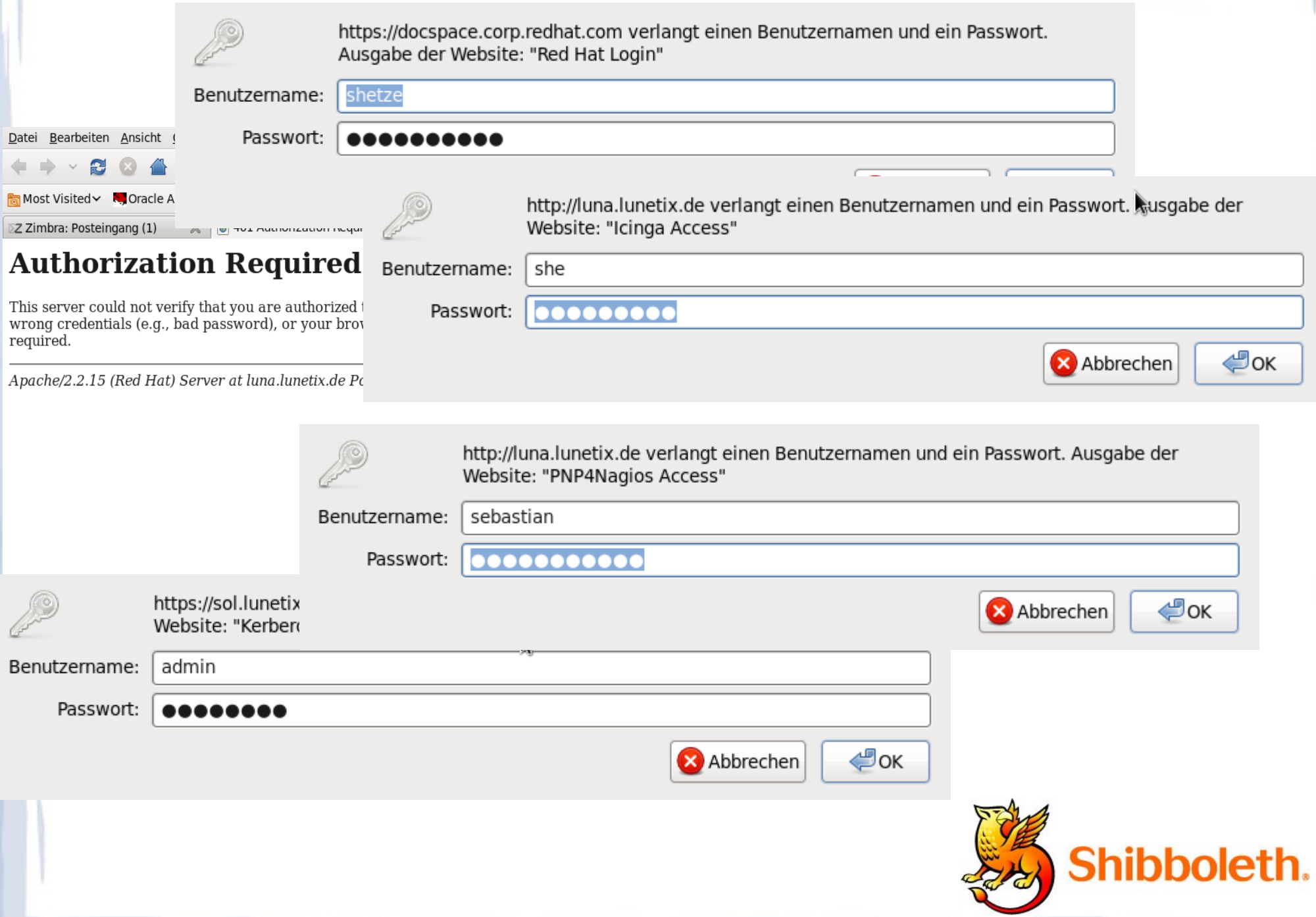
Shibboleth SSO

FFG 2012

Sebastian Hetze <she@lunetix.de>

Shibboleth


https://docspace.corp.redhat.com verlangt einen Benutzernamen und ein Passwort.
Ausgabe der Website: "Red Hat Login"
Benutzername: shetze
Passwort:
Datei Bearbeiten Ansicht
Most Visited
Oracle A
Z Zimbra: Posteingang (1)
Authorization Required
This server could not verify that you are authorized
wrong credentials (e.g., bad password), or your brov
required.
Apache/2.2.15 (Red Hat) Server at luna.lunetix.de Pc
http://luna.lunetix.de verlangt einen Benutzernamen und ein Passwort. usgabe der
Website: "Icinga Access"
Benutzername: she
Passwort:
Abbrechen
OK
http://luna.lunetix.de verlangt einen Benutzernamen und ein Passwort. Ausgabe der
Website: "PNP4Nagios Access"
Benutzername: sebastian
Passwort:
Abbrechen
OK
https://sol.lunetix
Website: "Kerber
Benutzername: admin
Passwort:
Abbrechen
OK
Shibboleth

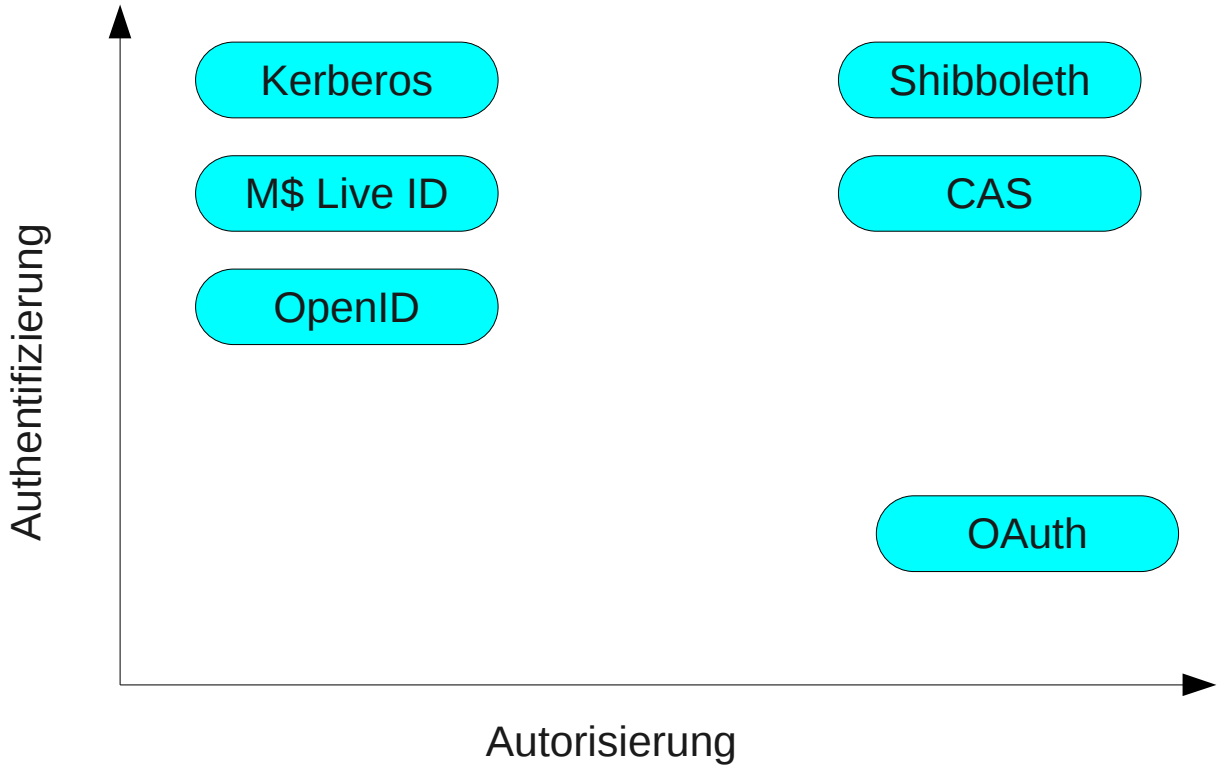
Shibboleth

Requirements

- B2C
  - User Managed Access
  - Shared Resources
  - Privacy
  - Ease of Use
- B2B
  - Org Managed Access
  - Hosted Resources
  - Accountability
  - Integration

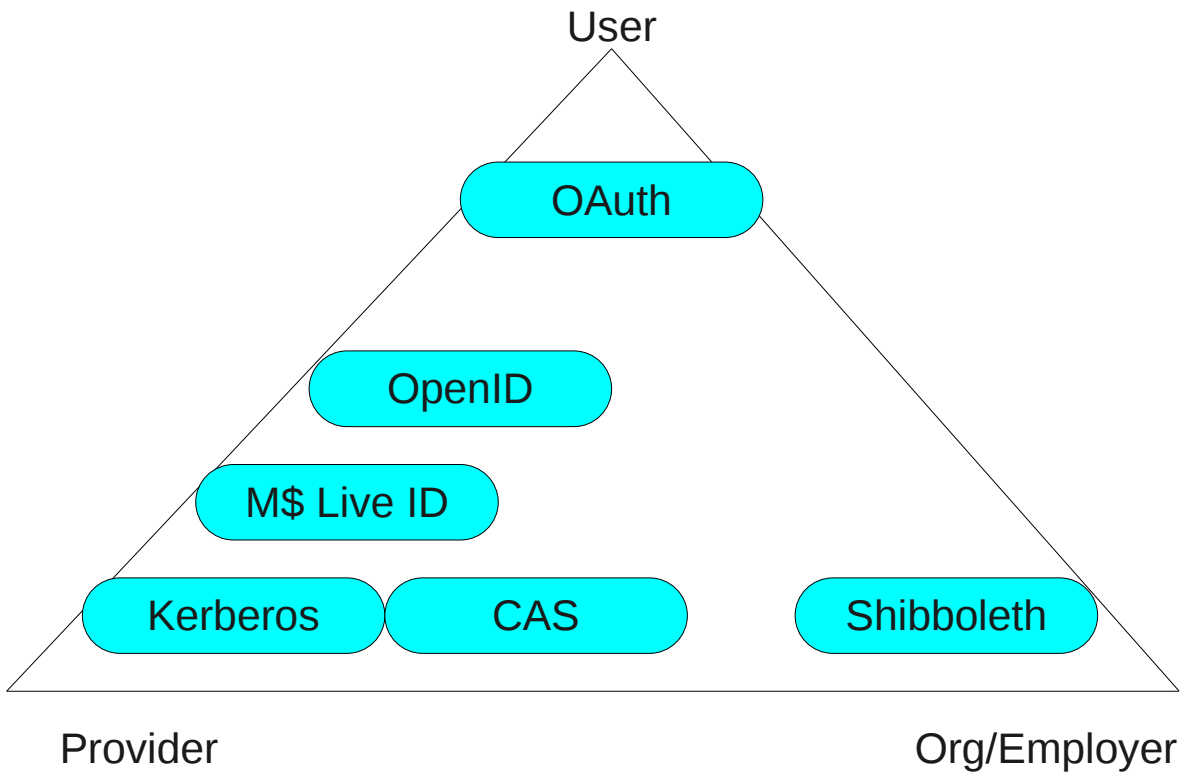
Shibboleth

Access Control



Shibboleth

Resource Control



Shibboleth

Shibboleth

- Projekt gestartet 2000 vom Middleware Architecture Committee for Education (MACE)
- Implementation der OASIS Security Assertion Markup Language (SAML)
- Shibboleth Version 2.x implementiert SAML-2.0

Shibboleth

Was macht SAML?

- Kommunikation zwischen Identity Provider (IdP) und Service Provider (SP)
- IdP ist Asserting Party, SP Relying Party
- Verschiedene Profile, z.B. Web Browser SSO
- Verschiedene Bindings, z.B. HTTP Post
- Assertions bestätigen Identität und Attribute

Shibboleth

Vertrauen und Sicherheit

- Die Beziehung zwischen IdP und SP wird durch den manuell/administrativen Austausch von Metadaten hergestellt
- Absicherung der Kommunikation durch Verschlüsselung und Signatur mit SSL Zertifikaten
- Metadaten identifizieren die Bindings und ordnen einer Partei das öffentliche SSL Zertifikat zu

Shibboleth

Web Browser SSO

- Client ist ein Web-Browser
- SSO bedeutet Herstellung eines persistenten Security Context im Browser
- Realisierung durch Cookies
- Authentifizierung im Apache Webserver

Shibboleth

Workflow

- Ohne gültigen Security Context wird zum IdP weitergeleitet
- Optional zwischenschalten von Discovery Service
- Identity Provider schickt Login-Formular an Browser und führt Login durch
- Ergebnis wird als Assertion zum SP geschickt

Shibboleth

Implementation IdP

- Shibboleth IdP ist Java Application
- Einrichtung der Laufzeitumgebung per install.sh
- Deployment eines idp.war in einen beliebigen Application Server

Shibboleth

Login

- Der IdP hängt sich an einen existierenden Login Mechanismus (LoginHandler): LDAP, AD, Radius, NIS, ...
- Gegebenenfalls Anbindung an JAAS

Shibboleth

Attribute sammeln

- Nach erfolgreicher Authentifizierung sammelt der IdP weitere Informationen (Attribute)
- DataConnector im AttributeResolver stellt die Verbindung z.B. zum LDAP her
- AttributeDefinition legt fest, welche Daten aus welchem Connector gelesen werden

Shibboleth

Attribute ausliefern

- Die gesammelten Attribute werden vom IdP vor dem ausliefern gefiltert
- Anhand von AttributeFilterPolicy und AttributeFilterRule wird festgelegt, welche SPs welche Attribute erhalten
- Die Attribute werden gemeinsam mit der Authentifizierung als Assertion ausgeliefert

Shibboleth

Implementation SP

- Apache Bibliothek mod_shib.so und Shibboleth Dämon shibd
- RPM und DEB Pakete bei Internet2Middleware Initiative erhältlich
- Zertifikate werden automatisch bei der Installation erzeugt
- Metadata muss generiert und mit dem IdP ausgetauscht werden

Shibboleth

Authentifizierung

- Einfach durch Ersetzen der Authentifizierungsmethode durch shibboleth

```
<Directory „/var/www/secure“>
    AuthName „Secure Website Access“
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    Require valid-user
</Directory>
```

Shibboleth

Autorisierung

- Die Attribute werden einfach als Umgebungsvariablen in den Kontext der Applikation gegeben

```
roles = getenv(`entitlement`);
role = strotok(roles,`;`);
if( strcmp(role,access_rule) == 0 ) {
 ...
}
```

Shibboleth

Demo

- Login in Icinga Monitoring Server mit PNP4Nagios
- Konfiguration des IdP
- Konfiguration des SP
- Konfiguration der Applikation

Shibboleth