ネットワーク推論機能を使用したネットワークデバイスのトラブルシューティング

ネットワーク推論機能の概要

ネットワーク推論機能ツールを使用すると、ネットワークのさまざまな問題を迅速にトラブルシューティングできます。メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択すると、ネットワーク推論機能ダッシュボードが起動します。ネットワーク推論機能ダッシュボードには、ネットワークの問題を事前にトラブルシューティングできる個別のワークフローが用意されています。ダッシュボードには、ワークフローに関する簡単な説明、過去 24 時間に影響を受けたデバイスの数、およびワークフローをネットワークで実行した場合の影響が表示されます。

（注） ネットワーク推論機能を使用するには機械推論パッケージをインストールする必要があり、インストールされていないと [Tools] メニューに表示されません。詳細については、*Cisco DNA Center* 管理者ガイドを参照してください。

MRE ワークフローを使用した Cisco SD-Access 移行の検証

次の機械推論エンジン（MRE）ワークフローは、Cisco SD-Access への移行を計画する際に役立ちます。

- SDA ハードウェアの準備状況チェック
- SDA ソフトウェアの準備状況チェック
- 冗長リンクチェック
- L3 アクセスチェック
- MTU リンクチェック
- SDA 正常性チェック
- SDA スケール制限チェック

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Reasoner] ダッシュボードで、必要に応じて次のワークフローをクリックします。

ワークフロー	説明	操作
SDA ハードウェアの準備状況チェック	ハードウェアが Cisco SD-Access の移行準備ができているかどうかを確認します。	1. [SDA Hardware Readiness Check] をクリックします。 2. [Run Machine Reasoning] をクリックします。
SDA ソフトウェアの準備状況チェック	ソフトウェアが Cisco SD-Access の移行準備ができているかどうかを確認します。	1. [SDA Software Readiness Check] をクリックします。 2. [Run Machine Reasoning] をクリックします。

ワークフロー	説明	操作
冗長リンクチェック	デバイスに冗長アップリンクが存在するかどうか、およびアクセススイッチで冗長アップリンクを設定して可用性を向上させる方法があるかどうかを確認します。	**1.** [Redundant Link Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
L3 アクセスチェック	最小限の設計変更で Cisco SD-Access に移行するレイヤ 3 ルーティングプロトコルを実行しているアクセススイッチがネットワークにあるかどうかを確認します。	**1.** [L3 Access Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
MTU リンクチェック	メインのネットワークデバイスとアクセス、コア、およびその他のスイッチ間のリンクが正しいMTUで設定されているかどうかを確認します。	**1.** [MTU Link Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
SDA 正常性チェック：ファブリック数	Cisco DNA Center クラスタの正常性をチェックし、ファブリックの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Fabric Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：SDA スケール制限チェック	Cisco DNA Center に設定されているクライアントエンドポイント、ネットワークデバイス、およびファブリックの数が、公開されている SDA の制限内であるかどうかを確認します。	**1.** [SDA Scale Limits Check] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：クライアント数	Cisco DNA Center クラスタの正常性をチェックし、クライアントの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Client Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：デバイス数	Cisco DNA Center クラスタの正常性をチェックし、ネットワークデバイスの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Device Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。

CPU 使用率が高い場合のトラブルシューティング

CPU 使用率のトラブルシューティングは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 3650 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [CPU Utilization] タブをクリックします。

[CPU Utilization] ウィンドウには、過去 24 時間の CPU 使用率が高いデバイスのフィルタ処理されたリストが表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、[CPU Utilization Threshold] にチェックする使用率を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

（注） 次のプロセスが確認されると、詳細な分析の対象となります。

- [MATM Process Group]：MATM RP Shim、NGWC Learning、VMATM Callback
- [IOSXE Process Group]：IP Input、ARP Input、IOSXE-RP Punt Se、SISF Main Thread、DAI Packet、ARP Snoop

[CPU Utilization] ウィンドウでは、選択したデバイスの CPU 使用率が高い原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、CPU の消費が多いプロセスとその使用率を確認します。

ステップ 9 それぞれのプロセスについて、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

電源障害のトラブルシューティング

電源トラブルシューティング ワークフローは、ソフトウェアバージョン 16.6.1 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Power Supply] タブをクリックします。

[Power Supply] ウィンドウに、過去 24 時間に電源障害が発生したデバイスのフィルタ処理されたリストが表示されます。

インベントリ内のすべてのデバイスのリストを表示するには、[All] をクリックします。ワークフローを実行する任意のデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力してデバイスをフィルタ処理します。

ステップ 4 [Troubleshoot] をクリックします。

[Power Supply] ウィンドウで、選択したデバイスの電源障害の原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 5 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 6 [Conclusion] タブをクリックして、選択したデバイスの電源の [Stack Identifier]、[Product ID]、[Serial Number]、および [Status] の情報と推奨されるアクションを確認します。

ステップ 7 それぞれのスタック識別子について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 8 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

インターフェイスが停止した場合のトラブルシューティング

インターフェイス ダウン トラブルシューティング ワークフローは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Interface Down] タブをクリックします。

[Interface Down] ウィンドウには、過去 24 時間にインターフェイスが停止したデバイスのフィルタ処理されたリストが表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、問題が疑われるインターフェイスの名前を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

[Interface Down] ウィンドウには、選択したデバイスのインターフェイスが停止する原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、インターフェイスが停止する問題についての考えられる根本原因と推奨されるアクションを確認します。

ステップ 9 それぞれの根本原因分析について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティングプロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

ネットワーク接続のトラブルシューティング

Cisco IOS-XE ソフトウェアバージョン 16.9.3 以降を実行している次のネットワークデバイスでのみ、ネットワーク接続のトラブルシューティングがサポートされています。

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ
- Cisco Catalyst 9600 シリーズ スイッチ

次の手順を使用して、IP アドレスを使用してデバイスからエンドポイントの到達可能性を確認します。

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Connectivity] タブをクリックします。

ステップ 3 **デバイス名**、**IP アドレス**、**デバイスタイプ**、**サイト**、**到達可能性**、**ロール**、**プラットフォーム**などの詳細情報を含むデバイステーブルを表示できます。

ステップ 4 デバイスを選択して、[Troubleshoot] を選択します。

ステップ 5 [Reasoner Inputs] ウィンドウの [Destination IP address] フィールドに有効な IP アドレスを入力し、[Run Machine Reasoning] をクリックします。

（注） Virtual Routing and Forwarding（VRF）の名前を入力します（該当する場合）。

ステップ 6 [Root Cause Analysis] ウィンドウの [Reasoning Activity] で、トラブルシューティング プロセスの一環として検証されるさまざまなワークフローを確認できます。

ステップ 7 [Conclusions] タブで、検証チェックのステータスと推奨アクションを確認できます。

デバイスの IP 接続のトラブルシューティング

ping はシンプルなコマンドであるため、すべてのネットワークデバイスで IP 接続のトラブルシューティングをサポートできます。

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Reasoner] ダッシュボードで、[Ping Device] をクリックします。

ステップ 3 [Devices] ウィンドウで、デバイスを選択し、[Troubleshoot] をクリックします。

ステップ 4 [Reasoner Inputs] ウィンドウで、[Target IP Address] に値を入力し、[Run Machine Reasoning] をクリックします。

ステップ 5 [View Details] をクリックして、ping ステータスを確認します。

MRE ワークフローを使用したワイヤレスクライアントのトラブルシューティング

この手順を使用して、MRE ワークフローを使用してワイヤレスクライアントの問題をトラブルシューティングします。

（注）
- ワイヤレスクライアントのトラブルシューティング ワークフローのサポートは、Cisco IOS-XE ソフトウェアバージョン 17.3.4 以降のネットワークデバイスでのみ使用できます。
- MRE ワークフローは HA をサポートしていません。つまり、ワークフロー中に切り替えが発生した場合は、ワークフローをやり直す必要があります。

始める前に

機械推論エンジン（MRE）ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco DNA Center* 管理者ガイド』の「Update the Machine Reasoning Knowledge Base」[英語] のトピックを参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、[Tools] > [Network Reasoner] の順に選択します。

ステップ 2 [Wireless Client Data Collection] タイルをクリックします。
[Devices] ウィンドウに、フィルタリングされたワイヤレス コントローラ デバイスが表示されます。

ステップ 3 トラブルシューティングするワイヤレスコントローラを選択し、[Troubleshoot] をクリックします。

ステップ 4 **[Reasoner Inputs]** ウィンドウで、次のフィールドに値を入力します。

- [Troubleshoot Duration]
- [Client MAC Address]
- [PCAP Interface]：ドロップダウン矢印をクリックし、リストからインターフェイスを選択します。パケットキャプチャが必要な場合は、このオプションを使用します。

ステップ 5 [Run Machine Reasoning] をクリックします。
[Wireless Client Data Collection] スライドインペインが表示されます。

ステップ 6 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。必要に応じて、[Stop] をクリックして進行中の推論アクティビティを停止します。

ステップ 7 トラブルシューティング処理が完了するまで待ちます。完了したら、[Conclusions] タブでトラブルシューティング ファイルを表示できます。

ステップ 8 （任意）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 9 （任意） ワイヤレスクライアントのトラブルシューティング ワークフローを開始すると、[Wireless Client Data Collection] slide-in paneで最新のトラブルシューティング ファイルを表示できます。

MRE ワークフローを使用した無線 AP のトラブルシューティング

この手順により、MRE ワークフローを使用して無線クライアントの問題をトラブルシュートします。

（注）
- 無線 AP のトラブルシューティングをするワークフローは、Cisco IOS-XE 17.3.4 以降を搭載したネットワークデバイスでのみ使用できます。
- MRE ワークフローは HA をサポートしていません。つまり、ワークフロー中に切り替えが発生した場合は、ワークフローをやり直す必要があります。

始める前に

MRE ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco DNA Center Administrator Guide*』の「Update the Machine Reasoning Knowledge Base」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Wireless Client Data Collection] タイルをクリックします。

ステップ 3 [Devices] ウィンドウに、フィルタリングされたワイヤレス コントローラ デバイスが表示されます。AP についてトラブルシュートするワイヤレス コントローラ デバイスを選択し、[Troubleshoot] をクリックします。

ステップ 4 **[Reasoner Inputs]** ウィンドウで、次のフィールドに値を入力します。

- [Troubleshoot Duration]
- [Two AP MAC Address]：AP の MAC アドレス（イーサネットと無線）を入力します。
- パケットキャプチャが必要な場合は、次のオプションを使用します。
  - [PCAP Interface]：ドロップダウンリストをクリックし、インターフェイスを選択します。
  - [AP IP Address]：AP の IP アドレスを入力します。
- **AP 名**

ステップ 5 [Run Machine Reasoning] をクリックします。
[Wireless AP Data Collection] slide-in paneが表示されます。

ステップ 6 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。必要に応じて、[Stop] をクリックして進行中の推論アクティビティを停止します。

ステップ 7 トラブルシューティング処理が完了するまで待ちます。完了したら、[Conclusions] タブでトラブルシューティング ファイルを表示できます。

ステップ 8 （任意） 同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 9 （任意） 無線 AP トラブルシューティング ワークフローを開始すると、[Wireless AP Data Collection] slide-in paneに 1 つ前のトラブルシューティングファイルが表示されます。

MRE ワークフローを使用したモニター対象外のデバイスのトラブルシューティング

この手順を使用して、監視されていないデバイスまたは アシュアランス データが表示されないデバイスのトラブルシューティングを行います。監視されていないデバイスのトラブルシューティング ワークフローは、スイッチ、Cisco AireOS ワイヤレスコントローラ、および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のみをサポートします。

始める前に

機械推論エンジン（MRE）ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco DNA Center* 管理者ガイド』の「Update the Machine Reasoning Knowledge Base」[英語] のトピックを参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Assurance Telemetry Analysis] タイルをクリックします。

ステップ 3 [Devices] ウィンドウには、監視されていないデバイスがフィルタリングされて表示されます。トラブルシューティングするデバイスを選択し、[Troubleshoot] をクリックします。

[Assurance Telemetry Analysis] slide-in pane が表示されます。[Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 4 進行中の推論アクティビティを停止するには、[Stop] をクリックします。

トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。

ステップ 5 **[Show Details]** をクリックします。

ステップ 6 [Conclusions] タブでトラブルシューティング ファイルを表示できます。問題はアイコン（⚠）で強調表示され、問題の下に [Suggested Action] が表示されます。

提示された推奨案を使用して、監視されていないデバイスのトラブルシューティングを行うことができます。

ステップ 7 同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 8 [Inventory] タブからデバイスのトラブルシューティングを行うこともできます。下にスクロールして [Health Score] 列を表示します。[Health Score] 列の下の [No Health] をクリックし、[View Assurance Telemetry Analysis] をクリックして、トラブルシューティング プロセスを実行します。

ネットワークのバグのスキャン

Cisco DNA Center のネットワークバグ ID ツールを使用すると、ネットワークをスキャンして、以前に識別され、シスコが認識している、選択された一連の障害またはバグを検出することができます。

Cisco DNA Center のネットワークバグ ID は、デバイス設定またはデバイスの動作データ内の特定パターンを識別するために役立ちます。それらのパターンに基づいて、既知の障害と照合することができます。このツールは、バグに焦点を合わせたビューとデバイスに焦点を合わせたビューの両方を提供します。

Cisco DNA Center は、ネットワークデバイスで CLI コマンドを実行してネットワークデバイスの構成と運用データを収集し、その情報を CX Cloud に送信して処理することで、潜在的なセキュリティアドバイザリやバグの公開に使用されます。Cisco DNA Center はネットワークバグ識別ツールの次の CLI コマンドを呼び出します。

- **show buffers summary**
- **show cef interfaces**
- **show clock**
- **show crypto eli all**
- **show crypto isakmp sa detail**
- **show eigrp service-family ipv4 neighbors**
- **show environment all**
- **show interfaces counters error**
- **show interfaces summary**
- **show inventory**
- **show ip interface brief**
- **show ip nat translations verbose**
- **show ip nbar protocol-discovery**
- **show ip nbar resources flow**
- **show ip nhrp**
- **show ip nhrp summary**
- **show ip route**
- **show ip ssh**
- **show ip vrf**
- **show logging**
- **show performance monitor cache detail**

- **show platform software route-map fp active map**
- **show pnp profile**
- **show redundancy**
- **show redundancy application group**
- **show running-config all**
- **show scp status**
- **show stackwise-virtual**
- **show startup-config**
- **show terminal**
- **show version**

次の手順では、ネットワークバグ識別ツールを使用してバグを識別する方法について説明します。

始める前に

- Cisco DNA Center のコアパッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Bug Identifier] を選択します。

ステップ 3 [Scan Network] をクリックします。

ステップ 4 [Scan Network] ウィンドウで、システムのバグを今すぐスキャンする（[Now]）か、後で実行するようにスケジュールする（[Later]）かを選択します。

ダッシュボードの進捗状況インジケータには、スキャンされたデバイスのリスト（10 台ずつ）が表示されます。スキャンが完了すると、[Network Bug Identifier] ウィンドウが表示されます。

ステップ 5 上部のペインを使用して、次のようにスキャンの結果に関する情報の表示、ネットワークの再スキャン、スキャン設定の変更を行います。

アイテム	説明
Bug Summary	ネットワーク内の [Catastrophic]、[Severe]、および [Moderate] のバグの数。
該当デバイス	スキャンされた次のデバイスタイプの数： • **Routers** • **スイッチとハブ**

アイテム	説明
Scan Mode	スキャンの実行に使用された方法： • **Essential**：Cisco Network Reasoner Engine（NRE）を使用して実行されるスキャン。 • **CX Cloud**：CX Cloud を使用して実行されるスキャン。
Re-scan Network	このボタンをクリックして、ネットワークを再度スキャンします。
Settings	[Settings] アイコンをクリックして、次の操作を行います。 • 毎週のスキャンを有効または無効にします。 • CX Cloud によるネットワークのスキャンを有効または無効にします。

ステップ 6 [Bugs on Devices] タブをクリックして、バグに関する情報を表示します（[Bug ID]、[Name]、[Affected Devices]、[Severity]、[Affected Versions]、[Workaround] など）。

ハイパーリンクされた値をクリックすると、その値に関する詳細が表示されます。

ステップ 7 [Devices] タブをクリックして、デバイスに関する情報を表示します（[Device Name]、[Image Version]、[IP Address]、[Device Type]、[Bugs]、[Scan Status]、[Scan Mode]、[Site]、[Reachability] など）。

ハイパーリンクされた値をクリックすると、その値に関する詳細が表示されます。

ステップ 8 [Devices] タブで、[Tag Device] をクリックして、デバイスのタグを作成、編集、または削除します。

Cisco DNA Center のバグのスキャン

システムバグ ID ツールには、Cisco DNA Center のバグを識別するためのオプションがあります。次の手順では、**システムバグ ID** ツールを有効にする方法について説明します。

始める前に

- Cisco DNA Center のコアパッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [System Bug Identifier] を選択します。

ステップ 3 [Scan System] をクリックします。

ステップ 4 **[Scan System]** ウィンドウで、システムのバグを今すぐスキャンする（**[Now]**）か、後でスキャンするようにスケジュールするか（**[Later]**）を選択します。

ステップ 5 [System Bug Identifier] ウィンドウには、[BUG SUMMARY] と [Bugs Identified on Your System] テーブルが表示されます。

このウィンドウには、基本的なバグ情報に加えて、バグが最初に特定された時期と最後に特定された時期、特定された頻度、影響を受けるバージョンなどの情報が表示されます。

ステップ 6 [Bug ID] をクリックします。
[Bug Details] ダイアログボックスに、バグの詳細情報が表示されます。

ステップ 7 [Bug ID] の横にある矢印をクリックし、[Bug Search Tools] ウィンドウに移動して、バグの詳細情報を確認します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。