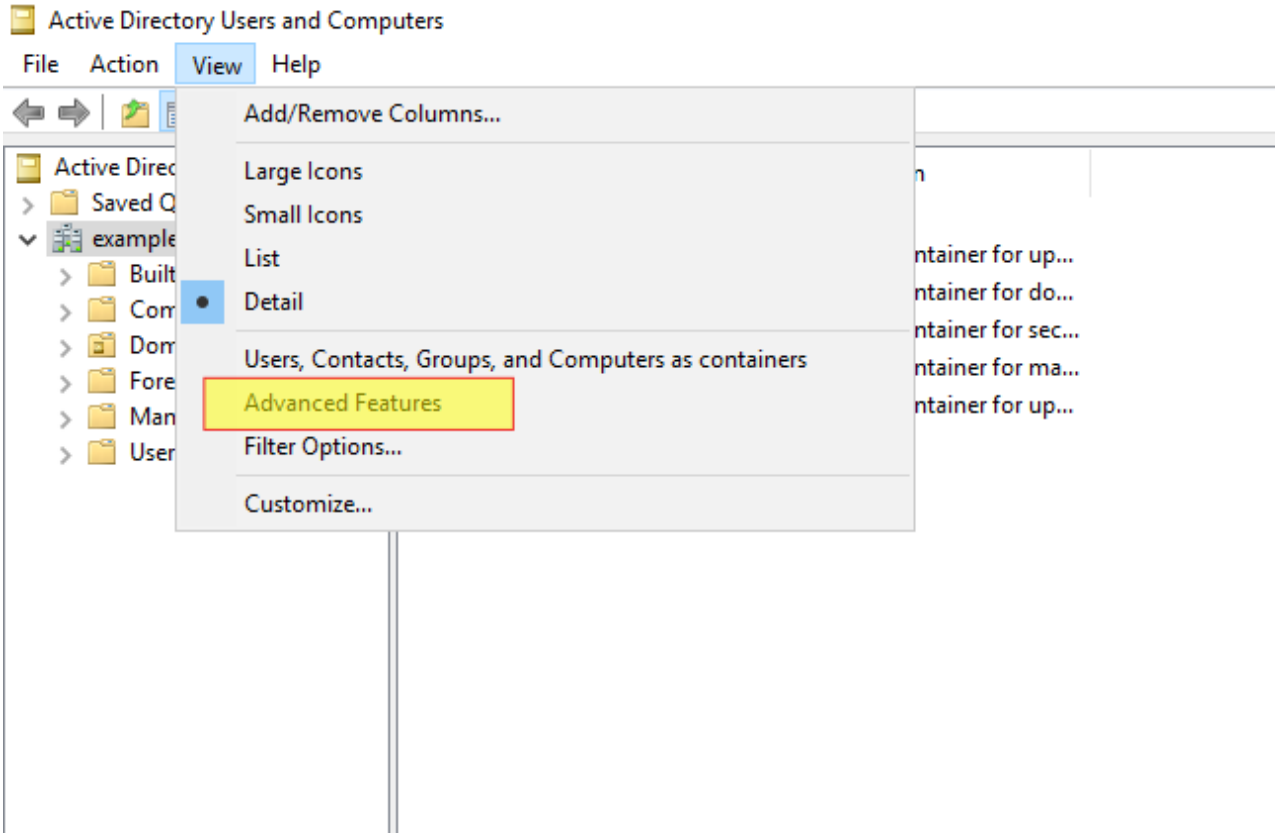
Store User SSH Keys in Active Directory for SSH Authentication

access.redhat.com/solutions/5353351

12 июня 2025 г.



-
- 38

Solution Verified - Updated June 12 2025 at 11:48 AM -
English

Environment

- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- Red Hat Enterprise Linux 10
- System Security Services Daemon (SSSD)
- OpenSSH

Issue

- Active Directory (AD) users want to login via SSH using ssh keys

- SSH public keys are to be stored centrally in AD
- SSSD joins AD directly [1], or IdM client enrolled into IdM domain with AD trust[2]

1. Integrating RHEL systems directly with Windows Active Directory: Connecting directly to AD ↩

2. Managing a cross-forest trust between an IdM and AD domain ↩

Resolution

First, store ssh key in `altSecurityIdentities` attribute. Then, configure SSSD to fetch the attribute of the user, and instruct OpenSSH to look up the user's public key with `sss_ssh_authorizedkeys` command.

1. Active Directory Server

2. SSSD

2.a. SSSD joins AD directly

1. Append `ssh` to `services` parameter in */etc/sssd/sssd.conf*

   Raw

   ```
   services = nss, pam, ssh
   ```

2. Add `ldap_user_extra_attrs` and `ldap_user_ssh_public_key` parameters to `[domain]` section of */etc/sssd/sssd.conf*

   Raw

   ```
   [domain/ad.example.com]
   ldap_user_extra_attrs = altSecurityIdentities
   ldap_user_ssh_public_key = altSecurityIdentities
   ```

3. Clear `sssd` cache and restart

   Raw

   ```
   # systemctl stop sssd; rm -rf /var/lib/sss/{db,mc}/*; systemctl start sssd
   ```

2.b. IdM client enrolled into IdM domain with AD trust

1. Add `ldap_user_extra_attrs` and `ldap_user_ssh_public_key` parameters to AD sub-domain `[domain]` section of */etc/sssd/sssd.conf*, on all IdM servers.

   Raw

   ```
   [domain/idm.example.com/ad.example.com]
   ldap_user_extra_attrs = altSecurityIdentities
   ldap_user_ssh_public_key = altSecurityIdentities
   ```

2. Clear `sssd` cache and restart

   Raw

   ```
   # systemctl stop sssd; rm -rf /var/lib/sss/{db,mc}/*; systemctl start sssd
   ```

3. As of SSSD 2.9, below warning message would appear in `/var/log/sssd/sssd.log`. These messages can safely be ignored. This logging bug is being tracked in RHEL-19186.

   Raw

   ```
   [rule/allowed_subdomain_options]: Attribute 'ldap_user_extra_attrs' is not
   allowed in section 'domain/idm.example.com/example.com'. Check for typos.
   [rule/allowed_subdomain_options]: Attribute 'ldap_user_ssh_public_key' is
   not allowed in section 'domain/idm.example.com/example.com'. Check for
   typos.
   ```

3. OpenSSH

1. Add below SSH parameters to */etc/ssh/sshd_config*

   Raw

   ```
   AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys
   AuthorizedKeysCommandUser nobody
   ```

2. Restart `sshd`

   Raw

   ```
   # systemctl restart sshd
   ```

Root Cause

AD user via IdM/AD trust can store SSH keys in IdM by overriding Default Trust View attributes.

Diagnostic Steps

`sss_ssh_authorizedkeys` shows authorized_keys of a user:

Raw

```
# sss_ssh_authorizedkeys bob@ad.example.com
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDU3PmPi... bob@ad.example.com
```

Product(s)

Red Hat Enterprise Linux

Component

openssh

sssd

Category

Configure

Tags

active_directory

ssh

sssd

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.

People who viewed this solution also viewed

Loading

SSH key authentication is not working
Solution -
6 авг. 2024 г.2024-08-06T06:30:47Z

SSH Public Key Authentication
Discussion -
6 янв. 2022 г.2022-01-06T07:36:04Z

Ideas on how to prevent locked active directory users from login with ssh key
Discussion -
15 дек. 2016 г.2016-12-15T14:54:26Z