

## Xinetd

### 1.1 Brief introduction

Xinetd provides visiting control, improved log function and resource management. It is standard super guardian process of Internet in Asianux 2.0 system.

Inetd is called super server, and it is used to control host network connection. When a request arrives at the port which is managed by Inetd, Inetd will require transmitting it to program called tcpd. tcpd will decide whether to allow service to respond to this request according to configuring file /etc/hosts.allow and /etc/hosts.deny. If the request is allowed, then corresponding server program (such as: telnetd) will be started up. This mechanism is also called tcp\_wrapper.

Xinetd (eXtended InterNET services daemon) provides function which is similar with inetd+tcp\_wrapper, but more powerful and safe. It contains following characteristics:

- Support tcp, udp and RPC service (but currently support to RPC is not stable enough, we can solve this problem by starting up protmap and xinetd).
- Visiting control based on time slice
- Full log function, it can record behavior of failed connection as well as successful connection.
- It can avoid DoS (Denial of Services) attack effectively.
- It can limit the quantity of same type servers that run at one time.
- It can limit the quantity of all started servers.
- It can limit the size of log file.
- It bind some service to especial system interface, so that it can implement that only allow private network to visit some service.
- It can act as proxy of other system. If integrate with IP disguise, it can implement visit of all inner private network.

### 1.2 Configuration of Xinetd

The configuring file of Xinetd is network connection configuring file directory called xinetd.d under directory /etc/xinetd.conf and /etc. Grammar in configuring file is completely different and not compatible with /etc/inetd.conf. It is essentially combination of /etc/inetd.conf, /etc/hosts.allow and /etc/hosts.deny.

The followings are files under directory /etc/xinetd.d:

```
[root@localhost root]# ls /etc/xinetd.d:
```

```
amanda      cups-lpd    finger     ntalk      rsh        swat
amandaidx   daytime    imap       pop3s      rsync      talk
amidxtape   daytime-udp imaps      proftpd    servers    telnet
chargen     echo       ipop2      rexec      services   time
chargenupd  echo-udp   ipop3      rlogin     sgi_fam    time-upd
```

Among them, each file delegates one kind of network server program, file generally have following format:

```
service service-name
{
```

```
.....
.....
}
```

Among it, service is keyword, every item defines service that defined by service-name. For example, the following is content of file /etc/xinetd.d/telnet:

```
[root@localhost xinetd.d]# cat telnet
# default: on
# description: The telnet server serves telnet session; it uses \
#      unencrypted username/password pairs for authentication.
service telnet
{
    flags          = REUSE
    socket_type    = stream
    wait          = no
    user          = root
    server         = /usr/sbin/in.telnetd
    log_on_failure += USERID
    disable       = yes
}
```

Service-name is discretionary, but it usually is standard network service name. It can also increase other non-standard services as long as they can be activated through network request include network requests that sent by localhost itself.

Operator can be =, += or -=. All properties can use =, its function is to distribute one or several values; some properties can use += or -= format, its function is respectively add this value to existed value-table or delete it from existed value-table.

- Useable attribute

### **Socket\_type**

Type of TCP/IP socket that is used, its value may be stream (TCP), dgram (UDP), raw and seqpacket (reliable ordered data packet).

### **protocol**

Appoint protocol used by this service, its value must have already been defined in /etc/protocols. If do not define, it use defaulted protocol of this service.

### **Server**

Process to be activated, it must appoint entire path.

### **Server\_args**

Appoint parameter that to be transmitted to this process, but do not contain service program name.

### **Port**

Define port number that is correlative to this service. If this service has been listed in /etc/services, they must match.

**Wait**

This attribute has two possible values. If it is “yes”, then xinetd will start up new process and stop dealing with request of this service till this process stops. This is a single-thread service. If it’s “no”, then xinetd will start up a process for each request, and dose not care about the state of the foregoing process. This is a multi-thread service.

**User**

Set UID of service process. If the valid UID of xinetd is 0, this attribute is noneffective.

**Group**

Set GID of process. If the valid UID of xinetd is 0, this attribute is noneffective.

**Nice**

Appoint priority of process.

**Id**

This attribute is used to uniquely appoint on service. Because difference between some services just that they use different protocol, so it needs to use this attribute to distinguish. For example, echo supports dgram and streama at one time. Set id=echo\_dgram and id=echo\_streama to respectively and uniquely identify two serices.

Type can be one or several value of follows: RFC (service for RFC), INTERNAL (service provided by xinetd itself, such as: echo), UNLISTED (services that do not list in standard system file such as /etc/rpc or /etc/service).

**Access\_time**

Set time interval when service is usable. Format is hh: mm\_hh: mm; for example 08:00-18:00 means that this service can be used from 8A.M to 6P.M.

**Banner**

No matter whether this connection is allowed, it will display this file to client when setting up connection.

**Flags**

It can be the combination of one or several options below:

<b>REUSE:</b>	Set TCP/IP socket to be re-useable. This is to set SO_REUSEADDR sign in socket of this service. Restart xinetd when interrupting.
<b>INTERCEPT:</b>	Intercept data packet to carry out visiting examination, in order to confirm that it comes from location that allows connecting.
<b>NORETRY:</b>	If fork failed, do not retry.
<b>IDONLY:</b>	Accept this connection only when long-distance port distinguishing long-distance user (this is to say, long-distance system must run ident server), this id only apply to connection-oriented service. If it dose not use USERID to record option, then this id is noneffective. Use log_on_success, /, or log_on_failure properties to set USERID to make this value work. Only used

	in multi-thread stream-service.
<b>NAMEINARGS:</b>	Allow the first parameter in server_args to be the fairly qualified path of process, in order to allow using TCP_Wrappers.
<b>NODELAY:</b>	If service is tcp service, and NODELAY sign is set, then TCP_NODELAY sign will be set. If service is not tcp service then this sign is noneffective.

### **Rpc\_version**

Appoint version number or service number of RPC. Version number can be a single value or among a range.

### **rpc\_number**

If RPC program number is not in /etc/rpc, then appoint it.

### **Env**

VAR=VALUE table separated by space, VAR is a shell environment variable and VALUE is its set value. These value and xinetd environments are activated when transmitted to service program. This attribute support operator = and +=.

### **Passenv**

Environment variable table in xinetd environment that separated by space, this table will transmit it to service program when activated. It will not transmit any variable if set to be “no”. This attribute supports all operators.

### **Only\_from**

Clients table that allowed visiting service and separated by space. Table 2 gives grammar of client. If do not appoint a value for this attribute, it will deny to visit this service. This attribute supports all operators.

### **No\_access**

Accept a integer that bigger than or equal to one or UNLIMITED. Set the maximum quantity of processes that can run at one time. UNLIMITED means xinetd dose not limit this value.

### **Log\_type**

Appoint record mode service log, it can be:

<b>SYSLOG</b> facility[level]:	Set this tool to be daemon, auth, user or local10-7. Set “level” to be optional, and the value of “level” can be emerg, alert, crit, err, warning, notice, info, debug, default is info;
file[soft[hard]]:	Appoint file to be used to record log but syslog. Use KB (optional) to appoint soft and hard limit. As long as it reaches soft limit, xinetd will record a piece of message. As long as it reaches hard limit, xinets will stop recording all services of using this file. If do not appoint hard limit, it is value is soft plus 1%, but it is not more than 20MB when defaulting. The defaulted soft limit is 5MB;

### **Redirect**

The grammar of this attribute is `redirect=Ipaddress port`. It redirect TCP service to another system. If using this attribute, attribute server will be ignored.

### Bind

Bind one service to a especial port. The grammar is `bind=Ipaddress`. This way, the client that has several interfaces (physical or logical) will allow special service on some interface but not other interfaces (or ports).

### Log\_on\_success

Appoint information that logged when success. Possible values are:

<b>ID:</b>	PID of process. If a new process is bifurcated, set PID to be 0.
<b>HOST:</b>	Host IP address of client.
<b>USERID:</b>	Catch user's UID through RFC 1413. It only can be used on multi-thread service.
<b>EXIT:</b>	Log stop and state of process.
<b>DURATION:</b>	Log persisting period of dialog.

Don't log any information when defaulting. This attribute supports all operators.

### Log\_on\_failure

Appoint logging information when failed. Always logs messages that express property of error. Possible value is `ATTEMPT`: record a failure attempt. All other values default to be this value.

<b>ATTEMPT:</b>	Record a failure attempt. All other values default to be this value.
<b>HOST:</b>	Host IP address of client.
<b>USERID:</b>	Catch user's UID through RFC 1413. It only can be used on multi-thread service <b>RECORD:</b> record additional client information such as local user, long-distance user and terminal type. Don't log any information when defaulting. This attribute supports all operators.
<b>RECORD:</b>	Record additional client information such as local user, long-distance user and terminal type. Don't log any information when defaulting. This attribute supports all operators.

### Disabled

It can only be used on "defaults" option (refer to "defaults" option), appoint closed service list, it is separated and can not use service list to express. It has same effect with logging out this service in `/etc/xinetd.conf`.

- Make configuration work

After modifying correlative configuring file of network service program, we can use the following command to restart xinetd guardian process to make configuration work.

```
/etc/rc.d/init.d/xinetd restart
```