Foreman - Feature #3528

When new users are created based on REMOTE_USER authentication, their attributes should be populated as well

10/28/2013 09:04 AM - Jan Pazdziora

Status:	Closed		
Priority:	Normal		
Assignee:	Jan Pazdziora		
Category:	Authentication		
Target version:	1.4.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The issue http://projects.theforeman.org/issues/3312 and related pull request https://github.com/theforeman/foreman/pull/967 attempts to make the REMOTE_USER authentication usable for other authentication mechanisms than just HTTP Basic. When the user is populated in Foreman database upon successful logon, they get redirected to add their email address. If the email address of the user is available in the remote authentication service (like FreeIPA), Foreman should populate the database with the data, saving the user manual edits that can lead to errors.

Based on http://www.freeipa.org/page/Environment_Variables#Proposed_Additional_Variables, the proposed environment variables that Foreman could observe besides REMOTE_USER are REMOTE_USER_EMAIL, REMOTE_USER_FIRSTNAME, and REMOTE_USER_LASTNAME for the user.

There is an experimental work going on in sssd which will make it possible to get the values from IPA and get them to the Apache, probably using a mod_lookup_identity module (https://github.com/adelton/mod_lookup_identity/, http://fedorapeople.org/cgit/adelton/public_git/mod_lookup_identity.git/).

The testing setup

One way to setup the population of the REMOTE_USER_* environment variables to see the patch from https://github.com/theforeman/foreman/pull/986 working is with IPA.

IPA server, enroll Foreman machine, setup mod_auth_kerb

On 1.4-to-be (develop) installation of Foreman, follow projects.theforeman.org/projects/foreman/wiki/Foreman_and_mod_auth_kerb to enable the Kerberos authentication and autopopulation of users in Foreman.

Configure sssd-dbus and mod_lookup_identity

Enable Jakub Hrozek's repository which has the builds of sssd-dbus and mod_lookup_identity. At http://copr-fe.cloud.fedoraproject.org/coprs/jhrozek/identity_demo/ choose the correct .repo file. For example, on my Foreman on RHEL 6 installation, I do

```
# wget -O /etc/yum.repos.d/jhrozek-identity_demo.repo \
  http://copr-fe.cloud.fedoraproject.org/coprs/jhrozek/identity_demo/repo/epel-6-i386/
```

Install the packages:

```
# yum install -y sssd-dbus mod_lookup_identity
```

Update /etc/sssd/sssd.conf to enable the Infopipe feature of sssd. On my installation, I did:

```
--- /etc/sssd/sssd.conf.orig    2013-12-10 03:09:20.751552952 -0500
+++ /etc/sssd/sssd.conf    2013-12-12 00:52:30.791240631 -0500
@@ -11,8 +11,10 @@
 chpass_provider = ipa
 ipa_server = _srv_, ipa.example.com
```

```
 dns_discovery_domain = example.com
+ldap_user_extra_attrs = mail, givenname, sn
+
 [sssd]
-services = nss, pam, ssh
+services = nss, pam, ssh, ifp
 config_file_version = 2

 domains = example.com
@@ -28,3 +30,7 @@

 [pac]

+[ifp]
+allowed_uids = 48, 0
+user_attributes = +mail, +givenname, +sn
+
```

With new enough selinux-policy, set the following boolean:

```
# setenforce 1
# setsebool -P httpd_dbus_sssd on
```

If your policy doesn't have httpd_dbus_sssd, set SELinux to permissive:

```
# setenforce 0
```

Configure mod_lookup_identity -- edit for example /etc/httpd/conf.d/lookup_identity.conf to have the following in it:

```
# cat >> /etc/httpd/conf.d/lookup_identity.conf <<EOF
LoadModule lookup_identity_module modules/mod_lookup_identity.so

<Location /users/extlogin>
LookupUserAttr mail REMOTE_USER_EMAIL " "
LookupUserAttr givenname REMOTE_USER_FIRSTNAME
LookupUserAttr sn REMOTE_USER_LASTNAME
</Location>
EOF
```

Restart sssd and Apache:

```
# service sssd restart
# service httpd restart
```

As admin, remove the previously autopopulated user from Foreman if there is some, to allow it to be created again, now with attributes.

Now when you use Kerberos obtained from the IPA server to log in to Foreman, you should see the full name of the user instead of the login name in the top right corner of the screen, and if you inspect user's details, the email address should be there as well.

Related issues:

Blocks Foreman - Tracker #5031: External authentication support	**New**	**04/02/2014**
Copied to Foreman - Feature #3696: Populate user or usergroup roles from LDAP...	**Duplicate**	**10/28/2013**
Copied to Foreman - Feature #3892: When new users are created based on REMOTE...	**Closed**	**10/28/2013**

Associated revisions

Revision 8ffa0b9a - 01/07/2014 10:44 AM - Jan Pazdziora

fixes #3528 - Populate first name, last name, and email, if available.

History

#1 - 10/28/2013 09:08 AM - Jan Pazdziora

Created pull request https://github.com/theforeman/foreman/pull/986 for the user attributes.

#2 - 10/28/2013 09:11 AM - Dominic Cleal

- Category set to Authentication

- Status changed from New to Ready For Testing

- Assignee set to Jan Pazdziora

- Target version set to 1.15.0

#3 - 11/12/2013 12:05 PM - Dominic Cleal

- Target version changed from 1.15.0 to 1.10.0

#4 - 11/20/2013 08:57 AM - Dominic Cleal

- Copied to Feature #3696: Populate user or usergroup roles from LDAP or REMOTE_USER_* added

#5 - 12/04/2013 01:11 PM - Dominic Cleal

- Target version changed from 1.10.0 to 1.9.3

#6 - 12/12/2013 06:36 AM - Jan Pazdziora

- Description updated

#7 - 12/12/2013 07:09 AM - Jan Pazdziora

- Description updated

#8 - 12/17/2013 07:52 AM - Jan Pazdziora

- Copied to Feature #3892: When new users are created based on REMOTE_USER authentication, their roles should be populated as well added

#9 - 12/17/2013 07:54 AM - Jan Pazdziora

- Subject changed from When new users are created based on REMOTE_USER authentication, their attributes and roles should be populated as well to When new users are created based on REMOTE_USER authentication, their attributes should be populated as well

- Description updated

I'm removing the roles part from this issue, now tracking it in http://projects.theforeman.org/issues/3892.

#10 - 01/07/2014 10:45 AM - Dominic Cleal

- translation missing: en.field_release set to 2

#11 - 01/07/2014 11:31 AM - Jan Pazdziora

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 8ffa0b9abbd917b0ab1cdd21477d577fa7c54f40.

#12 - 01/31/2014 09:56 AM - Jan Pazdziora

I have now updated http://projects.theforeman.org/projects/foreman/wiki/Foreman_and_mod_auth_kerb with this setup because the Kerberos authentication is currently where it can be seen and used.

#13 - 03/11/2014 11:39 AM - Dominic Cleal

Official documentation was added to the manual: http://theforeman.org/manuals/1.4/index.html#5.7SPNEGOauthentication

#14 - 04/02/2014 03:41 PM - Dominic Cleal

- Blocks Tracker #5031: External authentication support added

#15 - 04/25/2014 02:24 PM - Jan Pazdziora

- Description updated

#16 - 04/25/2014 02:27 PM - Jan Pazdziora

- Description updated