Cisco FindITネットワーク管理に関するFAQ

目的

Cisco FindITネットワーク管理は、Webブラウザを使用してシスコデバイスを含むネットワーク全体を簡単に管理できるソフトウェアです。ネットワーク内でサポートされているすべてのシスコデバイスを自動的に検出、監視、および設定します。また、このソフトウェアから、ネットワーク内のファームウェアのアップデートおよび保証でサポートされなくなったデバイスに関する情報が送信されます。

Cisco FindITネットワーク管理には、次の2つのコンポーネントがあります。FindITネットワークマネージャと呼ばれる単一のマネージャと、FindITネットワークプローブと呼ばれる1つ以上のプローブ。

この記事では、Cisco FindITネットワーク管理のセットアップ、設定、およびトラブルシューティングに関するFAQとその回答について説明します。

よく寄せられる質問（FAQ）

目次

リモート アクセス

ソフトウェアの更新

全般

1. FindITネットワーク管理でサポートされている言語を教えてください。

FindITネットワーク管理は、次の言語に翻訳されています。

- 中国語
- 英語
- フランス語
- ドイツ語
- 日本語
- スペイン語

ディスカバリ

2. FindITがデバイスの管理に使用するプロトコルは何ですか。

FindITは、ネットワークの検出と管理にさまざまなプロトコルを使用します。特定のデバイスで使用されている正確なプロトコルは、デバイスタイプによって異なります。次のプロトコルがあります。

- Multicast Domain Name System(mDNS)およびDNS Service Discovery：このプロトコルはBonjourとも呼ばれます。プリンタ、他のコンピュータ、それらのデバイスがローカルネットワーク上で提供するサービスなどのデバイスを特定します。mDNSの詳細に

ついては、ここをクリックしてください。DNSサービスの検出の詳細については、ここをクリックします。

- Cisco Discovery Protocol(CDP)：オペレーティングシステムのバージョンやIPアドレスなど、直接接続されている他のシスコ機器に関する情報を共有するために使用される、シスコ独自のプロトコル。
- Link Layer Discovery Protocol(LLDP)：オペレーティングシステムのバージョンやIPアドレスなど、直接接続されている他の機器に関する情報を共有するために使用される、ベンダー中立のプロトコル。
- Simple Network Management Protocol(SNMP)：情報を収集し、インターネットプロトコル(IP)ネットワーク上のサーバ、プリンタ、ハブ、スイッチ、ルータなどのネットワークデバイスを設定するために使用されるネットワーク管理プロトコル。
- RESTCONF:Internet Engineering Task Force（IETF；インターネット技術特別調査委員会）ドラフト。Yet Another Next Generation(YANG)データモデリング言語仕様をRESTfulインターフェイスにマッピングする方法を説明します。詳細については、ここをクリックしてください。

3. FindITはどのようにネットワークを検出しますか。

FindITネットワークプローブは、CDP、LLDP、およびmDNSアドバタイズメントを受信することから、ネットワーク内のデバイスの初期リストを作成します。プローブは、サポートされているプロトコルを使用して各デバイスに接続し、CDPとLLDPの隣接関係テーブル、メディアアクセス制御(MAC)アドレステーブル、および関連するデバイスリストなどの追加情報を収集します。この情報は、ネットワーク内の追加デバイスを識別するために使用され、すべてのデバイスが検出されるまでプロセスが繰り返されます。

4. FindITはネットワークスキャンを実行しますか。

FindITはネットワークアドレス範囲をアクティブにスキャンしません。特定のネットワークプロトコルのパッシブモニタリングと、ネットワークデバイスに情報をアクティブに照会する機能を組み合わせて使用します。

ポート管理

5.ポート管理でスタックポートが表示されないのはなぜですか。

ポート管理の図は、デバイスが管理プロトコルを介して提供するポートのリストに基づいて描かれています。スタックモードでは、スタックポートはスタック内の内部接続と見なされるため、デバイスは管理プロトコルによって提供されるリストにこれらのポートを含みません。

コンフィギュレーション

6.新しいデバイスが検出されると、どうなりますか。設定は変更されますか。

新しいデバイスがデフォルトデバイスグループに追加されます。設定プロファイルがデフォルトデバイスグループに割り当てられている場合、その設定は新しく検出されたデバイスにも適用されます。

7.デバイスをあるデバイスグループから別のデバイスグループに移動するとどうなりますか。

元のデバイスグループに現在適用され、新しいデバイスグループに適用されていないプロファイルに関連付けられた仮想ローカルエリアネットワーク(VLAN)またはワイヤレスローカルエリアネットワーク(WLAN)設定は削除され、元のグループに適用されていないプロファイルに関連付けられたVLANまたはWLAN設定が追加されます。システム設定は、新しいグループに適用されたプロファイルによって上書きされます。新しいグループにシステム設定プロファイルが定義されていない場合、デバイスのシステム設定は変更されません。

セキュリティの考慮事項

8. FindIT Network Managerにはどのようなポート範囲とプロトコルが必要ですか。

次の表に、FindITネットワークマネージャで使用されるプロトコルとポートを示します。

ポート	方向	プロトコル	用途
TCP 22	Inbound	SSH	マネージャへのコマンドラインアク
TCP 80	Inbound	HTTP	マネージャへのWebアクセス。セキュアWebサーバ（ポ
TCP 443	Inbound	HTTPS	マネージャへのセキュアなWebアク
TCP 1069	Inbound	NETCONF/TLS	プローブとマネージャ間の通信
TCP 9443	Inbound	HTTPS	プローブGUIへのリモートアクセ
TCP 50000 ~ 51000	Inbound	デバイス依存	デバイスへのリモートアクセス
UDP 53	Outbound	DNS	ドメイン名の解決
UDP 123	Outbound	NTP	時間同期
UDP 5353	Outbound	mDNS	マネージャをアドバタイズするローカルネットワークへのマルチキャ

9. FindITネットワークプローブにはどのようなポート範囲とプロトコルが必要ですか。

次の表に、FindITネットワークプローブで使用されるプロトコルとポートを示します。

ポート	方向	プロトコル	
TCP 22	Inbound	SSH	
TCP 80	Inbound	HTTP	マネージャへ
TCP 443	Inbound	HTTPS	
UDP 5353	Inbound	mDNS	ローカルネットワークから
TCP 10000	Inbound	デバイス依存	

~ 10100			
UDP 53	Outbound	DNS	
UDP 123	Outbound	NTP	
TCP 80	Outbound	HTTP	セ
UDP 161	Outbound	SNMP	
TCP 443	Outbound	HTTPS	セキュアなWebサービスを有効にしたデバイスの管理。ソフトウェア
TCP 1069	Outbound	NETCONF/TLS	
UDP 5353	Outbound	mDNS	プローブをアドバタイズ

10. FindIT Network ManagerとFindIT Network Probeの間の通信の安全性はどの程度ですか。

マネージャとプローブ間のすべての通信は、クライアントおよびサーバ証明書で認証されたTransport Layer Security(TLS)1.2セッションを使用して暗号化されます。セッションはプローブからマネージャに開始されます。マネージャとプローブの関連付けが最初に確立された時点で、ユーザはプローブからマネージャにログオンする必要があります。この時点で、マネージャとプローブは証明書を交換し、将来の通信を認証します。

11. FindITはデバイスに「バックドア」アクセスできますか。

いいえ。FindITは、サポートされているシスコデバイスを検出すると、そのデバイスの工場出荷時のデフォルトのクレデンシャルを使用して、デフォルトのユーザ名とパスワードでデバイスにアクセスしようとします。cisco、またはデフォルトのSNMPコミュニティ：パブリック.デバイス設定がデフォルトから変更されている場合は、ユーザが正しいクレデンシャルをFindITに提供する必要があります。

12. FindITに保存されるクレデンシャルの安全性は？

FindITにアクセスするためのクレデンシャルは、SHA512アルゴリズムを使用して不可逆的にハッシュされます。デバイスおよびその他のサービス(**Cisco Active Advisor**など)のクレデンシャルは、AES-128アルゴリズムを使用して可逆的に暗号化されます。

13.管理GUIで失われたパスワードを回復するにはどうすればよいですか。

管理GUIですべての管理者アカウントのパスワードを失った場合は、プローブまたはマネージャのコンソールにログインし、**recoverpasswordツールを実行してパスワードをリセットできます**。このツールは、シスコアカウントのパスワードをデフォルトのciscoにリセットします。シスコアカウントが削除されている場合は、デフォルトのパスワードでアカウントを再作成します。次に、このツールを使用してパスワードをリセットするためのコマンドの例を示します。

```
cisco@FindITProbe:# recoverpassword

(y/n) y
```

```
cisco@FindITProbe:#
```

リモート アクセス

14. FindIT Network Managementからデバイスの管理GUIに接続すると、セッションは安全ですか。

FindITネットワーク管理は、デバイスとユーザ間のリモートアクセスセッションをトンネリングします。使用されるプロトコルはエンドデバイスの設定によって異なりますが、FindITは、有効になっている場合は常にセキュアなプロトコルを使用してセッションを確立します（たとえば、HTTPSはHTTPよりも優先されます）。ユーザがマネージャ経由でデバイスに接続している場合、デバイスで有効になっているプロトコルに関係なく、セッションはマネージャとプローブの間を通過するときに、暗号化されたトンネルを通過します。

15.デバイスとのリモートアクセスセッションが、別のデバイスへのリモートアクセスセッションを開いたときに、すぐにログアウトするのはなぜですか。

FindITネットワーク管理を介してデバイスにアクセスすると、ブラウザは各接続が同じWebサーバ(FindIT)に接続されていると認識するため、各デバイスから他のすべてのデバイスにCookieが表示されます。複数のデバイスが同じCookie名を使用する場合、あるデバイスCookieが別のデバイスによって上書きされる可能性があります。これはセッションCookieで最もよく見られ、その結果、Cookieは最近アクセスしたデバイスでのみ有効になります。同じCookie名を使用する他のすべてのデバイスは、Cookieが無効であると認識し、セッションをログアウトします。

16.リモートアクセスのセッションが次のようなエラーで失敗するのはなぜですか。アクセスエラー：要求エンティティが大きすぎます。HTTPヘッダーフィールドがサポートされているサイズを超えていますか？

異なるデバイスで多数のリモートアクセスセッションを行った後、ブラウザにはプローブドメイン用に大量のクッキーが保存されます。この問題を回避するには、ブラウザコントロールを使用してドメインのCookieをクリアし、ページをリロードします。

ソフトウェアの更新

17. Managerオペレーティングシステムを最新の状態に保つにはどうすればよいですか。

マネージャは、オペレーティングシステムにCentOS Linuxディストリビューションを使用します。パッケージとカーネルは、標準のCentOSプロセスを使用して更新することができます。たとえば、手動更新を実行するには、シスコユーザとしてコンソールにログオンし、コマンドsudo yum -y updateを入力します。システムを新しいCentOSリリースにアップグレードしないでください。また、シスコが提供する仮想マシンイメージに含まれるパッケージ以外に追加パッケージをインストールしないでください。

18.マネージャでJavaを更新するにはどうすればよいですか。

JavaのアップデートはOracleからダウンロードし、次のコマンドを使用して手動でインストールする必要があります。

新しいJavaパッケージをマネージャに直接ダウンロードするには：

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

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

次に例を示します。

```
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"
```

更新されたJavaバージョンをインストールするには、次の手順に従います。

ステップ1:*sudo yum -y remove jre1.8.0_102コマンドを使用して古いバージョンを削除する*

ステップ2：コマンド*sudo yum -y localinstall jre-<version>-linux-x64.rpmを使用して、新しいバージョンをインストールします*

19. Probeオペレーティングシステムを最新の状態に保つにはどうすればいいですか。

プローブは、オペレーティングシステムにOpenWRTを使用します。同梱パッケージは、opkgツールを使用して更新**することが**できます。たとえば、システム上のすべてのパッケージを更新するには、コンソールにciscoユーザとしてログインし、コマンドupdate-packagesを入力します。必要に応じて、新しいバージョンのProbeの一部として、カーネルのアップデートがシスコから提供されます。シスコが提供する仮想マシンイメージに含まれるパッケージ以外に追加パッケージをインストールしないでください。

20. Cisco FindIT Kaseya Pluginとは何ですか。

Cisco FindIT Kaseya Pluginは、Cisco FindIT Network ManagerとKaseya Virtual System Administrator(VSA)を緊密に統合することで、運用効率を向上するように設計されています。 Cisco FindIT Kaseya Pluginは、アクション管理、ダッシュボード、デバイス検出、ネットワークトポロジ、リモートデバイス管理、アクション可能なアラート、イベント履歴などの強力な機能を提供します。

プラグインは非常に簡単にインストールできるように設計されており、数回のクリックだけで済みます。これは、KaseyaオンプレミスVSAバージョン9.3および9.4のすべてのサードパーティ統合要件に準拠しています。詳細については、ここをクリックしてください。