

Perguntas frequentes sobre o Cisco Business Dashboard

Objetivo

O Cisco Business Dashboard Network Management é um software que permite que você gerencie facilmente toda a sua rede, incluindo seus dispositivos da 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.

Este artigo contém as respostas às perguntas frequentes sobre configuração, configuração e solução de problemas do Cisco Business Dashboard Network Management.

Perguntas mais freqüentes

Table Of Contents

General

1. [Que idiomas são suportados pelo Cisco Business Dashboard Network Management?](#)

Descoberta

2. [Quais protocolos o Cisco Business Dashboard usa para gerenciar meus dispositivos?](#)
3. [Como o Cisco Business Dashboard descobre minha rede?](#)
4. [O Cisco Business Dashboard faz verificações de rede?](#)

Configuração

5. [O que acontece quando um novo dispositivo é descoberto? Sua configuração será alterada?](#)
6. [O que acontece quando eu movo um dispositivo de um grupo de dispositivos para outro?](#)

Considerações sobre segurança

7. [Quais intervalos de portas e protocolos são exigidos pelo Cisco Business Dashboard Network Manager?](#)
8. [Quais intervalos de portas e protocolos são exigidos pelo Cisco Business Dashboard Network Probe?](#)
9. [Qual é a segurança da comunicação entre o Cisco Business Dashboard e o Cisco Business Dashboard Probe?](#)
10. [O Cisco Business Dashboard tem acesso "backdoor" a meus dispositivos?](#)
11. [Qual é a segurança das credenciais armazenadas no Cisco Business Dashboard?](#)

12. [Como recupero uma senha perdida para a interface do usuário da Web?](#)
13. [Qual é o nome de usuário e a senha padrão do carregador de inicialização da Máquina virtual?](#)

Acesso Remoto

14. [Quando me conecto à interface do usuário da Web de um dispositivo do Cisco Business Dashboard Network Management, a sessão é segura?](#)
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?](#)
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?](#)

Atualização de software

17. [Como manter o sistema operacional Paineis atualizado?](#)
18. [Como atualizo o Java no painel?](#)
19. [Como manter o sistema operacional Probe atualizado?](#)
20. [Como manter o sistema operacional da Sonda atualizado ao usar um Raspberry Pi?](#)

General

[1. Que idiomas são suportados pelo Cisco Business Dashboard Network Management?](#)

O Cisco Business Dashboard Network Management é traduzido para os seguintes idiomas:

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

Descoberta

[2. Quais protocolos o Cisco Business Dashboard usa para gerenciar meus dispositivos?](#)

O Cisco Business Dashboard 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 Cisco Business Dashboard descobre minha rede?](#)

O Cisco Business Dashboard Probe cria uma lista inicial de dispositivos na rede, desde a escuta de 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 Cisco Business Dashboard faz verificações de rede?](#)

O Cisco Business Dashboard não verifica ativamente a rede mais ampla. A sonda usará o protocolo ARP para verificar a sub-rede IP à qual está diretamente conectada, mas não tentará verificar nenhum outro intervalo de endereços. O teste também testará cada dispositivo descoberto quanto à presença de um servidor Web e de um servidor SNMP nas portas padrão.

Configuração

[5. 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.

[6. 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

[7. Quais intervalos de portas e protocolos são exigidos pelo Cisco Business Dashboard Network Manager?](#)

A tabela a seguir contém os protocolos e as portas usados pelo Cisco Business Dashboard:

Porta	Direção	Protocolo	Uso
TCP 22	Entrada	SSH	Acesso de linha de comando ao Painel. O SSH é desabilitado por padrão na imagem da máquina virtual Cisco.
TCP 80	Entrada	HTTP	Acesso à Web para o Painel. Redireciona para o servidor web seguro (porta 443).
TCP 443	Entrada	TCP multiplexado HTTPS	Acesso seguro à Web para o Painel. Comunicação entre a sonda e o painel.
TCP 50000 - 51000	Entrada	HTTPS	Acesso remoto a dispositivos.
TCP 53	Saída	DNS	Resolução de nome de domínio.
UDP 123	Saída	NTP	Sincronização de hora.
TCP 443	Saída	HTTPS	Acesse os serviços da Web da Cisco para obter informações como atualizações de software, status de suporte e avisos de fim da vida útil. Acesse o SO e os serviços de atualização de aplicativos.
UDP 5353	Saída	mDNS	Anúncios de serviço DNS multicast para rede local anunciando o Gerente

[8. Quais intervalos de portas e protocolos são exigidos pelo Cisco Business Dashboard Probe?](#)

A tabela a seguir lista os protocolos e portas usados pelo Cisco Business Dashboard Probe:

Porta	Direção	Protocolo	Uso
TCP 22	Entrada	SSH	Acesso à linha de comando para o teste. O SSH é desabilitado por padrão na imagem da máquina virtual Cisco.
TCP 80	Entrada	HTTP	Acesso à Web para o teste. Redireciona para o servidor web seguro (porta 443)
TCP 443	Entrada	HTTPS	Acesso seguro à Web para o Probe.
UDP 5353	Entrada	mDNS	Anúncios de serviço DNS multicast da rede local. Usado para descoberta de 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 serviços seguros da Web ativados.
UDP 161	Saída	SNMP	Gerenciamento de dispositivos de rede
TCP 443	Saída	TCP multiplexado HTTPS	Gerenciamento de dispositivos com serviços da Web seguros habilitados. Acesse os serviços da Web da Cisco para obter informações como atualizações de software, status de suporte e avisos de fim da vida útil. Acesse o SO e os serviços de atualização de

UDP Saída mDNS
5353

aplicativos.
Comunicação entre a sonda e o painel.
Anúncios de serviço DNS multicast para a rede local
anunciando o teste.

9. Qual é a segurança da comunicação entre o Cisco Business Dashboard Network Manager e o Cisco Business Dashboard Probe?

Toda comunicação entre o Painel e o Teste é criptografada usando uma sessão TLS 1.2 autenticada com certificados de cliente e servidor. A sessão é iniciada do Teste para o Painel. No momento em que a associação entre o Painel e o Teste é estabelecida pela primeira vez, o usuário deve fazer login no Painel por meio do Teste.

10. O Cisco Business Dashboard tem acesso "backdoor" a meus dispositivos?

Não. Quando o Cisco Business Dashboard descobrir um dispositivo da Cisco suportado, tentará acessar 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 Cisco Business Dashboard.

11. Qual é a segurança das credenciais armazenadas no Cisco Business Dashboard?

As credenciais para acessar o Cisco Business Dashboard são hash irreversível usando o algoritmo SHA512. As credenciais para dispositivos e outros serviços, como o **Cisco Active Advisor**, são criptografadas reversivelmente usando o algoritmo AES-128.

12. Como recupero uma senha perdida para a interface do usuário da Web?

Se você tiver perdido a senha para todas as contas de administrador na IU da Web, poderá redefinir a senha fazendo login no console da Sonda e executando a ferramenta **cbdprobe recovery password**, ou fazendo login no console da Sonda e executando a **ferramenta cisco-business-dashboard 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@cisco-business-dashboard:~$ cisco-business-dashboard - senha de recuperação Tem certeza?  
(s/n) y Recuperada a conta da cisco para a senha padrão senha de recuperação do Cisco Business  
Dashboard bem-sucedida! cisco@Cisco Business DashboardProbe:~$
```

Ao usar o Cisco Business Dashboard para AWS, a senha será definida como a ID da instância do AWS.

13. Qual é o nome de usuário e a senha padrão do carregador de inicialização da Máquina virtual?

As credenciais padrão para o carregador de inicialização da Máquina virtual são nome de usuário: **raiz** e senha: **cisco**. Eles podem ser alterados executando a ferramenta `config_vm` e respondendo `yes` quando solicitado se você deseja alterar a senha do carregador de inicialização.

Acesso Remoto

14. Quando me conecto à interface do usuário da Web de um dispositivo do Cisco Business Dashboard Network Management, a sessão é segura?

O Cisco Business Dashboard conecta a sessão de acesso remoto entre o dispositivo e o usuário. O protocolo usado entre o testador e o dispositivo dependerá da configuração do dispositivo final, mas o Cisco Business Dashboard sempre estabelecerá a sessão usando um protocolo seguro se um estiver ativado (por exemplo, o HTTPS será preferido em relação ao HTTP). Se o usuário estiver se conectando ao dispositivo através do Painel, a sessão passará por um túnel criptografado à medida que passa entre o Painel e a Sonda, independentemente dos protocolos ativados no dispositivo. A conexão entre o navegador da Web do usuário e o painel sempre será HTTPS.

[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 Cisco Business Dashboard, o navegador vê cada conexão como estando com o mesmo servidor Web (o Painel) e, portanto, apresentará cookies de cada dispositivo para cada dispositivo. Se vários dispositivos usarem o mesmo nome de cookie, há a possibilidade de o cookie de um 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 farão logoff da sessão.

[16. Por que minha sessão de acesso remoto falha com um erro como este: Erro de acesso: Entidade de Solicitação Muito Grande, Campo de Cabeçalho HTTP excede 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 Painel. 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 Painel atualizado?](#)

O painel usa a distribuição Ubuntu Linux para um sistema operacional. Os pacotes e o kernel podem ser atualizados usando os processos padrão do Ubuntu. Por exemplo, para executar uma atualização manual, faça logon no console como o usuário cisco e insira os comandos:

```
sudo apt-get update e sudo apt-get upgrade
```

O sistema não deve ser atualizado para uma nova versão do Ubuntu, e recomenda-se que nenhum pacote adicional seja instalado além dos incluídos na imagem da máquina virtual fornecida pela Cisco ou dos instalados como parte de uma instalação mínima do Ubuntu.

[18. Como atualizo o Java no painel?](#)

O Cisco Business Dashboard usa os pacotes OpenJDK dos repositórios Ubuntu. O OpenJDK será atualizado automaticamente como parte da atualização do sistema operacional principal.

[19. Como manter o sistema operacional Probe atualizado?](#)

O Cisco Business Dashboard usa a distribuição Ubuntu Linux para um sistema operacional. Os pacotes e o kernel podem ser atualizados usando os processos padrão do Ubuntu. Por exemplo,

para executar uma atualização manual, faça login no console como o usuário da cisco e insira os comandos:

```
sudo apt-get update
```

e

```
sudo apt-get upgrade
```

O sistema não deve ser atualizado para uma nova versão do Ubuntu, e recomenda-se que nenhum pacote adicional seja instalado além dos incluídos na imagem da máquina virtual fornecida pela Cisco ou dos instalados como parte de uma instalação mínima do Ubuntu.

[20. Como manter o sistema operacional da Sonda atualizado ao usar um Raspberry Pi?](#)

Os pacotes e o kernel Raspbian podem ser atualizados usando os processos padrão usados para as distribuições Linux baseadas em Debian. Por exemplo, para executar uma atualização manual, faça login no console como o usuário da cisco e insira os comandos:

```
sudo apt-get update
```

e

```
sudo apt-get upgrade
```

O sistema não deve ser atualizado para uma nova versão principal do Raspbian. Recomenda-se que nenhum pacote adicional seja instalado além dos instalados como parte da versão 'Lite' da distribuição Raspbian e dos pacotes adicionados pelo instalador do Probe.