SSO implementation for zebrix

What is Single Sign-On

Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. (source: wikipedia)

Benefits

Benefits of using single sign-on include:

- Mitigate risk for access to 3rd-party sites (user passwords not stored or managed externally)
- Reduce password fatigue from different user name and password combinations
- Reduce time spent re-entering passwords for the same identity
- Reduce IT costs due to lower number of IT help desk calls about passwords

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

(source: wikipedia)

SSO implementation with zebrix

Compatibility

zebrix has been tested with following authentication/SSO protocols/technologies:

- CAS
- OAuth
- SAMLv2
- ADFS

How to enable SSO with zebrix

1. You need to contact zebrix support

2. You have to integrate zebrix metadata in your authentication server

```
<EntityDescriptor entityID="https://auth.zebrix.net"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
<ds:X509Certificate>MIICsDCCAZgCCQCGpnz8YkjxkDANBgkqhkiG9w0BAQUFADAaMRgwFgYD
VQQDDA9h
dXRoLnplYnJpeC5uZXQwHhcNMTcwOTA1MTAzMjE2WhcNMjcwOTA1MTAzMjE2WjAa
MRgwFgYDVQQDDA9hdXRoLnplYnJpeC5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDJWm+DsyZOtWyoPXetbNoFRsfxqs0vunXkZV5lCFOE3IrDGtxV
l+ulGY1R2d0Fy1SAVNdYjXQIHxPwSFRW3G8OjHsrsZwfVHvcCxuySLqxTHXMaM6U
+W7XDiB8zuGTut3C47tPzGh9DLUXKqBRCpfn1pOtzSGLyd8ZQbsE4RfOAcdk0sA1
tX0mi0jiFmy0G1Md/qaBsM4Rq5inAU6A/IBXgE18MWXJYNAIr0vc1O7IGzqfu2KB
gI7opKnxyowXxr192FJ8XizUEte8Q6v+nWS0VaMw/mLoXZGSIiNGtrwkp1TddGpI
ONYzoc8PUGczJtXGjTlOVbirFySnyzaajFklAgMBAAEwDQYJKoZIhvcNAQEFBQAD
ggEBALp4cUX5Geag79iQTYoxlbKPhzzSogRJ7ufLwWOEniC0jmjvxS5nkr2vcXRO
TQqWgpXnbTQWSxdz01prE6NQy9eLWjIgXpCCa+18RCPJvCykFsnKzKGTsQI+/9HF
5HeB6qEmtrzY2QT9Hn30Z4bRma2L6OCYvwHOZz05XOaRyOHFSIBGGfRNOU4iBMRp
PkN+1p+EX07etvsDdZ1UnVg1kZQD6Br3hn3oAUvIctFrctThMd9hSh5GSx1UOhHv
7GfBWQ4Q4tYFOisPreeMgkuan+0x5j1pJwD3Ws2UDwl89lgACS96XmHtsHiwwJBb
I2NhPG6CSSWaSxiAHjyRZIHWPls=</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://auth.zebrix.net/sso/logout"/>
    <AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://auth.zebrix.net/sso/postResponse" index="0"/>
  </SPSSODescriptor>
</EntityDescriptor>
```