

UNIX/LINUX 監視用プロファイルとサービスの使い方

aeMonitor には UNIX と Linux システム監視のためのホストプロファイル `host-profile-ssh-unix` が登録されています。これは UNIX および Linux システムを監視するために SSH を利用するサービスをまとめ、一括して Linux や Unix 監視を登録できるようにしたものです。

本資料では、この SSH プロファイル（とそれに含まれている SSH 経由の監視サービス/プラグイン）を活用するための方法について説明します。

1. SSH プロファイルと含まれるサービス

下記のプロファイルとサービスは、SSH を使用して UNIX/LINUX の状況を監視します。

これらを使って SSH 監視を行なうには、本書で説明する SSH 監視設定が必要です。

ホストプロファイル : `host-profile-ssh-unix`

サービスプロファイル : `ssh-unix`

サービス : `ssh_disk_root`

`ssh_load`

`ssh_memory`

`ssh_process_count`

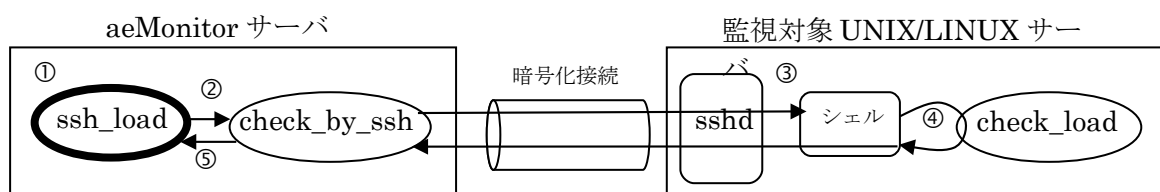
`ssh_swap`

2. SSH 監視の仕組み

これらは UNIX/LINUX の SSH によるリモートコマンド実行の仕組みを利用した監視方式です。

`ssh_load` サービスを例として、リモート UNIX/Linux システムの CPU ロードアベレージを調べる仕組みを説明します：

- 1 aeMonitor/Nagios によって `ssh_load` サービスが実行されるとサービスに関係付けられたプラグイン `check_by_ssh` が起動される
- 2 `check_by_ssh` は引数で指定された監視対象サーバに SSH 接続する。
- 3 SSH 接続が確立するとリモート側でシェルが起動され `check_by_ssh` からプラグインコマンド名 (`check_load`) とパラメータが送られる。
- 4 リモートのシェルは受け取ったコマンドを実行し結果応答を `check_by_ssh` に返す。
- 5 `check_by_ssh` は応答結果を `ssh_load` サービスに返す。



3. SSH 監視設定について

以下に説明する手順で SSH 監視のための設定を行なってください。

1) 前提条件

監視対象となる UNIX や LINUX システムは、下記の条件を満たす必要があります

- ログインアカウント **nagios** を追加できること
- **nagios** アカウントのホームディレクトリを割り当てられること
- **sshd** デーモンが稼動していること
- 公開キー認証が有効であること（有効にできること）
- **Nagios** プラグインをシステム上に配置できること

2) 監視対象システムでの作業

各サーバで以下の手順で、SSH 設定をします。下記では、Linux（RedHat/CentOS など）を例としますが、UNIX や他の Linux ディストリビューションでも同様に実施してください。

Step1: ターゲットのサーバに **root** としてログインする。

i) **nagios** ユーザとそのディレクトリを作成する。

```
useradd -m nagios
```

ii) ユーザディレクトリのパーミッション確認(755)。

```
ls -lad /home
```

iii) **passwd** コマンドでパスワードを設定する。

（設定の容易化のため、監視対象すべてに同一のパスワード使用を推奨）

```
passwd nagios
```

Step2: SSH 設定のため、ディレクトリ移動:

```
cd /etc/ssh
```

Step3: SSH デーモン設定ファイルを編集し、**PubkeyAuthentication** を有効にする。

```
vi sshd_config
```

—> **PubkeyAuthentication yes** の行を探し、
コメントアウトされていたら行頭の **#** を外す。
:wq で変更を書き込む。

Step4: SSH デーモンのリスタート

```
service sshd restart
```

3) aeMonitor サーバでキーを作成する

Step1: サーバに root としてログインし、su で nagios ユーザになる

```
su - Nagios
```

Step2: 公開キーと秘密キーを作成する

- ・ キー作成コマンドを入力 :

```
ssh-keygen -t dsa -b 1024
```

(パスフレーズ等の入力をうながされるが、Enter を押すのみ : 3 回)

- ・ 作成されたキー情報のパーミッションを設定する :

```
chmod 600 /home/nagios/.ssh/id_dsa
```

```
chown nagios:nagios /home/nagios/.ssh/id_dsa
```

4) aeMonitor サーバから各監視対象サーバにアクセスして作業 :

Step1: ssh (セキュアシェル) で各監視対象サーバへアクセスする

```
ssh <サーバ名 or IP アドレス>
```

- ー 最初にアクセスしたとき下記のようなメッセージが表示されます :

```
Are you sure you want to continue connecting (yes/no)?
```

yes と入力してください。

- ー 下記のようなメッセージが表示されます :

```
Warning: Permanently added 'サーバ名' (RSA) to the list of known hosts.
```

```
nagios@<サーバ名>'s password:
```

- ー 2)の Step1 で登録した nagios ユーザのパスワードを入力すると、相手サーバにログインできるはずです。

Step2: nagios プラグインのためのディレクトリを作ります。

```
mkdir libexec
```

Step3: このディレクトリに公開キーと秘密キーのためのディレクトリを作成します。

```
mkdir /home/nagios/.ssh
```

```
chmod 700 .ssh
```

Step4: セキュアシェルを終了します。

```
exit
```

Step5: 各監視対象サーバに公開キーをコピーします。

```
scp .ssh/id_dsa.pub nagios@<XXXXXX>:/home/nagios/.ssh/authorized_keys
```

(XXXXXX はサーバ名か IP アドレス)

Step6: ssh コネクションをテストします。

ssh <サーバ名 or IP アドレス>

でパスワードなしにログインできることの確認。直ぐにシェルのプロンプトが表示される。
確認できたら、**exit** で終了。

5) プラグインの導入とテスト

a) プラグイン導入

監視対象サーバが CentOS の場合 SCP で `/usr/local/groundwork/nagios/libexec/` 下のファイルを、`/home/Nagios/libexec` のコピーして使用できます。

例:

```
scp /usr/local/groundwork/nagios/libexec/* nagios@<XXXXXX>:/home/nagios/libexec
(XXXXXX はサーバ名か IP アドレス)
```

監視対象サーバの Linux ディストリビューションや UNIX 種別を考慮し、適切なプラグイン導入を行なってください。

b) プラグイン実行テスト

aeMonitor サーバの nagios ユーザで ssh プラグインを実行してみる。

例 : `./libexec/check_by_ssh -H <XXXXXX> -t 30 -l Nagios -C "/libexec/check_load -w 5,5,5 -c 15,15,15"`

――> ここで、正常なメッセージが表示されることを確認します。
(内容がエラーでもコマンドが起動されていればかまいません。)

例 : `CRITICAL - load average: 5.24, 4.09, 3.03`

c) トラブルシュート

b)のテストの結果、`ld-linux.so.2` がない旨のエラーが表示された場合、

yum install ld-linux.so.2

で、`ld-linux.so.2` をインストールしてください。