.conf2015

Securing Splunk with Single Sign On & SAML

Nachiket Mistry

Sr. Software Engineer, Splunk

Rama Gopalan

Sr. Software Engineer, Splunk

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

"Through 2016, Federated Single Sign-On Will Be the Predominant SSO Technology, Needed by 80 Percent of Enterprises."

- Gartner

Rama Gopalan

- Sr. Software Engineer
- 5+ Years with Splunk
- rgopalan@splunk.com

Nachiket Mistry

- Sr. Software Engineer
- 3+ Years with Splunk
- 5 Major Releases
- 50+ Maintenance Releases
- nmistry@splunk.com

Agenda

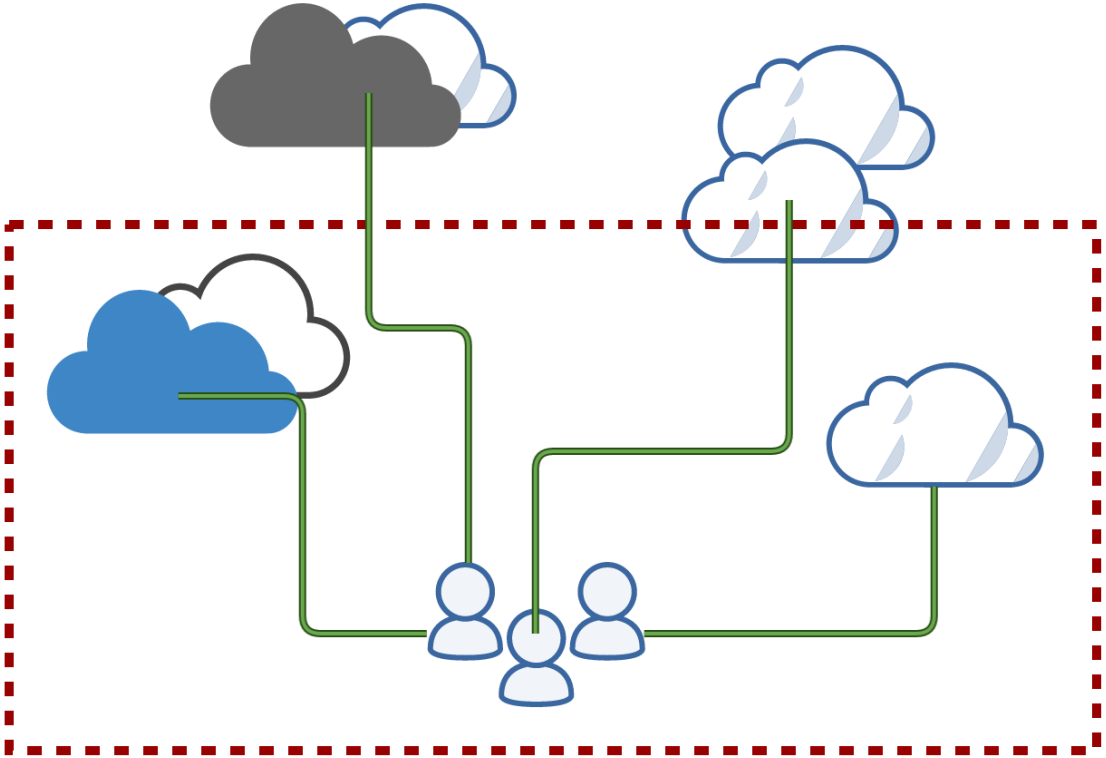
- Why Single Sign On (SSO)
- Splunk SSO
- Splunk SSO with SAML

Wikipedia on Single Sign On

Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in with a **single** ID to gain access to connected systems without being prompted for different usernames or passwords, or in some configurations seamlessly **sign on** at each system.

Single sign-on - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/**Single_sign-on** Wikipedia

More about Single sign-on



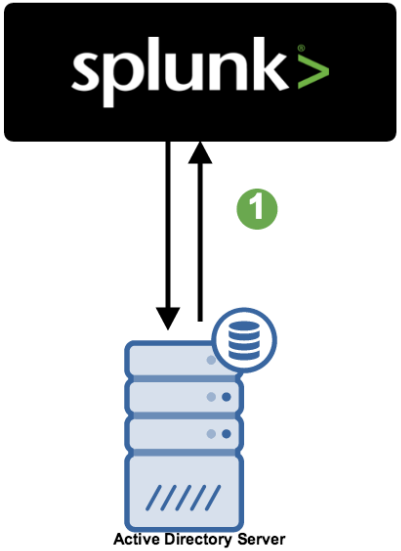
Why Single Sign On (SSO)

- Reduce administration
- Time savings for users
- Increase user adoption
- Increased security

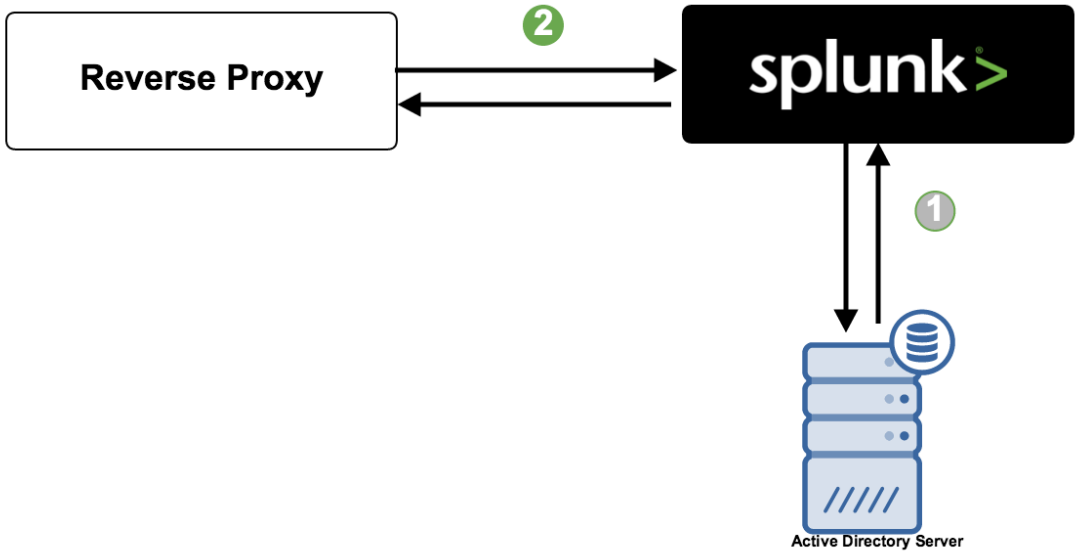
Configuring Splunk SSO

4 Step Process

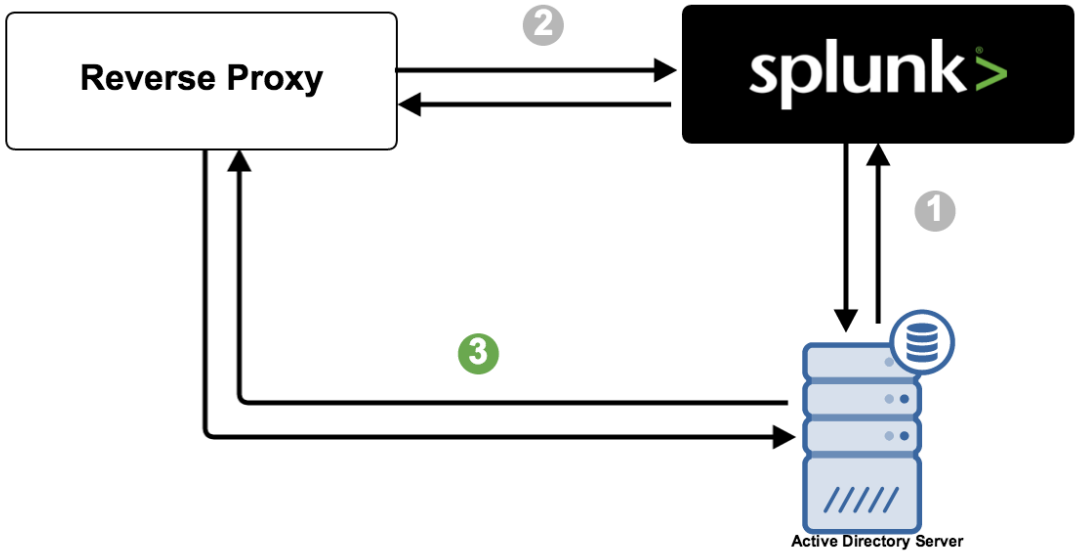
Configuring SSO in Splunk



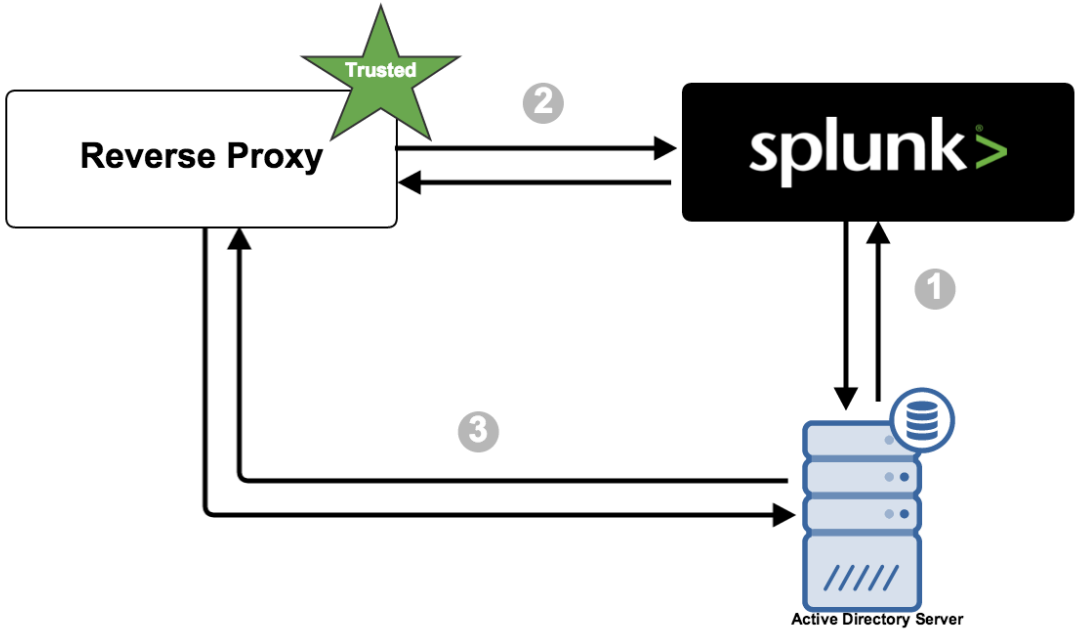
Configuring SSO in Splunk



Configuring SSO in Splunk

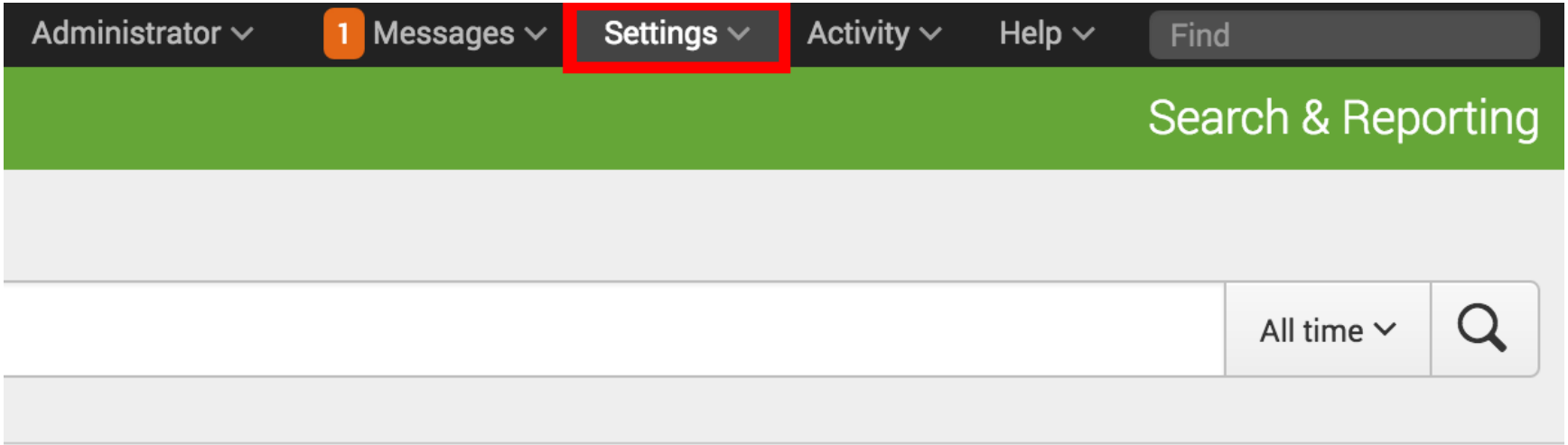


Configuring SSO in Splunk

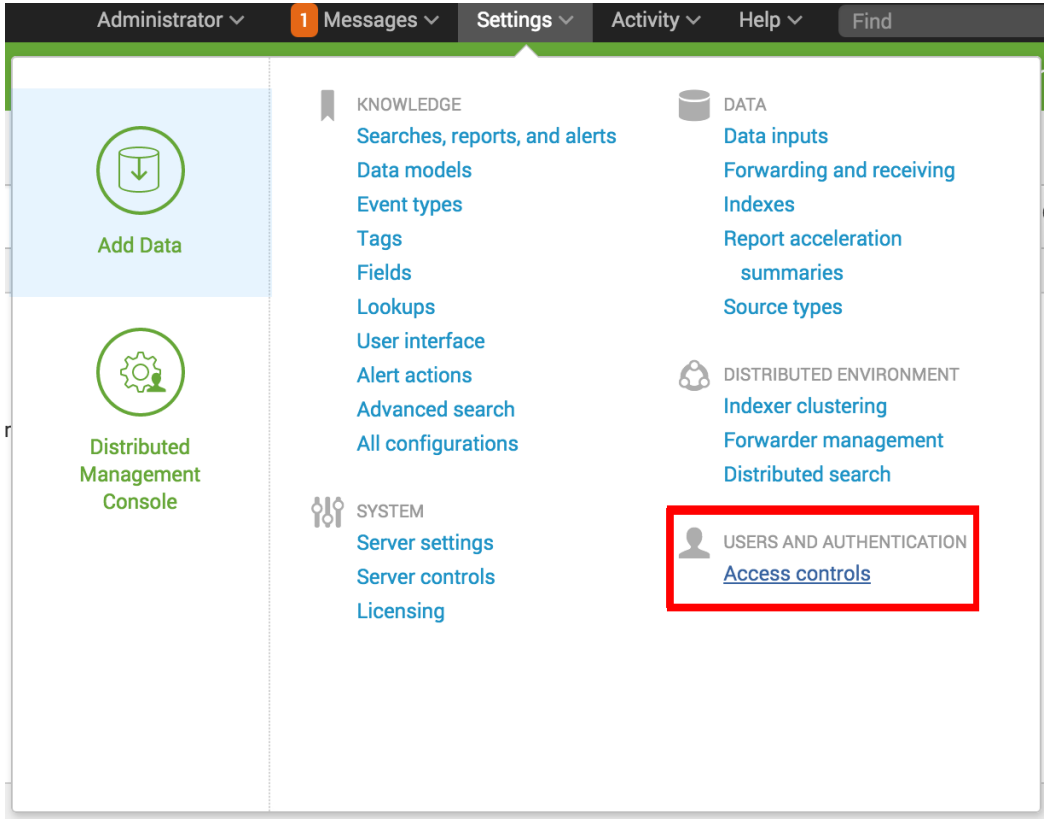


1: Configuring LDAP

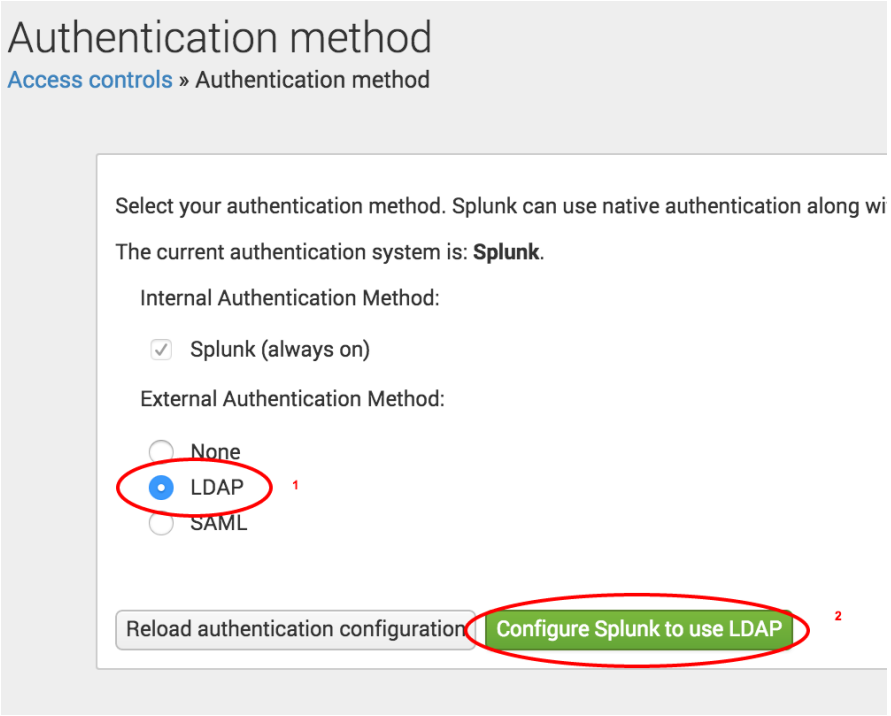
Configuring LDAP



Configuring LDAP



Configuring LDAP



Configuring LDAP

splunk> Apps Administrator 1 Messages Settings Activity Help Find

Add new

Access controls » Authentication method » LDAP strategies » Add new

LDAP strategy name *

OpenLDAP

Enter a unique name for this strategy.

LDAP connection settings

Host *

myldaphost.splunk.com

Your Splunk server must be able to resolve this host.

Port

389

The LDAP server port defaults to 389 if you are not using SSL, or 636 if SSL is enabled.

SSL enabled

You must also have SSL enabled on your LDAP server.

Bind DN

Configuring LDAP

```
$ cat etc/system/local/authentication.conf
[authentication]
authSettings = OpenLDAP
authType = LDAP

[OpenLDAP]
host = myldaphost.splunk.com
nestedGroups = 0
port = 389
bindDN = cn=manager,dc=openldap,dc=splunk,dc=com
...
```

Authorizing LDAP Users

splunk> Apps Administrator 1 Messages Settings Activity Help Find

LDAP strategies

Access controls » Authentication method » LDAP strategies

New

Showing 1-1 of 1 item

Results per page 100

LDAP strategy name	Host	Port	Connection order	Status	Actions
OpenLDAP	myldaphost.splunk.com	389	1	Enabled | Disable	Map groups | Clone | Delete

Authorizing LDAP Users

splunk> Apps Administrator 1 Messages Settings Activity Help Find

LDAP Groups

Access controls » Authentication method » LDAP strategies » LDAP Groups

| « Back to strategies

Showing 1-4 of 4 items

Results per page 100

LDAP Group Name	LDAP Strategy	Group type	Roles
Multi Nested Group	OpenLDAP	static	
Nested Group	OpenLDAP	static	user
Static Help Admin	OpenLDAP	static	admin
Static Sustaining Admin	OpenLDAP	static	admin

Authorizing LDAP Users

Available Roles — add all »

- admin
- can_delete
- power
- splunk-system-role
- user

Selected Roles — « clear all

- admin

LDAP Users

```
uid=Susan_User45380,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User45416,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User45638,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User45915,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User45932,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User45985,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User46784,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User46825,ou=people,dc=openldap,dc=splunk,dc=com
uid=Susan_User46971,ou=people,dc=openldap,dc=splunk,dc=com
```

Cancel | Save

Authorizing LDAP Users

Configuring LDAP

```
$ cat etc/system/local/authentication.conf

. . .

[roleMap_OpenLDAP]
admin = Static  Help Admin;Static  Sustaining Admin
user = Nested Group
```

2: Configuring Reverse Proxy

Configuring Apache as Reverse Proxy

```
$ sudo a2enmod proxy_http


...
ProxyRequests off
ProxyPass / http://mysplunkhost:8000/
ProxyPassReverse / http://mysplunkhost:8000/
...
```

3: Reverse Proxy Handles Authentication

Apache & LDAP

```
$ sudo a2enmod authnz_ldap ldap


...
AuthType Basic
AuthBasicProvider ldap
AuthName ”OpenLDAP”
AuthLDAPURL ldap://myldaphost.splunk.com:389/ou=people,dc=splunk,dc=com
AuthLDAPBindDN "cn=manager,dc=openldap,dc=splunk,dc=com"
AuthLDAPBindPassword ”password"
require valid-user
...
```

Finally: Enable SSO

Set the User Name Header

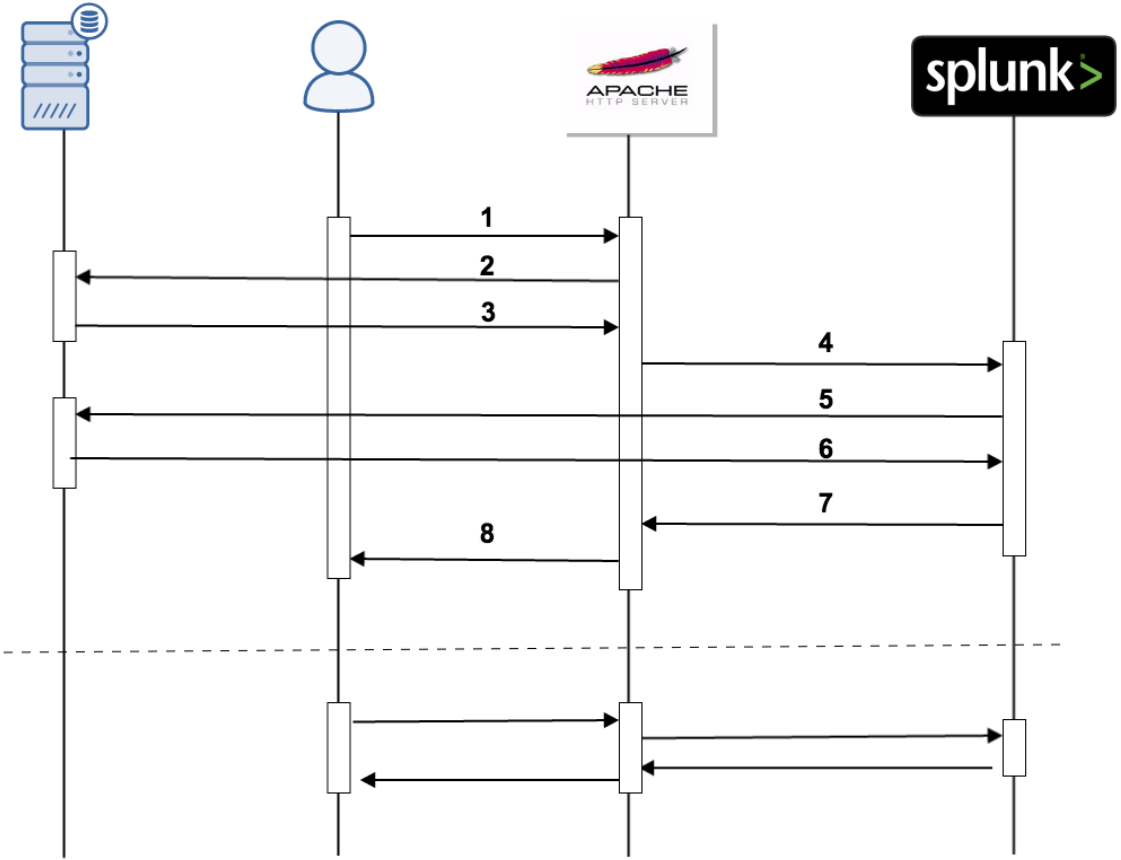
```
$ sudo a2enmod rewrite


...
RewriteEngine on
RewriteRule .* - [E=RU:%{REMOTE_USER}]
RequestHeader set REMOTE_USER %{RU}e
...
```

Enable SSO in Splunk

```
$ cat etc/system/local/server.conf
[general]
trustedIP = 127.0.0.1

$ cat etc/system/local/web.conf
[settings]
trustedIP = 127.0.0.1,10.162.255.123
```


APACHE
HTTP SERVER
splunk>
1
2
3
4
5
6
7
8

Troubleshooting SSO

/debug/sso

SSO settings

SSO Enabled	Yes
splunkd trustedIP	127.0.0.1
splunkweb trustedIP	10.160.255.74, 10.14.0.102, 10.160.255.116, 10.13.6.55, 192.168.42.2, 10.13.6.144, 10.14.0.136
splunkweb SSO Mode	permissive

Splunkweb settings

Host Name	mrt.sv.splunk.com
Host IP	10.1.42.2
Port	6200
Incoming request IP received by splunkweb	10.14.0.136
Is the incoming request IP in splunkweb's list of trustedIPs?	Yes. SSO will be used to authenticate this request.

Troubleshooting SSO

Remote user HTTP header

Remote User HTTP Header	X-REMOTE-USER
Value of X-REMOTE-USER	

Other HTTP headers

Host	mrt:6200
Connection	keep-alive
Cache-Control	max-age=0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4
Accept-Encoding	gzip, deflate, sdch
Accept-Language	en-US,en;q=0.8
Cookie	splunkweb_csrf_token_16230=9230851154214494320; splunkweb_csrf_token_16300=11903724244611128828 session_id_26300=6de25f63d3280ff4869e959c36921fd7d1937387; session_id_6200=d35745fa383550068278 splunkd_6200=kJBVl2Vqmj5t2oACmA4iK6IlRl4^JU^ZLMCgNL9gKNdO1Lpf1UFN6olcL1tROzA731DzneVuQzB28LTntr

Splunk SSO with SAML

SAML 2.0

- Security Assertion Markup Language
- XML based standard for browser based SSO
- Multiple protocols and bindings
- IDP - Identity Provider - Trusted Authority, SP - Service Provider
- IDPs out there – Ping Identity, Okta, OneLogin, Azure

Why SAML?

- Security
  - ❑ Credentials are not stored locally
  - ❑ Standard for Single Sign On
- Multi-Factor authentication

Splunk and SSO

- pre-SAML
- with SAML

[authentication]

authSettings = saml_settings

authType = SAML

Configure Splunk

General Settings

Single Sign On (SSO) URL ? https://qa-systest-01.sv.splunk.com:9031/idp/SSO.saml2

Single Log Out (SLO) URL ? https://qa-systest-01.sv.splunk.com:9031/idp/SLO.saml2

idP's certificate file ? /home/rgopalan/saml-install/etc/auth/ping.crt

Entity ID ? saml-test

Sign AuthnRequest ☑

Sign SAML response ☑

Attribute Query Requests

Attribute query requests are required for scheduled searches.

Attribute query URL ? https://qa-systest-01.sv.splunk.com:9031/idp/attrsvc.ssaml2

Sign attribute query request ☑

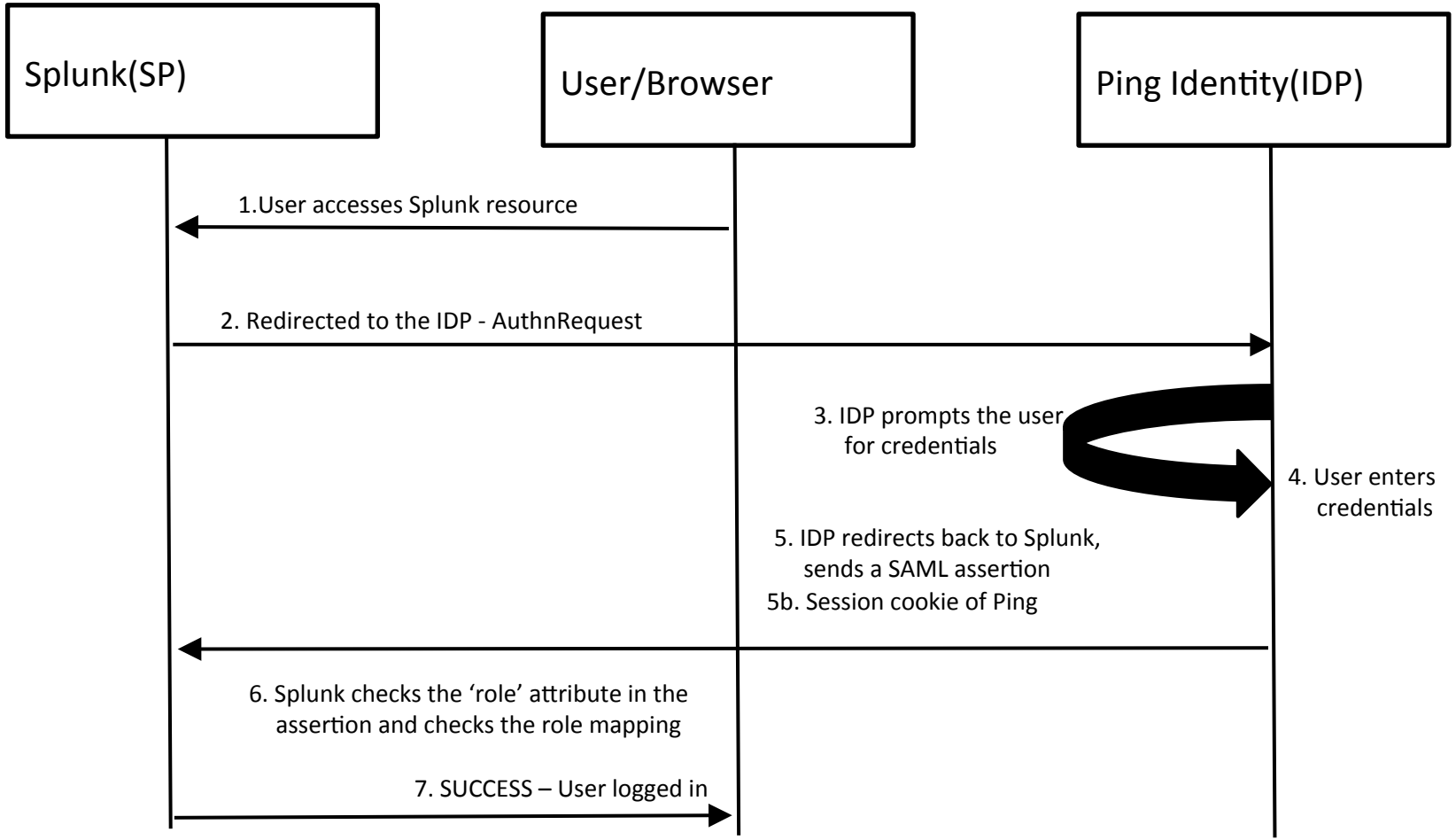
Sign attribute query response ☑

Export SP Metadata

wimpy.splunk.com:9332/saml/spmetadata


```
<md:EntityDescriptor entityID="Splunk-dev-core-rgo-ad" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"> <md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" AuthnRequestsSigned="false"
WantAssertionsSigned="false"> <md:KeyDescriptor> <ds:KeyInfo> <ds:X509Data> <ds:X509Certificate>
MIICLTCCAZYCCQCARwt76UmJHTANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDVNhbiBGcmFuY2lzY28xDzANBgNVBAoT
BlNwbHVuazEXMBUGA1UEAxMOU3BsdW5rQ29tbW9uQ0ExITAfBgkqhkiG9w0BCQEW
EnN1cHBvcnRAc3BsdW5rLmNvbTAeFw0xNDEyMDMwMTExMzhaFw0xNzEyMDIwMTEx
MzhaMDcxIDAeBgNVBAMMF1NwbHVua1NlcnZlckRlZmF1bHRDZXJ0MRMwEQYDVQQK
DApTcGx1bmtVc2VyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDky5t45raE
pkx79os2P9YOz5LxLABt1JZK5BLuhPl8pu6eD73Q5nSkaCzNaN1H7HENgFXb1LHi
rnXVlBav1lP+nE5MxyV5NqUXnuTT7qym56aj9wiXENJIgMiWVHSl9UvasJxGilG0
sR01Xe8KvPkXMah5i1WE4fFEPY4xarEE+wIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
ADc2AD3C4oZOZYkvAb0bCwqkwP6AG6iwHfGLIt4MllFaDYNZY4CKN6kEFHHQ95pm
JbnqcbHvIeAqQxonh9VNIz9/nXJMpcWd1vF0M36frLhmx3RTs8aX5vfh2y3h54gI
eNMkeDnoH3EZzvzCG+JatI8ok8N3+tMr+9cmhxf8XdIj
</ds:X509Certificate> </ds:X509Data> </ds:KeyInfo> </md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat> <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://wimpy.splunk.com:9332/saml/logout"
index="0"> </md:SingleLogoutService> <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://wimpy.splunk.com:9332/saml/acs" index="0">
</md:AssertionConsumerService> </md:SPSSODescriptor> </md:EntityDescriptor>
```

The Login Process


Splunk(SP)
User/Browser
Ping Identity(IDP)
1.User accesses Splunk resource
2. Redirected to the IDP - AuthnRequest
3. IDP prompts the user for credentials
4. User enters credentials
5. IDP redirects back to Splunk, sends a SAML assertion
5b. Session cookie of Ping
6. Splunk checks the 'role' attribute in the assertion and checks the role mapping
7. SUCCESS – User logged in

Configure the IDP (Ping Identity)

- IDP initiated SSO, SP intiated SSO, SP initiated SLO
- Attribute Query Request Supported
- Signed request/response
- Upload Splunk's certificate OR Import Splunk's metadata

Configure Ping for SSO

PingFederate®

Help | About | Logout (jkerai)

Main | SP Connection

Connection Type | Connection Options | Import Metadata | General Info | Browser SSO | Attribute Query | Credentials | Activation & Summary

Please select options that apply to this connection.

- [x] Browser SSO
- [x] Attribute Query

Cancel | < Previous | Next >

Version 7.0.1.1

Attributes in the SAML assertion

Help | About | Logout (jkerai)

Main | SP Connections | SP Connection | Attribute Query

Retrievable Attributes | Attribute Sources & User Lookup | Attribute Mapping Fulfillment | Issuance Criteria | Security Policy

Summary

Specify the list of attributes that may be returned to the SP in the response to an attribute request.

RETRIEVABLE ATTRIBUTES	ACTION
mail	Edit / Delete
realName	Edit / Delete
role	Edit / Delete
	Add

Save Draft | Cancel | Next >

Why Attribute Query?

- When saved searches need to run
- Splunk uses the attribute query url using basic auth and queries the IDP
- IDP returns ‘attributes’ - mainly AD group information
- Splunk uses the role mapping and creates a session for the user

Set up SHC with SAML

- Configure all search heads with SAML
- Additional settings if there is a proxy or load balancer
- Single logout - search heads share a Ping session index

.conf2015

Q & A

splunk>

THANK YOU