# Syslog、SNMP トラップ監視の設定

AdRem NetCrunch 8 **参考資料**

# Syslog、SNMP トラップ監視の設定

NetCrunch は AdRem Software が開発し所有する監視ソフトウェアである。
株式会社情報工房は日本における総販売代理店である。

# 目次

# 1. Syslog、SNMP トラップ監視の概要

本資料では、AdRem NetCrunch 8.7.2.3466 日本語版（以下 8）における Syslog、SNMP トラップ監視のイベントの定義方法について記載します。なお、ご利用の NetCrunch のビルド番号が異なりますと、仕様の変更などにより、動作、設定などが異なる場合がございます。あらかじめご了承ください。

Syslog もしくは SNMP トラップを利用して監視を行いたい場合、監視対象側から NetCrunch に対して Syslog、SNMP トラップを送信する必要がございます。監視対象側の設定については、本資料には記載しておりません。本資料では、NetCrunch が Syslog、SNMP トラップを受信するために必要な NetCrunch 側の設定について記載しております。

# 2. Syslog、SNMP トラップ監視の設定方法

NetCrunch 8 での設定方法について記載いたします。

なお、以下に NetCrunch アドミニストレーションコンソールの操作方法を例示しておりますが、ご利用の環境や設定したい内容によって操作が異なる場合がございます。あらかじめご了承ください。

## 2.1. NetCrunch オプションの設定

NetCrunch オプションにて、Syslog、SNMP トラップの受信を許可する設定を行います。

1. NetCrunch のメインメニュー→[ツール]→[オプション]を選択します。
2. [オプション]ウィンドウの上部にて[監視]タブを選択します。
3. ウィンドウの左側にて[Syslog]もしくは[SNMP トラップ]を選択します。
4. [Syslog メッセージを受信する]もしくは[SNMP トラップを受信する]を有効化します。
5. その他、受信するポート番号など、必要に応じて他の項目の設定を行い、[OK]をクリックします。

## 2.2. ノードの追加

Syslog、SNMP トラップの送信元 IP アドレスをノードとして追加します。すでにアトラス上に対象のノードが存在する場合は、新たに追加する必要はございません。

1. NetCrunch のメインメニュー→[アクション]→[監視]→[新規ノードの監視]を選択します。

2. [監視するノードの追加]ウィンドウにて、ノードの IP アドレスやネットワークマスクを入力の上、[OK]をクリックします。
   ※[ノードの設定を開く]を選択した状態で[OK]をクリックしますと、追加したノードの[ノードの設定]ウィンドウが表示されます。

## 2.3.ノードの設定（SNMP トラップの場合）

SNMP トラップを受信する場合は、SNMP トラップの送信元 IP アドレスとなるノードに対して SNMP の利用の設定を行います。

以下の手順では、デバイスタイプが設定されているノードに対する手順となります。デバイスタイプを設定していないノードの[ノードの設定]を選択しますと、ウィザードが表示されますので、ウィザードに従ってデバイスタイプの設定をご試行ください。

1. ノードを右クリック→[ノードの設定]を選択します。
2. SNMP の監視が無効になっている場合、新しく開いたウィンドウの[監視]タブの右上に[SNMP 無し（無効）]と表示されますので、[SNMP 無し（無効）]→[SNMP 監視の有効化]を選択します。
   SNMP の監視が有効になっている場合は、手順[3.]に進みます。
3. [監視]タブにある SNMP の項目の右端にある青いアイコンをクリックします。
4. SNMP プロフィールなど必要に応じて設定を行います。
   ※SNMP トラップに含まれるコミュニティは、SNMP プロフィールの[Notifications]に設定します。
5. 設定を変更した場合は[保存]ボタンが表示されますので、[保存]をクリックします。

## 2.4.Syslog、SNMP トラップ受信イベントの定義

NetCrunch では、Syslog、SNMP トラップをイベントとして扱います。イベントの定義方法について以下に例示いたします。

なお、以下の手順では例として、新たに作成した監視パックに対してイベントを追加しておりますが、ノードやマップ、自動監視パックに対して定義することも可能です。また、既存の監視パックに対して編集することも可能です。

1. NetCrunch のメインメニュー→[ツール]→[アラート＆レポート]→[設定]を選択します。
2. [NetCrunch アラート＆レポートの設定]ウィンドウの[監視パック]タブにて、[新しい監視パック]をクリックします。
3. [アラート＆レポート設定の作成]ウィンドウにて、[監視パック]をクリックします。
4. [監視パックの設定]ウィンドウの[アラート＆レポート]タブにて、[アラートの追加]をクリックします。

5. [監視イベントの追加]ウィンドウにて、下記のイベントをダブルクリックします。
   Syslog の場合：
   [基本]タブ
   ＜新しい Syslog メッセージ受信イベントを作成＞
   SNMP トラップの場合：
   [SNMP]タブ
   ＜新しい SNMP トラップ受信イベントを作成＞
6. [イベント定義の編集]ウィンドウにて必要に応じて設定を行い、[OK]をクリックします。
7. [監視パックの設定]ウィンドウの[割り当て]タブにて、[ノードの追加]をクリックします。
8. [ポリシーにノードの追加]ウィンドウにて、監視パックを割り当てるノードを選択し、[OK]をクリックします。
   ※Ctrl キーや Shift キーを利用して、ノードを複数選択することも可能です。

Syslog、SNMP トラップ受信イベントの定義について補足いたします。
Syslog、SNMP トラップ受信イベントでは、受信するパケットのフィルター条件を定義することができます。
Syslog の場合、イベント定義の[基準に適合するメッセージ]を利用して柔軟な条件を定義できます。重要度が Critical である場合、ある文字列を含む場合などのように、条件に合致した Syslog のみ受信することができます。
SNMP トラップの場合、フィルター条件として受信する SNMP トラップの汎用タイプや OID を指定できます。なお、ある特定の SNMP トラップ以外を受信するという定義はできません。あらかじめご了承ください。

# 3. Syslog、SNMP トラップを受信できない場合

Syslog、SNMP トラップを受信できない場合は、下記についてご確認ください。

## 3.1. 送信元 IP アドレスの確認

複数の IP アドレスを持つノードの場合などには、Syslog、SNMP トラップの送信元となる IP アドレスにご注意ください。
パケットの送信元がイベントを定義したノードと異なる IP アドレスと異なる場合、Syslog、SNMP トラップが送られてきましても NetCrunch ではイベントが発生しません。Syslog、SNMP トラップの送信元 IP アドレスのノードに対して、受信のためのイベントを定義する必要がございます。
また、SNMP トラップの agent-address が送信元 IP アドレス（source）と同一であるかをご確認ください。agent-address が送信元 IP アドレスと異なる場合、NetCrunch は agent-address の IP アドレスが SNMP トラップを送信してきたノードとして認識します。そのため、agent-address となっているノードに対して SNMP トラップ受信イベントを定義する必要がございます。

## 3.2.ファイアウォールの確認

ネットワーク上にあるファイアウォールや NetCrunch 搭載サーバー上のファイアウォールにて、Syslog、SNMP トラップがブロックされていないかご確認ください。

## 3.3.SNMP の設定の確認（SNMP トラップの場合）

SNMP トラップが受信できない場合は、SNMP トラップの送信元 IP アドレスとなるノードにおいて、SNMP の監視が有効化されているかをご確認ください。

1. ノードを右クリック→[ノードの設定]を選択します。
2. 新しく表示されたウィンドウの[監視]タブにて、SNMP の項目が表示されることを確認します。
3. SNMP の項目の右端の青いアイコンをクリックします。
4. [SNMP プロフィール]の右側にある[編集]をクリックします。
5. [SNMP プロフィールプロパティ]ウィンドウの[Notifications]に設定した SNMP のバージョン、コミュニティを確認します。

## 3.4.イベント状態の確認

監視パックやマップ単位でイベントを定義した場合、ノードにイベントが継承されていることをご確認ください。また、ノードにて定義したイベントのイベント状態が有効となっているかをご確認ください。
以下に確認手順を例示いたします。

1. NetCrunch のメインメニュー→[ツール]→[アラート＆レポート]→[設定]を選択します。
2. [NetCrunch アラート＆レポートの設定]ウィンドウの[設定がカスタマイズされたノード]タブにて、対象のノードが表示されている場合はノードをクリックします。表示されていない場合は、[ノードの設定の追加]から対象のノードを選択します。
3. [ノード監視設定]ウィンドウにて、対象のイベントのイベント状態が有効になっているかを確認します。

イベント状態が無効となっている場合は、監視を有効化する必要がございます。イベントを右クリック→[有効化]にてイベントを有効化できます。

## 3.5.イベント定義の確認

イベントにフィルター条件を定義している場合、フィルター条件に合致しない Syslog、SNMP トラップは受信できません。イベントにフィルター条件を定義しているかをご確認ください。
以下に確認手順を例示いたします。以下の手順ではノードにて確認しておりますが、実際にイベントを定義した監視パックやマップでもご確認いただけます。

1. NetCrunch のメインメニュー→[ツール]→[アラート＆レポート]→[設定]を選択します。
2. [NetCrunch アラート＆レポートの設定]ウィンドウの[設定がカスタマイズされたノード]タブにて、対象のノードが表示されている場合はノードをクリックします。表示されていない場合は、[ノードの設定の追加]から対象のノードを選択します。
3. [ノード監視設定]ウィンドウにて、対象のイベントを右クリック→[イベントルールの編集]を選択します。
4. [イベント定義の編集]ウィンドウにて、フィルター条件（Syslog の場合、[基準に適合するメッセージ]）が設定されているかを確認します。

イベントにフィルター条件を定義している場合は、新たに全ての Syslog、SNMP トラップを受信するイベントの追加をご試行ください。全ての Syslog、SNMP トラップを受信するイベントが発生する場合には、フィルター条件の不一致が原因であったものと考えられます。

## 3.6.イベントログの表示の確認

イベントログにはフィルター機能がございます。Syslog、SNMP トラップのイベントログが、フィルター機能によって非表示となっていないかご確認ください。
イベントログの[履歴]タブにて、[ビュー]を[全てのアラート]にしますと、全てのイベントログが表示の対象となります。
また、画面右側に[【確認】を表示/隠す]という項目がございます。【確認】が非表示となっている場合、状態が確認となっているイベントログは表示されませんのでご注意ください。

## 3.7.パケットキャプチャ

パケットキャプチャのソフトウェアを利用して、NetCrunch 搭載サーバー上で Syslog、SNMP トラップを受信できるかをご確認ください。