KIP-13 Environment variables should be usable when looking up passwords

Status

Current-Status: In-progress

Discussion thread:

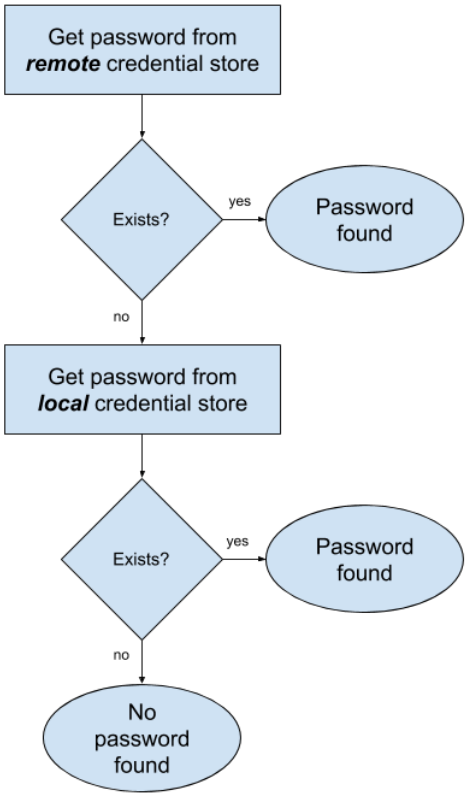
JIRA: KNOX-1794

Motivation

The Knox Gateway assumes that all passwords are stored in a local or remote credential store. Locally, the credential store is a Java keystore that is encrypted using Knox's master secret. Remotely, the credential store can be different implementations with may or may not be managed by Knox. For most cases, this works out well. However, management consoles may provide a keystore for the Gateway TLS identity and/or signing key. In this case, the passwords for the keystores and keys may be provided via environment variables and Knox will need to look there rather than the remote or local credential stores.

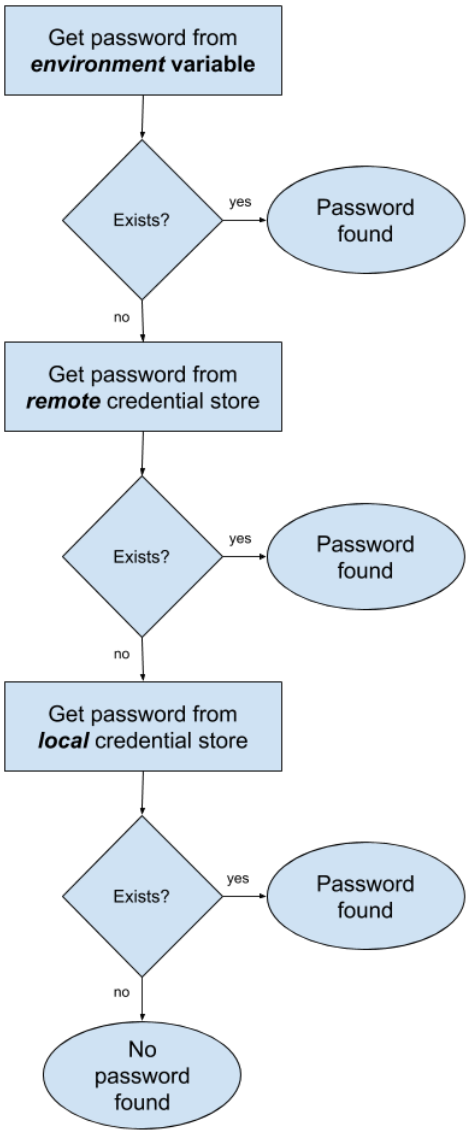
Design

The Knox Gateway looks up passwords using the Gateway's ***Alias Service***. The current implementation of the *Alias Service* first looks to the remote credential store (if configured). If a password is found for the given alias name, then it is assumed to be the desired value. If a password is not found, then the service looks to the local credential store. Using a given alias name, looks up the alias in the configured keystore. If a password is found, then it is assumed to be the desired value; else, no password value was found. The diagram below depicts this workflow.



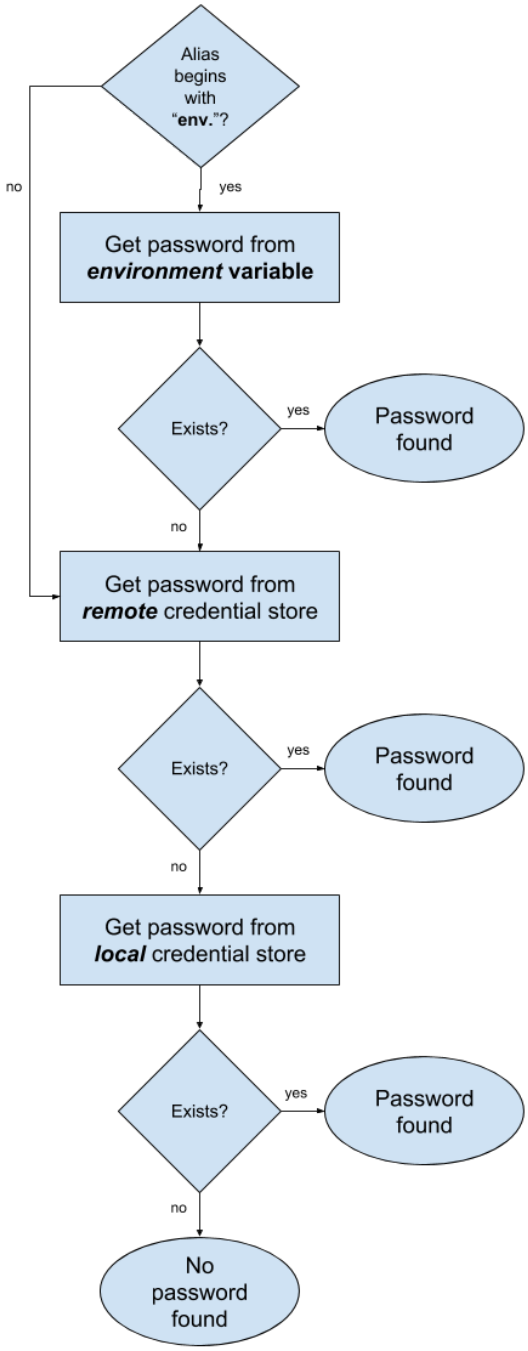
Current password lookup workflow.

To allow for passwords to be specified using environment variables, the *Alias Service* needs to be updated to look in the environment as well. This should be done before checking the remote and local credential stores, as shown below.



Proposed updated password lookup workflow.

Since it may not be desirable to always use the environment as a potential credential store, alias names should be decorated to indicate that the target container is the environment. The current implementation most of the relevant alias names are declared in the gateway-site.xml file. For example, the alias name for the password for the TLS identity's keystore file is specified using the property named *gateway.tls.keystore.password.alias*. By default the value is "gateway-identity-keystore-password". Without decorating this alias name, it could take up to 3 lookup operations to find the relevant password. However, if a convention is enforced, then the environment lookup can be skipped. To allow for an alias to be looked up in the environment, the alias name must begin with "**env.**". This prefix will be removed when performing the lookup. For example, to look for "gateway-identity-keystore-password" in the environment, the value of the *gateway.tls.keystore.password.alias* configuration property must be "env.gateway-identity-keystore-password". The "env." will be stripped from the alias name and "gateway-identity-keystore-password" will be used to search the environment, and then the remote and local credential stores (as necessary). However, if the value of the *gateway.tls.keystore.password.alias* configuration property is "gateway-identity-keystore-password", then "gateway-identity-keystore-password" will be used to search in the remote and local credential stores (as necessary).



Proposed updated password lookup workflow allowing the environment variable lookup to be skipped.