TCPポート･プロセス監視拡張機能

SNMP標準MIBによるTCPポート監視、プロセス監視に加えて
処理速度に優れた2つの拡張機能を追加しました

1.TCPポート監視拡張機能
2.プロセス監視拡張機能
3.プライベートMIBのインストールと設定
4.プライベートMIBのTCPポート監視、プロセス監視の動作試験と運用開始
5.NCATポート監視拡張機能

1. TCPポート監視拡張機能

1.1 監視マネージャから監視対象ホストのTCPポート状態を監視する3方式

標準MIB方式
　監視対象ホストのTCPポート標準MIB情報を取得し、監視マネージャ側の
　監視アプリでTCPポートを開閉をチェックする

プライベートMIB方式
　監視対象ホストにプライベートMIBとチェックアプリをインスールの上、
　定期的にTCPポートをチェックし、監視マネージャがチェック済の
　プライベートMIB情報を取得する

NCAT方式
　監視マネージャ側のNCATコマンドでTCPポート開閉をチェックする

1. TCPポート監視拡張機能

1.2 TCPポート監視方式の比較・得失

方式比較

○ 処理間
短い＜－－－－－－－－－－－－－－－－－－－－－－－－－－＞長い
プライベートMIB方式　＜　NCAT方式　＜　標準MIB方式

○ 構築容易さ
容易＜－－－－－－－－－－－－－－－－－－－－－－－－－－＞複雑
標準MIB方式　＜　NCAT方式　＜　プライベートMIB方式

得失

○ プライベートMIB方式
Windowsの監視対象ホストは不可、プライベートMIBが必要
○ NCAT方式
監視マネージャ側にNCATコマンドが必要

2. プロセス監視拡張機能

2.1 監視マネージャから監視対象ホストのプロセス状態を監視する2方式

標準MIB方式

監視対象ホストのプロセス標準MIB情報を取得し、監視マネージャ側の
監視アプリでプロセスの存在、不在をチェックする

プライベートMIB方式

監視対象ホストにプライベートMIBとチェックアプリをインスールの上、
定期的にプロセスをチェックし、監視マネージャがチェック済の
プライベートMIB情報を取得する

2. プロセス監視拡張機能

2.2 プロセス監視方式の比較・得失

方式比較

〇処理間
短い<ーーーーーーーーーーーーーーーー>長い
プライベートMIB方式　＜　標準MIB方式

〇構築容易さ
容易<ーーーーーーーーーーーーーーーー>複雑
標準MIB方式　＜　プライベートMIB方式

得失

プライベートMIB方式
Windowsの監視対象ホストは不可、プライベートMIBが必要

3. プライベートMIBのインストールと設定

3.1 プライベートMIBのインストール

3.1.1 GitHubのvisualmonitor/phplinux/vmmib/RPMSの
vmmib-x.x.x-x.elx.x86-64.rpmをインストール
例: *$ sudo rpm –ivh vmmib-2.0.3-1.el8.x86_64.rpm*
Net-snmp、chkconfig不足でエラーになる

3.1.2 インストール確認
例: *$ rpm –ql vmmib*

3. 2 インストールデータの変更と設定

3.2.1 /usr/local/etc/snmpd.conf.newのcommunity(デフォルトはremote)などを
カスタマイズし、/etc/snmp/snmpd.confと取り換える

3.2.2 OS再起動

3. 3 動作確認

3.3.1 vmmib自動起動確認
例: *$ ps –ef | grep vmmib*

3.3.2 vmmib動作確認
例: *$ snmpwalk –v1 –cremote localhost .1.3.6.1.4.1.999999.1*

```
SNMPv2-SMI::enterprises.999999.1.1.0 = INTEGER: 0
SNMPv2-SMI::enterprises.999999.1.2.0 = ""
SNMPv2-SMI::enterprises.999999.1.3.0 = "“
SNMPv2-SMI::enterprises.999999.1.4.0 = ""
SNMPv2-SMI::enterprises.999999.1.5.0 = ""
```

3. 3. 3 ファイウオール
リモートからのアクセスには、ファイアウオールのUDP161ポートを許可する

4. プライベートMIBの動作試験と運用開始

4.1 プライベートMIBの動作試験

4.1.1 チェックするTCPポート、プロセスをvmmibへセット

例: *$ snmpset -v1 -cremote localhost .1.3.6.1.4.1.999999.1.2.0 s "22;1234"*
$ snmpset -v1 -cremote localhost .1.3.6.1.4.1.999999.1.4.0 s "sshd;abcd"

4.1.2 TCPポート、プロセス情報のvmmibセット確認

例: *$ snmpget -v1 -cremote localhost .1.3.6.1.4.1.999999.1.2.0*
$ snmpget -v1 -cremote localhost .1.3.6.1.4.1.999999.1.4.0

4.1.3 vmmibチェックプログラム起動

例: *$ /usr/local/bin/snmptcpportcheck.sh*
$ /usr/local/bin/snmpprocesscheck.sh

4.1.4 チェック後のTCPポート、プロセス情報のvmmibセット確認

例: *$ snmpwalk -v1 -cremote localhost .1.3.6.1.4.1.999999.1*

SNMPv2-SMI::enterprises.999999.1.1.0 = INTEGER: 0
SNMPv2-SMI::enterprises.999999.1.2.0 = "22;1234"
SNMPv2-SMI::enterprises.999999.1.3.0 = "1234"
SNMPv2-SMI::enterprises.999999.1.4.0 = "ssh;abcd"
SNMPv2-SMI::enterprises.999999.1.5.0 = "abcd"

この例のlocalhostでは、TCPポート1234、プロセスabcdが存在していない

4.1.5 チェックプログラムをCRONTABで登録し運用開始

例: *$ sudo crontab -e*

0,30 * * * * /usr/local/bin/snmptcpportcheck.sh
1,31 * * * * /usr/local/bin/snmpprocesscheck.sh

5. NCAT監視拡張機能

5.1 NCATコマンドのインストール

5.1.1 WindowsおよびLinuxの監視マネージャで使用するNCATをインストールする

Windows

ダウンロードサイト *https://nmap.org/dist/*

Linux

$ sudo yum install nmap または sudo dnf install nmap

5.1.2 確認試験

ファイアウオールがある場合は、試験するポートを許可して置く

Windows例

```
> "c:¥Program Files (x86)¥nmap¥ncat.exe" -zv -w 1 <監視対象ホスト> 80
> echo %ERRORLEVEL%
> 0
> "c:¥Program Files (x86)¥nmap¥ncat.exe" -zv -w 1 <監視対象ホスト> 1234
> echo %ERRORLEVEL%
> 1
```

Linux例

```
$ ncat -zv -w 1 <監視対象ホスト> 80
$ echo $?
  0
$ ncat -zv -w 1 <監視対象ホスト> 1234
  1
```

5. NCAT監視拡張機能

5.2 監視マネージャの初期設定

5.2.1 Windowsの設定

…xampp/htdoc/kanshiphp/vmsetup/kanshiphp.iniへ
vpath_ncat = < ncatコマンドのパス >
例: vpath = “c:¥Program Files (x86)¥nmap”

5.2.2 Linuxの設定

デフォルトインストール先が/usr/binで無ければ、PATH環境変数にPATHを追加