指定労働日レポート

SNMPでネットワーク監視について

2019,07 ,20

社員番号：719755

Tuvdendorj　Gantulga

◆目的◆

今の現場ではリナックスオペレーティングシステムにSNMP ー 「simple network monitoring protocol」使ってサーバーとネットワーク機器を監視しています。なぜ監視している、それはこのデバイスに何か障害起きたらすぐ問題を見つけて直すことです。

◆作成 ◆

まず顧客さんのとネットワークのとこれでリナックスを設置します。その後監視したい機器を登録して接続をチェックする時ターミナルでPINGとか送ったりチェックします。

それを終わったらリナックスで顧客さんのこいうIDで登録した機器を監視していることをデータセンターの障害防止ウェッブサイトに登録します。

◆SNMP概要◆

\*　SNMPは、ネットワーク機器やサーバなどネットワークに接続された通信機器の監視や制御また、ネットワーク越しに実現するためのプロトコルである、ネットワーク機器の情報を取得することができる。

\* MIB

SNMPが使用する管理情報データベースに管理をする機器は対象機器のMIBに基づいて適切な設定をします。

\*　SNMPTRAP

SNMPを使用する機器が異常を検知した場合に監視端末に知らせるためのパケットです。これはSNMPTRAPと言います。

◆SNMP仕組み◆

SNMPを使用したネットワーク管理

\* SNMPマネージャとエージェント

ネットワーク機器には通常SNMPエージェント使ってている。サーバ上のSNMPマネージャと通信をしてことで色々な情報の取得や設定をする。

\*　MIBの参照

SNMPエージェントは管理対象機器のMIBを接続して情報の取得をします。この時参照するMIBにはRFCによって規定されている標準MIBとベンダが独自に拡張したプライベートMIBがあります、MIBのデータはオブジェクトID(OID)と言います、

\* マネージャとエージェント間のSNMPネットワーク

- Get

マネージャは、エージェントに対してgetrequestメッセージを送ります。エージェントはgetresponseメッセージを送信してOIDを返答する。この時に、マネージャからGetNextRequestが送らればエージェントは順番に情報を返答する。この改装のことをオブジェクトツリーという。

- Set

マネージャは、エージェントに対してSetRequestメッセージを発行します。エージェントは呼ばれたOIDに指定値を設定します。これによって、ネットワーク機器の設定を変更することができます。

- Trapエージェントは自動的にマネージャに対して、状態の変更を通知します。

表１

|  |  |  |
| --- | --- | --- |
| **SNMPメッセージ** | **送信側** | **意味** |
| Get Request | SNMPマネージャ | SNMPエージェントからもらいたい情報を、**OID**を指定して要求 |
| GetNext Request | SNMPマネージャ | 前に指定したOIDの次のOIDを指定して要求。 |
| Set Request | SNMPマネージャ | SNMPエージェントの設定変更を送りたい場合、OIDを指定して要求 |
| Get Response | SNMPエージェント | SNMPマネージャから要求された**OID**に対して、値を入れてて返信 |
| TRAP | SNMPエージェント | SNMPエージェントが機器の状態に変化があった場合、自発的に送信 |

**顧客さんの監視し**

**てされた機器**

**B会社**

SNMPマナージャ

リナックス機器

**Get Request　IODは.0.1.2.3.4.5.5.6**

**SNMP エージェント**

**Get Responce IODは.0.1.2.3.4.5.5.6**

**障害発生してSNMP で取得した**

**情報をメールで暗号して送付します**

**障害置きましたようと電話とメールで通知します**

**A会社**

**各顧客さんの登録された**

**機器を管理**

このようなメッセージ送ったり取得したり監視して情報をまとめてA社に送ってその後A社はB顧客さん連絡します。この機器がPowerOffになりました原因はそれですと伝えます。顧客さんに案件に従って応援します。

◆リナックスにSNMP設定◆

今回２台に設置しますCentOSとUbuntu

まずCENTOS７に下のコマンドを実行

Rootでアクセスして

yum update　 最新のアップデート

yum install net-snmp net-snmp-utils 　　　SNMPをダウンロード

二番目Ubuntu18.04

Rootでアクセスして

apt update 最新のアップデート

apt install snmpd snmp libsnmp-dev　SNMPをダウンロード

その後両方ともこのファイルを修正します

/etc/snmp/snmpd.conf

念の為cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak

このコマンドで保存してもらうます。

今ファイル修正

vim /etc/snmp/snmpd.conf　　　VIMでオペンして

...

# AGENT BEHAVIOUR

# Listen for connections from the local system only

**agentAddress udp:127.0.0.1:161,udp:192.168.43.154:161**

# Listen for connections on all interfaces (both IPv4 \*and\* IPv6)

#agentAddress udp:161,udp6:[::1]:161

...

#######################################################################

# ACCESS CONTROL

...

**rocommunity Ex@mPL3 192.168.43.101**

#######################################################################

#

# SYSTEM INFORMATION

上野赤IPは監視される、緑のはマナージャIPです。

その後再起動します

systemctl reload snmpd

実際に接続しているかどうかチェック

netstat -nlpu|grep snmp

udp 16128 0 **192.168.43.154:161** 0.0.0.0:\* 10057/snmpd

udp 3072 0 **127.0.0.1:161** 0.0.0.0:\*

これで終わりますがFIREWALLあったらこのコマンドでACCEPTします

ufw allow from 192.168.43.101 to any port 161 proto udp

ufw reload

◆実際にメッセージ送り◆

このコマンドでチェックします

snmpwalk -v2c -c Ex@mPL3 192.168.43.154

その後答えは

iso.3.6.1.2.1.1.1.0 = STRING: "Linux u18svr 4.15.0-46-generic #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019 x86\_64"

iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10

iso.3.6.1.2.1.1.3.0 = Timeticks: (1082) 0:00:10.82

iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"

iso.3.6.1.2.1.1.5.0 = STRING: "ubuntu18svr"

iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"

iso.3.6.1.2.1.1.7.0 = INTEGER: 72

iso.3.6.1.2.1.1.8.0 = Timeticks: (2) 0:00:00.02

iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1

iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1

でこれで接続したこと分かります

◆懸案事項◆

今回、SNMP使ってサーバーとかネットワーク機器を監視するSNMPのことを勉強して様々のことを理解できました。