How to add sudo rule for local user in IPA server and retrieve on IPA client

SOLUTION VERIFIED - Updated June 3 2016 at 5:33 AM - English ()

Environment

- Red Hat Enterprise Linux 7
- IPA server (as a source of sudorules)
- IPA client (having local users)

Issue

- How do I add sudo-rule in IPA for user locally present on IPA client ?
- How do I retrieve sudo-rule for local users on IPA client defined in IPA server ?

Resolution

- For this to get work, configure a proxy domain in sssd.conf. IPA domain will be the same as per existing setup, the proxy domain will provide sudo information for local users. To create a rule in IPA that will apply local users, set external user in the cli/webUI which is a plain text.
  This setup works, but it is still recommended to use /etc/sudoers for local users.

On IPA Server:

1. Create a sudo-rule for local user(external user) via **WebUI** or **CLI**:

2. Sudorule will appear as:

```
# ipa sudorule-find
-------------------
1 Sudo Rule matched
-------------------
  Rule name: testrule
  Enabled: TRUE
  Command category: all
  RunAs User category: all
  RunAs Group category: all
  Users: ipauser
  External User: localuser    <---------------
  Hosts: rhel7-ipa-2.example.com
----------------------------
Number of entries returned 1
----------------------------
```

On IPA Client:

1. Configure `sssd.conf` as shown below:

```
[domain/example.com]   <------ IPA domain

cache_credentials = True
krb5_store_password_if_offline = True
ipa_domain = example.com
id_provider = ipa
auth_provider = ipa
access_provider = ipa
ipa_hostname = rhel7-ipa-2.example.com
chpass_provider = ipa
ipa_server = rhel7-ipa-2.example.com
ipa_server_mode = True
ldap_tls_cacert = /etc/ipa/ca.crt
ldap_sudo_search_base = ou=sudoers,dc=example,dc=com

[domain/proxy]   <----------------------- Define this section(proxy domain)
id_provider = proxy
proxy_lib_name = files
proxy_pam_target = system-auth-ac
sudo_provider = ldap   <----------------- This could be 'ipa' as well
ldap_uri = ldaps://rhel7-ipa-2.example.com
ldap_sudo_search_base = ou=sudoers,dc=example,dc=com
ldap_tls_cacert = /etc/ipa/ca.crt

[sssd]
services = nss, sudo, pam, ssh
config_file_version = 2
domains = example.com, proxy <------- Add a 'proxy' domain here

[nss]
homedir_substring = /home

[pam]

[sudo]

[autofs]

[ssh]

[pac]

[ifp]
```

2. Configure `nsswitch.conf` to have following entries for `sudoers` :

```
# grep  /etc/nsswitch.conf
sudoers: files sss
```

3. User information will appear as:

```
# getent passwd localuser
localuser:x:1002:1002::/home/localuser:/bin/bash

# getent passwd ipauser
ipauser:*:659600005:659600005:ipa user:/home/ipauser:/bin/sh

# id localuser
uid=1002(localuser) gid=1002(localuser) groups=1002(localuser)

# id ipauser
uid=659600005(ipauser) gid=659600005(ipauser) groups=659600005(ipauser)
```

4. Test the configuration:

```
# sudo -l -U ipauser
Matching Defaults entries for ipauser on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY
HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME
LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
    LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User ipauser may run the following commands on this host:
    (ALL : ALL) ALL

# sudo -l -U localuser
Matching Defaults entries for localuser on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY
HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME
LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
    LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User localuser may run the following commands on this host:
    (ALL : ALL) ALL

# su - localuser
Last login: Wed May 25 19:44:22 IST 2016 on pts/1
[localuser@rhel7-ipa-2 ~]$ sudo -l
Matching Defaults entries for localuser on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY
HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME
LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
    LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User localuser may run the following commands on this host:
    (ALL : ALL) ALL

$ sudo service sssd restart
Redirecting to /bin/systemctl restart  sssd.service

$ echo $?
0             <------------ Successful
```

Product(s) Red Hat Identity Management (/taxonomy/products/red-hat-identity-management)

Red Hat Enterprise Linux (/taxonomy/products/red-hat-enterprise-linux)

Component ipa-client (/components/ipa-client) sudo (/components/sudo)

Category Configure (/category/configure) **Tags** ipa (/tags/ipa)

This solution is part of Red Hat's fast-track publication program, providing a huge library of solutions that Red Hat engineers have created while supporting our customers. To give you the knowledge you need the instant it becomes available, these articles may be presented in a raw and unedited form.

Comments