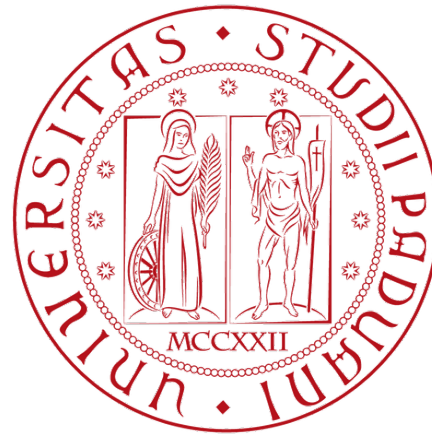


Università degli studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di laurea in Informatica



Autenticazione per Zimbra Collaboration Suite (ZCS) tramite protocollo SAML

Candidato

Francesco De Filippis

Esame di laurea

Padova, 27 Febbraio 2020

Indice

1. Azienda

2. Progetto

3. Resoconto

4. Conclusioni

Zextras

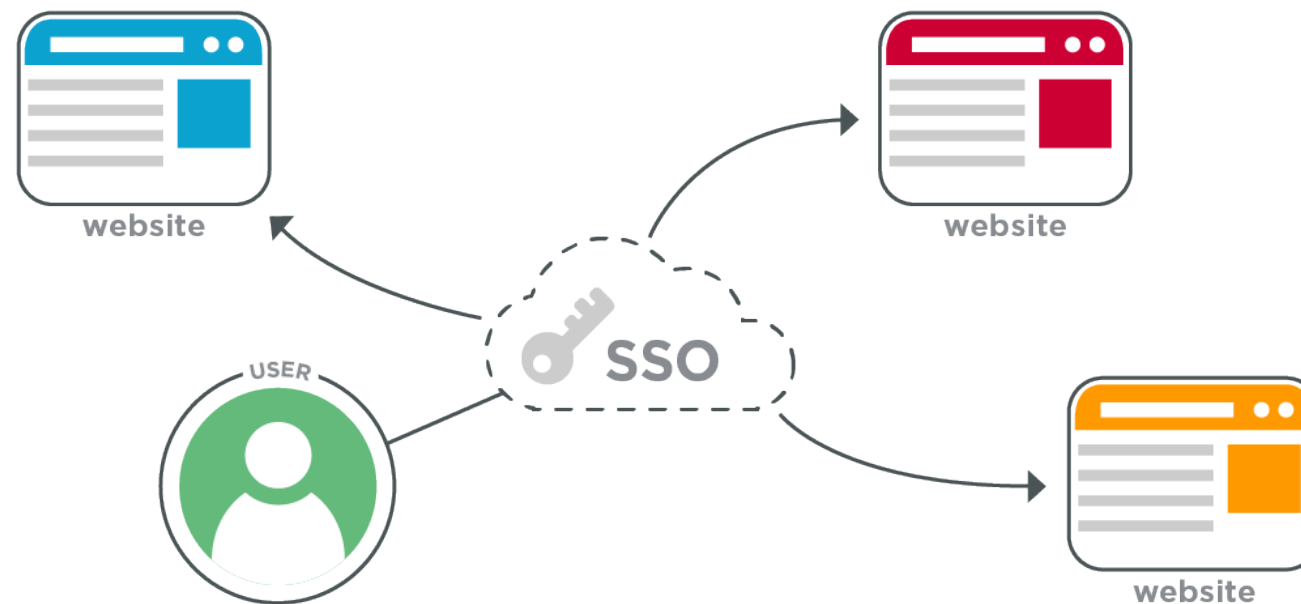
Filosofia Open source



Zimbra Collaboration Suite



SSO (Single Sign-On) personalizzato per ZCS



- * Creazione account Zimbra tramite anagrafica Okta
- * Autenticazione utente Zimbra tramite Okta
- * Mappatura classe di servizio Zimbra con gruppi Okta
- * Mappatura liste di distribuzione Zimbra con gruppi Okta

Protocolli di autenticazione: analisi stato dell'arte

- * Ricerca dei protocolli più diffusi
- * Individuazione dei loro casi d'uso
- * Valutazione vantaggi e svantaggi
- * Scelta del protocollo adeguato



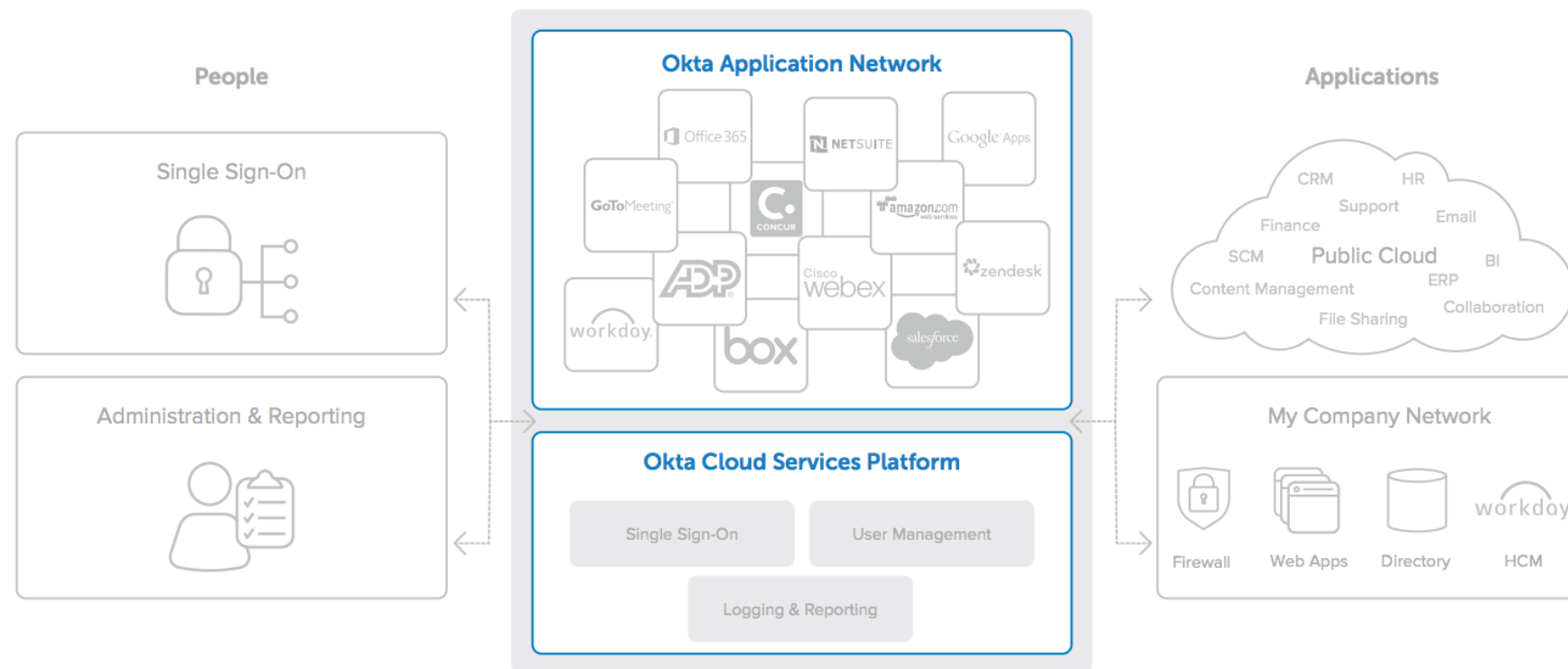
Protocollo scelto



Motivazioni

- * Protocollo diffuso e collaudato
- * Supportato dall'*IdP* Okta utilizzato per l'autenticazione ai servizi aziendali
- * Libreria *open source* per il *parsing* delle Assertion

Applicazione Okta



Okta: Managing Access across Any Application, Device or Person

- * Applicazione SAML ad hoc
- * Configurazione semplice ed essenziale
- * Comunica con l'esterno tramite *endpoint URL*

Handler HTTP

Comunicazione con l'applicazione SAML

SAML Settings		ATTRIBUTE STATEMENTS		
GENERAL		Name	Name Format	Value
Single Sign On URL	https://infra-fa2ac108.testarea.zextras.com/zx/sso/login?domain=zextras.com	firstName	Unspecified	user.firstName
Recipient URL	https://infra-fa2ac108.testarea.zextras.com/zx/sso/login?domain=zextras.com	lastName	Unspecified	user.lastName
Destination URL	https://infra-fa2ac108.testarea.zextras.com/zx/sso/login?domain=zextras.com	email	Unspecified	user.email
Audience Restriction	https://infra-fa2ac108.testarea.zextras.com/zx/sso/login?domain=zextras.com	login	Unspecified	user.login
		GROUP ATTRIBUTE STATEMENTS		
		Name	Name Format	Filter
		Group	Basic	Matches regex: .*

- * Classe Java in ascolto su uno o più *endpoint*
- * Dati utente da Okta tramite *SAML Assertion*
- * *Parsing SAML Assertion*
- * Creazione *account* Zimbra tramite dati Okta
- * Mappatura gruppi Okta con classe di servizio Zimbra
- * Mappatura gruppi Okta con liste di distribuzione Zimbra
- * Autenticazione tramite *cookie* impostato sul dominio della *webmail*

Mappatura classe di servizio

```
{  
  "zextras": "zextrasCos",  
  "developers": "dev"  
}
```

- * L'utente su Okta appartiene a più gruppi
- * L'utente su Zimbra possiede una sola classe di servizio
- * Associazione 1:1 tra gruppo Okta e classe di servizio Zimbra
- * Un utente con più gruppi mappati non viene assegnato a nessuna classe di servizio

Mappatura liste di distribuzione

```
{  
  "commercial": ["commercial@fa2ac108.testarea.zextras.com", "commercial@zextras.com"],  
  "developers": ["developers@fa2ac108.testarea.zextras.com", "developers@zextras.com"],  
  "zextras": ["zextras@fa2ac108.testarea.zextras.com", "zextras@zextras.com"],  
  "manager": ["manager@fa2ac108.testarea.zextras.com"],  
  "interns": ["interns@fa2ac108.testarea.zextras.com", "interns@zextras.com"]  
}
```

- * L'utente su Okta appartiene a più gruppi
- * L'utente su Zimbra può appartenere a più liste di distribuzione
- * Associazione 1:N tra gruppo Okta e liste di distribuzione Zimbra
- * Sincronizzazione ad ogni *login* tramite *SAML*

Configurazione Zimbra

* **Configurazione SAML**

- Attributo di tipo *JSON* per i dati necessari al funzionamento del protocollo

* **Configurazione mappatura classe di servizio**

- Attributo di tipo *JSON* per specificare l'associazione gruppi-classe di servizio

* **Configurazione mappatura liste di distribuzione**

- Attributo di tipo *JSON* per specificare l'associazione gruppi-liste di distribuzione

* ***Provisioning***

- Attributo di binario per attivare/disattivare la creazione automatica dell'*account*
- Configurabile globalmente o per dominio

* **Sincronizzazione liste di distribuzione**

- Attributo di tipo binario attivare/disattivare la sincronizzazione all'accesso
- Configurabile globalmente, per classe di servizio o per *account*

SAML Assertion

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema"
    [...]
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

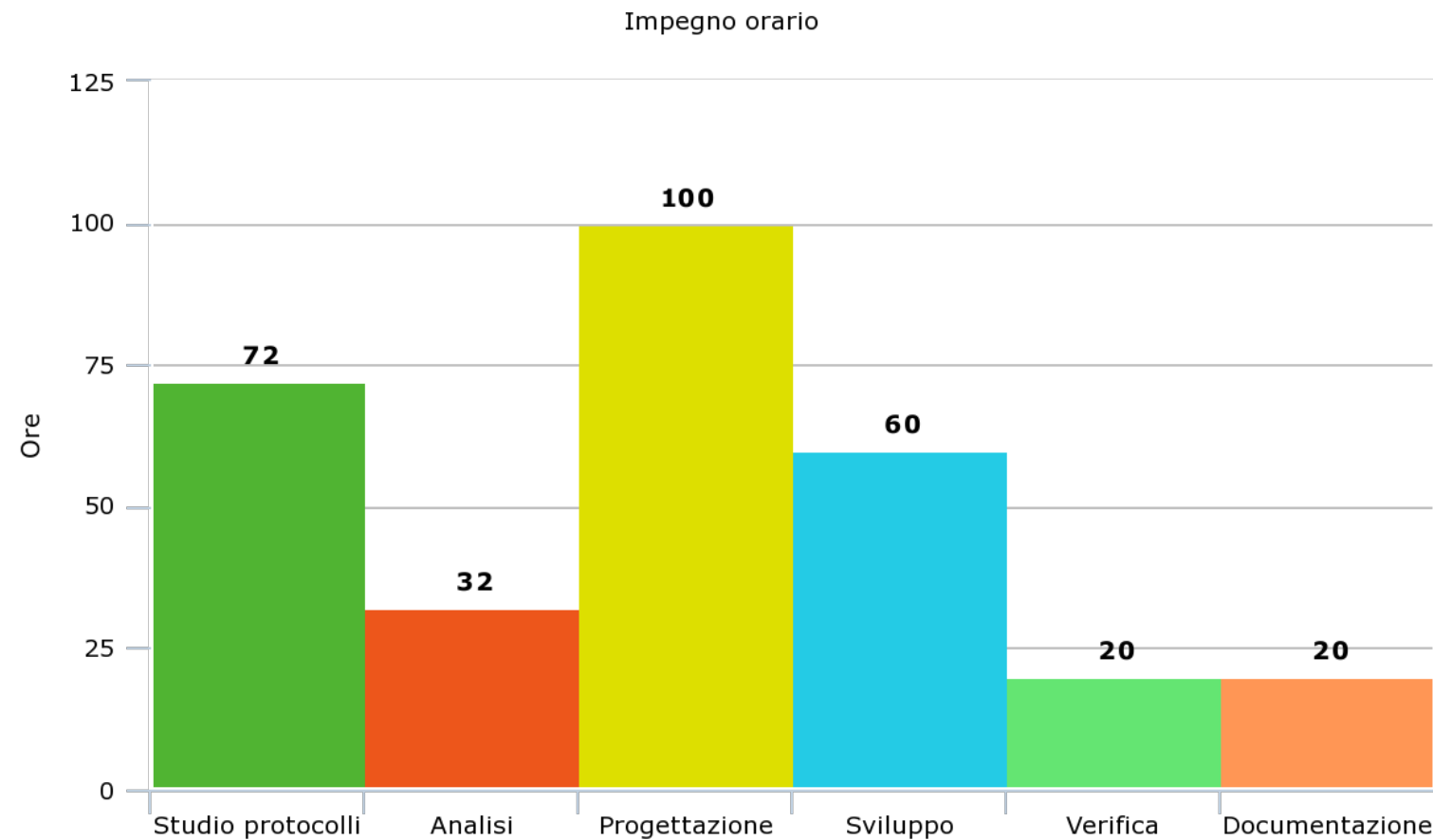
- * Libreria *Java-saml* per il parsing della *SAML Assertion*
- * Integrata nell'handler *HTTP*
- * Adattamento richieste e risposte *HTTP* da *java servlet* a *Netty*
- * Estrapolazione dati utente da *Okta*

Rilascio

- * 6/12/2019
 - Validazione prodotto
 - Sistemazioni pre-release
- * 11/12/2019
 - Release
 - Primo utilizzo aziendale
- * 11/12/2019 - 17/12/2019
 - Sistemazioni post-release



Bilancio finale



- * **Requisiti soddisfatti:** 94% (16/17)
- * **Test superati:** 100% (27/27)
- * **Documenti prodotti:** 3 (e documentazione del codice)
- * **SLOC:** ~1500