Perguntas frequentes sobre o gerenciamento de rede Cisco FindIT

Objetivo

O Cisco FindIT Network Management é um software que permite que você gerencie facilmente toda a sua rede, incluindo seus dispositivos Cisco através do navegador da Web. Ele descobre, monitora e configura automaticamente todos os dispositivos Cisco suportados na sua rede. Este software também envia notificações sobre atualizações de firmware e informações sobre os dispositivos na rede que não são mais suportados pela garantia.

O Cisco FindIT Network Management tem dois componentes separados: um único gerente conhecido como FindIT Network Manager e um ou mais Probes conhecidos como FindIT Network Probe.

Este artigo contém as perguntas frequentes sobre configuração, configuração e solução de problemas do Cisco FindIT Network Management e suas respostas.

Perguntas mais freqüentes

Table Of Contents

Acesso Remoto

Atualização de software

General

1. Que idiomas são suportados pelo FindIT Network Management?

FindIT Network Management é traduzido para os seguintes idiomas:

- chinês
- Inglês
- Francês
- alemão
- japonês
- Espanhol

Descoberta

2. Que protocolos o FindIT usa para gerenciar meus dispositivos?

FindIT usa uma variedade de protocolos para descobrir e gerenciar a rede. O protocolo exato que está sendo usado para um dispositivo específico varia dependendo do tipo de dispositivo. Esses protocolos incluem:

- Multicast Domain Name System (mDNS) e DNS Service Discovery — esse protocolo

também é conhecido como Bonjour. Ela localiza dispositivos como impressoras, outros computadores e os serviços que esses dispositivos oferecem em uma rede local. Para saber mais sobre o mDNS, clique aqui. Para obter mais informações sobre a descoberta de serviços DNS, clique aqui.
- Cisco Discovery Protocol (CDP) — Um protocolo proprietário da Cisco usado para compartilhar informações sobre outros equipamentos Cisco diretamente conectados, como a versão do sistema operacional e o endereço IP.
- Link Layer Discovery Protocol (LLDP) — Um protocolo neutro de fornecedor usado para compartilhar informações sobre outros equipamentos diretamente conectados, como a versão do sistema operacional e o endereço IP.
- Protocolo de gerenciamento de rede simples (SNMP - Simple Network Management Protocol) — Um protocolo de gerenciamento de rede usado para coletar informações e configurar dispositivos de rede, como servidores, impressoras, hubs, switches e roteadores em uma rede IP (Internet Protocol).
- RESTCONF — Um rascunho da IETF (Internet Engineering Task Force) que descreve como mapear uma especificação de linguagem de modelagem de dados Yet Other Next Generation (YANG) para uma interface RESTful. Para saber mais, clique aqui.

3. Como o FindIT descobre minha rede?

O FindIT Network Probe cria uma lista inicial de dispositivos na rede, desde ouvir anúncios CDP, LLDP e mDNS. A sonda se conecta a cada dispositivo usando um protocolo suportado e coleta informações adicionais, como tabelas de adjacência de CDP e LLDP, tabelas de endereços de Controle de Acesso ao Meio (MAC - Media Access Control) e listas de dispositivos associadas. Essas informações são usadas para identificar dispositivos adicionais na rede e o processo se repete até que todos os dispositivos tenham sido descobertos.

4. O FindIT faz verificações de rede?

FindIT não verifica ativamente os intervalos de endereços de rede. Ele usa uma combinação de monitoramento passivo de certos protocolos de rede e consulta ativa dispositivos de rede para obter informações.

Gerenciamento de portas

5. Por que o Port Management não mostra portas de pilha?

As ilustrações do Port Management são desenhadas com base na lista de portas fornecida pelo dispositivo através dos protocolos de gerenciamento. No modo de empilhamento, as portas da pilha são consideradas como uma conexão interna na pilha, de modo que o dispositivo não inclua essas portas nas listas fornecidas através dos protocolos de gerenciamento.

Configuração

6. O que acontece quando um novo dispositivo é descoberto? Sua configuração será alterada?

Novos dispositivos serão adicionados ao grupo de dispositivos padrão. Se os perfis de configuração tiverem sido atribuídos ao grupo de dispositivos padrão, essa configuração

também será aplicada a dispositivos recém-descobertos.

7. O que acontece quando eu movo um dispositivo de um grupo de dispositivos para outro?

Qualquer configuração de Rede Local Virtual (VLAN) ou Rede Local Sem Fio (WLAN) associada a perfis atualmente aplicados ao grupo de dispositivos original e não aplicados ao novo grupo de dispositivos será removida e a configuração de VLAN ou WLAN associada a perfis que são aplicados ao novo grupo e não são aplicados ao grupo original será adicionada ao dispositivo. As configurações do sistema serão substituídas por perfis aplicados ao novo grupo. Se nenhum perfil de configuração do sistema for definido para o novo grupo, a configuração do sistema para o dispositivo não será alterada.

Consideração de segurança

8. Quais intervalos de portas e protocolos são necessários para o FindIT Network Manager?

A tabela a seguir contém os protocolos e as portas usados pelo FindIT Network Manager:

Porta	Direção	Protocolo	Uso
TCP 22	Entrada	SSH	Acesso de linha de comando ao gerente
TCP 80	Entrada	HTTP	Acesso à Web para o Gerente. Redireciona para o servidor web seguro (porta 443)
TCP 443	Entrada	HTTPS	Acesso seguro à Web para o Manager
TCP 1069	Entrada	NETCONF/TLS	Comunicação entre o testador e o gerente
TCP 9443	Entrada	HTTPS	Acesso remoto à GUI do teste
TCP 50000-51000	Entrada	Dependente do dispositivo	Acesso remoto a dispositivos
UDP 53	Saída	DNS	Resolução de nomes de domínio
UDP 123	Saída	NTP	Sincronização de tempo
UDP 5353	Saída	mDNS	Anúncios de serviço DNS multicast para rede local anunciando o Gerente

9. Quais intervalos de portas e protocolos são exigidos pelo FindIT Network Probe?

A tabela a seguir lista os protocolos e portas usados pelo FindIT Network Probe:

Porta	Direção	Protocolo	Uso
TCP 22	Entrada	SSH	Acesso à linha de comando para a sonda
TCP 80	Entrada	HTTP	Acesso à Web para o Gerente. Redireciona para o servidor web seguro (porta 443)
TCP 443	Entrada	HTTPS	Acesso seguro à Web para o Manager
UDP 5353	Entrada	mDNS	Anúncios de serviço DNS multicast da rede local. Usado para descoberta

			de dispositivos.
TCP 10000-10100	Entrada	Dependente do dispositivo	Acesso remoto a dispositivos
UDP 53	Saída	DNS	Resolução de nomes de domínio
UDP 123	Saída	NTP	Sincronização de tempo
TCP 80	Saída	HTTP	Gerenciamento de dispositivos sem habilitação de serviços da Web seguros
UDP 161	Saída	SNMP	Gerenciamento de dispositivos de rede
TCP 443	Saída	HTTPS	Gerenciamento de dispositivos com serviços da Web seguros habilitados. Acesse os serviços da Web da Cisco para obter informações como atualizações de software, suporte, status e avisos de fim da vida útil
TCP 1069	Saída	NETCONF/TLS	Comunicação entre o testador e o gerente
UDP 5353	Saída	mDNS	Anúncios de serviço DNS multicast para a rede local anunciando o Probe

10. Qual é a segurança da comunicação entre o FindIT Network Manager e o FindIT Network Probe?

Toda comunicação entre o Gerente e o Sonda é criptografada usando uma sessão TLS (Transport Layer Security) 1.2 autenticada com certificados de cliente e servidor. A sessão é iniciada do Teste para o Gerente. No momento em que a associação entre o Gerente e a Sonda é estabelecida pela primeira vez, o usuário deve fazer logon no Gerente a partir da Sonda, momento em que o Gerente e a Sonda trocam certificados para autenticar futuras comunicações.

11. O FindIT tem acesso "backdoor" aos meus dispositivos?

Não. Quando o FindIT descobrir um dispositivo da Cisco suportado, tentará aceder ao dispositivo utilizando as credenciais predefinidas de fábrica para esse dispositivo com o nome de utilizador e a senha predefinidos: cisco ou a comunidade SNMP padrão: público. Se a configuração do dispositivo tiver sido alterada do padrão, será necessário que o usuário forneça as credenciais corretas ao FindIT.

12. Qual é a segurança das credenciais armazenadas no FindIT?

As credenciais para acessar o FindIT são irreversivelmente gravadas usando o algoritmo SHA512. As credenciais para dispositivos e outros serviços, como o **Cisco Ative Advisor**, são criptografadas reversivelmente usando o algoritmo AES-128.

13. Como recupero uma senha perdida para a GUI de administração?

Se você tiver perdido a senha para todas as contas de administrador na GUI da Administração, poderá redefinir a senha fazendo login no console do Teste ou do Gerente e executando a ferramenta **recovery password**. Essa ferramenta redefine a senha da conta cisco para o padrão cisco ou, se a conta cisco tiver sido removida, recriará a conta com a senha padrão. Veja a seguir um exemplo dos comandos a serem fornecidos para redefinir a

senha usando essa ferramenta.

```
cisco@FindITProbe:~# senha de recuperação

Tem certeza? (s/n) y

Redefina a conta cisco para a senha padrão

cisco@FindITProbe:~#
```

Acesso Remoto

14. Quando me conecto à GUI de administração de um dispositivo do FindIT Network Management, a sessão é segura?

FindIT Network Management tunela a sessão de acesso remoto entre o dispositivo e o usuário. O protocolo usado dependerá da configuração do dispositivo final, mas FindIT sempre estabelecerá a sessão usando um protocolo seguro se um estiver ativado (por exemplo, HTTPS será preferido em vez de HTTP). Se o usuário estiver se conectando ao dispositivo através do Gerenciador, a sessão passará por um túnel criptografado à medida que passa entre o Gerenciador e o Sonda, independentemente dos protocolos ativados no dispositivo.

15. Por que minha sessão de acesso remoto com um dispositivo faz logoff imediatamente quando eu abro uma sessão de acesso remoto para outro dispositivo?

Quando você acessa um dispositivo por meio do FindIT Network Management, o navegador vê cada conexão como estando com o mesmo servidor Web (FindIT) e, portanto, apresentará cookies de cada dispositivo para cada dispositivo. Se vários dispositivos usarem o mesmo nome de cookie, há a possibilidade de um cookie de dispositivo ser substituído por outro dispositivo. Isso é visto com mais frequência com cookies de sessão, e o resultado é que o cookie só é válido para o dispositivo visitado mais recentemente. Todos os outros dispositivos que usam o mesmo nome de cookie verão o cookie como inválido e encerrarão a sessão.

16. Por que minha sessão de acesso remoto falha com um erro como este: Erro de acesso: Entidade de solicitação muito grande, campo cabeçalho HTTP excede o tamanho suportado?

Depois de realizar muitas sessões de acesso remoto com dispositivos diferentes, o navegador terá um grande número de cookies armazenados para o domínio de Investigação. Para contornar esse problema, use os controles do navegador para limpar cookies para o domínio e, em seguida, recarregue a página.

Atualização de software

17. Como manter o sistema operacional do gerente atualizado?

O gerente usa a distribuição do CentOS Linux para um sistema operacional. Os pacotes e o kernel podem ser atualizados usando os processos padrão CentOS. Por exemplo, para executar uma atualização manual, faça logon no console como o usuário da cisco e digite o comando *sudo yum -y* update. O sistema não deve ser atualizado para uma nova versão do CentOS, e nenhum pacote adicional deve ser instalado além dos incluídos na imagem da

máquina virtual fornecida pela Cisco.

18. Como atualizo o Java no Gerenciador?

As atualizações para Java devem ser baixadas da Oracle e instaladas manualmente usando os seguintes comandos:

Para fazer o download de um novo pacote Java diretamente no Gerenciador:

```
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
```

A seguir, está um exemplo:

```
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"
```

Para instalar a versão Java atualizada:

Etapa 1. Remova a versão antiga com o comando *sudo yum -y remove jre1.8.0_102*

Etapa 2. Instale a nova versão com o comando *sudo yum -y localinstall jre-<version>-linux-x64.rpm*

19. Como manter o sistema operacional Probe atualizado?

A sonda usa o OpenWRT para um sistema operacional. Os pacotes incluídos podem ser atualizados usando a ferramenta **opkg**. Por exemplo, para atualizar todos os pacotes no sistema, faça logon no console como o usuário cisco e insira o comando update-packages. Quando necessário, as atualizações do kernel serão fornecidas pela Cisco como parte de uma nova versão do Probe. Nenhum pacote adicional deve ser instalado além dos incluídos na imagem da máquina virtual fornecida pela Cisco.

20. O que é o plug-in Kaseya do Cisco FindIT?

O plug-in Kaseya do Cisco FindIT foi projetado para aumentar a eficiência operacional integrando firmemente o Cisco FindIT Network Manager com o Kaseya Virtual System Administrator (VSA). O plug-in Kaseya do Cisco FindIT oferece recursos poderosos, incluindo gerenciamento de ações, painéis, descoberta de dispositivos, topologia de rede, gerenciamento remoto de dispositivos, alertas acionáveis e histórico de eventos.

O plugin foi projetado para ser extremamente fácil de instalar, exigindo apenas alguns cliques. Ele atende a todos os requisitos de integração de terceiros para o Kaseya in-loco VSA versões 9.3 e 9.4. Para saber mais, clique aqui.