Niagara 4.13 Feature Preview - Secure Communication and Certificate Management in Niagara

May 4, 2023

Q&A

1. **Why is Tridium pushing 4.10 so much, as in the 5th update, when 4.11 and 4.12 are released? Is 4.10 considered more stable?**

   4.10 is the Long-Term Supported release and will continue to get updates until the next Long-Term Supported release is out. This allows customers to use the same version of Niagara while continuing to receive critical updates.

2. **Does this mean we will be a Deep Packet Inspection to Decrypt?**

   For the context of this webinar, decryption will happen on the client or server as part of normal TLS communication, using the private key of the certificates.

   Deep Packet Inspection is typically used to inspect packets as they pass through the network and is not performed by the endpoints. It's not part of the 'normal' TLS exchange but it is sometimes used as a security measure to detect unusual traffic. We won't be covering that in this talk.

3. **If our Niagara connections are over FOXS, if the approved certificate expires will the connection fail?**

   If your certificate has been signed by a CA trusted by the client, once the certificate is expired the connection will fail.

   If the certificate has been approved in the "Allowed Hosts" tab in the Certificate Management view, the connection should continue to work. However, this is not good practice because you are trusting old certificates.

   To clarify, the cert in the "Allowed Hosts" tab will work while expired if it was approved while expired. If it expires after having been approved, it will need to be re-approved.

4. **At some point can you talk about best practices for certificates in a system that does not have names (just IP addresses), and possible no internet access? This is how most BAS systems traditional have been setup.**

   The same rules and steps apply. Simply use the ipAddress in lieu of domain name for the Common Name (or Subject).

5. If we create a server certificate from our own Root certificate, will we need to change these every year on supervisors and JACEs?

   During signing, the Certificate Authority will decide on how long your certificate will be valid for. For things like the Fox and Web service, a year is the recommended validity period.

   The certificate will not need to be completely changed at the end of the year, however, it will need to be re-signed. There are provisioning jobs that help with this. Additionally, there is some work in the pipeline to help automatically renew signed certificates.

6. Is the ability to auto renew web server certificates from trusted authorities, where account info is stored and auto-renew is in the contract with the authority in the pipeline?

   Yes! This feature is in the pipeline. A Signing Service is targeted to be available in 4.13. However, client-side implementations for the Fox and Web Services to connect to a Signing Service will be in a later release.

7. Are the certificates and the private keys stores in the certificate manager encrypted? Is it protected if someone dump the hard drive?

   Yes, they are encrypted with a key store in the Key Ring. The Key Ring itself is protected by a key whose location depends on the platform the station is running on.

8. Can Niagara handle formats other than PEM now?

   Niagara can now export certificates in PKCS7 format, but can still only import PEM certificates and private keys, and can only export private keys as PEMs.

9. Is the private key password used as the encryption hash? If so, what recommendations do you have for password complexity?

   The keystore itself is encrypted with a system generated key. The private key password is an additional protection that limits access to particular keys even when the keystore itself is accessible. Password requirements are enforced (10 characters, 1 uppercase, 1 lowercase, 1 digit, or 14 characters, 1 uppercase, 1 lowercase, 1 digit for FIPS mode), and should be appropriate for most use cases.

10. Which authority is the best to use?

    Your own because it's free and you are in charge! But if using a paid-for service, like anything, shop around to find the vendor that best suits your needs (services, pricing, etc).

11. In a non-BACnet SC implementation, is the Foxs protocol encrypted only between stations and station to workbench? What about third party head end software? Is this going to receive only unencrypted upstream communications (be it classic BACnet IP or others).

    Foxs protocol is used by both Wb to Station and Station to Station communication. Third party head end software would be dependent upon the protocols they support (could be as simple as https).