Modifications of ypbind Daemon for Network Security

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

About This Document

What follows is an explanation of new options for the ypbind command which is a part of NIS. More specifically, this document will address network security measures taken with the ypsetme command. The information below pertaining to the restrictions on ypset binding requiring using the -ypset or -ypsetme flags applies to all Version 4.1.X releases of AIX and applies to AIX Version 3.2.X releases that have had the PTF for apar IX43595 applied.

About ypbind

The NIS client contacts the NIS server via a mechanism referred to as binding. This process occurs the first time an NIS client needs NIS information or when the NIS server is not responding quickly enough to the requests of the NIS client.

When the NIS client needs to locate or bind to the NIS server, the ypbind daemon will do a network broadcast to locate the server. The first server to respond to the broadcast request of the client will be used for further client requests.

The use of the ypwhich command will check the binding on the NIS client. If a binding request has not yet been made, the act of executing the ypwhich command will have the ypbind daemon search for a NIS server binding. The first invocation of ypwhich (when the NIS client is not bound) will return that the client is not bound. The second invocation will usually return the NIS server that the client just bound to as a result of the first request.

Why ypbind Fails

The binding process will fail if the NIS server on the local network does not respond or if there isn't an NIS server on the local network. This occurs because network broadcasts are not usually transmitted through gateways or routers. Therefore the NIS client will not be able to locate an NIS server with the normal broadcast mechanism. To enable the successful binding of an NIS client, the ypset command is provided.

The ypset Command

The ypset command is used to specify a specific binding that is needed on the NIS client. Generally this is used for the configuration of an NIS client with a router or gateway between it and the NIS server. The syntax of the ypset command is:

/usr/sbin/ypset [-V1 | -V2] [-d domain]
[-h host] server

- The **server** parameter can either be a host name or IP address. The IP address is generally preferred.
- The **-h host** parameter is the name of the client and can allow the binding of this 'host' client to be set from another host. This has represented a potential security problem since the binding could be controlled from an untrusted host on the network.

  Note: On 4.1.x machines, the '-V2' option no longer applies.

ypbind Modification

A modification to the ypbind daemon was made to **disallow** the use of the ypset command. The PTF for APAR ix43595 contains the ypbind daemon with the default behavior modified. Before the application of this PTF, ypset could be used at any time or from any host to set the binding of the NIS client. After this PTF is applied, the ypbind daemon will not accept ypset requests. This default behavior (of not accepting ypset requests) was chosen since it is the most restrictive and thus more secure.

The new syntax for the ypbind daemon is:

```
ypbind [-s -ypset -ypsetme]
```

- The -s parameter defines that the ypbind daemon will use only privileged ports for communication.
- -ypset parameter defines that the ypbind daemon will accept ypset requests from any host (This is the previous less restrictive mode for ypbind).
- -ypsetme parameter defines that the ypbind daemon will only accept ypset requests from the local host. Any ypset commands from other hosts will be

rejected. **This flag will override the** -ypset **parameter if both are specified**.

Therefore, if the ypset command must be used because of the network configuration being used between NIS client and NIS server, the ypbind daemon must be started with the appropriate parameter. If this needs to be done, the preferred parameter to be used is -ypsetme.

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

END OF DOCUMENT (ypbind.ypset.tcp, 4FAX# 4255)