



Cisco Nexus Dashboard Insights フロー、
リリース 6.5.1 - Cisco NDFC また
は
スタンドアロン
NX-OS

目次

新規情報および変更情報	2
フロー.....	3
フロー.....	3
フローのハードウェア要件	3
フローのガイドラインと制約事項	3
フローの表示.....	5
L4-L7トラフィックパスの可視性.....	6
フローテレメトリイベント	7
マルチサイト トラフィック パス - ベータ機能	9
マルチサイト トラフィック パス トレースと障害相関	9
マルチサイト トラフィック パス トレースと障害相関の設定	9
著作権.....	11

初版：2024 年 6 月 28 日

米国本社

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax : 408 527-0883

新規情報および変更情報

次の表は、最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

Cisco Nexus Dashboard Insights の新機能と変更された動作

特長	説明	リリース	参照先
用語の	「サイト」という用語が「ファブリック」に名前変更されました。	6.5.1	ドキュメント全体

このドキュメントは、Nexus Insights の GUI とオンライン (www.cisco.com) から入手できます。このドキュメントの最新バージョンに関しては、「[Cisco Nexus Dashboard Insights Documentation](#)」を参照してください。

フロー

フロー

フローは、フロー レベルでの深いインサイトを提供し、平均遅延、パケット ドロップ インジケータなどの詳細を提供します。また、フローの遅延が増加した場合、あるいは輻輳や転送エラーのためにパケットがドロップされた場合に異常が発生します。

各フローには、一定期間にそのフローのASICに入るパケット数を表すパケットカウンタがあります。この期間は、集約間隔と呼ばれます。特定のフローのフロー統計を集約できるポイントがいくつかあります。集約は、ASIC、スイッチソフトウェア、およびサーバーソフトウェアで発生する可能性があります。

Nexus Dashboard Insights の「フロー (Flows)」セクションには、サイトに追加されたサイト内のさまざまなデバイスから収集されたテレメトリ情報が表示されます。

Cisco Nexus シリーズ スイッチおよびライン カードのフロー テレメトリ サポートの詳細については、『Nexus Dashboard Insights [Release Notes](#)』の「[互換性 Information](#)」セクションを参照してください。

フローのハードウェア要件

Cisco Nexusプラットフォームスイッチのフローテレメトリサポートの詳細については、[Nexus Dashboard Insightsリリースノート](#)の「Compatibility Information」セクションを参照してください。

フローのガイドラインと制約事項

フロー テレメトリのハードウェアサポートの詳細については、[Nexus Dashboard Insights リリース ノート](#)の「互換性情報 (Compatibility Information)」セクションを参照してください。

- ・ N9K-C93180YC-EX、N9K-C93108TC-EX、およびN9K-C93180LC-EXラインカードからの発信トラフィックの出力ポート情報は表示されません。
- ・ フローはマルチキャストトラフィックをサポートしていません。アクセスリストは、マルチキャストトラフィック フローを除外するようにプロビジョニングする必要があります。
- ・ フローテレメトリノードでは、最大63のVRFがサポートされます。
- ・ [ファブリックの概要 (**Fabric Overview**)] ダッシュボードの異常の数は、フロー参照ページの異常の数と一致しません。ファブリック ダッシュボードには、選択した時間範囲の異常カウントの合計が含まれています。複数のフローレコードが同じ異常エントリを指す場合があるフローブラウズビューでは、フローレコードは集約されません。
- ・ VXLANフローが入力ノードでドロップされた場合、L3-VNIフローはL2-VNIフローとして表示されます。VXLANパケットが最初のホップでドロップされると、エクスポートされたVXLANフローテレメトリレコードにドロップが示されます。ただし、それらにはVNI情報が含まれていません。フロー テレメトリ エクスポートからの入力インターフェイスとインターフェイスに関連付けられた VRF は、フローが L2-VNI または L3-VNI のどちらであるかを推測しません。この場合、Nexus Dashboard Insights ではフローに L2-VNI を関連付けます。
- ・ VXLANカプセル化パケットがCisco Nexus 9500-EXスイッチに入り、機能オーバーレイ(EVPN)が設定されている場合、パケットはVXLANトランジットノードパケットのように扱われます。また、フローテレメトリ エクスポートでは、入力インターフェイスと出力インターフェイスがゼロに設定されます。フローのこのレコードを考慮するには、入力および出力インターフェイスが必要です。これらのスイッチの制限

が原因で、スイッチが入力、トランジット、または出力方向にある場合、Cisco Nexus 9500-EX スイッチはパススティーティングおよび相関で考慮されません。Cisco Nexus 9500-EXスイッチは、オーバーレイパケットのトランジットノードのように扱われます。

- ・ Nexus Dashboard InsightsがVXLAN展開で機能するには、オーバーレイに含まれるスイッチで対称設定が必要です。これにより、Nexus Dashboard Insightsがオーバーレイフローを関連付けてつなぎ合わせることができます。このような対称設定が存在しない場合、VXLANの機能と転送は機能しますが、Nexus Dashboard Insightsはフローを正しくつなぎ合わせません。スイッチの対称設定の意味を理解するには、次の例を参照してください。
 - レイヤ 2 VXLAN VNI の場合：vlan-x が PE1 の VNI-A にマッピングされている場合、同じvlan-x を PE2 の VNI-Aに マッピングする必要があります。ここで、PE1 と PE2 はレイヤ 2 オーバーレイの VTEP エンドポイントです。
 - レイヤ 3 VXLAN VNI の場合：SVI-x が PE1 の VRF-A でマッピングされた VNI-P にマッピングされている場合、同じ SVI-x を PE2 の VRF-A でマッピングされた VNI-P にマッピングする必要があります。ここで、PE1 と PE2 は VTEPであり、レイヤ 3 オーバーレイのエンドポイントです。
- ・ このIDは 'overlay-id' に使用されるため、論理インターフェイス ID のエンコードのためにフローテレメトリ 'tenant-id' を使用するすべてのインターフェイスで、入力および VRF 情報は表示されません。論理インターフェイス(トランクポートを持つSVI、サブインターフェイス、トランクとポートチャネルを持つSVI)を導出し、それに関連付けられたVRFを取得することはできません。これを行うと、フローの参照ページと詳細ページに入力および出力VRFが表示されなくなります。
- ・ 現在の設計では、VPC ペアに接続された Cisco Nexus 9500-EX スイッチの VPC ペア間の入力リーフノードの識別が制限されており、その結果 Nexus Dashboard Insights でフローが失われます。
- ・ インデックスに2900万の異常がある場合、フローデータベースの書き込みが遅すぎるため、ソフトウェアテレメトリとフローテレメトリでサポートされている350のノードで、KAFKAのラグが発生します。KAFKAのラグの結果、Nexus Dashboard Insightsのユーザーインターフェイスにデータが部分的に表示されるようになります。
- ・ フロー情報は 7 日間、またはフローデータベースが 80% に達するまで（どちらか早い方）保持され、その後、古いフロー情報はデータベースから削除されます。
- ・ Cisco Nexus FX スイッチで出力 ACL のドロップがある場合、フロー テレメトリおよびフロー テレメトリイベントは**ドロップビット**をエクスポートしません。
- ・ Nexus Dashboard Insightsがフローテレメトリデータを受信するには、**ing-netflow**のTCAMリージョンを512に設定する必要があります。[Nexus 9000 TCAM Carving](#)を参照してください。
- ・ フローの場合、選択した時間範囲が 6 時間を超える場合、データが表示されないことがあります。6 時間以下の時間範囲を選択します。
- ・ 異常のスケール制限に達すると、正常でないフローの一部が [フロー レコードの詳細 (Flow Record Details)] ページに異常として表示されない場合があります。この状態が発生すると、システムの問題が発生します。[管理 (Admin)] > [システム設定 (System Settings)] > [システムの問題 (System Issues)] に移動して、システムの問題を表示します。
- ・ レイヤ 4 ~ レイヤ 7 サービスでは、フローに対して VRF 内のみがサポートされます。レイヤ 4 ~ レイヤ 7 サービスでは、フローに対して VRF 内のみがサポートされます。
- ・ NetFlow が設定され、トラフィック分析が有効になっている NDFC ファブリックでフロー テレメトリを有効にするには、次の手順を実行する必要があります。
 1. NDFC でネットフロー ポリシーを削除します。
 2. トラフィック分析を無効にします。「[トラフィック分析](#)」を参照してください。

3. フロー テレメトリを有効にします。「[使用する前に](#)」を参照してください。

- ・マルチキャストはフローテレメトリではサポートされていません。
- ・トラフィックがサブインターフェイスを通過する場合、[フローレコードの詳細 (**Flow Record Details**)] ページの [フロー パス (Flow Path)] エリアの入力方向にのみサブインターフェイスが表示されます。出力方向では、親インターフェイスが表示されます。
- ・フロー テレメトリのユニキャスト ルートの場合、レイヤ 4 ~ レイヤ 7 サービスのトラフィック経路の可視性は、Cisco Nexus 9300 -GX2 および -FX3 プラットフォーム スイッチでサポートされます。
- ・Nexus Dashboard Insights でスタンドアロン NX-OS ファブリックをオンボーディングする前にスイッチでNetFlowを設定し、Nexus Dashboard Insights から対応するファブリックでフロー テレメトリを有効にすると、誤った設定がスイッチにプッシュされるという異常が生成される可能性があります。

この問題を解決するには、次の手順を実行します。

1. スタンドアロン NX-OSファブリックからスイッチを削除します。
 2. スイッチから NetFlow を削除するには、**no feature netflow** コマンドを活用します。
 3. スタンドアロン NX-OS ファブリックにスイッチを再度追加します。
 4. フロー テレメトリを有効にします。
- ・スイッチの 1 つが到達不能であるときにフロー テレメトリが無効になると、サイトは **Disable Failed** 状態になります。これは想定されている動作です。この状態の後、スイッチが使用可能になってからフロー テレメトリを有効にすると、ACL 構成が破損します。

次のいずれかの回避策を推奨します。

- この状態が発生し、ファブリックが **Disable Failed** 状態の場合は、この状態のスイッチを再試行します。これにより、ACL が正常に構成解除をトリガーします。その後、ファブリックをイネーブルにするときに、**disable acl job** を開始して、スイッチ内の既存の ACL をクリーンアップします。
- スイッチで既存の ACL を消去せずにフローテレメトリをすでに有効にしている場合は、次のアクションを実行します。
 1. フロー テレメトリを無効にしてから有効にします。
 2. 問題のあるスイッチを DCNM ファブリックから削除し、ファブリックに追加し直します。

フローの表示

フロー ページには、オンライン ファブリック内のさまざまなデバイスから収集されたテレメトリ情報が表示されます。フロー レコードを使用すると、ユーザーにファブリックごとのフローを可視化します。特定のファブリックについて、異常スコア、パケット ドロップ インジケータ、および平均遅延別にフローを表示できます。

フロー エンジンには、フローの動作に対して機械学習アルゴリズムも実行し、平均遅延、パケット ドロップ インジケータなどにおける動作の異常を発生させます。グラフは一定期間における動作の異常数を表します。

フローテレメトリと分析により、データプレーンの詳細な可視性が得られます。フローは、ノードからストリーミングされたフローレコードを収集し、理解可能な EPG ベースのフローレコードに変換します。[フロー異常別の上位ノード]には、ネットワーク内で異常が最も多いノードが表示されます。



フローの詳細を表示するには、最初にフローを有効にする必要があります。
「[使用する前に](#)」を参照してください。

1. [管理 (Manage)] > [ファブリック (Fabrics)] に移動します。
2. ドロップダウン リストから [オンライン ファブリック (Online Fabrics)] を選択します。
3. ファブリック名をクリックすると、ファブリックの詳細が表示されます。
4. [接続 (Connectivity)] > [フロー (Flows)] に移動します。
5. 時間範囲を選択します。
6. [ファブリック フロー別 (Fabric Flows by)] エリアで、ドロップダウン リストからオプションを選択して、異常スコア、パケットドロップインジケータ、および平均遅延別にフローを表示します。グラフには、ファブリック全体で記録されたフロー プロパティの時系列プロットが表示されます。上位の送信元と上位の接続先について記録されたフローも表示されます。

異常スコア - スコアは、データベースに記録された検出済みの異常の数に基づいています。

パケット ドロップ インジケータ - フローレコードのドロップが分析されます。ドロップを検出する主な方法は、スイッチから受信したドロップビット(フローレコード)に基づいています。

遅延：パケットがサイト内の送信元から接続先までトラバースするのにかかる時間。ファブリック遅延測定の前条件は、すべてのノードが一定の時間で同期されることです。

7. [フロー (Flows)] テーブルには、異常スコア、フロー レコード時間、ノード、フロー タイプ、プロトコル、遅延、パケット ドロップ インジケータなどの情報が表示されます。
8. 検索バーを使用してフローをフィルタリングします。[フロー (Flows)] テーブルに、フィルタ処理されたフローが表示されます。列の見出しをクリックして、テーブルのフローを並べ替えます。
9. [レコード時間 (Record Time)] をクリックして、フロー レコードの詳細を表示します。詳細には、レコード時間、フロータイプ、集約されたフロー情報、入力および出力情報、フロー、異常、および平均遅延、トラフィック、パケットドロップインジケータ、バーストの傾向が含まれ経路。

L4-L7トラフィックパスの可視性

Nexus Dashboard Insightsリリース6.1.1以降、フローパスの可視性をファイアウォールなどのL4-L7外部デバイスに拡張できるようになりました。Nexus Dashboard Insightsは、サービスチェーン全体のエンドツーエンドフローをリアルタイムで追跡し、デバイスサイロ全体のデータプレーンの問題を特定するのに役立ちます。現在のリリースでは、すべてのサードパーティベンダーの非NAT環境がサポートされています。

L4-L7トラフィックパスを可視化するには、フローテレメトリを有効にし、適切なルールを設定する必要があります。「[使用する前に](#)」を参照してください。ルールに基づいて、フローがポリシーベースのリダイレクト(ファイアウォールなど)を通過している場合、フローパスにその情報が表示されます。

GUI でトラフィック経路の可視性を表示するには、

1. [管理 (Manage)] > [ファブリック (Fabrics)] に移動します。
2. ドロップダウン リストから [オンライン ファブリック (Online Fabrics)] を選択します。
3. ファブリック名をクリックすると、ファブリックの詳細が表示されます。

4. [接続 (Connectivity)] > [フロー (Flows)] に移動します。
5. 時間範囲を選択します。
6. フロー テーブルで、[レコード時間 (Record Time)] をクリックしてフロー レコードの詳細を表示します。

[パス] エリアでは、送信元から宛先までのエンドツーエンドの情報がグラフィカルなフロー パスで表示され、ファイアウォールが存在する場合はパス内のファイアウォールも特定されます。このグラフでは、発生しているエンドツーエンドのフローパスネットワークの遅延もキャプチャされます。グラフでは、異常がある場合、リーフスイッチまたはスパインスイッチの記号の横に赤いドットが表示されます。

7. [フローの詳細] ページの [アラート] タブをクリックして、異常に関連する詳細を表示します。



現在のリリースでは、ファイアウォールは異常に対してサポートされていません。

L4-L7 トラフィックパスの可視性に関するガイドラインと制約事項

- ・ この機能は現在、NDFC の L4 ~ L7 サービスを使用してポリシーベースのリダイレクトを設定できる場合にのみ推奨されています。
- ・ サービスノードが直接接続されている場合は、サービスノードのタイプが検出されます。ただし、複数のサービスノードが同じ物理ポートに接続されている場合、Nexus Dashboard Insights は正確なサービスノードのタイプ情報を識別しません。その結果、不明なサービスノードとして識別されます。
- ・ 現在のリリースでは、ファイアウォールは異常に対してサポートされていません。
- ・ 現在のリリースでは、表示されている遅延情報はネットワーク遅延であり、ファイアウォールで発生している遅延はキャプチャされません。
- ・ 現在のリリースでは、NAT はサポートされていません。
- ・ この機能は現在、次のスイッチを使用する場合にサポートされています。
 - Cisco Nexus 9300-FX プラットフォームスイッチ
 - Cisco Nexus 9300-FX2 プラットフォームスイッチ
 - Cisco Nexus 9300-GX プラットフォームスイッチ
- ・ L3Out でのポリシー ベースのリダイレクトの宛先はサポートされていません。そのような設定では内部 VRF が使用されるため、部分的なフローパスのみ使用できるためです。
- ・ L4-L7 のサービスグラフがない場合、クライアント > サービスノードが VRF_A であり、サービスノード > サーバーが VRF_B である場合、フローをステッチする共通または単一の契約がないため、パスは個別のフローとして記録されます。
- ・ ロードバランサはサポートされていません。

フローテレメトリイベント

フローテレメトリが有効になっていて、フロールールが設定されている場合、フローテレメトリイベントは暗黙的に有効になります。フローテレメトリにより、設定されたルールが満たされたときにイベントをトリガーでき、パケットが分析のためにコレクタにエクスポートされます。

フロー テレメトリ イベントは、{PlatformFullName} の現在のフローを強化および補完します。また、フローテレメトリおよびフローテレメトリイベントの異常生成を強化します。

セキュリティ、パフォーマンス、トラブルシューティングを監視します。これは、定期的なフロー テーブルを使用して

イベント レコードが 1 秒ごとにエクスポートされるようになります。

{PlatformFullName} へのデータのエクスポートは、データを処理するために必要なコントロール プレーンなしでハードウェアから直接実行されます。統計は、設定可能なMTUサイズと定義されたヘッダーを持つパケットとして集められます。それらのパケットは、NDFC ファブリックからインバンド トラフィックとして送信されます。ヘッダーはソフトウェアによって構成され、ストリーミングされるパケットは UDP パケットです。

トリガーされたフローテレメトリイベントでフローテレメトリを使用できる場合は、[フローの詳細 (Flow Details)] ページに移動して集約された情報を確認できます。それらのイベントは、次のドロップイベントに基づいています。

- ・ **Cisco ACL** ドロップ：パケットが **sup-tcam** ルールに抵触していて、そのルールがパケットをドロップするルールである場合、ドロップされたパケットは ACL_Drop としてカウントされ、転送ドロップカウンタでカウントされます。これが発生した場合、通常は、パケットが基本的なCisco ACIの転送の原則に反する転送をされようとしていることを意味します。**sup-tcam** ルールは主に一部の例外やコントロール プレーンのトラフィックを処理するためのものであり、ユーザーがチェックしたりモニタしたりするには意図されていません。
- ・ バッファドロップ - スイッチがフレームを受信し、入力または出力インターフェイスで使用できるバッファクレジットがない場合、フレームはバッファでドロップされます。これは通常、ネットワークで輻輳が発生していることを示唆しています。障害を示すリンクがいっぱいか、宛先を含むリンクが輻輳している可能性があります。この場合、フローテレメトリイベントでバッファドロップが報告されます。
- ・ 転送ドロップ - Cisco ASICのLookUp (LU)ブロックでドロップされるパケットです。LUブロックでは、パケット転送の判断はパケットヘッダー情報に基づいて行われます。パケットがドロップされた場合、転送ドロップがカウントされます。転送ドロップがカウントされる理由はさまざまです。

TCP パケット RTO の異常は、NDFC ではサポートされていません。

フローテレメトリイベントとフローテレメトリ

- ・ フローテレメトリイベントのパケットは、設定されたイベントが発生した場合にのみエクスポートされ、フローテレメトリのパケットは継続的にストリーミングされます。
- ・ フローテレメトリイベントはすべてのトラフィックに対してキャプチャされますが、フローテレメトリはフィルタ処理されたトラフィックに対してキャプチャされます。
- ・ フローテレメトリとフローテレメトリイベント間のコレクタの総数は256です。

フローテレメトリイベントのガイドラインと制約事項

- ・ フローテレメトリイベントの異常が集約されます。たとえば、T0からT1の間にパケットドロップの異常が発生したとします。時刻T1からT2まではパケットドロップの異常は発生していません。時刻T2からT3にかけて、別のパケットドロップの異常が発生しました。T1 から T2 まで異常がないにもかかわらず、集約されたパケットドロップの異常のタイムスタンプは T0 から T3 となります。
- ・ フロー テレメトリ イベントは、出力データ プレーン ポリサーがフロント パネル ポートに設定されていて、トラフィック ドロップがある場合、{PlatformFullName} でポリシングドロップ異常を報告しません。
- ・ FX プラットフォーム スイッチでフロー テレメトリ イベントをエクスポートするには、フロー テレメトリ フィルタを構成する必要があります。

マルチサイト トラフィック パス - ベータ機能

マルチサイト トラフィック パス トレースと障害相関



これはベータ機能です。テスト環境ではベータとマークされた機能を使用し、実稼働環境では使用しないことをお勧めします。

フローを監視するために、2つの異なるファブリックからのフローを 1 つのビューに結合できます。結合することで、パスのエンドツーエンドビュー、特定のフローのエンドツーエンドの詳細、およびそのフローの遅延情報を表示できます。

マルチサイト トラフィック パス トレースと障害相関のユースケース:

- ・ ファブリック間でフローを関連付け、フローの詳細を結合されたパスで表示できます。
- ・ ファブリック全体のフローを監視し、トリガー ベースのサイト間の異常を生成できます。
- ・ ファブリック間のフローを監視し、エンドツーエンドの遅延を提供できます。

マルチサイト トラフィック パス トレースと障害相関の設定

[検出 (Explore)] エリアで、2 つのポート間のフローパス、各ポートの IP アドレス と VRF を表示できます。

1. [フロー (Flows)] テーブルで、[レコード時間 (Record Time)] をクリックしてフローレコードの詳細を表示します。
2. [フローパス (Flow Path)] エリアのフローパスで、[マルチサイト フロー - フロー検索で表示 (Multi-Site Flow - View in Flow Explore)] タブをクリックして、[検出 (Explore)] ページに移動します。

[フローの検出 (Explore Flows)] ページの [検索 (Search)] フィールドにフロー情報のフィルタが自動入力され、フローが存在するファブリックを確認できます。[View] クエリエリアには、送信元 IP アドレス、送信元ポート情報、および宛先 IP アドレス、宛先ポート情報を含む情報が表示されます。[検出 (Explore)] は、指定された VRF でこのフローが検出されたすべてのサイトを検索して返します。

次に、適切な送信元サイトと送信先サイトを選択して、集約された情報、パスの概要、および異常を表示します。送信元として使用するファブリックと接続先として使用するファブリックを指定する必要があります。Cisco Nexus Dashboard Insightsは、入力に基づいて情報を結合します。この情報を結合するために、一度に1つの送信元と1つの宛先のみ選択できます。選択した送信元サイトと送信先ファブリックに基づいて、Cisco Nexus Dashboard Insights は見つかったサイトの名前を返します。

[フロー パスの概要]領域では、2 つのファブリックの詳細が、送信元から宛先までのエンドツーエンドの情報を表示するグラフィカルなフローパスとして [検出 (Explore)] ページに表示されます。エンドポイントと一連のノードがある最初のファブリックが表示され、2 番目のノードのセットの後にエンドポイントが続く2番目のファブリックに接続されていることがわかります。ファイアウォールが存在する場合は、パス内のファイアウォールも特定されます。このグラフでは、エンドツーエンドのフローパスネットワークの遅延もキャプチャされます。

送信元サイトと接続先ファブリックの特定の詳細は、各フロー テーブルに表示されます。[異常 (Anomalies)] テーブルで、[グループ化 (Grouped)] を選択して、選択フローのファブリックされた異常を表示します。



【検出 (Explore)】ページの [検索 (Search)] フィールドに別のフローの詳細を入力すると、入力したフローが存在するサイトを表示できます。または、【検出 (Explore)】ページの [検索 (Search)] フィールドに詳細を入力して、複数のファブリックにわたるフローおよびフローパスに関する詳細の検索を直接開始できます。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または黙示のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。

商標または登録商標です。シスコの商標の一覧は、<http://www.cisco.com/go/trademarks> でご確認ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。(1110R)。

© 2017-2024 Cisco Systems, Inc. All rights reserved.