AD Trust for Legacy Clients

Since you're too lazy to upgrade them

Tomas Babej

2014-02-17

What?

What is an Legacy Client?

- A client machine, that does not have a recent (>= 1.9) version of SSSD installed
  - Uses other tools to talk to FreeIPA server as to LDAP server,

    such as:
    - *nss-ldap*
    - *nss-pam-ldapd*
    - *SSSD < 1.9*
  - The only requirement for the client is that it uses LDAP protocol to communicate with the FreeIPA server.
  - Legacy client can be easily configured manually, or using output script from ipa-advise tool.

AD Trust for Legacy Clients Feature

- Creates a way how to provide AD user / group information and authentication to the legacy clients
- Does not provide HBAC capabilities for the legacy clients (not even for ones running SSSD < 1.9)

How to make it work?

(high level overview)

it = AD Trust for Legacy Clients Feature

Setup overview - server

- We need FreeIPA and its trust add-on

  ```
  # yum install ipa-server ipa-server-trust-ad
  ```

- We need to have a working FreeIPA server

  ```
  # ipa-server-install ...
  ```

- We need to install the AD Trust support

  ```
  # ipa-adtrust-install –enable-compat ...
  ```

- We need to establish the trust

  ```
  # ipa trust-add ad.example.org
  ```

Setup overview - client

- We need to configure the client to look up users / groups in a special part of the tree.
- The *ipa-advise* tool can help administrators to configure legacy clients to access user / group information from AD.

ipa-advise tool

- Generic tool that generates specific advice
- Runs on FreeIPA server only
- Leverages information it can get from the FreeIPA server
- Pluggable, each advice is a generated by a plugin

```
 # ipa-advise

----------------------------------------------------------------------
List of available advices
----------------------------------------------------------------------
    config-fedora-authconfig             : Authconfig instructions for
                                           configuring Fedora 18/19 client with
                                           IPA server without use of SSSD.
    config-freebsd-nss-pam-ldapd         : Instructions for configuring a
                                           FreeBSD system with nss-pam-ldapd.
    config-generic-linux-nss-pam-ldapd   : Instructions for configuring a system
                                           with nss-pam-ldapd. This set of
                                           instructions is targeted for linux
                                           systems that do not include the
                                           authconfig utility.
  ....
```

What advice is available?

- config-fedora-authconfig
- config-freebsd-nss-pam-ldapd
- config-generic-linux-nss-pam-ldapd
- config-generic-linux-sssd-before-1-9
- config-redhat-nss-ldap
- config-redhat-nss-pam-ldapd
- config-redhat-sssd-before-1-9

Setup overview - client

- Plugins that generate configuration advice for legacy clients output bash scripts
- Advice was designed to be copy&pasted into the client terminal session – that is *everything* you need to do to *configure the client*
- Always proof-read the script that was generated!

```
 $ ipa-advise config-redhat-nss-pam-ldapd
#!/bin/sh
# -----------------------------------------------------------------------
# Instructions for configuring a system with nss-pam-ldapd as a FreeIPA
# client. This set of instructions is targeted for platforms that
# include the authconfig utility, which are all Red Hat based platforms.
# -----------------------------------------------------------------------
# Install required packages via yum
yum install -y wget openssl nss-pam-ldapd pam_ldap authconfig


...
```

Setup overview – example of generated advice

```
$ ipa-advise config-redhat-nss-pam-ldapd
#!/bin/sh
# ----------------------------------------------------------------------
# Instructions for configuring a system with nss-pam-ldapd as a FreeIPA
# client. This set of instructions is targeted for platforms that
# include the authconfig utility, which are all Red Hat based platforms.
# ----------------------------------------------------------------------
# Schema Compatibility plugin has not been configured on this server. To
# configure it, run "ipa-adtrust-install --enable-compat"
# Install required packages via yum
yum install -y wget openssl nss-pam-ldapd pam_ldap authconfig

# NOTE: IPA certificate uses the SHA-256 hash function. SHA-256 was
# introduced in RHEL5.2. Therefore, clients older than RHEL5.2 will not
# be able to interoperate with IPA server 3.x.
# Please note that this script assumes /etc/openldap/cacerts as the
# default CA certificate location. If this value is different on your
# system the script needs to be modified accordingly.
# Download the CA certificate of the IPA server
mkdir -p -m 755 /etc/openldap/cacerts
wget http://ipa.example.com/ipa/config/ca.crt -O /etc/openldap/cacerts/ipa.crt

...
```

Setup overview – example of generated advice

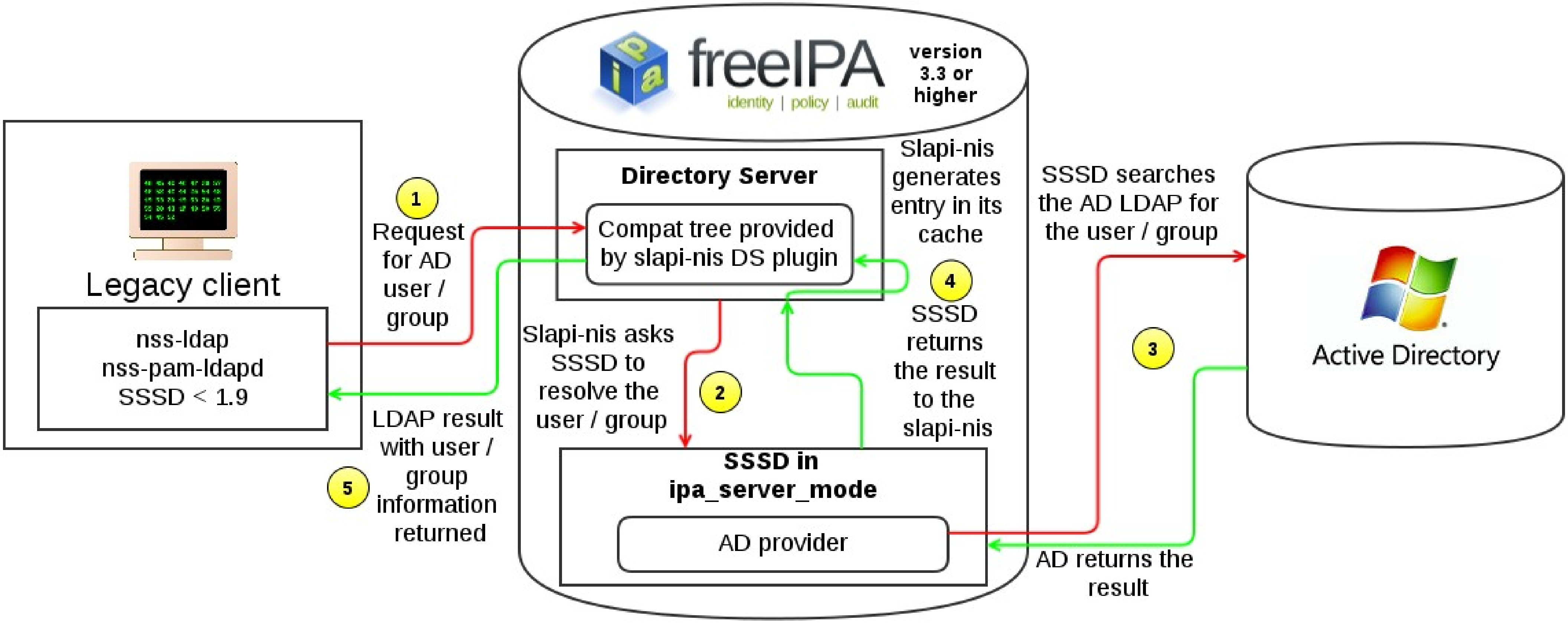
```
# Generate hashes for the openldap library
command -v cacertdir_rehash
if [ $? -ne 0 ] ; then
 wget "https://fedorahosted.org/authconfig/browser/cacertdir_rehash?format=txt" -O cacertdir_rehash ;
 chmod 755 ./cacertdir_rehash ;
 ./cacertdir_rehash /etc/openldap/cacerts/ ;
else
 cacertdir_rehash /etc/openldap/cacerts/ ;
fi

# Use the authconfig to configure nsswitch.conf and the PAM stack
authconfig --updateall --enableldap –enableldapauth --ldapserver=ldap://ipa.example.com
--ldapbasedn=cn=compat,dc=ipa,dc=example,dc=com
```

How does it work?

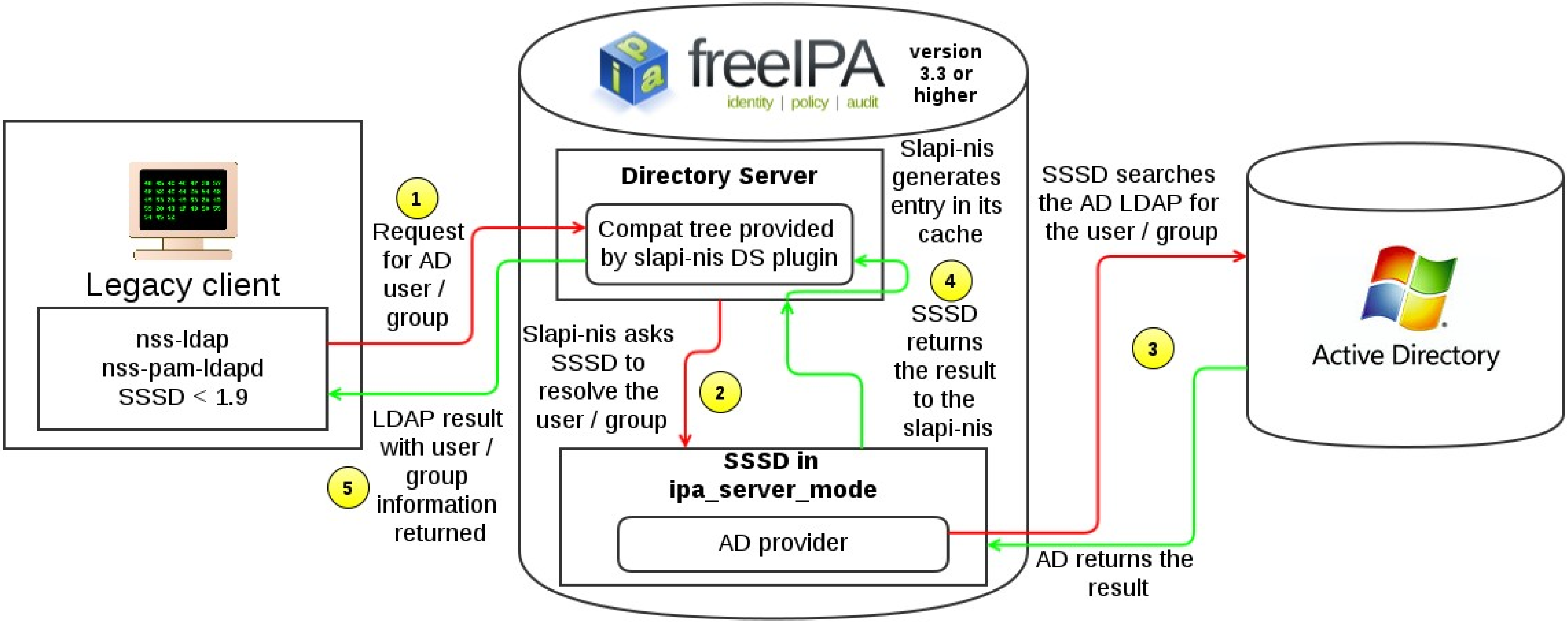
(information lookup)

AD User / group information look-up on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
1
Request for AD user / group
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis generates entry in its cache
SSSD searches the AD LDAP for the user / group
4
SSSD returns the result to the slapi-nis
Slapi-nis asks SSSD to resolve the user / group
2
3
Active Directory
LDAP result with user / group information returned
5
SSSD in ipa_server_mode
AD provider
AD returns the result

1. Legacy client is configured to look-up users and groups in a special part of the LDAP tree, called the compat tree, which is provided by the *slapi-nis* DS plugin

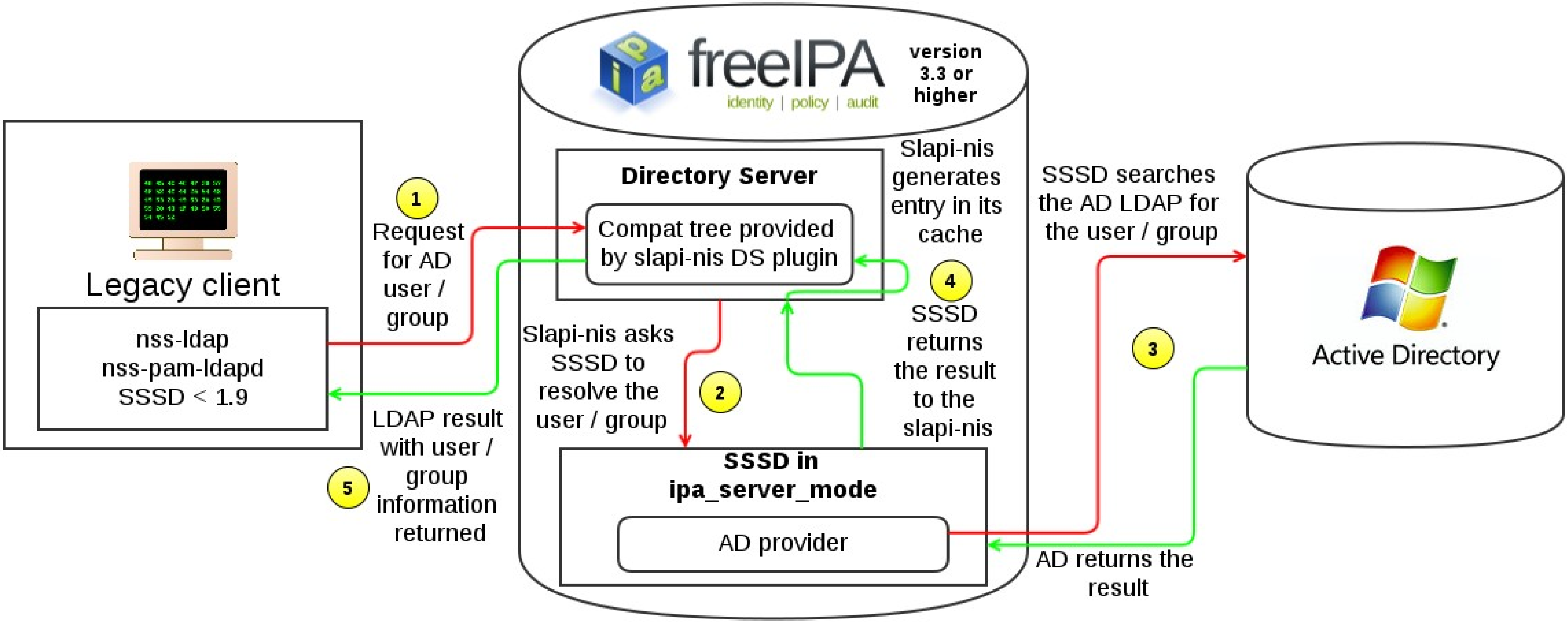
AD User / group information look-up on legacy clients



freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
1
Request for AD user / group
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis generates entry in its cache
SSSD searches the AD LDAP for the user / group
4
SSSD returns the result to the slapi-nis
3
Active Directory
Slapi-nis asks SSSD to resolve the user / group
2
LDAP result with user / group information returned
5
SSSD in ipa_server_mode
AD provider
AD returns the result

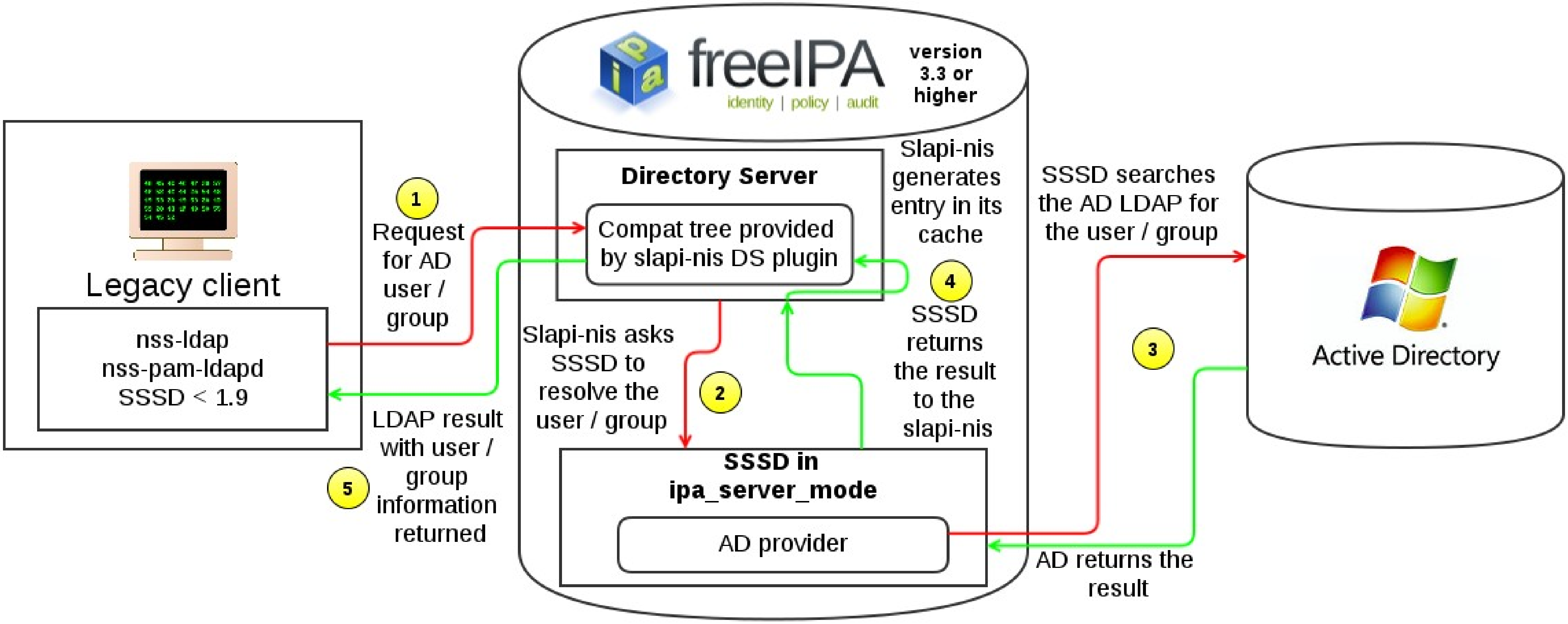
2.The *slapi-nis* DS plugin asks SSSD (being the default in NSSWITCH) running on the server to resolve the user / group. SSSD uses trust information stored in FreeIPA to configure an AD provider internally.

AD User / group information look-up on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
1
Request for AD user / group
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis generates entry in its cache
SSSD searches the AD LDAP for the user / group
4
SSSD returns the result to the slapi-nis
3
Active Directory
Slapi-nis asks SSSD to resolve the user / group
2
LDAP result with user / group information returned
5
SSSD in ipa_server_mode
AD provider
AD returns the result

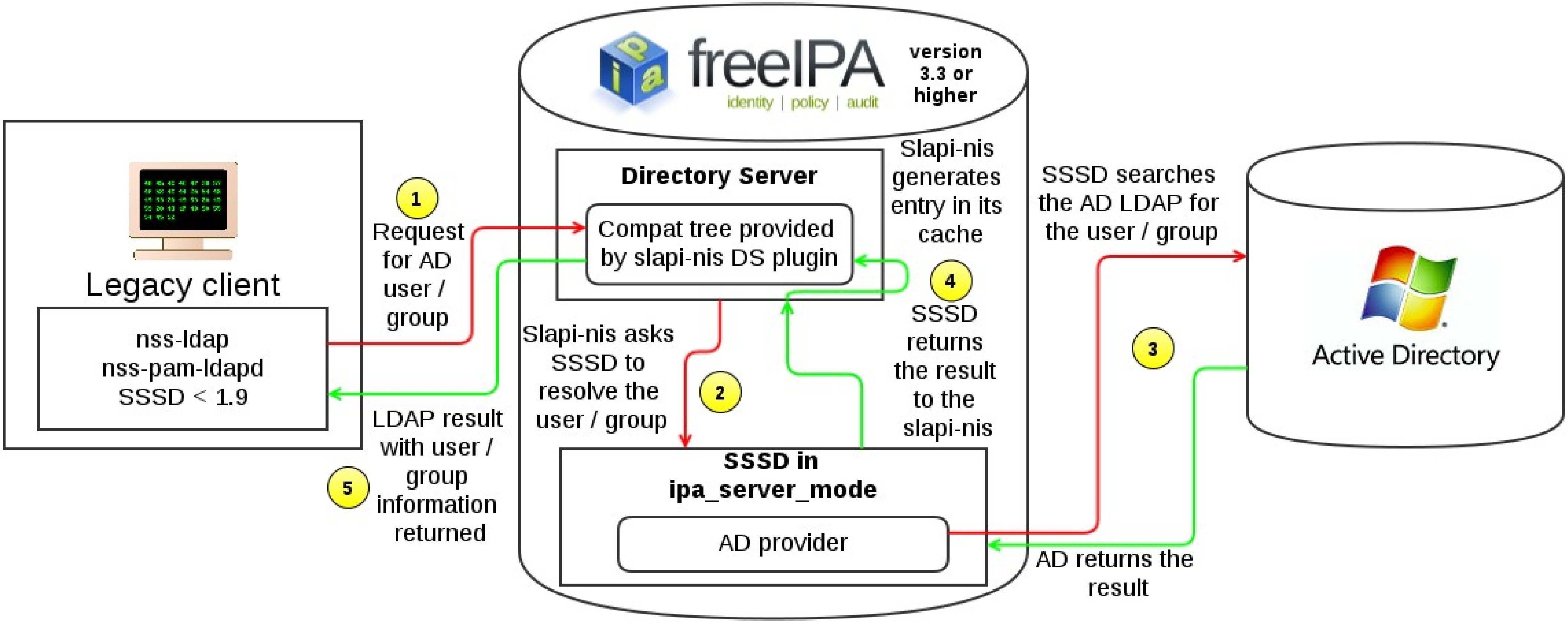
3. SSSD's AD provider searches the Active Directory's LDAP for user / group entry belonging to the user / group requested.

AD User / group information look-up on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
1
Request for AD user / group
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis generates entry in its cache
SSSD searches the AD LDAP for the user / group
4
SSSD returns the result to the slapi-nis
3
Active Directory
2
Slapi-nis asks SSSD to resolve the user / group
LDAP result with user / group information returned
5
SSSD in ipa_server_mode
AD provider
AD returns the result

4. If the SSSD resolved the user / group, slapi-nis will generate an user / group entry in its **cache** (not in actual LDAP tree) based on the result from SSSD.

AD User / group information look-up on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
1
Request for AD user / group
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis generates entry in its cache
4
SSSD returns the result to the slapi-nis
Slapi-nis asks SSSD to resolve the user / group
2
SSSD in ipa_server_mode
AD provider
SSSD searches the AD LDAP for the user / group
3
Active Directory
AD returns the result
5
LDAP result with user / group information returned

5. An LDAP result for the search is returned. If the entry was generated, to the legacy client it seems as though it has been there already.

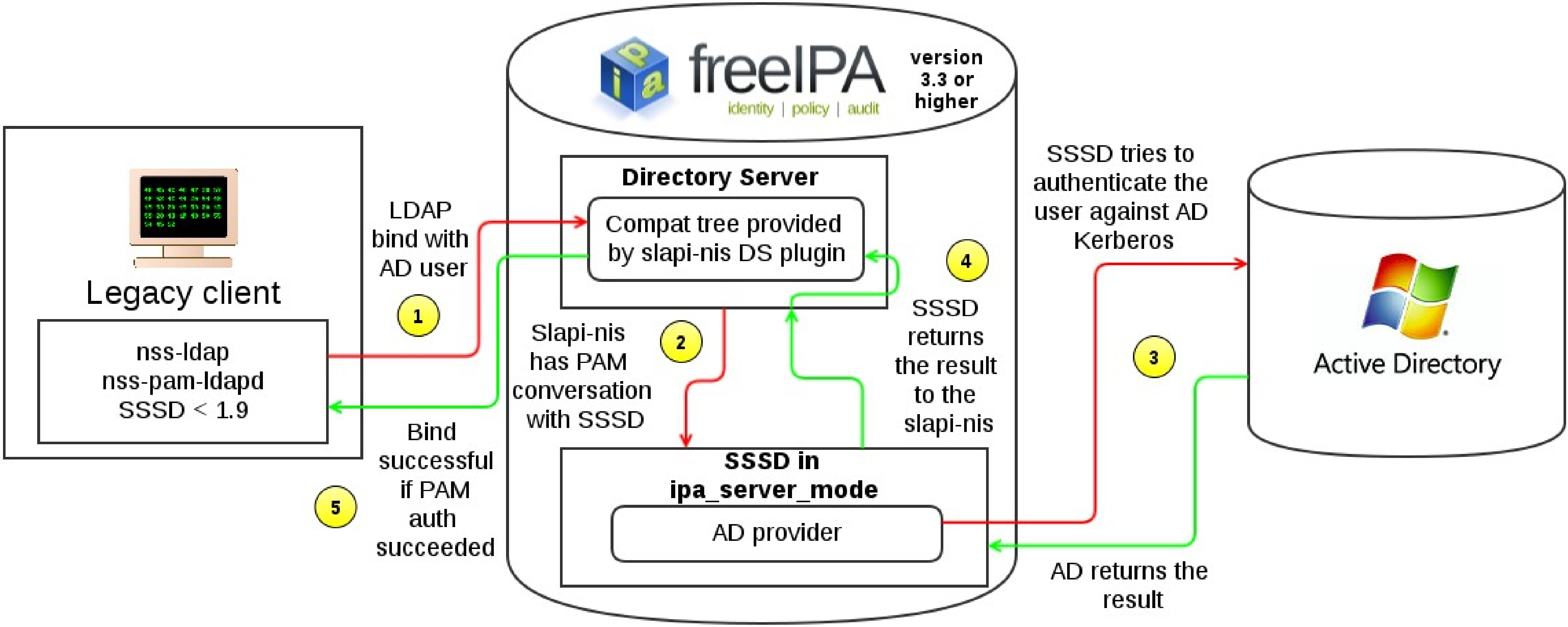
SSSD in ipa_server_mode

- Serves as a replacement for winbind
  - SSSD uses its AD provider to lookup user/group information on the AD
- How it is configured?
  - SSSD running on the server obtains information about the trusted domains from the FreeIPA
  - Then appropriate AD providers (one for each trusted domain) are created within SSSD automatically when a new trust is added

How does it work?

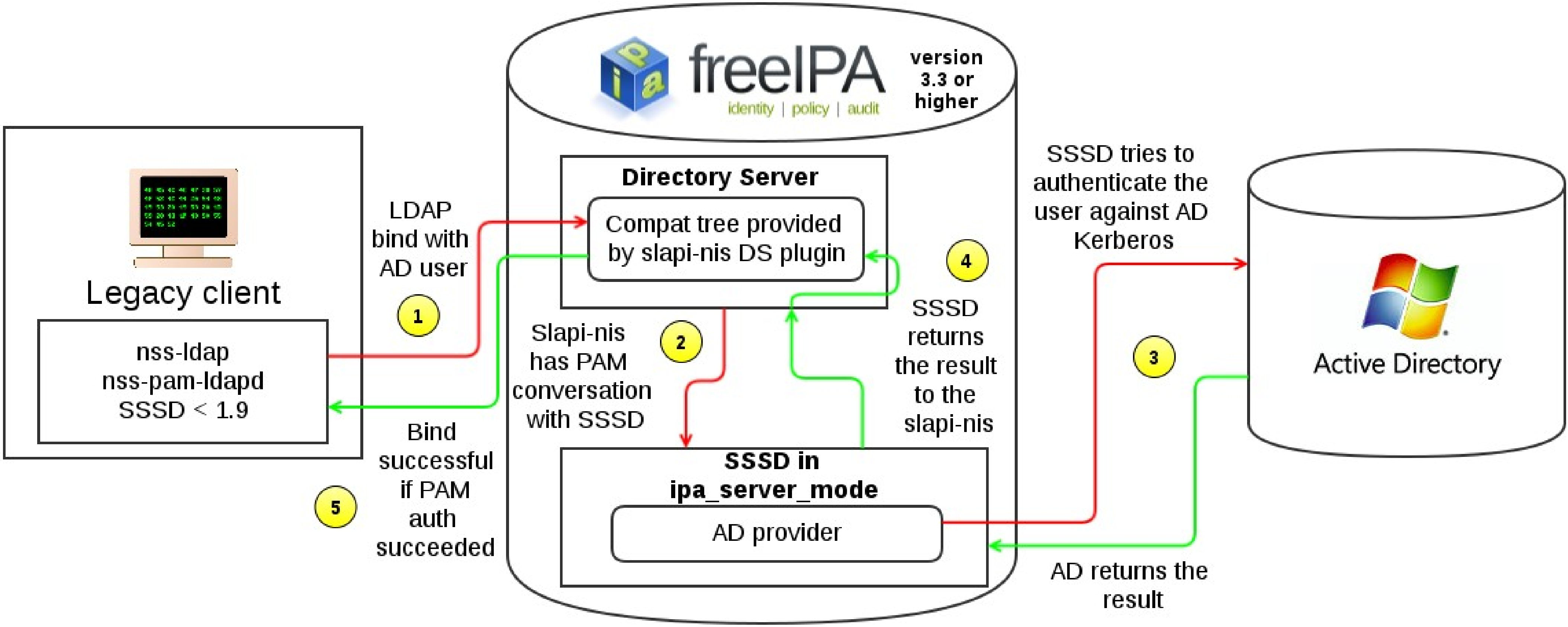
(user authentication)

AD User / group authentication on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Directory Server
Compat tree provided by slapi-nis DS plugin
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
LDAP bind with AD user
1
Slapi-nis has PAM conversation with SSSD
2
SSSD tries to authenticate the user against AD Kerberos
3
4
SSSD returns the result to the slapi-nis
Bind successful if PAM auth succeeded
5
SSSD in ipa_server_mode
AD provider
Active Directory
AD returns the result

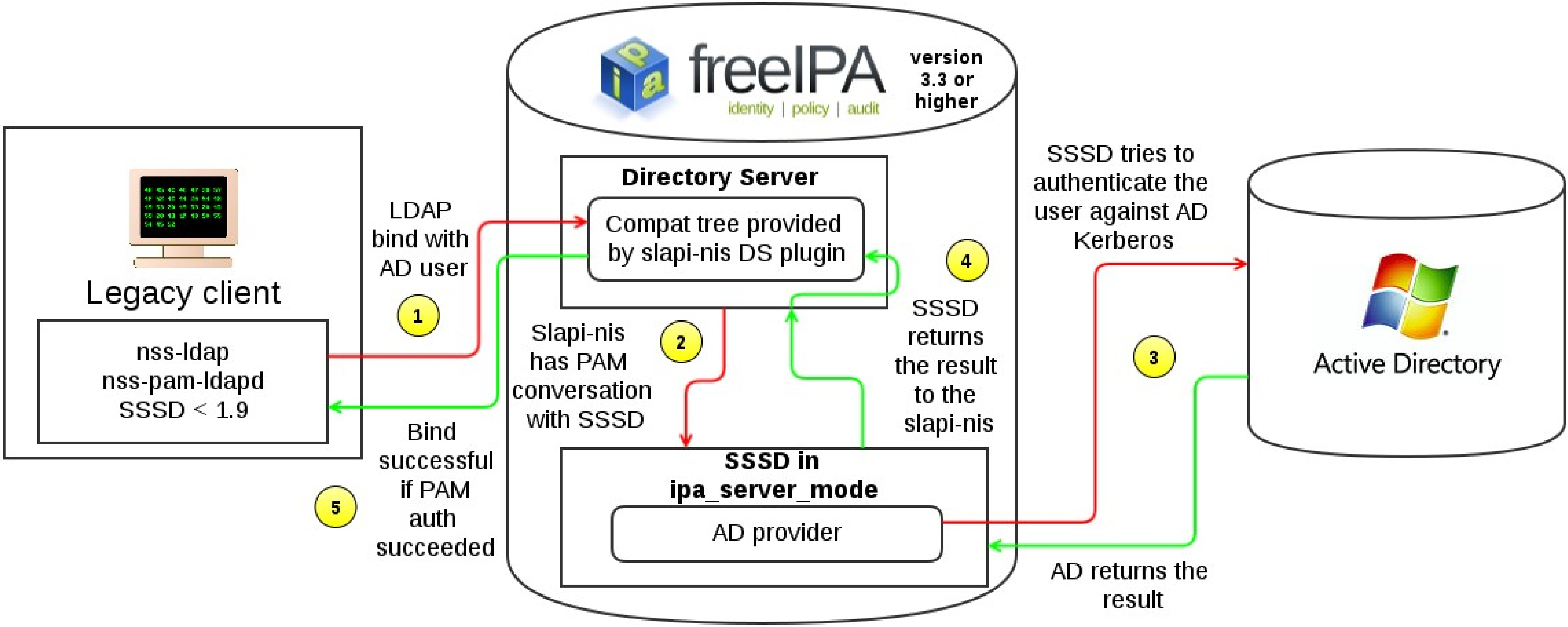
1. To authenticate the AD user against LDAP, legacy client performs LDAP bind against the compat tree.

AD User / group authentication on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
LDAP bind with AD user
1
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis has PAM conversation with SSSD
2
SSSD in ipa_server_mode
AD provider
SSSD tries to authenticate the user against AD Kerberos
3
Active Directory
AD returns the result
4
SSSD returns the result to the slapi-nis
5
Bind successful if PAM auth succeeded

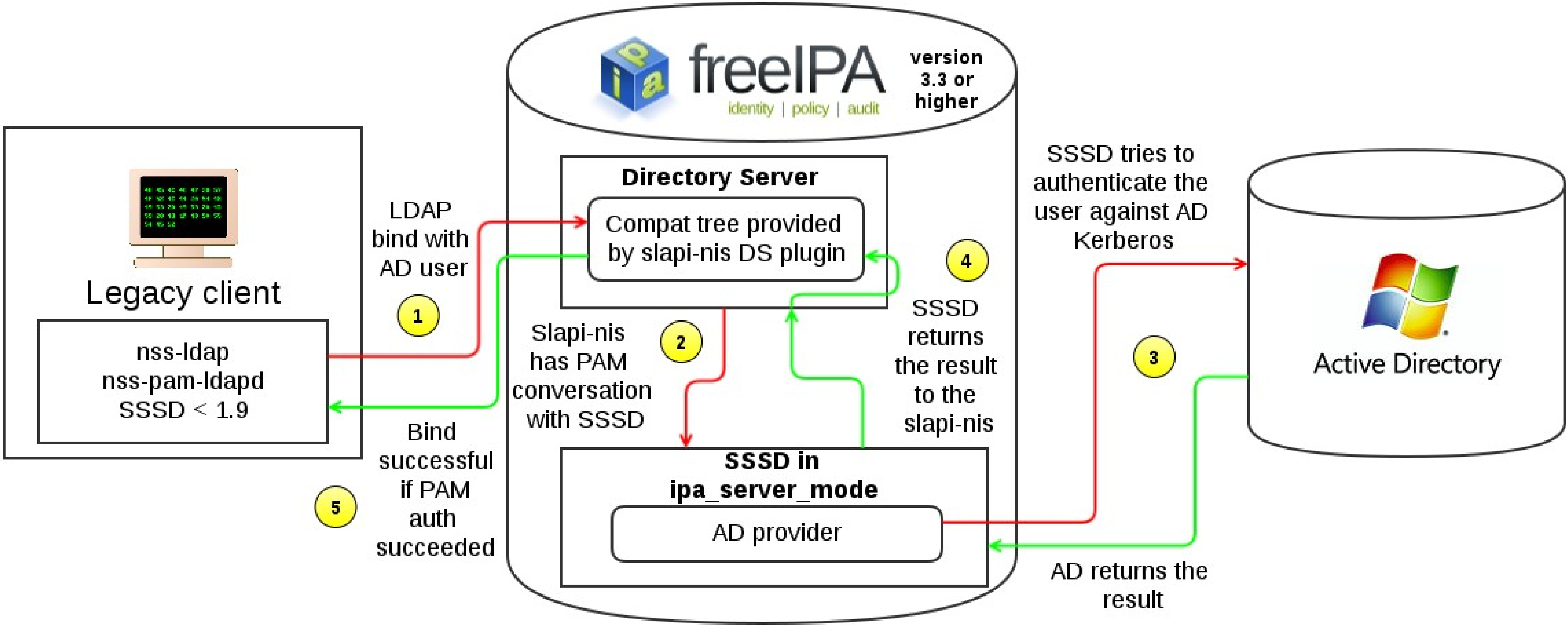
2. The request is intercepted by the *slapi-nis* plugin. It performs PAM auth as *system-auth* service on the FreeIPA server on user's behalf.

AD User / group authentication on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Directory Server
Compat tree provided by slapi-nis DS plugin
SSSD in ipa_server_mode
AD provider
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
Active Directory
1
LDAP bind with AD user
2
Slapi-nis has PAM conversation with SSSD
3
SSSD tries to authenticate the user against AD Kerberos
AD returns the result
4
SSSD returns the result to the slapi-nis
5
Bind successful if PAM auth succeeded

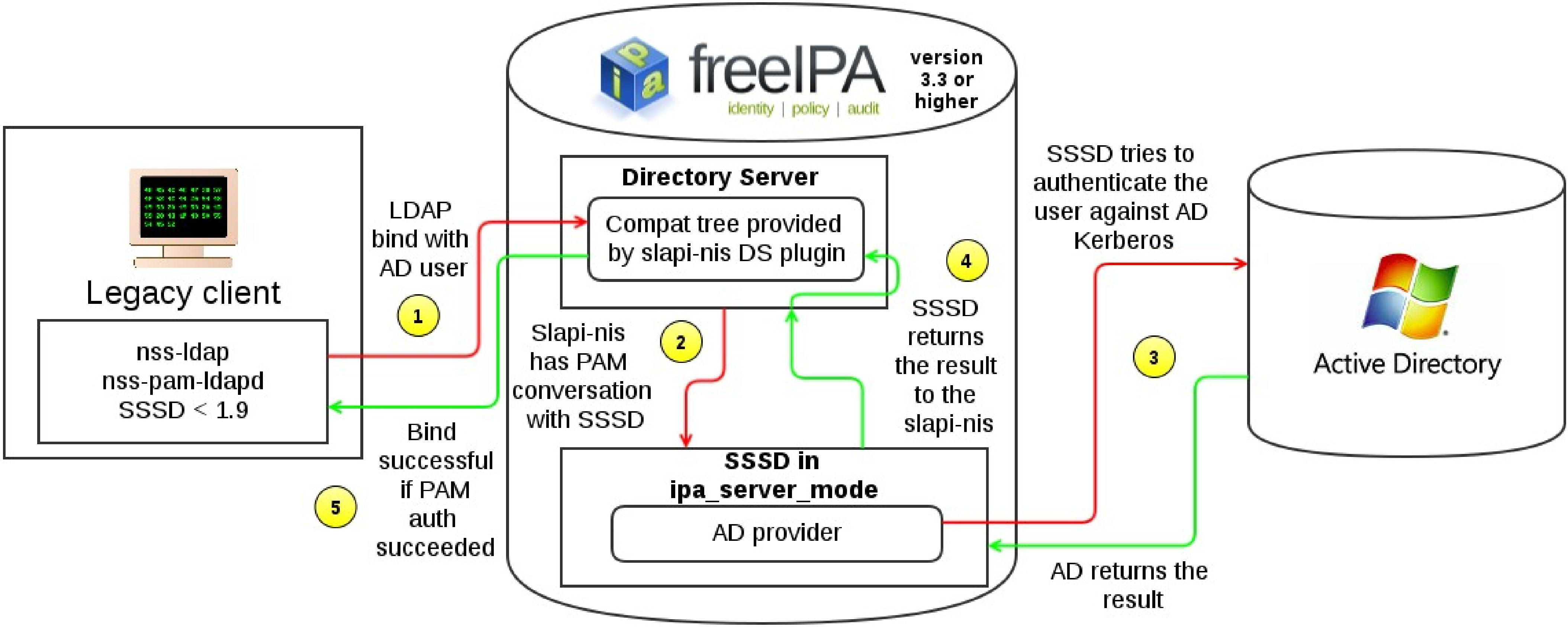
3. In default configuration, PAM auth is performed by SSSD, which in turn tries to authenticate the AD user against Active Directory.

AD User / group authentication on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
LDAP bind with AD user
1
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis has PAM conversation with SSSD
2
SSSD in ipa_server_mode
AD provider
SSSD tries to authenticate the user against AD Kerberos
3
Active Directory
AD returns the result
4
SSSD returns the result to the slapi-nis
5
Bind successful if PAM auth succeeded

4. SSSD returns the result of the PAM auth to *slapi-nis* depending on the success of the authentication against Kerberos.

AD User / group authentication on legacy clients


freeIPA
identity | policy | audit
version 3.3 or higher
Legacy client
nss-ldap
nss-pam-ldapd
SSSD < 1.9
LDAP bind with AD user
1
Bind successful if PAM auth succeeded
5
Directory Server
Compat tree provided by slapi-nis DS plugin
Slapi-nis has PAM conversation with SSSD
2
SSSD returns the result to the slapi-nis
4
SSSD in ipa_server_mode
AD provider
SSSD tries to authenticate the user against AD Kerberos
3
AD returns the result
Active Directory

5. If the authentication was successful, *slapi-nis* returns LDAP_SUCCESS.

Pitfalls

Common mistakes

- Make sure you ran ipa-adtrust-install with –enable-compat option. Otherwise the compatibility tree that provides AD information will not be available. Please note you can run

  ```
  # ipa-adtrust-install –enable-compat
  ```

  even after the first run of ipa-adtrust-install to enable the compatibility tree.
- If you have HBAC's allow_all rule disabled, you will need to allow *system-auth* service on the FreeIPA master, so that authentication of the AD users can be performed.

freeIPA

identity | policy | audit