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（Filters）] 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（Filters）]** 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 （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、**[はい（Yes）]** が表示され、それ以外の場合は **[いいえ（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（Protocol）	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（Advanced Filter(s)）]	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（Last Modified By）]	フィルタを最後に変更したユーザー。

[フィルタ（Filters）] 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（Add Filter）]** — 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（Delete Filter）]**：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（Actions）]**>**[フィルタの削除（Delete Filter）]** 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

フィルタを追加するには、この手順に従います。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（Components）] > [フィルタ（Filter）]** 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をフィルタ処理する場合は、このボックスをオンにします。送信元 IP、送信元ポートまたは送信元MACアドレスから接続先IP、接続先ポート、または接続先MACアドレスを取得すること、および接続先IP、接続先ポート、または接続先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ことができます。

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（Ethernet Type）]：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（All Ethernet Types）]
	  • [事前定義されたイーサネット タイプ（Predefined Ethernet Types）]： 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事前定義されたイーサネット タイプがルールに関連付けられていること、さらにほかのパラメータは構成されていないことが必要です。
	  • [イーサネット タイプの入力（Enter Ethernet Type）]：このオプションを選択した場合、イーサネット タイプを 16 進形式で入力します。
	• [VLAN 識別番号（VLAN Identification Number）]：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 優先度（VLAN Priority）]：トラフィックの VLAN 優先度を入力します。VLAN 優先度は、レイヤ 2 トラフィックにのみマッチします。
	• 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 トラフィックにのみマッチします。
	• [接続先 MAC アドレス（Destination MAC Address）]：接続先デバイスの MAC アドレスを入力します。MAC アドレスは、レイヤ2トラフィックにのみマッチします。

フィールド	説明
	• [MPLS ラベル値（MPLS Label Value）]：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。 **[PLS 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 に設定されている場合にのみ表示されます。MPLS ラベル値がマッチします。

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、[レイヤ 2（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[イーサネット タイプ（Ethertype）]** として選択します。	

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（Source IP Address）]： 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。
	  • 標準の IPv4 または IPv6 形式のホスト IP アドレス
	  • IPv4 または IPv6 のアドレス範囲
	  • 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
	  • コンマで区切られた連続していない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 アドレスの範囲を設定する場合、レイヤ4の送信元または接続先ポートの範囲を設定することはできません。
	レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはできません。
	• [接続先 IP アドレス（Destination IP Address）]：レイヤ3トラフィックの接続先IPアドレスを入力します。次のいずれかになります。
	  • 標準の IPv4 または IPv6 形式のホスト IP アドレス
	  • IPv4 または IPv6 のアドレス範囲
	  • 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
	  • コンマで区切られた連続していない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 アドレスの範囲を設定する場合、レイヤ4の送信元または接続先ポートの範囲を設定することはできません。
	レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはできません。

フィールド	説明
	• 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（Protocol Number）**を入力します。 • [高度なフィルタ（Advanced Filter）]：このボタンをクリックすると、高度なフィルタ処理が有効になり、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使用できるようになります。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（Custom Filter）]：このボタンをクリックすると、ユーザー定義フィールド（UDF）を使用したカスタム フィルタ処理が有効になります。**[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 は、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（Value）]：マッチさせる値（0 ～ 65535）を 10 進表記で入力します。たとえば、0x0806 と一致させたい場合は、0x0806 の 10 進表記である 2054 を入力します。 • [マスク（Mask）]：照合の際、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 にデフォルトの UDF を追加（Add Default UDF for inner vlan）]** チェックボックスを選択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（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[Ethertype]** として選択し、[レイヤ 3（Layer 3）] タブで **[TCP]** または **[UDP]** を **[L4 プロトコル（L4 Protocol）]** として選択します。	

フィールド	説明
	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（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 • [送信元ポートを入力（Enter Source Port）]：送信元ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先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。 • [接続先ポート（Destination Port）]：ドロップダウンリストで、接続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 • [接続先ポートを入力（Enter Destination Port）]：接続先ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先ポート番号の範囲を入力できます。 （注） レイヤ 4 接続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

フィールド	説明
	イヤ 3 IP アドレスの範囲を設定できません。
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

この手順に従い、フィルタを編集するか、またはフィルタのクローンを作成します。

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。

フィルタのクローンつまり複製とは、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加えることを意味します。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、いずれかの**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（Actions）]** をクリックし、**[フィルタのクローン（Clone Filter）]** を選択します。

ステップ 4 **[フィルタのクローン（Clone Filter）]** または **[フィルタの編集（Edit Filter）]** 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:* フィルタの編集/クローン（*Edit/Clone Filter*）

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をフィルタ処理する場合は、このボックスをオンにします。送信元 IP、送信元ポートまたは送信元 MAC アドレスから接続先 IP、接続先ポート、または接続先 MAC アドレスを取得すること、および接続先 IP、接続先ポート、または接続先 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ことができます。

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（Ethernet Type）]：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（All Ethernet Types）] • [事前定義されたイーサネット タイプ（Predefined Ethernet Types）]： 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事前定義されたイーサネット タイプがルールに関連付けられていること、さらにほかのパラメータは構成されていないことが必要です。 • [イーサネット タイプの入力（Enter Ethernet Type）]：このオプションを選択した場合、イーサネット タイプを 16 進形式で入力します。 • [VLAN 識別番号（VLAN Identification Number）]：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 優先度（VLAN Priority）]：トラフィックの VLAN 優先度を入力します。 VLAN優先度は、レイヤ2トラフィックにのみマッチします。 • 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 トラフィックにのみマッチします。 • [接続先 MAC アドレス（Destination MAC Address）]：

フィールド	説明
	接続先デバイスの MAC アドレスを入力します。 MAC アドレスは、レイヤ 2 トラフィックにのみマッチします。 • [MPLS ラベル値（MPLS Label Value）]：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。 **[PLS 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 に設定されている場合にのみ表示されます。MPLS ラベル値がマッチします。

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、[レイヤ 2（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[イーサネット タイプ（Ethertype）]** として選択します。	

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（Source IP Address）]： 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。 • 標準の IPv4 または IPv6 形式のホスト IP アドレス • IPv4 または IPv6 のアドレス範囲 • 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 • コンマで区切られた連続していない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 アドレスの範囲を設定する場合、レイヤ4の送信元または宛て先ポートの範囲を設定することはできません。 レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはできません。 • [接続先 IP アドレス（Destination IP Address）]：レイヤ3トラフィックの接続先IPアドレスを入力します。次のいずれかになります。 • 標準の IPv4 または IPv6 形式のホスト IP アドレス • IPv4 または IPv6 のアドレス範囲 • 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 • コンマで区切られた連続していない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 アドレスの範囲を設定する場合、レイヤ4の送信元または接続先ポートの範囲を設定することはできません。 レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはできません。

フィールド	説明
	• [L4プロトコル（L4 Protocol）]：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。 • [高度なフィルタ（Advanced Filter）]：高度なフィルタ処理を有効にする場合には、このボタンをクリックして、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（Custom Filter）]：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（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[Ethertype]** として選択し、[レイヤ 3（Layer 3）] タブで **[TCP]** または **[UDP]** を **[L4 プロトコル（L4 Protocol）]** として選択します。	

フィールド	説明
	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。 • [送信元ポート（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 • [送信元ポートを入力（Enter Source Port）]：送信元ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先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。 • [接続先ポート（Destination Port）]：ドロップダウンリストで、接続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 • [接続先ポートを入力（Enter Destination Port）]：接続先ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先ポート番号の範囲を入力できます。 （注） レイヤ 4 接続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

フィールド	説明
	イヤ 3 IP アドレスの範囲を設定できません。
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
IPv4 と UDP	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
IPv6 と UDP	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 デバイスの場合、NX-OS バージョン 7.0(3)I6(1) 以降では、TTL 値を最大 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した。

高度なフィルタリングの使用に関する制限

高度なフィルタの構成中、次のことはできません。

- DSCP と優先順位を一緒に設定すること。
- フラグメントと ACK または SYN または FIN または PSH または RST を一緒に構成すること。
- 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すること。
- IPv4 と TCP の組み合わせで優先順位と HTTP メソッドを構成すること。

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**の名前をクリックして、デバイスのグローバル構成の詳細を取得できます。
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（Non-symmetric）
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（MPLS Filter）]	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（Global Configuration）]** タブから実行できます。

- **[グローバル構成の編集（Edit Global Configuration）]**：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 （24 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

この手順に従って、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は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。

デバイスの作成時には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（Components）]** > **[グローバル構成（Global Configuration）]** 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（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（General）]	
[デバイス（Device）]	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（Load Balancing Type Configuration）]	ドロップダウン リストから **[対称（Symmetric）]** または **[非対称（Non-symmetric）]** 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（Hashing Configuration）]	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（Hashing Type）]	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 Configuration）]	
[MPLS ストリップ タイプの設定（MPLS Strip Type Configuration ）]	グレーのボタンをクリックして、MPLS ストリップ タイプの設定を有効にします。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 パケットで、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（Label Age）]	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 シリーズの 93128TX、3172、3164、3232、3132C-Z スイッチです。

フィールド	説明
[MPLS フィルタ構成を有効にする（Enable MPLS Filter Configuration）]	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 設定（sFlow Configuration）]	
[sFlow の有効化（Enable sFlow）]	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 （34 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（Agent IP Address）]**：エージェントの IP アドレスを入力します。 • **[VRF の選択（Select VRF）]** — 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（Collector IP Address）]**：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（Collector UDP Port）]**：sFlow コレクタの UDP ポートを入力します。 • **[カウンタ ポーリング間隔（Counter Poll Interval）]**：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（Max Datagram Size）]**：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（Max Sampled Size）]**：最大サンプル サイズを入力します。 • **[サンプリング レート（Sampling Rate）]**：データ サンプリング レートを入力します。 • **[データ ソース（Data Sources）]**：**[ポートの選択（Select Ports）]** 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（Add）]** 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 構成（PTP Configuration）]	

フィールド	説明
[PTP の有効化（Enable PTP）]	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、入力ポートと監視ツールのタイムスタンプで使用されます。 PTP の詳細については、高精度時間プロトコル （32 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（Source IP Address）]**：PTP アップデートを受信するための送信元 IP アドレスを入力します。 • **[ポート（Ports）]**：**[ポートの選択（Select Ports）]** をクリックし、チェックボックスをオンにして、PTP 送信元 IP を接続するために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（Jumbo MTU Configuration）]	
[MTU 値（MTU Value）]	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の 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（Reset to Default）]** をクリックすると、MTU 値はデフォルト値の 1500 に設定されます。 （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（NetFlow Configuration）]	

フィールド	説明
[Netflow の有効化（Enable NetFlow）]	灰色のボタンをクリックして、NetFlow 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 （33 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） 完了してください。 • NetFlow のレコードの追加 （28 ページ） • NetFlow のエクスポータの追加 （30 ページ） • NetFlow のモニターの追加 （31 ページ） NetFlow 設定を完了するには、NetFlow モニターを入力ポートに関連付けます。入力ポートの追加 （36 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（Edit Global Configuration）]** 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（Components）]** > **[グローバル構成（Global Configuration）]** 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（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 **Netflow を有効化**します。

ステップ 5 **[レコードの追加（Add Record）]** 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。 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（Layer 2）**および**レイヤ 3/4（Layer 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 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

この手順に従って、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（Components）]** > **[グローバル構成（Global Configuration）]** 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（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 **NetFlow を有効化**します。

ステップ 5 **[エクスポータを追加（Add Exporter）]** 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。
説明	エクスポータの説明。
宛先（**Destination**）	エクスポート先の 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接続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 のエクスポート 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（Option Exporter）]	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（Add Exporter）]** をクリックします。

NetFlow のモニターの追加

この手順に従って、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
- エクスポータの追加

ステップ 1 **[コンポーネント（Components）]** > **[グローバル構成（Global Configuration）]** 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（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 **NetFlow を有効化**します。

ステップ 5 **[モニターの追加（Add Monitor）]** 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（Select Record）]** をクリックします。**[レコードの選択（Select Record）]** 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（Exporter）]	**[エクスポータの選択（Select Exporter）]** をクリックします。**[エクスポータの選択（Select Exporter）]** 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（Precision Time Protocol）デバイスには、通常のクロック、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 を設定すると、デフォルトの PTP 設定が、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 （24 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 （24 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 （24 ページ） を参照してください。

入力ポート

[入力ポート（Input Ports）] 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** コマンドを構成してください。

次の詳細を示す表が表示されます。

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（Port）]	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（Port）]**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のアクションは次のとおりです。 • *[入力ポートの編集（Editing an Input Port）]* • 構成の削除：デバイスの入力ポートとしてのポートは削除されます。

列名	説明
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。
設定	入力ポートの構成情報（入力ポートの追加（36ページ） で設定されたパラメータに基づく）。
タイプ（**Type**）	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 エッジ：SPAN • パケットの切り捨て
[スパン接続先/タップ名（Span Destination/Tap Name）]	入力ポートに接続されているスパン先の詳細。 • ポートが実稼働スイッチに接続されている場合、*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 については、DN 値がポッドとパスの詳細とともに表示されます。DNAC については、「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（Input Ports）] 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（Add Input Port）]**：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 （36 ページ） を参照してください。
- **[入力ポートの削除（Delete Input Port）]**：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求められます。

入力ポートの追加

入力ポートを作成するには、この手順に従います。

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（Grobal Configuration）]** 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（以下のリスト）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 フィルタリング
- Jumbo MTU

ステップ 1 **[コンポーネント（Components）]** > **[入力ポート構成（Input port Configuration）]** 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（Add Input Port）]** 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（*Add Input Port*）

フィールド	説明
[全般（General）]	
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、次の手順に従います。 **[デバイスの選択（Select Device）]** をクリックします。**[デバイスの選択（Select Device）]** 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。

フィールド	説明
[ポート（Port(s)）]	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（Select Port）]** をクリックします。**[ポートの選択（Select Port）]** 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。
[ポート タイプ（Port Type）]	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。 • **[エッジ ポート - SPAN（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。 • **[エッジ ポート - TAP（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。 • **[リモート ソース エッジ ポート - SPAN（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（Block-Tx）]	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。

フィールド	説明
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 スイッチについては、ユーザーは ICMP トラフィックを拒否またはブロックする場合、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。
[タイムスタンプ タギングの有効化（Enable Timestamp Tagging）]	チェックボックスをオンにして、タイムスタンプ タグ付け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 タギング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ギングされません。 （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（Enable MPLS Filtering）]	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（Apply Jumbo MTU）]	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。

フィールド	説明
[Netflow モニター（Netflow Monitor）]	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（Port Type）]**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、入力ポートの送信元（SPANの接続先）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 • 実稼働スイッチ 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（Select Controller）]** をクリックします。**[ACI]** または **[DNAC]** を選択します。
[接続先デバイス タイプ（Destination Device Type）]：**[コントローラ（Controller）] > [ACI]** のフィールド （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（Span Destination Name）]	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。
[接続先デバイス タイプ（Destination Device Type）]：**[コントローラ（Controller）] > [DNAC]** のフィールド	
[スパン先名（Span Destination Name）]	スパン先の名前を入力します。

フィールド	説明
[SPAN 接続先ポート（Span Destination Port）]	**[SPAN 接続先ポート（Span Destination Port）]** をクリックし、Catalyst スイッチとポートを選択します。
[接続先デバイス タイプ]：**[実稼働スイッチ]** のフィールド （注） SPAN 接続先を構成する前に、Nexus または Catalyst デバイスを追加する必要があります。	
[SPAN 先デバイス（Span Destination Device）]	**[デバイスの選択（Select Device）]** をクリックし、デバイスを選択します。
[SPAN 先ポート（Span Destination Port）]	**[ポートの選択（Select Port）]** をクリックして、ポートを選択します。

b) （**[ポート タイプ（Port Type）]** — 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（Tap Configuration Name）]	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（Tap Configuration Type）]	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（Tap Configuration Name）]** の詳細に基づいています。タップ構成の追加 （63 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（Port Type）]**：リモート ソース エッジ-SPAN の場合のみ）次の詳細を入力します。

（注） リモート送信元からのトラフィックを受信するために、最大 4 つのリモート送信元エッジ -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（Remote Input Termination Session）]	
[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 インターフェイスを使用（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使用します。

フィールド	説明
ループバック（Loopback）	**[ループバックの選択（Select Loopback）]** 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（Add Loopback）]** 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接続先ポートに到達します。最初のリモート送信元エッジ スパン入力ポートをループバックで作成した場合、次のリモート送信元エッジ-SPANポートも同じループバック インターフェイスで構成する必要があります。最初のリモート送信元エッジ スパン入力ポートをループバックなしで作成した場合、次のリモート送信元エッジ SPAN ポートもループバック インターフェイスなしで構成する必要があります。
[セッション接続先（Session Destination）]	**[接続先ポートの選択（Select Destination Port）]** をクリックして、接続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（Remote Input Session）]	
[リモート入力ポート（Remote Input Port）]	**[リモート入力ポート（Remote Input Port）]** 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） リモート送信元エッジ-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構成している場合、リモート入力ポートは、リモート送信元エッジ-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、最初のリモート送信元エッジ-SPAN ポートを構成する場合だけです。次の 3 つのポートを構成する際には、同じIPアドレスがリモート送信元エッジ-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。

フィールド	説明
[接続先デバイスのタイプ（Destination Device Type）]	ドロップダウン リストから [デバイス タイプ（Device Type）] を選択します。 リモート送信元エッジ-SPAN ポートの場合、サポートされる接続先タイプは ACI です。
[スパン先 ACI ファブリック（Span Destination ACI Fabric）]	[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（Application Profile）]	**[アプリケーション プロファイルの選択（Select Application Profile ）]** 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、送信元パケットの IP サブネットのベース IP アドレスです。
[接続先 IP アドレス（Destination IP Address）]	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（Remote Input Port）]** 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、これは接続先ポート（リモート入力ポート）であるため、接続先 IP と呼ばれます。
[フロー ID（ Flow 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 ポートに前に指定した 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（Add Input Port）]** 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（Input Ports）]** > **[アクション（Actions）]** > **[入力ポートの追加（And Input Ports）]** 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。
IP アドレス（IP Address）	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。

次の詳細を示す表が表示されます。

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：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：リンクが起動して動作していることを示します。 • 赤：リンクがダウンしていることを示します。 • 黄：リンクが管理上ダウンしていることを示します。
[モニタリング ツール（Monitoring Tool）]	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**の名前をクリックします。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 （50 ページ）
ポート	モニタリングツールのポート（デバイスに接続）。 ポートの詳細を表示するには、**[ポート（Port）]** の名前をクリックします。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 （50 ページ）

列名	説明
[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（Local Monitoring Tool）]：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（Remote Monitoring Tool）]：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（Packet Truncation）]	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（Yes）]** と表示されます。
作成者	モニタリング ツールを作成したユーザー。
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（Monitoring Tools）] 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（Add Monitoring Tool）]**：これを使用して、新しい監視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 ツールの追加を参照してください。
- **[モニタリング ツールの削除（Delete Monitoring Tool(s)）]**：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求められます。

（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。
- モニタリング 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アップ状態（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 ステータスをアップに変更するには、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（General）]	
モニタリング ツール名	モニタリングツール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（Select Port）]** 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（Port Description）]	ポートの説明を入力します。
[ローカル監視ツール（Local Monitor Tool）]	ラジオ ボタンを選択して、ローカル モニター 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）。 • [受信のブロック（Block Rx）] • [ICMPv6 ネイバー勧誘をブロック（Block ICMPv6 Neighbour Solicitation）] • [タイムスタンプ タギングの有効化（Enable Timestamp Tagging）] • 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（Enable Timestamp Strip）] • [ジャンボ MTU を適用（Apply Jumbo MTU）]

フィールド	説明
[受信のブロック（Block Rx）]	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と、このオプションをオフにできます。 （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（Block ICMPv6 Neighbour Solicitation）]	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）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。 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（Enable Timestamp Tagging）]	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。モニタリング ツール ポートのすべての発信パケットにタイムスタンプ タグが付加されます。 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のタグ付け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、つまり Edge-SPAN/Edge-TAP とモニタリング ツールのいずれかの側で構成されていない場合、パケットのタイムスタンプによるタグ付けは行われません。

フィールド	説明
[パケットの切り捨て（Packet Truncation）]	チェックボックスをオンにしてパケットの切り捨てを有効にし、MTU サイズを入力します。 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、モニタリング ツールに到達します。 パケット切り捨てポートを設定するには、**[パケット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 （53 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（Enable Timestamp Strip）]	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。これにより、送信元のパケットからタイムスタンプ タグが削除されます。
[ジャンボ MTU を適用（Apply Jumbo MTU）]	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 は、デバイスにより大きなパケット サイズを設定します。**[ジャンボMTU（Jumbo MTU）]** を **[グローバル構成（Global Configuration）]** で有効にして、デバイスのポートにジャンボ MTU のサイズを適用します。
[リモート モニタリング ツール（Remote Monitoring Tool）]	ラジオ ボタンを選択して、リモート モニター デバイスを選択します。このオプションを選択すると、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。 リモート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）。 • 受信のブロック • 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。

フィールド	説明
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 スイッチのカプセル化リモート スイッチ ポート アナライザ（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（Add Monitoring）]** 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**の名前をクリックします。

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（Edit Monitoring Tool）]** 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（General）]	
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（Port Description）]	ポートの説明を入力します。

フィールド	説明
[ローカル監視ツール（Local Monitor Tool）]	ラジオ ボタンを選択して、ローカル モニター 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）。 • [受信のブロック（Block Rx）] • [ICMPv6 ネイバー勧誘をブロック（Block ICMPv6 Neighbour Solicitation）] • [タイムスタンプ タギングの有効化（Enable Timestamp Tagging）] • 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（Enable Timestamp Strip）] • [ジャンボ MTU を適用（Apply Jumbo MTU）]
[受信のブロック（Block Rx）]	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と、このオプションをオフにできます。 （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（Block ICMPv6 Neighbour Solicitation）]	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）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。 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（Enable Timestamp Tagging）]	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。モニタリング ツール ポートのすべての発信パケットにタイムスタンプ タグが付加されます。 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のタグ付け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、つまり Edge-SPAN/Edge-TAP とモニタリング ツールのいずれかの側で構成されていない場合、パケットのタイムスタンプによるタグ付けは行われません。
[パケットの切り捨て（Packet Truncation）]	チェックボックスをオンにしてパケットの切り捨てを有効にし、MTU サイズを入力します。モニタリング 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（Select Packet Truncation Port）]** は無効になります。
[タイムスタンプ ストリップの有効化（Enable Timestamp Strip）]	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。これにより、送信元のパケットからタイムスタンプ タグが削除されます。
[ジャンボ MTU を適用（Apply Jumbo MTU）]	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 は、デバイスにより大きなパケット サイズを設定します。**[ジャンボ MTU（Jumbo MTU）]** を **[グローバル構成（Global Configuration）]** で有効にして、デバイスのポートにジャンボ MTU のサイズを適用します。
[リモート モニタリング ツール（Remote Monitoring Tool）]	ラジオ ボタンを選択して、リモート モニター デバイスを選択します。このオプションを選択すると、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。 リモート 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）。 • 受信のブロック • インターフェイスIP • 宛先 IP • ERSPAN ID

フィールド	説明
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 スイッチのカプセル化リモート スイッチ ポート アナライザ（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 （34 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。パケットの切り捨てが必要になるのは、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（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 デバイスとポートを選択し、**[パケット切り捨て（Packet Truncation）]** 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（Select Packet Truncation Port）]** 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（Select Packet Truncation Port）]** ウィンドウで、**[パケット切り捨てポートの追加（Add Packet Truncation Port）]** 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（***Add Packet Truncation***）*]*

フィールド	説明
[全般（General）]	
Device	デバイス名が表示されます。
[ポート（Port）]	**[ポートの選択（Select Port）]** をクリックします。**[ポートの選択（Select Port）]** 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（Port Type）]	デフォルトでは、パケット切り捨て（Packet Truncation）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（Drop ICMPv6 Neighbour Solicitation）]	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（Input Port Group）]** : デバイスの（または複数デバイスの）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（Monitoring Tool Group）]** : デバイスの（または複数デバイスの）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、モニタリング ツール グループを参照してください。

入力ポート グループ

デバイス（または複数の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。グループ化することで、接続の作成中、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同時に選択できます。

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（Input Port Group Name）]	入力ポートのグループ名。 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（Input Port Group Name）]** 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。
[関連する接続（Associated Connections）]	グループに関連付けられた接続。
[メンバー（Member(s)）]	グループのメンバー入力ポートの数。
[作成者（Created By）]	グループを作成したユーザー。
[最終修正者（Last Modified By）]	グループを最後に変更したユーザー。

[入力ポート グループ（Input Port Group）] 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（Add Input Port Group）]**：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（Delete Input Port Group(s)）]**：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（Actions）]** > **[入力ポート グループの削除（Delete Input Port Group）]** 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（Add Input Port Group）]** 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（***Add Input Port Group***）*]*

フィールド	説明
[全般（General）]	
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（**Select Node**）	*[*すべてのノード（*All Nodes*）*]* 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（Choose Port(s)）]	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（Add All）]** 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（Selected Port(s)）]	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（Remove All）]** 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

この手順に従って、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。

新しいペインが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（General）]	
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（Choose Port(s)）]	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（Add All）]** 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（Selected Port(s)）]	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（Remove All）]** 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 5 **[入力ポート グループの編集（Edit Input Port Group）]** をクリックします。

モニタリング ツール グループ

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 :* モニタリング ツール グループ

列名	説明
[モニタリング ツール グループ名（Monitoring Tool Group Name）]	モニタリング ツール グループの名前。 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 グループ**の名前をクリックします。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（Associated Connections）]	モニタリング ツール グループを利用する接続。
[メンバー（Member(s)）]	グループのメンバーモニタリング ツール ポートの数。
[作成者（Created By）]	グループを作成したユーザー。
[最終修正者（Last Modified By）]	グループを最後に変更したユーザ。

[モニタリング ツール グループ（Monitoring Tool Group）] 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（Delete Monitoring Tool Group(s)）]**：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（Action）]** > **[モニタリング ツール グループの削除（Delete Monitoring Tool Group(s)）]** 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

この手順に従って、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（General）]	
グループ名	モニタリング ツール 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（Select Node）	*[*すべてのノード（*All Nodes*）*]* 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（Choose Port(s)）]	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（Add All）]** 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（Selected Port(s)）]	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（Remove All）]** 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（Add Monitoring Tool Group）]** 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**の名前をクリックします。

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（Actions）]** をクリックし、**[モニタリング ツール グループの編集（Edit Monitoring Tool Group）]** 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（Edit Monitoring Tool Group）]** 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（*Edit Monitoring Tool Group*）*]*

フィールド	説明
[全般（General）]	
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（Choose Port(s)）]	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（Add All）]** 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（Selected Port(s)）]	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（Remove All）]** 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 5 **[モニタリング ツール グループの編集（Edit Monitoring Tool Group）]** をクリックします。

スパン接続先

[スパン接続先（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。スパン接続先は、入力ポートのトラフィック ソース（ACI または NX-OS デバイスから）です。L2 スパン接続先（ローカル）はエッジ スパン ポートに作成され、L3 スパン接続先（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 : [*スパン接続先（***Span Destination***）*]*

列名	説明
名前	スパン接続先ポートの名前。
接続先（**Destinations**）	スパン接続先が 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（**Input Port**）**]**	スパン接続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 SPAN ポート • リモート送信元のエッジ-SPAN ポート
[スパン デバイス（**Span Device**）**]**	スパン デバイス（トラフィック送信元）。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	スパン接続先を作成したユーザー。
[最終更新者（**Last Modified By**）**]**	スパン接続先を最後に変更したユーザー。

[スパン接続先（**Span Destinations**）**]** タブから、次のアクションを実行できます。

- **[**スパン接続先の削除（**Delete Span Destinations**）**]**：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（**Actions**）**]** > **[**スパン接続先の削除（**Delete Span Destinations**）**]** をクリックします。選択したスパン接続先が削除されます。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。スパン接続先を選択するよう求められます。

（注） スパン接続先の追加については、入力ポートの追加（36ページ）の手順を参照してください。スパン接続先（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接続先を追加できます。

APIC SPAN接続先の場合、入力ポートをエッジ-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SPAN接続先として設定できます。NX-OS（実稼働スイッチ）のSPAN接続先で、入力ポートをエッジ-SPANポートとして設定し、ポートをNX-OSデバイスに接続した場合、NX-OSデバイスのノードとポートを選択し、ポートをSPAN接続先として設定します。

タップ構成

[タップ構成（Tap Configurations）] タブには、Nexus Dashboard Data Broker コントローラ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。

表には次の詳細が表示されます。

表 *25 : [タップ構成（Tap Configurations）]*

列名	説明
[タップ名（Tap Name）]	タップ構成名です。 タップ名をクリックすると、新しいペインが右側に表示されます。次の追加の手順を実行できます。 • タップ構成の編集 （65 ページ）
Device	タップ構成が作成されたタップ 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]	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-1 ミラー（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 エッジ Port-TAP に転送するタップ デバイスのポート。
[Port-2 ミラー（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 エッジ Port-TAP に転送するタップ デバイスのポート。
[Port-1 エッジ Port-TAP（Port-1 Edge Port-TAP）]	タップ デバイスの **Port-1 ミラー** 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 エッジ Port-TAP（Port-2 Edge Port-TAP）]	タップデバイスの **Port-2 ミラー** 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（Tap Configurations）] 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（Add Tap Configuration）]**：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 （63 ページ）を参照してください。
- **[タップ構成の編集（Edit Tap Configuration）]**：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 （65 ページ）を参照してください。
- **[タップ構成の削除（Delete Tap Configuration）]**—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（Actions）]** > **[タップ構成の削除（Delete Tap Configuration）]** をクリックします。
- **[タップ構成の同期（Sync Tap Configuration）]**：タップ デバイスのタップ構成を Nexus Dashboard Data Broker コントローラのタップ構成と同期します。

タップ構成の追加

この手順に従って、タップ構成を追加します。

始める前に

1 台以上のタップ 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 : [タップ構成の追加（Add Tap Configuration）]

フィールド	説明
[タップ名（Tap Name）]	タップ構成の名前を入力します。

フィールド	説明
[タップ デバイス（Tap Device）]	タップ構成を構成中のタップ デバイスを選択します。 **[デバイスの選択（Select Device）]** をクリックし、表示される **[タップ デバイスの選択（Select Tap Device）]** 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（Add Tap Device）]** 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（ Port(s) to Tap Incoming Traffic）]	[ポート-1（Port-1）]、[ポート-2（Port-2）]、[両方（Both）] のオプションから選択します。 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	**[ポートの選択（Select Port）]** をクリックして、[ポート-1（Port-1）] および [ポート-2（Port-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（Mirror Port(s)）]	**[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。 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） 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際のオプションとして **[両方（Both）]** を選択した場合のみです。
[NDB エッジ ポート-TAP（NDB Edge Port-TAP）]	**[ポートの選択（Select Port）]** 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 エッジ ポート-TAP ポートを選択しない場合は、入力ポートの追加 （36 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（Edit Tap Configuration）]** 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（Edit Tap Configuration）]*

フィールド	説明
[タップ名（Tap Name）]	タップ構成名です。
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： [ポート-1（Port-1）]、[ポート-2（Port-2）]、[両方（Both）] のオプションから選択します。 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。

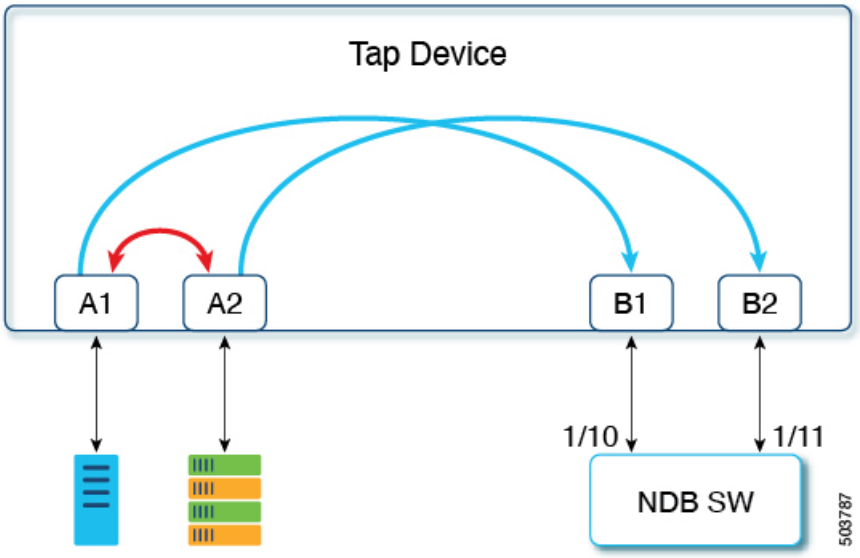
フィールド	説明
ポートのミラー（Mirror Port(s)）	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択（Select Port）]** をクリックして、トラフィックをミラーリングするポートを選択します。ネットワーク ポート 1 からのトラフィックはミラー ポート 1 に送信され、ネットワーク ポート 2 からのトラフィックはミラー ポート 2 に送信されます。 （注） ポート 1 とポート 2 の両方を使用できるのは、着信トラフィックをタップする際のオプションとして **[両方（Both）]** を選択した場合のみです。
[NDB エッジ ポート-TAP（NDB Edge Port-TAP）]	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（Select Port）]** 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 エッジ ポート-TAP ポートを選択しない場合は、入力ポートの追加 （36 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。

以下の参照用トポロジでは、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 Dashboard Data Broker 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 3550-F L1 は、Cisco Nexus Dashboard Data Broker GUI を使用して設定し、管理できます。
- コスト効率。Cisco Nexus 3550-F Fusion L1 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 バイト以内で照合できます。

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 [英語]
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* の対象リージョン

プラットフォーム [英語]	UDF の適格 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

次のような詳細を記した表が表示されます。

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 の名前をクリックすると、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（**Type**）	**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。
[使用中（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。
[オフセット（Offset）]	設定されたオフセット値。
長さ（**Length**）	一致したパケットの長さ（バイト数）。
[デバイス（Devices）]	UDF が適用されているデバイスの数。
[作成者（Created By）]	UDF を作成したユーザ。
[最終更新者（Last Modified By）]	UDF を最後に変更したユーザ。

[ユーザ定義フィールド（User Defined Field）] タブから、次のアクションを実行できます。

- **UDF の追加（Add UDF）** ：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（Delete UDF(s)）]** : 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、デバイスの再起動が必要です。

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 バイトにマッチできます。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 Name）]	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（Keyword）]	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（Header）]**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（Header）]**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（Offset）]	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行われます。パケットは設定されたオフセット値から照合されます。

フィールド	説明
[長さ（Length）]	照合を行うパケットの長さ（バイト数）。範囲は 1 ～ 2 です。 位置はオフセット値に依存します。1 に設定されている場合、設定されたオフセット バイトの後の 1 バイトの照合を行います。
[デバイス（Devices）]	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（Add UDF）]** 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、作成直後は黄色です。デバイスを再起動したとき、UDF が正常にインストールされた場合には UDF アイコンの色は緑色に変わり、そうでない場合は赤色に変わります。

ユーザー定義フィールドの編集またはクローン処理

この手順に従って、ユーザー定義フィールドを編集またはクローンします。

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と、既存の UDF と同じパラメーターを使用する新しい UDF が作成されます。必要に応じて、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（Components）]** > **[ユーザー定義フィールド（User Definition Fields）]**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（Actions）]** をクリックし、**[UDF のクローン処理（Clone UDF）]** または **[UDF の編集（Edit UDF）]** を選択します。

ステップ 4 **[UDF のクローン処理（Clone UDF）]** または **[UDF の編集（Edit UDF）]** 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 Name）]	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（Keyword）]	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（Layer）]	UDF の作成中に選択されたレイヤー。 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行われます。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	照合を行うパケットの長さ（バイト数）。範囲は 1 ～ 2 です。 位置はオフセット値に依存します。1 に設定されている場合、設定されたオフセットバイトの後の 1 バイトの照合を行います。

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 を削除すること、または他のデバイスに UDF を適用することができます。 **[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（Edit UDF）]** または **[UDF のクローン処理（Clone UDF）]** 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。