SCALING CHEF COMPLIANCE SCANNER
Version 1.0
6 April 2017
Imre Jonk

To scale Chef compliance scanner deployments, we have to consider these requirements:

1. The Chef compliance scanner needs secure administrator access to all subjects;
2. The scanner has to scan all subjects, preferably scheduled;
3. Compliance reports and statistics should be available from a central location.

In a large computer cluster, individual computing units are often managed with configuration management software like Chef or Puppet. We can use this infrastructure to automatically create accounts on these units, give these accounts administrator privileges, provision them with the public key and provide remote shell access for the compliance scanner.

Additionally, if the cluster uses LDAP for authentication and authorization, we can insert the public key of the scanner into the LDAP database. This would also allow the compliance scanner to authenticate the subjects. One such implementation is FreeIPA. FreeIPA provides easy-to-use Identity, Policy and Audit (IPA) software for large organizations. It is possible to use the command line[1] or web interface[2] to manage public SSH keys. These public keys can then be accessed by the whole cluster and every node can authenticate every other node.

Active Directory can also manage public keys for a large organization, in the form of certificates[3] . The subjects would then need to be configured (with configuration managed software) to use HTTPS with AD certificates for all WinRM connections.

Now that secure administrator access is taken care of, the scanner needs to be configured to scan all subjects. Chef compliance scanner has a web interface which can be used to manually add nodes, define compliance benchmarks to test against and schedule scans, but this does not scale well. Instead, we can write a script that regularly pulls subject information from the LDAP database and updates Chef compliance scanner's Postgres database accordingly. The script would also have functionality to specify the benchmarks to test against.

Chef compliance scanner can already centrally generate compliance reports. If we implement all of the above, we should be able to achieve scalable compliance scanning.

---

[1] Jan Cholasta, *SSH Public Keys in FreeIPA* (01-15-2013)
https://www.freeipa.org/images/d/d2/Freeipa30_SSH_Public_Keys.pdf
[2] Red Hat, *Managing Public SSH Keys for Hosts* (2017)
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Identity_Management_Guide/host-keys.html
[3] Microsoft, *Active Directory Certificate Services and Public Key Management* (2017)
https://technet.microsoft.com/en-us/library/cc753828(v=ws.11).aspx