

.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 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.

.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 derver
 - 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?



“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_17...  
5:10:27.960 PM ..._53_8089_..._DC-all HTTP/1.0" 200 24 - - - 2ms  
host = ... 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= [REDACTED] uts=linux-x
6:30:06.244 PM 86_64 id=589025c9d87908d473e1b8af83bad99e name=DC-all
host = [REDACTED] | 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:\Splunk
10:06:29.680 AM kForwarder\var\run\All-Windows'
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?



“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.”

```
node /opt/splunk/bin/splunkd --source /opt/splunk/var/log/splunk/splunkd.log --sourcetype = splunkd
> 9/8/14 09-08-2014 18:55:02.016 -0700 INFO DeployedApplication - Checksum mismatch 11961082866254951452 <> 15310549620697355544 for a
6:55:02.016 PM pp=Splunk_TA_nix. Will reload from=':8089/services/streams/deployment?name=default:ParseTA:Splunk_TA_nix'
host = : source = /opt/splunk/var/log/splunk/splunkd.log | sourcetype = splunkd
```

How does this work?



“I need the latest version of Outputs_To_Indexers.”

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

How does this work?



“Sure, here you go.”

```
> 9/8/14 09-08-2014 18:55:02.053 -0700 INFO DeployedApplication - Downloaded url=j[redacted]: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 = [redacted] | 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 09-08-2014 18:55:01.972 -0700 INFO DeployedApplication - Installing app=Splunk_TA_nix to='/opt/splunk/e
6:55:01.972 PM tc/apps/Splunk_TA_nix'
host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
```

```
> 9/10/14 09-10-2014 12:13:38.805 -0700 INFO ClientSessionsManager - ip=[REDACTED] name=DC-all Updating record
12:13:38.805 PM 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[REDACTED]
```

Things to remember

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



.conf2014

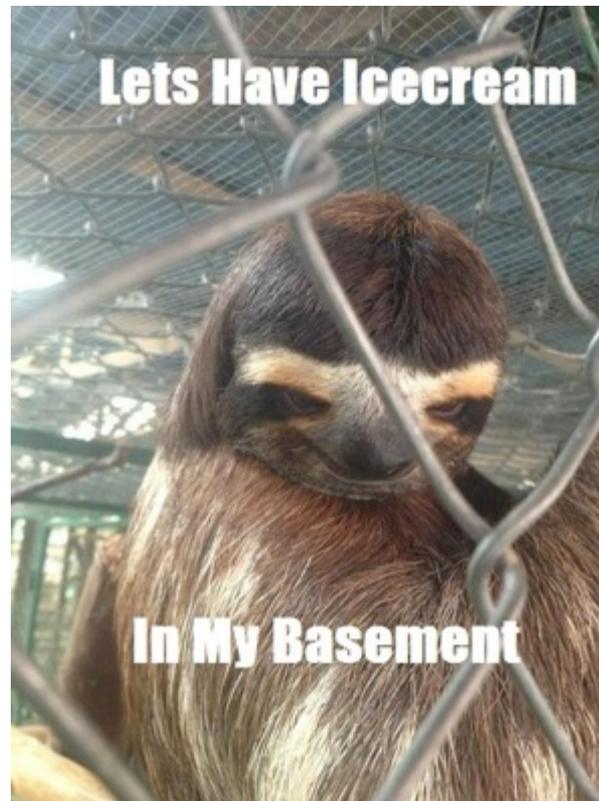
YOUR DATA ADVENTURE

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 9 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 with: nt=00 rt=3 sr=1 ct=00 st=00 ft=00 rct=00 rst=00 rrt=00 rmst=000 rrrt=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 core 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`)

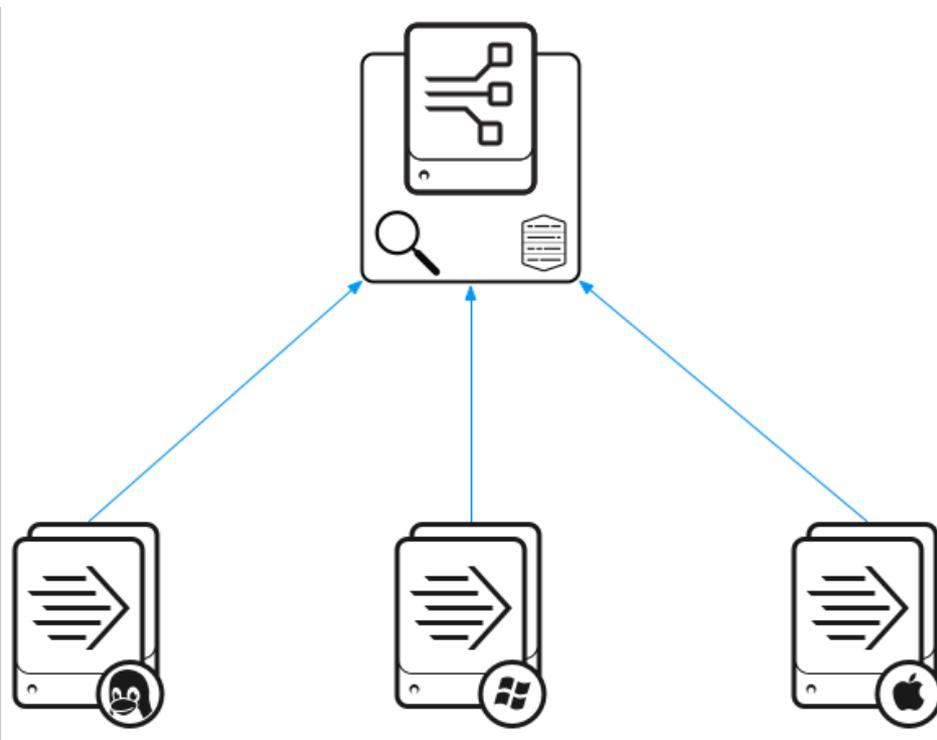
.conf2014

YOUR DATA ADVENTURE

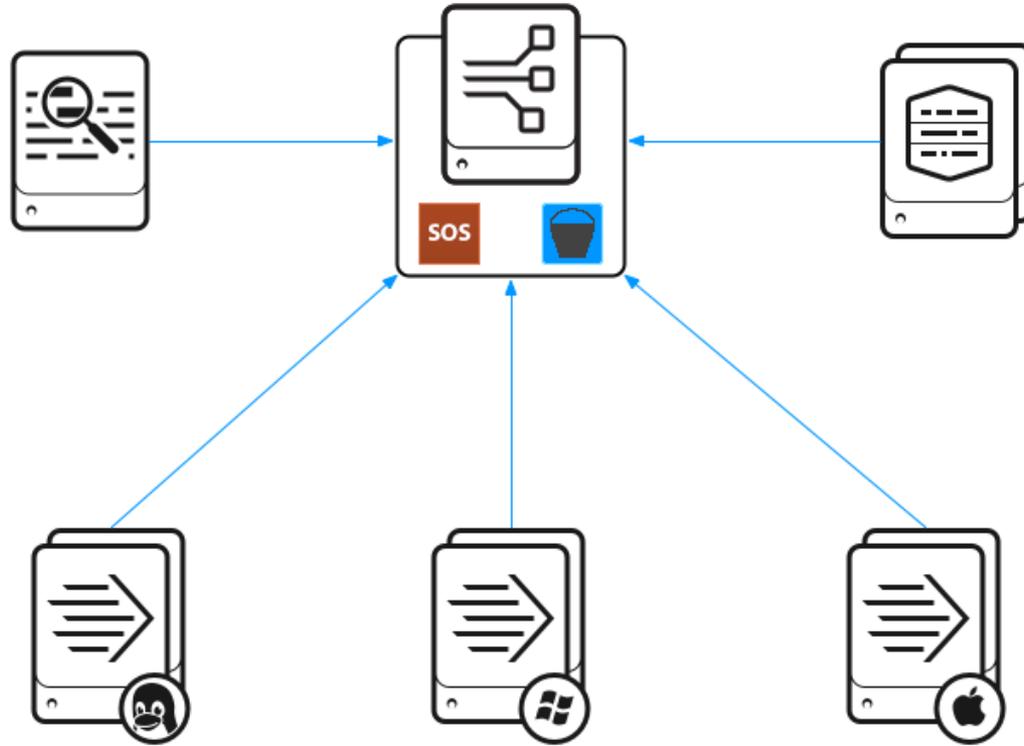
Typical Deployment
Patterns

splunk>

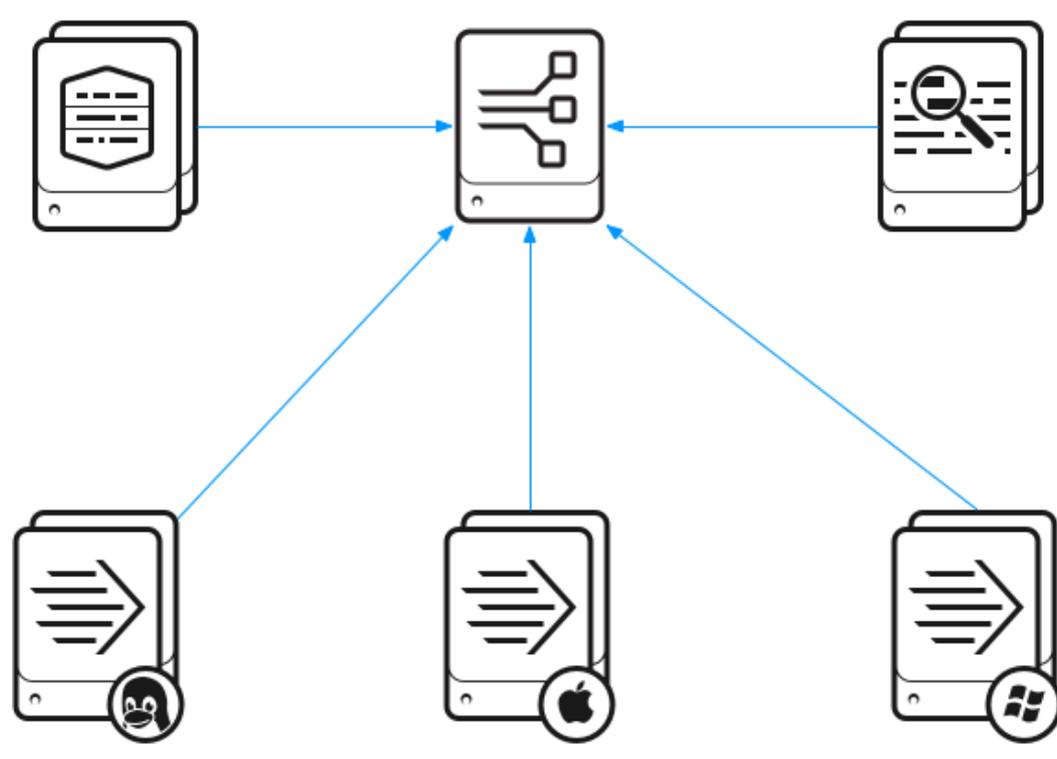
The all-in-one



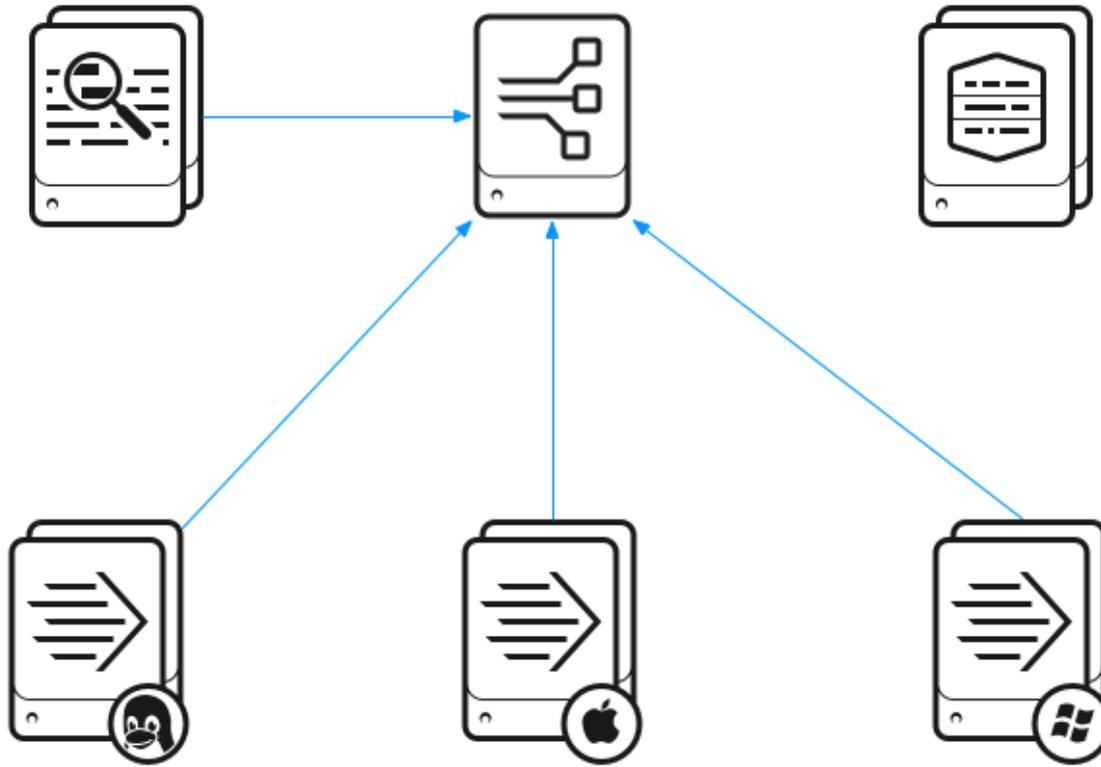
The Admin Server



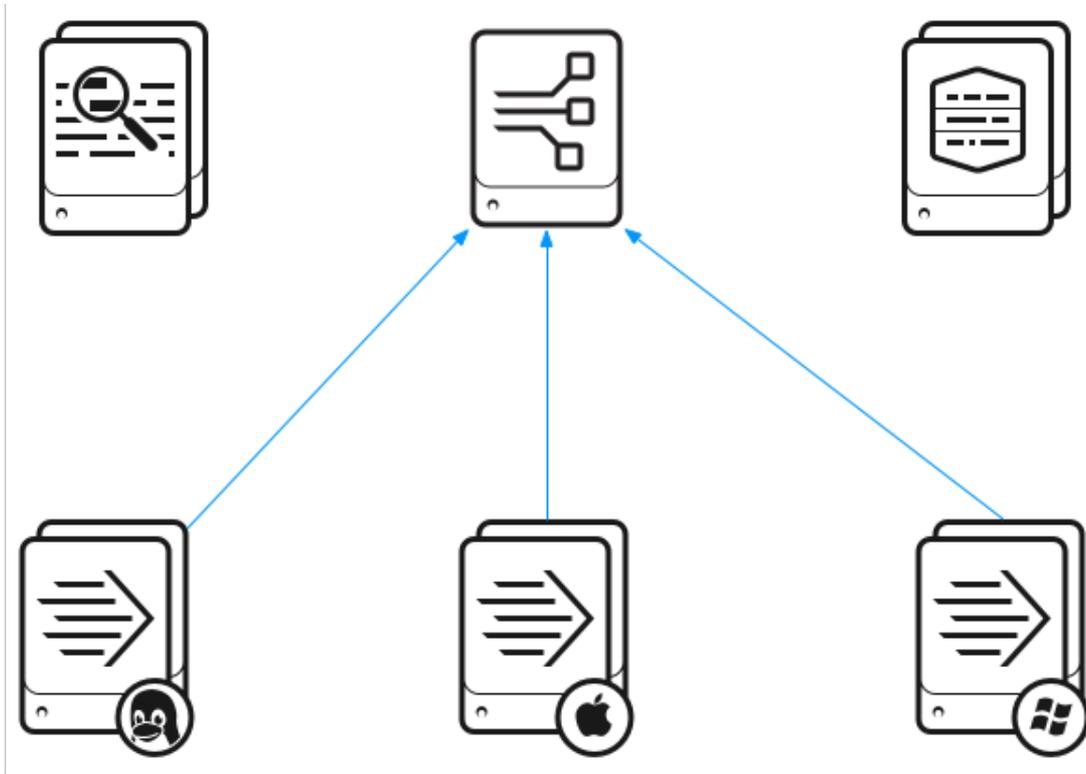
Dedicated Deployment Server



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 I				outputs.conf 2 O
indexes.conf 3 Ix	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...

```
Davids-MacBook-Pro:Aplura_DS_Base-1.7.0 dave$ ls
CHANGELOG
DS-DEPT-Output-to_IHF
DS-DEPT-Output-to_IUF
DS-all_departments-DC-all
DS-all_departments-HF-base
DS-all_departments-IDX-ActiveDirectory
DS-all_departments-IDX-DeploymentMonitor
DS-all_departments-IDX-ES
DS-all_departments-IDX-Exchange
DS-all_departments-IDX-FISMA
DS-all_departments-IDX-NIX
DS-all_departments-IDX-SoS
DS-all_departments-IDX-Volumes
DS-all_departments-IDX-base
DS-all_departments-IDX-default_indexes
DS-all_departments-IDX-org_specific
DS-all_departments-IDX-vmware
DS-all_departments-IHF-base
DS-all_departments-IUF-base
DS-all_departments-Input-all_deploymentclient_script
DS-all_departments-Input-linux_fs
DS-all_departments-Input-linux_logs
DS-all_departments-Input-linux_perfmon
DS-all_departments-Input-linux_und_errors
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_data
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
DS-all_departments-utils
```

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

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

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

The screenshot shows a Splunk search interface with the following details:

- Search Query:** `index=_internal source=*splunkd.log component="DC:UpdateServerclassHandler"`
- Time Range:** Last 15 minutes
- Results:** 46 events (9/9/14 9:24:27.000 AM to 9/9/14 9:39:27.000 AM)
- Navigation:** Job, Fast Mode, and pagination controls (1, 2, 3, Next).
- Fields:** `host`, `source`, `sourcetype`
- Event Log:**

i	Time	Event
>	9/9/14 9:38:27.803 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 9:38:27.787 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 9:38:27.740 AM	09-09-2014 09:38:27.740 -0700 INFO DC:UpdateServerclassHandler - Changed state from=HandlingPhonehome to=Phonehome

Client: Refreshing a serverclass

New Search Save As Close

index=_internal source=*splunkd.log component="DeployedServerclass" Last 15 minutes Q

✓ 104 events (9/9/14 9:25:30.000 AM to 9/9/14 9:40:30.000 AM) Job || ■ ↶ ↓ 🔄 ⚡ Fast Mode

Events (104) Statistics Visualization

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

		i	Time	Event
< Hide Fields ≡ All Fields Selected Fields a host 2 a source 2 a sourcetype 1 Interesting Fields a component 1 a index 1 # linecount 1 a splunk_server 12	>		9/9/14 9:39:28.900 AM	09-09-2014 09:39:28.900 -0700 INFO DeployedServerclass - name=allsystems Reload; workingDir='E:\Splunk\var\run\allsystems' host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
	>		9/9/14 9:39:28.900 AM	09-09-2014 09:39:28.900 -0700 INFO DeployedServerclass - name=ParseTA Reload; workingDir='E:\Splunk\var\run\ParseTA' host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
	>		9/9/14 9:39:28.900 AM	09-09-2014 09:39:28.900 -0700 INFO DeployedServerclass - name=HeavyForwarders Reload; workingDir='E:\Splunk\var\run\HeavyForwarders' host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
	>		9/9/14 9:39:28.900 AM	09-09-2014 09:39:28.900 -0700 INFO DeployedServerclass - name=Forwarders, [REDACTED] Reload; workingDir='E:\Splunk\var\run\ForwardersADC-TL2' host = [REDACTED] source = E:\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd

Client: Downloading and installing apps

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** `index=_internal source=*splunkd.log component="DeployedApplication" host=`
- Time Range:** Last 24 hours
- Results:** 12 events (9/8/14 9:00:00.000 AM to 9/9/14 9:41:47.000 AM)
- Navigation:** Events (12), Statistics, Visualization
- Format:** Timeline, List, Format, 20 Per Page
- Fields:** host, source, sourcetype
- Log Entries:**
 - 9/8/14 4:27:16.219 PM: DeployedApplication - Installing app=Splunk_TA_nix to='E:\Splunk\etc\apps\Splunk_TA_nix'
 - 9/8/14 4:27:16.063 PM: DeployedApplication - Downloaded url=i...:8089/services/streams/deployment?name=default:ParseTA:Splunk_TA_nix to file='E:\Splunk\var\run\ParseTA\Splunk_TA_nix-1410218690.bundle' sizeKB=1120
 - 9/8/14 4:27:16.048 PM: DeployedApplication - Checksum mismatch 0 <> 15310549620697355544 for app=Splunk_TA_nix. Will reload from='...:8089/services/streams/deployment?name=default:ParseTA:Splunk_TA_nix'

Client: PhoneHome

New Search Save As Close

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

✓ 172 events (9/8/14 9:00:00.000 AM to 9/9/14 9:44:38.000 AM) Job || ■ → ↓ 🖨 ⚡ Fast Mode

Events (172) Statistics Visualization

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

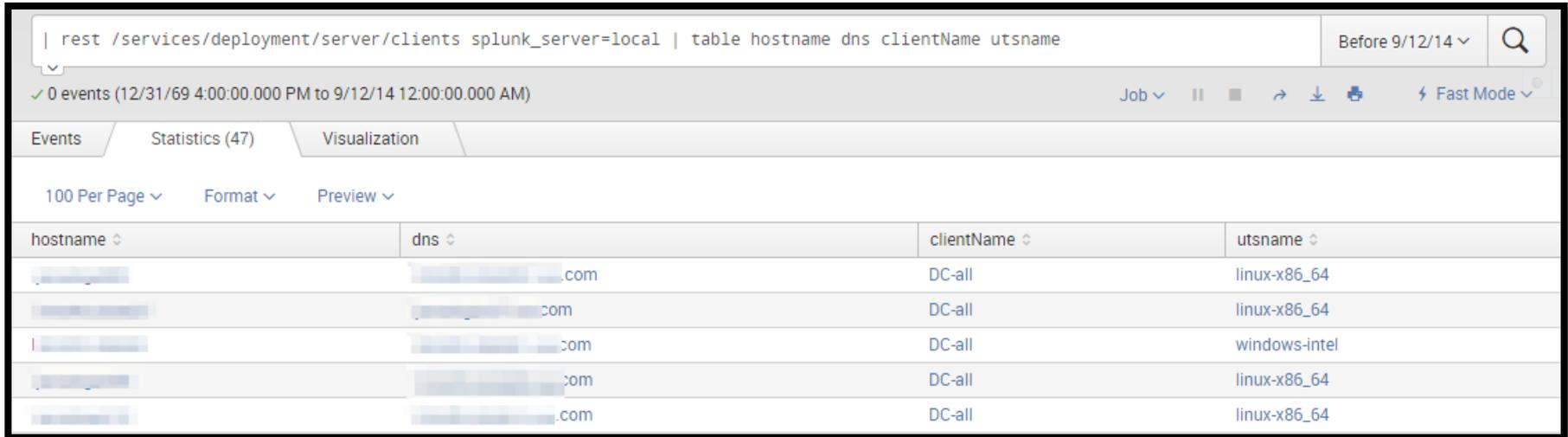
< Hide Fields All Fields	i	Time	Event
Selected Fields a host 38 a source 2 a sourcetype 1	>	9/8/14 8:40:21.974 PM	09-08-2014 20:40:21.974 -0700 INFO DC:PhonehomeThread - handshakeRetryInterval=12000 ms host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
	>	9/8/14 8:40:21.974 PM	09-08-2014 20:40:21.974 -0700 INFO DC:PhonehomeThread - Phonehome thread start, intervals: handshakeRet ry=0 phonehome=60. host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
Interesting Fields a component 1 a index 1	>	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: handshakeRet ry=0 phonehome=60. host = [REDACTED] source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

Server: Recording client check-ins

The screenshot shows a Splunk search interface with the following search query: `index=_internal source=*splunkd.log component=ClientSessionsManager "Adding client"`. The search results show 581 events from 9/12/14 12:00:00.000 AM to 9/13/14 12:00:00.000 AM. The results are displayed in a table with columns for index, time, and event details.

i	Time	Event
>	9/12/14 6:07:03.281 PM	09-12-2014 18:07:03.281 -0700 INFO ClientSessionsManager - Adding client: ip=[redacted] uts=linux-x86_64 id=d972828060bc3ebfd0584a6f0f44a418 name=DC-all eventtype = splunkd-log ; host = [redacted] ; message = Adding client: ip=[redacted] uts=linux-x86_64 id=d972828060bc3ebfd0584a6f0f44a418 name = DC-all ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd
>	9/12/14 6:07:03.279 PM	09-12-2014 18:07:03.279 -0700 INFO ClientSessionsManager - Adding client: ip=[redacted] uts=linux-x86_64 id=0b44a6276b0188064a3da99b7a499a2d name=DC-all eventtype = splunkd-log ; host = [redacted] ; message = Adding client: ip=[redacted] uts=linux-x86_64 id=0b44a6276b0188064a3da99b7a499a2d name = DC-all ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd
>	9/12/14 6:07:02.184 PM	09-12-2014 18:07:02.184 -0700 INFO ClientSessionsManager - Adding client: ip=[redacted] uts=linux-x86_64 id=70b7a44a5261b6d165f65a92765a80f2 name=DC-all eventtype = splunkd-log ; host = [redacted] ; message = Adding client: ip=[redacted] uts=linux-x86_64 id=70b7a44a5261b6d165f65a92765a80f2 name = DC-all ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd
>	9/12/14	09-12-2014 18:07:01.864 -0700 INFO ClientSessionsManager - Adding client: ip=[redacted] uts=linux-x86_64 id=[redacted] name=DC-all eventtype = splunkd-log ; host = [redacted] ; message = Adding client: ip=[redacted] uts=linux-x86_64 id=[redacted] name = DC-all ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd

Server: List the deployment clients



The screenshot shows a Splunk search interface. The search bar contains the query: `| rest /services/deployment/server/clients splunk_server=local | table hostname dns clientName utsname`. The search results show 0 events for the time range 12/31/69 4:00:00.000 PM to 9/12/14 12:00:00.000 AM. The interface includes tabs for Events, Statistics (47), and Visualization. Below the tabs are controls for 100 Per Page, Format, and Preview. The main content area displays a table with four columns: hostname, dns, clientName, and utsname. The table contains five rows of data, each representing a deployment client.

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 Save As ▾ Close

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 ▾ || ■ → ↓ 📄 ⚡ Fast Mode ▾

Events (146) Statistics Visualization

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

< Hide Fields		≡ All Fields	i	Time	Event
Selected Fields a host 1 a source 1 a 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 = [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 = [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 a component 1 a index 1 # linecount 1 a splunk_server 1					

Server: Reload

New Search Save As Close

index=_internal source=*splunkd.log component="DSManager" host="[REDACTED]" Last 7 days Q

✓ 27 events (9/2/14 9:00:00.000 AM to 9/9/14 9:47:42.000 AM) Job || ■ → ↓ ♻ ⚡ Fast Mode

Events (27) Statistics Visualization

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

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

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
		host = [REDACTED] ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd
>	9/4/14 4:53:02.971 PM	09-04-2014 16:53:02.971 -0700 INFO DSManager - Loaded count=26 configured SCs
		host = [REDACTED] ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd
>	9/4/14 4:53:02.337 PM	09-04-2014 16:53:02.337 -0700 INFO DSManager - Shutdown serverclassess
		host = [REDACTED] ; source = /opt/splunk/var/log/splunk/splunkd.log ; 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
		host = [REDACTED] ; source = /opt/splunk/var/log/splunk/splunkd.log ; sourcetype = splunkd
>	9/4/14 3:35:37.491 PM	09-04-2014 15:35:37.491 -0700 INFO DSManager - Shutdown serverclassess
		host = [REDACTED] ; source = /opt/splunk/var/log/splunk/splunkd.log ; 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 Save As Close

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

✓ 5,665 events (9/2/14 9:00:00.000 AM to 9/9/14 9:49:23.000 AM) Job || ■ ↶ ↓ ⊞ ⚡ Fast Mode

Events (5,665) Statistics Visualization

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

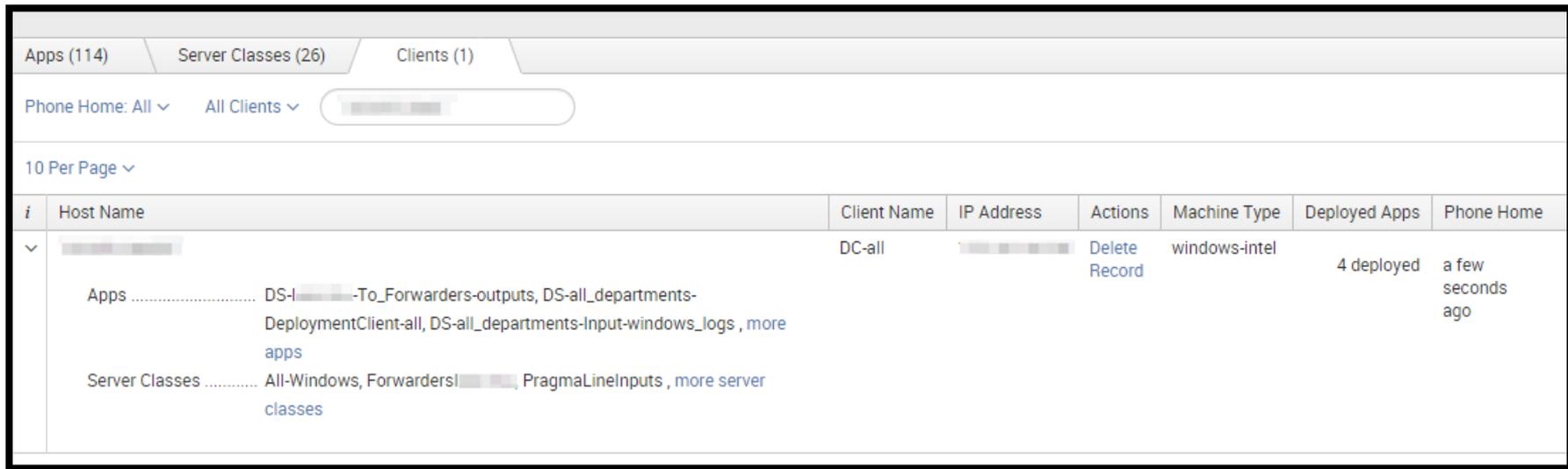
< Hide Fields ≡ All Fields	i	Time	Event
Selected Fields a host 1 a source 1 a sourcetype 1	>	9/8/14 6:55:02.147 PM	09-08-2014 18:55:02.147 -0700 INFO ClientSessionsManager - ip=██████████ name=DC-all Updating record for sc=ParseTA app=TA-livedata: action=Install result=0k host = ██████████ source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
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 New record for sc=ParseTA app=TA-livedata: action=Download result=0k 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=0k 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=1██████████ name=DC-all Updating record for sc=All-Linux app=Splunk_TA_nix: action=Install result=0k host = i██████████ source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

Oh yeah, Forwarder Management

The screenshot displays the Splunk Forwarder Management interface. At the top, there are three summary statistics: 47 Clients (PHONED HOME IN THE LAST 24 HOURS), 0 Clients (DEPLOYMENT ERRORS), and 0 Total downloads. Below these are navigation tabs for Apps (112), Server Classes (26), and Clients (47). There are also dropdown menus for 'Phone Home: All' and 'All Clients', and a search filter box. A '20 Per Page' dropdown is visible on the left, and pagination controls show '< Prev 1 2 3'. The main content is a table with columns: i, Host Name, Client Name, IP Address, Actions, Machine Type, Deployed Apps, and Phone Home. The table lists several clients, all with 'DC-all' as the Client Name and 'Delete Record' as the primary action. The Machine Types include 'linux-x86_64' and 'windows-intel'. The Deployed Apps column shows counts like '42 deployed' and '53 deployed'. The Phone Home column shows timestamps like 'a few seconds ago' and 'a minute ago'.

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

Oh yeah, Forwarder Management



The screenshot displays the Splunk Forwarder Management interface. At the top, there are tabs for 'Apps (114)', 'Server Classes (26)', and 'Clients (1)'. Below the tabs, there are dropdown menus for 'Phone Home: All' and 'All Clients', and a search input field. A '10 Per Page' dropdown is also visible. The main content is a table with the following columns: 'i', 'Host Name', 'Client Name', 'IP Address', 'Actions', 'Machine Type', 'Deployed Apps', and 'Phone Home'. The table contains one entry for a client named 'DC-all' with IP address '10.10.10.10'. The 'Actions' column for this client has a 'Delete Record' link. The 'Machine Type' is 'windows-intel'. The 'Deployed Apps' column shows '4 deployed'. The 'Phone Home' column shows 'a few seconds ago'. Below the 'Host Name' column, there are expandable sections for 'Apps' and 'Server Classes'. The 'Apps' section lists 'DS-10.10.10.10-To_Forwarders-outputs, DS-all_departments-DeploymentClient-all, DS-all_departments-Input-windows_logs , more apps'. The 'Server Classes' section lists 'All-Windows, Forwarders10.10.10.10, PragmaLineInputs , more server classes'.

i	Host Name	Client Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
▼	10.10.10.10	DC-all	10.10.10.10	Delete Record	windows-intel	4 deployed	a few seconds ago
	Apps DS-10.10.10.10-To_Forwarders-outputs, DS-all_departments-DeploymentClient-all, DS-all_departments-Input-windows_logs , more apps						
	Server Classes All-Windows, Forwarders10.10.10.10, 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>