#splunkconf

.conf2013

YOUR DATA
NO LIMITS

Securing Splunk for the Enterprise

Darren Dance, UNIX Technical Lead, WorldPay

Implementing the correct controls to meet regulatory and compliance requirements

splunk>


.conf2013
YOUR DATA
NO LIMITS
Introduction
splunk>

About Me

- Worked in Finance since 2003
- Started at WorldPay in 2005 as a Technical Support
- Joined the WorldPay UNIX team in 2007
- Started work on the WorldPay project to extract from The Royal Bank of Scotland in 2010
- Became the UNIX Technical Lead and Splunk evangelist in Q4 2012

About WorldPay

A leading provider of electronic payment processing solutions

A brief history

- 1989 – Streamline established
- 2002 – WorldPay becomes wholly owned part of RBS
- 2010 – RBS Group sells WorldPay
- 2013+ - We are at an exciting stage of our development
  - We are committed to investing in both our people and our technology to realise our ambitions

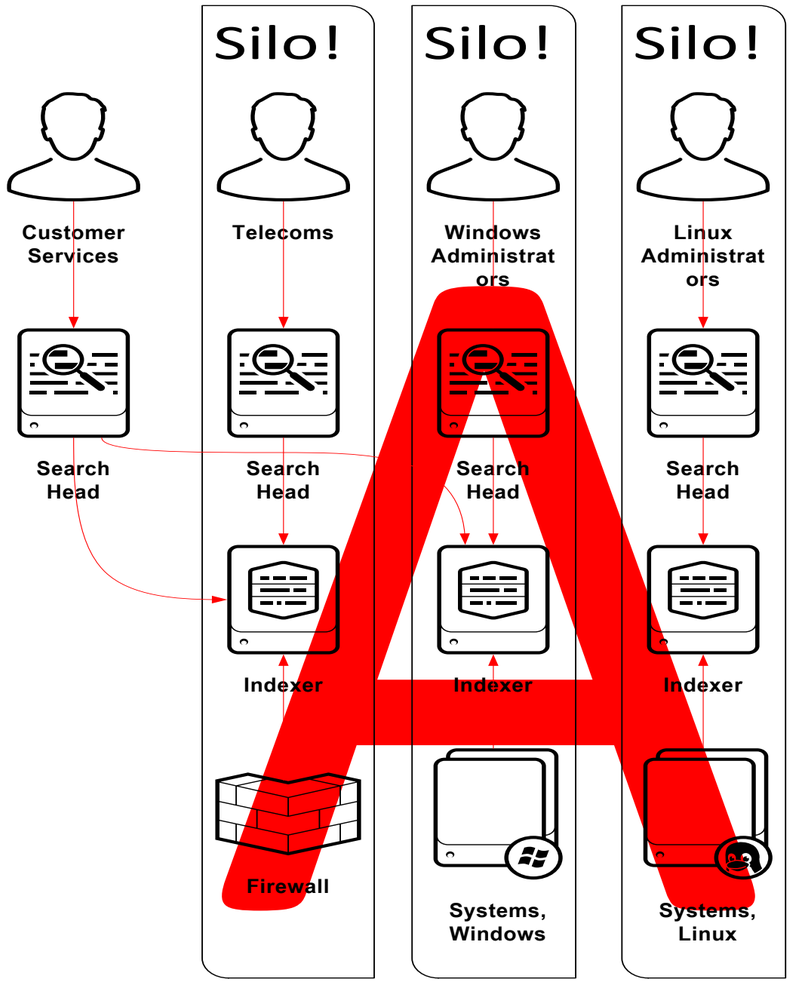
Interesting facts (2012):

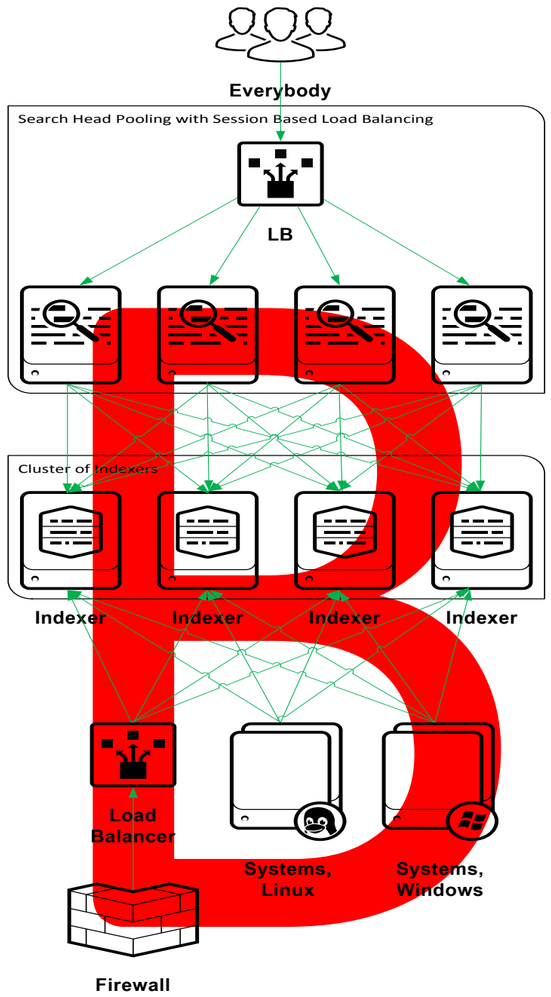
- 8B merchant acquiring transactions
- £279B Merchant acquiring turnover
- 120 currencies covered
- 252,000 Streamline merchants
- 200+ payment types
- 745 maximum transactions per second

Session Overview

- Making the default install more secure
  - Making simple changes to the default installation
  - Integrating the web interface to active directory
- Using roles to control access to the data
- Separating source types and indexes
  - Separating source types
  - Separating indexes
  - Creating retention policies for indexes
- A few final points

Show of Hands?






.conf2013
YOUR DATA
NO LIMITS
Making the Default
Install More Secure
splunk>

Making the Default Install More Secure

- Enforcing SSL v3
- Binding Splunk to specific interfaces (multi-interface configurations only)
- Replacing the self signed certificates

Binding Splunk to Specific Interfaces
Multi-Interface Configurations Only

Why?

- If you are running a server in the DMZ, you may not want to restrict what can talk to the Splunk application

Who likes this?

- Penetration Testers, Enterprise Security

Which file to alter? (assuming standard installs)


:/opt/splunk/etc/splunk-launch.conf


: c:\Program Files/Splunk/etc/splunk-launch.conf

Which parameters to change?

```
SPLUNK_BINDIP=192.168.0.23
```

Hands-on Demo

Enforcing SSLv3 and Strong Ciphers

Why?

- It's better to force more secure versions of SSL if there is no requirement to allow the older versions

Who Likes this?

- Penetration Testers, Enterprise Security, Auditors

Which File to alter? (assuming standard installs)

:/opt/splunk/etc/system/local/server.conf

:c:\Program Files/splunk/etc/system/local/server.conf

Which Parameters to change?

```
[sslConfig]
supportSSLV3Only = true
cipherSuite = TLSv1+HIGH:@STRENGTH
```

Hands-on Demo

Replacing the Self Signed Certs (1)

Why?

- The self signed certs are the same on all default installations, as such someone could poison or pretend to be your own infrastructure

Who Likes this?

- Penetration Testers, Enterprise Security, Auditors

Which File to alter? (assuming standard installs)


:/opt/splunk/etc/system/local/{outputs.conf,inputs.conf}


:c:\Program Files\Splunk\etc\system\local\inputs.conf


:c:\Program Files\Splunk\etc\system\local\outputs.conf

Replacing the Self Signed Certs (2)

What to change?

(Indexer/Intermediary Forwarder) inputs.conf

```
[splunktcp-ssl:9997]

[SSL]
password = $1$XSoZY/pQNSDCOvZV
rootCA = /opt/splunk/etc/auth/mycerts/
myCACertificate.pem
serverCert = /opt/splunk/etc/auth/mycerts/
myNewServerCertificate.
pem
```

(Forwarder) outputs.conf

```
[tcpout]
defaultGroup = splunkssl

[tcpout:splunkssl]
compressed = false
server = 192.168.205.4:9997
sslCertPath = $SPLUNK_HOME\etc\auth\mycerts
\myNewServerCertificate.pem
sslPassword = $1$b9NuwohxdMmzYjMO
sslRootCAPath = $SPLUNK_HOME\etc\auth\mycerts
\myCACertificate.pem
sslVerifyServerCert = true
```

Special Notes on replacing SSL Certs:

- If the password is put into the `inputs/outputs.conf in $SPLUNK_HOME/etc/system/local/…` then you can type the plain text password and Splunk Enterprise will automatically replace the plain text with the encrypted string in that file on restart
- If your certificates are being deployed to a mixed estate be conscious of your passwords

Hands-on Demo

Centralised Authentication (1)
Using Microsoft Active Directory

Why?

- It's so much easier to manage, better for RBAC and is nicer for the users as it is one less username and password to remember

Who Likes this?

- Enterprise Security, Auditors

Which File to alter? (assuming standard installs)


:/opt/splunk/etc/system/local/authentication.conf


:c:\Program Files\Splunk\etc\system\local\authentication.conf

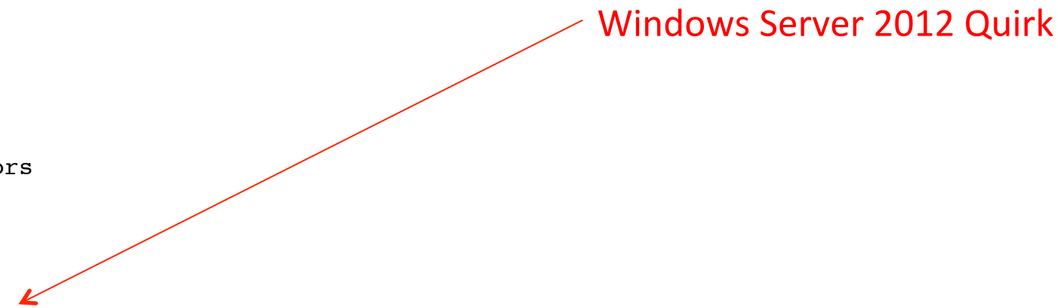
Centralised Authentication (2)
Using Microsoft Active Directory

What to add?

```
[authentication]
authSettings = lab
authType = LDAP

[roleMap_lab]
admin = Splunk Administrators

[lab]
SSLEnabled = 0
anonymous_referrals = 0
bindDN = svc_splunk@my.lab
bindDNpassword = $1$WDcBIvtDJT+y
charset = utf8
groupBaseDN = dc=my,dc=lab
groupMappingAttribute = dn
groupMemberAttribute = member
groupNameAttribute = cn
host = lab-dc.my.lab
nestedGroups = 1
network_timeout = 20
port = 389
realNameAttribute = displayname
sizelimit = 1000
timelimit = 15
userBaseDN = cn=Users,dc=my,dc=lab
userNameAttribute = samaccountname
```



Hands-on Demo

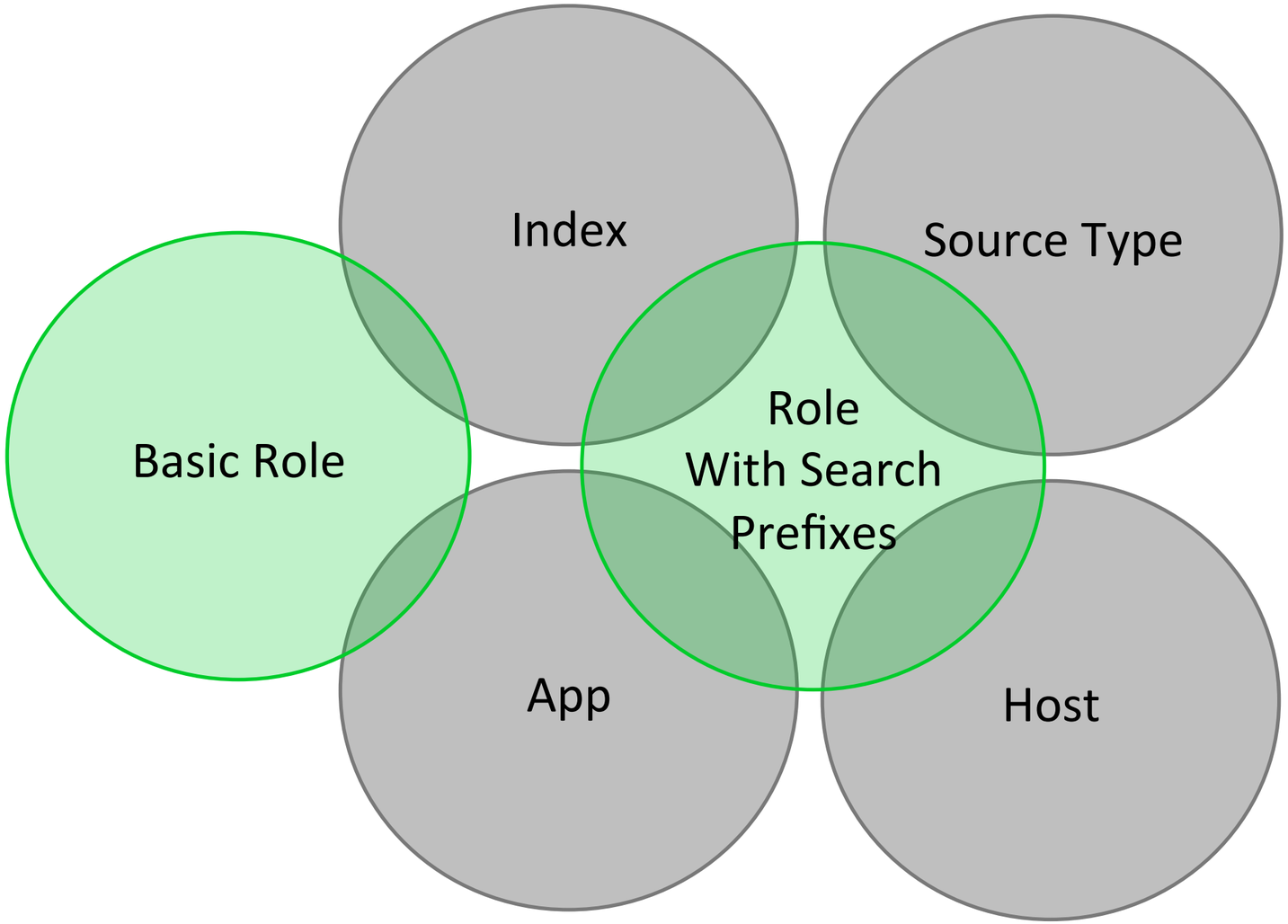
Using Splunk Roles to Control Access

splunk>

Using Splunk Roles to Control Access

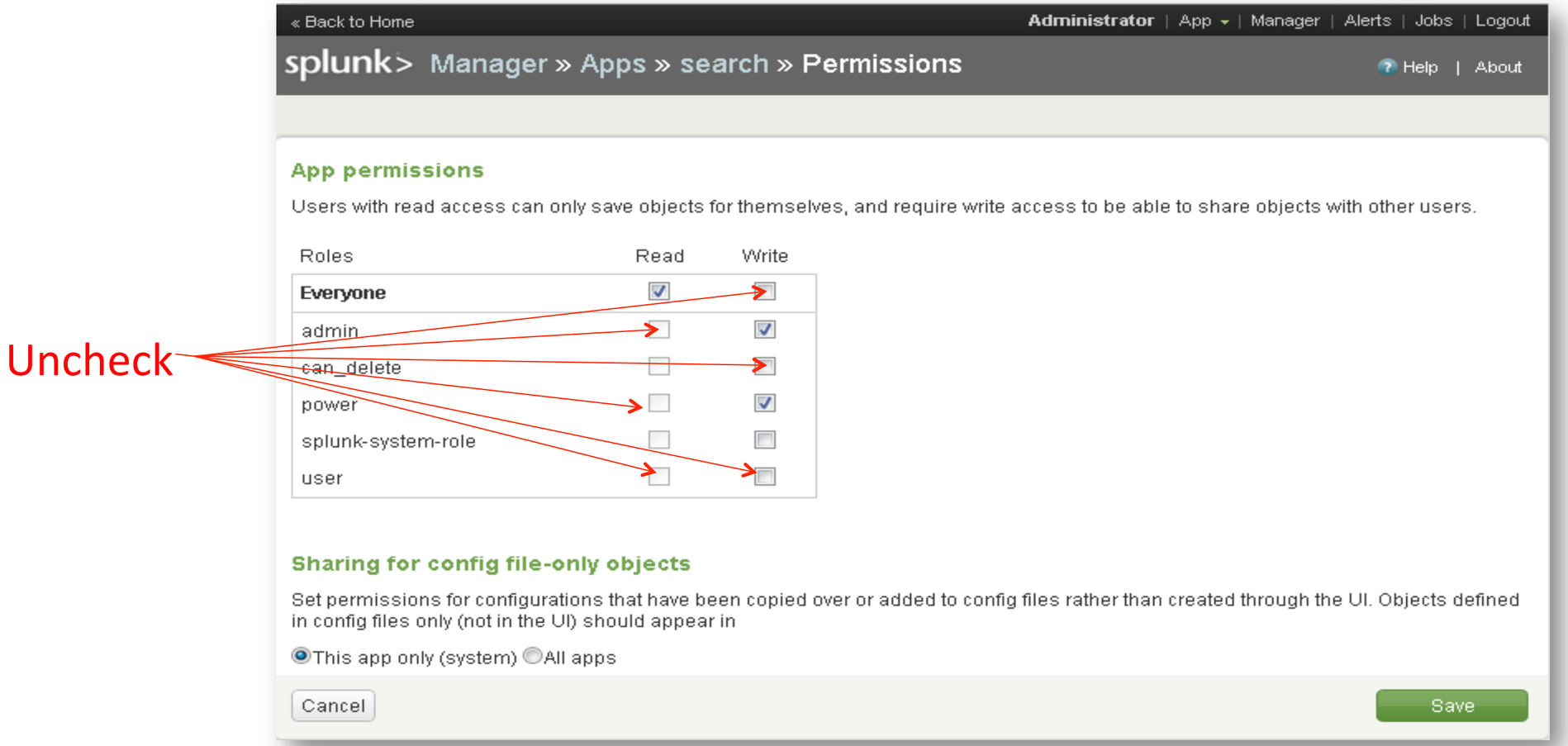
- Disable app access for the default user and power user roles
- Create new roles that inherit basic permissions from default roles
- Control access to an app access using roles
- Further limit access within an app by prefixing searches with hidden limitations for additional control

Using Splunk Roles to Control Access



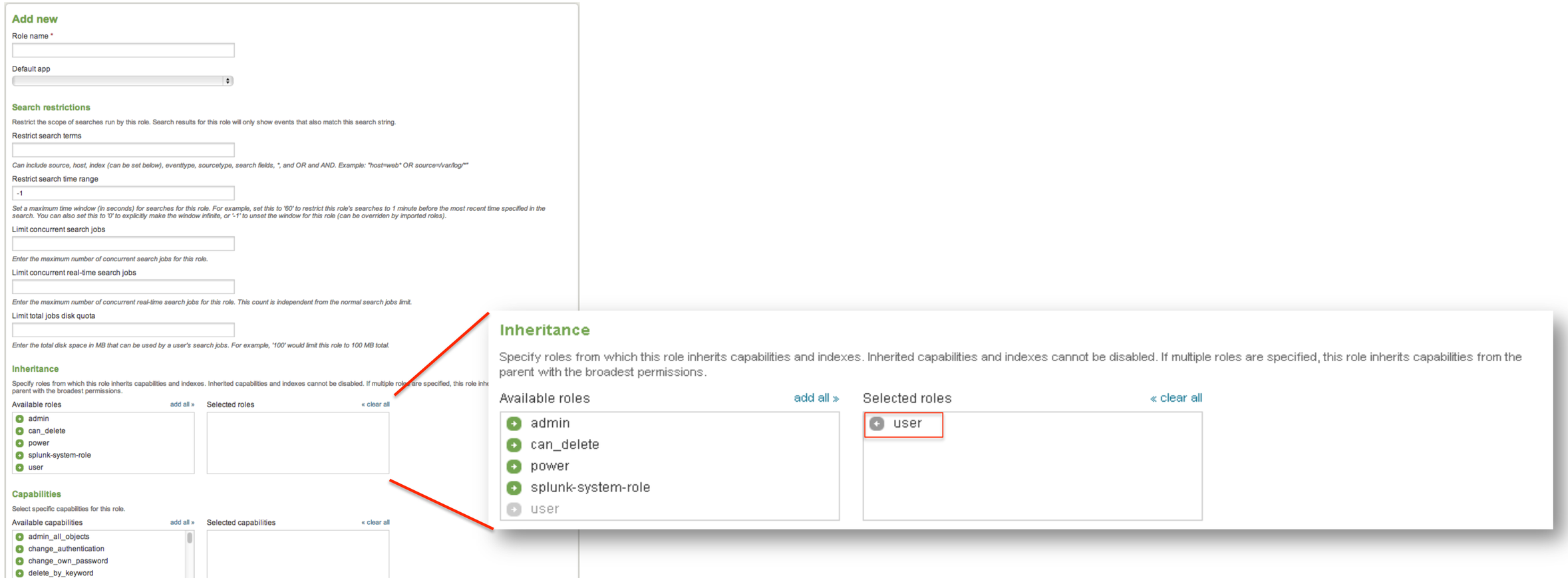
Disable App Access for the Default User and Power User Roles

Manager >> Apps >> Search >> Permissions



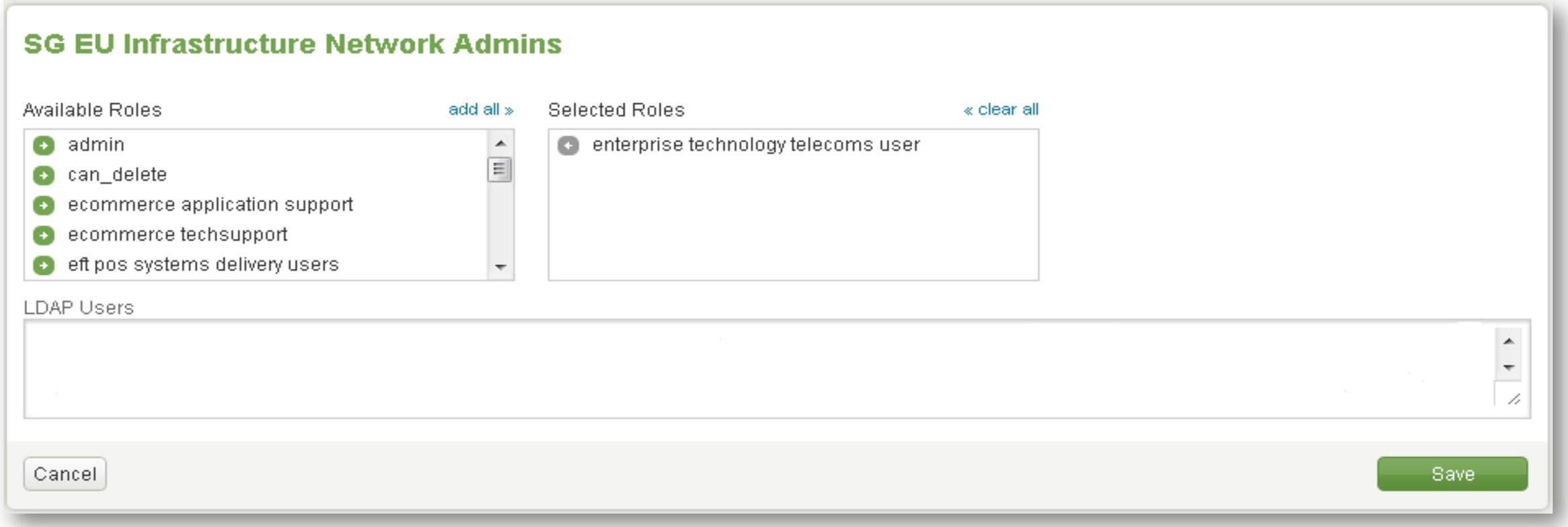
Create New Roles That Inherit Basic Permissions from the Default Roles

Manager >> Access Controls >> Roles >> Add New



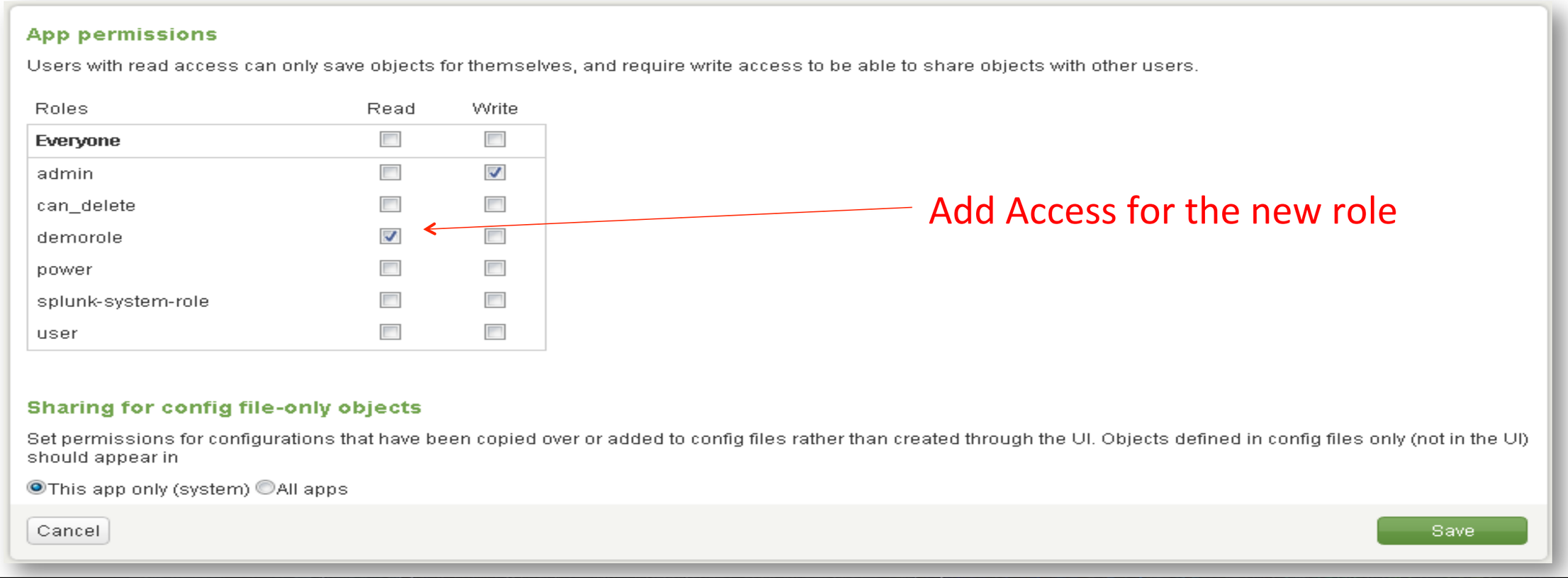
Link Your New Role to an AD Group

Manager >> Access Controls >> Authentication method >> LDAP strategies >> LDAP Groups



Control Access to an App Access Using Roles

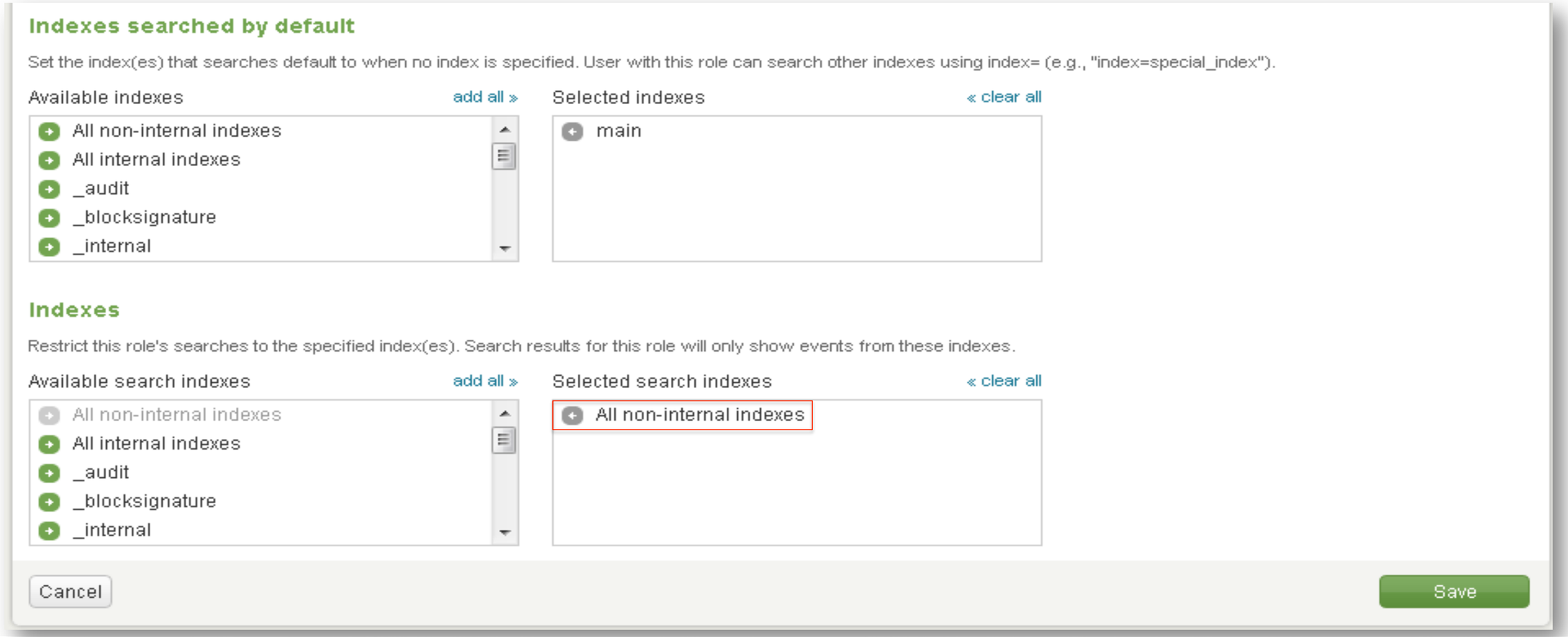
Manager >> Apps >> Search >> Permissions



Add Access for the new role

Control Access to an Index Access Using Roles

Manager >> Access Control >> Roles >> demo role



Further Limit Access Within an App

Prefix Searches with Hidden Limitations for Additional Control

Manager >> Access Control >> Roles >> demo role

For example:

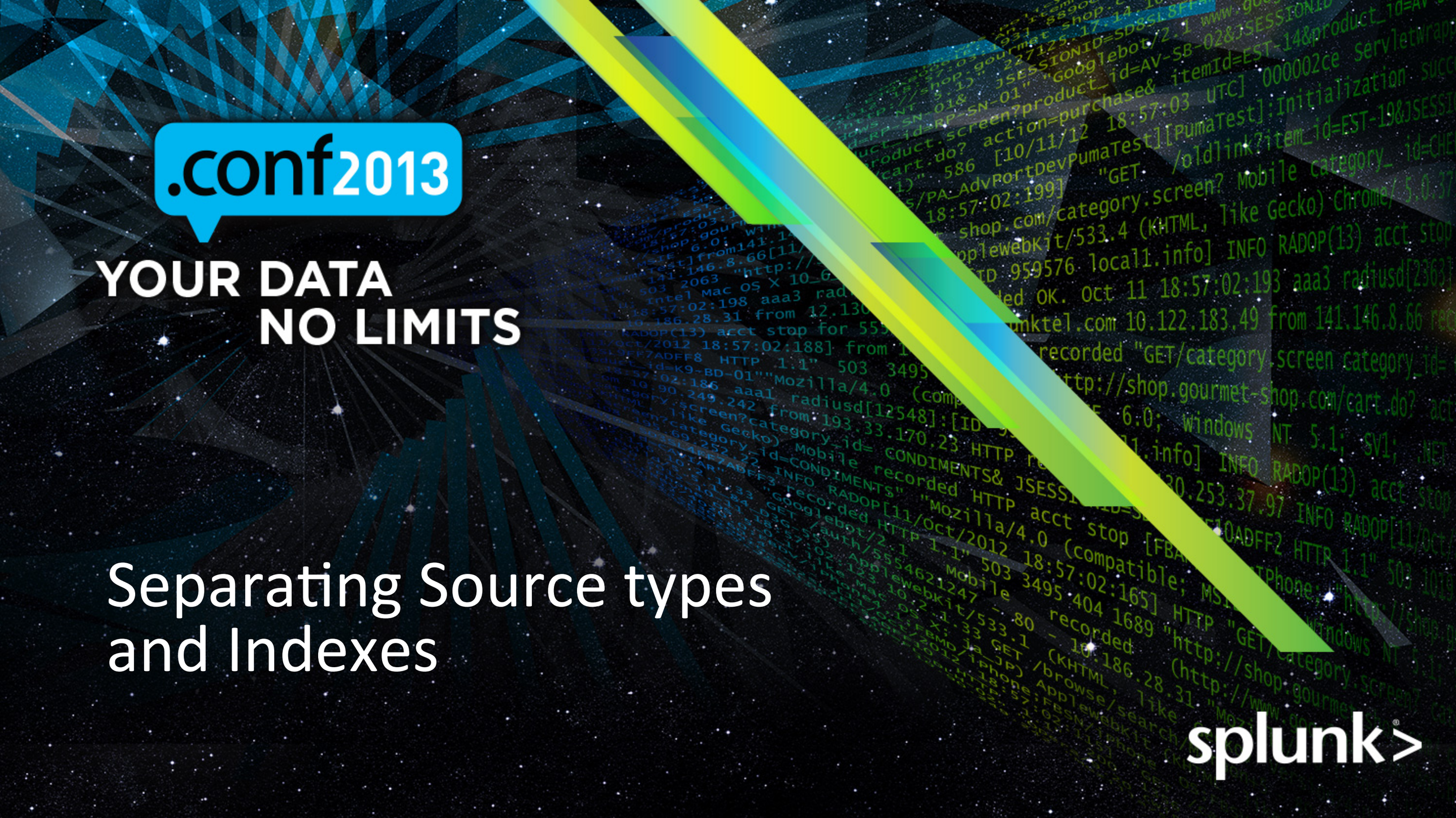
```
NOT sourcetype=syslog

host=server1 OR server2 NOT sourcetype=linux_secure

source="/var/log/*"
```

Note: Exclusions are less efficient than inclusions

Hands-on Demo


.conf2013
YOUR DATA
NO LIMITS
Separating Source types
and Indexes
splunk>

Separating Source types and Indexes

- Separating source types
- Separating indexes

Separating Source Types

- Why?
  - To allow you to make RBAC more granular
  - To make your searches more efficient
- How to Separate Data into it's own source type?

```
#props.conf
[syslog]
TRANSFORMS-sourcetypeOverride =
sourcetypeNetscaler
```

```
#transforms.conf
[sourcetypeNetscaler]
DEST_KEY = MetaData:Sourcetype
REGEX = (host1|host2)
FORMAT = sourcetype::netscaler_syslog
SOURCE_KEY = MetaData:Host
```

Hands-on Demo

Separating Indexes

- Why?
  - To allow you to make RBAC more granular
  - To separate data for different retention periods

How to separate data into its own Indexes?
How to set up a retention policy for that Index?

How to Separate Data Into its Own Index

- Overview
  - Define the new index on your indexers in indexes.conf
  - Use props.conf and transforms.conf to relocate your inbound data to your new index

indexes.conf:

```
[newindex]
homePath=$SPLUNK_DB/newindex/db
coldPath=$SPLUNK_DB/newindex/colddb
thawedPath=$SPLUNK_DB/newindex/thaweddb
maxTotalDataSizeMB=10000
```

props.conf:

```
[ActiveDirectory]
TRANSFORMS-indexoverride =
indexWindows
```

transforms.conf:

```
[indexWindows]
DEST_KEY = _MetaData:Index
REGEX = (ActiveDirectory)
FORMAT = windows
SOURCE_KEY = MetaData:Sourcetype
```

Setting up a Retention Policy For an Index

- Overview

Define your retention policy

Define whether you want to keep data offline after your retention period

`indexes.conf`

```
[main]
maxMemMB = 20
maxConcurrentOptimizes = 6
maxDataSize = auto_high_volume
frozenTimePeriodInSeconds = 7776000
maxWarmDBCount = 10
maxHotIdelSecs = 86400
maxHotBuckets = 10
coldToFrozenDir = /opt/splunk/frozen/main
```

Hands-on Demo

A Few Other Points

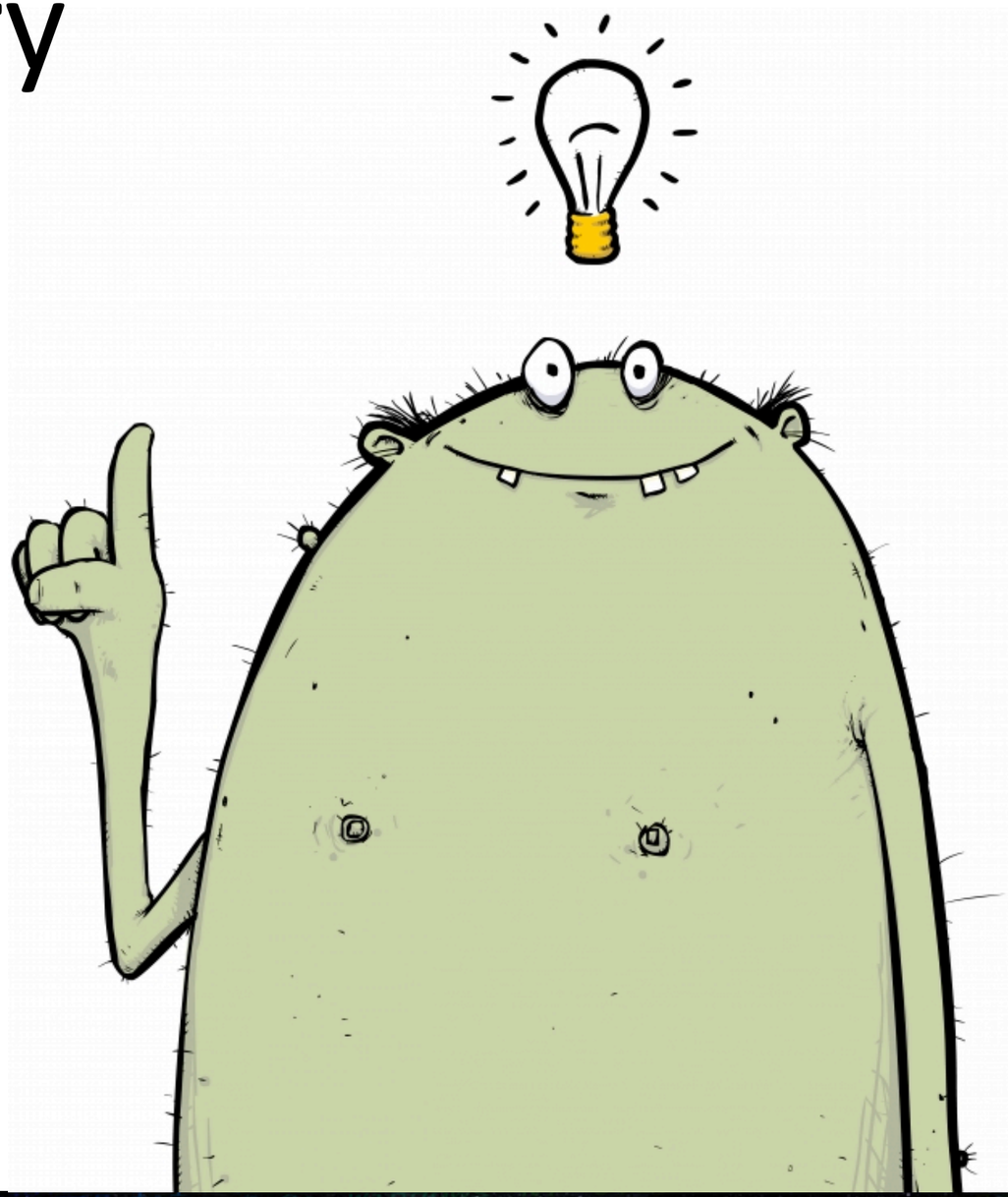
- Disable splunk web anywhere you don't need it for security (web.conf)

```
[settings]
Startwebserver = 0
```

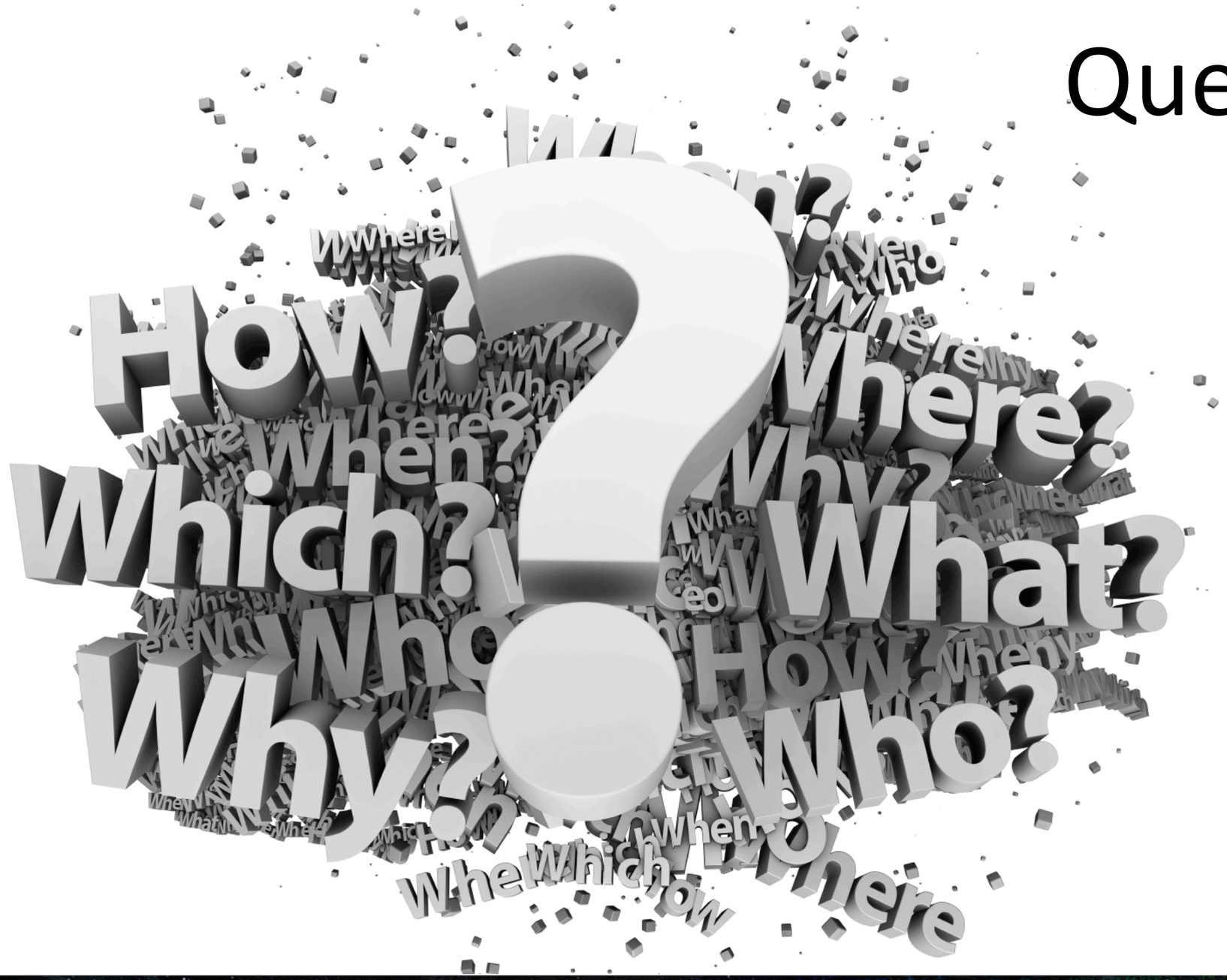
- Change the default password of all Splunk components
- Use Splunk On Splunk App to find issues in your setup: http://apps.splunk.com/app/748
- Use https for search heads
- If you use Splunk deployment server, be careful who can access it, as it can be used for evil
- Restrict who has direct access to your indexers
- Harden your Splunk Enterprise servers
- Audit your system to see what your users get up to
- Only give users the access they need to do their jobs

Summary

- To conclude…



Questions




.conf2013
YOUR DATA
NO LIMITS
THANK YOU
splunk>