CHAPTER 3

# トラフィック可視化のための NetFlow の設定

この章の内容は、次のとおりです。



NetFlow レコードは、ネットワーク トラフィックの集計ビューを示します。NetFlow データ ソースは、ブランチ ルータまたはスイッチでイネーブル化されると、Cisco NAM VSB で使用可能になります。NetFlow は、アプリケーション、ホスト、およびカンバセーションの統計情報を提供します。一部の特定のインターフェイスに対しては、カスタム データ ソースを設定できます。NetFlow を使用して、ブランチで使用されているデータセンターでホストされるビジネス クリティカルなアプリケーションを特定できます。

## NAM VSB での NetFlow データ ソースの設定

データ ソース エントリは、外部デバイスからの NetFlow レコードを受け入れるために NAM に存在する必要があります。データ ソース エントリは NAM Web GUI または CLI を使用して手動で作成されることがあります。手動でデータ ソースを作成する場合は、そのデータ ソースに任意の名前を指定できます。

便宜上、NetFlow データ ソースの手動作成は必須ではありません。**自動作成**機能がデフォルトでイネーブルになっています。自動作成機能によって、最初のパケット受信時に NAM に NDE のトラフィックを送信する各デバイスに対して新しいデータ ソースが自動的に作成されます。

自動作成された NetFlow データ ソースには、「NDE-<IP Address>-ID-<Integer>」の形式で名前が割り当てられます。<IP Address> はエクスポートしているデバイスの IP アドレス、<Integer> はデバイスによってパケットに追加されるエンジン ID（NetFlow Data Export 規格の一部）です。たとえば、[Engine ID] フィールドが 12 に設定されている NDE パケットを送信しているデバイス 192.168.0.1 の場合は、「NDE-192.168.0.1-ID-12」になります。これらの自動作成されたデータ ソースは編集したり、必要に応じて名前を変更できます。必要に応じて、後述のように、デバイスの SNMP クレデンシャルを指定することもできます。

### NetFlow データ ソースの自動作成の設定

外部デバイスから NDE パケットを受信したときに、データ ソースを自動的に作成するように NAM を設定するには、次の手順を実行します。ただし、自動作成機能はデフォルトでオンになっているため、通常はこれらの手順を実行する必要はありません。

### Web GUI による NetFlow データ ソースの自動作成のイネーブル化

**ステップ 1**　[Setup] > [Traffic] > [NAM Data Sources] を選択します。

**ステップ 2**　ウィンドウの左下にある [Auto Create] ボタンをクリックします。

**ステップ 3**　NDE データ ソースの自動作成のオン/オフを切り替えるには、[NetFlow] チェックボックスをオンにします。

**ステップ 4**　[Submit] ボタンをクリックします。

### CLI による NetFlow データ ソースの自動作成のイネーブル化

自動作成機能の設定は、NAM CLI でも行うことができます。ただし、自動作成機能はデフォルトでオンになっているため、ほとんどの場合、これらの手順を実行する必要はありません。

外部デバイスから NDE パケットを受信したときに、データ ソースを自動的に作成するように NAM を設定するには、次の手順を実行します。

次のように、「autocreate-data-source」コマンドを使用します。

```
root@172-20-104-107.cisco.com# autocreate-data-source netflow
NDE data source autocreate successfully ENABLED
```

NAM により、NetFlow パケットを送信してくる各デバイスの NetFlow データ ソースが自動的に作成されます。データ ソースには、NAM に送信される NDE パケットにデバイスによって追加された特定のエンジン ID が設定されます。同じデバイスから異なるエンジン ID 値の NDE パケットが NAM に送信された場合、そのデバイスから送信された一意の各エンジン ID に対して別々のデータ ソースが作成されます。

### CLI による NetFlow データ ソースの自動作成のディセーブル化

NetFlow データ ソースの自動作成をディセーブルにするには、次のように「no autocreate-data-source」コマンドを使用します。

```
root@172-20-104-107.cisco.com# no autocreate-data-source netflow
NDE data source autocreate successfully DISABLED
root@172-20-104-107.cisco.com#
```

### Web GUI による NetFlow データ ソースの作成

たとえば、自動作成機能がオフになっている場合に、GUI を使用して NAM の NetFlow データ ソースを手動で設定するには、次の手順を実行します。

**ステップ 1**　[Setup] > [Traffic] > [NAM Data Sources] を選択します。

**ステップ 2**　ウィンドウ下部にある [Create] ボタンをクリックします。

**ステップ 3**　[Type] ドロップダウン リストから、[NETFLOW] を選択します。

**ステップ 4**　NAM に NDE をエクスポートするデバイスの IP アドレスを入力します（必須）。

**ステップ 5**　データ ソースに名前を付けます。この名前は、[Data Source] ドロップダウン リストがある任意の場所に表示されます。

**ステップ 6**　（任意）モニタするデバイスのエンジン ID の個別の値がわかっている場合は、[Engine] チェックボックスをオンにして、エンジン ID の値を入力します。[Engine] チェックボックスがオフの場合、デバイスによってエクスポートされるすべての NDE レコードは、NDE パケットに追加されたエンジン ID に関係なく、同じデータ ソースにグループ化されます（ほとんどの場合 [Engine] チェックボックスはオフのままにでき、エンジン ID 値を気にする必要はありません）。

一部のデバイスには、個別に NDE レコードをエクスポートする複数のエンジンがあります。たとえば、シスコの一部のルータでは、NDE レコードを、スーパーバイザ モジュール、および個々のラインカードによってエクスポートできます。エクスポートされるパケットの送信元 IP アドレスは同じ場合がありますが、スーパーバイザからエクスポートしたエンジン ID は、ラインカードからエクスポートされたエンジン ID とは異なる値になります。データ ソースにエンジンを 1 つだけ含める場合は、[Engine] チェックボックスをオンにして、そのエンジン ID の値を入力する必要があります。

**ステップ 7**　（任意）SNMP v1/v2c RW コミュニティ ストリング：SNMP v1 または v2c を使用してデバイスと通信する場合は、NAM に NetFlow パケットをエクスポートするデバイスに設定されているコミュニティ ストリングを入力します。

**ステップ 8**　（任意）「SNMP v3 のイネーブル化」：SNMP v3 を使用してデバイスと通信する場合は、v3 固有のダイアログ内のフィールドに入力します。

**ステップ 9**　（任意）必要に応じて、デバイスの SNMP クレデンシャルを入力します。有効な SNMP クレデンシャルを指定すると、NAM が読み取り可能なテキスト ストリングをデバイスからアップロードできるようになり、そのデバイスのインターフェイスを単に番号としてではなく、説明的なテキストで表示できるようになります。SNMPv2c または SNMPv3 のクレデンシャルを指定できます。表 3-1 を参照してください。

**表 3-1　SNMP クレデンシャル**

| フィールド | 説明 |
|---|---|
| Mode: No Auth, No Priv | SNMP が、認証もプライバシーもないモードで使用されます。 |
| Mode: Auth, No Priv | SNMP が、認証はあるがプライバシーのないモードで使用されます。 |
| Mode: Auth and Priv | SNMP が、認証とプライバシーの両方があるモードで使用されます。 |
| User Name | デバイスに設定されたユーザ名と一致するユーザ名を入力します。 |
| Auth Password | デバイスに設定されているユーザ名に関連付けられた認証パスワードを入力します。パスワードを確認します。 |
| Auth Algorithm | デバイスに設定されている認証規格を選択します（MD5 または SHA-1）。 |
| Privacy Password | デバイスに設定されているプライバシー パスワードを入力します。パスワードを確認します。 |
| Privacy Algorithm | デバイスに設定されているプライバシー アルゴリズムを入力します（AES または DES）。 |

**ステップ 10**　[Submit] ボタンをクリックします。

### Web GUI による NetFlow データ ソースの削除

既存の NetFlow データ ソースを削除するには、次の手順を実行します。自動作成機能がオンになっていて、デバイスが NDE パケットを NAM に送信し続ける場合、次の NDE パケットが到着すると、すぐにデータ ソースが自動的に再作成されます。したがって、既存の NetFlow データ ソースを削除する場合、通常は、前述したように、まず NetFlow 自動作成機能をオフにすることを推奨します。

**ステップ 1**　[Setup] > [Traffic] > [NAM Data Sources] を選択します。

**ステップ 2**　削除するデータ ソースを選択します。

**ステップ 3**　ウィンドウ下部にある [Delete] ボタンをクリックします。

### CLI による NetFlow データ ソースの作成

たとえば、自動作成機能がオフになっている場合に、CLI を使用して NAM の NetFlow データ ソースを手動で設定するには、次の手順を実行します。CLI を使用する場合、次の 2 段階の手順を実行します。まず NAM の「デバイス」エントリを作成し、そのデバイス ID を記憶する必要があります。次に、このデバイス ID を使用してデータ ソース エントリを作成する必要があります。便宜上、GUI を使用して NetFlow データ ソースを作成する場合、これら 2 つの段階は 1 つになっています。

**ステップ 1**　**device netflow** コマンドを入力します。これで、netflow デバイス サブコマンド モードになります（次を参照）。

```
root@172-20-104-107.cisco.com# device netflow
Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.
root@172-20-104-107.cisco.com(sub-device-netflow)#
```

**ステップ 2**　**?** を入力すると、このコマンドに使用できるオプションがすべて表示されます（次の例を参照）。

```
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
?                         - display help
address                   - device IP address (*)
cancel                    - discard changes and exit from subcommand mode
community                 - SNMPv2c community string
exit                      - create device and exit from sub-command mode
help                      - display help
show                      - show current config that will be applied on exit
snmp-version              - SNMP version to use to communicate with device
v3-auth-passphrase        - SNMPv3 authentication passphrase
v3-auth-protocol          - SNMPv3 authentication protocol
v3-priv-passphrase        - SNMPv3 privacy passphrase
v3-priv-protocol          - SNMPv3 privacy protocol
v3-sec-level              - SNMPv3 security level
v3-username               - SNMPv3 username
(*) - denotes a mandatory field for this configuration.
root@172-20-104-107.cisco.com(sub-device-netflow)#
```

**ステップ 3**　次の例のように、デバイスの IP アドレスを入力します（必須）。

```
root@172-20-104-107.cisco.com(sub-device-netflow)# address 192.168.0.1
```

**ステップ 4**　必要に応じて、デバイスの SNMP クレデンシャルを入力します（次の例を参照）。snmp-version v2c を指定する場合は、デバイスのコミュニティ ストリングを入力する必要があります。snmp-version v3 を指定する場合は、セキュリティ レベル、ユーザ名、認証プロトコル、認証パスフレーズ、プライバシー プロトコル、およびプライバシー パスフレーズを入力する必要があります。

```
root@172-20-104-107.cisco.com(sub-device-netflow)# snmp-version v2c
root@172-20-104-107.cisco.com(sub-device-netflow)# community public
```

**ステップ 5**　**show** と入力して、適用されるデバイスの設定を調べ、それが正しいことを確認します。

```
root@172-20-104-107.cisco.com(sub-device-netflow)# show
DEVICE TYPE         : NDE (Netflow Data Export)
DEVICE ADDRESS      : 192.168.0.1
SNMP VERSION        : SNMPv2c
V2C COMMUNITY       : public
V3 USERNAME         :
V3 SECURITY LEVEL   : No authentication, no privacy
V3 AUTHENTICATION   : MD5
V3 AUTH PASSPHRASE  :
V3 PRIVACY          : DES
V3 PRIV PASSPHRASE  :
root@172-20-104-107.cisco.com(sub-device-netflow)#
```

**ステップ 6**　**exit** と入力して、サブコマンド モードを終了し、デバイスを作成します。新しいデバイスに割り当てられた ID 値を覚えておいてください。データ ソースを作成するために必要になります。

```
root@172-20-104-107.cisco.com(sub-device-netflow)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#
```

**ステップ 7**　**data-source netflow** コマンドを入力します。これで、netflow データ ソース サブコマンド モードになります（次を参照）。

```
root@172-20-104-107.cisco.com# data-source netflow
Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.
root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

**ステップ 8**　**?** を入力すると、このコマンドに使用できるオプションがすべて表示されます（次の例を参照）。

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# ?
?                         - display help
cancel                    - discard changes and exit from subcommand mode
device-id                 - netflow device ID (*)
engine-id                 - netflow Engine ID
exit                      - create data-source and exit from sub-command mode
help                      - display help
name                      - data-source name (*)
show                      - show current config that will be applied on exit
(*) - denotes a mandatory field for this configuration.
root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

**ステップ 9**　ステップ 4 のデバイス ID を入力します（必須）。

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# device-id 1
```

**ステップ 10**　データ ソースに付ける名前を入力します（必須）。

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# name MyFirstNdeDataSource
```

**ステップ 11**　必要に応じて、この NDE データ ソースに固有のエンジン ID を指定します（任意）。

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# engine-id 123
```

**ステップ 12**　**show** と入力し、適用されるデータ ソースの設定を調べ、それが正しいことを確認します。

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show
DATA SOURCE NAME : MyFirstNdeDataSource
DATA SOURCE TYPE : NDE (Netflow Data Export)
DEVICE ID        : 1
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123
root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

**ステップ 13**　**exit** と入力して、サブコマンド モードを終了し、データ ソースを作成します。

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# exit
Data source created successfully, ID = 3
```

---

これでデータ ソースが作成され、デバイスからの NDE レコードが NAM に着信すると、受信され、受け入れられるようになります。

### CLI による NetFlow データ ソースの削除

CLI を使用して NetFlow データ ソースを削除するには、次の手順を実行します。CLI を使用する場合、通常は次の 2 段階の手順を実行します。まずデータ ソースを削除し、次に、同じデバイスを使用している（たとえば、別のエンジン ID 値を持つ）他のデータ ソースがない場合はそのデバイスを削除します。簡単な方法もあり、デバイスを削除すると、そのデバイスを使用しているすべてのデータ ソースも削除されます。

**ステップ 1**　すべてのデータ ソースを表示して、削除する ID を探します。

```
root@172-20-104-107.cisco.com# show data-source
DATA SOURCE ID   : 1
DATA SOURCE NAME : DATA PORT 1
TYPE             : Data Port
PORT NUMBER      : 1
-----------
DATA SOURCE ID   : 2
DATA SOURCE NAME : DATA PORT 2
TYPE             : Data Port
PORT NUMBER      : 2
-----------
DATA SOURCE ID   : 3
DATA SOURCE NAME : MyFirstNdeDataSource
TYPE             : NDE (Netflow Data Export)
DEVICE ID        : 2
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123
-----------
root@172-20-104-107.cisco.com#
```

**ステップ 2**　「no data-source」コマンドを使用して、データ ソースを削除します。

```
root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#
```

**ステップ 3**　すべてのデバイスを表示して、削除するデバイスの ID を探します。

```
root@172-20-104-107.cisco.com# show device
DEVICE ID            : 1
DEVICE TYPE          : NDE (Netflow Data Export)
IP ADDRESS           : 192.168.0.1
SNMP VERSION         : SNMPv2c
V2C COMMUNITY        : public
V3 USERNAME          :
V3 SECURITY LEVEL    : No authentication, no privacy
V3 AUTHENTICATION    : MD5
V3 AUTH PASSPHRASE   :
V3 PRIVACY           : DES
V3 PRIV PASSPHRASE   :
INFORMATION          : No packets received
STATUS               : Inactive
------
root@172-20-104-107.cisco.com#
```

**ステップ 4**　「no device」コマンドを使用して、デバイスを削除します。

```
root@172-20-104-107.cisco.com# no device 1
Sucessfully deleted device 1
root@172-20-104-107.cisco.com#
```

自動作成モードがオンになっていて、デバイスが NDE パケットを NAM に送信し続ける場合、次の NDE パケットが到着すると、すぐにデータ ソース（およびデバイス エントリ）が自動的に再作成されます。したがって、既存の NetFlow データ ソースを削除する場合、通常は、前述したように、まず NetFlow 自動作成機能をオフにすることを推奨します。

# デバイス上での NetFlow の設定

NDE パケットを NAM にエクスポートするための NetFlow デバイスのコンフィギュレーション コマンドは、プラットフォームおよびデバイス固有です。ここで例として示すコンフィギュレーション コマンドは、Cisco IOS を実行するデバイスで最もよく見られるものです。詳細については、お使いのデバイスのマニュアルを参照してください。

### Cisco IOS を実行するデバイスの場合

**ステップ 1**　ルーティングされるフローのキャッシュを有効にするインターフェイスを選択します。

```
Prompt# configure terminal
Prompt(config)# interface <type slot/port>

Prompt(config-if)# ip route-cache flow
```

**ステップ 2**　ルーティングされるフローのキャッシュ エントリを、NAM の UDP ポート 3000 にエクスポートします。

```
Prompt(config)# ip flow-export destination <NAM IP address> 3000
```

### Cisco IOS を実行し、マルチレイヤ スイッチング キャッシュをサポートするデバイスの場合

**ステップ 1**　NDE のバージョンを選択します。

```
Prompt(config)# mls nde sender version <version-number>
```

**（注）**　NAM は、NDE バージョン 1、5、6、7、8、および 9 の集約キャッシュをサポートします。

**ステップ 2**　NDE フロー マスクを選択します。

```
Prompt(config)# mls flow ip full
```

**ステップ 3**　NetFlow エクスポートをイネーブルにします。

```
Prompt(config)# mls nde sender
```

**ステップ 4**　NAM の UDP ポート 3000 に NetFlow をエクスポートします。

```
Prompt(config)# ip flow-export destination <NAM IP address> 3000
```

### Cisco IOS を実行し、NDE v8 集約をサポートするデバイスの場合

**ステップ 1**　v8 集約を選択します。

```
Prompt(config)# ip flow-aggregation cache <aggregation-type>
```

*aggregation-type* には、次のいずれかを指定できます。

- destination-prefix
- source-prefix
- protocol-port
- prefix

**ステップ 2**　集約キャッシュをイネーブルにします。

```
Prompt(config-flow-cache)# enable
```

**ステップ 3**　集約キャッシュ内のフロー エントリを NAM UDP ポート 3000 にエクスポートします。

```
Prompt(config-flow-cache)#export destination <NAM address> 3000
```

### ブリッジ フロー統計情報からの NDE エクスポートをサポートするデバイスの場合

**ステップ 1**　VLAN 上でのブリッジ フロー統計情報をイネーブルにします。

```
Prompt>(enable) set mls bridged-flow-statistics enable <vlan-list>
```

**ステップ 2**　NAM の UPD ポート 3000 に NDE パケットをエクスポートします。

```
Prompt>(enable) set mls nde <NAM address> 3000
```

### デバイス スロットにある NAM の場合

NAM がデバイス スロットのいずれかにある場合は、NDE パケットを NAM にエクスポートするようにデバイスを設定できます。

**ステップ 1**　NDE のバージョンを選択します。

```
Prompt>(enable) set mls nde version <nde-version-number>
```

**ステップ 2**　full にする NDE フロー マスクを選択します。

```
Prompt>(enable) sel mls nde full
```

**ステップ 3**　NDE エクスポートをイネーブルにします。

```
Prompt>(enable) set mls nde enable
```

**ステップ 4**　NDE パケットを NAM にエクスポートします。

```
Prompt>(enable) set snmp extendedrmon netflow enable <NAM-slot>
```