

.conf2014

YOUR DATA ADVENTURE



In Depth with
Deployment Server
Sanford Owings
Principal Consultant,
Splunk Professional Services
David Shpritz
Security Consultant, Aplura, LLC

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 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.

.conf2014

YOUR DATA ADVENTURE

What is Splunk
Deployment Server?

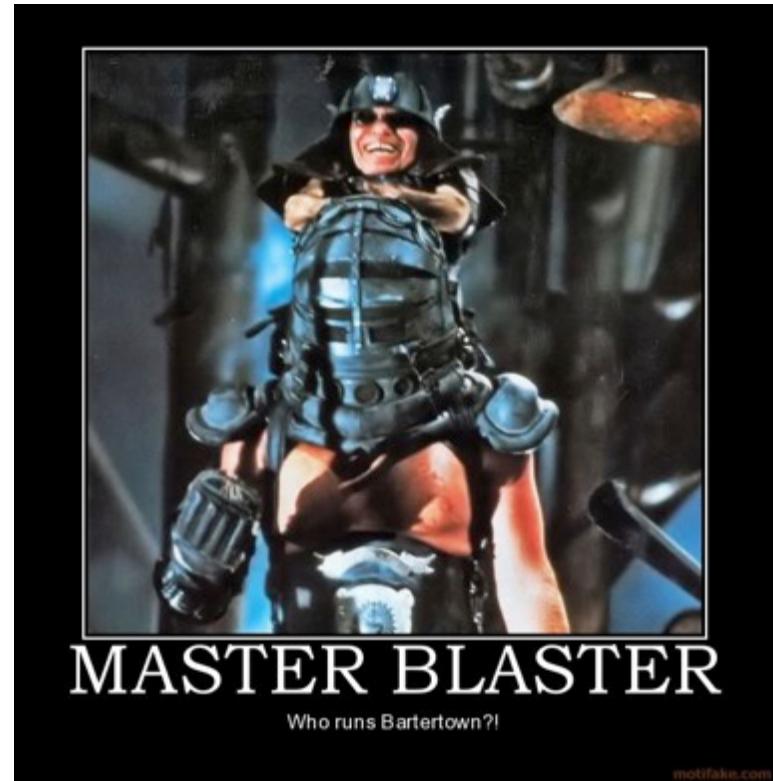
splunk®

What is Splunk Deployment Server?

- Doesn't actually deploy Splunk (common misperception)
- Acts as a configuration server
- Configurations are held in “apps” or “configuration bundles”
- Listens on the Splunk management port (8089 by default)
- Serves up lists of apps for clients to download and install
- The server configuration (serverclass.conf) describes what systems should download what apps

Why use Deployment Server?

- No touching endpoints!
- Distribute add-ons to search heads to give users consistent field extractions
- Make sure you are getting a common set of inputs (satisfy auditors), that is, consistent configs
- Deployment server clients can be any part of Splunk infrastructure (search heads, indexers, forwarders of all types)
(well, not clustered indexers)



How can I select what systems are in what class?

- Serverclass.conf!
- Allows you to whitelist/blacklist/filter on different aspects of what is reported to the deployment server
 - IP address
 - Host
 - ClientName (configured in deploymentclient.conf on the client)
 - machineTypesFilter (OS and architecture)

```
[serverClass:IntermediateHFs]
restartSplunkd = true
whitelist.0 = splk-heavyforwarder*
[serverClass:IntermediateHFs:app:DS-all_departments-IHF-base]
[serverClass:IntermediateHFs:app:DS-all_departments-Input-splunk_tcp_9997]
[serverClass:IntermediateHFs:app:DS-all_departments-Splunk-no_web]
```

machineTypesFilter

- Acts as just what it says, filters systems based on OS and Arch
- Happens after the whitelist/blacklist
- This means that machineTypesFilter by itself won't match anything
- If you want all windows machines, you would need something like:

```
[serverClass:All-Windows]
restartSplunkd = true
whitelist.0 = *
machineTypesFilter = windows-intel,windows-x64
[serverClass:All-Windows:app:DS-all_departments-Input-windows_logs]
```

How does this work?

- Serverclass.conf contains stanzas that define classes of systems (servers)
- Clients check in and subscribe to the classes they are included in
- Deployment server (DS) tarballs the deployment app, and hashes it
- The client keeps track of the hash of the app it has installed
- When it checks in, if the hash on the DS differs from what it has, the client downloads the new version
- After downloading, the client deletes the version it has and extracts the new version
- Restarting is optional (configured per serverclass)

How does this work?



“Hmm, I haven’t checked in in a while, better do that.”

>	9/9/14 10:05:31.104 AM	09-09-2014 10:05:31.104 -0700 INFO DC:UpdateServerclassHandler - Changed state from=HandlingPhonehome to=Phonehome	host = [REDACTED] source = E\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	9/9/14 10:05:31.089 AM	09-09-2014 10:05:31.089 -0700 INFO DC:UpdateServerclassHandler - Changed state from=Phonehome to=HandlingPhonehome	host = [REDACTED] source = E\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd

How does this work?



TCP 8089 (HTTPS)



“Hi, my name is forwarder1.
My IP is 192.168.1.2.
I have a ClientName of ForwarderSys.
I am running Windows on a 64-bit architecture.
I’m a Sagittarius (okay, not really).”

```
> 9/17/14      172.16.101.153 - - [17/Sep/2014:17:10:27.960 -0700] "POST /services/broker/phonehome/connection_11  
5:10:27.960 PM 53_8089_53_8089.com_53_8089_DC-all HTTP/1.0" 200 24 - - 2ms  
host = 53_8089 | index = _internal | source = /opt/splunk/var/log/splunk/splunkd_access.log | sourcetype = splunkd_access
```

How does this work?

“Hmm. I haven’t heard from this client since my last reload. I’ll add it to the list of clients.



```
> 9/8/14      09-08-2014 18:30:06.244 -0700 INFO ClientSessionsManager - Adding client: ip=... uts=linux-x  
6:30:06.244 PM 86_64 id=589025c9d87908d473e1b8af83bad99e name=DC-all  
host = ... | source = /opt/splunk/var/log/splunk/splunkd.log | sourcetype = splunkd
```

How does this work?



Response (same TCP connection)



“Hi, forwarder1. You belong in these classes:

- WindowsForwarder
 - LocalForwarder”

```
> 9/9/14      09-09-2014 10:06:29.680 -0700 INFO DeployedServerclass - name=All-Windows Reload; workingDir='E:\SplunkForwarder\var\run\All-Windows'  
10:06:29.680 AM host = [REDACTED] | source = E:\SplunkForwarder\var\log\splunk\splunkd.log | sourcetype = splunkd
```

How does this work?



“I need a list of the apps in these classes:

- WindowsForwarder
- LocalForwarder”

How does this work?



Response (same TCP connection)



“Sure, here are the apps and their hashes:

- Splunk_TA_windows (hash: 93619374927206593098)
- Outputs_To_Indexers (hash: 11961082866254951452)”

How does this work?



“Hmm, I have the right hash for Splunk_TA_windows, but for Outputs_To_Indexers I have a hash of 0. Better download it.”

```
9/8/14 09:08:20 09:55:02.016 -0700 INFO DeployedApplication - Checksum mismatch 11961082866254951452 <> 15310549620697355544 for a  
6:55:02.016 PM pp=Splunk_TA_nix. Will reload from='[REDACTED]':8089/servicesstreams/deployment?name=default:ParseTA:Splunk_TA_nix'  
host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
```

How does this work?



“I need the latest version of Outputs_To_Indexers.”

A screenshot of a computer screen displaying a table of log entries. The table has a header row and a single data row. The data row contains the following information:

>	9/9/14 10:06:29.680 AM	09-09-2014 10:06:29.680 -0700 INFO DeployedServerclass - name=All-Windows Reload; workingDir='E:\SplunkForwarder\var\run\All-Windows'
		host = [REDACTED] source = E:\SplunkForwarder\var\log\splunk\splunkd.log sourcetype = splunkd

How does this work?



Response (same TCP connection)



“Sure, here you go.”

```
> 9/8/14      09-08-2014 18:55:02.053 -0700 INFO DeployedApplication - Downloaded url=j...:8089/services/streams/deployment?name=default:ParseTA:Splunk_TA_nix to file='/opt/splunk/var/run/ParseTA/Splunk_TA_nix-1410218690.bundle' sizeKB=1120
host = ... | source = /opt/splunk/var/log/splunk/splunkd.log | sourcetype = splunkd
```

How does this work?



“Okay, now that I have the new version, I’ll delete the existing one, and replace it with the new and shiny version. After that, I’ll restart the Splunk services, because I was told to. Then I’ll tell the DS the good news.”

> 9/8/14 6:55:01.972 PM	09-08-2014 18:55:01.972 -0700 INFO DeployedApplication - Installing app=Splunk_TA_nix to='/opt/splunk/etc/apps/Splunk_TA_nix'
	host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

> 9/10/14 12:13:38.805 PM	09-10-2014 12:13:38.805 -0700 INFO ClientSessionsManager - ip=[REDACTED] name=DC-all Updating record for sc=SyslogFileInputs app=DS-all_departments-Input-syslog_files: action=Install result=0k
	action = Install eventtype = splunkd-log host = iyxvplogld01 index = _internal source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd splunk_server = i...

Things to remember

- Think of this as configuration enforcement (DS version wins!)
- Remember that delete portion. It will save you some headache.



.conf2014

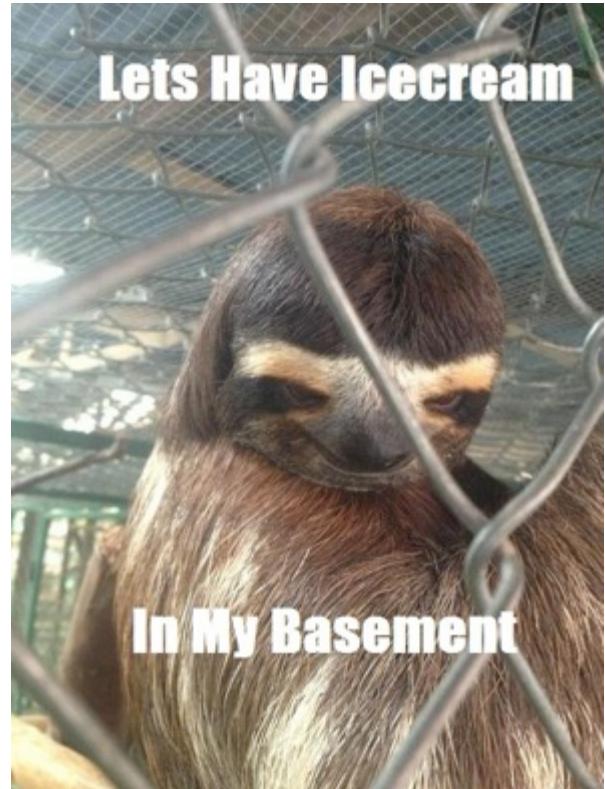
YOUR DATA ADVENTURE

Problems can happen...

splunk®

Gotchas!

- Careful with lookups
- Splunk 6.2 resolves this problem, but older versions will overwrite the local lookup
- Careful with apps that have clickable content (setup GUIs, for example)
- General rule: Don't distribute apps with a UI where users can click to change configs
- Remember that delete thing? Yeah, the saved content would get nuked too
- Careful with what you restart
- Indexers and cluster masters can be touchy, restarting search heads means users may be unhappy



Gotchas! (continued)

- A Deployment Server cannot deploy to itself
- 6.x will tell you about that, then may kill both.

>	9/17/14 10:57:58.956 PM	09-17-2014 22:57:58.956 -0400 INFO DS_DC_Common - Deployment Client not initialized. host = davids-mbp source = /splunk/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	9/17/14 10:57:58.956 PM	09-17-2014 22:57:58.956 -0400 WARN DC:DeploymentClient - Deployment Client validation failed: host = davids-mbp source = /splunk/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	9/17/14 10:57:58.956 PM	09-17-2014 22:57:58.956 -0400 ERROR DC:DeploymentClient - DC shares a Splunk instance with its DS; unsupported configuration. targetUri=127.0.0.1:8089 hostname=Davids-MacBook-Pro.local mgmtPort=8089 host = davids-mbp source = /splunk/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	9/17/14 10:57:58.956 PM	09-17-2014 22:57:58.956 -0400 WARN DC:DeploymentClient - This DC shares a host with its DS. targetUri=127.0.0.1:8089 hostname=Davids-MacBook-Pro.local host = davids-mbp source = /splunk/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

Gotchas! (continued)

- The client hostname is important

```
09-08-2014 20:08:34.652 -0400 INFO ClusteringMgr - initing clustering withn: nt=b0 ff=j st=i ct=b0 st=b0 rt=b0 rct=b0 rst=b0 rrft=b0 rmst=b000 rmrt=1  
0 sfrt=600 pe=1 im=0 is=0 mob=5 mor=5 pb=5 rep_port= pptr=10  
09-08-2014 20:08:34.652 -0400 INFO ClusteringMgr - clustering disabled  
09-08-2014 20:08:34.652 -0400 INFO DS_DC_Common - Initializing the PubSub system.  
09-08-2014 20:08:34.652 -0400 INFO DS_DC_Common - Initializing some facilities of PubSub system  
09-08-2014 20:08:34.671 -0400 WARN DC:DeploymentClient - Unable to resolve my hostname. DeploymentClient is disabled.  
09-08-2014 20:08:34.671 -0400 INFO DS_DC_COMMON - Deployment Client not initialized.  
09-08-2014 20:08:34.671 -0400 INFO DS_DC_Common - Loading and initializing Deployment Server...  
09-08-2014 20:08:34.671 -0400 INFO DeploymentServer - Attempting to reload entire DS: reason='init'
```

Gotchas! (continued)

- Careful with the numbering of your whitelists/blacklists in serverclass.conf

```
143 [serverClass:Level2Forwarders]
144 restartSplunkd = true
145 whitelist.1 = dns.company.com
146 whitelist.2 = loslobos.company.com
147 whitelist.3 = splunk.dept./*
148 whitelist.4 = 10.10.123.4
149 blacklist.0 = splunk01.dept.company.com
150 blacklist.1 = splunk02.dept.company.com
151 [serverClass:Level2Forwarders:app:DS-all_departments-Input-syslog_generic ]
152
```

Gotchas! (continued)

- Splunk precedence still applies!
- \$SPLUNK_HOME/etc/system/local/*.conf still wins
- The names of your apps still matter
- Splunk configuration layering is king!
- A fun Splunk tongue-twister:

```
grep conf conf.conf | grep -v confdb
```

(run in \$SPLUNK_HOME/etc/system/default)

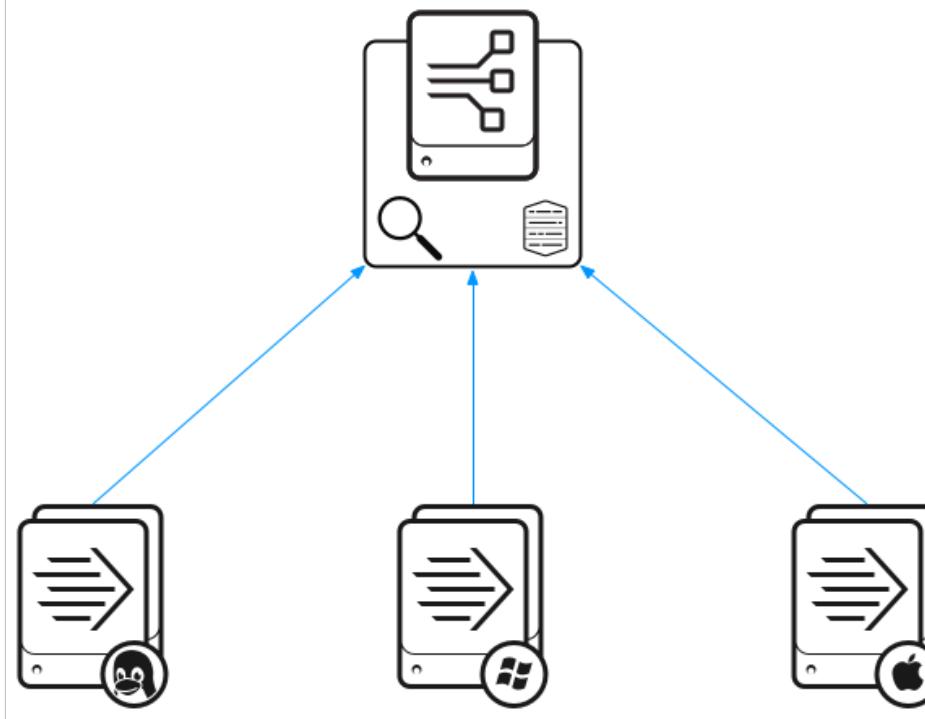
.conf2014

YOUR DATA ADVENTURE

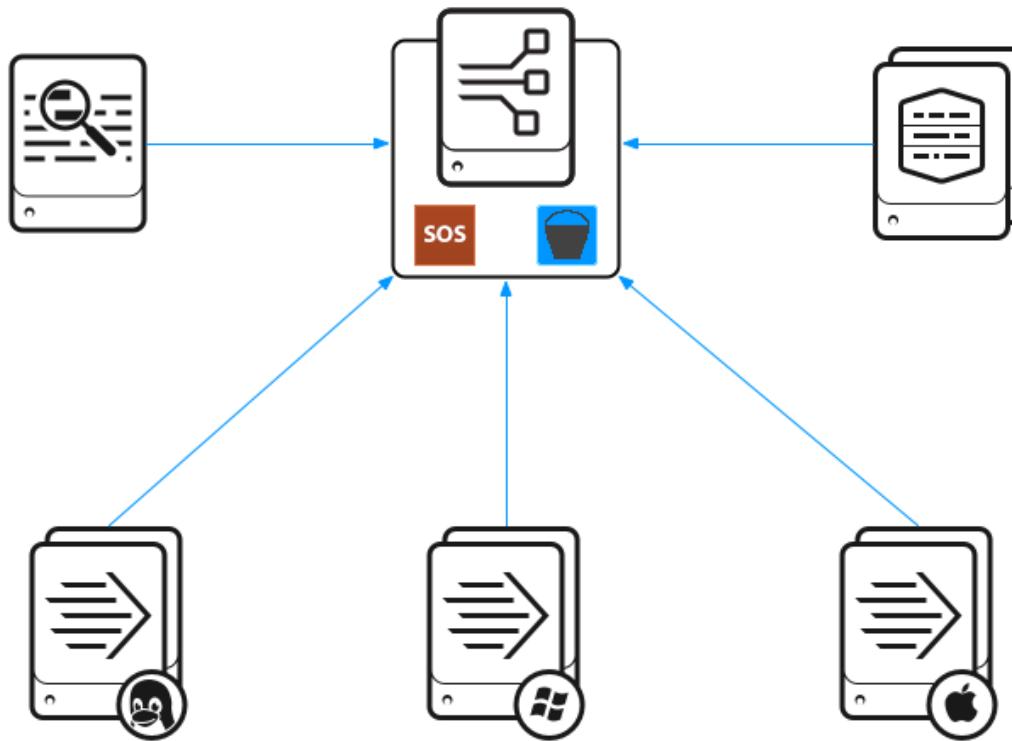
Typical Deployment
Patterns

splunk®

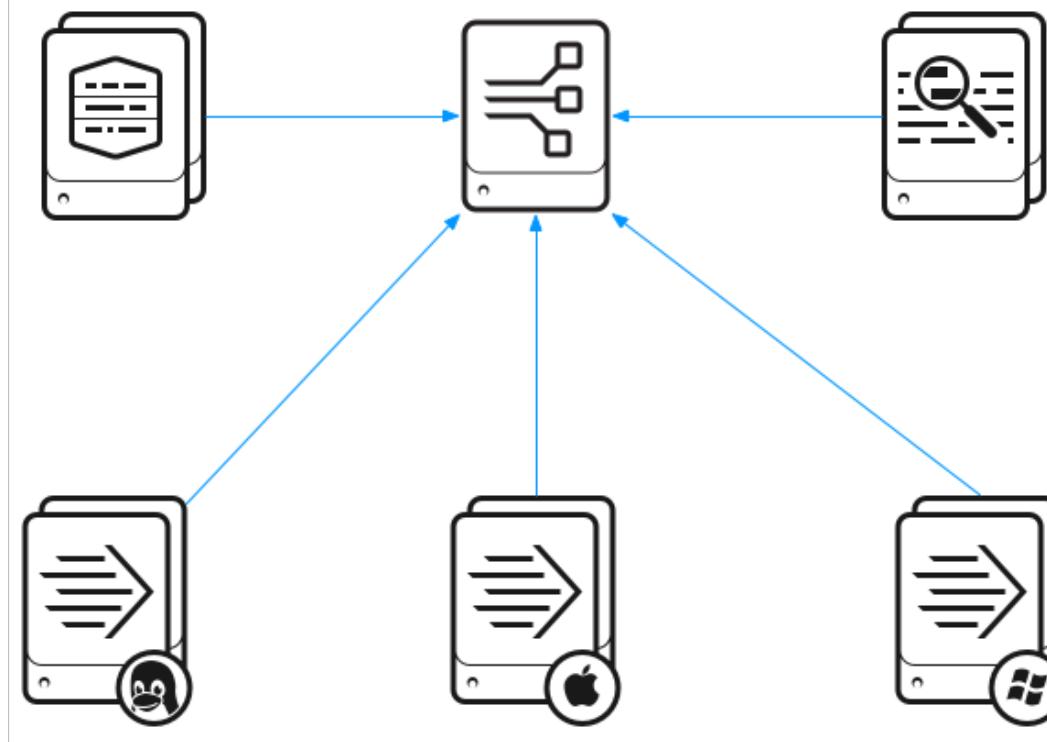
The all-in-one



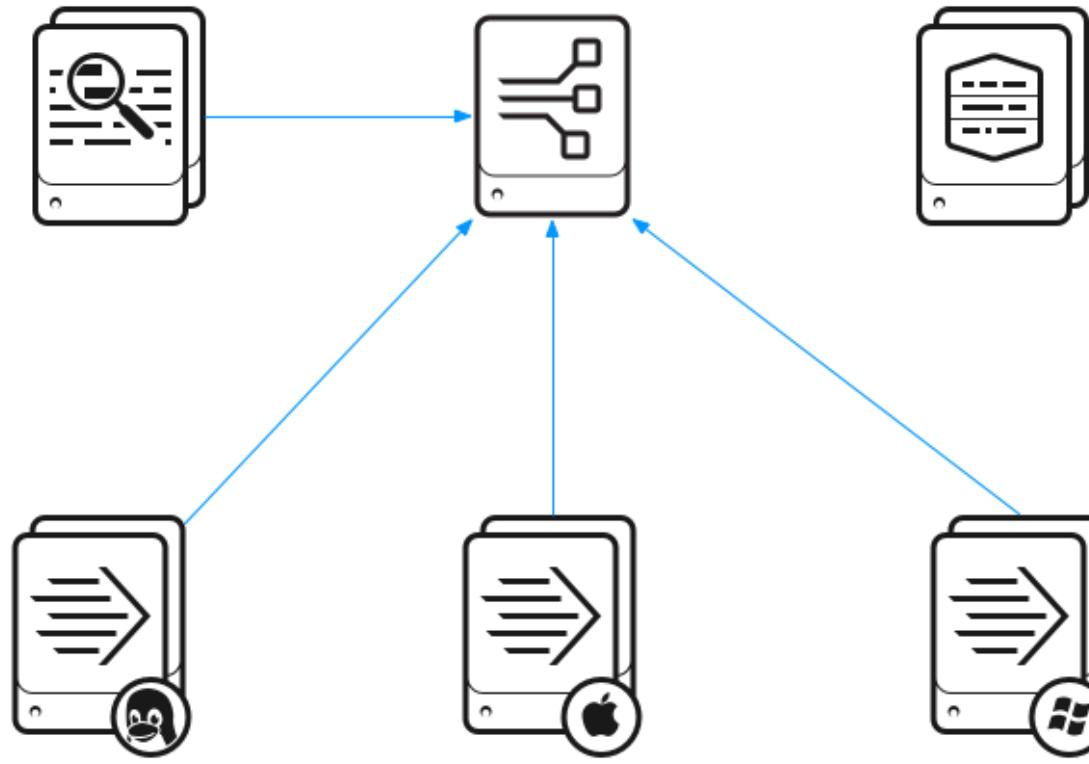
The Admin Server



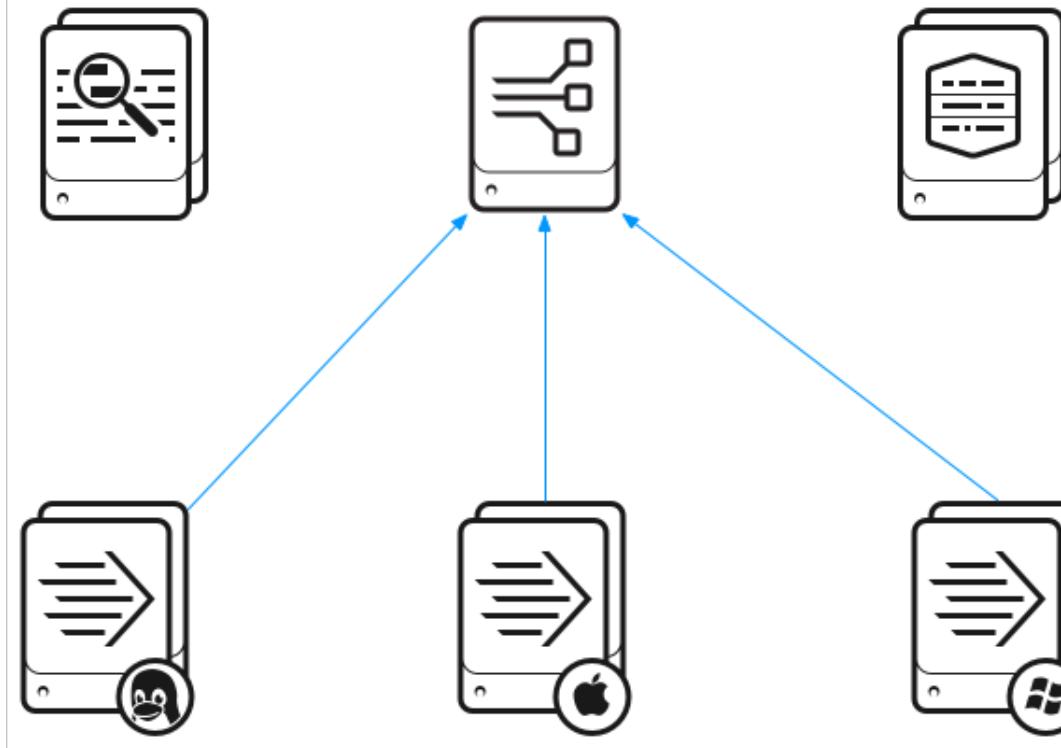
Dedicated Deployment Server



Don't touch my indexers!



Forwarders Only



.conf2014

YOUR DATA ADVENTURE

Advanced tips and tricks

splunk®

Don't chain yourself to a host/IP

- Hosts change (age out, break, need to be upgraded, it's the circle of life)
- If you are using a host name or an IP in your deploymentclient.conf, and that IP or host name changes, that config file will need to be changed EVERYWHERE
- Instead, use a separate DNS record (A or CNAME) to enter into your client configs ("splunk-ds.mycompany.com")

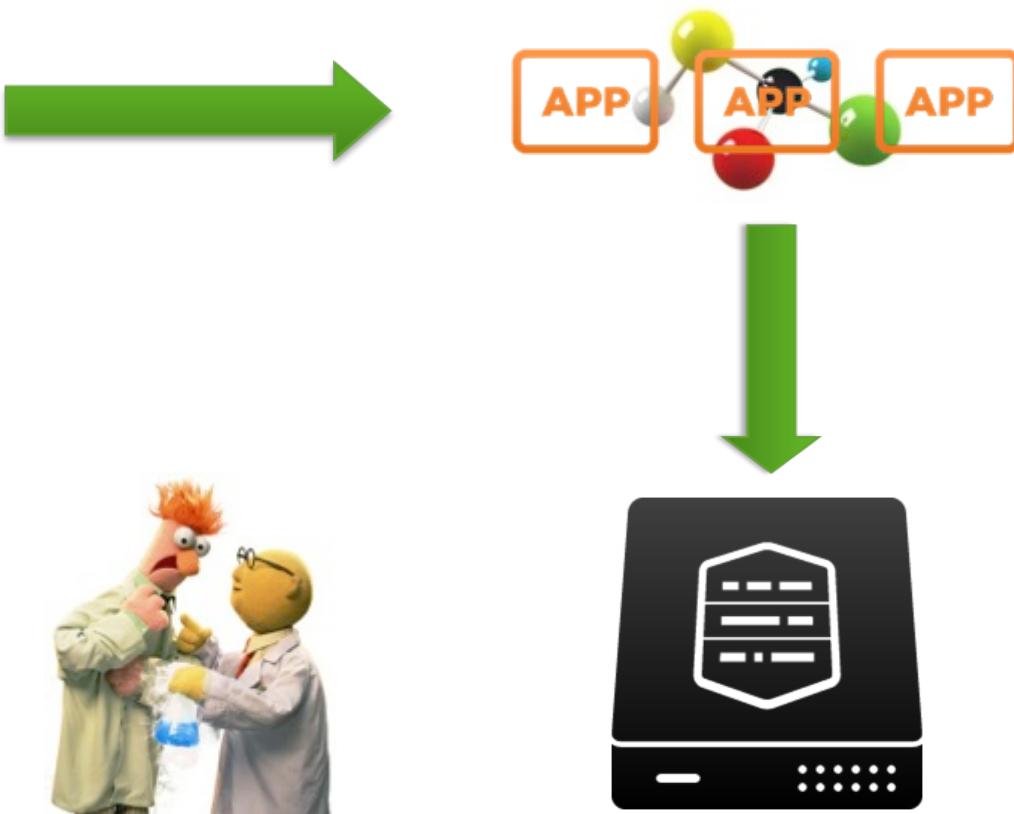
Create smaller, more discrete apps

- Keep the number of config files per app low
- This creates smaller, reusable modules
- Lets you take advantage of Splunk's configuration layering
- Turns out, this is easier to debug
- Use a naming convention for the apps
- Example: DS-<org group>-<class>-<description>
DS-dmz-Output-To_Forwarder
- Create classes of apps
- Input apps
- Index apps
- Web control apps (turn off Splunkweb)

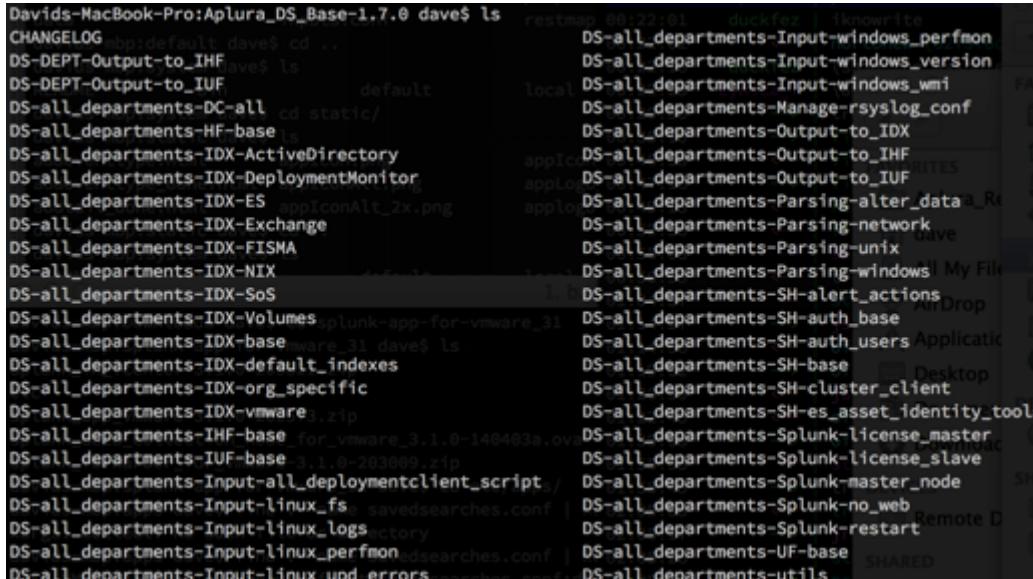


Atomic apps combine to make larger config molecules

inputs.conf 1 				outputs.conf 2 O
indexes.conf 3 lx	alert_actions.conf 4 Aa		app.conf 5 A	audit.conf 6 Au
authentication.conf 7 Al	authorization.conf 8 Ar	datamodels.conf 9 Dm	deploymentclient.conf 10 Dc	serverclass.conf 11 Sc
server.conf 12 S	web.conf 13 W	props.conf/ transforms.conf 14 Pt		



Yes, you may end up with a lot of apps...



A screenshot of a Mac terminal window showing a long list of deployment apps. The list includes various departments like DS-all_departments, DS-all_departments-Input-windows_perfmon, DS-all_departments-Input-windows_version, DS-all_departments-Input-windows_wmi, DS-all_departments-Manage-rsyslog_conf, DS-all_departments-Output-to_IDX, DS-all_departments-Output-to_IHF, DS-all_departments-Output-to_IUF, DS-all_departments-Parsing-alter_dataa_R, DS-all_departments-Parsing-network, DS-all_departments-Parsing-unix, DS-all_departments-Parsing-windows, DS-all_departments-SH-alert_actions, DS-all_departments-SH-auth_base, DS-all_departments-SH-auth_users, DS-all_departments-SH-base, DS-all_departments-SH-cluster_client, DS-all_departments-SH-es_asset_identity_tools, DS-all_departments-Splunk-license_master, DS-all_departments-Splunk-license_slave, DS-all_departments-Splunk-master_node, DS-all_departments-Splunk-no_web, DS-all_departments-Splunk-restart, DS-all_departments-UF-base, and DS-all_departments-utils. The terminal also shows a CHANGELOG file and several .zip files.

```
# find /opt/splunk/etc/deployment-apps props.conf | xargs grep mysourceType
```

- Naming convention + tab auto-completion FTW!
- On Linux? The “find” command is awesome!

Why not larger apps?

- Very hard to reuse
- Configurations quickly become clumsy
- Makes debugging problems more difficult
- Not as flexible



Remember that whole etc/system/local thing?

- Configuration layering always applies!
- Changing your deployment server? Migrating? Rename?
- \$SPLUNK_HOME/etc/system/local/deploymentclient.conf WINS!
- Prepare to touch all your endpoints
- Puppet? Chef? SCOM? Pick your poison
- What about...

Scripted inputs to the rescue

- Can run a script on a regular basis
- Can run on all of the deployment clients
- .sh, .bat
- Rename or remove the \$SPLUNK_HOME/etc/system/local/deploymentclient.conf!
- The “splunk” user should already own the file
- Distribute the app to all systems, or create a server class that only applies to a section of clients

Breaking up serverclass.conf...

- The configs can get long
- Serverclass.conf is like other Splunk config files, stanzas get added to each other

... maybe not

- If you use the Forwarder Management GUI, it may fragment the configs in unexpected ways.
- May be the **one** file we actually only want in system/local



I am a sad panda.

.conf2014

YOUR DATA ADVENTURE

Troubleshooting Splunk
Deployment Server

splunk®

Troubleshooting Deployment Server

- Host != FQDN
- Can the client resolve the name of the deployment server?
- Can the client communicate?
- Use the GUI to check for check-ins from the client
- Settings > Forwarder Management
- Search: `index=_internal source=*splunkd.log ClientSessionManager`
- Check that the correct apps are on the client
- Search from DS:
`index=_internal source=*splunkd.log ClientSessionsManager action=*`

Client: PhoneHome state

New Search

index=_internal source=*splunkd.log component="DC:UpdateServerclassHandler"

Last 15 minutes

46 events (9/9/14 9:24:27.000 AM to 9/9/14 9:39:27.000 AM)

Events (46) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾ < Prev 1 2 3 Next >

i	Time	Event
>	9/9/14 09:38:27.803 AM	09-09-2014 09:38:27.803 -0700 INFO DC:UpdateServerclassHandler - Changed state from=HandlingPhonehome to=Phonehome host = [REDACTED] source = E:\SplunkForwarder\var\log\splunk\splunkd.log sourcetype = splunkd
>	9/9/14 09:38:27.787 AM	09-09-2014 09:38:27.787 -0700 INFO DC:UpdateServerclassHandler - Changed state from=Phonehome to=HandlingPhonehome host = [REDACTED] source = E:\SplunkForwarder\var\log\splunk\splunkd.log sourcetype = splunkd
>	9/9/14 09:38:27.740 AM	09-09-2014 09:38:27.740 -0700 INFO DC:UpdateServerclassHandler - Changed state from=HandlingPhonehome to=Phonehome

< Hide Fields All Fields

Selected Fields

- a host 2
- a source 2
- a sourcetype 1

Interesting Fields

- a component 1

Client: Refreshing a serverclass

New Search

index=_internal source=*splunkd.log component="DeployedServerclass"

Last 15 minutes

104 events (9/9/14 9:25:30.000 AM to 9/9/14 9:40:30.000 AM)

Events (104) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾

< Prev 1 2 3 4 5 6 Next >

< Hide Fields		All Fields		i	Time	Event
Selected Fields					9/9/14 09:39:28.900 AM	INFO DeployedServerclass - name=allsystems Reload; workingDir='E:\Splunk\var\run\allsystems'
a host 2						host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
a source 2					9/9/14 09:39:28.900 AM	INFO DeployedServerclass - name=ParseTA Reload; workingDir='E:\Splunk\var\run\ParseTA'
a sourcetype 1						host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
Interesting Fields					9/9/14 09:39:28.900 AM	INFO DeployedServerclass - name=HeavyForwarders Reload; workingDir='E:\Splunk\var\run\HeavyForwarders'
a component 1						host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
a index 1					9/9/14 09:39:28.900 AM	INFO DeployedServerclass - name=Forwarders, [REDACTED] Reload; workingDir='E:\Splunk\var\run\ForwardersADC-TL2'
# linecount 1						host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
a splunk_server 12						

Client: Downloading and installing apps

New Search

index=_internal source=*splunkd.log component="DeployedApplication" host= [REDACTED]

Last 24 hours

✓ 12 events (9/8/14 9:00:00.000 AM to 9/9/14 9:41:47.000 AM)

Job Fast Mode

Events (12) Statistics Visualization

Format Timeline List Format 20 Per Page

<input type="checkbox"/> Hide Fields	All Fields	i	Time	Event
Selected Fields		>	9/8/14 4:27:16.219 PM	09-08-2014 16:27:16.219 -0700 INFO DeployedApplication - Installing app=Splunk_TA_nix to='E:\Splunk\etc\apps\Splunk_TA_nix' host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
a host 1		>	9/8/14 4:27:16.063 PM	09-08-2014 16:27:16.063 -0700 INFO DeployedApplication - Downloaded url=[REDACTED]:8089/services/streams/deployment?name=default:ParseTA:Splunk_TA_nix to file='E:\Splunk\var\run\ParseTA\Splunk_TA_nix-1410218690.bundle' sizeKB=1120 host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
a source 1		>	9/8/14 4:27:16.048 PM	09-08-2014 16:27:16.048 -0700 INFO DeployedApplication - Checksum mismatch 0 <> 15310549620697355544 for app=Splunk_TA_nix. Will reload from='[REDACTED]:8089/services/streams/deployment?name=default:ParseTA:Splunk_TA_nix' host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
a sourcetype 1				
Interesting Fields				
a component 1				
a index 1				
# linecount 1				
a splunk_server 2				

Client: PhoneHome

New Search

index=_internal source=*splunkd.log component="DC:PhoneHomeThread"| Last 24 hours

172 events (9/8/14 9:00:00.000 AM to 9/9/14 9:44:38.000 AM)

Events (172) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾ 1 2 3 4 5 6 7 8 9 Next < Prev

i	Time	Event
>	9/8/14 8:40:21.974 PM	09-08-2014 20:40:21.974 -0700 INFO DC:PhonehomeThread - handshakeRetryInterval=12000 ms host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	9/8/14 8:40:21.974 PM	09-08-2014 20:40:21.974 -0700 INFO DC:PhonehomeThread - Phonehome thread start, intervals: handshakeRetry=0 phonehome=60. host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	9/8/14 8:28:14.583 PM	09-08-2014 20:28:14.583 -0700 INFO DC:PhonehomeThread - handshakeRetryInterval=12000 ms host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	9/8/14 8:28:14.583 PM	09-08-2014 20:28:14.583 -0700 INFO DC:PhonehomeThread - Phonehome thread start, intervals: handshakeRetry=0 phonehome=60. host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

< Hide Fields All Fields

Selected Fields

- a host 38
- a source 2
- a sourcetype 1

Interesting Fields

- a component 1
- a index 1

Server: PhoneHome

index=_internal source="/opt/splunk/var/log/splunk/splunkd_access.log" uri="/services/broker/phonehome/connection*" Last 15 minutes

✓ 839 events (9/17/14 4:55:29.000 PM to 9/17/14 5:10:29.000 PM) Job ▾ || ↻ ↴ Verbose Mode ▾

Events (839) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields		All Fields		i	Time	Event
				>	9/17/14 5:10:28.359 PM	1 [17/Sep/2014:17:10:28.359 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
Selected Fields						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
a host 1				>	9/17/14 5:10:27.960 PM	1 [17/Sep/2014:17:10:27.960 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
a index 1						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
a source 1				>	9/17/14 5:10:26.837 PM	1 [17/Sep/2014:17:10:26.837 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
a sourcetype 1						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
Interesting Fields				>	9/17/14 5:10:26.360 PM	1 [17/Sep/2014:17:10:26.360 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
# bytes 22						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
a clientip 49				>	9/17/14 5:10:23.099 PM	1 [17/Sep/2014:17:10:23.099 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
# date_hour 2						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
# date_mday 1				>	9/17/14 5:10:23.099 PM	1 [17/Sep/2014:17:10:23.099 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
# date_minute 16						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
a date_month 1				>	9/17/14 5:10:23.099 PM	1 [17/Sep/2014:17:10:23.099 -0700] "POST /services/broker/phonehome/connection_1 host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access
# date_second 40						host = index = _internal source = /opt/splunk/var/log/splunkd_access.log sourcetype = splunkd_access

Server: Recording client check-ins

New Search

```
index=_internal source=*splunkd.log component=ClientSessionsManager "Adding client"
```

581 events (9/12/14 12:00:00.000 AM to 9/13/14 12:00:00.000 AM)

Job ▾ | Verbose Mode ▾

Events (581) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 50 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields	All Fields	i	Time	Event
Selected Fields			> 9/12/14 6:07:03.281 PM	09-12-2014 18:07:03.281 -0700 INFO ClientSessionsManager - Adding client: ip=██████████ uts=linux-x86_6 eventtype = splunkd-log host = ██████████ message = Adding client: ip=██████████ uts=linux-x86_64 id=d972828060bc3ebfd0584a6f0f44a418 name=DC-all source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
a eventtype 1			> 9/12/14 6:07:03.279 PM	09-12-2014 18:07:03.279 -0700 INFO ClientSessionsManager - Adding client: ip=██████████ uts=linux-x86_6 eventtype = splunkd-log host = ██████████ message = Adding client: ip=██████████ uts=linux-x86_64 id=0b44a6276b0188064a3da99b7a499a2d name=DC-all source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
a host 1				
a message 47				
a name 1				
a source 1				
a sourcetype 1				
Interesting Fields			> 9/12/14 6:07:02.184 PM	09-12-2014 18:07:02.184 -0700 INFO ClientSessionsManager - Adding client: ip=██████████ uts=linux-x86_6 eventtype = splunkd-log host = ██████████ message = Adding client: ip=██████████ uts=linux-x86_64 id=70b7a44a5261b6d165f65a92765a80f2 name=DC-all source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
a component 1				
# date_hour 4				
# date_mday 1				
# date_minute 22			> 9/12/14 09-12-2014 18:07:01.864 -0700 INFO ClientSessionsManager - Adding client: ip=██████████ uts=linux-x86_6	

Server: List the deployment clients

A screenshot of a Splunk search interface. The search bar contains the command: `| rest /services/deployment/server/clients splunk_server=local | table hostname dns clientName utsname`. The search results show 0 events from 12/31/69 4:00:00.000 PM to 9/12/14 12:00:00.000 AM. The results table has four columns: hostname, dns, clientName, and utsname. The data shows five rows of deployment client information.

hostname	dns	clientName	utsname
[REDACTED]	[REDACTED].com	DC-all	linux-x86_64
[REDACTED]	[REDACTED].com	DC-all	linux-x86_64
[REDACTED]	[REDACTED].com	DC-all	windows-intel
[REDACTED]	[REDACTED].com	DC-all	linux-x86_64
[REDACTED]	[REDACTED].com	DC-all	linux-x86_64

Server: Loading classes and apps

New Search

index=_internal source=*splunkd.log component="ServerClass"

Last 24 hours

✓ 146 events (9/8/14 9:00:00.000 AM to 9/9/14 9:46:21.000 AM)

Job

Events (146) Statistics Visualization

Format Timeline 20 Per Page < Prev 1 2 3 4 5 6 7 8 Next >

Hide Fields	All Fields	i	Time	Event
Selected Fields host 1 source 1 sourcetype 1		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO Serverclass - Reloading application=DS-all_departments-Input-windows_rsa from location='/opt/splunk/etc/deployment-apps' host = i [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO Serverclass - Reloading serverclass=windows_rsa_input from repository='/opt/splunk/etc/deployment-apps' host = i [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO Serverclass - Reloading application=DS-all_departments-Input-windows_dhcp from location='/opt/splunk/etc/deployment-apps' host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO Serverclass - Reloading serverclass=windows_dhcp_input from repository='/opt/splunk/etc/deployment-apps'
Interesting Fields component 1 index 1 linecount 1 splunk_server 1		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO Serverclass - Reloading application=DS-all_departments-Input-windows_dhcp from location='/opt/splunk/etc/deployment-apps' host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO Serverclass - Reloading serverclass=windows_dhcp_input from repository='/opt/splunk/etc/deployment-apps'

Server: Reload

New Search

index=_internal source=*splunkd.log component="DSManager" host="██████████"]

Last 7 days

✓ 27 events (9/2/14 9:00:00.000 AM to 9/9/14 9:47:42.000 AM)

Job

Events (27) Statistics Visualization

Format Timeline 20 Per Page 1 2 Next >

Hide Fields	All Fields	i	Time	Event
Selected Fields		>	9/8/14 4:24:51.409 PM	09-08-2014 16:24:51.409 -0700 INFO DSManager - Loaded count=26 configured SCs host = ██████████ source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
a host 1		>	9/8/14 4:24:50.463 PM	09-08-2014 16:24:50.463 -0700 INFO DSManager - Shutdown serverclassess host = ██████████ source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
a source 1		>	9/5/14 5:00:24.536 PM	09-05-2014 17:00:24.536 -0700 INFO DSManager - Loaded count=26 configured SCs host = ██████████ source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
Interesting Fields				

Server: Reload (oops!)

	2:42:28.348 PM	host = [REDACTED]	source = /opt/splunk/var/log/splunk/splunkd.log	sourcetype = splunkd
>	9/5/14 2:42:27.709 PM	09-05-2014 14:42:27.709 -0700 INFO DSManager - Shutdown serverclassess		
>	9/4/14 4:53:02.971 PM	09-04-2014 16:53:02.971 -0700 INFO DSManager - Loaded count=26 configured SCs		
>	9/4/14 4:53:02.337 PM	09-04-2014 16:53:02.337 -0700 INFO DSManager - Shutdown serverclassess	sourcetype = splunkd	
>	9/4/14 3:42:19.753 PM	09-04-2014 15:42:19.753 -0700 INFO DSManager - Loaded count=26 configured SCs	sourcetype = splunkd	
>	9/4/14 3:35:37.491 PM	09-04-2014 15:35:37.491 -0700 INFO DSManager - Shutdown serverclassess	sourcetype = splunkd	
>	9/4/14 3:35:24.576 PM	09-04-2014 15:35:24.576 -0700 ERROR DSManager - Failed to reload serverclass=ParseTA: Failed to create dir=/opt/splunk/etc/deployment-apps/TA-livedata/local, needed for application=TA-livedata: Permission denied	host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log	sourcetype = splunkd

Server: Updating app installs

New Search

index=_internal source=*splunkd.log component="ClientSessionsManager" host="..." | Last 7 days

5,665 events (9/2/14 9:00:00.000 AM to 9/9/14 9:49:23.000 AM)

Events (5,665) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields		All Fields		i	Time	Event
Selected Fields						
a host 1						
a source 1						
a sourcetype 1						
Interesting Fields						
a component 1						
a index 1						
# linecount 1						
a splunk_server 14						
> 9/8/14 6:55:02.147 PM						09-08-2014 18:55:02.147 -0700 INFO ClientSessionsManager - ip='...' name=DC-all Updating record for sc=ParseTA app=TA-livedata: action=Install result=Ok host = ... source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
> 9/8/14 6:55:02.147 PM						09-08-2014 18:55:02.147 -0700 INFO ClientSessionsManager - ip='...' name=DC-all New record for sc=ParseTA app=TA-livedata: action=Download result=Ok host = i... source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
> 9/8/14 6:55:02.147 PM						09-08-2014 18:55:02.147 -0700 INFO ClientSessionsManager - ip='...' name=DC-all New record for sc=ParseTA app=Splunk_TA_nix: action=Download result=Ok host = ... source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
> 9/8/14 6:55:02.147 PM						09-08-2014 18:55:02.147 -0700 INFO ClientSessionsManager - ip='...' name=DC-all Updating record for sc=All-Linux app=Splunk_TA_nix: action=Install result=Ok host = i... source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
> 9/9/14 9:49:23.000 AM						09-09-2014 12:55:02.147 -0700 INFO ClientSessionsManager - ip='...' name=DC-all New record for

Oh yeah, Forwarder Management

The screenshot shows a dashboard for managing forwarders. At the top, there are three summary metrics: "47 Clients PHONED HOME IN THE LAST 24 HOURS", "0 Clients DEPLOYMENT ERRORS", and "0 Total downloads". Below these are tabs for "Apps (112)", "Server Classes (26)", and "Clients (47)", with "Clients (47)" being the active tab. A search bar includes filters for "Phone Home: All" and "All Clients", and a "filter" input field. A pagination control shows "20 Per Page" and page numbers 1, 2, 3. The main table lists 11 client entries, each with a "Delete Record" action, machine type (e.g., linux-x86_64, windows-intel), deployment count (e.g., 42 deployed, 53 deployed), and a timestamp (e.g., a few seconds ago, a minute ago). The last entry is partially visible.

i	Host Name	Client Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>		DC-all		Delete Record	linux-x86_64	42 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a minute ago
>		DC-all		Delete Record	windows-intel	4 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago
>		DC-all		Delete Record	linux-x86_64	53 deployed	a few seconds ago

Oh yeah, Forwarder Management

The screenshot shows a web-based management interface for Splunk Forwarder Management. At the top, there are three tabs: "Apps (114)", "Server Classes (26)", and "Clients (1)". Below the tabs, there are dropdown menus for "Phone Home: All" and "All Clients", followed by a search bar containing a blurred IP address. A "10 Per Page" link is also present. The main table displays a single forwarder entry:

i	Host Name	Client Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
▼	██████████	DC-all	██████████	Delete Record	windows-intel	4 deployed	a few seconds ago

Below the table, detailed information about the forwarder is shown:

- Apps**: DS-I█████-To_Forwarders-outputs, DS-all_departments-DeploymentClient-all, DS-all_departments-Input-windows_logs , more apps
- Server Classes**: All-Windows, Forwarders!██████████, PragmaLineInputs , more server classes

Serverclass.xml

- Present on the clients
- Is a copy of the response from the deployment server to the deployment client
- Tells you which server classes the client thinks it belongs to, and which apps it thinks it should have
- But, it's all the way out on the endpoint
- If only we had a way to capture this data, and bring it to a central repository, perhaps index it so that we might be able to search it later ;-)

.conf2014

YOUR DATA ADVENTURE

Scaling Splunk
Deployment Server

splunk®

How much Deployment Server do I need?

- Not a lot of clients? Maybe a small VM
- Moar clients? MOAR SERVER!



What if I have a lot of clients?

- Lots of clients = lots of check-ins
- Current maximum number of clients per Deployment server is:
- Windows: 500 – 2,000 (closer to the bottom one)
- Linux: 5,000 – 10,000
- (note that this is using reference hardware)
- By default, these clients check in every minute

Change the default phoneHomeIntervalInSecs

- Found in deploymentclient.conf
- Defaults to 60 seconds
- How often are you changing those configs?
- Five minutes? Thirty minutes?
- Play the numbers game

No, really, I mean ALOT of clients

- Currently no built-in solution
- May mean having multiple deployment servers



Dedicated or Collocated?

- Keep in mind, there will be a lot of connections
- You don't want to run out of sockets
- What if you need to restart the deployment server?
- Remember, a deployment server can't be a client of itself
- Deployment server + license master works well
- If the server that the deployment server is on isn't a client of itself, you have to manage its configuration another way
- Can lead to configuration mismatches and inconsistency

Load balancing?

- Does not work as expected
- Remember that hash? Yeah, that's the reason
- Not just the files and contents
- Includes modified time and other info
- If the hash doesn't match what the client currently has, it will grab a "new" version. This could mean a loop of restarts (fun!)



FIN

- Some other talks to check out:
 - Avoid the SSLippery Slope of Default SSL - Duane Waddle and George Starcher
 - Using Lesser Known Commands in Splunk Search Processing Language (SPL) - Kyle Smith
 - Masters of IRC Community Panel
 - Building a Common Information Model (CIM) Compliant Technical Add-on (TA)
 - Brian Wooden and Jack Coates
 - Curating User Experience: Dashboarding Tips and Tricks – Sanford Owings
 - Getting The Most Out of Your Splunk License: Keeping the Junk Out of Splunk – David Paper
 - How Splunkd Works – Amrit Bath and Jag Karai



.conf2014

YOUR DATA ADVENTURE

THANK YOU

splunk®