コンポーネント

この章では、Cisco Nexus Dashboard Data Broker のコンポーネントについて詳しく説明します。

リリース 3.10.1 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。

フィルタ

[フィルタ] タブには、Nexus Dashboard Data Broker コントローラで使用可能なすべてのフィルタの詳細が表示されます。このタブには、着信トラフィックのフィルタリング基準（接続で使用される）の情報が表示されます。

デフォルトのフィルタには、パケット フィルタリング用の次のプロトコルが含まれています。

- Default-match-all
- Default-match-IP
- Default-match-ARP
- Default-match-MPLS（ユニキャストおよびマルチキャスト）
- Default-match-ICMP
- Default-match-ICMP-All

次の詳細を含む表が表示されます。

表 *1*: フィルタ

列名	説明
使用中	緑色のチェック マークは、接続でフィルタが使用中であることを示します。
[フィルタ（Filter）]	フィルタ名。 **[フィルタ]** をクリックします。右側に新しいペインが表示され、フィルタに関する詳細情報が表示されます。ここから、次の追加のアクションを実行できます。 • フィルタの編集またはクローン処理 （注） デフォルトのフィルタは編集できません。
双方向	フィルタが双方向の場合、**Yes** が表示されます。それ以外の場合は **No** が表示されます。 フィルタが双方向とマークされている場合、着信トラフィックと発信トラフィックは同じポートでフィルタリングされます。
Ethertype	フィルタのレイヤ 2 イーサタイプ。
プロトコル	フィルタが使用するレイヤ 3 プロトコル。
高度なフィルタ	フィルタに関連付けられた高度なフィルタ。
作成者	フィルタを作成したユーザー。
最終更新者	フィルタを最後に変更したユーザー。

[フィルタ] タブでは、次のアクションを実行できます。

- **フィルタの追加** — これを使用して、新しいフィルタを追加します。このタスクの詳細については、「フィルタの追加」を参照してください。
- **フィルタの削除** — 行の先頭にあるチェックボックスをオンにして、削除するフィルタを選択し、**[アクション]** > **[フィルタの削除]** をクリックします。選択したフィルタが削除されます。チェック ボックスを選択せずに削除アクションを選択すると、エラーが表示されます。フィルタを選択するように求められます。

フィルタの追加

この手順を使用して、フィルタを追加します。着信トラフィックは、フィルタで定義されたパラメータに基づいて照合されます。

ステップ 1 **[コンポーネント]** > **[フィルタ]** に移動します。

ステップ 2 **[アクション]** ドロップダウン メニューから **[フィルタの追加（Add Filter）]** を選択します。

ステップ 3 **[フィルタの追加（Add Filter）]** ダイアログボックスで、次の詳細を入力します。

表 *2:* フィルタの追加

フィールド	説明
フィルタ名	フィルタの名前を入力します。
双方向	双方向トラフィック情報、すなわち、送信元 IP、送信元ポートまたは送信元MACアドレスから宛先IP、宛先ポート、または宛先MACアドレス、および宛先IP、宛先ポート、または宛先MACから送信元IP、送信元ポート、または送信元MACアドレスを取得するためにフィルタ処理する場合は、このボックスをオンにします。

フィールド	説明
レイヤ 2	

フィールド	説明
	レイヤ2フィルタリングの使用中に表示されるオプションは次のとおりです。 • イーサネット タイプ — ドロップダウン リストからイーサネット タイプを選択します。次のオプションがあります。 • IPv4 • IPv6 • LLDP • MPLS • ARP • すべてのイーサネット タイプ • 事前定義されたイーサネット タイプ — このオプションを選択する場合、config.ini ファイルに含まれているすべてのイーサネット タイプは、このルールに関連付けられており、ほかのパラメータを構成してはなりません。 • イーサネット タイプの入力 — このオプションを選択する場合、16進形式でいーアsネットタイプを入力します。 • VLAN 識別番号 — レイヤ 2 トラフィックの VLAN ID を入力します。単一の VLAN ID、VLAN ID の範囲、カンマ区切りの VLAN ID と VLAN ID 範囲を入力できます。 最大値は 4095 です。 • VLAN 優先順位 — トラフィックの VLAN 優先順位を入力します。VLAN優先順位は、レイヤ2トラフィックのみに対して一致します。 • 送信元 MAC アドレス — 送信元デバイスの MAC アドレスを入力します。MAC アドレスは、レイヤ 2 トラフィックのみに対して一致します。 • 宛先 MAC アドレス — 宛先デバイスの MAC アドレスを入力します。MACアドレスは、レイヤ2トラフィックのみに対して一致します。 • MPLS ラベル値 — ラベル 1、ラベル 2、ラベル 3、ラベル 4 の MPLS 値を入力します。

フィールド	説明
	[MPLS ラベル値（MPLS Label Value）] フィールドは、**[イーサネット タイプ（Ethernet Type）]** が MPLS に設定される場合のみ表示されます。MPLS ラベル値が一致します。

フィールド	説明
レイヤ 3 レイヤ3のオプションを有効にするには、**IPv4** または **IPv6** を **Ethertype** として [レイヤ 2] タブの下で選択します。	

フィールド	説明
	レイヤ3フィルタリングで表示されるオプションは次のとおりです。 • 送信元 IP アドレス — レイヤ 3 トラフィックの送信元 IPアドレスを入力します。次のいずれかになります。 • 標準的な IPv4 または IPv6 形式のホスト IP アドレス • IPv4 または IPv6 アドレス範囲 • アドレス範囲と標準 IP アドレスの組み合わせ。例: 10.1.1.1、10.1.1.2-10.1.1.5 • コンマ区切りの不連続IPアドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 4 送信元または送信先ポートの範囲を構成することはできません。 レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 2 VLAN 識別子の範囲は設定できません。 • 宛先 IP アドレス — レイヤ 3 トラフィックの宛先 IP アドレスを入力します。次のいずれかになります。 • 標準的な IPv4 または IPv6 形式のホスト IP アドレス • IPv4 または IPv6 アドレス範囲 • アドレス範囲と標準 IP アドレスの組み合わせ。例: 10.1.1.1、10.1.1.2-10.1.1.5 • コンマ区切りの不連続IPアドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 4 送信元または送信先ポートの範囲を構成することはできません。 レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 2 VLAN 識別子の範囲は設定できません。 • L4 プロトコル — ドロップダウン リストからレイヤ 4 プロトコルを選択するか、**プロトコル番号**を入力しま

フィールド	説明
	す。 • 高度なフィルタ — このボタンをクリックして、高度なフィルタ処理を有効にして、必要なオプションを選択するためのチェックボックスをオンにしてください。高度なフィルタに関連するオプションの詳細については、「詳細フィルタ」を参照してください。 • カスタム フィルタ — このボタンをクリックして、ユーザー定義フィールド（UDF）を使用したカスタム フィルタ処理を有効にします。**[UDF の選択（Select UDFs）]** をクリックして、**[カスタム フィルタの選択（Select Custom Filters）]** ウィンドウでフィルタを選択します。ユーザー定義フィールドの追加 を使用して作成された UDF がここに表示されます。 選択した UDF がテーブルに表示されます。選択した UDF について、次の詳細を入力します。 • 値 - 10 進表記（0 ～ 65535）で一致する値です。たとえば、0x0806 に一致させたい場合は、10 進表記で 0x0806 である 2054 を入力します。 • マスク - マッチングのために値に適用されるマスクです。たとえば、2054（0x0806）に正確に一致させるには 65535（0xffff）と入力し、2048-2063（0x0800-0x080f）に一致させるには 65520（0xfff0）を使用します。 （注） モニタリング ツール ポートが ISL デバイス上にある場合は、**[内部 VLAN にデフォルト UDF を追加]** チェックボックスをオンにする必要があります。入力ポートに Q-in-Q が構成されていることを確認します。

フィールド	説明
Layer 4（レイヤ 4） レイヤ 4 のオプションを有効にするには、[レイヤ 2] タブで **[Ethertype]** として **[IPv4]** または **[IPv6]** を選択し、[レイヤ 3] タブで **[L4 プロトコル]** として **[TCP]** または **[UDP]** を選択します。	レイヤ4フィルタリングで表示されるオプションは次のとおりです。 • 送信元ポート — ドロップダウン リストから送信元ポートを選択します。次のオプションがあります。 • FTP（データ） • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • 送信元ポートを入力 — 送信元ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） レイヤ 4 送信元ポートの範囲を入力すると、レイヤ 3 IP アドレスまたはレイヤ 2 VLAN 識別子の範囲を構成できません。 • Destination Port — ドロップダウン リストで、宛先ポートを選択します。次のオプションがあります。 • FTP（データ） • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • 宛て先ポートの入力 — 宛て先ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） レイヤ 4 宛先ポートの範囲を入力すると、レイヤ 2 VLAN 識別子またはレイヤ 3 IP アドレスの範囲を設定できません。

フィールド	説明
レイヤ 7	未サポート

（注） カスタム フィルタリングの場合: 1 つのフィルタに最大 4 つの UDF を追加できます。UDF オプションは、IPv4 および IPv6 のイーサタイプに対して有効になっています。

ステップ 4 **[フィルタの追加（Add Filter）]** をクリックして、フィルタを追加します。

フィルタの編集またはクローン処理

この手順を使用して、フィルタを編集またはクローン処理をします。

フィルタの編集は、既存のフィルタのパラメータを変更することを意味します。

フィルタの複製とは、既存のフィルタと同じパラメータを使用して新しいフィルタを作成し、フィルタ パラメータに必要な変更を行うことを意味します。保存する前に、フィルタの名前を変更してください。

（注） デフォルトのフィルタは編集できません。

始める前に

1 つ以上のフィルタを追加します。

ステップ 1 **[コンポーネント（Components）]** > **[フィルタ（Filters）]** に移動します。

ステップ 2 表示された表で、**フィルタ**をクリックします。

新しいペインが右側に表示されます。

ステップ 3 **[アクション]** をクリックし、**[フィルタのクローン]** を選択します。

ステップ 4 **[フィルタのクローン]** または **[フィルタの編集]** ダイアログ ボックスに、現在のフィルタ情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *3*: 編集/フィルタのクローン

フィールド	説明
フィルタ名	フィルタの名前。

フィールド	説明
双方向	双方向トラフィック情報、すなわち、送信元 IP、送信元ポートまたは送信元MACアドレスから宛先IP、宛先ポート、または宛先MACアドレス、および宛先IP、宛先ポート、または宛先MACから送信元IP、送信元ポート、または送信元MACアドレスを取得するためにフィルタ処理する場合は、このボックスをオンにします。

フィールド	説明
レイヤ 2	

フィールド	説明
	レイヤ2の使用中に表示されるオプションは次のとおりです。 • イーサネット タイプ — ドロップダウン リストからイーサネット タイプを選択します。次のオプションがあります。 • IPv4 • IPv6 • LLDP • MPLS • ARP • すべてのイーサネット タイプ • 事前定義されたイーサネット タイプ — このオプションを選択する場合、config.ini ファイルに含まれているすべてのイーサネット タイプは、このルールに関連付けられており、ほかのパラメータを構成してはなりません。 • イーサネット タイプの入力 — このオプションを選択する場合、16進形式でいーアsネットタイプを入力します。 • VLAN 識別番号 — レイヤ 2 トラフィックの VLAN ID を入力します。単一の VLAN ID、VLAN ID の範囲、カンマ区切りの VLAN ID と VLAN ID 範囲を入力できます。 最大値は 4095 です。 • VLAN 優先順位 — トラフィックの VLAN 優先順位を入力します。 VLAN優先順位は、レイヤ2トラフィックのみに対して一致します。 • 送信元 MAC アドレス — 送信元デバイスの MAC アドレスを入力します。 MAC アドレスは、レイヤ 2 トラフィックのみに対して一致します。 • 宛先 MAC アドレス — 宛先デバイスの MAC アドレスを入力します。 MAC アドレスは、レイヤ 2 トラフィックのみに対し

フィールド	説明
	て一致します。 • MPLS ラベル値 — ラベル 1、ラベル 2、ラベル 3、ラベル 4 の MPLS 値を入力します。 **[MPLS ラベル値（MPLS Label Value）]** フィールドは、**[イーサネット タイプ（Ethernet Type）]** が MPLS に設定される場合のみ表示されます。MPLS ラベル値が一致します。

フィールド	説明
レイヤ 3 レイヤ3のオプションを有効にするには、**IPv4** または **IPv6** を **Ethertype** として [レイヤ 2] タブの下で選択します。	

フィールド	説明
	レイヤ3の使用中に表示されるオプションは次のとおりです。 • 送信元 IP アドレス — レイヤ 3 トラフィックの送信元 IP アドレスを入力します。次のいずれかになります。 • ホスト IP アドレスは、標準的な IPv4 または IPv6 形式です • IPv4 または IPv6 アドレス範囲 • アドレスの範囲と標準的な IP アドレスの組み合わせ。例：10.1.1.1, 10.1.1.2-10.1.1.5 • コンマ区切りの不連続 IP アドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 4 送信元または宛先ポートの範囲を構成することはできません。 レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 2 VLAN 識別子の範囲は設定できません。 • 宛先 IP アドレス — レイヤ 3 トラフィックの宛先 IP アドレスを入力します。次のいずれかになります。 • ホスト IP アドレスは、標準的な IPv4 または IPv6 形式です • IPv4 または IPv6 アドレス範囲 • アドレスの範囲と標準的な IP アドレスの組み合わせ。例：10.1.1.1, 10.1.1.2-10.1.1.5 • コンマ区切りの不連続 IP アドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 4 送信元または送信先ポートの範囲を構成することはできません。 レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 2 VLAN 識別子の範囲は設定できません。 • L4 プロトコル — ドロップダウン リストからレイヤ 4 プロトコルを選択します。

フィールド	説明
	• 高度なフィルタ — このボタンをクリックして、高度なフィルタ処理を有効にして、必要なオプションを選択するためのチェックボックスをオンにしてください。高度なフィルタの詳細については、「詳細フィルタ」を参照してください。 • カスタム フィルタ — このボタンをクリックして、ユーザー定義フィールド（UDF）を使用したカスタム フィルタ処理を有効にします。**[UDF の選択（Select UDFs）]** をクリックして、**[カスタム フィルタの選択（Select Custom Filters）]** ウィンドウでフィルタを選択します。

フィールド	説明
Layer 4（レイヤ 4） レイヤ 4 のオプションを有効にするには、[レイヤ 2] タブで **[Ethertype]** として **[IPv4]** または **[IPv6]** を選択し、[レイヤ 3] タブで **[L4 プロトコル]** として **[TCP]** または **[UDP]** を選択します。	レイヤ4の使用中に表示されるオプションは次のとおりです。 • Source Port — ドロップダウン リストから送信元ポートを選択します。次のオプションがあります。 • FTP（データ） • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • Enter Source Port — 送信元ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） レイヤ 4 送信元ポートの範囲を入力すると、レイヤ 3 IP アドレスまたはレイヤ 2 VLAN 識別子の範囲を構成できません。 • Destination Port — ドロップダウン リストで、宛先ポートを選択します。次のオプションがあります。 • FTP (データ) • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • Enter Destination Port — 送信先ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） レイヤ 4 宛先ポートの範囲を入力すると、レイヤ 2 VLAN 識別子またはレイヤ 3 IP アドレスの範囲を設定できません。

フィールド	説明
レイヤ 7	未サポート

ステップ 5 **[フィルタの編集（Edit Filter）]** または **[フィルタのクローン（Clone Filter）]** をクリックします。

詳細フィルタ

高度なフィルタリングには、イーサネット タイプと、確認応答、FIN、フラグメント、PSH、RST、SYN、DSCP、優先順位、TTL、パケット長、NVE などの属性に基づいてトラフィックをフィルタリング（許可または拒否）するための複数のオプションが用意されています。高度なフィルタリングは、次のイーサネット タイプとオプションで利用できます。

表 *4:* 高度なフィルタリングのサポート

データ タイプ	サポートされるオプション
IPv4	DSCP、フラグメント、優先順位、および TTL
IPv4 と TCP	確認応答、DSCP、フラグメント、FIN、優先順位、PSH、RST、SYN、および TTL
UDP を使用した IPv4	DSCP、フラグメント、優先順位、および TTL
IPv6	DSCP とフラグメント
IPv6 と TCP	確認応答、DSCP、フラグメント、FIN、PSH、RST、および SYN
UDP を使用した IPv6	DSCP とフラグメント

（注） 高度なフィルタリングは、Cisco Nexus 9000 プラットフォームの NX-API でのみ使用できます。

Time to Live (TTL) 属性の範囲は 0 ～ 255 です。Nexus 9200 端末の場合、設定できる TTL の最大値は 3 です。残りの Nexus 9000 シリーズ デバイスでは、NX-OS バージョン 7.0(3)I6(1) 以降の最大 TTL 値を 3 にすることができます。NXOS バージョン 7.0(3)I4(1) 以前では、範囲内の任意の値を設定できます。

高度なフィルタリングの使用に関する制限

高度なフィルターの構成中、次のことはできません。

- DSCP と優先順位を一緒に構成します。

- フラグメントと ACK または SYN または FIN または PSH または RST を一緒に構成します。
- UDP と IPv4 または IPv6 の組み合わせでフラグメントとポート番号を構成します。
- IPv4 と TCP の組み合わせで優先順位と HTTP メソッドを構成します。

グローバル設定

[グローバル構成（Global Configuration）] タブには、Nexus Dashboard Data Broker コントローラに接続されているデバイスが表示されます。Nexus Dashboard Data Broker コントローラに追加された新しいデバイスは、デフォルトでここに表示されます。

（注） ここには、接続されているデバイス（接続状態が緑色で表示）のみが表示されます。デバイスが Nexus Dashboard Data Broker コントローラに追加されているが、接続されていない場合（接続ステータスは赤で示されます）、そのデバイスはここに表示されません。デバイスのステータスを確認するには、NDB デバイスを参照してください。

次の詳細の表が表示されます。

表 *5:* グローバル設定

列名	説明
Device	デバイス名 これはハイパーリンクです。**デバイス**名をクリックして、デバイスのグローバル構成の詳細を取得します。
Loadbalancing	ロード バランシングのタイプを表示します。次のオプションがあります。 • Symmetric • 非対称
PTP	PTP が有効かどうかを表示します。次のオプションがあります。 • 有効 • 無効

列名	説明
Jumbo MTU	デバイスのジャンボ MTU サイズ。 ジャンボMTUは、デバイスに構成できる最大の MTU です。
MPLS ストリップ	デバイスでMPLSストリッピングが有効になっているかどうかを表示します。次のオプションがあります。 • 有効 • 無効
MPLS フィルタ	デバイスの MPLS フィルタリングが有効かどうかを表示します。次のオプションがあります。 • 有効 • 無効
Netflow	デバイスのNetflowが有効かどうかを表示します。次のオプションがあります。 • 有効 • 無効

次のアクションは、**[グローバル構成]** タブから実行できます。

- **グローバル構成の編集**：手順の詳細については、デバイスのグローバル構成の編集 （22 ページ）を参照してください。

デバイスのグローバル構成の編集

この手順を使用して、デバイスのグローバル構成を編集します。デバイスのパラメータをグローバルに変更できます。たとえば、ここで設定するジャンボMTU値は、デバイスの入力ポートの MTU 値を定義します。

デバイスが作成されると、いくつかの基本構成が作成され、いくつかのデフォルト値が設定されます。この手順を使用して、デバイスの 1 つ以上のパラメータを変更または追加します。

始める前に

1 つ以上のデバイスを作成します。デバイスのステータスを確認します。

ステップ 1 **[コンポーネント]** > **[グローバル構成]** に移動します。

ステップ 2 業の先頭のチェックボックスをオンにして、デバイスを選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

ステップ 4 **[グローバル構成の編集（Edit Global Configuration）]** ダイアログボックスで、次の詳細情報を入力します。

表 *6*: グローバル構成の編集

フィールド	説明
全般	
デバイス	デバイス名は、以前の選択に基づいて表示されます。
負荷分散タイプの構成	ドロップダウン リストから **[対称]** または **[非対称]** を選択します。 負荷分散の詳細については、対称型および非対称型ロード バランシング を参照してください。
ハッシュ構成	ドロップダウン リストからハッシュ構成を選択します。表示されるドロップダウン リストは動的で、選択した負荷分散タイプによって異なります。
ハッシュ タイプ	ドロップダウン リストからハッシュ タイプを選択します。
MPLS の構成	
MPLS ストリップ タイプの構成	グレーのボタンをクリックして、MPLS ストリップ タイプの構成を有効にします。ボタンが青色に変わり、右に移動します。 入力ポートからのすべての MPLS パケットは、MPLS ヘッダーが取り除かれます。 （注） Cisco Nexus 9300-GX シリーズ スイッチでは、MPLS ストリップ機能は、スイッチのリロード後にのみ機能します。
ラベルのエージング	MPLS ラベルが期限切れになるまでの期間を設定します。このフィールドは、選択したデバイスでのみ使用できます。 サポートされているプラットフォームは、次の Cisco Nexus シリーズ スイッチです - 93128TX、3172、3164、3232、3132C-Z。

フィールド	説明
MPLS フィルタ構成を有効にする	グレーのボタンをクリックして、MPLS フィルタ構成を有効にします。ボタンが青色に変わり、右に移動します。 ここで有効になっている MPLS フィルタ構成は、デバイスの入力ポートに適用されます。
sFlow 構成	
sFlow の有効化	グレーのボタンをクリックして、サンプル フロー（sFlow）を有効にします。ボタンが青色に変わり、右に移動します。 sFlow の詳細については、サンプリングされたフロー （31 ページ） を参照してください。 次の詳細を入力します。 • **エージェントの IP アドレス** — エージェントの IP アドレスを入力します。 • **VRF の選択** — ドロップダウンリストから [VRF] を選択します。 • **コレクタ IP アドレス** — コレクタ ポートの IP アドレスを入力します。 • **コレクタ UDP ポート** — sFlow コレクターの UDP ポートを入力します。 • **カウンタ ポーリング間隔** — sFlow のポーリング間隔値を入力します。 • **最大データグラム サイズ** — 最大データグラム サイズを入力します。 • **最大サンプル サイズ** — 最大サンプル サイズを入力します。 • **サンプリング レート** — データ サンプリング レートを入力します。 • **データ ソース** — **[ポートの選択]** をクリックし、必要なチェック ボックスをオンにしてポートを選択し、**[追加]** をクリックします。 （注） デバイスの sflow 設定を確認するには、 **show sflow** コマンドを使用します。
PTP 設定	

フィールド	説明
PTP の有効化	グレーのボタンをクリックしてPTPを有効にし、マスターから更新を受信します。ボタンが青色に変わり、右に移動します。 ここで有効になっている PTP は、入力ポートとモニタリング ツールのタイムスタンプに使用されます。 PTP の詳細については、高精度時間プロトコル （30 ページ） を参照してください。 次のフィールドが表示されます。 • **送信元 IP アドレス** — PTP アップデートを受信するためのソース IP アドレスを入力します。 • **ポート** ：**[ポートの選択]** をクリックし、チェックボックスをオンにして、PTP ソース IP が接続されている必要なポートを選択します。 （注） PTP クロック タイムの同期を確保するには、ネットワーク内のすべてのデバイスでPTPを有効にする必要があります。
ジャンボ MTU構成	
MTU 値	MTU 値を入力します。範囲は 1502 ～ 9216 です。ジャンボMTUは、デバイスが受け入れることができる最大MTU値を設定します。 トラフィックの MTU サイズは通常 1500 です。MTU が 1500 を超えるトラフィックを受信するには、これを有効にします。ここで定義されたMTU値は、デバイスの入力ポートの着信トラフィックに適用されます。 **[デフォルトにリセット]** をクリックして、MTU 値をデフォルト値の 1500 に設定します。 （注） MTU値は、指定された範囲内の偶数である必要があります。
Netflow の構成	

フィールド	説明
Netflow の有効化	灰色のボタンをクリックして、ネットフローを有効にします。ボタンが青色に変わり、右に移動します。 Netflow の詳細については、NetFlow （31 ページ） を参照してください。 Netflowパラメータを定義するには、次の構成を（指定された順序で）完了します。 • NetFlow のレコードの追加 （26 ページ） • NetFlow のエクスポータの追加 （28 ページ） • NetFlow のモニターの追加 （29 ページ） NetFlow設定を完了するには、NetFlowモニタリングを入力ポートに関連付けます。入力ポートの追加 （34 ページ）を参照してください。

ステップ 5 **[グローバル構成の編集]** をクリックします。

NetFlow のレコードの追加

この手順を使用して、NetFlow レコードを作成します。

フロー レコードでは、パケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。フロー レコードによってフロー用に収集するデータのサイズが決まります。キー フィールドは、*match* キーワードで指定されます。

ステップ 1 **[コンポーネント]** > **[グローバル構成]** に移動します。

ステップ 2 業の先頭のチェックボックスをオンにして、デバイスを選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

ステップ 4 **[グローバル構成の編集（Edit Global Configuration）]** ダイアログ ボックスで、灰色のボタンをクリックして、**ネットフローを有効にします**。

ステップ 5 **[レコードの追加]** をクリックして、次の詳細を入力します。

表 *7:* レコードを追加

フィールド	説明
名前（Name）	レコードの名前。

フィールド	説明
説明	レコードの説明。
収集	コレクション パラメータを定義します。 check box 対応するチェックボックスをオンにして、次の 1 つ以上のパラメータに基づいたコレクションを有効にします。 • Counter Bytes • Counter Packets • IP バージョン • Transport TCP Flags • システム稼動開始時間 • システム稼動終了時間
アクションの	一致パラメータを定義します。 使用可能なオプションは、**レイヤ 2** および**レイヤ 3/4** です。いずれかをクリックして、一致パラメータを選択します。これらのパラメータについては、後続の行で説明します。
レイヤ 2	チェックボックスをオンにして、一致する 1 つ以上のレイヤ 2 パラメータを有効にします。 • 送信元 MAC アドレス • 宛先 MAC アドレス • イーサタイプ • VLAN

フィールド	説明
レイヤ 3/4	チェックボックスをオンにして、一致する 1 つ以上のレイヤ 3 および/またはレイヤ 4 パラメータを有効にします。 • IPプロトコル • IP TOS • Transport Source Port • Transport Destination Port • IPv4 送信元アドレス • IPv4 宛先アドレス • 送信元 IPv6 アドレス • 宛先 IPv6 アドレス • IPv6 フロー ラベル • IPv6 オプション

ステップ 6 **[レコードの追加（Add Record）]** をクリックします。

NetFlow のエクスポータの追加

この手順を使用して、NetFlowエクスポータを作成します。フローエクスポータの設定では、フローに対するエクスポートパラメータを定義し、リモートNetFlow Collectorへの到達可能性情報を指定します。

フローエクスポータでは、NetFlowエクスポートパケットに関して、ネットワーク層およびトランスポート層の詳細を指定します。

ステップ 1 **[コンポーネント]** > **[グローバル構成]** に移動します。

ステップ 2 行の先頭にあるチェック ボックスをオンにしてデバイスを選択します。

ステップ 3 **[アクション]** ドロップダウン メニューから、**[グローバル構成の編集]** を選択します。

ステップ 4 **[グローバル構成の編集]** ダイアログ ボックスで、灰色のボタンをクリックして **Netflow を有効**にします。

ステップ 5 **[エクスポータを追加]** をクリックし、次の詳細を入力します。

表 *8:* エクスポータの追加

フィールド	説明
名前（Name）	エクスポータ名。

フィールド	説明
説明	エクスポータの説明。
宛先（Destination）	エクスポート宛先 IP アドレス。 対応するチェックボックスをオンにして、次のパラメータの 1 つ以上に基づいて収集を有効にします。
ソース（Source）	発信元の IP アドレス。 フローキャッシュが宛先に到達するために経由するデバイス上のインターフェイス。
UDP ポート	NetFlow コレクタが NetFlow パケットをリスニングする UDP ポート。値の範囲は 1 ～ 65535 です。
DSCP	差別化されたコード ポイント値。範囲は 0 ～ 63 です。
バージョン	NetFlow エクスポート バージョン。このフィールドは変更できません。 （注） Cisco NX-OS は、バージョン 9 のエクスポート形式をサポートします。
オプション エクスポータ	フローエクスポータ統計情報の再送信タイマー。値の範囲は 1 ～ 86400 秒です。
テンプレート データ タイムアウト	テンプレートデータ再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。

ステップ 6 **[エクスポータを追加]** をクリックします。

NetFlow のモニターの追加

この手順を使用して、NetFlow モニターを作成します。

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。1 つのモニタに属しているすべてのフローは、様々なフィールド上で照合するために関連するフロー レコードを使用します。データは指定されたフローエクスポータにエクスポートされます。

始める前に

次のように構成を行います。

- レコードの追加
- エクスポーターの追加

ステップ 1 **[コンポーネント]** > **[グローバル構成]** に移動します。

ステップ 2 業の先頭のチェックボックスをオンにして、デバイスを選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

ステップ 4 **[グローバル構成の編集（Edit Global Configuration）]** ダイアログ ボックスで、灰色のボタンをクリックして、**ネットフローを有効にします**。

ステップ 5 **[モニターの追加]** をクリックし、次の詳細を入力します。

表 *9:* モニタを追加

フィールド	説明
名前（Name）	モニターの名前。
説明	モニターの説明。
レコード	**[レコードの選択]** をクリックします。**[レコードの選択]** ウィンドウで、対応するラジオボタンをクリックしてレコードを選択します。選択したレコードの詳細が右側に表示されます。[選択（Select）] をクリックします。
エクスポータ	**[エクスポータを選択]** をクリックします。**[エクスポータの選択]** ウィンドウで、対応するチェック ボックスをオンにしてエクスポーターを選択します。選択したエクスポータの詳細が右側に表示されます。[選択（Select）] をクリックします。 （注） モニターには最大 2 つのフロー エクスポータを選択できます

ステップ 6 **[モニターの追加（Add Monitor）]** をクリックします。

高精度時間プロトコル

PTP（2Precision Time Protocol）デバイスには、オーディナリ クロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、通常のネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。PTP システムは、PTP および非 PTP デバイスの組み合わせで構成できます。

PTP は、システムのリアルタイム PTP クロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスター クロック（階層の最上部にあるクロック）を持つマスター/メンバー同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTP タイ

ミングメッセージを交換することによって実現されます。PTPは、PTPドメインと呼ばれる論理範囲内で動作します。

PTPはネットワークに分散したノードの時刻同期プロトコルです。そのハードウェアタイムスタンプ機能は、優れた精度を提供します。

PTPは、次のプラットフォームでのみサポートされています。

- Cisco Nexus 9200スイッチ
- Cisco Nexus 9300スイッチ — 9300-FX、FX2、EX
- Cisco Nexus 9500スイッチ — 9500-FX、EX
- Cisco Nexus 3548スイッチ

（注） PTPを構成すると、デフォルトのPTP構成が対応するデバイスのすべてのISLポートと同期されます。

PTPの構成については、デバイスのグローバル構成の編集 （22ページ） を参照してください。

NetFlow

NetFlowは入力IPパケットについてパケットフローを識別し、各パケットフローに基づいて統計情報を提供します。NetFlowのためにパケットやネットワーキングデバイスを変更する必要はありません。

Cisco Nexus 9300-FXプラットフォームスイッチでは、フローをモニタするための十分な空き領域を確保するため、ing-netflow TCAMリージョンはデフォルトで512ずつに分割されます。さらに多くのスペースが必要な場合は、**hardware access-list tcam region ing-netflow size** コマンドを使用し、TCAMリージョンのサイズを512の倍数に変更します。

Netflowは、次のプラットフォームでサポートされています。

- Cisco Nexus 9300スイッチ — 9300-FX、FX2、EX
- Cisco Nexus 9500スイッチ — 9500-FX、EX

NetFlowの構成については、デバイスのグローバル構成の編集 （22ページ） を参照してください。

詳細については、『*Cisco Nexus 9000 Series NX-OS* システム管理構成ガイド』を参照してください。

サンプリングされたフロー

NX-APIのNexus Dashboard Data Brokerでサンプリングされた Flow（sFlow）を管理することができます。sFlow使用すると、スイッチやルータを含むデータネットワーク内のリアルタイム

トラフィックをモニターできます。sFlow では、トラフィックをモニタするためにスイッチとルータ上の sFlow エージェント ソフトウェアでサンプリング メカニズムを使用して、サンプル データを中央のデータ コレクタに転送します。

sFLow の構成については、デバイスのグローバル構成の編集 （22 ページ） を参照してください。

入力ポート

[入力ポート] タブには、NDB デバイスの入力ポートの詳細が表示されます。

Edge-SPAN、Edge-TAP、またはリモート ソース Edge-SPAN ポートが NX-API モードの構成で定義されている場合、**spanning-tree bpdufilter enable** コマンドはポートのインターフェイス モードで自動的に構成され、BPDUパケットをフィルタリングします。この構成は、すべての Cisco Nexus 3000 および 9000 シリーズ スイッチに適用されます。

Cisco Nexus シリーズ スイッチのすべてのスイッチ間ポートで **spanning-tree bpdufilter enable** コマンドを設定してください。

次の詳細の表が表示されます。

表 *10 :* 入力ポート

列名	説明
Device	入力ポートが構成されているデバイス。 このフィールドはハイパーリンクです。デバイス名をクリックすると、そのデバイスの詳細情報が表示されます。詳細と手順については、デバイス の章を参照してください。
ポート	入力ポートとして構成されているデバイスのポート。 このフィールドはハイパーリンクです。**ポート**をクリックして、ポートの詳細を表示します。ここから実行できる追加アクションは次のとおりです。 • 入力ポートの編集 • 構成の削除 — ポートはデバイスの入力ポートとして削除されます。
使用中	緑色のチェック マークは、入力ポートが使用中であることを示します。

列名	説明
設定	入力ポートの構成情報（入力ポートの追加（34ページ） で設定されたパラメータに基づく）。
タイプ	ポート タイプ。表示されるオプションは、次のとおりです。 • エッジ ポート-SPAN • エッジポート-TAP • リモート ソース Edge-SPAN • パケットの切り捨て
スパン宛先/タップ名	入力ポートに接続されているスパン宛先の詳細。 • ポートが実稼働スイッチに接続されている場合は、*PS*、続いてデバイス ID、接続されたインターフェイスが表示されます。 • ポートが APIC/ACI コントローラまたは DNAC コントローラに接続されている場合、APIC の場合、DN 値がポッドとパスの詳細とともに表示されます。DNAC の場合、「DNAC」の後に Catalyst デバイス ID とインターフェイスが表示されます。 • ポートが Tap デバイスに接続されている場合、タップ構成名が表示されます。
作成者	入力ポートを作成したユーザー。
変更者	入力ポートを最後に変更したユーザー。

[入力ポート] タブから、次のアクションを実行できます。

- **入力ポートの追加** — これを使用して、新しい入力ポートを追加します。このタスクの詳細については、入力ポートの追加 （34 ページ） を参照してください。
- **入力ポートの削除** — 行の先頭にあるチェック ボックスをオンにして、必要な入力ポートを選択します。**[アクション（Actions）]** < **[入力ポートの削除（Delete Input Port(s)）]** をクリックします。選択したポートが削除されます。

（注） 使用中の入力ポートは削除できません。

チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイスを選択するように、指示メッセージが表示されます。

入力ポートの追加

この手順を使用して、入力ポートを作成します。

デバイスの入力ポートは、トラフィックがパケット ブローカー ネットワークに入り、モニタリング ツールに送信されるポートです。

始める前に

1 つ以上のデバイスを追加します。

一部の入力ポート パラメータは、**[グローバル構成]** タブを使用してデバイス レベルで定義されます。これらのパラメータ（以下にリスト）を定義するには、「デバイスのグローバル構成の編集」を参照してください。

- PTP
- NetFlow
- MPLS フィルタ処理
- Jumbo MTU

ステップ 1 **[コンポーネント]** > **[入力ポート構成]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[入力ポートの追加（Add Input Port）]** を選択します。

ステップ 3 **[入力ポートの追加]** ダイアログ ボックスで、次の詳細を入力します。

表 *11* : 入力ポートの追加

フィールド	説明
全般	
デバイス（Device）	入力ポートが構成されているデバイスを選択するには。 **[デバイスの選択（Select Device）]** をクリックします。**[デバイスの選択]** ウィンドウで、ラジオ ボタンを選択し、デバイスを選択します。[選択（Select）] をクリックします。
ポート	入力ポートとして構成するポートを選択します。 **[ポートの選択]** をクリックします。**[ポートの選択]** ウィンドウで、必要なポートを選択します。[選択（Select）] をクリックします。

フィールド	説明
ポート タイプ	ドロップダウン リストから選択して、入力ポート タイプを定義します。次のオプションがあります。 • **Edge Port- - SPAN** — 実稼働スイッチの構成済みセッションからの着信トラフィック用のエッジ ポートを作成します。 • **Edge Port- TAP** — ISL 上の物理デバイスからの着信トラフィック用のエッジ ポートを作成します。 • **Remote Source Edge - SPAN** — 実稼働スイッチの構成済みリモート セッションからの着信トラフィック用のエッジ ポートを作成します。
ポートの説明	ポートの説明を入力します。
VLAN（QinQ はサポートされていない）	ポートは、実稼働 VLAN 情報を保持するために dot1q として設定されます。VLAN ID は、トラフィックの送信元のポートを識別するために使用されます。 （注） インターフェイスに Q-in-Q を設定した後は、Q-in-Q 構成済みインターフェイスに VLAN フィルタを設定しないでください。
ブロック送信	チェックボックスをオンにして、入力ポートから送信されているトラフィックをブロックします。 （注） ユニキャストおよびマルチキャスト トラフィックのみがブロックされます。
ICMP v6 ネイバー請求をドロップ	チェックボックスをオンにして、すべての ICMP トラフィックをドロップします。 デフォルトでは、Nexus 9300-EX および 9200 シリーズ スイッチの Edge-SPAN および Edge-TAP ポート タイプでは、すべての ICMP トラフィックがブロックされます。残りの Nexus 9000 シリーズ スイッチについて、ユーザーは ICMP トラフィックを拒否またはブロックするために、この機能を手動で有効化しなければなりません。この機能は、現在 NX-OS バージョン I5 以降の NX-API ベースのスイッチに使用できます。

フィールド	説明
タイムスタンプ タギング	チェックボックスをオンにして、タイムスタンプ タギング機能を使用してパケットにタイムスタンプ タグを追加します。 Nexus 9300-EX および 9200 シリーズ スイッチの場合、この機能は Edge-SPAN および Edge-TAP ポートに適用されます。タイムスタンプ タギング機能を設定するには、デバイスで PTP 機能が有効になっていることを確認します。監視デバイスとエッジポートでタイムスタンプ タギングを有効にする必要があります。接続のいずれかの側、Edge-SPAN/Edge-TAP およびモニタリング デバイスでタイムスタンプ タグ付け機能が構成されていない場合、パケットはタイムスタンプでタグ付けされません。 （注） グローバル設定を使用してデバイスで PTP が有効になっていない場合、このオプションはグレー表示されます。
MPLS フィルタリングを有効にする	チェックボックスをオンにし、MPLS フィルタ処理を有効にします。 （注） グローバル設定を使用してデバイスに対して MPLS フィルタ処理が有効になっていない場合、このオプションはグレー表示されます。
ジャンボ MTU を適用	チェックボックスをオンにして、このポートで設定されたジャンボ MTU 値を有効にします。 （注） グローバル構成を使用してデバイスにジャンボ MTU が構成されていない場合、このオプションはグレー表示されます。
Netflow モニター	ドロップダウン リストからオプションを選択します。グローバル構成レベルで作成されたモニター名がここにリストされています。 （注） グローバル設定を使用してデバイスに対して NetFlow が有効になっていない場合、このオプションはグレー表示されます。

各**ポート タイプ**に表示されるフィールドについては、以下で説明します。

a) （**ポート タイプ** — エッジ ポート-SPAN の場合のみ）次の詳細を入力します。

フィールド	説明
接続先デバイスのタイプ	これは、入力ポートのソース（スパン宛先）です。 ドロップダウン リストから、必要なオプションを選択します。次のオプションがあります。 • コントローラ • 生産スイッチ 上記のそれぞれのオプションについては、後続の行で説明します。
コントローラ	**[コントローラの選択]** をクリックします。**ACI** または **DNAC** を選択します。
宛先デバイス タイプのフィールド：**コントローラ > ACI** （注）　スパン先を設定する前に、APIC/ACI デバイスを追加する必要があります。	
スパン先名	スパン先の名前を入力します。
ポッド	ポッドを選択します。
ノード	ノードを選択します。
[ポート（Port）]	ポートを選択します。
[MTU]	APIC のスパン先の MTU 値を設定します。
宛先デバイス タイプのフィールド: **コントローラ > DNAC**	
スパン先名	スパン先の名前を入力します。
SPAN 先ポート	**[SPAN 先ポート]** をクリックし、Catalyst スイッチとポートを選択します。
宛先デバイス タイプのフィールド: 生産スイッチ （注）　スパン先を構成する前に、Nexus または Catalyst デバイスを追加する必要があります。	
スパン先デバイス	**[デバイスの選択]** をクリックし、デバイスを選択します。
スパン先ポート	**[ポートの選択]** をクリックして、ポートを選択します。

b) （**ポート タイプ** — エッジ ポート-TAP のみ）次の詳細を入力します。

フィールド	説明
タップ構成名	ドロップダウン リストから [タップ構成] を選択します。
タップ構成タイプ	タップデバイスからミラーリングされたトラフィックを受信する NDB デバイスのポートを選択します。 表示されるオプションは、選択した**タップ構成名**の詳細に基づいています。タップ構成の追加 （60 ページ）中にミラー ポートのいずれかまたは両方をタップすることを選択した場合、対応する NDB エッジ ポート-タップ ポートが表示されます。

c) （**ポート タイプ** — リモート ソース Edge-SPAN の場合のみ）次の詳細を入力します。

（注） リモート ソースからのトラフィックを受信するために、最大 4 つのリモート ソース Edge-SPAN ポートを構成できます。

フィールド	説明
リモート入力終了セッション	
ERSPAN ID	ERSPAN ID を入力します。指定できる範囲は 1 ～ 1023 です。 ここで入力された ERSPAN ID は、リモート ソースのソース セッション ID と一致します。
ループバック インターフェイスの使用	チェックボックスをオンにして、ループバック インターフェイスを使用します。
ループバック（**Loopback**）	**[ループバックの選択]** をクリックして、ループバック インターフェイスを選択します。構成されたループバック インターフェイスがない場合は、**[ループバックの追加]** をクリックします。「ループバックの構成」を参照してください。 ループバック インターフェイスを使用して、複数のリモート入力ポートを用意します。L3 インターフェイスからのトラフィックは、ループバック インターフェイスに到達し、そこからセッションの宛先ポートに到達します。最初のリモート ソース エッジ スパン入力ポートがループバックで作成された場合、次のリモート ソース エッジ SPAN ポートも同じループバック インターフェイスで設定する必要があります。最初のリモート ソース エッジ スパン入力ポートがループバックなしで作成された場合、次のリモート ソース エッジ SPAN ポートもループバック インターフェイスなしで設定する必要があります。

フィールド	説明
セッション宛先	**[宛先ポートの選択]** をクリックして、宛先ポートを選択します（NDB デバイス上）。（（
リモート入力セッション	
[リモート入力ポート（Remote Input Port）]	**[リモート入力ポート]** をクリックし、（NDB デバイス上の）リモート入力ポートを選択します。 （注） リモート ソース Edge-SPAN ポートに到達するトラフィック用に構成できるリモート入力ポートは 1 つだけです。ループバック インターフェイスを設定している場合、リモート入力ポートは、リモート ソース エッジ SPAN ポートごとに異なる可能性があります。
IP アドレス	IP アドレスを入力します。ここで入力する IP アドレスは、L3 ネットワーク経由でパケットが到達するリモート送信元ポートの IP アドレスです。 この値を入力する必要があるのは、最初のリモート ソース Edge-SPAN ポートを構成する場合だけです。構成する次の 3 つのポートでは、同じ IP アドレスがリモート ソース エッジ SPAN ポートを持つ 4 つのセッションすべてに適用されるため、このフィールドはグレー表示されます。
宛先デバイスのタイプ	ドロップダウン リストから [デバイス タイプ] を選択します リモート ソース Edge-SPAN ポートの場合、サポートされる宛先タイプは ACI です。
スパン先 ACI ファブリック	**[ACI ファブリックの選択]** をクリックし、ACI ファブリックを選択します。
スパン先名	スパン先の名前を入力します。
テナント	**[テナントの選択（Select Tenant）]** をクリックして、テナントを選択します。
アプリケーション プロファイル	**[アプリケーション プロファイルの選択]** をクリックして、アプリケーション プロファイルを選択します。
EPG	**[EPG の選択]** をクリックして、EPG を選択します。
送信元 IP アドレス	送信元 IP アドレスを入力します。この IP アドレスは、ソース パケットの IP サブネットのベース IP アドレスです。

フィールド	説明
宛先 IP アドレス	このフィールドには自動的に値が入力されます。 ここで入力されるIPアドレスは、**リモート入力ポート**のIP アドレスとして入力したものと同じアドレスです。 （注） APIC/ACI デバイスの場合、これは宛先ポート（リモート入力ポート）であるため、宛先 IP と呼ばれます。
フロー ID	このフィールドには自動的に値が入力されます。 フローIDは、SPANパケットのフローIDです。これは、リモート ソース エッジ SPAN ポートに以前に指定された ERSPAN ID と一致します。
TTL	TTL 値を入力します。デフォルト値は 64 ホップです。
DSCP	ドロップダウン リストから DSCP 値を選択します。
[MTU]	スパン宛先ポートの MTU 値を入力します。範囲は 64 ～ 9216 です。

ステップ 4 **[入力ポートの追加]** をクリックします。

ループバックの構成

この手順を使用して、リモート ソースエッジ スパン入力ポートのループバックを設定します。

ステップ 1 **[入力ポート]** > **[アクション]** > **[入力ポートの追加]** に移動します。

ステップ 2 **[ポート タイプ（Port Type）]** を [リモート ソース エッジ スパン ポート（Remote Source Edge Span Port）] として選択し、**[ループバック インターフェイスの使用（Use Loopback Interface）]** チェックボックスをオンにして、ループバック インターフェイスを選択します。

ステップ 3 **[ループバックの構成（Configure Loopback）]** をクリックして、新しいループバック インターフェイスを作成します。

[ループバックの構成（Configure Loopback）] ダイアログ ボックスで、次の詳細を入力します。

表 *12 :* ループバックの構成

フィールド	説明
全般	
ループバックID	ループバック ID を入力します。

フィールド	説明
IP アドレス	ループバック IP アドレスを入力します。

ステップ 4 **[ループバックの構成（Configure Loopback）]** をクリックします。

モニタリングツール

[モニタリング ツール] タブには、NDB デバイスのモニタリング ツール ポートの詳細が表示されます。NDB デバイスのモニタリング ツール ポートからのトラフィックは、モニタリング ツールに送信されます。

次の詳細の表が表示されます。

表 *13*：モニタリングツール

列名	説明
Status	ステータスは、2つの列を使用して定義されます。 最初の列は、モニタリングツールのトラフィックを示しています。 • 緑-モニタリングツールが現在トラフィックを伝送していることを示します。 • 黄色 - モニタリング ツールが現在トラフィックを伝送していないことを示します。 2 番目の列は、モニタリング ツール ポートとモニタリング ツール間のリンクの状態を示します。モニタリングツール ポートとモニタリング ツール間のリンクが稼働している場合、色は緑色です。 • 緑色：リンクが起動して動作していることを示します。 • 赤色：リンクがダウンしていることを示します。 • 黄色 - リンクが管理上ダウンしていることを示します。

列名	説明
モニタリング ツール	モニタリング ツール名。 このフィールドはハイパーリンクです。**モニタリング ツール**名をクリックします。右側に新しいペインが表示され、モニタリング ツールに関する詳細が表示されます。次の追加アクションがここで実行できます。 • モニタリング ツールの編集 （47 ページ）
ポート	モニタリング ツール ポート（デバイス付き）。 ポートの詳細を表示するには、**ポート**名をクリックします。次の追加アクションがここで実行できます。 • モニタリング ツールの編集 （47 ページ）
[タイプ（Type）]	モニタリング ツールのタイプ。次のオプションがあります。 • ローカル モニタリング ツール - ローカル ネットワークの NDB デバイス上にあるポート（L2 ポート）。 • リモート モニタリング ツール - ローカル ネットワークの外部にあり、L3 ネットワーク経由で到達可能なポート。
使用中	モニタリング ツール ポートが使用されている場合は、緑色のチェック マークが表示されます。それ以外の場合は空白のままです。
パケットの切り捨て	モニタリング ツール ポートでパケットの切り捨てが有効になっている場合は、緑色のチェック マークが表示されます。それ以外の場合は空白のままです。
ブロック受信	モニタリング ツールからモニタリング ツール ポート（NDB デバイス上）への着信トラフィックがブロックされている場合、**[はい]** が表示されます。
作成者	モニタリング ツールを作成したユーザー。

列名	説明
最終更新者	モニタリング ツールを最後に変更したユーザー。

[モニタリング ツール] タブから、次のアクションを実行できます。

- **モニタリング ツールの追加** — これを使用して、新しいモニタリング デバイスを追加します。このタスクの詳細については、「モニタリング ツールの追加」の追加を参照してください。
- **モニタリング ツールの削除** — 行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。選択したデバイスが削除されます。**[アクション（Actions）]** < **[モニタリング ツールの削除（Delete Monitoring Tool(s)）]** をクリックします。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイスを選択するように、指示メッセージが表示されます。

（注） 使用中のモニタリング ツールは削除できません。

モニタリング ツールの追加

この手順を使用して、モニタリング ツール ポートを追加します。次のものを作成できます。

- ローカル モニタリング ツール - ローカル ネットワークの NDB デバイス上にあるポート（L2 ポート）。
- リモート モニタリング ツール - ローカル ネットワークの外部にあり、L3 ネットワーク経由で到達可能なポート。

パケットの出力ポートであるモニタリング ツールに関連付けるパケットの切り捨てポート（入力トラフィックをブロックするために使用）を作成できます。

始める前に

制約事項：

- 接続ごとに、スイッチごとに複数のリモート配信ポートを使用することはできません。
- インター スイッチド リンクを含むリモート モニタリング ツールは、ISL ごとに 1 つの接続のみに制限されます。
- 監視ツールをパケット切り捨てインターフェイスで使用する場合は、パケット切り捨てポートのステータスが管理上(緑色のアイコン)であり、リンクのもう一方の端がどのNDBデバイスにも接続されていないことを確認します。ポートのレイヤ 2 ステータスを Up に変更するには、別の非 NDB デバイスに接続して、サード パーティのループバック光ファイバを使用してループバックを作成する必要があります。

（注） スイッチ上でパケットの切り捨てを使用して、最大4つのモニタリング ツールを設定できます。

ステップ 1 **[コンポーネント（Components）]** > **[モニタリング ツール（Monitoring Tools）]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[モニタリング ツールの追加（Add Monitoring Tool）]** を選択します。

ステップ 3 **[モニタリング ツールの追加（Add Monitoring Tool）]** ダイアログ ボックスで、次の詳細を入力します。

表 *14 :* モニタリング ツールの追加

フィールド	説明
全般	
モニタリング ツール名	モニタリング ツール名の名前を入力します。
デバイス名（Device Name）	**[デバイスの選択（Select Device）]** をクリックします。表示されたデバイス一覧から、ラジオ ボタンでデバイスを選択します。デバイスの詳細が右側に表示されます。 モニタリング ツールのポートはこのデバイスにあります。 **[デバイスの選択（Select Device）]** をクリックします。
[ポート（Port）]	**[ポートの選択]** をクリックします。開いた **[インターフェイスの選択（Select Interface）]** ウィンドウで、ラジオ ボタンを使用してポートを選択します。表示されるインターフェースは、選択したデバイスによって異なります。 [選択（Select）] をクリックします。 選択したポートはモニタリング ツール ポートとしてマークされます。トラフィックはここからモニタリング ツールにリダイレクトされます。
ポートの説明	ポートの説明を入力します。

フィールド	説明
ローカル モニタリング ツール	ラジオ ボタンでローカル モニタリング ツールを選択します。このオプションを選択することで、モニタリングデバイスがローカル ネットワークから指定されます。 次のオプションは、ローカルモニタリングデバイスに対して表示されます（以下の行で詳細が説明されます）。 • Block Rx • ICMPv6 ネイバー勧誘をブロック • タイムスタンプ タギングの有効化 • パケットの切り捨て • タイムスタンプ ストリップの有効化 • ジャンボ MTU の適用
Rx のブロック	モニタリング ツールからのトラフィックをブロックします（NDB デバイスのモニタリング ツール ポートに指定）。このオプションは、デフォルトで選択されます。チェックボックスをオフにすることで、このオプションをオフにすることができます。 （注） Rx トラフィックは、N9K-X97160YC-EX ラインカード（NX-OS 9.3(3) 以降）を搭載した Cisco N9K-95xx スイッチの単方向イーサネットを使用してブロックされます。
ICMPv6 ネイバー勧誘をブロック	モニタリング ツールからの ICMP トラフィックをブロックします（NDB デバイスのモニタリング ツール ポートに指定）。このオプションは、デフォルトで選択されます。チェックボックスをオフにすることで、このオプションをオフにすることができます。 Nexus 9300-EX および 9200 スイッチでサポートされます。残りの Nexus 9000 シリーズ スイッチについて、ユーザーは ICMP トラフィックを拒否またはブロックするために、この機能を手動で有効化しなければなりません。

フィールド	説明
タイムスタンプ タギングの有効化	チェックボックスをオンにして、タイムスタンプ タギングを有効にします。タイムスタンプ タグは、モニタリング ツール ポートのすべての送信パケットに追加されます。 単一のデバイスまたは複数のデバイスで、この機能を構成できます。 タイムスタンプ タギングを構成するために、デバイスで PTP が有効になっていることを確認します。モニタリング デバイスとエッジ ポートでタイムスタンプを有効にする必要があります。タイムスタンプのタグ付けが接続のいずれかの側で構成されていない場合、Edge-SPAN/Edge-TAP とモニタリング ツール、次にパケットがタイムスタンプにタグ付けされていません。
パケットの切り捨て	Check the check box to enable packet truncation and enter the MTU siz パケットの切り捨ては、MTUサイズに基づいて着信パケットからバイトを破棄します。これは、必要なトラフィックのみをモニタリング ツールのポートに送信するために行われます。これは、トラフィックを入力ポートからパケットの切り捨てポートにリダイレクトすることによって実現されます。パケットチューニング ポートからの切り捨てられたパケットは、監視ツールに到達します。 パケットの切り捨てポートを設定するには、**[パケットの切り捨てポートの選択（Select Packet Truncation Port）]** をクリックします。詳細な手順については、パケット切り捨てポートの追加 （50 ページ） を参照してください。
タイムスタンプ ストリップの有効化	チェックボックスをオンにして、タイムスタンプ ストリップを有効にします。これは送信元パケットからタイムスタンプ タグを削除します。
ジャンボ MTU を適用	チェックボックスをオンにして、ジャンボ MTU を有効にします。 ジャンボ MTU にデバイスのより大きなパケット サイズを設定します。**ジャンボ MTU** を **グローバル構成**で有効にして、デバイスのポートにジャンボ MTU サイズを適用します。

フィールド	説明
リモート モニタリング ツール	ラジオ ボタンでリモート モニタリング ツールを選択します。このオプションを選択することで、リモート ネットワークからのモニタリング デバイスが有効になります。 次のオプションは、リモートモニタリングデバイスに対して表示されます（以下の行で詳細が説明されます）。 • Block Rx • インターフェイスIP • 宛先 IP • ERSPAN ID
インターフェイスIP	モニタリング ツール ポートに割り当てられるIPアドレス。
宛先 IP	ERSPAN が終端し、選択したポートから到達可能になる IP アドレス。
ERSPAN ID	ERSPAN ID を入力します。範囲は 1 ～ 1023 です。 Cisco Nexus 9300 FX および EX シリーズ スイッチの Encapsulated Remote Switch Port Analyzer（ERSPAN）送信元セッション機能を使用して、ネットワーク外のデバイスをモニタリング デバイスとして使用できます。

ステップ 4 **[モニタリング ツールの追加]** をクリックします。

モニタリング ツールの編集

この手順を使用して、モニタリング ツールのパラメータを編集します。

始める前に

1 つ以上のモニタリング ツールを追加します。

ステップ 1 **[コンポーネント（Components）]** > **[モニタリング ツール（Monitoring Tools）]** に移動します。

ステップ 2 表示された表で、監視ツール名をクリックします。

新しいペインは右側に表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[編集（Edit）]** を選択します。

ステップ 4 **[モニタリング ツールの編集]** ダイアログボックスには、モニタリング ツールの最新の情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *15 :* モニタリング ツールの編集

フィールド	説明
全般	
モニタリング ツール名	モニタリング ツール名が表示されます。これは編集できません。
デバイス名（**Device Name**）	モニタリング ツール ポートが存在するデバイス。
[ポート（Port）]	モニタリング ツールのポート。
ポートの説明	ポートの説明を入力します。
ローカル モニタリング ツール	ラジオ ボタンを選択して、ローカル モニタリング デバイスを選択します。このオプションを選択すると、モニタリングデバイスはローカルネットワークからのものになります。 ローカルモニターデバイスには次のオプションが表示されます (以下の行で詳しく説明します)。 • Block Rx • ICMPv6 ネイバー勧誘をブロック • タイムスタンプ タギングの有効化 • パケットの切り捨て • タイムスタンプ ストリップの有効化 • ジャンボ MTU を適用
Rx のブロック	モニタリング ツールから (NDB デバイスのモニタリング ツール ポートへの) トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすることで、このオプションをオフにすることができます。 （注） Rx トラフィックは、N9K-X97160YC-EX ライン カード（NX-OS 9.3(3) 以降）を搭載した Cisco N9K-95xx スイッチの単方向イーサネットを使用してブロックされます。

フィールド	説明
ICMPv6 ネイバー勧誘をブロック	モニタリングツールから（NDBデバイスの監視ツールポートへの）ICMP トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすることで、このオプションをオフにすることができます。 Nexus 9300-EX および 9200 スイッチでサポートされます。残りの Nexus 9000 シリーズ スイッチについて、ユーザーは ICMP トラフィックを拒否またはブロックするために、この機能を手動で有効化しなければなりません。
タイムスタンプ タギングの有効化	チェックボックスをオンにして、タイムスタンプのタグ付けを有効にします。タイムスタンプ タグは、モニタリング ツール ポートのすべての送信パケットに追加されます。 単一のデバイスまたは複数のデバイスで、この機能を構成できます。 タイムスタンプ タギングを構成するために、デバイスで PTP が有効になっていることを確認します。モニタリング デバイスとエッジポートでタイムスタンプを有効にする必要があります。タイムスタンプのタグ付けが接続のいずれかの側で構成されていない場合、Edge-SPAN/Edge-TAP とモニタリング ツール、次にパケットがタイムスタンプにタグ付けされていません。
パケットの切り捨て	Check the check box to enable packet truncation and enter the MTU siz 監視ツールの追加時にパケット切り捨てポートが構成されていない場合、**[パケット切り捨てポートの選択]** は無効になります。
タイムスタンプ ストリップの有効化	チェックボックスをオンにして、タイムスタンプ ストリップを有効にします。これは送信元パケットからタイムスタンプ タグを削除します。
ジャンボ MTU の適用	チェックボックスをオンにして、ジャンボ MTU を有効にします。 ジャンボ MTU にデバイスのより大きなパケット サイズを設定します。**ジャンボ MTU** を **グローバル構成**で有効にして、デバイスのポートにジャンボ MTU サイズを適用します。

フィールド	説明
リモート モニタリング ツール	ラジオ ボタンでリモート モニタリング ツールを選択します。このオプションを選択することで、リモート ネットワークからのモニタリング デバイスが有効になります。 次のオプションは、リモートモニタリングデバイスに対して表示されます（以下の行で詳細が説明されます）。 • Block Rx • インターフェイスIP • 宛先 IP • ERSPAN ID
インターフェイスIP	モニタリング ツール ポートに割り当てられる IP アドレス。
宛先 IP	ERSPAN が終端し、選択したポートから到達可能になる IP アドレス。
ERSPAN ID	ERSPAN ID を入力します。範囲は 1 ～ 1023 です。 Cisco Nexus 9300 FX および EX シリーズ スイッチの Encapsulated Remote Switch Port Analyzer（ERSPAN）送信元セッション機能を使用して、ネットワーク外のデバイスをモニタリング デバイスとして使用できます。

ステップ 5 **[保存（Save）]** をクリックします。

パケット切り捨てポートの追加

この手順を使用して、パケット切り捨てポートを作成します。パケット切り捨てポートは、モニタリング ツール ポートの入力ポートとして機能します。したがって、作成されたパケット モニタリング ツールポートは入力ポートとしてリストされ、未使用のパケット切り捨てポートは 入力ポート （32 ページ） タブから削除できます。

始める前に

パケットの切り捨てでは、指定されたバイト位置から始まるパケットからバイトを破棄します。指定されたバイト位置以降のデータはすべて切り捨てられます。目的の主な情報がパケットのヘッダーまたはパケットの最初の部分にある場合、パケットの切り捨てが必要です。

表 *16 :* パケット切り捨てのサポート

EX シャーシ	FX シャーシ	Nexus 9364C、Nexus 9332C	Nexus 9336 C FX2	-EX または -FX LC を備えた EOR スイッチ
MTU サイズの範囲は 320 ～ 1518 バイトです	MTU サイズの範囲は 64 ～ 1518 バイトです	MTU サイズの範囲は 64 ～ 1518 バイトです	MTU サイズの範囲は 64 ～ 1518 バイトです	LC に依存します

ステップ 1 **[コンポーネント]** > **[モニタリング ツール]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[モニタリング ツールの追加（Add Monitoring Tool）]** を選択します。

ステップ 3 デバイスとポートを選択し、**[パケット切り捨て]** チェックボックスをオンにして、パケット切り捨てを有効にします。

ステップ 4 **[パケット切り捨てポートの選択]** をクリックします。

ステップ 5 表示される **[パケット切り捨てポートの選択]** ウィンドウで、**[パケット切り捨てポートの追加]** をクリックします。

ステップ 6 **[パケット切り捨ての追加（Add Packet Truncation）]** ダイアログ ボックスで、次の詳細を入力します。

表 *17 :* パケット切り捨ての追加

フィールド	説明
全般	
Device	デバイス名が下に表示されます。
ポート	**[ポートの選択]** をクリックします。**[ポートの選択]** ウィンドウで、ラジオボタンを選択してポートを選択します。 **[送信（Submit）]** をクリックします。
ポート タイプ	デフォルトでは、パケット切り捨てポートが選択されています。
ポートの説明	切り捨てポートのポートの説明。
ICMPv6 ネイバー請求をドロップ	パケット トランケーション ポートの入力 ICMP トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすると、このオプションをオフにできます。

ステップ 7 [追加（Add）] をクリックします。

ポート グループ

[ポート グループ（Port Groups）] タブには次のサブタブがあります。

- **入力ポート グループ** — デバイスの（またはデバイス全体の）入力ポートがグループ化されて、入力ポート グループを形成します。詳細については、入力ポート グループを参照してください。
- **モニタリング ツール グループ** ：デバイスの（またはデバイス全体の）モニタリング ツール ポートがグループ化されて、モニタリング ツール グループが形成されます。詳細については、ツール グループのモニタリングを参照してください。

入力ポート グループ

デバイス（またはさまざまなデバイス）の入力ポートがグループ化されて、ポート グループが形成されます。ポート グループは、さまざまなデバイスのエッジ スパン ポートとエッジ タップ ポートの組み合わせにすることができます。接続を作成する間に、入力ポートを個別に選択する代わりに、複数の入力ポートをグループ化して同時に選択することができます。

次の詳細の表が表示されます。

表 *18 :* 入力ポート グループ

列名	説明
入力ポート グループ名	入力ポート グループ名。 このフィールドはハイパーリンクです。**入力ポート グループ名**をクリックします。入力ポート グループに関する詳細情報を提供する新しいペインが右側に表示されます。ここから実行できる追加のタスクは次のとおりです。 • 入力ポート グループの編集
説明	入力ポート グループの説明。
関連づけられた接続	グループに関連付けられた接続。
メンバー	グループのメンバー入力ポートの数。
作成者	グループを作成したユーザー。
最終修正者	グループを最後に修正したユーザー。

[入力ポート グループ] タブから、次のアクションを実行できます。

- **入力ポート グループの追加** — これを使用して、新しい入力ポート グループを追加します。このタスクの詳細については、「入力ポート グループの追加」を参照してください。
- **入力ポート グループの削除** — 行の先頭にあるチェック ボックスをオンにして、削除する入力ポート グループを選択し、**[アクション]** > **[入力ポート グループの削除]** をクリックします。選択した入力ポート グループが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。入力ポート グループを選択するよう求められます。

入力ポート グループの追加

この手順を使用して、入力ポート グループを作成します。

接続の作成中に、入力ポートを個別に選択する代わりに、グループ化することで複数の入力ポートを同時に選択できます。

始める前に

1 つ以上のデバイスを作成します。

ステップ 1 **[コンポーネント]** > **[ポート グループ]** > **[入力ポート グループ]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[入力ポートの追加（Add Input Port）]** を選択します。

ステップ 3 **[入力ポート グループの追加]** ダイアログ ボックスで、次の詳細を入力します。

表 *19* : 入力ポート グループの追加

フィールド	説明
全般	
グループ名	入力ポート グループの名前を入力します。
説明	グループの説明を入力します。
ノードの選択	*[*すべてのノード*]* ボックスで、ラジオ ボタンをクリックしてデバイスを選択します。
ポートの選択	入力ポートとして構成されているポートが表示されます。ポートをクリックして選択します。**[すべて追加]** をクリックして、デバイスのすべての (入力) ポートを選択できます。
選択したポート	選択したポートがここに入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの横に表示されている×印をクリックします。**[すべて削除]** をクリックして、選択したすべてのポートを削除できます。

ステップ 4 **[入力ポート グループの追加（Add Input Port Group）]** をクリックします。

入力ポート グループの編集

この手順を使用して、入力ポート グループのパラメータを編集します。

始める前に

1 つ以上の入力ポート グループを作成します。

ステップ 1 **[コンポーネント（Components）]** > **[ポート グループ（Port Groups）]** > **[入力ポート グループ（Input Port Group）]** に移動します。

ステップ 2 表示された表で、**入力ポート グループ**名をクリックします。

新しいペインは右側に表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[入力ポート グループの編集（Edit Input Port Group）]** を選択します。

ステップ 4 **[入力ポート グループの編集]** ダイアログ ボックスに、グループの現在の情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *20 :* 入力ポート グループの編集

フィールド	説明
全般	
グループ名	入力ポート グループ名。
説明	グループの説明です。
ノードの選択（Select Node）	*[*すべてのノード（*All Nodes*）*]* ボックスから、ラジオ ボタンをクリックしてデバイスを選択します。
ポートの選択	入力ポートとして構成されているポートが表示されます。ポートをクリックして、選択します。**[すべて追加]** をクリックして、デバイスのすべてのポートを選択できます。
選択したポート	選択したポートがここに自動入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの隣のバツ印（x）をクリックします。**[すべてを削除（Remove All）]** をクリックして、すべての選択したポートを削除します。

ステップ 5 **[入力ポート グループの編集（Edit Input Port Grou）]** をクリックします。

ツール グループのモニタリング

デバイス間でグループ化されたモニタリング ツール ポートは、モニタリング ツール グループを形成します。

次の詳細の表が表示されます。

表 *21 :* ツール グループのモニタリング

列名	説明
モニタリング ツール グループ名	モニタリング ツール グループ名 このフィールドはハイパーリンクです。**モニタリング ツールのグループ名**をクリックします。右側に新しいペインが表示され、モニタリング ツール グループに関する詳細情報が提供されます。ここから実行できる追加のタスクは次のとおりです。 • モニタリング ツール グループの編集
説明	モニタリング ツール グループの説明。
関連する接続	モニタリング ツール グループを利用した接続。
メンバー	グループのメンバーモニタリングツールのポート数。
作成者	グループを作成したユーザー。
最終修正者	最後にグループを修正したユーザー。

[モニタリング ツール グループ] タブから、次のアクションを実行できます。

- **モニタリング ツール グループの追加** — これを使用して、新しいモニタリング ツール グループを追加します。このタスクの詳細については、「モニタリング ツール グループの追加」を参照してください。
- **モニタリング ツール グループの削除** — 行の先頭にあるチェックボックスをオンにして、削除するツール グループを選択し、**[アクション]** > **[モニタリング ツール グループの削除]** をクリックします。選択したツール グループが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。ツール グループを選択するように求められます。

モニタリング ツール グループの追加

この手順を使用して、モニタリング ツール グループを作成します。

始める前に

1 つ以上のモニタリング ツールを作成します。

ステップ 1 **[コンポーネント（Components）]** > **[ポート グループ（Port Groups）]** > **[モニタリング ツール グループ（Monitoring Tool Group）]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[モニタリング ツール グループの追加（Add Monitoring Tool Group）]** を選択します。

ステップ 3 **[モニタリング ツール グループの追加（Add Monitoring Tool Group）]** ダイアログ ボックスで、次の詳細を入力します。

表 *22*：モニタリング ツール グループの追加

フィールド	説明
全般	
グループ名	モニタリング ツール グループ名の名前を入力します。
説明	グループの説明を入力します。
ノードの選択	*[*すべてのノード*]* ボックスで、ラジオ ボタンをクリックしてデバイスを選択します。
ポートの選択	モニタリング ツール ポートとして構成されるポートが表示されます。ポートをクリックして選択します。**[すべて追加]** をクリックして、デバイスのすべての（モニタリング）ポートを選択できます。
選択したポート	選択したポートがここに入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの横に表示されている×印をクリックします。**[すべて削除]** をクリックして、選択したすべてのポートを削除できます。

ステップ 4 **[モニタリング ツール グループの追加]** をクリックします。

モニタリング ツール グループの編集

この手順を使用して、モニタリング ツール グループのパラメータを編集します。

始める前に

1 つ以上のモニタリング ツール グループを作成します。

ステップ 1 **[コンポーネント]** > **[ポート グループ]** > **[モニタリング ツール グループ]** に移動します。

ステップ 2 表示された表で、**モニタリング ツール グループ**名をクリックします。

新しいペインが右側に表示されます。

ステップ 3 **[アクション]** をクリックし、**[モニタリング ツール グループの編集]** を選択します。

ステップ 4 **[モニタリング ツールグループの編集]** ダイアログボックスに、現在のグループの情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *23*：モニタリング ツールグループの編集

フィールド	説明
全般	
グループ名	モニタリング ツール グループの名前。
説明	グループの説明。
ノードの選択（**Select Node**）	*[*すべてのノード（*All Nodes*）*]* ボックスから、ラジオ ボタンをクリックしてデバイスを選択します。
ポートの選択	モニタリング ツールのポートとして設定されているポートが表示されます。ポートをクリックして、選択します。**[すべて追加]** をクリックして、デバイスのすべての（モニタリング）ポートを選択できます。
選択したポート	選択したポートがここに自動入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの隣のバツ印（x）をクリックします。**[すべてを削除（Remove All）]** をクリックして、すべての選択したポートを削除します。

ステップ 5 **[モニタリング ツール グループの編集]** をクリックします。

スパン宛先

[スパン宛先（Span Destination）] タブには、NDB デバイスの入力ポートに接続されているスパン ポートの詳細が表示されます。スパン宛先は、入力ポートのトラフィックの送信元（ACI または NX-OS デバイスから）です。L2 スパン宛先（ローカル）はエッジ スパン ポートに作成され、L3 スパン宛先 (リモート) はリモート エッジ スパン ポートに作成されます。

次の詳細の表が表示されます。

表 *24 :* スパン宛先

列名	説明
名前	スパン宛先ポートの名前。
宛先（**Destinations**）	スパン宛先が ACI/APIC、DNAC、Nexus、またはCatalystデバイス上にあるかどうかを示します。
入力ポート	スパン先に接続されているNDBデバイスの入力ポート。
入力タイプ タイプ	入力ポート タイプ。次のオプションがあります。 • エッジ スパン ポート • リモート ソース エッジ スパン ポート
スパン デバイス	スパンデバイス（トラフィック ソース）。次のオプションがあります。 • APIC/ACI または DNAC コントローラ • CatalystまたはNexus スイッチ（実稼働スイッチ）
作成者	スパン宛先を作成したユーザー。
最終更新者	スパン宛先を最後に更新したユーザー。

[スパン宛先] タブから、次のアクションを実行できます。

- **[スパン宛先の削除]**：行の先頭にあるチェックボックスをオンにして、削除するスパン先を選択し、**[アクション]** > **[スパン宛先の削除]** をクリックします。選択したスパン宛先が削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。スパン宛先を選択するよう求められます。

（注） スパン宛先の追加については、入力ポートの追加 （34 ページ） の手順を参照してください。スパン宛先（ACI/NX-OS デバイス上）は、NDB デバイスの入力ポートに接続されています。ACI/NX-OS デバイスがネットワークに正常に追加された後にのみ、SPAN 宛先を追加できます。

APIC SPAN 宛先の場合、入力ポートを Edge-SPAN ポートとして構成し、そのポートが ACI 側に接続されている場合、ACI側からポッド、ノード、およびポートを選択し、ポートをスパン

宛先として構成できます。 NX-OS（実稼働スイッチ）の SPAN 宛先の場合、入力ポートを Edge-SPAN ポートとして設定し、ポートが NX-OS デバイスに接続されている場合、NX-OS デバイスのノードとポートを選択し、 SPAN 宛先としてのポート。

タップ構成

[タップ構成] タブには、Nexus Dashboard Data Broker コントローラーのタップ構成の詳細が表示されます。このタブには、タップ デバイスのネットワーク ポートとミラー ポート、およびタップ デバイスに接続されている NDB デバイス ポートのマッピングに関する情報が表示されます。

票には次の詳細が表示されます。

表 *25*：タップ構成

列名	説明
Tap Name	タップ構成名。 タップ名をクリックします。新しいペインが右側に表示されます。次の追加手順を実行できます。 • タップ構成の編集 （62 ページ）
Device	タップ構成が作成されるタップ デバイス。
Port-1	実稼働ネットワークからトラフィックを受信するタップ デバイスのポート。
Port-2	本番ネットワークからトラフィックを受信するタップ デバイスのポート。
Port-1 Mirror	タップ デバイスの **Port-1** からミラーリングされたトラフィックを受信し、NDB Port-1 Edge Port-TAP に転送するタップ デバイスのポート。
Port-2 Mirror	タップ デバイスの **Port-2** からミラーリングされたトラフィックを受信し、NDB Port-2 Edge Port-TAP に転送するタップ デバイスのポート。
Port-1 Edge Port-TAP	タップ デバイスの **Port-1 Mirror** ポートからトラフィックを受信する NDB デバイスのポート。

列名	説明
Port-2 Edge Port-TAP	タップ デバイスの **Port-2 Mirror** ポートからトラフィックを受信する NDB デバイスのポート。
作成者	タップ構成を作成したユーザー。
変更者	タップ構成を変更したユーザー。

[タップ構成] タブから、次のアクションを実行できます。

- **[タップ構成の追加]**— これを使用して、タップ構成を追加します。詳細については、タップ構成の追加 （60 ページ）を参照してください。
- **[タップ構成の編集]** — これを使用して、既存のタップ構成を編集します。詳細については、タップ構成の編集 （62 ページ）を参照してください。
- **[タップ構成の削除]**—行の先頭にあるチェックボックスをオンにして、削除するタップ構成を選択し、**[アクション]** > **[タップ構成の削除]** をクリックします。
- **[タップ構成の同期（Sync Tap Configuration）]** — このオプションを使用して、タップ デバイスのタップ設定を Nexus Dashboard Data Broker コントローラのタップ設定と同期します。

タップ構成の追加

タップ構成を追加するために、この手順を使用します。

始める前に

1 つ以上のタップ デバイスを追加します。

ステップ 1 **[構成（Components）]** > **[タップ構成（Tap Configurations）]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[タップ構成の追加（Add Tap Configuration）]** を選択します。

ステップ 3 **[タップ構成の追加（Add Tap Configuration）]** ダイアログ ボックスで、次の詳細を入力します。

表 *26 :* タップ構成を追加

フィールド	説明
Tap Name	タップ構成の名前を入力します。

フィールド	説明
Tap Device	タップ構成が構成されているタップ デバイスを選択します。 **[デバイスの選択]** をクリックし、表示される **[タップ デバイスの選択]** ウィンドウからタップ デバイスを選択します。**[タップ デバイスの追加]** をクリックして、タップ デバイスの追加を選択することもできます。
タップ着信トラフィックのポート	次のオプションから選択してください。ポート-1、ポート-2、両方 いずれかのポートまたは両方のポートからタップ トラフィックを選択できます。
ネットワークポート	**[ポートの選択（Select Port）]** をクリックして、ポート-1 および ポート-2 を選択します。 これらは、実稼働ネットワークからトラフィックを受信するタップ デバイスのポートです。両方のネットワーク ポート間で双方向トラフィックが確立されます。
ミラー ポート	**[ポートの選択（Select Port）]** をクリックして、トラフィックをミラーするポートを選択します。ネットワーク ポート-1 からのトラフィックは、ミラー ポート-1 に送られ、ネットワーク ポート-2 からのトラフィックはミラー ポート-2 に送信されます。 ネットワーク ポートからのトラフィックは、ミラー ポートに送信（ミラーリング）され、次にNDBデバイスに送信されます （注） タップ受信トラフィックに **[両方（Both）]** としてオプションを選択した場合のみ、ポート-1 および ポート-2 の両方が使用可能になります。
NDB Edge ポート-TAP	**[ポートの選択（Select Port）]** をクリックして、NDB デバイスの Edge ポート-TAP ポートを選択します。ミラー ポートからのトラフィックをここで受信しました。 （注） ここで NDB Edgeポート-TAP ポートを選択しない場合は、入力ポートの追加 （34 ページ） の手順を使用してポートを関連付けることができます。

ステップ 4 **[タップ構成の追加（Add Tap Configuration）]** をクリックします。

タップ構成の編集

この手順を使用して、タップ構成のパラメータを編集します。

始める前に

1 つ以上のタップ構成を追加します。

ステップ 1 **[コンポーネント]** > **[タップ構成]** に移動します。

ステップ 2 表示された表で、**タップ名**をクリックします。

新しいペインは右側に表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[タップ構成の編集（Edit Tap Configuration）]** を選択します。

ステップ 4 **[タップ構成の編集]** ダイアログボックスには、タップ構成の現在の情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *27* : タップ構成の編集

フィールド	説明
タップ名	構成名をタップします。
タップ デバイス	タップ構成が作成されたタップ デバイス。
タップ受信トラフィックのためのポート	以前に選択したオプションが表示されます。変更したい場合： これらのオプション（ポート 1、ポート 2、両方）から選択します。 いずれかのポートまたは両方のポートからのトラフィックをタップするように選択できます。
ネットワークポート	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択]** をクリックして、Port-1 と Port-2 を選択します。

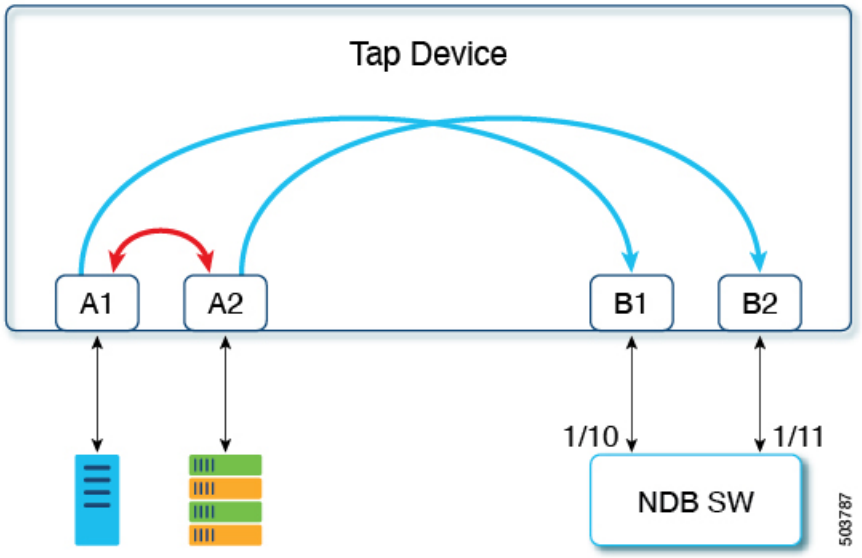
フィールド	説明
ポートのミラー（**Mirror Port(s)**）	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択]** をクリックして、トラフィックをミラーリングするポートを選択します。ネットワーク ポート 1 からのトラフィックはミラー ポート 1 に送信され、ネットワーク ポート 2 からのトラフィックはミラー ポート 2 に送信されます。 （注） ポート 1 とポート 2 の両方を使用できるのは、着信トラフィックをタップするためのオプションを**両方**として選択した場合のみです。
NDB エッジ ポート-タップ	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択]** をクリックして、NDB デバイスのエッジ ポート-TAP ポートを選択します。ミラー ポートからのトラフィックはここで受信されます。 （注） ここで NDB Edge Port-TAP ポートを選択しない場合は、入力ポートの追加 （34 ページ） の手順を使用してポートを関連付けることができます。

ステップ 5 **[タップ構成の編集（Edit Tap Configuration）]** をクリックします。

タップ構成について

タップ デバイスは、1 つ以上の本番スイッチ/ネットワークからのネットワーク トラフィックのコピー（ミラー）を作成します。Cisco Nexus 3550-F L1 シリーズ スイッチをタップ デバイスとして使用することをお勧めします。

以下のトポロジを参照すると、タップ デバイスのポート A1 および A2 は、実稼働スイッチ/ネットワークからトラフィックを受信します。これらはネットワーク ポートと呼ばれます。ネットワーク ポート間で双方向トラフィック フローが確立されます。ネットワーク ポート上のトラフィックは、ミラー ポートと呼ばれるポート B1 および B2 にミラーリングされます。ミラー ポートからのトラフィックは、NDB デバイスのエッジ ポート-TAP ポートに到達します。タップ デバイスのミラー ポートと NDB デバイスのエッジ ポート-TAP ポートは物理的に接続されています。



Cisco Nexus ダッシュボード データ ブローカーで Cisco Nexus 3550-F L1 スイッチをタップ デバイスとして使用する利点

- 使いやすさ。Cisco Nexus ダッシュボード データ ブローカー GUI を使用して、Cisco Nexus 3550-F L1 を設定および管理できます。
- コスト効率。Cisco Nexus 3550-F Fusion は、1 つの 1RU デバイスで 16 個のファイバタップ（48 ポート）を代替できます。

ユーザ定義フィールド

[ユーザー定義フィールド (UDF)] タブには、NDB デバイスの UDF の詳細が表示されます。

UDF を使用すると、オフセット値に基づいてパケットをフィルタリングできます。パケット内のオフセット値は、128 バイト以内で一致できます。

デフォルトでは、Nexus Dashboard Data Broker コントローラは、*udfInnerVlan* および *udfInnerVlanv6* という名前の 2 つの UDF を生成します。これらは、ISL ポートの内部 VLAN を照合するために使用されます。

表 *28 : UDF* サポート マトリックス

UDF EtherType	プラットフォーム
IPv4	Cisco Nexus 9200 および 9300 シリーズのスイッチ
IPv6	Cisco Nexus 93xx EX/FX、95xx EX/FX、92xx シリーズ スイッチ

表 *29 : UDF* の対象地域

プラットフォーム	UDF 適格 TCAM リージョン
Cisco Nexus 9200、9300-EX/9300-FX、および 9500-EX/9500-FX シリーズ スイッチ	ing-ifacl
その他のプラットフォーム	ifacl

次の詳細の表が表示されます。

表 *30 :* ユーザ定義フィールド

列名	説明
UDF	UDF 名。 このフィールドはハイパーリンクです。UDF 名をクリックすると、右側に新しいペインが表示され、UDF の詳細が表示されます。ここから実行できる追加のタスクは次のとおりです。 • ユーザー定義フィールドの編集またはクローン処理 。
タイプ	**IPv4** または **IPv6** を表示します。
キーワード	**Packet-Start** または **Header** を表示します。
In Use	緑色のチェック マークは、UDF が現在使用中であることを示します。
Offset	設定されたオフセット値。
Length	一致したパケットの長さ
Devices	UDF が適用されているデバイスの数。
作成者	UDF を作成したユーザー。
最終修正者	UDF を最後に修正したユーザー。

[ユーザー定義フィールド] タブから、次のアクションを実行できます。

- **UDF の追加** — これを使用して、新しい UDF を追加します。このタスクの詳細については、「ユーザー定義フィールドの追加 」を参照してください。
- **UDF の削除** — 行の先頭にあるチェック ボックスをオンにして、UDF を選択します。**[アクション（Actions）]** < **[UDF の削除（Delete UDF）]** をクリックします。

チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。UDFを選択するように求められます。

（注） UDF 定義の変更には、デバイスのリブートが必要です。

ユーザー定義フィールドの追加

この手順を使用して、ユーザー定義フィールドを追加します。

一部のプロトコルは、一部の NX-OS デバイスではデフォルトでサポートされていません。これらのデバイスでのパケットのフィルタリングをサポートするには、UDF を使用します。

（注） UDF は、最大 2 つのオフセット バイトに一致できます。パケット内の 3 つの連続するバイトをフィルタリングするには、UDF をスタックする必要があります。NDB GUI を使用して、2 つの UDF を順番に作成します。2 番目の UDF は、スタッキング UDF と呼ばれます。

ステップ 1 **[コンポーネント（Components）]** > **[ユーザー定義フィールド（User Defined Field）]** に移動します。

ステップ 2 **[アクション（Actions）]** ドロップダウンリストで、**[UDFの追加（Add UDF）]** を選択します。

ステップ 3 **[UDF の追加（Add UDF）]** ダイアログボックスで、次の詳細を入力します。

表 *31 : UDF* の追加

フィールド	説明
UDF 名	UDF の名前。
タイプ	ドロップダウン リストから選択します。次のオプションがあります。 • IPv4 • IPv6

フィールド	説明
キーワード	ドロップダウン リストから選択します。次のオプションがあります。 • ヘッダー • Packet-Start **ヘッダー** オプションが選択されている場合、内側（内側/外側ヘッダーからのオフセット ベース）および L3/L4（L3/L4 ヘッダーからのオフセット ベース）が有効になります。**Packet-Start** が選択されている場合、オフセットベースはパケットから始まります。
ヘッダー	ドロップダウン リストから選択します。次のオプションがあります。 • 内部 • 外部 このフィールドは、選択したキーワードが**ヘッダー**の場合にのみ有効です。内側または外側のヘッダーからベース オフセット値を選択できるようにします。
レイヤー	ドロップダウン リストから選択します。次のオプションがあります。 • レイヤ 3 • レイヤ 4 このフィールドは、選択したキーワードが**ヘッダー**の場合にのみ有効です。オフセットの開始値がレイヤ 3 またはレイヤ 4 のどちらであるかを指定できます。
オフセット	バイトの**オフセット**値を設定します。範囲は 0 ～ 127 です。 パケットのフィルタ処理は、UDF で設定されたオフセット値に基づいて行われ、パケットは設定されたオフセット値と等しくなります。

フィールド	説明
長さ	一致するパケットの長さ（バイト数）。範囲は 1 ～ 2 です。 オフセット値が 1 に設定されている場合、長さはオフセット値に依存します。その後、設定されたオフセット バイトで始まる 1 バイトが一致します。
デバイス	UDF が作成されているデバイス。 **[デバイスの選択（Select Devices）]** をクリックします。 **[デバイスの選択（Select Devices）]** ウィンドウで、デバイスを選択して、**[デバイスの選択（Select Devices）]** をクリックします。

ステップ 4 **[UDF の追加]** をクリックします。

作成された UDF は、接続のフィルタを作成するときにカスタム フィルタとして使用されます。詳細については、フィルタの追加を参照してください。

（注） UDF のアイコンは、作成直後は黄です。デバイスを再起動すると、UDF が正常にインストールされると、UDF アイコンの色が緑に変わり、そうでない場合は赤に変わります。

ユーザー定義フィールドの編集またはクローン処理

この手順を使用して、ユーザー定義フィールドを編集またはクローン処理します。

UDF の編集は、既存の UDF のパラメータを変更することを意味します。

UDF のクローンを作成することは、既存の UDF と同じパラメーターを使用して新しい UDF が作成されることを意味します。必要に応じて、テストのデフォルト パラメータを変更できます。

始める前に

1 つ以上のユーザー定義フィールドを作成します。

ステップ 1 **[コンポーネント]** > **[ユーザー定義フィールド]**に移動します。

ステップ 2 表示されたテーブルで、**UDF** をクリックします。

新しいペインは右側に表示されます。

ステップ 3 **[アクション]** をクリックし、**[UDF のクローン処理]** または **[UDF の編集]** を選択します。

ステップ 4 **[UDF のクローン処理]** または **[UDF の編集]** ダイアログ ボックスに、現在の UDF 情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *32 : UDF*の編集

フィールド	説明
UDF 名	UDF の名前。 このフィールドは変更できません。
タイプ	UDF の作成中に選択されたタイプ。 このフィールドは変更できません。
キーワード	ドロップダウン リストから選択します。次のオプションがあります。 • ヘッダー • パケット開始
ヘッダー	UDF の作成中に選択されたヘッダー。 このフィールドは変更できません。
レイヤー	UDF の作成中に選択されたレイヤ。 このフィールドは変更できません。
オフセット	バイト **オフセット**値を設定します。範囲は 0 ～ 127 です。 パケットのフィルタリングは、UDF で設定されたオフセット値に基づいて実行され、パケットは設定されたオフセット値から照合されます。
長さ	一致するパケットの長さ (バイト数)。範囲は 1 ～ 2 です。 1 に設定されている場合、長さはオフセット値に依存します。次に、設定されたオフセットバイトで始まる 1 バイトが一致します。

フィールド	説明
デバイス	UDF が現在適用されているデバイス。現在のデバイスから UDF を削除するか、他のデバイスに UDF を適用できます。 **[デバイスの選択（Select Devices）]** をクリックします。 **[デバイスの選択（Select Devices）]** ウィンドウで、デバイスを選択して、**[デバイスの選択（Select Devices）]** をクリックします。 （注） 使用中の UDF をデバイスから削除することはできません。

ステップ 5 **[UDF の編集]** または **[UDF のクローン処理]** をクリックします。

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。