Configure Jenkins to Use Cornell Shibboleth (SAML)

It is much easier to configure the SAML plugin for Jenkins using the Configuration-as-Code Jenkins plugin. Configuration would be something like this:

```
jenkins
  securityRealm:
    saml:
      binding: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      displayNameAttributeName: "urn:oid:2.16.840.1.113730.3.1.241"
      emailAttributeName: "urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
      encryptionData:
        # forceSignRedirectBindingAuthnRequest:
        #   true, for production Shibboleth
        #   false, for test Shibboleth
        forceSignRedirectBindingAuthnRequest: false
        keystorePassword: changeit
        keystorePath: "/var/jenkins_home/saml-key.jks"
        privateKeyAlias: "saml-key"
        privateKeyPassword: changeit
        # wantsAssertionsSigned:
        #   Does production Shibboleth want true or false?
        #   Test Shibboleth wants false
        wantsAssertionsSigned: false
      groupsAttributeName: "urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
      idpMetadataConfiguration:
        period: 1440
        url: "https://shibidp.cit.cornell.edu/idp/shibboleth"
        # url: "https://shibidp-test.cit.cornell.edu/idp/shibboleth"
      maximumAuthenticationLifetime: 86400
      usernameAttributeName: "urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
      usernameCaseConversion: "none"
```

These instructions have been validated against Jenkins version 2.289.3 and SAML Plugin version 2.0.7.

Be aware that our experience indicates a change in behavior between SAML Plugin version 1.x and 2.x. The Jenkins SAML integration broke when updating the SAML Plugin from version 1.x to 2.x if configuration isn't updated.

1. Make a backup of your Jenkins deployment.
2. Create a keypair inside the Jenkins container (or directly on the VM if not running Jenkins as a Docker container).
    a. Do this by creating and running a Jenkins job with the following for Bash script:

```
$JAVA_HOME/bin/keytool -noprompt -genkeypair -alias saml-key \
    -keypass changeit \
    -storepass changeit \
    -keystore /var/jenkins_home/saml-key.jks  \
    -keyalg RSA -keysize 2048 -validity 3650 \
    -dname "CN=jenkins.example.cucloud.net"
```

3. Be sure that the "SAML Plugin" is enabled: Jenkins Manage Plugins
4. Go to SAML plugin under Jenkins Configure Global Security
5. Under Access Control Security Realm select "SAML 2.0", and configure the following:
    a. IdP Metadata: Retrieve from either:
        i. https://shibidp.cit.cornell.edu/idp/shibboleth
        ii. https://shibidp-test.cit.cornell.edu/idp/shibboleth
    b. IdP Metadata URL: leave blank
    c. Refresh Period: 0
    d. Display Name Attribute: urn:oid:2.16.840.1.113730.3.1.241
    e. Group Attribute: urn:oid:1.3.6.1.4.1.5923.1.5.1.1
        i. NOTE: You will need to let IdM know that you would like to use Groups. That attribute is not provided by default. See IdM notes below.
    f. Maximum Authentication Lifetime: leave 86400
    g. Username Attribute: urn:oid:0.9.2342.19200300.100.1.1
    h. Email Attribute: urn:oid:1.3.6.1.4.1.5923.1.1.1.6
    i. Username Case Conversion: None
    j. Data Binding Method: HTTP-Redirect

    k. Logout URL: leave blank
    l. Advanced Configuration: leave unchecked
    m. Encryption Configuration: check
    n. Keystore Path: /var/jenkins_home/saml-key.jks
    o. Keystore Password: changeit
    p. Private Key Alias: saml-key
    q. Private Key Password: changeit
    r. Auth Request Signature: check
    s. Wants Assertion Signed: check
6. Now, be very careful with the following steps:
    a. Use the "Save" button to save that SAML configuration. **Don't use "Apply"! Also, be sure to stay on this configuration page.**
    b. Grab the SP Metadata XML from the link labeled: "Service Provider Metadata" and save to a file. Cornell IdM will need this file.
    c. Now, go back to the top of the page and switch back to your previous form of security. Hit "Save" and "Apply". The reason for this is that you can't fully switch to SAML until you hear back from Cornell IdM, and you don't want a Jenkins restart to switch to SAML without you being ready for it.
7. Goto https://shibrequest.cit.cornell.edu/shibrequest/cornell/main.html and make a request for Shibboleth SP integration, providing the SP metadata you saved in the previous step.
    a. If you want to use AD group membership for Jenkins privileges, be sure to let IdM know that. They will have to setup a group name prefix filter or an OU filter to return a limited set of groups to Jenkins in the SAML responses. Also, the current SAML IdP implementation does NOT allow for nested AD groups, so any AD group will need to contain users as members, not other AD groups.
8. Once IdM has configured the SP in the IdP, continue with the steps below.
9. In a browser session, re-enter the SAML settings above, **but don't create a new key–use the same key you used the first time.** This time you should **Apply** the changes in Jenkins, but **DO NOT LEAVE** this page.
10. Now, open a different browser (not just a new browser window–open a completely different browser) and navigate to your Jenkins URL. If things have gone right, Cornell Two-Step Login should be invoked as part of the Jenkins login process.
11. If you do not see the Cornell Two-Step Login process, working correctly, go back to your original browser and revert back to whatever authentication you were using before in the Jenkins security configuration. If you don't do that you will have lost access to your Jenkins deployment.