PERFORCE SOFTWARE

Authentication Options in Perforce

Perforce authentication mechanisms unlocked

Presentation for the 2007 Perforce User Conference

By Dan Steele

Perforce USER CONFERENCE 2007

Choices

- Internal Perforce Authentication
  - Supports varying levels of password authentication and tickets.
- P4Auth
  - Allow multiple edge servers to authenticate off a central server.
- Authentication Triggers
  - Allows Perforce to authenticate users via a third party authorization server.

Notes..

- A server can have only one security model
- Passwords passed from the client to server during a login event are always encrypted
- Password length is currently limited to 15 characters regardless of what authentication mechanism you are using.

Notes cont..

- All authentication in Perforce is centred around two commands.
  - Login: Is used to authenticate to a server. Successful authentication generates a ticket.
  - Passwd: This command is used to change your password.

Tickets

- Introduced in 2004.2
- Set expiry through group 'Timeout' option.
- Tickets can be used anywhere a password was before.
- Tickets can be locked to an IP or created globally.

Internal P4 Authentication

- Security level is defined by the security counter (set with p4 counter -f security #)
- Can enforce strong passwords
- Can force the usage of tickets only

Counter level	
0	No enforcement
1	Strong passwords enforced on client versions 2003.2 and later
2	Strong passwords enforced
3	Ticket based authentication enforced. Password based authentication disabled

P4Auth

- Introduced in 2002.2
- Undocumented and officially unsupported.
- See 'p4 help undoc' for documentation.
- Shares protections, groups, users, and passwords with the central server.
- Servers need constant access to the central server. If the network connection is down no commands can be authenticated.

P4Auth implementation

- Pass -a to p4d at startup point to the central server or set P4AUTH=<ip:port> and restart the server.
- Protections table entries that use IPs need to be Prefixed with proxy- for clients connecting through edge servers.
- The user 'remote' account needs to be configured on the central auth servers.

Authentication triggers

- Introduced in 2004.2
- The first time authentication triggers are added to the triggers table the server must be restarted to enable them.
- Enforces security=3 behavior automatically.
- Allows authentication against third party servers such as LDAP and Active Directory.
- Triggers are not interpreted by a shell: 'echo access denied;exit 1' and the like will not work.
- See Technical note 74 for more details.

Authentication trigger implementation

- Entries for auth-check or auth-set are added to the triggers table via the 'p4 triggers' command.
- The triggers are passed the password via standard in and can be passed arguments such as %user%.

A simple trigger example

```
test auth-check auth "/script/checkpass"

#!/usr/bin/perl
##
## Perforce requires messages on stdout
##
open(STDERR, ">&STDOUT") or die "Can't dup stdout";
##
## read the password from <stdin< and truncate the newline
##
chomp (my $password = <STDIN>);
$password =~ s/\r$//;
##
## success
##
if($password eq "secret"){
    exit 0;
}
##
## failure
##
die "You got the password wrong!\n";
```

- Here's an extremely simple trigger example
- Note that the password is read from <stdin>
- Note also in this case the user name is not passed.

About LDAP & AD

- Users are authenticated with a combination of password and DN.
- The DN contains domain and user information.
- To Authenticate against the server the entire DN string must be correct.

Authentication AD servers.

- Triggers available in the public depot and linked from Technical note 74.
- The Microsoft AdsVw.exe is a great tool for working out issues with the users CN.
  - You can find AdsVw in the ADSI development kit from Microsoft.
- New script attempts authentication against sAMAccount name.

How to use AdsVw

- Start AdsVw.exe and:
  - Select ObjectViewer and click on the OK button.
  - Make sure the "Use OpenObject" checkbox is unchecked.
  - Type LDAP: in the "Enter ADs path:" edit box and then click the OK button.
- You should now be able to browse your Ads tree to your users. This will give you the full Adspath (DN).

Help I've locked myself out!

- If you are using internal authentication and you've locked yourself out you'll need to delete db.protect. This will reset all your protections.
- If you are using authentication triggers you have two options.
  - Move the db.triggers file, restart the server, and then move it back. This will preserve your triggers but start the server without authentication triggers enabled.
  - Run 'p4d -xf 18362 echo' on your server. This will reset your trigger to always allow access. You do not need to restart your server.

Tips on protections

- The protections table is read from the bottom up. To prevent yourself from being accidentally locked out by an errant exclusionary mapping always put your super lines at the very bottom of the table.

```
Protections:
    write user dan * //depot/test/...
    write user fred * //...
    admin user P4DTI * //...
    write group dev * //depot/dev/...
    write user * * -//depot/projects/...
    super user dan * //...
    super user trigger * //...
```

Basic tips

- Tickets can be used anywhere that a password could. For instance 'p4 -P <ticket> ...'.
- 'p4 login' will display your ticket rather than add it to the p4tickets file with 'p4 login -p'.

fin.