interlook

The *interlook* network monitoring system uses SNMP probes to perform basic health checks against one or more network targets. A simple configuration file is read each time interlook runs; blank lines and comments (the usual: **// ; #**) are ignored, lines which begin with an IP address identify a device to be probed, and lines beginning with a word are treated as options. Arguments are separated by whitespace, and may take the form of simple *words* or *key=value* pairs (in some cases the value is a comma-separated list). Valid arguments vary with target type.

Any target requires at least one argument identifying the target type; supported types are *chassis* (minimal system MIB) *net* (network devices) and *host* (hosts running an appropriate snmpd). If the next argument is a word, this word will be used as the community string when probing the target.

The **chassis** target accepts no additional arguments and probes only the system MIB (description, hostname, uptime, location). It can be used with any device which supports RFC1213. Because no additional information is exposed, this target is suitable for insecure links such as the Internet.

The **net** target will check a list of interfaces whose names match *ifname* or whose types are listed in *iftype*; known types are *ethernet*, *vlan* (a trunked subinterface), *ppp*, and *frame-relay*. An interface is considered to be “up” if the operational state is “up” **or** the administrative state is not “up”. (Interface state will directly track the administrative state if the adminstate flag is given; this option is generally used for testing.)

For the **host** target, the *run* argument configures a list of processes which must be running. The *disk* and *swap* arguments set a “safe” utilization percentage, and the *service* argument invokes one or more service checks. Virtual IP addresses are configured by appending them to the service name with a colon (see example below).

Service checks are defined with the **service** configuration keyword, which is followed by the name of the service. The remainder of the line will be executed as a command-line which is assumed to exit with status 0 if successful; the target IP address will be substituted for the string `%%ip%%`.

The **alert** keyword specifies one or more email addresses (separated by commas) to which messages will be sent when the state of a monitored device changes. (Note that the source of these notification emails is hardcoded into the *interlook* script.)

Dashboard

Install the supplied `index.php` in an appropriate place and modify the first few lines (base URL, location of *interlook* state file) as appropriate. Access controls may be implemented with standard `.htaccess` methods, by adding additional checks for `REMOTE_ADDR` to the beginning of `index.php`, firewall rules, or whatever other mechanism is appropriate for the site.

Host Configuration

Install the *net-snmp* package (and any prerequisites). If desired, edit **/etc/snmp/snmpd.conf** to change the **default** in the first com2sec rule to limit access to the *interlook* server; for example:

```
# default is to allow anything
# com2sec notConfigUser default public
# restrict to the monitor subnet
com2sec notConfigUser 172.29.5.0/24 public
```

(See the `snmpd.conf` manual page for examples of more complex access-control strategies.) Only a handful of OID prefixes are actually used by *interlook*; to limit the system view to these OIDs, replace the default view statements with these:

```
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.2
view    systemview    included   .1.3.6.1.2.1.25
```

Device Configuration

For both ASA and IOS devices, the SNMP “location” and “contact” are set with the snmp-server command:

```
snmp-server location headquarters
snmp-server contact it-staff@example.com
```

IOS devices can use an access-list to restrict access; this is highly recommended for devices which are exposed to the Internet:

```
access-list 51 permit 172.18.91.0 0.0.0.255
snmp-server community public ro 51
```

ASA devices have implicit access restrictions; both the source interface and IP address must match:

```
snmp-server host corp 172.29.5.9 community public
```

Example interlook.conf

A simple configuration which monitors a firewall, router, a few servers, and a remote office:

```
# example
community public
alert 4085551212@vtext.com,it-staff@example.com
# check for webserver
service www wget --timeout=5 -O /dev/null http://%%ip%%/
# check for dns
service dns dig +time=1 +tries=1 +retry=1 +norecurse @%%ip%% google.com a
# the firewall
172.31.1.1 net secret iftype=ethernet,vlan
# the router
172.29.5.1 net ifname=fastethernet,serial
# webservers
172.31.1.27 host run=httpd,mysqld disk=70 swap=20 service=www
172.31.1.31 host run=nginx,mongod,memcached disk=70 swap=20 service=www
172.31.1.44 host run=httpd,oracleXE disk=70 swap=40 service=www:172.31.1.33
# mail/nameservice
172.31.1.82 host run=smtpd,named disk=60 service=dns:172.31.1.11
# remote office
10.185.28.147 chassis
```