

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on May 21, 2024 and its most recent report on Form 10-K filed on September 7, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or 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 or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk and Splunk> are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.

Administrators Anonymous Deep Dive:

Hands-on with the Splunk
Deployment Server

Interactive Workshop
PLA1310C



**Bring on
the future.**



Splunk Show Link:

[https://splk.it/
pla1310c](https://splk.it/pla1310c)

Who the heck are these guys?



Robert Palcisko

Splunk Administrator
Hurricane Labs



Tom Kopchak

Director of Technical Operations
Hurricane Labs

Enough about us!

Who are you?

Tools For Today

Tools For Today



Splunk Show

Lab Environment

Photo credit:
<https://www.pexels.com/photo/a-smart-boy-doing-a-science-experiment-8471836/>
<https://www.pexels.com/photo/girl-in-red-dress-sitting-on-bed-reading-book-3661488/>
<https://www.pexels.com/photo/blue-jeans-3036405/>
<https://www.pexels.com/photo/students-sitting-at-the-table-8423053/>

Tools For Today



Splunk Show

Lab Environment



Lab Materials

Workshop instructions

Photo credit:
<https://www.pexels.com/photo/a-smart-boy-doing-a-science-experiment-8471836/>
<https://www.pexels.com/photo/girl-in-red-dress-sitting-on-bed-reading-book-3661488/>
<https://www.pexels.com/photo/blue-jeans-3036405/>
<https://www.pexels.com/photo/students-sitting-at-the-table-8423053/>

Tools For Today



Splunk Show

Lab Environment



Lab Materials

Workshop instructions



Help from us

We brought our friends

Photo credit:
<https://www.pexels.com/photo/a-smart-boy-doing-a-science-experiment-8471836/>
<https://www.pexels.com/photo/girl-in-red-dress-sitting-on-bed-reading-book-3661488/>
<https://www.pexels.com/photo/blue-jeans-3036405/>
<https://www.pexels.com/photo/students-sitting-at-the-table-8423053/>

Tools For Today



Splunk Show

Lab Environment



Lab Materials

Workshop instructions



Help from us

We brought our friends



Audience Participation

We're all here to learn from each other

Photo credit:
<https://www.pexels.com/photo/a-smart-boy-doing-a-science-experiment-8471836/>
<https://www.pexels.com/photo/girl-in-red-dress-sitting-on-bed-reading-book-3661488/>
<https://www.pexels.com/photo/blue-jeans-3036405/>
<https://www.pexels.com/photo/students-sitting-at-the-table-8423053/>

Let's get started!

Part 1: Accessing Splunk Show

Lab 1: Accessing Splunk Show

- Log into Splunk Show and obtain your login credentials
- Access Splunk Web for your Show instance
 - Navigate to the Forwarder Management Interface
 - Confirm you see Universal Forwarders checking in
- SSH to your Show instance (via web browser)
 - SSH runs on HTTPS on port 7469 (use a web browser, NOT an SSH client)
 - Splunk Enterprise is installed in /opt/splunk
 - Universal Forwarder instances are installed in /opt/splunkforwarder<#>
 - UF #1: /opt/splunkforwarder1
 - UF #2: /opt/splunkforwarder2
 - UF #3: /opt/splunkforwarder3
 - Splunk is running as root user
- Make sure you know where you are when running commands!

Lab 1: Splunk Show Credentials

- SplunkWeb UI = admin / R3sili3nt!
- SSH = splunk / Sp1unkH00di3

SSH to your Splunk Show Instance!

SSH to your Show instance (via web browser)

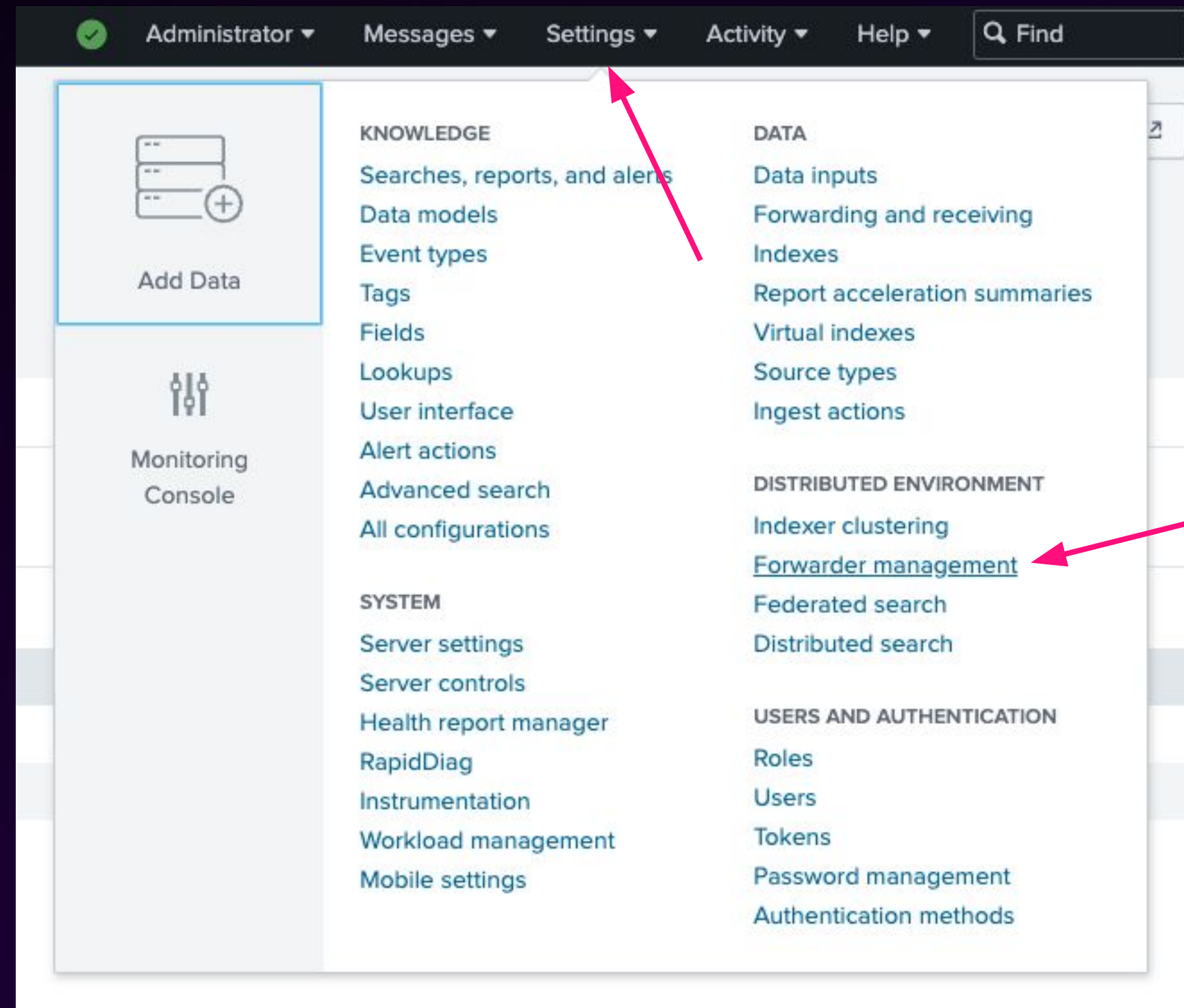
SSH runs on HTTPS on port 7469 (use a web browser, NOT an SSH client)

Switch to root user: `sudo -i`

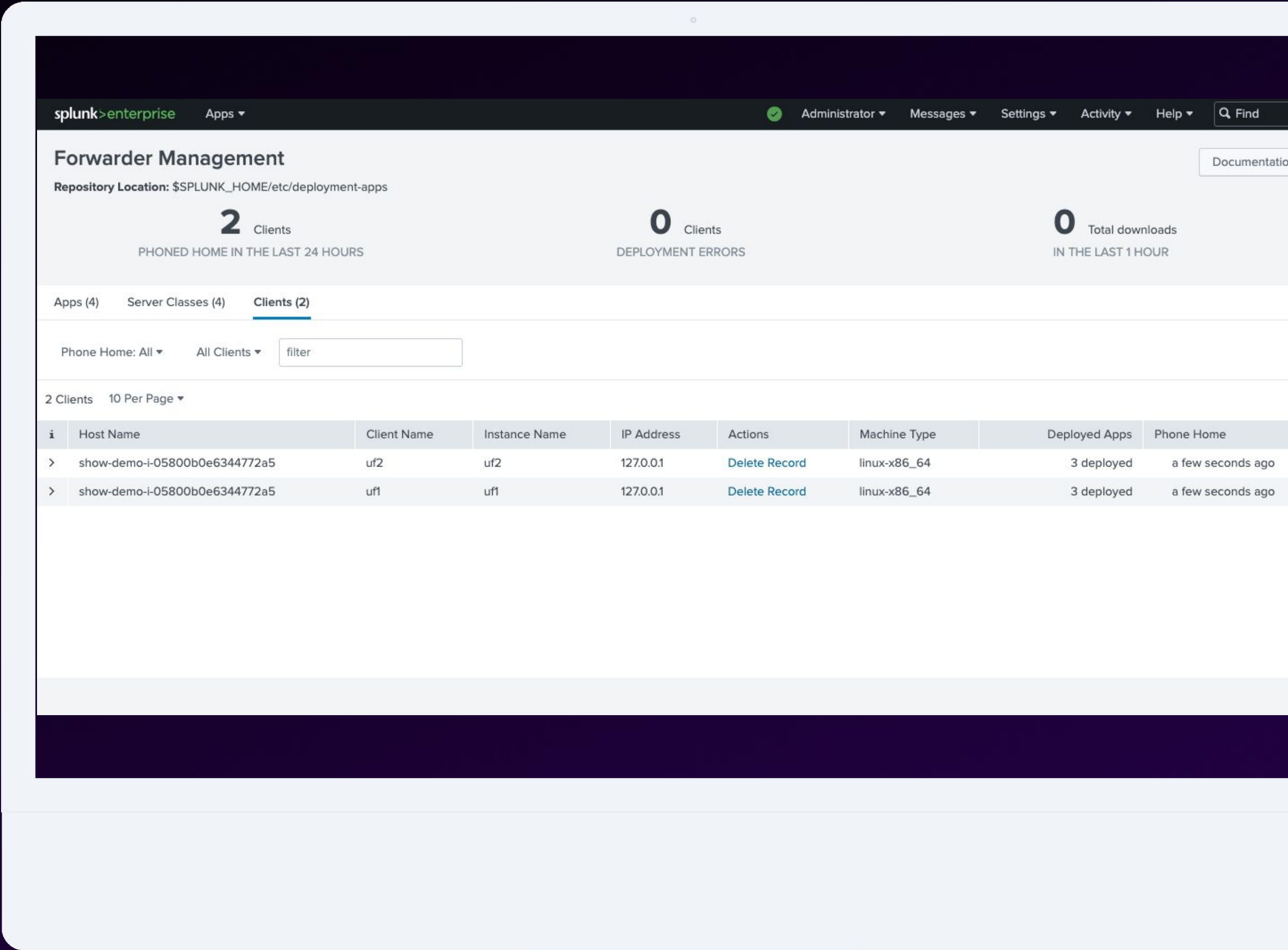
Switch to Splunk Enterprise: `cd /opt/splunk/`

Switch to Universal Forwarders: `cd /opt/splunkforwarder1/`

Explore the Forwarder Management Interface



Explore the Forwarder Management Interface



Confirm
your UFs
are logging

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New Search

Save AsCreate Table ViewClose

index=main host=uf*

Last 15 minutes

23 events (4/24/24 7:22:40.000 PM to 4/24/24 7:37:40.000 PM)No Event Sampling

JobPauseRefreshDownloadSmart Mode

Events (23)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect1 minute per column

ListFormat20 Per Page

Prev12Next

< Hide FieldsAll Fields

SELECTED FIELDS

host 2

source 2

sourcetype 1

INTERESTING FIELDS

index 1

linecount 1

punct 1

splunk_server 1

timestamp 1

+ Extract New Fields

i	Time	Event
>	4/24/24 7:37:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:36:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:35:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:34:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:33:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:32:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:31:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec
>	4/24/24 7:30:27.000 PM	This is uf1! host = uf1 source = /opt/splunkforwarder1/etc/apps/uf1_identifier/bin/identify.sh sourcetype = exec

© 2024 SPLUNK INC.

Are we there yet?

Accessing the show environment

- Logged into Splunk Web
- SSH into your instance
- Can view UFs in the forwarder management interface
- Familiar with the directory structure for UF installations



Part 2: The Deployment Server (and how it works)

Why a Deployment Server?



Why a Deployment Server?

1. Centralized App updates



Why a Deployment Server?

1. Centralized App updates
2. Consistency in apps deployed to hosts



Why a Deployment Server?

1. Centralized App updates
2. Consistency in apps deployed to hosts
3. Automated App deployment to specific hosts



Config Files

serverclass.conf

- Defines serverclasses and associated apps
- Maps apps to groups of Forwarders
- Can configure restarting splunkd on the Forwarder

```
#cat /opt/splunk/etc/system/local/serverclass.conf
[serverClass:all_UniversalForwarders]
blacklist.0 = splunkinfra*
whitelist.0 = *

[serverClass:all_UniversalForwarders:app:outputs]
restartSplunkWeb = 0
restartSplunkd = 1

[serverClass:uf1]
whitelist.0 = uf1*

[serverClass:uf1:app:uf1_identifier]
restartSplunkWeb = 0
restartSplunkd = 1

[serverClass:uf2]
whitelist.0 = uf2*
```


serverclass.conf (continued)

- Like all .conf files, multiple serverclass.conf files can exist and be combined together
 - Standard order of precedence applies
- `/opt/splunk/bin/splunk btool serverclass list --debug | awk '{ print $1 }' | sort -u`

```
# /opt/splunk/bin/splunk btool serverclass list --debug |  
awk '{ print $1 }' | sort -u  
/opt/splunk/etc/apps/search/local/serverclass.conf  
/opt/splunk/etc/system/default/serverclass.conf  
/opt/splunk/etc/system/local/serverclass.conf
```


deploymentclient.conf

- Exists on every Deployment Client
- Provides deployment server related instructions to the Forwarder
- Location may vary - use btool to locate
- phoneHomeIntervalInSecs - how frequently the Forwarders check in to the DS

```
[deployment-client]

[target-broker:deploymentServer]
targetUri = my.deployment.server:8089
phoneHomeIntervalInSecs = 300
```


Enabling Read-Only Forwarder Management

- Prevent changes from being made to serverclasses from the GUI
- Useful if managing configuration via external version control

```
#cat /opt/splunk/etc/system/local/serverclass.conf
[global]
# This exists to make the web interface read-only
whitelist.0 = -
```

Forwarder Management

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

 The forwarder management interface does not support some [settings](#) in your serverclass.conf file. The interface is now read-only. [Learn More](#)

3 Clients

PHONED HOME IN THE LAST 24 HOURS

0 Clients

DEPLOYMENT ERRORS

Apps (9) Server Classes (6) **Clients (2)**

Phone Home: All ▾ All Clients ▾ filter

2 Clients 10 Per Page ▾

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type
>	show-demo-i-05800b0e6344772a5	uf3	uf3	127.0.0.1	Delete Record	linux-x86_64
>	show-demo-i-05800b0e6344772a5	uf1	uf1	127.0.0.1	Delete Record	linux-x86_64

How does the Forwarder check-in process work?



How does the Forwarder check-in process work?

- Forwarder starts up, has deploymentclient.conf telling it what DS to use

How does the Forwarder check-in process work?

- Forwarder starts up, has deploymentclient.conf telling it what DS to use
- Forwarder connects to DS and subscribes to serverclass channel

How does the Forwarder check-in process work?

- Forwarder starts up, has deploymentclient.conf telling it what DS to use
- Forwarder connects to DS and subscribes to serverclass channel
- Forwarder downloads apps from DS

How does the Forwarder check-in process work?

- Forwarder starts up, has deploymentclient.conf telling it what DS to use
- Forwarder connects to DS and subscribes to serverclass channel
- Forwarder downloads apps from DS
- Forwarder restarts (if applicable)

**Let's look at
some logs**

Forwarder Initialization

```
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing the PubSub system.
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing core facilities of PubSub system.
04-23-2024 16:41:44.318 +0000 WARN  DC:DeploymentClient [732603 MainThread] - This DC shares a host with its DS.
targetUri=localhost:8089 hostname=show-demo-i-05800b0e6344772a5
04-23-2024 16:41:44.321 +0000 WARN  HTTPAuthManager [732603 MainThread] - pass4SymmKey length is too short. See
pass4SymmKey_minLength under the general stanza in server.conf.
04-23-2024 16:41:44.321 +0000 INFO  DCManager [732603 MainThread] - No server classes currently installed. Could not find
conf=/opt/splunkforwarder1/var/run/serverclass.xml
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732603 MainThread] - Starting phonehome thread.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Client initialized.
04-23-2024 16:41:44.321 +0000 INFO  ServerRoles [732603 MainThread] - Declared role=deployment_client.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Server not available on a dedicated
forwarder.
04-23-2024 16:41:44.321 +0000 INFO  HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Initial attempt to obtain
connection will try after=3.369 seconds.
04-23-2024 16:41:44.321 +0000 INFO  DC:PhonehomeThread [732618 PhonehomeThread] - Phonehome thread start, intervals:
handshakeRetry=12.0 phonehome=60.0.
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732618 PhonehomeThread] - channel=tenantService/handshake Will retry
sending handshake message to DS; err=not_connected
```


Forwarder Initialization

```
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing the PubSub system.
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing core facilities of PubSub system.
04-23-2024 16:41:44.318 +0000 WARN  DC:DeploymentClient [732603 MainThread] - This DC shares a host with its DS.
targetUri=localhost:8089 hostname=show-demo-i-05800b0e6344772a5
04-23-2024 16:41:44.321 +0000 WARN  HTTPAuthManager [732603 MainThread] - pass4SymmKey length is too short. See
pass4SymmKey_minLength under the general stanza in server.conf.
04-23-2024 16:41:44.321 +0000 INFO  DCManager [732603 MainThread] - No server classes currently installed. Could not find
conf=/opt/splunkforwarder1/var/run/serverclass.xml
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732603 MainThread] - Starting phonehome thread.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Client initialized.
04-23-2024 16:41:44.321 +0000 INFO  ServerRoles [732603 MainThread] - Declared role=deployment_client.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Server not available on a dedicated
forwarder.
04-23-2024 16:41:44.321 +0000 INFO  HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Initial attempt to obtain
connection will try after=3.369 seconds.
04-23-2024 16:41:44.321 +0000 INFO  DC:PhonehomeThread [732618 PhonehomeThread] - Phonehome thread start, intervals:
handshakeRetry=12.0 phonehome=60.0.
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732618 PhonehomeThread] - channel=tenantService/handshake Will retry
sending handshake message to DS; err=not_connected
```

Forwarder Initialization

04-23-2024 16:41:44.312 +0000 INFO DS_DC_Common [732603 MainThread] - Initializing the PubSub system.

04-23-2024 16:41:44.312 +0000 INFO DS_DC_Common [732603 MainThread] - Initializing core facilities of PubSub system.

04-23-2024 16:41:44.318 +0000 WARN DC:DeploymentClient [732603 MainThread] - This DC shares a host with its DS.
targetUri=localhost:8089 hostname=show-demo-i-05800b0e6344772a5

04-23-2024 16:41:44.321 +0000 WARN HTTPAuthManager [732603 MainThread] - pass4SymmKey length is too short. See
pass4SymmKey.minlength under the general stanza in server.conf

04-23-2024 16:41:44.321 +0000 INFO DCManager [732603 MainThread] - No server classes currently installed. Could not find
conf=/opt/splunkforwarder1/var/run/serverclass.xml

04-23-2024 16:41:44.321 +0000 INFO DC:DeploymentClient [732603 MainThread] - Starting phonehome thread.

04-23-2024 16:41:44.321 +0000 INFO DS_DC_Common [732603 MainThread] - Deployment Client initialized.

04-23-2024 16:41:44.321 +0000 INFO ServerRoles [732603 MainThread] - Declared role=deployment_client.

04-23-2024 16:41:44.321 +0000 INFO DS_DC_Common [732603 MainThread] - Deployment Server not available on a dedicated
forwarder.

04-23-2024 16:41:44.321 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Initial attempt to obtain
connection will try after=3.369 seconds.

04-23-2024 16:41:44.321 +0000 INFO DC:PhonehomeThread [732618 PhonehomeThread] - Phonehome thread start, intervals:
handshakeRetry=12.0 phonehome=60.0.

04-23-2024 16:41:44.321 +0000 INFO DC:DeploymentClient [732618 PhonehomeThread] - channel=tenantService/handshake Will retry
sending handshake message to DS; err=not_connected

Forwarder Initialization

```
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing the PubSub system.
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing core facilities of PubSub system.
04-23-2024 16:41:44.318 +0000 WARN  DC:DeploymentClient [732603 MainThread] - This DC shares a host with its DS.
targetUri=localhost:8089 hostname=show-demo-i-05800b0e6344772a5
04-23-2024 16:41:44.321 +0000 WARN  HTTPAuthManager [732603 MainThread] - pass4SymmKey length is too short. See
pass4SymmKey_minLength under the general stanza in server.conf.
04-23-2024 16:41:44.321 +0000 INFO  DCManager [732603 MainThread] - No server classes currently installed. Could not find
conf=/opt/splunkforwarder1/var/run/serverclass.xml
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732603 MainThread] - Starting phonehome thread.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Client initialized.
04-23-2024 16:41:44.321 +0000 INFO  ServerRoles [732603 MainThread] - Declared role=deployment_client.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment server not available on a dedicated
forwarder.
04-23-2024 16:41:44.321 +0000 INFO  HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Initial attempt to obtain
connection will try after=3.369 seconds.
04-23-2024 16:41:44.321 +0000 INFO  DC:PhonehomeThread [732618 PhonehomeThread] - Phonehome thread start, intervals:
handshakeRetry=12.0 phonehome=60.0.
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732618 PhonehomeThread] - channel=tenantService/handshake Will retry
sending handshake message to DS; err=not_connected
```

Forwarder Initialization

```
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing the PubSub system.
04-23-2024 16:41:44.312 +0000 INFO  DS_DC_Common [732603 MainThread] - Initializing core facilities of PubSub system.
04-23-2024 16:41:44.318 +0000 WARN  DC:DeploymentClient [732603 MainThread] - This DC shares a host with its DS.
targetUri=localhost:8089 hostname=show-demo-i-05800b0e6344772a5
04-23-2024 16:41:44.321 +0000 WARN  HTTPAuthManager [732603 MainThread] - pass4SymmKey length is too short. See
pass4SymmKey_minLength under the general stanza in server.conf.
04-23-2024 16:41:44.321 +0000 INFO  DCManager [732603 MainThread] - No server classes currently installed. Could not find
conf=/opt/splunkforwarder1/var/run/serverclass.xml
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732603 MainThread] - Starting phonehome thread.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Client initialized.
04-23-2024 16:41:44.321 +0000 INFO  ServerRoles [732603 MainThread] - Declared role=deployment_client.
04-23-2024 16:41:44.321 +0000 INFO  DS_DC_Common [732603 MainThread] - Deployment Server not available on a dedicated
forwarder.
04-23-2024 16:41:44.321 +0000 INFO  HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Initial attempt to obtain
connection will try after=3.369 seconds.
04-23-2024 16:41:44.321 +0000 INFO  DC:PhonehomeThread [732618 PhonehomeThread] - Phonehome thread start, intervals:
handshakeRetry=12.0 phonehome=60.0.
04-23-2024 16:41:44.321 +0000 INFO  DC:DeploymentClient [732618 PhonehomeThread] - channel=tenantService/handshake Will retry
sending handshake message to DS; err=not_connected
```

Forwarder Phonehome

splunkd.log (on UF)

```
04-23-2024 16:41:47.769 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - SSL connection with id: connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

```
04-23-2024 16:41:47.771 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Running phone uri=/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:41:47.769 +0000] "POST /services/broker/connect/uf1/show-demo-i-05800b0e6344772a5/a414fc70250e/linux-x86_64/9089/9.1.4/D9A525F7-3C11-426E-8B94-89003A9FAF9F/universal_forwarder/uf1 HTTP/1.1" 200 132 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/channel/subscribe/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1/tenantService%2Fhandshake%2Freply%2Fshow-demo-i-05800b0e6344772a5%2Fuf1 HTTP/1.1" 200 58 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

Forwarder Phonehome

splunkd.log (on UF)

```
04-23-2024 16:41:47.769 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - SSL connection with id: connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

```
04-23-2024 16:41:47.771 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Running phone uri=/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:41:47.769 +0000] "POST /services/broker/connect/uf1/show-demo-i-05800b0e6344772a5/a414fc70250e/linux-x86_64/9089/9.1.4/D9A525F7-3C11-426E-8B94-89003A9FAF9F/universal_forwarder/uf1 HTTP/1.1" 200 132 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/channel/subscribe/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1/tenantService%2Fhandshake%2Freply%2Fshow-demo-i-05800b0e6344772a5%2Fuf1 HTTP/1.1" 200 58 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```


Forwarder Phonehome

splunkd.log (on UF)

```
04-23-2024 16:41:47.769 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - SSL connection with id: connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

```
04-23-2024 16:41:47.771 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Running phone uri=/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:41:47.769 +0000] "POST /services/broker/connect/uf1/show-demo-i-05800b0e6344772a5/a414fc70250e/linux-x86_64/9089/9.1.4/D9A525F7-3C11-426E-8B94-89003A9FAF9F/universal_forwarder/uf1 HTTP/1.1" 200 132 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/channel/subscribe/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1/tenantService%2Fhandshake%2Freply%2Fshow-demo-i-05800b0e6344772a5%2Fuf1 HTTP/1.1" 200 58 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

Forwarder Phonehome

splunkd.log (on UF)

```
04-23-2024 16:41:47.769 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - SSL connection with id: connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

```
04-23-2024 16:41:47.771 +0000 INFO HttpPubSubConnection [732617 HttpClientPollingThread_uf1] - Running phone uri=/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:41:47.769 +0000] "POST /services/broker/connect/uf1/show-demo-i-05800b0e6344772a5/a414fc70250e/linux-x86_64/9089/9.1.4/D9A525F7-3C11-426E-8B94-89003A9FAF9F/universal_forwarder/uf1 HTTP/1.1" 200 132 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/channel/subscribe/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1/tenantService%2Fhandshake%2Freply%2Fshow-demo-i-05800b0e6344772a5%2Fuf1 HTTP/1.1" 200 58 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

```
127.0.0.1 - - [23/Apr/2024:16:41:47.771 +0000] "POST /services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

Forwarder Phonehome

splunkd.log (on DS)


```
04-23-2024 16:41:47.771 +0000 INFO  PubSubSvr [731668 TcpChannelThread] - Subscribed:
channel=tenantService/handshake/reply/show-demo-i-05800b0e6344772a5/uf1
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00

04-23-2024 16:41:56.322 +0000 INFO  PubSubSvr [731668 TcpChannelThread] - Subscribed:
channel=deploymentServer/phoneHome/default/reply/show-demo-i-05800b0e6344772a5/uf1
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00
```

Forwarder Phonehome

splunkd.log (on DS)


```
04-23-2024 16:41:47.771 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=tenantService/handshake/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00  
  
04-23-2024 16:41:56.322 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=deploymentServer/phoneHome/default/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00
```



Forwarder Phonehome

splunkd.log (on DS)

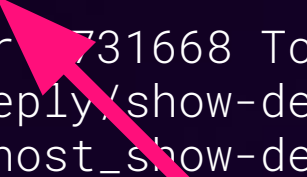
```
04-23-2024 16:41:47.771 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=tenantService/handshake/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00  
  
04-23-2024 16:41:56.322 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=deploymentServer/phoneHome/default/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00
```



Forwarder Phonehome

splunkd.log (on DS)


```
04-23-2024 16:41:47.771 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=tenantService/handshake/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00  
  
04-23-2024 16:41:56.322 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=deploymentServer/phoneHome/default/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00
```



Forwarder Phonehome

splunkd.log (on DS)


```
04-23-2024 16:41:47.771 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=tenantService/handshake/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00  
  
04-23-2024 16:41:56.322 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=deploymentServer/phoneHome/default/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00
```



Forwarder Phonehome

splunkd.log (on DS)

```
04-23-2024 16:41:47.771 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=tenantService/handshake/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00  
  
04-23-2024 16:41:56.322 +0000 INFO PubSubSvr [731668 TcpChannelThread] - Subscribed:  
channel=deploymentServer/phoneHome/default/reply/show-demo-i-05800b0e6344772a5/uf1  
connectionId=connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 listener=0x7f41ac830c00
```



Forwarder App Download

splunkd.log (on UF)

```
04-23-2024 16:42:56.325 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Checksum mismatch 0 <>
14291942956695506570 for app=outputs. Will reload
from='localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs'

04-23-2024 16:42:56.326 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Downloaded
url=localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs to
file='/opt/splunkforwarder1/var/run/all_UniversalForwarders/outputs-1713890268.bundle' sizeKB=10
```

splunkd.log (on DS)

```
04-23-2024 16:42:56.326 +0000 INFO PackageDownloadRestHandler [731668 TcpChannelThread] - peer=127.0.0.1:34720 Download
started and completed for path=/opt/splunk/var/run/tmp/all_UniversalForwarders/outputs-1713890268.bundle.gz
serverclass=all_UniversalForwarders app=outputs
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:42:56.324 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.325 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 988 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.326 +0000] "POST /services/streams/deployment?name=default:all_UniversalForwarders:outputs
HTTP/1.1" 200 528 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

Forwarder App Download

splunkd.log (on UF)

```
04-23-2024 16:42:56.325 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Checksum mismatch 0 <>
14291942956695506570 for app=outputs. Will reload
from='localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs'
```

```
04-23-2024 16:42:56.326 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Downloaded
url=localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs to
file='/opt/splunkforwarder1/var/run/all_UniversalForwarders/outputs-1713890268.bundle' sizeKB=10
```

splunkd.log (on DS)

```
04-23-2024 16:42:56.326 +0000 INFO PackageDownloadRestHandler [731668 TcpChannelThread] - peer=127.0.0.1:34720 Download
started and completed for path=/opt/splunk/var/run/tmp/all_UniversalForwarders/outputs-1713890268.bundle.gz
serverclass=all_UniversalForwarders app=outputs
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:42:56.324 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.325 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 988 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.326 +0000] "POST /services/streams/deployment?name=default:all_UniversalForwarders:outputs
HTTP/1.1" 200 528 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```


Forwarder App Download

splunkd.log (on UF)

```
04-23-2024 16:42:56.325 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Checksum mismatch 0 <>
14291942956695506570 for app=outputs. Will reload
from='localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs'
```

```
04-23-2024 16:42:56.326 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Downloaded
url=localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs to
file='/opt/splunkforwarder1/var/run/all_UniversalForwarders/outputs-1713890268.bundle' sizeKB=10
```

splunkd.log (on DS)

```
04-23-2024 16:42:56.326 +0000 INFO PackageDownloadRestHandler [731668 TcpChannelThread] - peer=127.0.0.1:34720 Download
started and completed for path=/opt/splunk/var/run/tmp/all_UniversalForwarders/outputs-1713890268.bundle.gz
serverclass=all_UniversalForwarders app=outputs
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:42:56.324 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.325 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 988 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.326 +0000] "POST /services/streams/deployment?name=default:all_UniversalForwarders:outputs
HTTP/1.1" 200 528 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

Forwarder App Download

splunkd.log (on UF)

```
04-23-2024 16:42:56.325 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Checksum mismatch 0 <>
14291942956695506570 for app=outputs. Will reload
from='localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs'

04-23-2024 16:42:56.326 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Downloaded
url=localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs to
file='/opt/splunkforwarder1/var/run/all_UniversalForwarders/outputs-1713890268.bundle' sizeKB=10
```

splunkd.log (on DS)

```
04-23-2024 16:42:56.326 +0000 INFO PackageDownloadRestHandler [731668 TcpChannelThread] - peer=127.0.0.1:34720 Download
started and completed for path=/opt/splunk/var/run/tmp/all_UniversalForwarders/outputs-1713890268.bundle.gz
serverclass=all_UniversalForwarders app=outputs
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:42:56.324 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.325 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 988 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.326 +0000] "POST /services/streams/deployment?name=default:all_UniversalForwarders:outputs
HTTP/1.1" 200 528 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```

Forwarder App Download

splunkd.log (on UF)

```
04-23-2024 16:42:56.325 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Checksum mismatch 0 <>
14291942956695506570 for app=outputs. Will reload
from='localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs'
```

```
04-23-2024 16:42:56.326 +0000 INFO DeployedApplication [732617 HttpClientPollingThread_uf1] - Downloaded
url=localhost:8089/services/streams/deployment?name=default:all_UniversalForwarders:outputs to
file='/opt/splunkforwarder1/var/run/all_UniversalForwarders/outputs-1713890268.bundle' sizeKB=10
```

splunkd.log (on DS)

```
04-23-2024 16:42:56.326 +0000 INFO PackageDownloadRestHandler [731668 TcpChannelThread] - peer=127.0.0.1:34720 Download
started and completed for path=/opt/splunk/var/run/tmp/all_UniversalForwarders/outputs-1713890268.bundle.gz
serverclass=all_UniversalForwarders app=outputs
```

splunkd_access.log (on DS)

```
127.0.0.1 - - [23/Apr/2024:16:42:56.324 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 24 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.325 +0000] "POST
/services/broker/phonehome/connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1 HTTP/1.1" 200 988 "-"
"Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms

127.0.0.1 - - [23/Apr/2024:16:42:56.326 +0000] "POST /services/streams/deployment?name=default:all_UniversalForwarders:outputs
HTTP/1.1" 200 528 "-" "Splunk/9.1.4 (Linux 6.5.0-1014-aws; arch=x86_64)" - - - 0ms
```


Forwarder App Installation & Restart

splunkd.log (on UF)

```
04-23-2024 16:42:56.338 +0000 INFO ApplicationManager [732617 HttpClientPollingThread_uf1] - Detected app creation: outputs
04-23-2024 16:42:56.647 +0000 INFO loader [732609 HTTPDispatch] - Shutdown HTTPDispatchThread
04-23-2024 16:42:56.647 +0000 INFO Shutdown [732622 Shutdown] - Shutting down splunkd
04-23-2024 16:42:56.346 +0000 WARN DC:DeploymentClient [732617 HttpClientPollingThread_uf1] - Restarting Splunkd...
```

Forwarder App Installation & Restart

splunkd.log (on UF)

```
04-23-2024 16:42:56.338 +0000 INFO ApplicationManager [732617 HttpClientPollingThread_uf1] - Detected app creation: outputs
04-23-2024 16:42:56.647 +0000 INFO loader [732609 HTTPDispatch] - Shutdown HTTPDispatchThread
04-23-2024 16:42:56.647 +0000 INFO Shutdown [732622 Shutdown] - Shutting down splunkd
04-23-2024 16:42:56.346 +0000 WARN DC:DeploymentClient [732617 HttpClientPollingThread_uf1] - Restarting Splunkd...
```

Forwarder App Installation & Restart

splunkd.log (on UF)

```
04-23-2024 16:42:56.338 +0000 INFO ApplicationManager [732617 HttpClientPollingThread_uf1] - Detected app creation: outputs
04-23-2024 16:42:56.647 +0000 INFO loader [732609 HTTPDispatch] - Shutdown HTTPDispatchThread
04-23-2024 16:42:56.647 +0000 INFO Shutdown [732622 Shutdown] - Shutting down splunkd
04-23-2024 16:42:56.346 +0000 WARN DC:DeploymentClient [732617 HttpClientPollingThread_uf1] - Restarting Splunkd...
```


Lab 2: Troubleshooting a Broken UF

You have a UF that is sending data to Splunk but not checking into the Deployment Server

- UF1 & UF2 = checking in successfully to the Deployment Server
- UF3 = Not checking in successfully

Your task: troubleshoot why this is broken!

Hint: `/opt/splunkforwarder3/bin/splunk btool deploymentclient list --debug`

Lab 2: Troubleshooting a Broken UF


```
root@show-demo-i-05800b0e6344772a5:/opt/splunkforwarder3/etc/apps/all_deploymentclient/local# cat deploymentclient.conf
[deployment-client]
phoneHomeIntervalInSecs = 30

[target-broker:deploymentServer]
targetUri = localhost:8089
```

Two red arrows are present. One arrow points from the bottom left towards the 'targetUri = localhost:8089' line. The other arrow points from the bottom right towards the 'phoneHomeIntervalInSecs = 30' line.

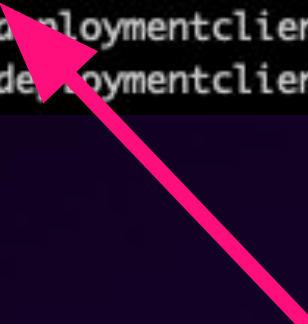
Lab 2: Troubleshooting a Broken UF

```
root@show-demo-i-05800b0e6344772a5:/opt/splunkforwarder3/etc/apps/all_deploymentclient/local# /opt/splunkforwarder3/bin/splunk btool deploymentclient list
[deployment-client]
clientName = uf3
phoneHomeIntervalInSecs = 30
targetUri = old-deployment-server.hurricanelabs.nope:8089
[target-broker:deploymentServer]
targetUri = localhost:8089
```



Lab 2: Troubleshooting a Broken UF

```
root@show-demo-i-05800b0e6344772a5:/opt/splunkforwarder3/etc/apps/all_deploymentclient/local# /opt/splunkforwarder3/bin/splunk btool deploymentclient list --debug
/opt/splunkforwarder3/etc/apps/all_deploymentclient/local/deploymentclient.conf [deployment-client]
/opt/splunkforwarder3/etc/system/local/deploymentclient.conf           clientName = uf3
/opt/splunkforwarder3/etc/apps/all_deploymentclient/local/deploymentclient.conf phoneHomeIntervalInSecs = 30
/opt/splunkforwarder3/etc/system/local/deploymentclient.conf           targetUri = old-deployment-server.hurricanelabs.nope:8089
/opt/splunkforwarder3/etc/apps/all_deploymentclient/local/deploymentclient.conf [target-broker:deploymentServer]
/opt/splunkforwarder3/etc/apps/all_deploymentclient/local/deploymentclient.conf targetUri = localhost:8089
```



The Deployment Server Recap

- Remember, btool is your friend
- Config precedence can make updating deploymentclient.conf configurations challenging
- When troubleshooting a broken UF, start with the basics first
 - Correct Splunk configuration
 - Network connectivity to DS



Part 3:

App Bundles &

serverclass.xml

App Bundles

DS - Explore a Bundle

/opt/splunk/var/run/tmp/serverclassname

Bundle = compressed tarball of the deployment app

- appname-epochtimeofserverclass
- uf1_identifier-1713892441.bundle (tar archive)
- uf1_identifier-1713892441.bundle.gz (gunzip compressed)



How are bundles created?

Consistency is key

How are bundles created?

Consistency is key

- Bundles are structured in a defined way.

How are bundles created?

Consistency is key

- Bundles are structured in a defined way.
- Bundles are re-created when the serverclass is reloaded, only after modifications to the serverclass' contents are made.

How are bundles created?

Consistency is key

- Bundles are structured in a defined way.
- Bundles are re-created when the serverclass is reloaded, only after modifications to the serverclass' contents are made.
 - Files are sorted consistently within the tarball
 - Forces file ownership using a userid and groupid of **0**, and the username and groupname of **splunk**

How are bundles created?

Consistency is key

- Bundles are structured in a defined way.
- Bundles are re-created when the serverclass is reloaded, only after modifications to the serverclass' contents are made.
 - Files are sorted consistently within the tarball
 - Forces file ownership using a userid and groupid of **0**, and the username and groupname of **splunk**
- Permissions and ownership:
 - User information in the tarball is ignored
 - Owner is the user that the SplunkForwarder is configured to use

How are bundles created?

Consistency is key

- Bundles are structured in a defined way.
- Bundles are re-created when the serverclass is reloaded, only after modifications to the serverclass' contents are made.
 - Files are sorted consistently within the tarball
 - Forces file ownership using a userid and groupid of **0**, and the username and groupname of **splunk**
- Permissions and ownership:
 - User information in the tarball is ignored
 - Owner is the user that the SplunkForwarder is configured to use
 - Permissions are kept:
 - Scripted inputs set to executable will remain that way

How are bundles created?

File Permissions & ownership

```
root@show-demo-i-05800b0e6344772a5:/opt/splunk/var/run/tmp/uf1#  
tar --numeric-owner -tvf uf1_identifier-1713892441.bundle
```

```
-rwxr-xr-x 0/0
```

```
20 2024-04-08 18:17 bin/identify.sh
```

```
-rw-r--r-- 0/0
```

```
218 2024-04-08 18:34 local/app.conf
```

```
-rw-r--r-- 0/0
```

```
115 2024-04-08 18:42 local/inputs.conf
```

```
-rw-r--r-- 0/0
```

```
61 2023-02-06 20:43 metadata/local.meta
```


serverclass.xml

serverclass.xml

**Exists on every Deployment Client
after initialization:**

\$SPLUNK_HOME/var/run/
serverclass.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false"
stateOnClient="enabled" issueReload="false"
repositoryLocation="$SPLUNK_HOME/etc/apps"
endpoint="$deploymentServerUri$/services/streams/deployment?name
=$tenantName$:serverClassName$:appName$">
  <serverClass name="all_UniversalForwarders">
    <app name="outputs" checksum="14291942956695506570"
restartSplunkd="true" restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalForward
ers/outputs-1713890268.bundle" installed="true"/>
  </serverClass>
</deployResponse>
```

serverclass.xml


Identifies the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false"
stateOnClient="enabled" issueReload="false"
repositoryLocation="$SPLUNK_HOME/etc/apps"
endpoint="$deploymentServerUri$/services/streams/deployment?name
=$tenantName$:serverClassName$:appName$" >
  <serverClass name="all_UniversalForwarders">
    <app name="outputs" checksum="14291942956695506570"
restartSplunkd="true" restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalForward
ers/outputs-1713890268.bundle" installed="true" />
  </serverClass>
</deployResponse>
```

serverclass.xml

Identifies the following:

- Each serverclass where the Forwarder is configured




```
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false"
stateOnClient="enabled" issueReload="false"
repositoryLocation="$SPLUNK_HOME/etc/apps"
endpoint="$deploymentServerUri$/services/streams/deployment?name
=$tenantName$: $serverClassName$: $appName$" >
  <serverClass name="all_UniversalForwarders">
    <app name="outputs" checksum="14291942956695506570"
restartSplunkd="true" restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalForward
ers/outputs-1713890268.bundle" installed="true"/>
  </serverClass>
</deployResponse>
```


serverclass.xml

Identifies the following:

- Each serverclass where the Forwarder is configured
- Apps associated with each serverclass

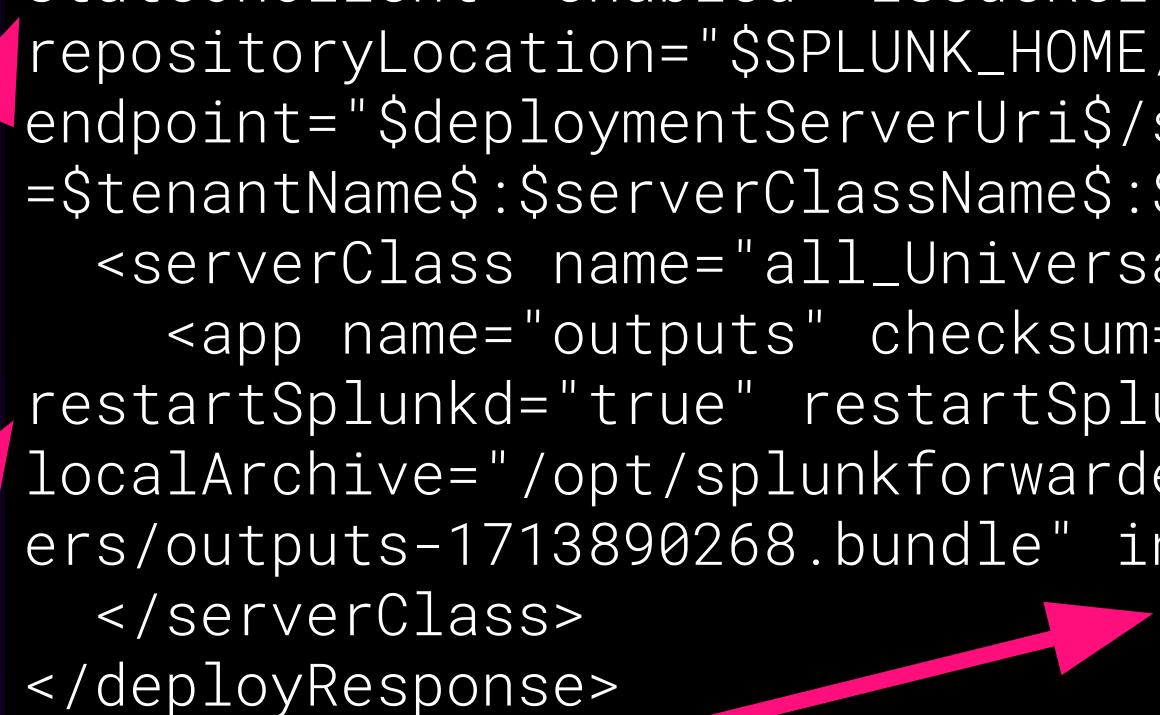


```
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false"
stateOnClient="enabled" issueReload="false"
repositoryLocation="$SPLUNK_HOME/etc/apps"
endpoint="$deploymentServerUri$/services/streams/deployment?name
=$tenantName$:serverClassName$:appName$">
  <serverClass name="all_UniversalForwarders">
    <app name="outputs" checksum="14291942956695506570"
restartSplunkd="true" restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalForward
ers/outputs-1713890268.bundle" installed="true"/>
  </serverClass>
</deployResponse>
```

serverclass.xml

Identifies the following:

- Each serverclass where the Forwarder is configured
- Apps associated with each serverclass
- App installation status, restart configuration, and state



The diagram shows three pink arrows originating from the list items on the left and pointing to specific parts of the XML code on the right. The first arrow points from 'Each serverclass where the Forwarder is configured' to the `<serverClass name='all_UniversalForwarders'>` tag. The second arrow points from 'Apps associated with each serverclass' to the `<app name='outputs'>` tag. The third arrow points from 'App installation status, restart configuration, and state' to the `restartSplunkd='true'` attribute.

```
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false"
stateOnClient="enabled" issueReload="false"
repositoryLocation="$SPLUNK_HOME/etc/apps"
endpoint="$deploymentServerUri$/services/streams/deployment?name
=$tenantName$: $serverClassName$: $appName$" >
  <serverClass name="all_UniversalForwarders">
    <app name="outputs" checksum="14291942956695506570"
restartSplunkd="true" restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalForward
ers/outputs-1713890268.bundle" installed="true"/>
  </serverClass>
</deployResponse>
```

serverclass.xml

Identifies the following:

- Each serverclass where the Forwarder is configured
- Apps associated with each serverclass
- App installation status, restart configuration, and state
- Associated bundle file

```
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false"
stateOnClient="enabled" issueReload="false"
repositoryLocation="$SPLUNK_HOME/etc/apps"
endpoint="$deploymentServerUri$/services/streams/deployment?name
=$tenantName$:serverClassName$:appName$" >
  <serverClass name="all_UniversalForwarders">
    <app name="outputs" checksum="14291942956695506570"
restartSplunkd="true" restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalForward
ers/outputs-1713890268.bundle" installed="true"/>
  </serverClass>
</deployResponse>
```

Lab 3: Serverclass XML Investigation

- Parse serverclass XML to understand the previously deployed configuration
- Investigate UF4

Lab 3: Serverclass XML Investigation

```
root@show-demo-i-05800b0e6344772a5:~# cat /opt/splunkforwarder4/var/run/serverclass.xml
<?xml version="1.0" encoding="UTF-8"?>
<deployResponse restartSplunkd="false" restartSplunkWeb="false" stateOnClient="enabled" issueReload="false" repositoryLocation="$SPLUNK_HOME/etc/apps" endpoint="$deploymentServerUri$/services/streams/deployment?name=$tenantName$:serverClassName:$appName$">
  <serverClass name="100_IngestAction_AutoGenerated">
    <app name="splunk_ingest_actions" checksum="17136782134994119078" restartSplunkd="false" restartSplunkWeb="false" stateOnClient="enabled" issueReload="true" localArchive="/opt/splunkforwarder4/var/run/100_IngestAction_AutoGenerated/splunk_ingest_actions-1714074586.bundle" installed="true"/>
  </serverClass>
  <serverClass name="all_UniversalForwarders">
    <app name="all_deploymentclient" checksum="8236339152916141319" restartSplunkd="true" restartSplunkWeb="false" localArchive="/opt/splunkforwarder4/var/run/all_UniversalForwarders/all_deploymentclient-1714074586.bundle" installed="true"/>
    <app name="outputs" checksum="15120128795082040217" restartSplunkd="true" restartSplunkWeb="false" localArchive="/opt/splunkforwarder4/var/run/all_UniversalForwarders/outputs-1714074586.bundle" installed="true"/>
  </serverClass>
  <serverClass name="uf4">
    <app name="uf4_identifier" checksum="2805611991501769146" restartSplunkd="true" restartSplunkWeb="false" localArchive="/opt/splunkforwarder4/var/run/uf4/uf4_identifier-1714074587.bundle" installed="true"/>
  </serverClass>
</deployResponse>
```

Lab 3: Serverclass XML Investigation

```
root@show-demo-i-05800b0e6344772a5:/opt/splunkforwarder4/var/run#  
grep -i -e "serverclass name" -e "app name" serverclass.xml | awk ' { print $1, $2 }'  
<serverClass name="100_IngestAction_AutoGenerated">  
<app name="splunk_ingest_actions"  
<serverClass name="all_UniversalForwarders">  
<app name="all_deploymentclient"  
<app name="outputs"  
<serverClass name="uf4">  
<app name="uf4_identifier"
```


App Bundles Recap

- Use serverclass.xml to determine what apps are managed by the DS
- When moving a Forwarder to a new DS, this can be used to identify apps that are on the Forwarder but missing on the DS



New Splunk 9.2 Features

9.2 Migration Tasks

- Deploy new internal indexes
 - _dsclient
 - _dsphonehome
 - _dsappevent
- Ensure your deployment server can search the search peers or selectively indexes data
- Reference:
<https://docs.splunk.com/Documentation/Splunk/9.2.1/Updating/Upgradepre-9.2deploymentservers>



_dsclient index: shows client info

```
{ [-]
  component: DSclient
  data: { [+]
  }
  datetime: 04-23-2024 16:41:47.769 +0000
  log_level: INFO
}
```

Show as raw text

Event Actions ▾

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host ▾	show-demo-i-05800b0e6344772a5	▾
	<input checked="" type="checkbox"/> source ▾	/opt/splunk/var/log/client_events/clients_CCE1C20E-9370-49CA-8259-F28B74BA14BC.log	▾
	<input checked="" type="checkbox"/> sourcetype ▾	dsclient	▾
Event	<input type="checkbox"/> component ▾	DSclient	▾
	<input type="checkbox"/> data.build ▾	a414fc70250e	▾
	<input type="checkbox"/> data.clientId ▾	D9A525F7-3C11-426E-8B94-89003A9FAF9F	▾
	<input type="checkbox"/> data.connectionId ▾	connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_uf1	▾
	<input type="checkbox"/> data.dns ▾	localhost	▾
	<input type="checkbox"/> data.guid ▾	D9A525F7-3C11-426E-8B94-89003A9FAF9F	▾
	<input type="checkbox"/> data.hostname ▾	show-demo-i-05800b0e6344772a5	▾
	<input type="checkbox"/> data.instanceId ▾	D9A525F7-3C11-426E-8B94-89003A9FAF9F	▾
	<input type="checkbox"/> data.instanceName ▾	uf1	▾
	<input type="checkbox"/> data.ip ▾	127.0.0.1	▾
	<input type="checkbox"/> data.mgmt ▾	9089	▾
	<input type="checkbox"/> data.name ▾	uf1	▾
	<input type="checkbox"/> data.package ▾	universal_forwarder	▾
	<input type="checkbox"/> data.packageType ▾		▾
	<input type="checkbox"/> data.splunkVersion ▾	9.1.4	▾
	<input type="checkbox"/> data.upgradeStatus ▾		▾
	<input type="checkbox"/> data.upgradeTime ▾		▾
	<input type="checkbox"/> data.utsname ▾	linux-x86_64	▾
	<input type="checkbox"/> datetime ▾	04-23-2024 16:41:47.769 +0000	▾
	<input type="checkbox"/> log_level ▾	INFO	▾
Time ⛶	_time ▾	2024-04-23T16:41:47.769+00:00	
Default	<input type="checkbox"/> index ▾	_dsclient	▾
	<input type="checkbox"/> linecount ▾	1	▾
	<input type="checkbox"/> punct ▾	{"";--...+_"";"";"";"";"";{"";_"";"";"";""}	▾
	<input type="checkbox"/> splunk_server ▾	splunk-enterprise	▾

_dsphonehome index: shows check in info

▼ 4/24/24
8:39:59.939 PM

```
{ [-]
  component: DSphonehome
  data: { [+]
    }
  datetime: 04-24-2024 20:39:59.939 +0000
  log_level: INFO
}
```

Show as raw text

Event Actions ▼

Type	<input checked="" type="checkbox"/> Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host ▼	show-demo-i-05800b0e6344772a5	▼
	<input checked="" type="checkbox"/> source ▼	/opt/splunk/var/log/client_events/phonehomes_CCE1C20E-9370-49CA-8259-F28B74BA14BC.log	▼
	<input checked="" type="checkbox"/> sourcetype ▼	dsphonehome	▼
Event	<input type="checkbox"/> component ▼	DSphonehome	▼
	<input type="checkbox"/> data.clientId ▼	D9A525F7-3C11-426E-8B94-89003A9FAF9F	▼
	<input type="checkbox"/> data.connectionId ▼	connection_127.0.0.1_9089_localhost_show-demo-i-05800b0e6344772a5_ufl	▼
	<input type="checkbox"/> data.lastPhoneHomeTime ▼	1713991199	▼
	<input type="checkbox"/> datetime ▼	04-24-2024 20:39:59.939 +0000	▼
	<input type="checkbox"/> log_level ▼	INFO	▼
Time ╖	_time ▼	2024-04-24T20:39:59.939+00:00	
Default	<input type="checkbox"/> index ▼	_dsphonehome	▼
	<input type="checkbox"/> linecount ▼	1	▼
	<input type="checkbox"/> punct ▼	{""," _...+"" "" "" "" "" "" {" "" " "" "" "" --	▼
	<input type="checkbox"/> splunk_server ▼	splunk-enterprise	▼

© 2024 SPLUNK INC.

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	host ▾	show-demo-i-05800b0e6344772a5	▾
	<input checked="" type="checkbox"/>	source ▾	/opt/splunk/var/log/client_events/appevents_CCE1C20E-9370-49CA-8259-F28B74BA14BC.log	▾
	<input checked="" type="checkbox"/>	sourcetype ▾	dsappevent	▾
Event	<input type="checkbox"/>	component ▾	DSappevent	▾
	<input type="checkbox"/>	data.action ▾	Install	▾
	<input type="checkbox"/>	data.appName ▾	splunk_ingest_actions	▾
	<input type="checkbox"/>	data.checksum ▾	17136782134994119078	▾
	<input type="checkbox"/>	data.clientId ▾	D9A525F7-3C11-426E-8B94-89003A9FAF9F	▾
	<input type="checkbox"/>	data.failedReason ▾	"	▾
	<input type="checkbox"/>	data.key ▾	D9A525F7-3C11-426E-8B94-89003A9FAF9F_100_IngestAction_AutoGenerated_splunk_ingest_actions	▾
	<input type="checkbox"/>	data.result ▾	Ok	▾
	<input type="checkbox"/>	data.serverClassName ▾	100_IngestAction_AutoGenerated	▾
	<input type="checkbox"/>	data.timestamp ▾	1713927716	▾
	<input type="checkbox"/>	datetime ▾	04-24-2024 03:01:56.934 +0000	▾
	<input type="checkbox"/>	log_level ▾	INFO	▾
Time ⛶	<input type="checkbox"/>	_time ▾	2024-04-24T03:01:56.934+00:00	
Default	<input type="checkbox"/>	index ▾	_dsappevent	▾
	<input type="checkbox"/>	linecount ▾	1	▾
	<input type="checkbox"/>	punct ▾	{ "ts": "_time", "type": "event", "sourcetype": "dsappevent", "index": "main" }	▾
	<input type="checkbox"/>	splunk_server ▾	splunk-enterprise	▾

Part 4: DS Design & App Checksums

Deployment Server Scaling



Deployment Server Design

Scaling your implementation

- Scaling your deployment server
- Distributed/load-balanced DS
- DS Clustering
- Cross-Server Checksums

Scaling Your Deployment Server

When to do it?

Scaling Your Deployment Server

When to do it?

- When you need a dedicated deployment server?
 - More than 50 clients

Scaling Your Deployment Server

When to do it?

- When you need a dedicated deployment server?
 - More than 50 clients
- Maximum clients per deployment server?
 - 25k (new in Splunk 9.2)
 - Older versions: ~10k(ish)

Scaling Your Deployment Server

When to do it?

- When you need a dedicated deployment server?
 - More than 50 clients
- Maximum clients per deployment server?
 - 25k (new in Splunk 9.2)
 - Older versions: ~10k(ish)
- Need more?
 - Distributed Deployment Servers
 - Deployment Server Clustering

Distributed Deployment Servers

Distributed Deployment Servers

- The forwarder check in is an HTTP request = can be load balanced

Distributed Deployment Servers

- The forwarder check in is an HTTP request = can be load balanced
- Approach
 - Synchronize configurations across multiple DSes (outside of Splunk)

Distributed Deployment Servers

- The forwarder check in is an HTTP request = can be load balanced
- Approach
 - Synchronize configurations across multiple DSes (outside of Splunk)
 - Use a load-balancer to balance forwarder check ins across multiple DS

Distributed Deployment Servers

- The forwarder check in is an HTTP request = can be load balanced
- Approach
 - Synchronize configurations across multiple DSes (outside of Splunk)
 - Use a load-balancer to balance forwarder check ins across multiple DS
 - Consideration - load balancer stickiness must be longer than phoneHomeInterval

Deployment Server Clustering

Deployment Server Clustering

- Still requires load balancing or a multi-value DNS record

Deployment Server Clustering

- Still requires load balancing or a multi-value DNS record
- Requires shared drive between DSes

Deployment Server Clustering

- Still requires load balancing or a multi-value DNS record
- Requires shared drive between DSes
- All deployment servers use the same deployment-apps location and log to the same client_events log

crossServerChecksum

- Each app has a calculated checksum to identify when the content changes
- Recall - bundles contain the modification times of the files

crossServerChecksum

- Each app has a calculated checksum to identify when the content changes
- Recall - bundles contain the modification times of the files
- Problem: if different modification times exist on different deployment servers, each will have a different checksum

crossServerChecksum

- Each app has a calculated checksum to identify when the content changes
- Recall - bundles contain the modification times of the files
- Problem: if different modification times exist on different deployment servers, each will have a different checksum
- Problem: infinite loop of app downloads as forwarders switch between different DSes

**How are
checksums
calculated?**

Checksum Values

- First 64 bits of the MD5 hash of the .bundle file, represented as a decimal (base 10) integer.



Checksum Values

- First 64 bits of the MD5 hash of the .bundle file, represented as a decimal (base 10) integer.



```
# md5sum all_deploymentclient-1714600173.bundle  
724d5ad2533555074f299cbfffb99fcf7
```

Checksum Values

- First 64 bits of the MD5 hash of the .bundle file, represented as a decimal (base 10) integer.

```
# md5sum all_deploymentclient-1714600173.bundle  
724d5ad2533555074f299cbfffb99fcf7
```

```
# grab the first 64 bits  
724d5ad253355507
```




Checksum Values

- First 64 bits of the MD5 hash of the .bundle file, represented as a decimal (base 10) integer.

```
# md5sum all_deploymentclient-1714600173.bundle  
724d5ad2533555074f299cbfffb99fcf7
```

```
# grab the first 64 bits  
724d5ad253355507
```

```
# convert from hex to decimal  
# echo $((0x724d5ad253355507))  
8236339152916141319
```



Checksum Values


- First 64 bits of the MD5 hash of the .bundle file, represented as a decimal (base 10) integer.

```
# md5sum all_deploymentclient-1714600173.bundle
724d5ad2533555074f299cbfffb99fcf7
```

```
# grab the first 64 bits
724d5ad253355507
```

```
# convert from hex to decimal
# echo $((0x724d5ad253355507))
8236339152916141319
```

```
# compare to serverclass.xml
<serverClass name="all_UniversalForwarders">
  <app name="all_deploymentclient"
checksum="8236339152916141319" restartSplunkd="true"
restartSplunkWeb="false"
localArchive="/opt/splunkforwarder1/var/run/all_UniversalFo
rwarders/all_deploymentclient-1714600173.bundle"
installed="true"/>
```



What does `crossServerChecksum` do?



What does `crossServerChecksum` do?

- Simple! The modification time of every file is set to 0



What does `crossServerChecksum` do?

- Simple! The modification time of every file is set to 0
- Ensures that differences in file modification times across servers do not result in the checksum being different



What does `crossServerChecksum` do?

- Simple! The modification time of every file is set to 0
- Ensures that differences in file modification times across servers do not result in the checksum being different
 - Caveat - running the `touch` command to update an app will no longer work to force the app to be redeployed, since the `modtime` is no longer factored in the bundle checksum.



Other Scaling Considerations

- Multiple DS environments for different use cases
 - Server DS
 - Workstation DS
- Different DS environments per region
- How else might we scale DS load?

Lab 4: crossServerChecksum demonstration

- Investigate checksum before and after
- Observe the behavior by exploring the contents of the bundle files

Lab 4: crossServerChecksum demonstration

Explore the contents of the serverclass bundle directories:

```
root@show-demo-i-05800b0e6344772a5:~# cd /opt/splunk/var/run/tmp/all_UniversalForwarders; ls -l
total 32
-rw----- 1 root root 10240 Apr 30 01:52 all_deploymentclient-1714441937.bundle
-rw----- 1 root root  530 Apr 30 01:52 all_deploymentclient-1714441937.bundle.gz
-rw----- 1 root root 10240 Apr 30 01:52 outputs-1714441937.bundle
-rw----- 1 root root  532 Apr 30 01:52 outputs-1714441937.bundle.gz
```


Lab 4: crossServerChecksum demonstration

Extract the bundle file:

```
root@show-demo-i-05800b0e6344772a5:/opt/splunk/var/run/tmp/all_UniversalForwarders# tar -zxvf  
all_deploymentclient-1714441937.bundle.gz -C /tmp/all_deploymentclient_original  
local/app.conf  
local/deploymentclient.conf  
metadata/local.meta
```

Lab 4: crossServerChecksum demonstration

Explore the contents of the extracted bundle:

```
root@show-demo-i-05800b0e6344772a5:/opt/splunk/var/run/tmp/all_UniversalForwarders# ls -ltrah  
/tmp/all_deploymentclient_original/local/  
total 16K  
-rw-r--r-- 1 splunk splunk 257 Apr 25 18:38 app.conf  
-rw-r--r-- 1 splunk splunk 110 Apr 25 19:48 deploymentclient.conf  
drwxr-xr-x 4 root root 4.0K May 1 17:23 ..  
drwxr-xr-x 2 root root 4.0K May 1 17:23 .
```

Lab 4: crossServerChecksum demonstration

Enable crossServerChecksum:

```
root@show-demo-i-05800b0e6344772a5:~# head -2 /opt/splunk/etc/system/local/serverclass.conf  
[global]  
crossServerChecksum = true
```


Lab 4: crossServerChecksum demonstration

Note the modification times of the serverclass directories:

```
root@show-demo-i-05800b0e6344772a5:~# cd /opt/splunk/var/run/tmp/; ls -l
total 24
drwx----- 2 root root 4096 May  1 21:17 100_IngestAction_AutoGenerated
drwx----- 2 root root 4096 May  1 21:25 all_UniversalForwarders
drwx----- 2 root root 4096 May  1 21:17 linux_webservers
drwx----- 2 root root 4096 May  1 21:17 uf1
drwx----- 2 root root 4096 May  1 21:17 uf2
drwx----- 2 root root 4096 May  1 21:17 uf3
```

Lab 4: crossServerChecksum demonstration

View the bundle files:

```
root@show-demo-i-05800b0e6344772a5:~# cd /opt/splunk/var/run/tmp/all_UniversalForwarders; ls -l
total 32
-rw----- 1 root root 10240 May  1 21:17 all_deploymentclient-1714598276.bundle
-rw----- 1 root root   508 May  1 21:17 all_deploymentclient-1714598276.bundle.gz
-rw----- 1 root root 10240 May  1 21:17 outputs-1714598276.bundle
-rw----- 1 root root   511 May  1 21:17 outputs-1714598276.bundle.gz
```

Lab 4: crossServerChecksum demonstration

Extract a new bundle to a new temp directory:

```
root@show-demo-i-05800b0e6344772a5:/opt/splunk/var/run/tmp/all_UniversalForwarders# tar -zxvf all_deploymentclient-1714598276.bundle.gz -C /tmp/all_deploymentclient_crossServer
local/app.conf
local/deploymentclient.conf
metadata/local.meta
```


Lab 4: crossServerChecksum demonstration

View the extracted bundle:

```
root@show-demo-i-05800b0e6344772a5:~# ls -ltrah /tmp/all_deploymentclient_crossServer/local/
total 16K
-rw-r--r-- 1 splunk splunk 110 Jan 1 1970 deploymentclient.conf
-rw-r--r-- 1 splunk splunk 257 Jan 1 1970 app.conf
drwxr-xr-x 4 root root 4.0K May 1 21:37 ..
drwxr-xr-x 2 root root 4.0K May 1 21:37 .
```

Scaling and Design Recap

- What did you see in the bundle files after enabling crossServerChecksum?
- How can we increase the capacity of our deployment server infrastructure?



Part 5:

DS Hardening

Let's Talk Security

DS - Forwarder Security

Why protect the DS?

DS - Forwarder Security

Why protect the DS?

- By default, any forwarder can connect to a DS and obtain configuration

DS - Forwarder Security

Why protect the DS?

- By default, any forwarder can connect to a DS and obtain configuration
- What do you need to know to get configuration information for a different host?

DS - Forwarder Security

Why protect the DS?

- By default, any forwarder can connect to a DS and obtain configuration
- What do you need to know to get configuration information for a different host?
- Where might this be a problem?

DS - Forwarder Security

Why protect the DS?

- By default, any forwarder can connect to a DS and obtain configuration
- What do you need to know to get configuration information for a different host?
- Where might this be a problem?
- What else can the DS do?

DS Security Tips

- Restrict who can access the DS
 - Run the DS on a dedicated instance
 - SplunkWeb and SSH access to the DS should be limited

Impersonating Another Forwarder

- Serverclasses typically will filter on:
 - Hostname
 - Machine Type
- A rogue deployment client with the same hostname will get the same apps
- Deployment Server cannot easily identify systems with conflicting hostnames
 - Clean up conflicting client names with the `clone-prep-clear-config` command on affected forwarders
 - Deployment server will log when known forwarder attributes change
 - We can use this search to find duplicate GUIDs
 - `index=_internal sourcetype=splunkd "has changed some of its properties on the latest phone home"`

Authenticating Forwarders

Securing the connection

- Forwarders can be authenticated via:
 - pass4SymmKey
 - Shared certificates
- Most straightforward: pass4SymmKey

Implementing Authentication



Implementing Authentication

- Requires server.conf and restmap.conf changes



Implementing Authentication

- Requires server.conf and restmap.conf changes

On Deployment Server

```
$ cat restmap.conf  
[broker:broker]  
authKeyStanza=deployment  
requireAuthentication = true  
  
[streams:deployment]  
authKeyStanza=deployment  
requireAuthentication = true
```


Implementing Authentication

- Requires server.conf and restmap.conf changes
- Use a **different** shared secret from other pass4Symmkey values in your environment

```
##### On Deployment Server #####
```

```
$ cat restmap.conf  
[broker:broker]  
authKeyStanza=deployment  
requireAuthentication = true
```

```
[streams:deployment]  
authKeyStanza=deployment  
requireAuthentication = true
```

```
$ cat server.conf  
[deployment]  
pass4SymmKey = <shared_secret>
```

Implementing Authentication

- Requires server.conf and restmap.conf changes
- Use a **different** shared secret from other pass4Symmkey values in your environment

```
##### On Deployment Server #####
```


```
$ cat restmap.conf  
[broker:broker]  
authKeyStanza=deployment  
requireAuthentication = true
```

```
[streams:deployment]  
authKeyStanza=deployment  
requireAuthentication = true
```

```
$ cat server.conf  
[deployment]  
pass4SymmKey = <shared_secret>
```

```
##### On Universal Forwarder/Deployment Client #####
```

```
$ cat server.conf  
[deployment]  
pass4SymmKey = <shared_secret>
```



Lab 5: Implement Pass4SymmKey Authentication for UF

- Implementing authentication between forwarders and the Deployment Server

Lab 5: Implement Pass4SymmKey Authentication for UF

```
root@show-demo-i-05800b0e6344772a5:~# cat /opt/splunk/etc/deployment-apps/uf_authentication/local/server.conf
#If you are using shared secrets for authentication to the Deployment Server, add the unique
#pass4SymmKey for this authentication here. This needs to match the key in infra_ds_authentication

[deployment]
pass4SymmKey = Really_S3cure_P@ssword!
```

Lab 5: Implement Pass4SymmKey Authentication for UF

```
root@show-demo-i-05800b0e6344772a5:/opt/splunk# cat /opt/splunk/etc/disabled-apps/infra_ds_authentication/local/server.conf
#Set the password here
#Currently set to Really_S3cure_P@ssword!
[deployment]
pass4SymmKey = Really_S3cure_P@ssword!
root@show-demo-i-05800b0e6344772a5:/opt/splunk# cat /opt/splunk/etc/disabled-apps/infra_ds_authentication/local/restmap.conf
[broker:broker]
authKeyStanza=deployment
requireAuthentication = true

[streams:deployment]
authKeyStanza=deployment
requireAuthentication = true
```

Lab 5: Implement Pass4SymmKey Authentication for UF

splunk>enterprise

Apps

✓

Administrator

Messages

Settings

Activity

Help

Find

Forwarder Management

Documentation

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

3

Clients
PHONED HOME IN THE LAST 24 HOURS

0

Clients
DEPLOYMENT ERRORS

17

Total downloads
IN THE LAST 1 HOUR

Apps (9)

Server Classes (6)

Clients (3)

Phone Home: All

All Clients

filter

3 Clients

10 Per Page

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	show-demo-i-05800b0e6344772a5	uf2	uf2	127.0.0.1	Delete Record	linux-x86_64	5 deployed	a few seconds ago
>	show-demo-i-05800b0e6344772a5	uf3	uf3	127.0.0.1	Delete Record	linux-x86_64	6 deployed	a few seconds ago
>	show-demo-i-05800b0e6344772a5	uf1	uf1	127.0.0.1	Delete Record	linux-x86_64	6 deployed	a few seconds ago

Lab 5: Implement Pass4SymmKey Authentication for UF

```
root@show-demo-i-05800b0e6344772a5:/opt/splunk/etc/apps/infra_ds_authentication/local# cat server.conf
#Set the password here
#Currently set to Really_S3cure_P@ssword!
[deployment]
pass4SymmKey = $7$guZWNt00+Lj4a0mHaqaQo4u0WWhN9rbw6tUqDvW4S8VzAvFne/Cg1508YWDWHvuBZ5RSkpjyIg==
```

Lab 5: Implement Pass4SymmKey Authentication for UF

```
root@show-demo-i-05800b0e6344772a5:~# /opt/splunk/bin/splunk show-decrypted --value  
'$7$guZWNt00+Lj4a0mHaqaQo4u0WWhN9rbw6tUqDvW4S8VzAvFne/Cg1508YWDWHvuBZ5RSkpjyIg=='  
Really_S3cure_P@ssword!
```

Deployment Server Hardening Recap

- Why deploy Forwarder authentication?
- How to implement pass4SymmKey authentication



Part 6: Serverclass Design and Automation

Serverclass Design

Best practices in serverclasses

Serverclass Design

Best practices in serverclasses

- Multiple Serverclasses can apply to the same host

Serverclass Design

Best practices in serverclasses

- Multiple Serverclasses can apply to the same host
- We can utilize narrow-scoped serverclasses to deploy serverclasses in an cumulative manner

Serverclass Design

Best practices in serverclasses

- Multiple Serverclasses can apply to the same host
- We can utilize narrow-scoped serverclasses to deploy serverclasses in an cumulative manner
- Keep each app in as few serverclasses as possible

Serverclass Design

Best practices in serverclasses

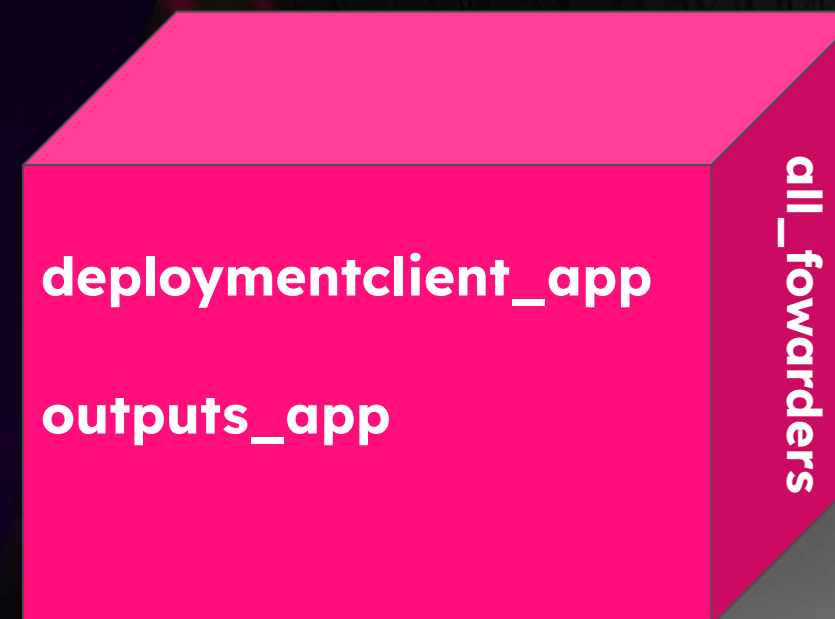
Role: Windows Web Servers

Role: Windows Print Servers

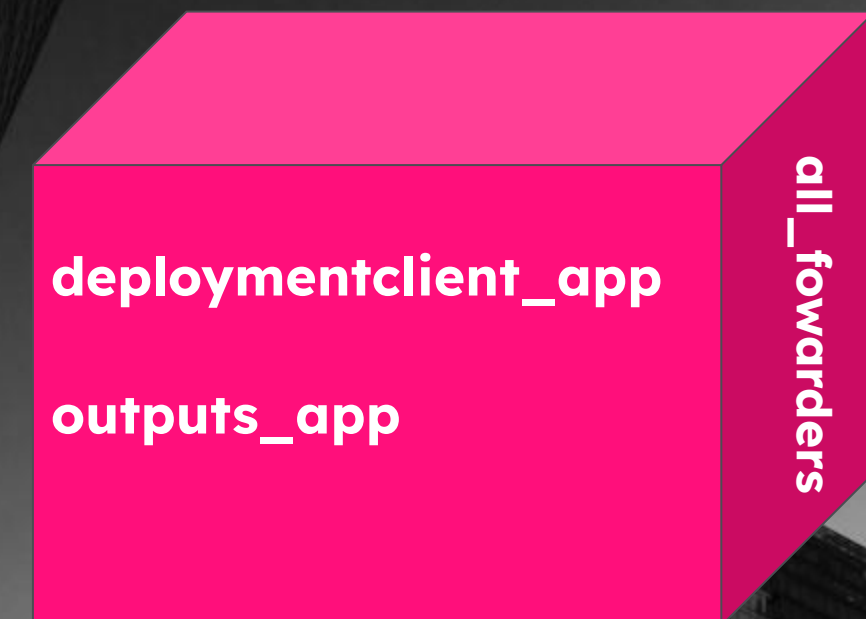
Serverclass Design

Best practices in serverclasses

Role: Windows Web Servers



Role: Windows Print Servers



Serverclass Design

Best practices in serverclasses

apps contained in
serverclass

Role: Windows Web Servers

Role: Windows Print Servers

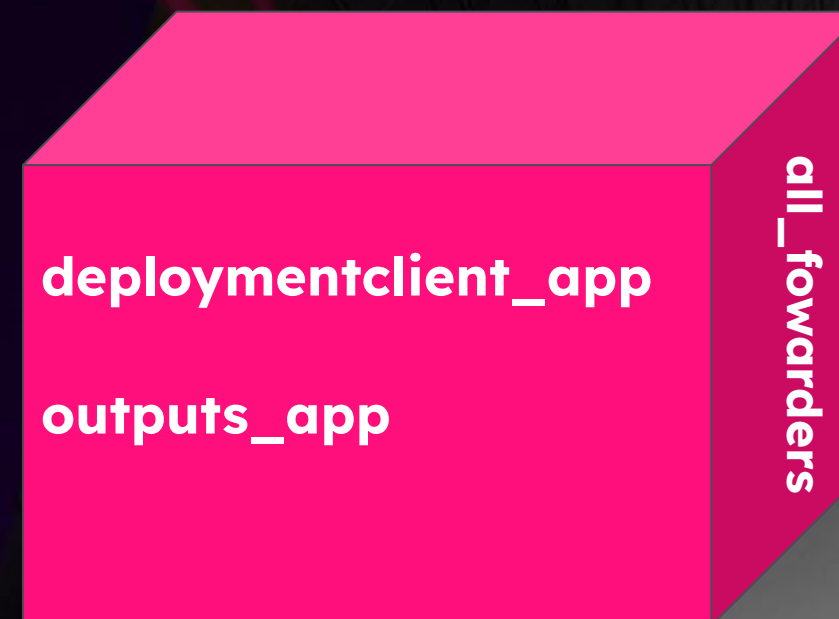


serverclass

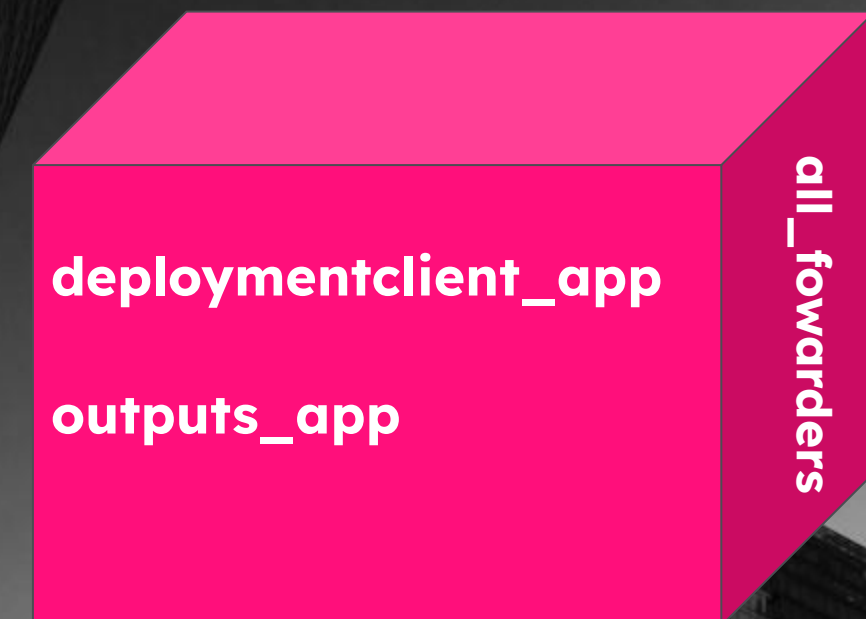
Serverclass Design

Best practices in serverclasses

Role: Windows Web Servers



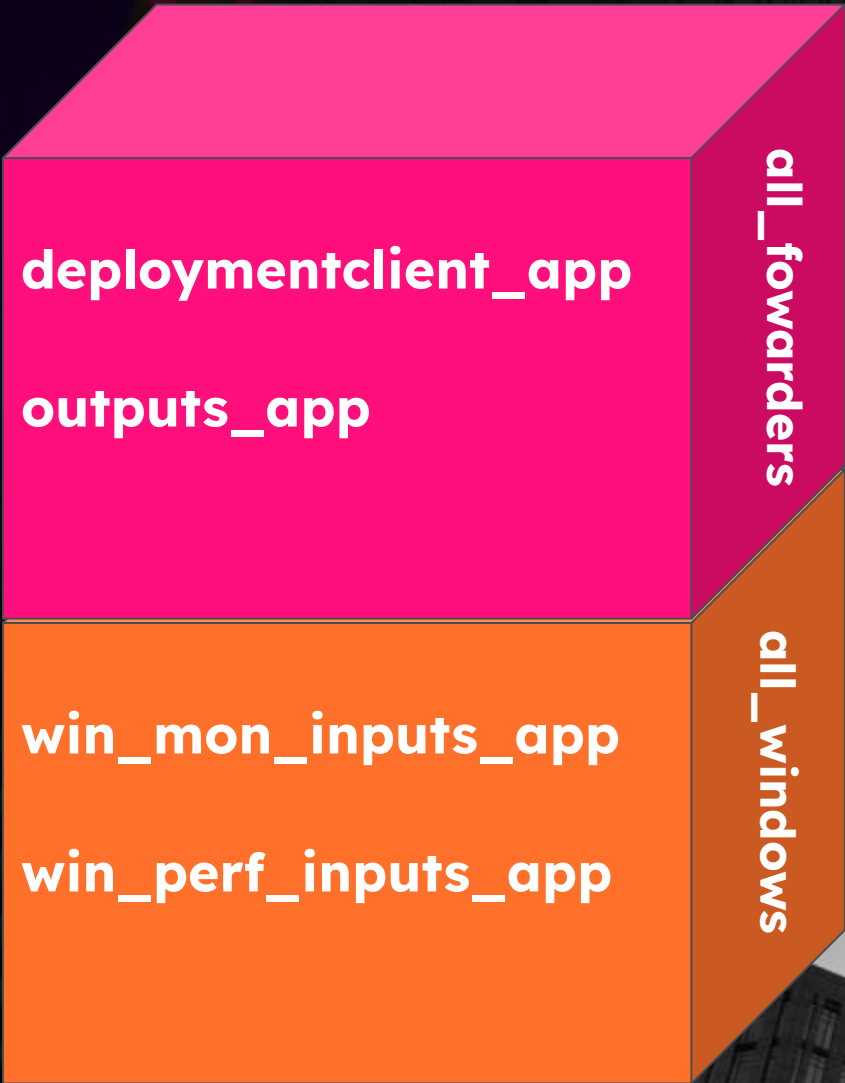
Role: Windows Print Servers



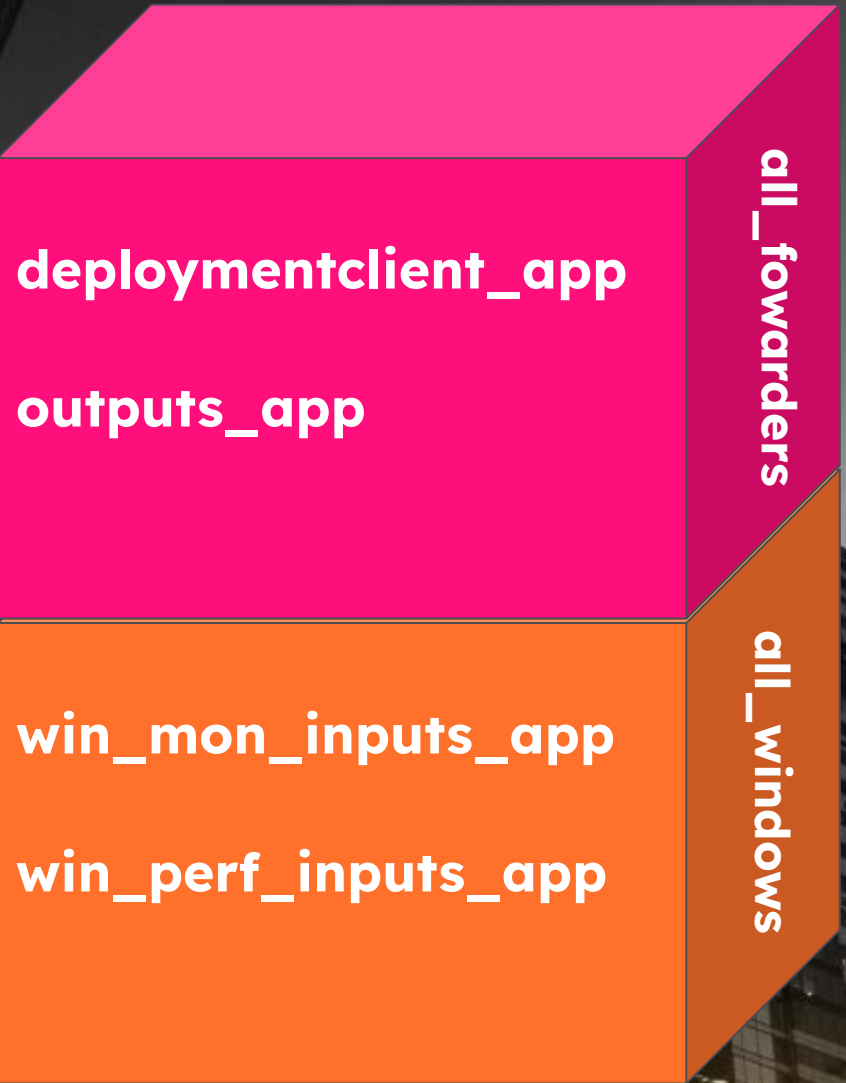
Serverclass Design

Best practices in serverclasses

Role: Windows Web Servers



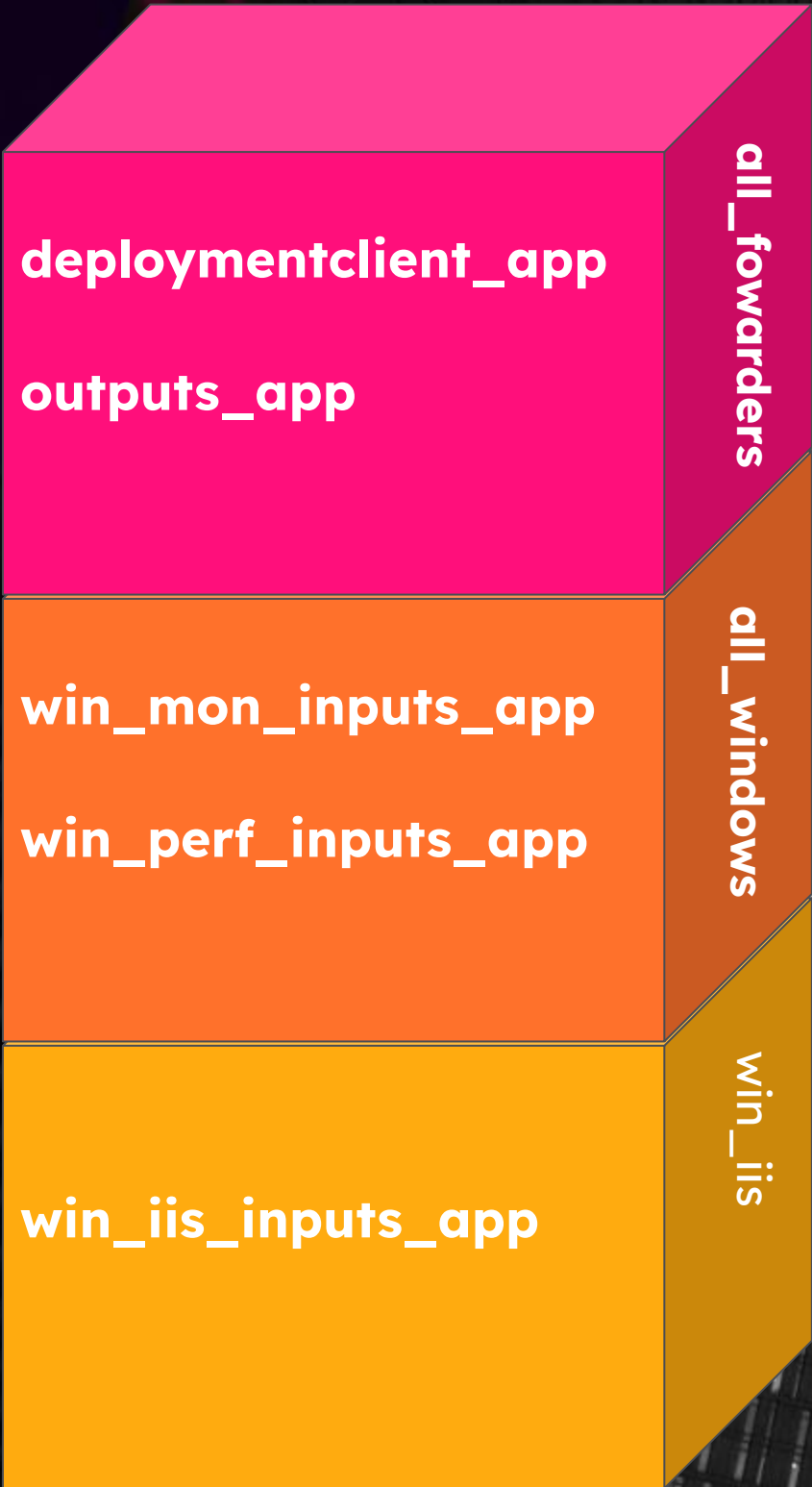
Role: Windows Print Servers



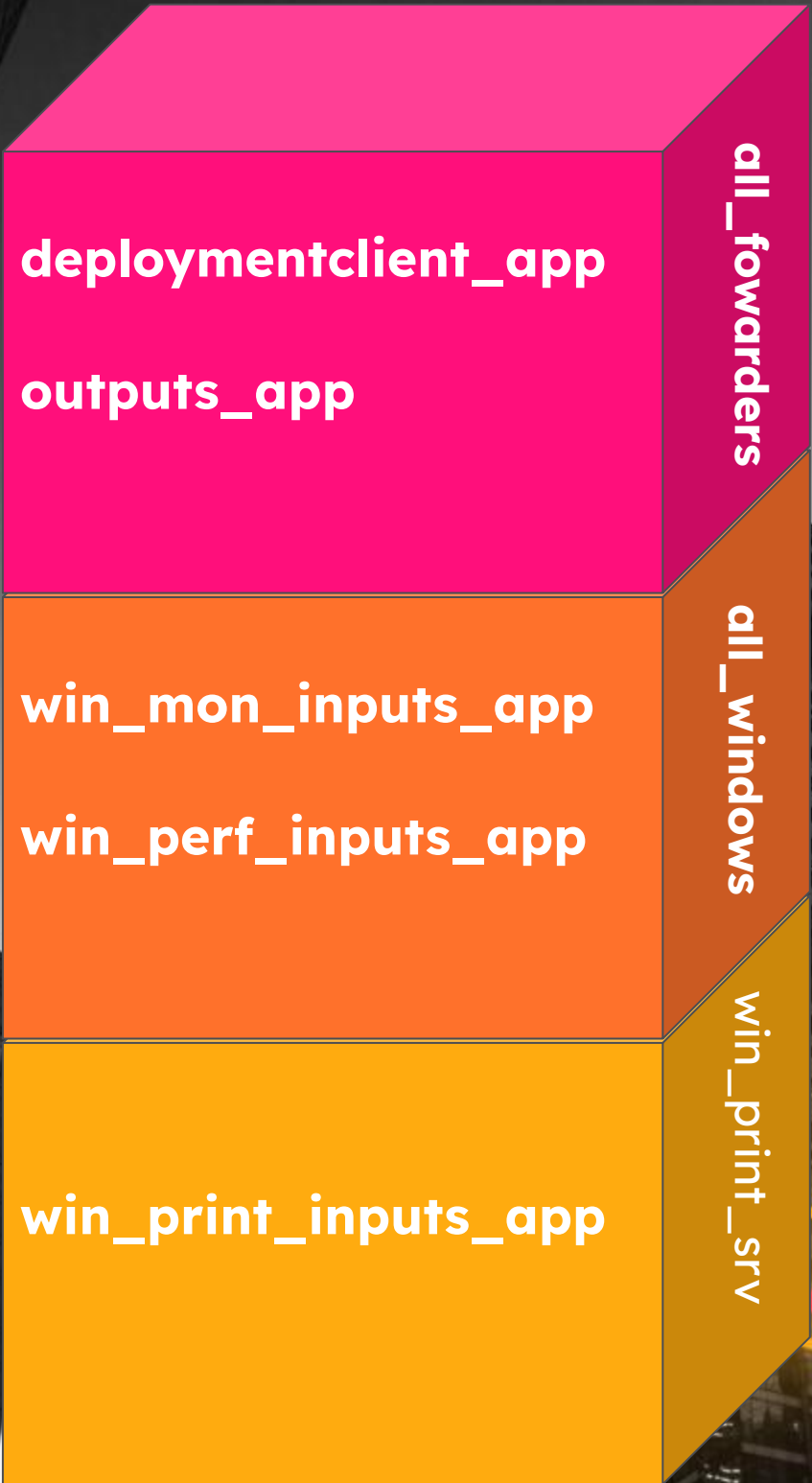
Serverclass Design

Best practices in serverclasses

Role: Windows Web Servers



Role: Windows Print Servers



Serverclass Design

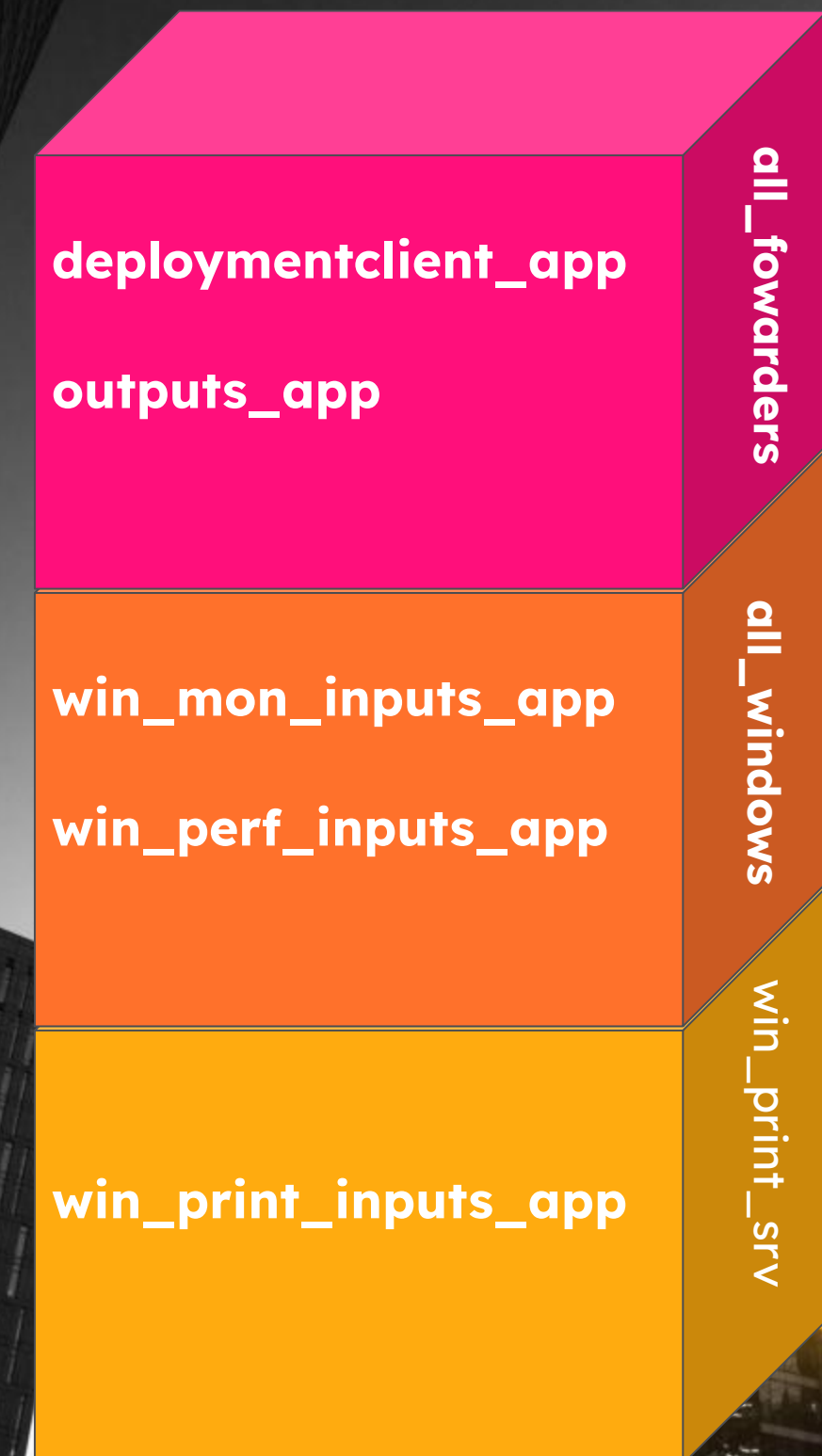
Best practices in serverclasses

- Reduces need to exclude hosts from serverclasses

Role: Windows Web Servers



Role: Windows Print Servers

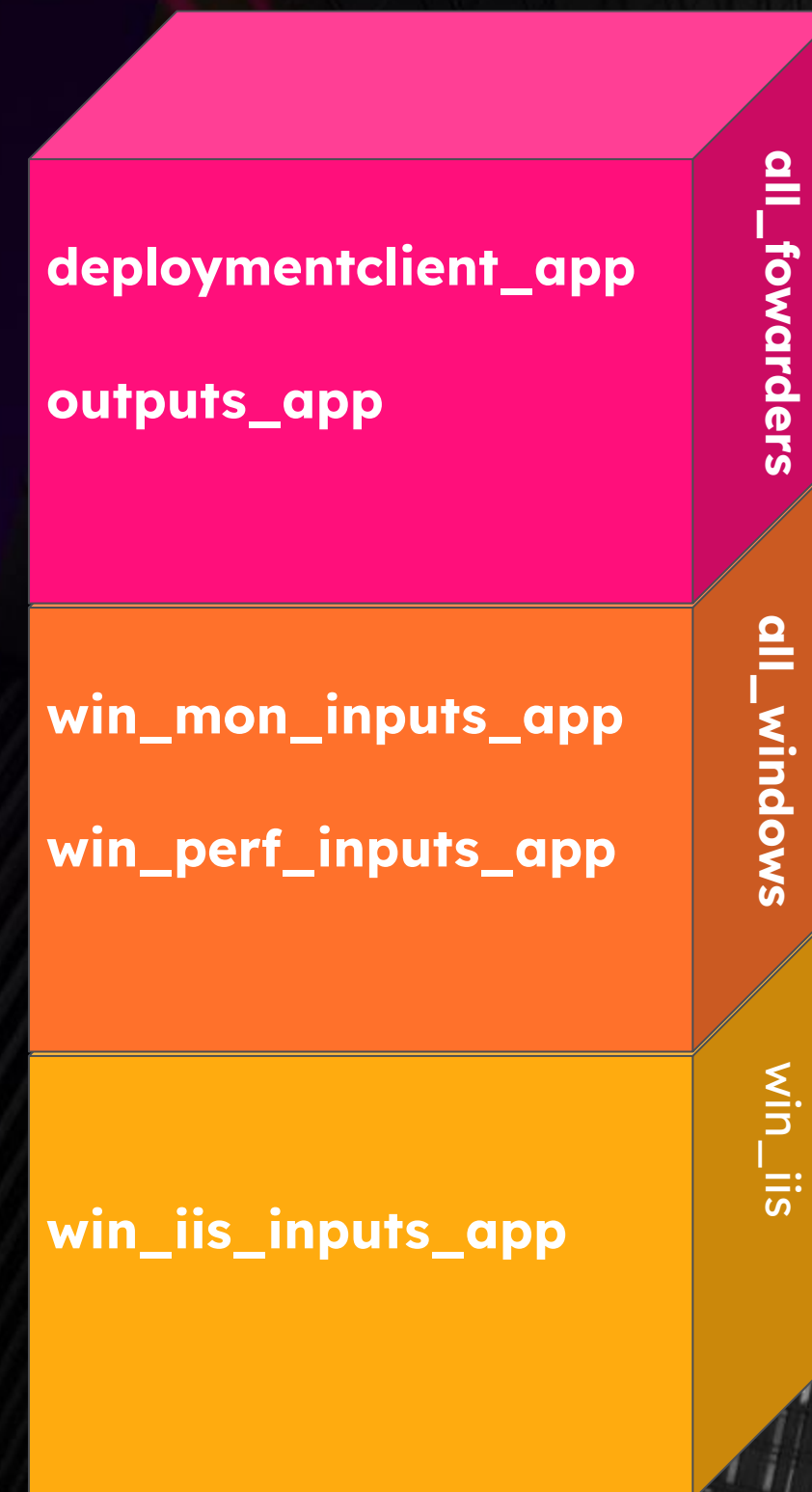


Serverclass Design

Best practices in serverclasses

- Reduces need to exclude hosts from serverclasses
- Reduces bundles created every reload after an app is changed

Role: Windows Web Servers



Role: Windows Print Servers



Serverclass Design

How to handle updating serverclasses

Serverclass Design

How to handle updating serverclasses

- Manually update serverclass.conf

Serverclass Design

How to handle updating serverclasses

- Manually update serverclass.conf
- Use regex for whitelist/blacklists

Serverclass Design

How to handle updating serverclasses

- Manually update serverclass.conf
- Use regex for whitelist/blacklists
- Build a lookup using data from Splunk!

Serverclass Design

How to handle updating serverclasses

- Manually update serverclass.conf
- Use regex for whitelist/blacklists
- Build a lookup using data from Splunk!
- Protip: avoid some of this trouble with an organization-wide naming convention!

Serverclass Lookup Strategies

Using Regex

- Match an expected host naming convention
- Match an expected IP address or range

Serverclass Filter Strategies

- whitelist.<n> = <clientName> | <IP address> | <hostname> | <instanceId>
- blacklist.<n> = <clientName> | <IP address> | <hostname> | <instanceId>
 - (Modified PCRE allowed)
 - . means \ .
 - * means . *

	P-DC*	.*-SQL.*202.*	P-(SQL DC)*	D-.*
P-DC-afk2019	✓		✓	
D-DC-brb2019				✓
P-DC-brb2022	✓		✓	
P-SQL-hmm2022		✓	✓	
D-SQL-bak2022		✓		✓
P-SQL-aob2016			✓	

- machineTypesFilter
 - OS architecture filtering

Automate it!

Serverclass Lookup Strategies

Using a Splunk lookup

Serverclass Lookup Strategies

Using a Splunk lookup

- Generate to match hosted application or service results

Serverclass Lookup Strategies

Using a Splunk lookup

- Generate to match hosted application or service results
- Generate based on problematic system logs

Serverclass Lookup Strategies

Using a Splunk lookup

- Generate to match hosted application or service results
- Generate based on problematic system logs
- Generate based on |ldapsearch results

Serverclass Lookup Strategies

Using a Splunk lookup

Serverclass Lookup Strategies

Using a Splunk lookup

- `whitelist.from_pathname|blacklist.from_pathname`
 - File path to text file or csv

Serverclass Lookup Strategies

Using a Splunk lookup

- `whitelist.from_pathname|blacklist.from_pathname`
 - File path to text file or csv
 - May be used with `(whitelist|blacklist).select_field`
 - Selects the field containing the clientName, IP address, or hostname

Serverclass Lookup Strategies

Using a Splunk lookup

- `whitelist.from_pathname|blacklist.from_pathname`
 - File path to text file or csv
 - May be used with `(whitelist|blacklist).select_field`
 - Selects the field containing the clientName, IP address, or hostname
 - May be used with `(whitelist|blacklist).where_field`
 - Selects a field that can be used as an additional filter in the CSV

Serverclass Lookup Strategies

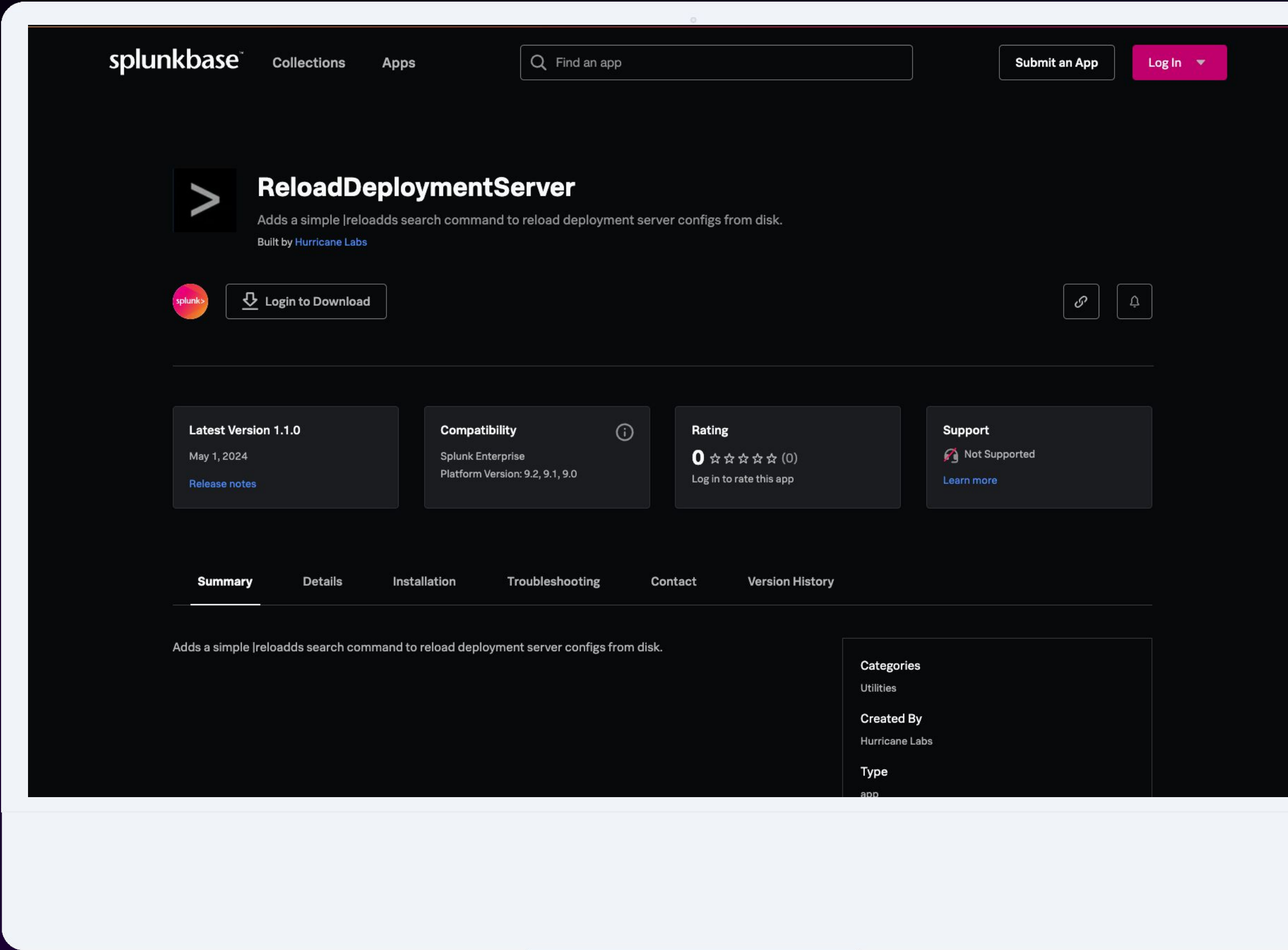
Using a Splunk lookup

- `whitelist.from_pathname|blacklist.from_pathname`
 - File path to text file or csv
 - May be used with `(whitelist|blacklist).select_field`
 - Selects the field containing the clientName, IP address, or hostname
 - May be used with `(whitelist|blacklist).where_field`
 - Selects a field that can be used as an additional filter in the CSV
 - Requires use of `(whitelist|blacklist).where_equals` to specify the filter match
 - `(whitelist|blacklist).where_equals` allows for PCRE matches

ReloadDeploymentServer app

<https://splunkbase.splunk.com/app/7339>

- Adds a |reloadds standalone search command
- Provides a “Reload Deployment Server” alert action



Lab 6: Complex serverclass Population

- Generate a lookup from a search
- Use this to populate a serverclass

Lab 6: Complex serverclass Population

New Search

Save As ▼Create Table ViewClose

index=os process IN (apache nginx postgres) | dedup host| table host process

Last 15 minutes ▼

Q

✓ 3 events (5/1/24 7:28:08.000 PM to 5/1/24 7:43:08.000 PM)

Job ▼

||

→

🖨

⬇

💡 Smart Mode ▼

No Event Sampling ▼

Events

Patterns

Statistics (3)

Visualization

20 Per Page ▼

✍ Format

Preview ▼

host ⬆	process ⬆
uf1	nginx
uf2	postgres
uf3	apache

Lab 6: Complex serverclass Population

Save As Alert

Settings

Title

serverclass_gen

Description

Generates a list of server hosts from processes

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run on Cron Schedule

Time Range

Last 15 minutes

Cron Expression

*/2 ****

e.g. 00 18 *** (every day at 6PM). [Learn More](#)

Expires

24

hour(s)

Trigger Conditions

Trigger alert when

Number of Results

is greater than

0

Trigger

Once

For each result

Throttle

☐

Trigger Actions

+ Add Actions

When triggered

Output results to lookup

Remove

File name

serverclass.csv

Provide a new or existing .csv lookup table file name.

Results

Append

Replace

Each time the report runs, its new results are added to the lookup table or replace the lookup table.

Reload Deployment Server

Remove

Cancel

Save

Lab 6: Complex serverclass Population

```
[serverClass:linux_webservers]
whitelist.from_pathname = etc/apps/search/lookups/serverclass.csv
whitelist.select_field = host
whitelist.where_field = process
whitelist.where_equals = nginx, apache
machineTypesFilter = linux-x86_64

[serverClass:linux_webservers:app:webserver_inputs]
restartSplunkWeb = 0
restartSplunkd = 1
```

Lab 6: Complex serverclass Population

Server Class: linux_webserver

Back to Forwarder Management

Edit

Documentation

1 App

IN THE SERVER CLASS

2 Clients

IN THE SERVER CLASS

100% Clients

DEPLOYED APPS SUCCESSFULLY

Apps

Edit

Deployed Successfully

filter

1 Apps

10 Per Page

Name	Actions	After Installation	Clients
webserver_inputs	Edit	Enable App, Restart Splunkd	2 deployed

Clients

Edit

Phone Home: All

All Clients

filter

2 Clients

10 Per Page

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	show-demo-i-05800b0e6344772a5	uf3	uf3	127.0.0.1	Delete Record	linux-x86_64	6 deployed	a few seconds ago
>	show-demo-i-05800b0e6344772a5	uf1	uf1	127.0.0.1	Delete Record	linux-x86_64	6 deployed	a few seconds ago

Lab 6: Complex serverclass Population

New Search

Save As ▼Create Table ViewClose

index=main sourcetype=webserver_identifier | stats values(host)

Last 15 minutes ▼

Q

✓ 11 events (4/30/24 1:25:17.000 AM to 4/30/24 1:40:17.000 AM)

Job ▼||→🖨️⬇️💡 Smart Mode ▼

No Event Sampling ▼

EventsPatternsStatistics (1)Visualization

20 Per Page ▼✎ FormatPreview ▼

values(host) ⬆️✎

uf1uf3

Serverclass Design Recap

- Populate a serverclass and reload the deployment server via a savedsearch
- Create a serverclass that utilizes a filtered lookup as a whitelist
- Use hostname schemes to accurately identify serverclass hosts



Let's Recap!

What did we learn?

What did we learn?



How the DS works

Photo credit:
<https://www.pexels.com/photo/boy-repairing-toy-car-19364584/>
<https://www.pexels.com/photo/a-girl-carrying-a-stack-of-books-5561162/>
<https://www.pexels.com/photo/concentrated-asian-kid-in-policeman-costume-blowing-whistle-5560552/>
<https://www.pexels.com/photo/group-of-children-playing-on-green-grass-8613319/>

What did we learn?



How the DS works



**Bundles &
Checksums**

Photo credit:
<https://www.pexels.com/photo/boy-repairing-toy-car-19364584/>
<https://www.pexels.com/photo/a-girl-carrying-a-stack-of-books-5561162/>
<https://www.pexels.com/photo/concentrated-asian-kid-in-policeman-costume-blowing-whistle-5560552/>
<https://www.pexels.com/photo/group-of-children-playing-on-green-grass-8613319/>

What did we learn?



How the DS works



**Bundles &
Checksums**



Security Tips

Photo credit:
<https://www.pexels.com/photo/boy-repairing-toy-car-19364584/>
<https://www.pexels.com/photo/a-girl-carrying-a-stack-of-books-5561162/>
<https://www.pexels.com/photo/concentrated-asian-kid-in-policeman-costume-blowing-whistle-5560552/>
<https://www.pexels.com/photo/group-of-children-playing-on-green-grass-8613319/>

What did we learn?



How the DS works



**Bundles &
Checksums**



Security Tips



**Automation and
Scaling**

Photo credit:
<https://www.pexels.com/photo/boy-repairing-toy-car-19364584/>
<https://www.pexels.com/photo/a-girl-carrying-a-stack-of-books-5561162/>
<https://www.pexels.com/photo/concentrated-asian-kid-in-policeman-costume-blowing-whistle-5560552/>
<https://www.pexels.com/photo/group-of-children-playing-on-green-grass-8613319/>

Questions?

Need more help?

Come visit us at the Hurricane Labs booth!



Take this and run.

Thank you!



Thank you

