

**NAME**

pluginviewer - list loadable SASL plugins and their properties

**SYNOPSIS**

**pluginviewer** [-a] [-s] [-c] [-b min=N,max=N] [-e ssf=N,id=ID] [-m MECHS] [-x AUXPROP\_MECH] [-f FLAGS] [-p PATH]

**DESCRIPTION**

*pluginviewer* can be used by a server administrator to troubleshoot SASL installations. The utility can list loadable (properly configured) client and server side plugins, as well as auxprop plugins.

**OPTIONS**

**-a** List auxprop plugins.

**-s** List server authentication (SASL) plugins.

**-c** List client authentication (SASL) plugins.

**-b min=N1,max=N2**

List client authentication (SASL) plugins. Strength of the SASL security layer in bits. min=N1 specifies the minimum strength to use (1 => integrity protection). max=N2 specifies the maximum strength to use. Only SASL mechanisms which support security layer with strength M such that N1 <= M <= N2 will be shown.

**-e ssf=N,id=ID**

Assume that an external security layer (e.g. TLS) with N-bit strength is installed. The ID is the authentication identity used by the external security layer.

**-m MECHS**

Limit listed SASL plugins to the ones included in the MECHS (space separated) list.

**-x AUXPROP\_MECHS**

Limit listed auxprop plugins to the one listed in the AUXPROP\_MECHS (space separated) list.

**-f FLAGS**

Set security flags. FLAGS is a comma separated list of one or more of the following security flags: noplain (SASL mechanism doesn't send password in the clear during authentication), noactive (require protection from active attacks), nodict (require mechanisms which are secure against passive dictionary attacks), forwardsec (require forward secrecy), passcred (require mechanisms that can delegate client credentials), maximum (require all security flags).

**-p PATH**

Specifies a colon-separated search path for plugins.

**SEE ALSO**

rfc4422 - Simple Authentication and Security Layer (SASL)