Foreman - Tracker #5031

External authentication support

04/02/2014 03:37 PM - Jan Pazdziora

Status:	New	**% Done:**	0%
Priority:	Normal		
Assignee:			
Category:	Authentication		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1095276	**Red Hat JIRA:**	

Description

This feature is being opened as an overview tracker of using Foreman with external authentication and identity providers like FreeIPA. The general setup is described at http://www.freeipa.org/page/Web_App_Authentication.

We've identified the following places where external authentication and/or identity provider can be used:

- Kerberos SSO using ticket
- Using FreeIPA host based access control to drive access to the Kerberized application
- Making use of the external authentication provider to authenticate the normal logon form, using PAM
- Populating user attributes based on the external identity provider
- Populating user group membership based on the external identity provider
- Keeping user's attributes and group membership up-to-date even during subsequent logons
- Using the authentication in non WebUI situations -- using API, CLI

Parts that are included in the Foreman 1.5 are documented at http://theforeman.org/manuals/1.5/index.html#5.7ExternalAuthentication.

Planned update of Foreman 1.6 documentation for the WebUI authentication features that did not make it to Foreman 1.5 but that are in Foreman-devel and thus will be in Foreman 1.6 is staged in https://github.com/theforeman/theforeman.org/commit/d562de8cc15d3d8361a1d629fb8f5a7dfa5d6eee.

Kerberos SSO using ticket

This feature was fully implemented via http://projects.theforeman.org/issues/3312 and is available in Foreman 1.4 and documented at http://projects.theforeman.org/projects/foreman/wiki/Foreman_and_mod_auth_kerb and in Foreman manual http://theforeman.org/manuals/1.5/index.html#5.7ExternalAuthentication. Since Foreman needs to maintain even externally-authenticated users in its internal database (for foreign keys to work), if the user authenticated via Kerberos was never seen by Foreman before, the record is created in new External auth source.

Using FreeIPA host based access control to drive access to the Kerberized application

This feature can be used by configuring the mod_authnz_pam Apache module and require pam-account foreman-prod together with PAM service and HBAC service in FreeIPA, as described at http://www.freeipa.org/page/Web_App_Authentication. No change was needed in Foreman.

Making use of the external authentication provider to authenticate the normal logon form, using PAM

Using Apache module mod_intercept_form_submit, it is possible to run PAM authentication based on the credentials entered by user on the standard logon form, and signal the application when the authentication passed. Similar to the Kerberos ticket-based authentication, the externally authenticated user record needs to be created in Foreman's database.

The feature is tracked and documented as http://projects.theforeman.org/issues/4462 and was merged to be available in Foreman 1.5.

Populating user attributes based on the external identity provider

When user record is populated based on external authentication, traditionally only the login (username) is available to the application. Foreman will then redirect the user to a page asking to provide at least their email address to proceed.

Using mod_lookup_identity Apache module, it is possible to retrieve this information together with user's name from central identity provider like FreeIPA, and populate record in Foreman's database with it.

This feature was implemented via http://projects.theforeman.org/issues/3528 and is available in Foreman 1.4 and documented at http://projects.theforeman.org/projects/foreman/wiki/Foreman_and_mod_auth_kerb and in Foreman manual http://theforeman.org/manuals/1.5/index.html#5.7ExternalAuthentication.

Populating user group membership based on the external identity provider

Besides user attributes, Foreman can use user group membership information from external identity provider to drive role assignment.

Merged into Foreman develop on 2014-05-06 via http://projects.theforeman.org/issues/3892, group memebership of externally authenticated user whose record is being populated in Foreman's internal database will be set to match the group membership of the user in the central identity provider, using environment variables REMOTE_USER_GROUP_N, REMOTE_USER_GROUP_1, REMOTE_USER_GROUP_2, etc.

The feature is enabled by using Apache module mod_lookup_identity (the same one used for user attribute population) and configuration

```
LookupUserGroupsIter REMOTE_USER_GROUP
```

API for external user groups

The external user groups might need API, tracked in http://projects.theforeman.org/issues/5734.

Keeping user's attributes and group membership up-to-date even during subsequent logons

Keeping the attributes up-to-date

When populating attributes based on external identity provider, the code change was modelled after the current implementation of the similar feature for Foreman's internal LDAP auth sources. In those cases, the user attributes only get set during initial population of the user record.

Keeping the group membership up-to-date

When populating group membership based on external identity provider, the code change was modelled after the population of user attributes. In those cases, the user attributes only get set during initial population of the user record.

Tracking

Merged into Foreman develop on 2014-05-07 via http://projects.theforeman.org/issues/5242, user's attributes and group memberships get updated upon every successful authentication using the External auth source.

Using the authentication in non WebUI situations -- using API, CLI

It should be possible to use the external authentication and identity providers and their features including Kerberos ticket-based SSO not just in WebUI but for API and CLI as well. It is tracked via http://projects.theforeman.org/issues/8923.

Related issues:

Blocked by Foreman - Feature #3312: Make it possible to use the REMOTE_USER /...	**Closed**	**10/17/2013**
Blocked by Foreman - Feature #4462: Add support for PAM authentication via mo...	**Closed**	**02/26/2014**
Blocked by Foreman - Feature #3528: When new users are created based on REMOT...	**Closed**	**10/28/2013**
Blocked by Foreman - Feature #3892: When new users are created based on REMOT...	**Closed**	**10/28/2013**
Blocked by Foreman - Feature #5242: Keeping user's attributes and group membe...	**Closed**	**04/18/2014**
Blocked by Foreman - Feature #5734: Add API for external groups management	**Closed**	**05/15/2014**

Blocked by Installer - Feature #6445: External authentication via FreeIPA sho...	**Closed**	**06/30/2014**
Blocked by Hammer CLI - Feature #8923: Ability to use Negotiate/Kerberos auth...	**Closed**	

History

#1 - 04/02/2014 03:40 PM - Dominic Cleal

- Tracker changed from Feature to Tracker

- Category set to Authentication

#2 - 04/02/2014 03:41 PM - Dominic Cleal

- Blocked by Feature #3312: Make it possible to use the REMOTE_USER / sso/apache.rb authentication with mod_auth_kerb added

#3 - 04/02/2014 03:41 PM - Dominic Cleal

- Blocked by Feature #4462: Add support for PAM authentication via mod_intercept_form_submit added

#4 - 04/02/2014 03:41 PM - Dominic Cleal

- Blocked by Feature #3528: When new users are created based on REMOTE_USER authentication, their attributes should be populated as well added

#5 - 04/02/2014 03:41 PM - Dominic Cleal

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

#6 - 04/02/2014 03:42 PM - Jan Pazdziora

- Tracker changed from Tracker to Feature

- Description updated

- Category deleted (Authentication)

#7 - 04/03/2014 06:10 AM - Jan Pazdziora

- Tracker changed from Feature to Tracker

- Category set to Authentication

I seem to have cancelled Dominic's changes, reverting. Sorry about that.

#8 - 04/03/2014 09:57 AM - Jan Pazdziora

- Description updated

#9 - 04/18/2014 11:31 AM - Jan Pazdziora

- Blocked by Feature #5242: Keeping user's attributes and group membership up-to-date even during subsequent logons added

#10 - 04/18/2014 11:43 AM - Jan Pazdziora

- Description updated

#11 - 05/06/2014 11:05 AM - Jan Pazdziora

- Description updated

#12 - 05/07/2014 11:30 AM - Jan Pazdziora

- Description updated

https://github.com/theforeman/foreman/pull/1424 merged.

#13 - 05/07/2014 12:05 PM - Bryan Kearney

- Bugzilla link set to https://bugzilla.redhat.com/show_bug.cgi?id=1095276

#14 - 05/15/2014 01:56 PM - Jan Pazdziora

- Blocked by Feature #5734: Add API for external groups management added

#15 - 05/15/2014 01:58 PM - Jan Pazdziora

- Description updated

#16 - 05/19/2014 09:06 AM - Jan Pazdziora

- Description updated

#17 - 05/20/2014 11:08 AM - Jan Pazdziora

- Description updated

#18 - 05/20/2014 11:20 AM - Jan Pazdziora

- Description updated

#19 - 05/20/2014 11:27 AM - Jan Pazdziora

- Description updated

#20 - 06/30/2014 12:10 PM - Jan Pazdziora

- Blocked by Feature #6445: External authentication via FreeIPA should be configurable with foreman-installer added

#21 - 01/13/2015 07:26 AM - Jan Pazdziora

- Blocked by Feature #8923: Ability to use Negotiate/Kerberos authentication to API and hammer added

#22 - 01/13/2015 07:27 AM - Jan Pazdziora

- Description updated