NAME

monkeysphere−authentication - Monkeysphere authentication admin tool.

SYNOPSIS

monkeysphere−authentication *subcommand* **[***args***]**

DESCRIPTION

Monkeysphere is a framework to leverage the OpenPGP Web of Trust (WoT) for key-based authentication. OpenPGP keys are tracked via GnuPG, and added to the authorized_keys files used by OpenSSH for connection authentication.

monkeysphere−authentication is a Monkeysphere server admin utility for configuring and managing SSH user authentication through the WoT.

SUBCOMMANDS

monkeysphere−authentication takes various subcommands:

update−users [USER]...

Rebuild the monkeysphere-controlled authorized_keys files. For each specified account, the user ID's listed in the account's authorized_user_ids file are processed. For each user ID, gpg will be queried for keys associated with that user ID, optionally querying a keyserver. If an acceptable key is found (see KEY ACCEPTABILITY in monkeysphere(7)), the key is added to the account's monkeysphere-controlled authorized_keys file. If the RAW_AUTHORIZED_KEYS variable is set, then a separate authorized_keys file (usually ˜USER/.ssh/authorized_keys) is appended to the monkeysphere-controlled authorized_keys file. If no accounts are specified, then all accounts on the system are processed. ‘u’ may be used in place of ‘update−users’.

keys−for−user USER

Output to stdout authorized_keys lines for USER. This command behaves exactly like update−users (above), except that the resulting authorized_keys lines are output to stdout, instead of being written to the monkeysphere-controlled authorized_keys file.

refresh−keys

Refresh all keys in the monkeysphere-authentication keyring. If no accounts are specified, then all accounts on the system are processed. ‘r’ may be used in place of ‘refresh−keys’.

add−id−certifier KEYID|FILE

Instruct system to trust user identity certifications made by KEYID. The key ID will be loaded from the keyserver. A file may be loaded instead of pulling the key from the keyserver by specifying the path to the file as the argument, or by specifying ‘−’ to load from stdin. Using the ‘−n’ or ‘−−domain’ option allows you to indicate that you only trust the given KEYID to make identifications within a specific domain (e.g. "trust KEYID to certify user identities within the @example.org domain"). A certifier trust level can be specified with the ‘−t’ or ‘−−trust’ option (possible values are ‘marginal’ and ‘full’ (default is ‘full’)). A certifier trust depth can be specified with the ‘−d’ or ‘−−depth’ option (default is 1). ‘c+’ may be used in place of ‘add−id−certifier’.

remove−id−certifier KEYID

Instruct system to ignore user identity certifications made by KEYID. ‘c−’ may be used in place of ‘remove−id−certifier’.

list−id−certifiers

List key IDs trusted by the system to certify user identities. ‘c’ may be used in place of ‘list−id−certifiers’.

version

Show the monkeysphere version number. ‘v’ may be used in place of ‘version’.

help Output a brief usage summary. ‘h’ or ‘?’ may be used in place of ‘help’.

Other commands:

setup Setup the server in preparation for Monkeysphere user authentication. This command is idempotent and run automatically by the other commands, and should therefore not usually need to be run manually. ‘s’ may be used in place of ‘setup’.

diagnostics
Review the state of the server with respect to authentication. ‘d’ may be used in place of ‘diagnostics’.

gpg−cmd
Execute a gpg command, as the monkeysphere user, on the monkeysphere authentication ‘sphere’ keyring. As of monkeysphere 0.36, this takes its arguments separately, not as a single string. Use this command with caution, as modifying the authentication sphere keyring can affect ssh user authentication.

SETUP USER AUTHENTICATION

If the server will handle user authentication through monkeysphere-generated authorized_keys files, the server must be told which keys will act as identity certifiers. This is done with the **add−id−certifier** command:

```
# monkeysphere−authentication add−id−certifier KEYID
```

where KEYID is the key ID of the server admin, or whoever’s certifications should be acceptable to the system for the purposes of authenticating remote users. You can run this command multiple times to indicate that multiple certifiers are trusted. You may also specify a filename instead of a key ID, as long as the file contains a single OpenPGP public key. Certifiers can be removed with the **remove−id−certifier** command, and listed with the **list−id−certifiers** command.

A remote user will be granted access to a local account based on the appropriately-signed and valid keys associated with user IDs listed in that account’s authorized_user_ids file. By default, the authorized_user_ids file for an account is ˜/.monkeysphere/authorized_user_ids. This can be changed in the monkeysphere−authentication.conf file.

The **update−users** command is used to generate authorized_keys files for a local account based on the user IDs listed in the account’s authorized_user_ids file:

```
# monkeysphere−authentication update−users USER
```

Not specifying USER will cause all accounts on the system to updated. The ssh server can use these monkeysphere-generated authorized_keys files to grant access to user accounts for remote users. In order for sshd to look at the monkeysphere-generated authorized_keys file for user authentication, the AuthorizedKeysFile parameter must be set in the sshd_config to point to the monkeysphere−generated authorized_keys files:

```
AuthorizedKeysFile /var/lib/monkeysphere/authorized_keys/%u
```

It is recommended to add "monkeysphere−authentication update−users" to a system crontab, so that user keys are kept up-to-date, and key revocations and expirations can be processed in a timely manner.

ENVIRONMENT

The following environment variables will override those specified in the config file (defaults in parentheses):

MONKEYSPHERE_MONKEYSPHERE_USER
User to control authentication keychain. (monkeysphere)

MONKEYSPHERE_LOG_LEVEL
Set the log level. Can be SILENT, ERROR, INFO, VERBOSE, DEBUG, in increasing order of verbosity. (INFO)

MONKEYSPHERE_KEYSERVER
OpenPGP keyserver to use. (pool.sks−keyservers.net)

MONKEYSPHERE_CHECK_KEYSERVER
Whether or not to check the keyserver when making gpg queries. (true)

MONKEYSPHERE_AUTHORIZED_USER_IDS
Path to user's authorized_user_ids file. %h gets replaced with the user's homedir, %u with the username. (%h/.monkeysphere/authorized_user_ids)

MONKEYSPHERE_RAW_AUTHORIZED_KEYS
Path to regular ssh-style authorized_keys file to append to monkeysphere-generated authorized_keys. 'none' means not to add any raw authorized_keys file. %h gets replaced with the user's homedir, %u with the username. (%h/.ssh/authorized_keys)

MONKEYSPHERE_PROMPT
If set to 'false', never prompt the user for confirmation. (true)

MONKEYSPHERE_STRICT_MODES
If set to 'false', ignore too-loose permissions on known_hosts, authorized_keys, and authorized_user_ids files. NOTE: setting this to false may expose users to abuse by other users on the system. (true)

FILES

/etc/monkeysphere/monkeysphere−authentication.conf
System monkeysphere-authentication config file.

/etc/monkeysphere/monkeysphere−authentication−x509−anchors.crt or /etc/monkeysphere/monkeysphere−x509−anchors.crt
If monkeysphere-authentication is configured to query an hkps keyserver, it will use the PEM-encoded X.509 Certificate Authority certificates in this file to validate any X.509 certificates used by the keyserver. If the monkeysphere-authentication-x509 file is present, the monkeysphere-x509 file will be ignored.

/var/lib/monkeysphere/authorized_keys/USER
Monkeysphere-controlled user authorized_keys files.

˜/.monkeysphere/authorized_user_ids
A list of OpenPGP user IDs, one per line. OpenPGP keys with an exactly-matching User ID (calculated valid by the designated identity certifiers), will have any valid authorization-capable keys or subkeys added to the given user's authorized_keys file. Any line with initial whitespace will be interpreted as ssh authorized_keys options applicable to the preceding User ID.

AUTHOR

This man page was written by: Jameson Rollins <jrollins@finestructure.net>, Daniel Kahn Gillmor <dkg@fifthhorseman.net>, Matthew Goins <mjgoins@openflows.com>

SEE ALSO

monkeysphere(1), **monkeysphere−host**(8), **monkeysphere**(7), **gpg**(1), **ssh**(1), **sshd**(8), **sshd_config**(5)