Foreman - Bug #9215

LDAPS AD bind fails with one user after upgrade to 1.7.2.

02/04/2015 06:23 AM - Jose Antonio Insua

Status:	Rejected		
Priority:	Normal		
Assignee:			
Category:	Authentication		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.7.2
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Foreman 1.7.1 worked perfectly binding to our Active Directory.

After updating to 1.7.2, that user doesn't seem to be able to bind to the Active Directory anymore.

The user works properly for other systems to bind, so it seems the user is not blocked.
In the foreman host I'm able to successfully run ldapsearch to bind t o the Active Directory using that user.

If I change that user to my personal user, Foreman works fine.

In my troubleshooting steps I've run this upgrade steps with foreman stopped:

foreman-rake db:migrate
foreman-rake db:seed
foreman-rake tmp:cache:clear
foreman-rake tmp:sessions:clear

Since the system is not critical, I also rebooted it.

I'm running a fully updated CentOS 6.6

History

#1 - 02/05/2015 04:29 AM - Dominic Cleal

- Category set to Authentication

I can't see any changes in this area between 1.7.1 and 1.7.2. Perhaps the production.log would give some indication?

#2 - 02/05/2015 06:23 AM - Jose Antonio Insua

Hello!

The only reference to the login in production.log I can find is the following:

```
Started POST "/users/login" for 10.132.4.81 at 2015-02-05 09:43:51 +0000
Processing by UsersController#login as HTML
  Parameters: {"utf8"=>"▯", "authenticity_token"=>"mNgIaAJfwqF8F/uT7kQTeJPtUxxxxxcyffscRIP8IvZk=
", "login"=>{"login"=>"loginuser", "password"=>"[FILTERED]"}, "commit"=>"Login"}
Operation FAILED: Could not bind to ActiveDirectory user DOMAINNAME\binduser
  Rendered common/500.html.erb within layouts/application (4.5ms)
  Rendered layouts/base.html.erb (1.4ms)
Completed 500 Internal Server Error in 190ms (Views: 10.1ms | ActiveRecord: 6.4ms)

Started POST "/api/reports" for 192.168.145.2 at 2015-02-05 09:43:54 +0000
Processing by Api::V2::ReportsController#create as JSON
  Parameters: {"report"=>"[FILTERED]", "apiv"=>"v2"}
processing report for managedhost.corp.domainname.com
Imported report for managedhost.corp.domainname.com in 0.03 seconds
Completed 201 Created in 42ms (Views: 2.4ms | ActiveRecord: 0.0ms)
```

```
Started GET "/favicon.ico" for 10.132.4.81 at 2015-02-05 09:44:02 +0000

ActionController::RoutingError (No route matches [GET] "/favicon.ico"):
  /usr/lib/ruby/gems/1.8/gems/passenger-4.0.18/lib/phusion_passenger/rack/thread_handler_extension.rb:77:in `p
rocess_request'
  /usr/lib/ruby/gems/1.8/gems/passenger-4.0.18/lib/phusion_passenger/request_handler/thread_handler.rb:140:in 
`accept_and_process_next_request'
  /usr/lib/ruby/gems/1.8/gems/passenger-4.0.18/lib/phusion_passenger/request_handler/thread_handler.rb:108:in 
`main_loop'
  /usr/lib/ruby/gems/1.8/gems/passenger-4.0.18/lib/phusion_passenger/request_handler.rb:441:in `block (3 level
s) in start_threads'
```

Please be aware that I sanitized the hostnames, tokens and usernames :)

Do not hesitate to ask for anything else you might need!!

Cheers!

#3 - 02/05/2015 06:38 AM - Dominic Cleal

This error message appears to come from Foreman binding with its own user account, rather than the user who's logging in. Could you try binding with ldapsearch using the credentials configured under the LDAP Auth Source?

#4 - 02/05/2015 07:56 AM - Jose Antonio Insua

Hello!

Yes, we use one specific user to LDAP-bind to the Active Directory.

That user is working in all systems, it only fails for Foreman.

And yes, I've executed an ldapsearch in the same host as foreman, with the LDAP-bind user, and it is successful.

I've tried binding with my own user, and then, Foreman works, but when I set back the LDAP-bind user, it fails again.

#5 - 02/18/2015 11:00 AM - Jose Antonio Insua

Another system started failing erratically with the same LDAP-bind user.

It seems to be a glitch in the Active Directory that is not working 100% properly, and for some reason The Foreman is more affected than the other systems.

Please close the bug.

#6 - 02/18/2015 11:05 AM - Dominic Cleal

- Status changed from New to Rejected

Thanks for confirming Jose, glad you tracked it down somewhat. Maybe some sort of rate limiting or auth failure timeout?

#7 - 02/25/2015 01:46 PM - Jose Antonio Insua

Hello!

Yes, it seems that the bind account was being blocked by a high number of failures from a script with the wrong password.

Curiously, our Jenkins was able to recover from the failures, but the Foreman was completely blocked out.

Thank you very much for your help :-)