Foreman - Feature #29492

DNS discovery for LDAP backends

04/07/2020 09:31 AM - Stephan Schultchen

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Authentication		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

please implement ldap server discovery via DNS.

right now one can only specify one LDAP server as backend. if this server fails, foreman has to be manually reconfigured.

but since ldap servers most likely are either FreeIPA/RedHat IdM or Microsoft AD servers, DNS Service discovery should work for those.

a well setup AD or IdM/IPA REALM should answer to this query:

dig srv _ldap._tcp.example.com

0 100 389 ipa-1.linux.com.
0 100 389 ipa-2.linux.com.
0 100 389 ipa-3.linux.com.

usually to perform this query, you use the fqdn of the host, and strip the host part of it, if this fails, and the domain part has still some segments left, you start stripping the next part from the left, and retry the query.

example fqdn: foreman.prod.location.example.com
discovery url1: _ldap._tcp.prod.location.example.com
discovery url2: _ldap._tcp.location.example.com
discovery url3: _ldap._tcp.example.com

dns service discovery should stop, until the first query delivered a valid result.

it might make sense to alternatively allow to specify the url that should be used for service discovery. this would come in handy in case the foreman server is enrolled to an IdM/IPA realm, but the users live in a AD realm, DNS discovery then would yield the wrong result in this case.