollen gebruikt FindIT om mijn apparaten te beheren?

FindIT gebruikt een verscheidenheid aan protocollen om het netwerk te ontdekken en te beheren. Het exacte protocol dat voor een bepaald apparaat wordt gebruikt, varieert afhankelijk van het type apparaat. Deze protocollen omvatten:

- Multicast Domain Name System (mDNS) en DNS-servicedetectie — Dit protocol wordt ook bekend als Bonjour. Het lokaliseert apparaten zoals printers, andere computers, en

de services die deze apparaten op een lokaal netwerk aanbieden. Klik hier voor meer informatie over mDNS. Klik hier voor meer informatie over DNS-servicedetectie.
- Cisco Discovery Protocol (CDP) - een eigen Cisco-protocol dat wordt gebruikt om informatie te delen over andere rechtstreeks aangesloten Cisco-apparatuur, zoals de versie van het besturingssysteem en IP-adres.
- Link Layer Discovery Protocol (LLDP) — een verkoopneutraal protocol dat wordt gebruikt om informatie te delen over andere rechtstreeks aangesloten apparatuur, zoals de versie van het besturingssysteem en het IP-adres.
- Simple Network Management Protocol (SNMP) - een netwerkbeheerprotocol dat wordt gebruikt voor het verzamelen van informatie en het configureren van netwerkapparaten zoals servers, printers, knooppunten, switches en routers op een IP-netwerk (Internet Protocol).
- RESTCONF — Een ontwerp van de Internet Engineering Task Force (IETF) die beschrijft hoe een ABBYY-gegevensmodellering van de volgende generatie (YANG) op een RESTful-interface in kaart moet worden gebracht. Klik hier voor meer informatie.

3. Hoe ontdekt FindIT mijn netwerk?

De FindIT Network Probe maakt een eerste lijst met apparaten in het netwerk vanaf het luisteren naar CDP-, LLDP- en mDNS-advertenties. De sonde sluit dan aan op elk apparaat dat een ondersteund protocol gebruikt en verzamelt extra informatie zoals CDP en LDP nabijheidstabellen, Media Access Control (MAC) adrestabellen en bijbehorende apparaatlijsten. Deze informatie wordt gebruikt om extra apparaten in het netwerk te identificeren, en het proces herhaalt tot alle apparaten zijn ontdekt.

4. Werkt FindIT wel met netwerkscans?

FindIT scant de netwerkadresbereik niet actief. Het maakt gebruik van een combinatie van passieve controle van bepaalde netwerkprotocollen en actief gebruik van netwerkapparaten voor informatie.

Poortbeheer

5. Waarom laat Port Management geen stapelpoorten zien?

De illustraties van het havenbeheer zijn gebaseerd op de lijst van havens die door het apparaat via de beheersprotocollen worden geleverd. In de stapelmodus worden de stapelpoorten beschouwd als een interne verbinding binnen de stapel. Daarom bevat het apparaat deze poorten niet in de lijsten die via de beheerprotocollen worden geleverd.

Configuratie

6. Wat gebeurt er wanneer een nieuw apparaat wordt ontdekt? Zal de configuratie worden gewijzigd?

Nieuwe apparaten zullen worden toegevoegd aan de standaardinstelling van het apparaat. Als de configuratieprofielen zijn toegewezen aan de standaardapparatengroep, dan zal die configuratie ook op pas ontdekte apparaten worden toegepast.

7. Wat gebeurt er als ik een apparaat van de ene naar de andere apparaatgroep verplaats?

Alle Virtual Local Area Network (VLAN) of Wireless Local Area Network (WLAN) configuratie die is gekoppeld aan profielen die momenteel op de oorspronkelijke apparaatgroep worden toegepast en niet op de nieuwe apparaatgroep worden toegepast, wordt verwijderd en VLAN of WLAN-configuratie die wordt gekoppeld aan profielen die worden toegepast op de nieuwe groep en niet worden toegepast op de oorspronkelijke groep, wordt aan het apparaat toegevoegd. De instellingen voor de systeemconfiguratie worden overschreven door profielen die op de nieuwe groep worden toegepast. Als er geen systeemconfiguratieprofielen zijn gedefinieerd voor de nieuwe groep, dan zal de systeemconfiguratie voor het apparaat niet veranderen.

Veiligheidsoverweging

8. Welke poortbereik en -protocollen worden door FindIT Network Manager vereist?

De volgende tabel bevat de protocollen en poorten die door FindIT Network Manager worden gebruikt:

Port	Richting	Protocol	Gebruik
TCP 22	Inkomend	SSH	Opdracht-line toegang tot Manager
TCP 80	Inkomend	HTTP	Webtoegang tot Manager. Omleidingen naar beveiligde webserver (poort 443)
TCP 443	Inkomend	HTTPS	Beveiligde toegang via web tot Manager
TCP 1069	Inkomend	NETCONF/TLS	Communicatie tussen Probe en Manager
TCP 9443	Inkomend	HTTPS	Toegang op afstand tot Probe GUI
TCP 5000-51000	Inkomend	Apparaatafhankelijk	Externe toegang tot apparaten
UDP 53	Uitgaand	DNS	Resolutie van domeinnaam
UDP 123	Uitgaand	NTP	Tijdsynchronisatie
UDP 5353	Uitgaand	mDNS	Multicast DNS-serviceresponsen voor lokaal netwerk dat adverteert met de Manager

9. Welke poortbereik en -protocollen worden door de FindIT-netwerkmodule vereist?

De volgende tabel toont de protocollen en poorten die door FindIT Network Probe worden gebruikt:

Port	Richting	Protocol	Gebruik
TCP 22	Inkomend	SSH	Opdracht-line toegang tot de sonde
TCP 80	Inkomend	HTTP	Webtoegang tot Manager. Omleidingen naar beveiligde webserver (poort 443)
TCP 443	Inkomend	HTTPS	Beveiligde toegang via web tot Manager
UDP 5353	Inkomend	mDNS	Multicast DNS-serviceresponsen via het lokale netwerk. Gebruikt voor apparaatontdekking.

TCP 1000-10100	Inkomend	Apparaatafhankelijk	Externe toegang tot apparaten
UDP 53	Uitgaand	DNS	Resolutie van domeinnaam
UDP 123	Uitgaand	NTP	Tijdsynchronisatie
TCP 80	Uitgaand	HTTP	Beheer van apparaten zonder beveiligde webdiensten
UDP 161	Uitgaand	SNMP	Beheer van netwerkapparaten
TCP 443	Uitgaand	HTTPS	Beheer van apparaten met beveiligde webdiensten. Access Cisco-webservices voor informatie zoals softwareupdates, ondersteuning, status en end-of-life details
TCP 1069	Uitgaand	NETCONF/TLS	Communicatie tussen Probe en Manager
UDP 5353	Uitgaand	mDNS	Multicast DNS-serviceresponsen voor het lokale netwerk dat de Probe aanmaakt

10. Hoe veilig is de communicatie tussen FindIT Network Manager en FindIT Network Probe?

Alle communicatie tussen de Manager en de Probe wordt versleuteld met een TLS 1.2-sessie (Transport Layer Security) die is beveiligd met client- en servercertificaten. De sessie wordt gestart vanuit de sonde naar de Manager. Op het moment dat de associatie tussen Manager en Probe voor het eerst wordt ingesteld, moet de gebruiker zich aanmelden bij de Manager vanuit de Probe, op welk punt de Manager en de Probe-certificaten worden uitgewisseld om toekomstige communicatie te controleren.

11. Heeft FindIT toegang tot mijn apparaten?

Nee. Wanneer FindIT een ondersteund Cisco-apparaat ontdekt, zal het proberen om het apparaat te benaderen met behulp van de standaard fabrieksreferenties voor dat apparaat met de standaard gebruikersnaam en het wachtwoord: Cisco, of de standaard SNMP-gemeenschap: openbaar. Als de apparaatconfiguratie is gewijzigd van de standaardinstelling, dan moet de gebruiker de juiste aanmeldingsgegevens leveren om FindIT te vinden.

12. Hoe veilig zijn de aanmeldingsgegevens die in FindIT zijn opgeslagen?

Credentials voor toegang tot FindIT worden onherroepelijk gehashed met behulp van het SHA512 algoritme. Credentials voor apparaten en andere services, zoals de **Cisco Active Adviseur** van **Cisco**, worden reversibel versleuteld met het AES-128-algoritme.

13. Hoe herstel ik een verloren wachtwoord voor de Administratie GUI?

Als u het wachtwoord voor alle Admin-accounts in de beheerGUI hebt verloren, kunt u het wachtwoord terugstellen door te loggen op de console van de proxy of Manager en het **wachtwoord** voor het **herstellen** uit te voeren. Dit gereedschap stelt het wachtwoord voor de cisco-account in op de standaard cisco-account of, als de cisco-account is verwijderd, wordt de account met het defaultwachtwoord opnieuw gecreëerd. Hieronder volgen een voorbeeld van de opdrachten die moeten worden geleverd om het wachtwoord te herstellen met behulp

van dit gereedschap.

```
cisco@FindITProbe:~# wachtwoord voor herstel

Weet je het zeker? (y/n) y

Zet de cisco-account terug op het defaultwachtwoord

cisco@FindITProbe:~#
```

Externe toegang

14. Wanneer ik verbinding maak met de Administration GUI van een apparaat van FindIT Network Management, is de sessie beveiligd?

FindIT Network Management-tunnels de externe toegangssessie tussen het apparaat en de gebruiker. Het gebruikte protocol zal afhangen van de configuratie van het eindapparaat, maar FindIT zal altijd de sessie instellen met behulp van een beveiligd protocol als er een is geactiveerd (bijvoorbeeld HTTPS krijgt de voorkeur boven HTTP). Als de gebruiker via Manager verbinding maakt met het apparaat, zal de sessie door een versleutelde tunnel gaan terwijl deze tussen de Manager en de sonde passeert, ongeacht de protocollen die op het apparaat zijn ingeschakeld.

15. Waarom logt mijn afstandstoegangssessie met een apparaat onmiddellijk uit als ik een externe toegangssessie naar een ander apparaat open?

Wanneer u toegang krijgt tot een apparaat via FindIT Network Management, ziet de browser elke verbinding als een verbinding met dezelfde webserver (FindIT) en geeft deze dus koekjes van elk apparaat aan elk ander apparaat. Als meerdere apparaten dezelfde koekjesnaam gebruiken, dan is er de mogelijkheid dat één apparaatkoekje overschreven kan worden door een ander toestel. Dit wordt het vaakst gezien bij sessiekoekjes, en het resultaat is dat het koekje alleen geldig is voor het meest recent bezochte apparaat. Alle andere apparaten die dezelfde koekjesnaam gebruiken zullen het koekje als ongeldig zien en zullen de sessie uitloggen.

16. Waarom faalt mijn externe toegangssessie met een fout als: Toegangsfout: Entiteit te groot aanvragen, HTTP-headerveld groter dan ondersteunde grootte?

Nadat u veel externe toegangssessies met verschillende apparaten hebt uitgevoerd, zal de browser een groot aantal koekjes hebben opgeslagen voor het Probe domein. Om rond dit probleem te werken, gebruikt u de knoppen van de browser om koekjes voor het domein te verwijderen en dan de pagina opnieuw te laden.

Software update

17. Hoe kan ik het Manager-besturingssysteem op de hoogte houden?

De Manager gebruikt de distributie van CentOS Linux voor een besturingssysteem. De pakketten en de kern kunnen worden bijgewerkt met behulp van de standaard CentOS-processen. Bijvoorbeeld, om een handmatige update uit te voeren, open aan de console als de gebruiker van Cisco en voer het bevel *toe zoals yum -y* update. Het systeem mag niet worden opgewaardeerd tot een nieuwe CentOS-release en er mogen geen extra pakketten worden geïnstalleerd die verder gaan dan de pakketten die zijn meegeleverd in de virtuele

machine-afbeelding die door Cisco is meegeleverd.

18. Hoe update ik Java op de Manager?

U kunt updates voor Java downloaden van Oracle en handmatig installeren met de volgende opdrachten:

U kunt een nieuw Java-pakket rechtstreeks aan de Manager downloaden:

```
curl -L-O-H "Cookie: Oraclelicense=take-SECURITY back-up-koekje" -k
http://download.oracle.com/otn-pub/java/jdk/<versie>-<build>/jre-<versie>-linux-x64.rpm
```

Hieronder zie je een voorbeeld:

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

U installeert de bijgewerkte Java-versie als volgt:

Stap 1. Verwijder de oude versie met de opdracht *sudo yum -y verwijder jre 1.8.0_102*

Stap 2. Installeer de nieuwe versie met de opdracht *sudo yum -y localinstall jre-<versie>-linux-x64.rpm*

19. Hoe hou ik het besturingssysteem van de Probe bij?

De sonde gebruikt OpenWRT voor een besturingssysteem. Ingesloten pakketten kunnen worden bijgewerkt met behulp van het **opkg-**gereedschap. Bijvoorbeeld, om alle pakketten op het systeem bij te werken, logt u in op de console als de gebruiker van Cisco en voer de opdracht update-pakketten in. Indien nodig worden de aangepaste bronnen door Cisco geleverd als onderdeel van een nieuwe versie van de Probe. Er moeten geen extra pakketten worden geïnstalleerd buiten de pakketten die zijn meegeleverd in de virtuele machine-afbeelding die door Cisco is meegeleverd.

20. Wat is de Kaseya Plugin van Cisco FindIT?

De Cisco FindIT Kaseya plug-in is ontworpen om de operationele efficiëntie te verhogen door Cisco FindIT Network Manager nauw te integreren met de Kaseya Virtual System Administrator (VSA). De Cisco FindIT Kaseya Plugin biedt krachtige functies zoals actiebeheer, dashboards, ontdekking van apparaten, netwerktopologie, afstandsbediening, actieve waarschuwingen en geschiedenis van gebeurtenissen.

De stekker is zo ontworpen dat hij bijzonder gemakkelijk kan worden geïnstalleerd, zodat u slechts een paar klikken nodig hebt. Het voldoet aan alle integratie-eisen van derden voor Kaseya op de VSA versies 9.3 en 9.4. Klik hier voor meer informatie.