Katello - Feature #30428

Allow api access to gpgkey/content credentials via name

07/17/2020 09:23 AM - Dirk Götz

Status:	New		
Priority:	Normal		
Assignee:			
Category:	API		
Target version:	Katello Backlog		
Difficulty:		**Fixed in Releases:**	
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

At the moment you can get the GPG key or Content credentials via the api using one of the URLs:
https://katello.localhost/katello/api/v2/gpg_keys/1/content
https://katello.localhost/katello/api/v2/content_credentials/1/content

Now we have the problem that SLES requires us to import GPG keys before using them (zypper does not ask to import like yum/dnf). We solved this by exporting the keys to the filesystem and provide them for bootstraping via http://katello.localdomain/pub. But we want to get rid of the additional steps and redundant data so thought about using the API, but with the ID it is also not so easy, so it would be great if the name could be used like this:
https://katello.localhost/katello/api/v2/content_credentials/RPM-GPG-KEY-EPEL-7/content

History

#1 - 07/17/2020 09:30 AM - Dirk Götz

One additional idea for easier access would be having the GET for the API-Endpoint without requiring authentication.

#2 - 07/22/2020 05:54 PM - Chris Roberts

- Status changed from New to Need more information

- Target version set to Katello Backlog

Dirk,

You can use scoped search with the API to search by name and get the ID of the key, let us know if that does not work?

#3 - 07/23/2020 07:11 AM - Dirk Götz

Chris, can you give me an example?
What I know I can do is a query at https://katello.localhost/katello/api/v2/content_credentials to get the id to a name and then do another query for the content. This is perfectly ok for scripting, but I would like to avoid scripting to much in the provisioning scripts (especially in autoyast).
This is why the customer started to export the keys and use the exported ones. When I showed how to access the key directly from Katello, I had to agree that it will make the provision script much more complicated, so I came up with this feature request.

#4 - 07/29/2020 05:47 PM - Justin Sherrill

Hey Dirk,

This is actually possible for gpg keys associated with a repository. If you associate some gpg key with a repository of id '5', you'd fetch the gpgkey content via:

GET /katello/api/v2/repositories/5/gpg_key_content

Does that work for you? We could do something similar on a per-content-credential basis, but it would need to be opt in in some way as you wouldn't want to expose ssl client keys without any authentication

#5 - 07/29/2020 05:50 PM - Justin Sherrill

and to add more info, this is actually how we configure yum repositories in the redhat.repo file. If you associate a gpg key with a yum repository, subscription manager will configure the client's redhat.repo file to use the GpG key at a similar URL

#6 - 08/07/2020 09:17 AM - Dirk Götz

Thanks, Justin. I know that the URL is working and that yum is doing fine with it as it allows the user simply to say yes to accept a new key. The problem is zypper which does not do so, why we have to install the certificate first and while we can get it from Katello it is not so easy when requiring to know IDs and Authentication. Especially when you are limited to bash during provisioning.

This is really only about make our life easier when dealing with SLES and its limitations.

#7 - 08/12/2020 05:44 PM - Justin Sherrill

That particular api end point does not require any sort of authentication. It does require knowing the repository id, but if we exposed being able to fetch the gpg key it would probably also require knowing an id without doing something quite different than anywhere else.

GPG keys are not unique per org, so it'd have to be something like:

https://katello.localhost/katello/api/v2/organization/MyOrg/content_credentials/RPM-GPG-KEY-EPEL-7/content

#8 - 08/14/2020 11:05 AM - Dirk Götz

Ok, the Organization makes the URL longer but it would be still much better to read, write and remember. If you know your Organization and keep the keys in a consistent naming schema at least. Combined with no authentication I think this would be useful for our case and makes it easier. :-)

#9 - 08/19/2020 05:39 PM - John Mitsch

- Triaged changed from No to Yes

#10 - 08/19/2020 05:39 PM - John Mitsch

- Status changed from Need more information to New