I’m A Windows Girl, In A Redhat World: Reducing The Massive Splunk Learning Curve

Kelly Zimmerman

Indiana University

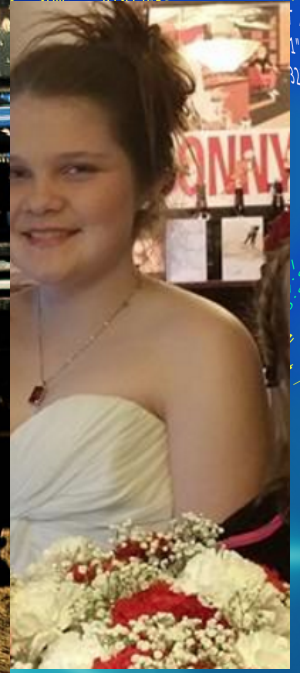
Session Title: I'm A Windows Girl, In A Redhat World: Reducing The Massive Splunk Learning Curve

Track: Splunk Foundations

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.

Introd

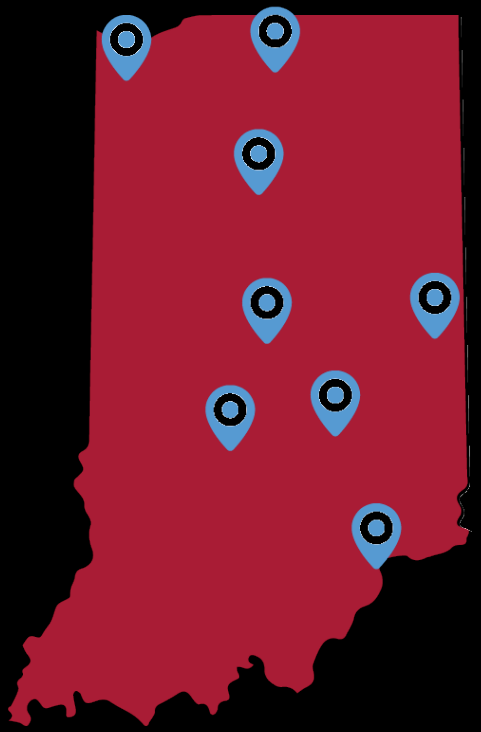


splunk>

Brief Overview Of Indiana University

.conf2016

splunk>



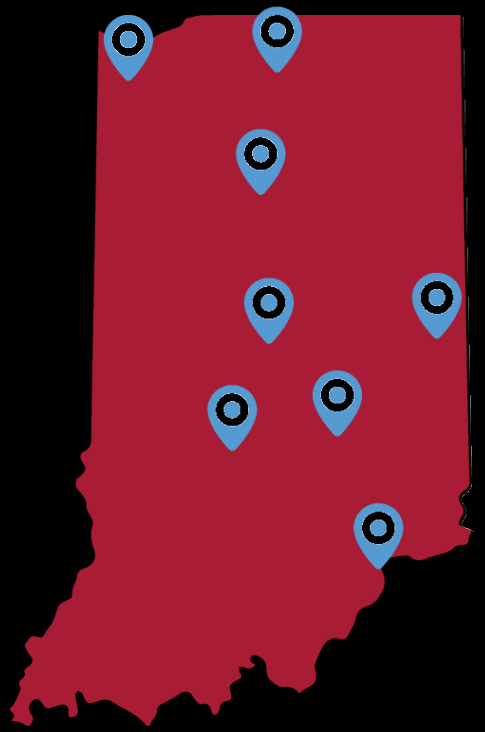
Indiana University, *est. 1820*

- $3.3B Enterprise
- Partnered with $6B IU Health system

- 115,000 Students
- 1.3M Credit Hours per semester
- >20,000 Degrees per year
- $1.1B In Financial Aid
- $450M In research grants

- 8,000 Acres
- 882 Buildings, 36M square feet
- >600,000 *Living* Alumni

- 10,500 Faculty and Staff



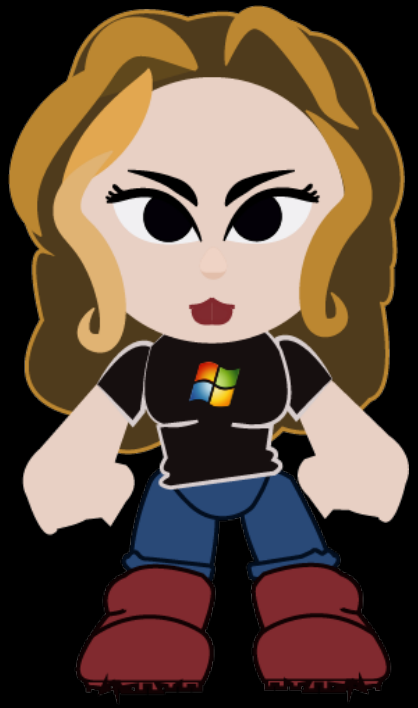
CENTRALIZED enterprise I.T.
with
DECENTRALIZED departmental I.T.

109 Departmental IT Groups
5213 Total Servers within IU

Assumptions

splunk>enterprise

OR



OR

Agenda

- IU Architecture
- “Rules Of Precedence”
- Search Head Deployer
- Deployment Server
- Command Line Security
- Command Line Only
- Linux-enough To Be Dangerous With Splunk + Windows Hacks

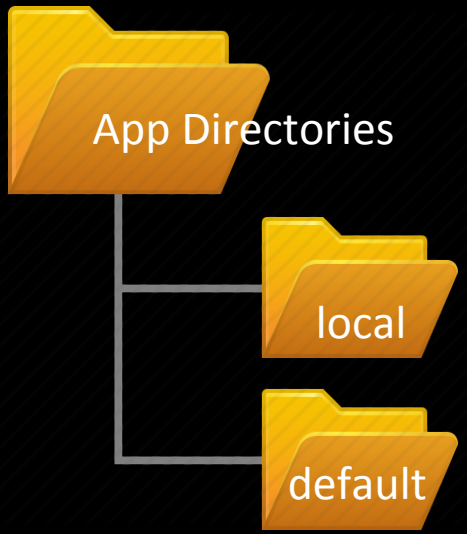
Architecture


Bloomington
Indianapolis
Search Cluster
splunk>
Deployer
Deployment
License Master
Indexers
.LOG
Forwarders

“Rules of Precedence”

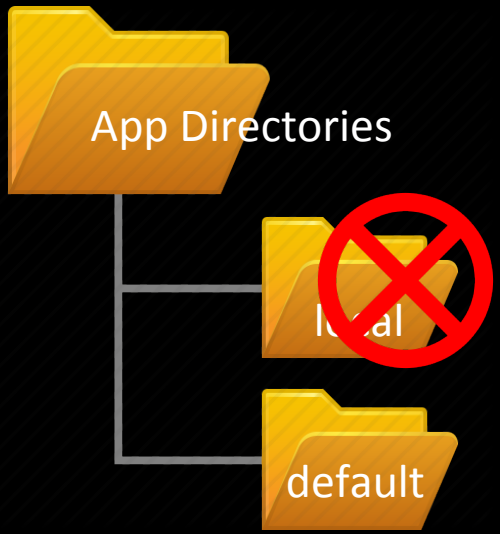
Brief Note About Rules Of Precedence

Editing .Conf Files



/opt/spl etc/sys de /opt/splunk/etc/apps/ /opt/splunk/etc/users/'username'/search/local

Custom And Splunkbase Apps



Search Head Deployer

The Deployer

Deployer

Deployer

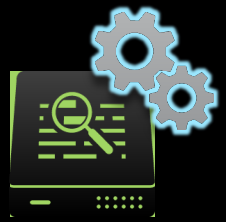
Search head

Search head

Search head

The Deployer Cont.

Deployer



Search head

Search head

Search head

Command Line Deployer/SearchHead

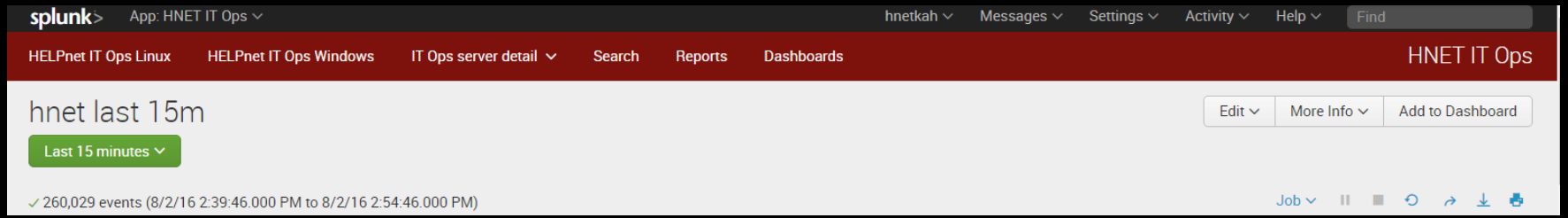
deployer

search head

Opt/splunk/etc/shcluster/apps → opt/splunk/etc/apps

opt/splunk/etc/shcluster/apps/hnet_it_ops → opt/splunk/etc/apps/hnet_it_ops

opt/splunk/etc/shcluster/apps/hnet_it_ops/local → opt/splunk/etc/apps/hnet_it_ops/default



Command Line Deployer/SearchHead

Deployer

Search head

opt/splunk/etc/users/hnetkah/hnet_it_ops/local

opt/splunk/etc/users/hnetkah/hnet_it_ops/local/savedsearches.conf

nothing

```
[hnet last 15m]
action.email.useNSSubject = 1
alert.track = 0
dispatch.earliest_time = -15m
dispatch.latest_time = now
display.visualizations.show = 0
request.ui_dispatch_app = hnet_it_ops
request.ui_dispatch_view = search
search = index=iuhnet
```

Command Line Deployer/SearchHead

Deployer

```
-bash-4.1$ pwd
/opt/splunk/etc/shcluster/apps/hnet_it_ops/local
-bash-4.1$ ls
alert_actions.conf  app.conf  data  props.conf
savedsearches.conf  times.conf  transforms.conf
```

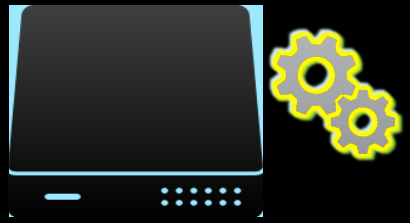
Search head

```
-bash-4.1$ cd etc/apps/hnet_it_ops/default/
-bash-4.1$ ls
alert_actions.conf  app.conf  data  props.conf
savedsearches.conf  times.conf  transforms.conf
```

Deployment Server

Deployment

The Deployment Server



Deployment

Indexer

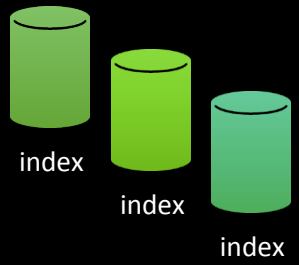
Forwarder A group

Forwarder B group

Deployment

Create Indexes

Deployment



Indexer

/opt/splunk/etc/deployment-apps/config_indexer/local
-bash-4.1$ ls
app.conf authentication.conf authorize.conf indexes.conf inputs.conf
limits.conf props.conf server.conf transforms.conf

Deployment

Configure Forwarders

-bash-4.1$ pwd
/opt/splunk/etc/system/local
-bash-4.1$ ls
authentication.conf eventtypes.conf inputs.conf migration.conf README
serverclass.conf server.conf ui-tour.conf web.conf

Forwarder A group

Forwarder B group

Command Line Deployment/Client

Deployment

Client

opt/splunk/etc/deployment-apps → $SPLUNK_HOME/etc/apps

opt/splunk/etc/deployment-apps/win_TA → $SPLUNK_HOME/etc/apps/win_TA

opt/splunk/etc/deployment-apps/win_TA/local → $SPLUNK_HOME/etc/apps/win_TA/local

Command Line Deployment/Client

Deployment

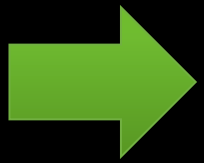
Client

[deployment-client]
phoneHomeIntervalInSecs = 300

[target-broker:deploymentServer]
targetUri=IN-HNET-DPS01.hnet.iupui.edu:8089

[deployment-client]
clientName = in-win-hnet-iu-hnet-lartfs1

[target-broker:deploymentServer]
targetUri=in-hnet-dps01.hnet.iupui.edu:8089

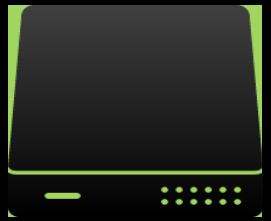


[deployment-client]
clientName = in-win-hnet-iu-hnet-lartfs1
phoneHomeIntervalInSecs = 300

[target-broker:deploymentServer]
targetUri=in-hnet-dps01.hnet.iupui.edu:8089

Command Line Security

Quick Notes About Under The Hood Security (Where Is My authentication.Conf?)



Deployer

LDAP setup for application groups in AD is created in the deployer

/opt/splunk/etc/shcluster/apps/config_auth/local/authentication.conf

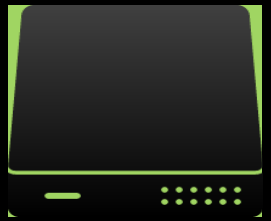
```
[authentication]
authSettings = iuhelpnet01
authType = LDAP

[configurations stanza for LDP]

RoleMap_iuhelpnet01
Admin=ad-groupname-1
group1=ad-groupname-2
group2=ad-groupname-3
```

opt/splunk/etc/apps/config_auth/default

Quick Notes About Under The Hood Security (Where Is My authorize.Conf?)



Deployer

To manage the roles, go here:

/opt/splunk/etc/shcluster/apps/config_auth/local/authorize.conf

```
[role_hnet]
search = enabled
srchIndexesAllowed = iuhnet
srchIndexesDefault = iuhnet
srchJobsQuota   = 12
srchDiskQuota   = 750
rest_properties_get = enabled
accelerate_search = enabled
rtsearch = enabled
```

opt/splunk/etc/apps/config_auth/default

Command Line Only

Stuff The CLI Does That The GUI Can't Always Do

- Reload deploy-server (pushes new apps into the runtime area)
- Splunk apply shcluster-bundle –target <server> -auth <pwd>
- Btool
- Pushing custom code in the default app
- Adding indexes under unusual circumstances
- Editing config files to lock out users
- Changing the default behavior E.G. adding images or branding
- Almost everything on the deployer & deployment server

“Linux-Enough”

Learning Enough Linux To Be Dangerous With Splunk

- http://linuxcommand.org/index.php
- https://www.learnenough.com/command-line-tutorial
- Get the book by William Shotts, *The Linux Command Line*. http://sourceforge.net/projects/linuxcommand/files/TLCL/13.07/TLCL-13.07.pdf/download
- http://regexone.com/
- https://regex101.com/

What Now?

Related Breakout Session

If you want to know more about the CLI and security, and missed Daniel Daily's talk, please go check it out online after .conf:

"Multitenant Architecture: Securing Splunk to Combat Snooping Users"

THANK YOU

splunk>