Rocky Enterprise Linux 9.2 Manual Pages on command 'sss_ssh_authorizedkeys.1'

$ man sss_ssh_authorizedkeys.1

SSS_SSH_AUTHORIZEDKE(1) SSSD Manual pages SSS_SSH_AUTHORIZEDKE(1)

NAME

sss_ssh_authorizedkeys - get OpenSSH authorized keys

SYNOPSIS

sss_ssh_authorizedkeys [options] USER

DESCRIPTION

sss_ssh_authorizedkeys acquires SSH public keys for user USER and

outputs them in OpenSSH authorized_keys format (see the

?AUTHORIZED_KEYS FILE FORMAT? section of sshd(8) for more information).

sshd(8) can be configured to use sss_ssh_authorizedkeys for public key

user authentication if it is compiled with support for

?AuthorizedKeysCommand? option. Please refer to the sshd_config(5) man

page for more details about this option.

If ?AuthorizedKeysCommand? is supported, sshd(8) can be configured to

use it by putting the following directives in sshd_config(5):

AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys

AuthorizedKeysCommandUser nobody

KEYS FROM CERTIFICATES

In addition to the public SSH keys for user USER sss_ssh_authorizedkeys can return public SSH keys derived from the public key of a X.509 certificate as well.

To enable this the ?ssh_use_certificate_keys? option must be set to true (default) in the [ssh] section of sssd.conf. If the user entry contains certificates (see ?ldap_user_certificate? in sssd-ldap(5) for details) or there is a certificate in an override entry for the user (see sss_override(8) or sssd-ipa(5) for details) and the certificate is valid SSSD will extract the public key from the certificate and convert it into the format expected by sshd.

Besides ?ssh_use_certificate_keys? the options

? ca_db

? p11_child_timeout

? certificate_verification

can be used to control how the certificates are validated (see sssd.conf(5) for details).

The validation is the benefit of using X.509 certificates instead of SSH keys directly because e.g. it gives a better control of the lifetime of the keys. When the ssh client is configured to use the private keys from a Smartcard with the help of a PKCS#11 shared library (see ssh(1) for details) it might be irritating that authentication is still working even if the related X.509 certificate on the Smartcard is already expired because neither ssh nor sshd will look at the certificate at all.

It has to be noted that the derived public SSH key can still be added to the authorized_keys file of the user to bypass the certificate validation if the sshd configuration permits this.

OPTIONS

-d,--domain DOMAIN

Search for user public keys in SSSD domain DOMAIN.

-?,--help

Display help message and exit.

EXIT STATUS

In case of success, an exit value of 0 is returned. Otherwise, 1 is returned.

SEE ALSO

sssd(8), sssd.conf(5), sssd-ldap(5), sssd-ldap-attributes(5), sssd-krb5(5), sssd-simple(5), sssd-ipa(5), sssd-ad(5), sssd-files(5), sssd-sudo(5), sssd-session-recording(5), sss_cache(8), sss_debuglevel(8), sss_obfuscate(8), sss_seed(8), sssd_krb5_locator_plugin(8), sss_ssh_authorizedkeys(8), sss_ssh_knownhostsproxy(8), sssd-ifp(5), pam_sss(8). sss_rpcidmapd(5) sssd-systemtap(5)

AUTHORS

The SSSD upstream - https://github.com/SSSD/sssd/