SiteMinder – Raccordement Sharepoint

Fonctionnalités de l'agent SiteMinder pour Sharepoint

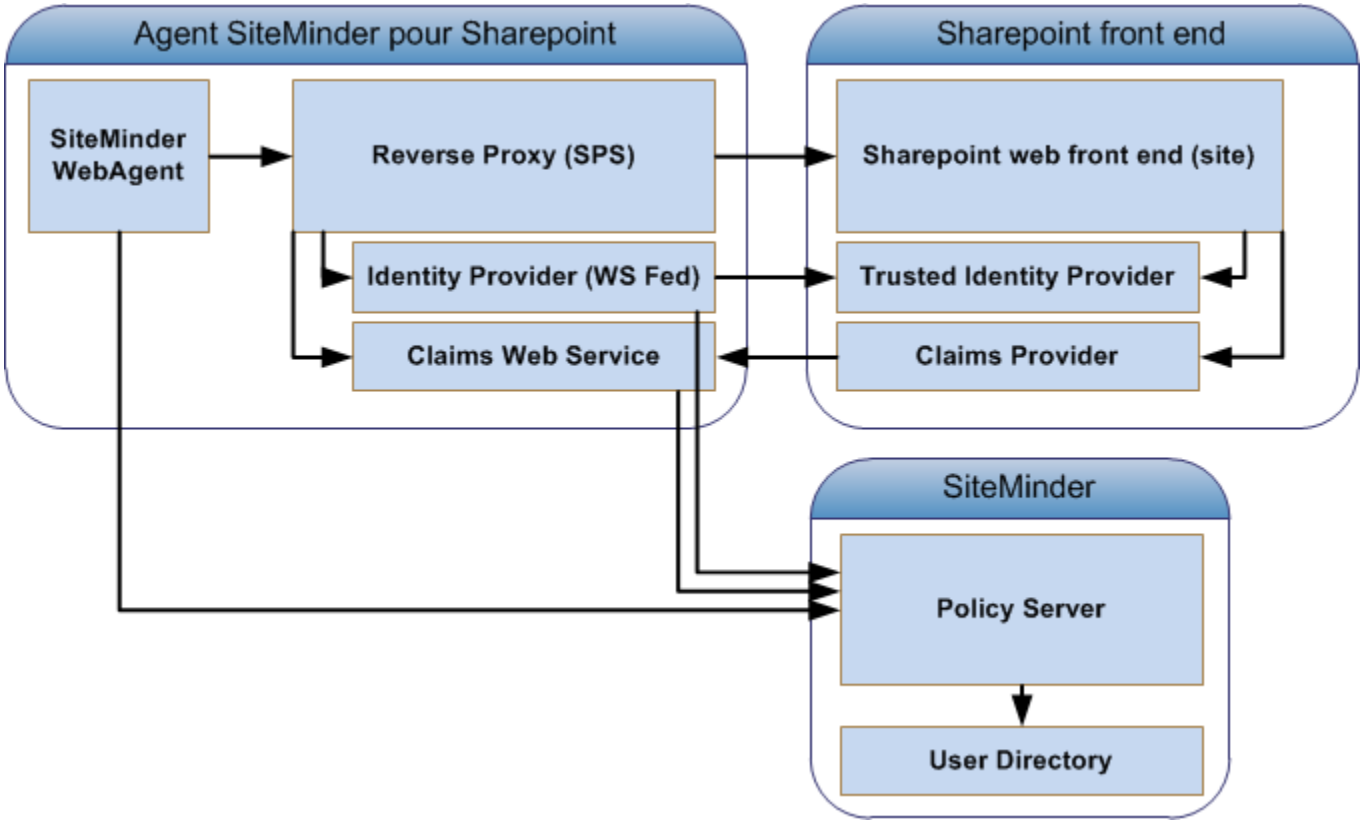
- Authentification des utilisateurs et partage de l'identité avec Sharepoint.
- Prise en charge des requêtes de recherches de groupes et d'utilisateurs pour les claims SiteMinder.

- Routage des flux frontaux Sharepoint.
- Sécurisation des flux Sharepoint en liant le claims Sharepoint à la session SiteMinder.

SiteMinder – Raccordement Sharepoint
Composants de l'agent SiteMinder pour Sharepoint

- L'agent SiteMinder se compose:
  - D'un Reverse Proxy (Secure Proxy Server) en charge de focaliser et de router les flux frontaux.
  - D'un IdP (Identity Provider) en charge d'identifier l'utilisateur et de générer une assertion en fonction de celle-ci.
  - D'un Claims Provider (People Picker) en charge traiter les requêtes de recherches de groupes et d'utilisateurs provenant de SharePoint.

SiteMinder – Raccordement Sharepoint
Schéma de principe



SiteMinder – Raccordement Sharepoint
Gestion des authentification & autorisations Sharepoint

— Depuis Sharepoint 2010, Sharepoint repose sur la notion d'authentification « Claims-based authentication » reposant lui-même sur la brique « Windows Identity Foundation (WIF) »

— L'implémentation du « Claims based Provider » utilise le standard WS-Fed pour consommer l'identité fournie par un tiers.

— Les autorisations et la publication des contenus Sharepoint sont exclusivement liées aux claims. Lors d'une tentative d'accès à un contenu soumis à autorisations, Sharepoint recherche le claims de l'utilisateur. Si aucun claims n'existe pour l'utilisateur Sharepoint applique le schéma d'authentification. Ceci est vrai quelque soit le client (browser ou client lourd).

— L'intégration entre SiteMinder Sharepoint consiste à transmettre une identité issue de l'identification par SiteMinder à Sharepoint. Sharepoint génère un Claims après validation de la preuve d'authentification.

SiteMinder – Raccordement Sharepoint
Format d'un claims Sharepoint

<IdentityClaim>:0<ClaimType><ClaimValueType><AuthMode>l<OriginalIssuer (optional)>l<ClaimValue>

<IdentityClaim> indicates the type of claim and is the following:
- "**i**" for an identity claim
- "**c**" for any other claim

<ClaimType> indicates the format for the claim value and is the following:
- "**#**" for a user logon name
- "**.**" for an anonymous user
- "**5**" for an email address
- "**!**" for an identity provider
- "**+**" for a Group security identifier (SID)
- "-" for a role
- "**%**" for a farm ID
- "**?**" for a name identifier
- "****" for a private personal identifier (PPID)

<ClaimValueType> indicates the type of formatting for the claim value and is the following:
- "**.**" for a string
- "**+**" for an RFC 822-formatted name

<AuthMode> indicates the type of authentication used to obtain the identity claim and is the following:
- "**w**" for Windows claims (no original issuer)
- "**s**" for the local SharePoint security token service (STS) (no original issuer)
- "**t**" for a trusted issuer
- "**m**" for a membership issuer
- "**r**" for a role provider issuer
- "**f**" for forms-based authentication
- "**c**" for a claim provider

<OriginalIssuer> indicates the original issuer of the claim.
<ClaimValueType> indicates the value of the claim in the <ClaimType> format.

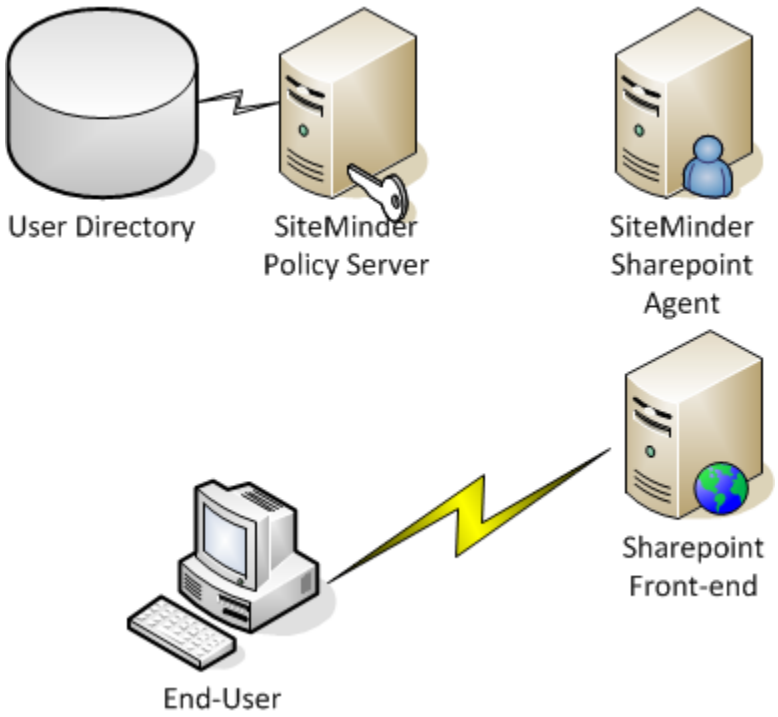
SiteMinder – Raccordement Sharepoint
Implémentations possibles

- Déploiement de l'agent SiteMinder pour Sharepoint en mode IdP STS.
- Déploiement de l'agent SiteMinder pour Sharepoint en mode Reverse Proxy.
  - Avec ou sans Session Linker

SiteMinder – Raccordement Sharepoint
Architecture en mode IdP STS

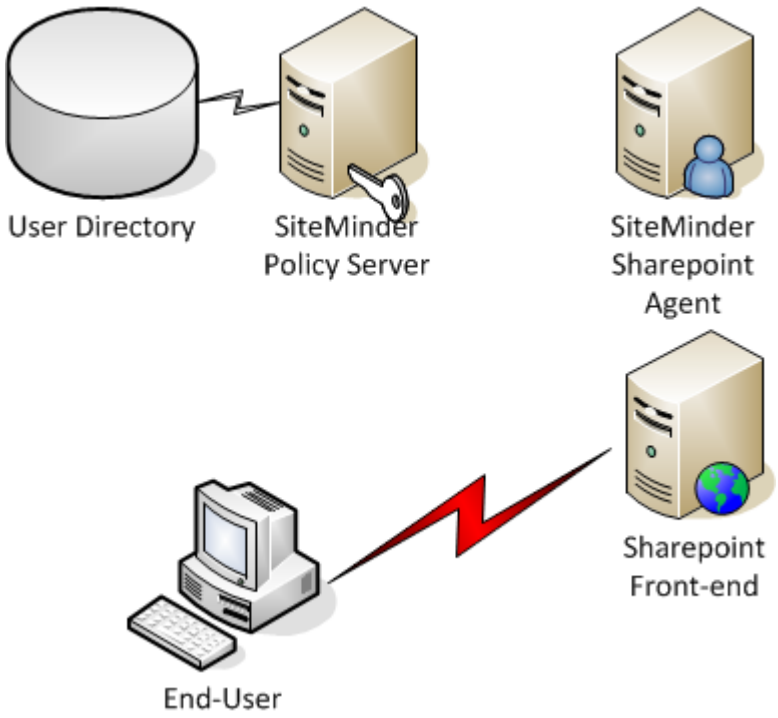
- L'agent SiteMinder n'agit pas en mode proxy, seul le flux d'authentification et Claims Web Service transite par l'agent. Une fois l'authentification procédée, les flux Sharepoint transitent directement sur le Front-end.
  - L'agent SiteMinder ne procède à aucune évaluation de règle d'autorisation.
  - Cette implémentation permet de déployer un agent sur chaque Front-end ou de déployer une ferme agent pour tous les Front-ends.
  - La présence d'un claims persistent n'est pas controlable.

SiteMinder – Raccordement Sharepoint
Architecture en mode IdP STS



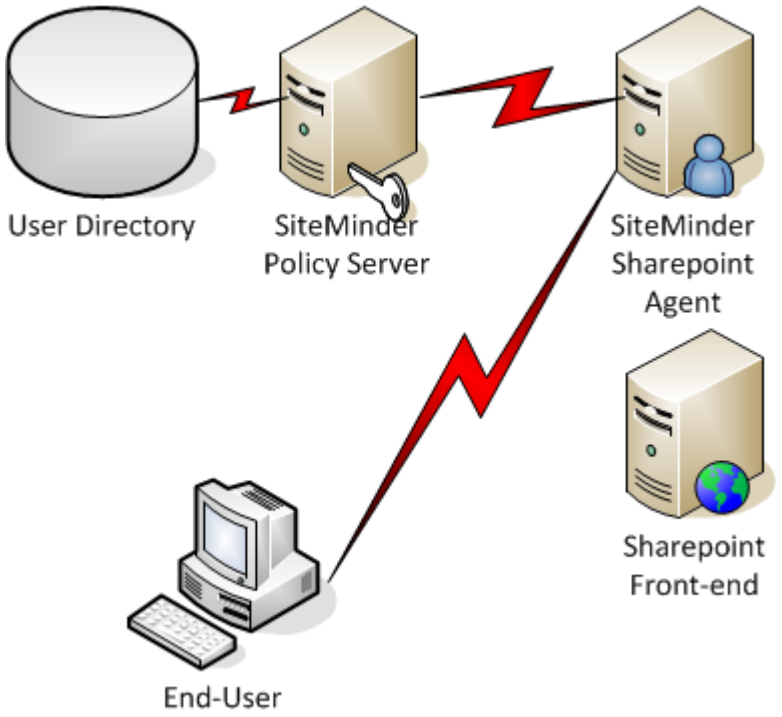
- L'utilisateur se connecte sur Sharepoint sur un contenu publique.
- Sharepoint publie le contenu sans demande d'authentification.

SiteMinder – Raccordement Sharepoint
Architecture en mode IdP STS



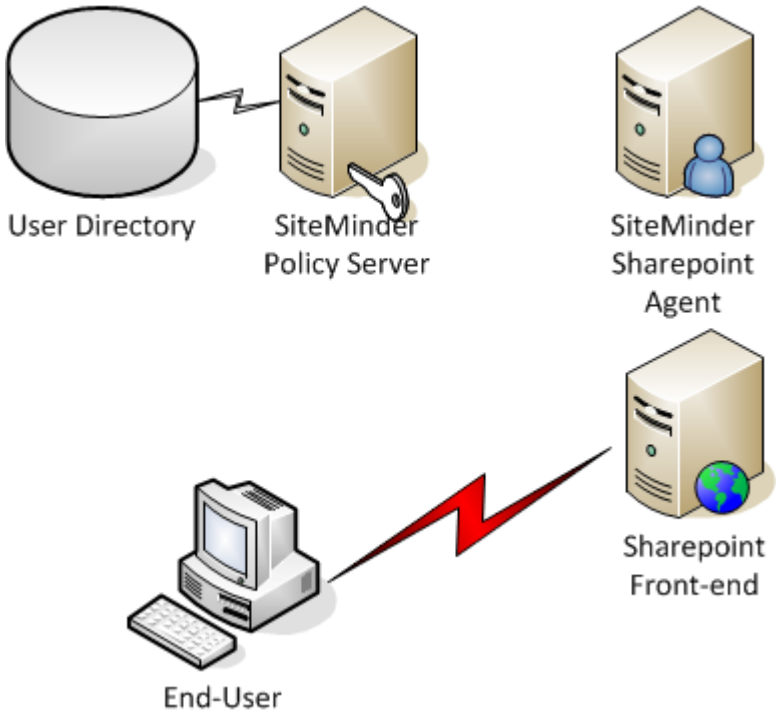
- L'utilisateur se connecte sur Sharepoint sur un contenu soumis à autorisations.
- Sharepoint recherche un Claims pour l'utilisateur en interrogeant le cookie FedAuth.
- Si le Claims est valide et que l'identité correspond à une autorisation, le contenu est publié.
- Sinon, Sharepoint invoque le schéma d'authentification configuré pour le site

SiteMinder – Raccordement Sharepoint
Architecture en mode IdP STS



- Sharepoint redirige l'utilisateur l'Identity Provider configuré dans son objet « trusted authentication provider ».
- L'agent SiteMinder pour Sharepoint interroge le Policy Server pour évaluer la politique de partenariat entre SiteMinder et le site Sharepoint.
- Il recherche l'identité SiteMinder en extraient le cookie SMSession. Dans le cas où la session ne dispose pas cookie SiteMinder, il procède à l'authentification de l'utilisateur.

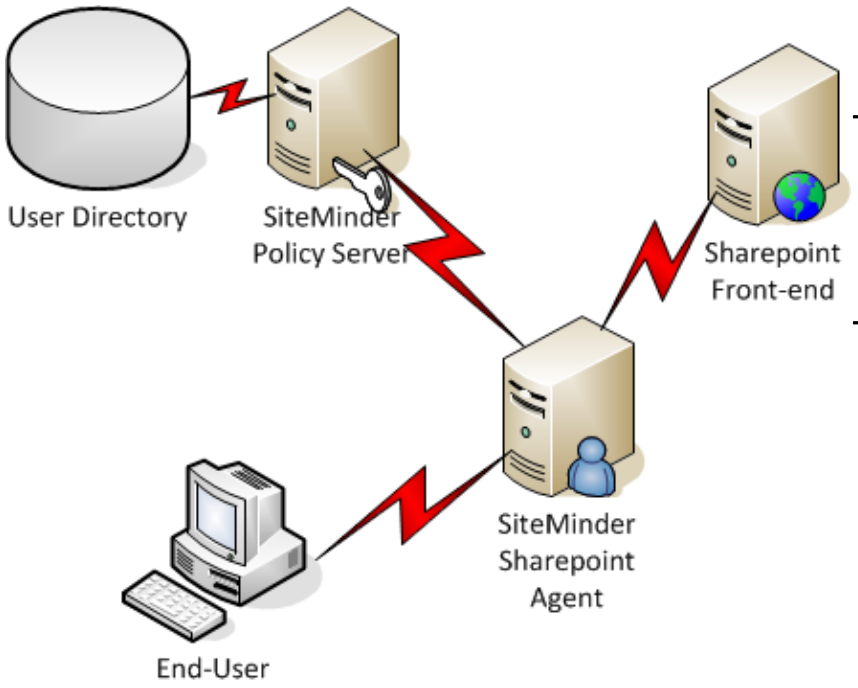
SiteMinder – Raccordement Sharepoint
Architecture en mode IdP STS



- Une fois l'utilisateur désambigué et autorisé à se connecter à Sharepoint, l'agent SiteMinder génère une assertion WS-Fed contenant l'identité de l'utilisateur.
- L'assertion est chiffrée & signée avec les certificats configurés dans le partenariat WS-Fed (coté Policy Server) et dans le « trusted authentication provider » (coté Sharepoint).
- Le « trusted authentication provider » valide la conformité de l'assertion et construit un claims sur cette base.

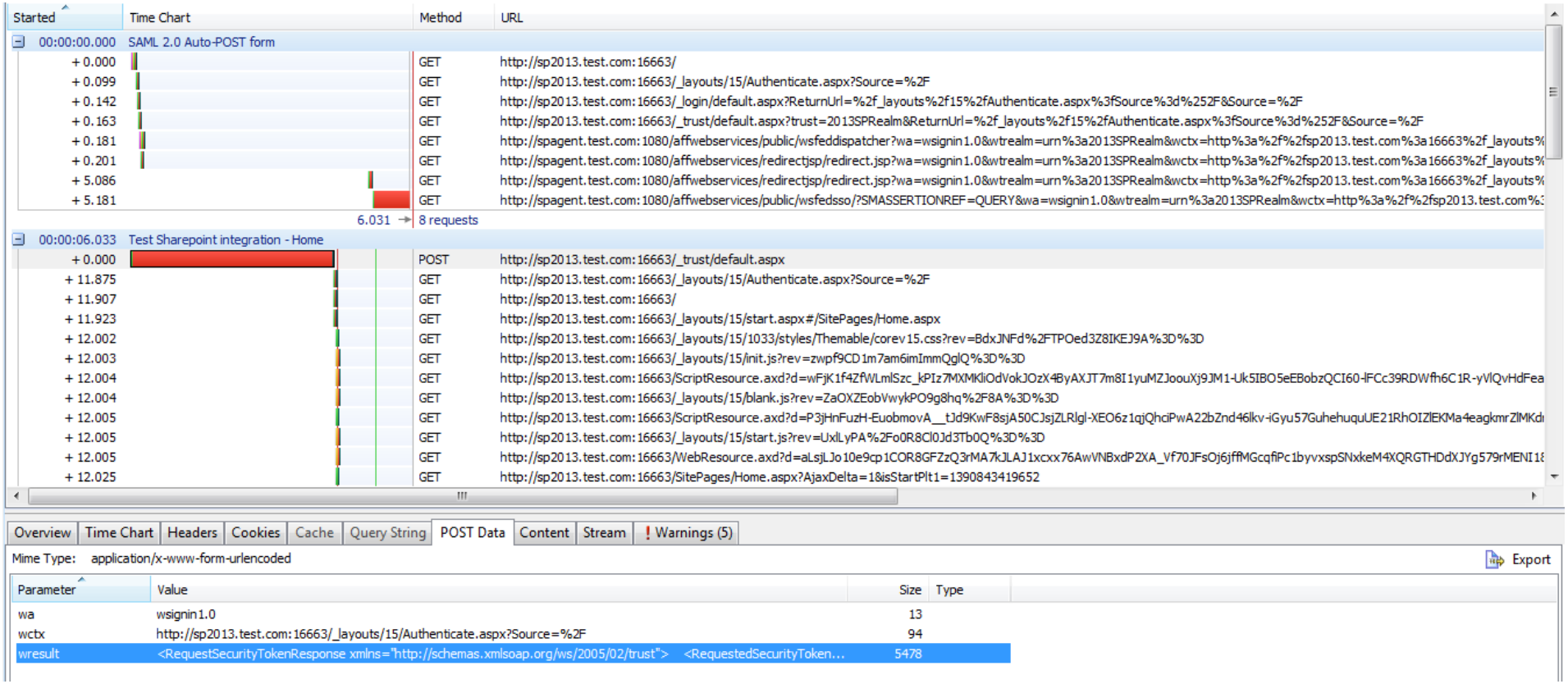
  Ex: i:0?.tl2013sprealmllalfr01
- Une fois le claims généré, le flux transite entre le navigateur et le Front-end Sharepoint.

SiteMinder – Raccordement Sharepoint
Architecture en mode Proxy



- La procédure d'authentification est similaire dans une architecture proxy à la différence près que tous les flux transitent par l'agent SiteMinder pour Sharepoint.
- Il est donc possible de contrôler le flux entre les clients (browser ou lourd et les Front-end Sharepoint)
- L'utilisation du module « session linker » permet de lier la session SiteMinder (SMSession) avec le claims Sharepoint (FedAuth). L'apparition d'une incohérence dans ce couple de session entraine la déstruction des deux sessions. Ce qui conduit à ré-authentifier l'utilisateur tant sur SiteMinder que sur Sharepoint.

SiteMinder – Raccordement Sharepoint
Flow d'authentification



Started	Time Chart	Method	URL
00:00:00.000	SAML 2.0 Auto-POST form		
+ 0.000		GET	http://sp2013.test.com:16663/
+ 0.099		GET	http://sp2013.test.com:16663/_layouts/15/Authenticate.aspx?Source=%2F
+ 0.142		GET	http://sp2013.test.com:16663/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
+ 0.163		GET	http://sp2013.test.com:16663/_trust/default.aspx?trust=2013SPRealm&ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
+ 0.181		GET	http://spagent.test.com:1080/affwebservices/public/wsfeddispatcher?wa=wsignin1.0&wtrealm=urn%3a2013SPRealm&wctx=http%3a%2f%2fsp2013.test.com%3a16663%2f_layouts%
+ 0.201		GET	http://spagent.test.com:1080/affwebservices/redirectjsp/redirect.jsp?wa=wsignin1.0&wtrealm=urn%3a2013SPRealm&wctx=http%3a%2f%2fsp2013.test.com%3a16663%2f_layouts%
+ 5.086		GET	http://spagent.test.com:1080/affwebservices/redirectjsp/redirect.jsp?wa=wsignin1.0&wtrealm=urn%3a2013SPRealm&wctx=http%3a%2f%2fsp2013.test.com%3a16663%2f_layouts%
+ 5.181		GET	http://spagent.test.com:1080/affwebservices/public/wsfedsso/?SMASSERTIONREF=QUERY&wa=wsignin1.0&wtrealm=urn%3a2013SPRealm&wctx=http%3a%2f%2fsp2013.test.com%3
	6.031 → 8 requests		
00:00:06.033	Test Sharepoint integration - Home		
+ 0.000		POST	http://sp2013.test.com:16663/_trust/default.aspx
+ 11.875		GET	http://sp2013.test.com:16663/_layouts/15/Authenticate.aspx?Source=%2F
+ 11.907		GET	http://sp2013.test.com:16663/
+ 11.923		GET	http://sp2013.test.com:16663/_layouts/15/start.aspx#/SitePages/Home.aspx
+ 12.002		GET	http://sp2013.test.com:16663/_layouts/15/1033/styles/Themable/corev15.css?rev=BdxJNFd%2FTPOed3Z8IKEJ9A%3D%3D
+ 12.003		GET	http://sp2013.test.com:16663/_layouts/15/init.js?rev=zwpf9CD1m7am6imImmQglQ%3D%3D
+ 12.004		GET	http://sp2013.test.com:16663/ScriptResource.axd?d=wFjK1f4ZfWLmlSzc_kPIz7MXMKliOdVokJOzX4ByAXJT7m8I1yuMZJoouXj9JM1-Uk5IBO5eEBobzQCI60-lFCc39RDWfh6C1R-yVlQvHdFea
+ 12.004		GET	http://sp2013.test.com:16663/_layouts/15/blank.js?rev=ZaOXZEobVwykPO9g8hq%2F8A%3D%3D
+ 12.005		GET	http://sp2013.test.com:16663/ScriptResource.axd?d=P3jHnFuzH-EuobmovA__tJd9KwF8sjA50CJsjZLRlgl-XEO6z1qjQhciPwA22bZnd46lkv-iGyu57GuhehuquUE21RhOIZlEKMa4eagkmrZlMKd
+ 12.005		GET	http://sp2013.test.com:16663/_layouts/15/start.js?rev=UxlLyPA%2Fo0R8Cl0Jd3Tb0Q%3D%3D
+ 12.005		GET	http://sp2013.test.com:16663/WebResource.axd?d=aLsjLJo10e9cp1COR8GFZzQ3rMA7kJLAJ1xcxx76AwVNBxdP2XA_Vf70JFsOj6jffMGcqfiPc1byvxspSNxkeM4XQRGTHDdXJYg579rMENI18
+ 12.025		GET	http://sp2013.test.com:16663/SitePages/Home.aspx?AjaxDelta=1&isStartPlt1=1390843419652

Overview | Time Chart | Headers | Cookies | Cache | Query String | POST Data | Content | Stream | ! Warnings (5)

Mime Type: application/x-www-form-urlencoded

Export

Parameter	Value	Size	Type
wa	wsignin1.0	13	
wctx	http://sp2013.test.com:16663/_layouts/15/Authenticate.aspx?Source=%2F	94	
wresult	<RequestSecurityTokenResponse xmlns="http://schemas.xmlsoap.org/ws/2005/02/trust"> <RequestedSecurityToken...	5478	

ca technologies

SiteMinder – Raccordement Sharepoint
Demo

