Foreman - Bug #14715

LDAP authentication with bundle of CA certs

04/19/2016 02:40 PM - Bryan Kearney

Status:	Resolved		
Priority:	Normal		
Assignee:			
Category:	Authentication		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1323998	**Red Hat JIRA:**	
Pull request:			

Description

Customer has lots of different self-signed CA and SubCA in our company, therefore, the package to be deployed is a bundle, like once a year more or less. He doesn't know which is the certificate that will be in usage by LDAP or other tools. Therefore, he wants to use certificate bundle to configure LDAP authentication with Satellite.

History

#1 - 04/19/2016 02:40 PM - Bryan Kearney

- Bugzilla link set to 1323998

#2 - 04/19/2016 02:41 PM - Bryan Kearney

- Category set to Authentication

- Bugzilla link deleted (1323998)

#3 - 04/19/2016 02:42 PM - Bryan Kearney

- Bugzilla link set to 1323998

#4 - 04/20/2016 03:03 AM - Dominic Cleal

- Status changed from New to Feedback

The system CA store is used, so install all of the certs there - as many as you like. Foreman doesn't store individual certs for LDAP auth, so this bug report doesn't make much sense.

#5 - 07/28/2016 01:07 PM - Bryan Kearney

Dominic Cleal wrote:

> The system CA store is used, so install all of the certs there - as many as you like. Foreman doesn't store individual certs for LDAP auth, so this bug report doesn't make much sense.

I got this from downstream

(In reply to Bryan Kearney from comment #6)

> Take a look at
>
> https://theforeman.org/manuals/1.11/index.html#4.1.1LDAPAuthentication
>
> and let me know if that process addresses your concerns.

Hi Bryan,
this is the outcome from CU tests:

########

Hi Andrea

I have tryed your solution, but not work. When I remove my previus pem from bundle (see https://access.redhat.com/solutions/1593413), and I use

```
# cp example.crt /etc/pki/tls/certs/
# ln -s example.crt /etc/pki/tls/certs/$(openssl x509 -noout -hash -in /etc/pki/tls/certs/example.crt).0
```

the connection was wrong.

```
 | Foreman::WrappedException: ERF50-1006 [Foreman::WrappedException]: Unable to connect to LDAP server ([Net::
LDAP::Error]: SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certific
ate verif...)
 | /usr/share/foreman/app/models/auth_sources/auth_source_ldap.rb:149:in `rescue in test_connection'
 | /usr/share/foreman/app/models/auth_sources/auth_source_ldap.rb:142:in `test_connection'
 | /usr/share/foreman/app/controllers/auth_source_ldaps_controller.rb:43:in `test_connection'
```

I must do split the pem chain in to single file. Like this and now work:

```
[root@xlgnutlsat2 ~]# csplit -f cert- prod_ldap.pem '/-----BEGIN CERTIFICATE-----/' '{*}'
0
834
1411
1359
1574
1740
2906
1224
1716
1334
1216
1805
1371
[root@xlgnutlsat2 ~]#

[root@xlgnutlsat2 ~]# ls -l cert-*
-rw-r--r--. 1 root root    0 Jul 12 12:38 cert-00
-rw-r--r--. 1 root root  834 Jul 12 12:38 cert-01
-rw-r--r--. 1 root root 1411 Jul 12 12:38 cert-02
-rw-r--r--. 1 root root 1359 Jul 12 12:38 cert-03
-rw-r--r--. 1 root root 1574 Jul 12 12:38 cert-04
-rw-r--r--. 1 root root 1740 Jul 12 12:38 cert-05
-rw-r--r--. 1 root root 2906 Jul 12 12:38 cert-06
-rw-r--r--. 1 root root 1224 Jul 12 12:38 cert-07
-rw-r--r--. 1 root root 1716 Jul 12 12:38 cert-08
-rw-r--r--. 1 root root 1334 Jul 12 12:38 cert-09
-rw-r--r--. 1 root root 1216 Jul 12 12:38 cert-10
-rw-r--r--. 1 root root 1805 Jul 12 12:38 cert-11
-rw-r--r--. 1 root root 1371 Jul 12 12:38 cert-12

[root@xlgnutlsat2 ~]# cp cert-* //etc/pki/tls/certs/
[root@xlgnutlsat2 ~]# cd /etc/pki/tls/certs/
[root@xlgnutlsat2 certs]# ll
total 108
lrwxrwxrwx. 1 root root    10 Jul 12 12:18 8df30ae9.0 -> RootCA.pem
lrwxrwxrwx. 1 root root    49 Jul  4 15:59 ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
lrwxrwxrwx. 1 root root    55 Jul  4 15:59 ca-bundle.trust.crt -> /etc/pki/ca-trust/extracted/openssl/ca-bundl
e.trust.crt
-rw-r--r--. 1 root root     0 Jul 12 12:43 cert-00
-rw-r--r--. 1 root root   834 Jul 12 12:43 cert-01
-rw-r--r--. 1 root root  1411 Jul 12 12:43 cert-02
-rw-r--r--. 1 root root  1359 Jul 12 12:43 cert-03
-rw-r--r--. 1 root root  1574 Jul 12 12:43 cert-04
-rw-r--r--. 1 root root  1740 Jul 12 12:43 cert-05
-rw-r--r--. 1 root root  2906 Jul 12 12:43 cert-06
-rw-r--r--. 1 root root  1224 Jul 12 12:43 cert-07
-rw-r--r--. 1 root root  1716 Jul 12 12:43 cert-08
-rw-r--r--. 1 root root  1334 Jul 12 12:43 cert-09
-rw-r--r--. 1 root root  1216 Jul 12 12:43 cert-10
-rw-r--r--. 1 root root  1805 Jul 12 12:43 cert-11
-rw-r--r--. 1 root root  1371 Jul 12 12:43 cert-12
-r--r--r--. 1 root root 18490 Jul 12 11:14 ldap.pem
-rw-------. 1 root root  1505 Jul  5 10:48 localhost.crt
-rwxr-xr-x. 1 root root   610 Apr 29 15:00 make-dummy-cert
-rw-r--r--. 1 root root  2388 Apr 29 15:00 Makefile
-r--r--r--. 1 root root 18490 Jul  6 16:04 prod.pem
-rwxr-xr-x. 1 root root   829 Apr 29 15:00 renew-dummy-cert
-rw-r--r--. 1 root root  1356 Jul 12 12:18 RootCA.pem
```

```
[root@xlgnutlsat2 certs]# for i in `seq 1 9`; do ln -s cert-0$i /etc/pki/tls/certs/$(openssl x509 -noout -hash
 -in /etc/pki/tls/certs/cert-0$i).0; done
[root@xlgnutlsat2 certs]# for i in `seq 10 12`; do ln -s cert-$i /etc/pki/tls/certs/$(openssl x509 -noout -has
h -in /etc/pki/tls/certs/cert-$i).0; done
[root@xlgnutlsat2 certs]# ll
total 108
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 0eb08fbe.0 -> cert-11
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 2c543cd1.0 -> cert-10
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 2d1cd87e.0 -> cert-03
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 3e7acb8a.0 -> cert-02
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 415660c1.0 -> cert-01
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 48ef30f1.0 -> cert-07
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 5b0c9667.0 -> cert-12
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 5f267794.0 -> cert-05
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 8df30ae9.0 -> cert-09
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 91795530.0 -> cert-06
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 aee5f10d.0 -> cert-04
lrwxrwxrwx. 1 root root    49 Jul  4 15:59 ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
lrwxrwxrwx. 1 root root    55 Jul  4 15:59 ca-bundle.trust.crt -> /etc/pki/ca-trust/extracted/openssl/ca-bundl
e.trust.crt
-rw-r--r--. 1 root root     0 Jul 12 12:43 cert-00
-rw-r--r--. 1 root root   834 Jul 12 12:43 cert-01
-rw-r--r--. 1 root root  1411 Jul 12 12:43 cert-02
-rw-r--r--. 1 root root  1359 Jul 12 12:43 cert-03
-rw-r--r--. 1 root root  1574 Jul 12 12:43 cert-04
-rw-r--r--. 1 root root  1740 Jul 12 12:43 cert-05
-rw-r--r--. 1 root root  2906 Jul 12 12:43 cert-06
-rw-r--r--. 1 root root  1224 Jul 12 12:43 cert-07
-rw-r--r--. 1 root root  1716 Jul 12 12:43 cert-08
-rw-r--r--. 1 root root  1334 Jul 12 12:43 cert-09
-rw-r--r--. 1 root root  1216 Jul 12 12:43 cert-10
-rw-r--r--. 1 root root  1805 Jul 12 12:43 cert-11
-rw-r--r--. 1 root root  1371 Jul 12 12:43 cert-12
lrwxrwxrwx. 1 root root     7 Jul 12 12:50 d04a5cf7.0 -> cert-08
-r--r--r--. 1 root root 18490 Jul 12 11:14 ldap.pem
-rw-------. 1 root root  1505 Jul  5 10:48 localhost.crt
-rwxr-xr-x. 1 root root   610 Apr 29 15:00 make-dummy-cert
-rw-r--r--. 1 root root  2388 Apr 29 15:00 Makefile
-r--r--r--. 1 root root 18490 Jul  6 16:04 prod.pem
-rwxr-xr-x. 1 root root   829 Apr 29 15:00 renew-dummy-cert
-rw-r--r--. 1 root root  1356 Jul 12 12:18 RootCA.pem
```

Best regards.

########

Please let me know if we need something else from CU.

#6 - 07/29/2016 03:27 AM - Dominic Cleal

- Status changed from Feedback to Resolved

Sounds like it's working then. There are OS tools for installing bundles of certificates, such as /etc/pki/ca-trust/source/anchors/ + update-ca-trust, but this isn't Foreman - see ca-certificates docs.