© 2017 SPLUNK INC.

splunk> .conf2017

Pushing Configuration Bundles in an Indexer Cluster

Kartheek Kolla | Software Engineer, Splunk

Meema Esguerra | Software Engineer, Splunk

© 2017 SPLUNK INC.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

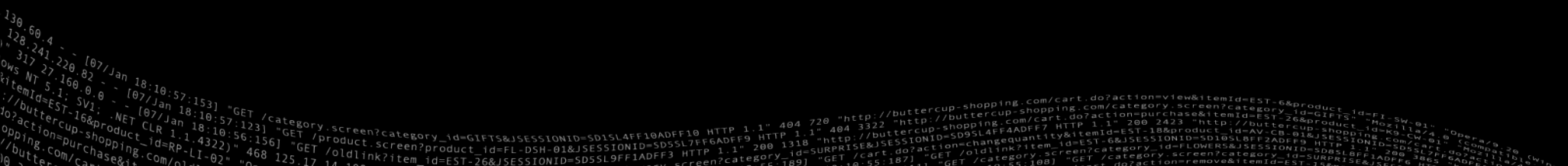
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

splunk> .conf2017

© 2017 SPLUNK INC.

Agenda

- Overview of Indexer Clustering
- Configuration Management in an Indexer Cluster.
  - What is a bundle? And why should I care?
  - Creating and distributing the bundle to all peers
  - Other bundle operations (validate, check restart, and roll back)
  - To restart or not to restart
  - Phased bundle downloads
- Demo
- Troubleshooting and Best Practices
- QA



splunk> .conf2017

© 2017 SPLUNK INC.

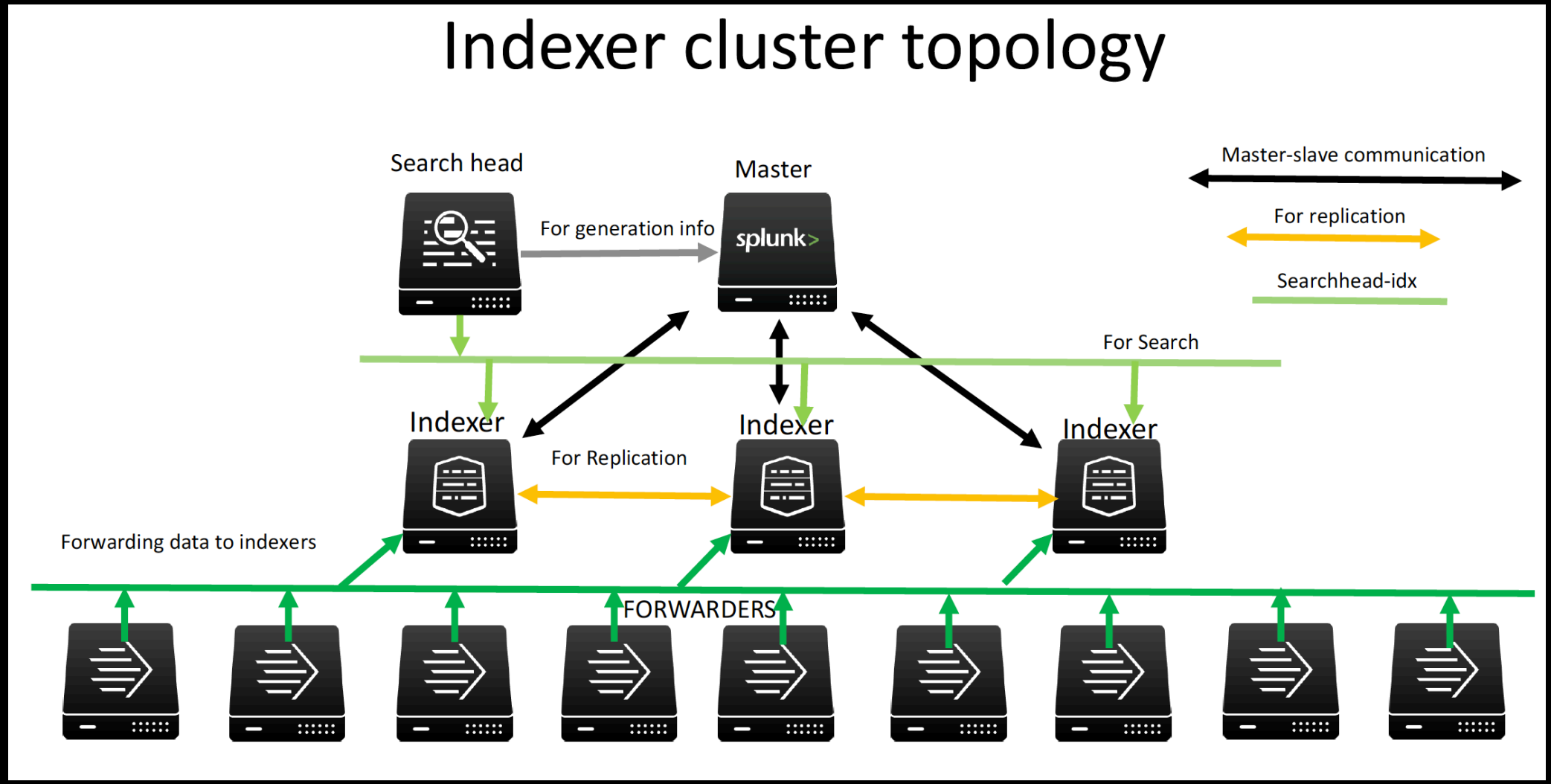
Indexer Cluster Overview

Pushing Configuration Bundles in an Indexer Cluster

splunk> .conf2017

© 2017 SPLUNK INC.

Indexer Clustering



splunk> .conf2017

© 2017 SPLUNK INC.

Why Use Clustering?

Index Replication, Of Course

Data Availability

Data Fidelity

Data Resiliency

Disaster Recovery

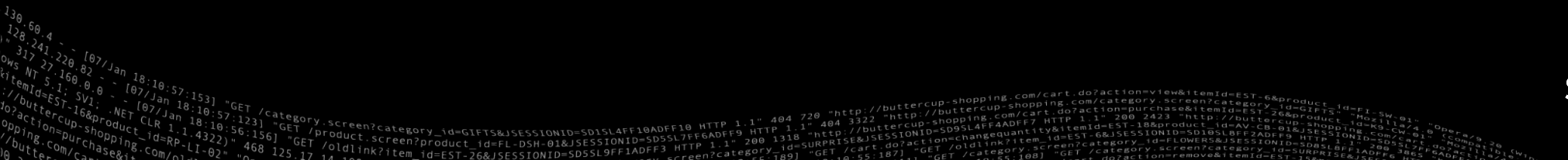
Search Affinity

splunk> .conf2017

© 2017 SPLUNK INC.

Elements of an Indexer Cluster

- Cluster Master
  - Manages the cluster activities (peer addition, configuration distribution)
  - Maintains an in-memory state of all the peers & their corresponding buckets, configs
  - Orchestrates remedial activities during peer failures
  - Tells search heads where to search
- Cluster Peer (Indexer)
  - Receive and index incoming data (typically from forwarders)
  - Replicate data to other peers for data availability
  - Respond to the incoming searches by providing search results
  - Update cluster master on any state change (peer, buckets, configs etc.)



© 2017 SPLUNK INC.

Configuration Management in the Cluster

Pushing Configuration Bundles in an Indexer Cluster

splunk> .conf2017

© 2017 SPLUNK INC.

Configuration Bundles

What is a bundle? And why should you care?

The Mysterious Bundle

- The set of configuration files and apps common to all peers
- Managed from the master
- Distributed to the peers in a single operation
  - i.e. indexes.conf, props.conf, and transforms.conf
  - apps will also include versions of these configuration files

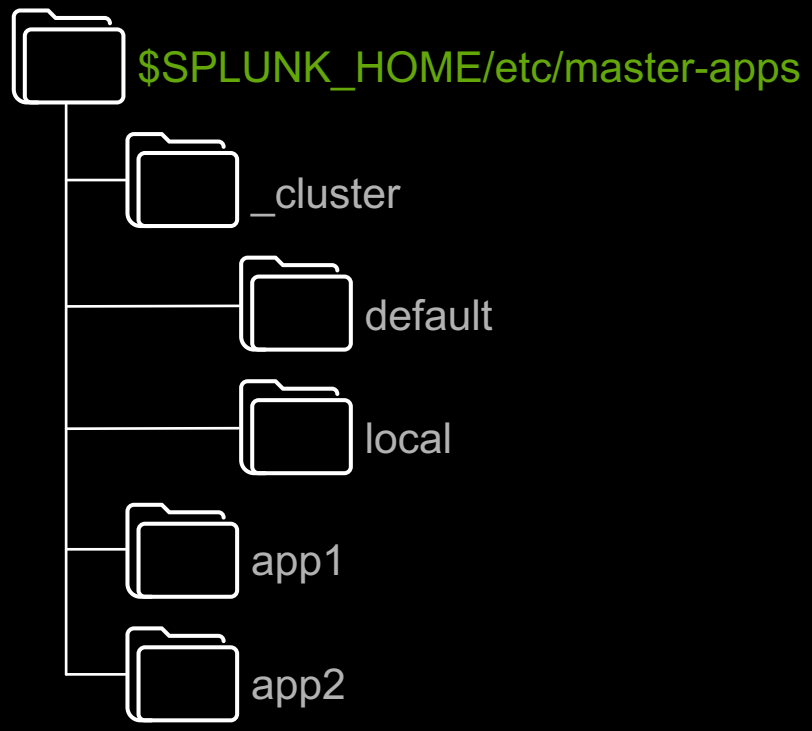
splunk> .conf2017

© 2017 SPLUNK INC.

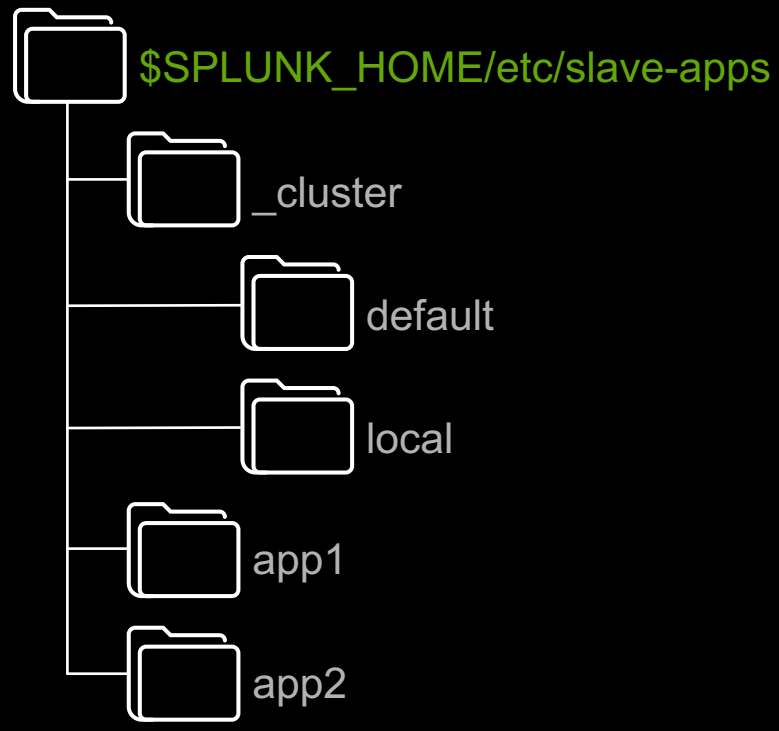
Where do the Bundles reside?

Both in the Cluster Master and the Cluster Peers

Cluster Master



Cluster Peer



splunk> .conf2017

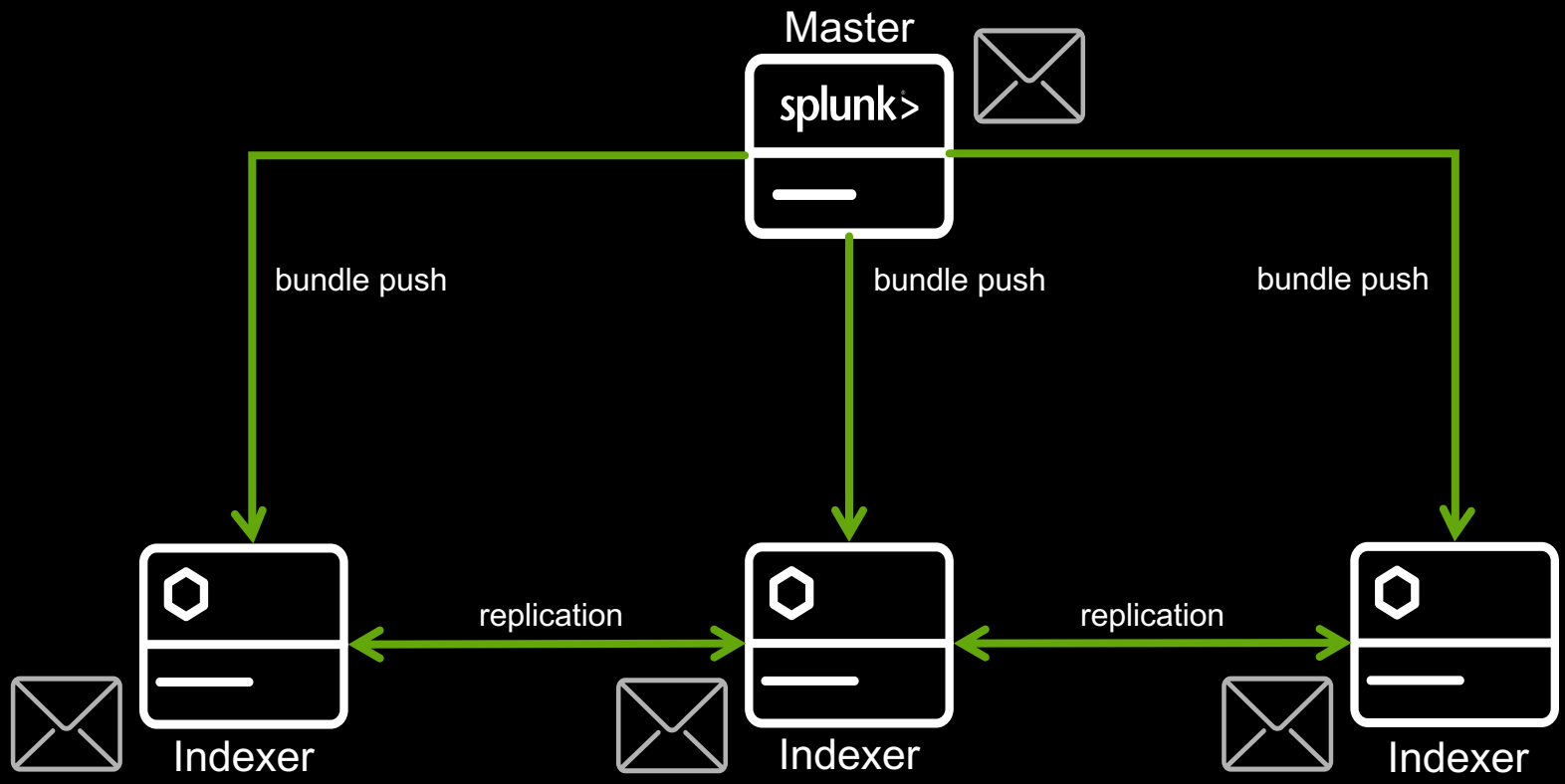
© 2017 SPLUNK INC.

To distribute new or edited configuration files or apps across peers, execute a Bundle Push Operation.

© 2017 SPLUNK INC.

Bundle Pushing

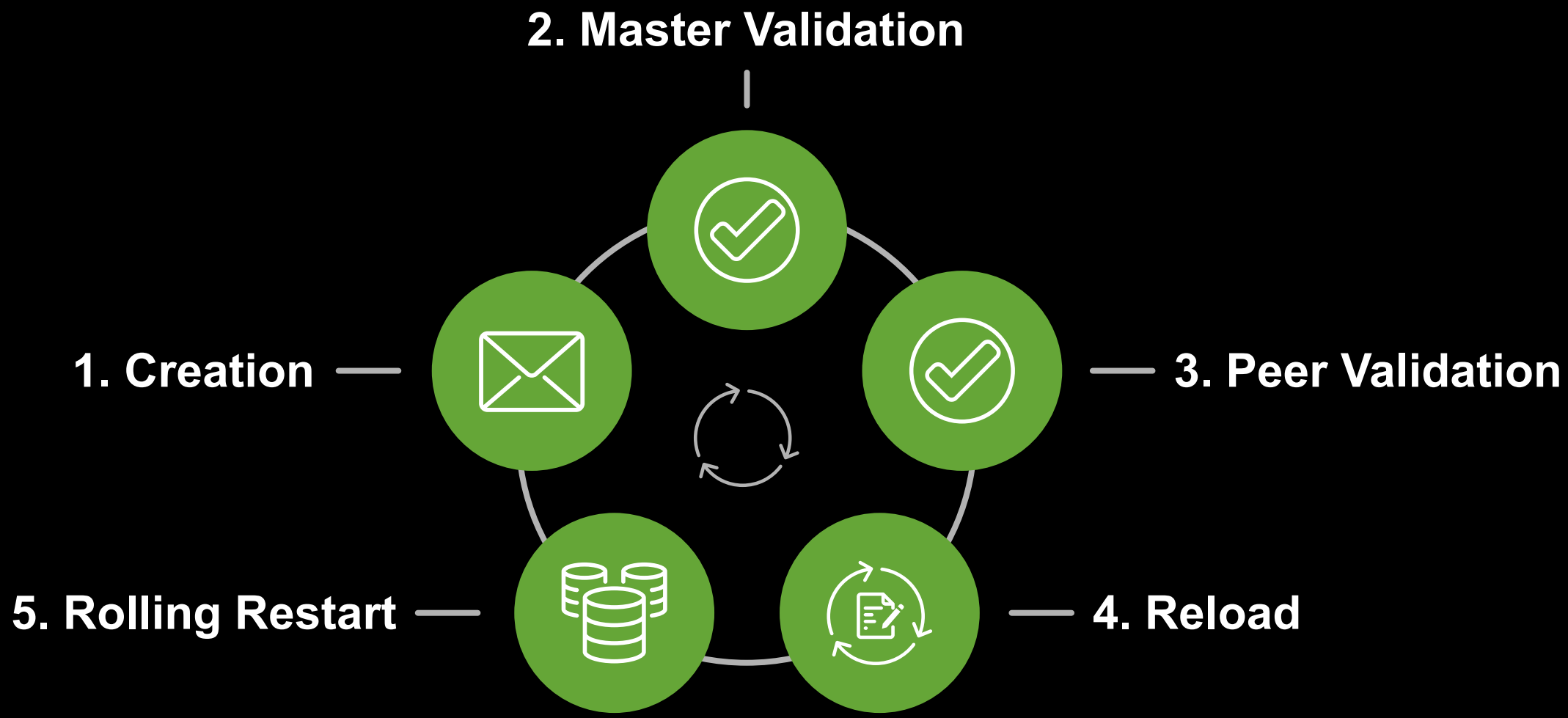
It's not like replication



© 2017 SPLUNK INC.

States of a Bundle Push

States in a Bundle Push Status Report



splunk> .conf2017

© 2017 SPLUNK INC.

Validating a Bundle

- Validate a bundle with the peers if bundle is acceptable
- $ ./bin/splunk validate cluster-bundle

splunk> .conf2017

© 2017 SPLUNK INC.

Rolling Back a Bundle

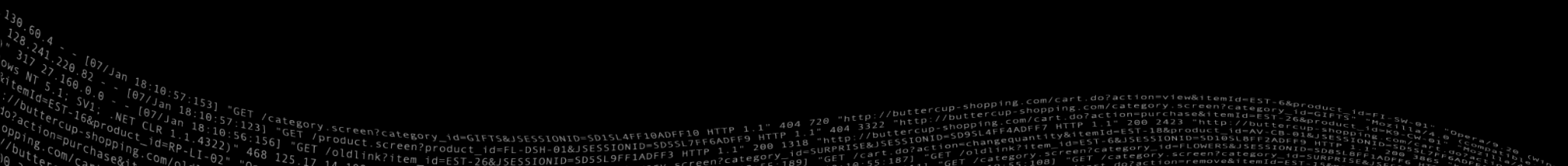
- Did something go wrong with the bundle that was just pushed? You can rollback the latest bundle
- $ ./bin/splunk rollback cluster-bundle

splunk> .conf2017

© 2017 SPLUNK INC.

To Restart or Not To Restart

- Configuration changes which need a restart to apply
  - Changes to indexes.conf (deleting an index), inputs.conf
  - Change home path in index.conf
  - Delete an existing App
- Configuration changes which do not need a restart to apply
  - Adding a new index in indexes.conf, or a new app with reloadable configuration
  - Changes or additions to transforms.conf or props.conf



splunk> .conf2017

© 2017 SPLUNK INC.

Checking for Restart

- Do you want to know whether your config changes require a restart?
- Allows admins to plan ahead when the configuration changes will trigger a rolling restart.
- $ ./bin/splunk validate cluster-bundle –check-restart

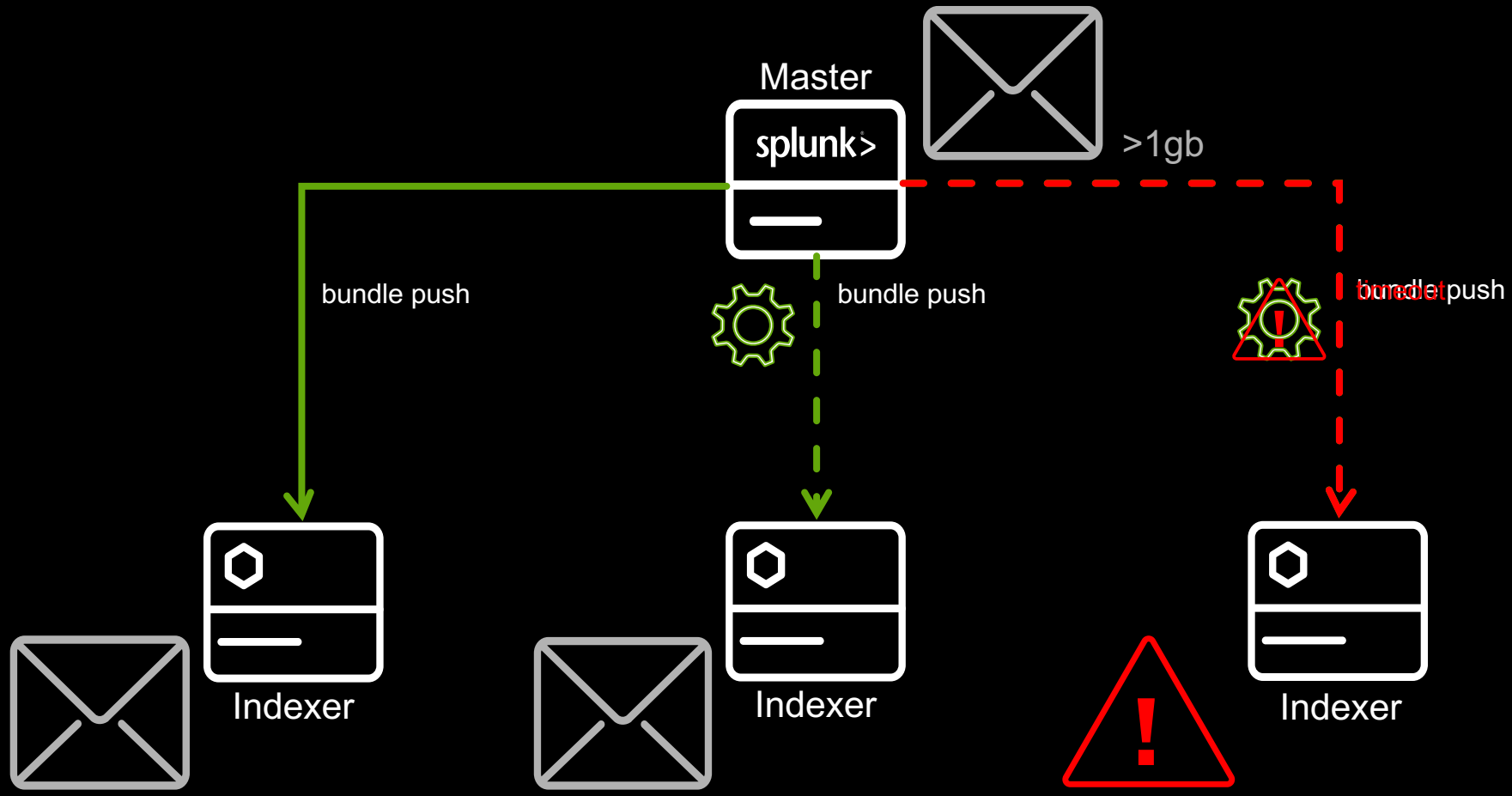
Reload and Restart Simulation

splunk> .conf2017

© 2017 SPLUNK INC.

Oh No! Large Bundles

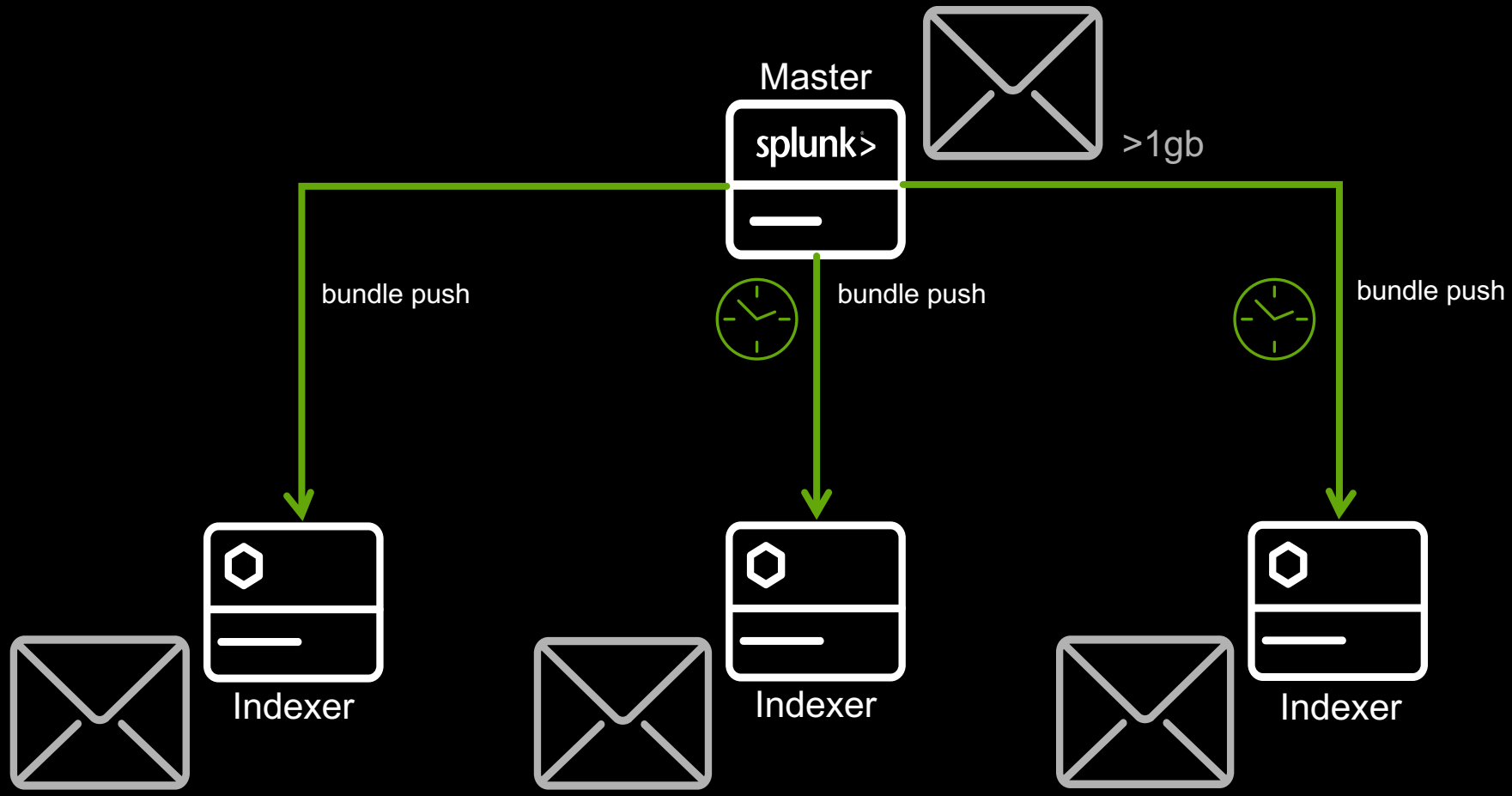
Network Congestion and Timeouts



© 2017 SPLUNK INC.

Phased Bundle Downloads

Sending to One Peer at a time



© 2017 SPLUNK INC.

Enabling Phased Bundle Downloads

- This is recommended if a cluster master is pushing large bundles or even a smaller bundle but to a large cluster (20 or more indexers).
- To enable, set the following configuration within server.conf

```
#inside server.conf
[clustering]
mode=master
max_peers_to_download_bundle = 1
```

splunk> .conf2017

© 2017 SPLUNK INC.

Recap

Bundle Push and Other Operations

1. Configuration Bundle
2. Bundle Operations: Apply, Validate, Check for Restart, Rollback
3. States during Bundle Push
4. Phased Bundle Downloads

© 2017 SPLUNK INC.

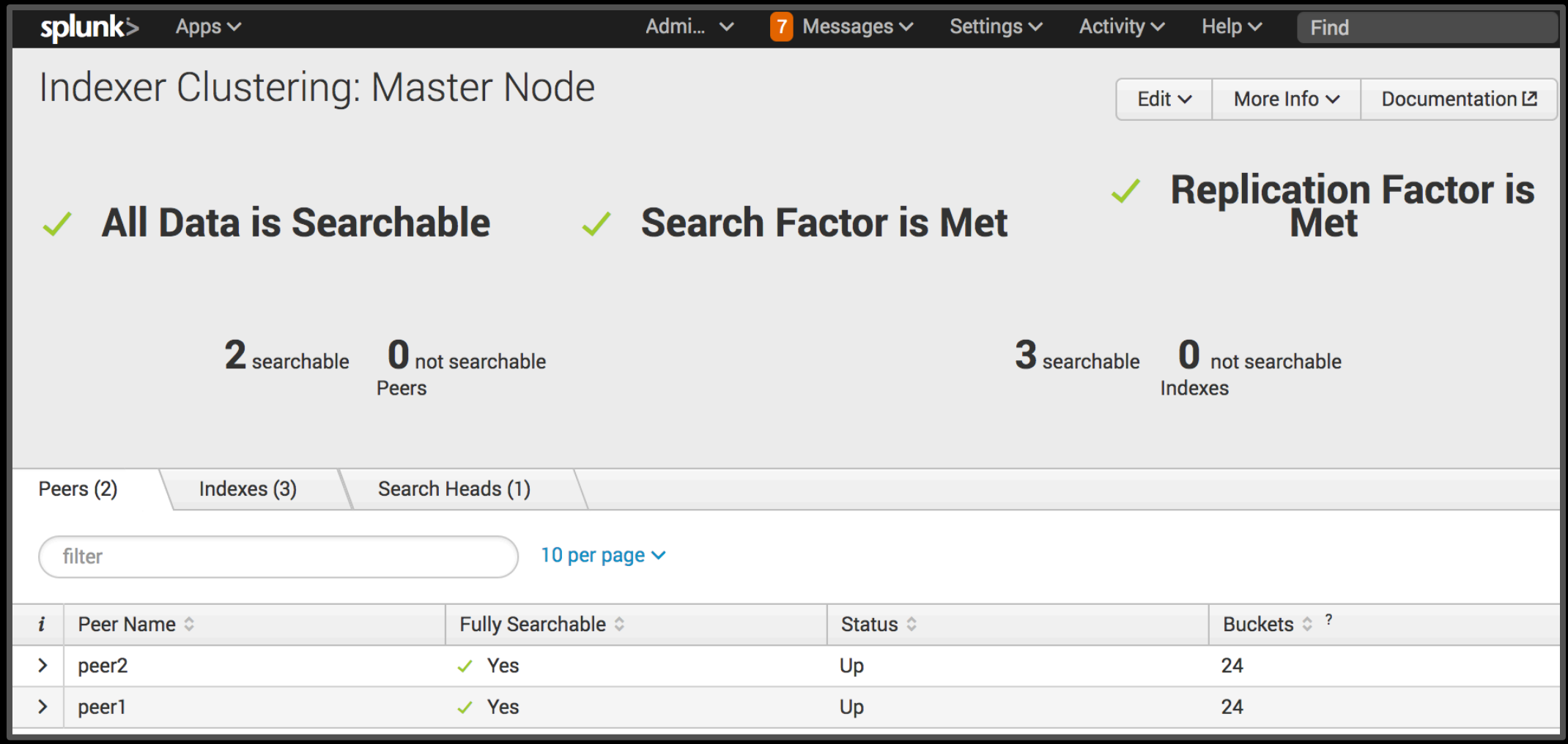
DEMO

Skip Screenshots

© 2017 SPLUNK INC.

Bundle Operations

Cluster Master UI – Indexer Clustering

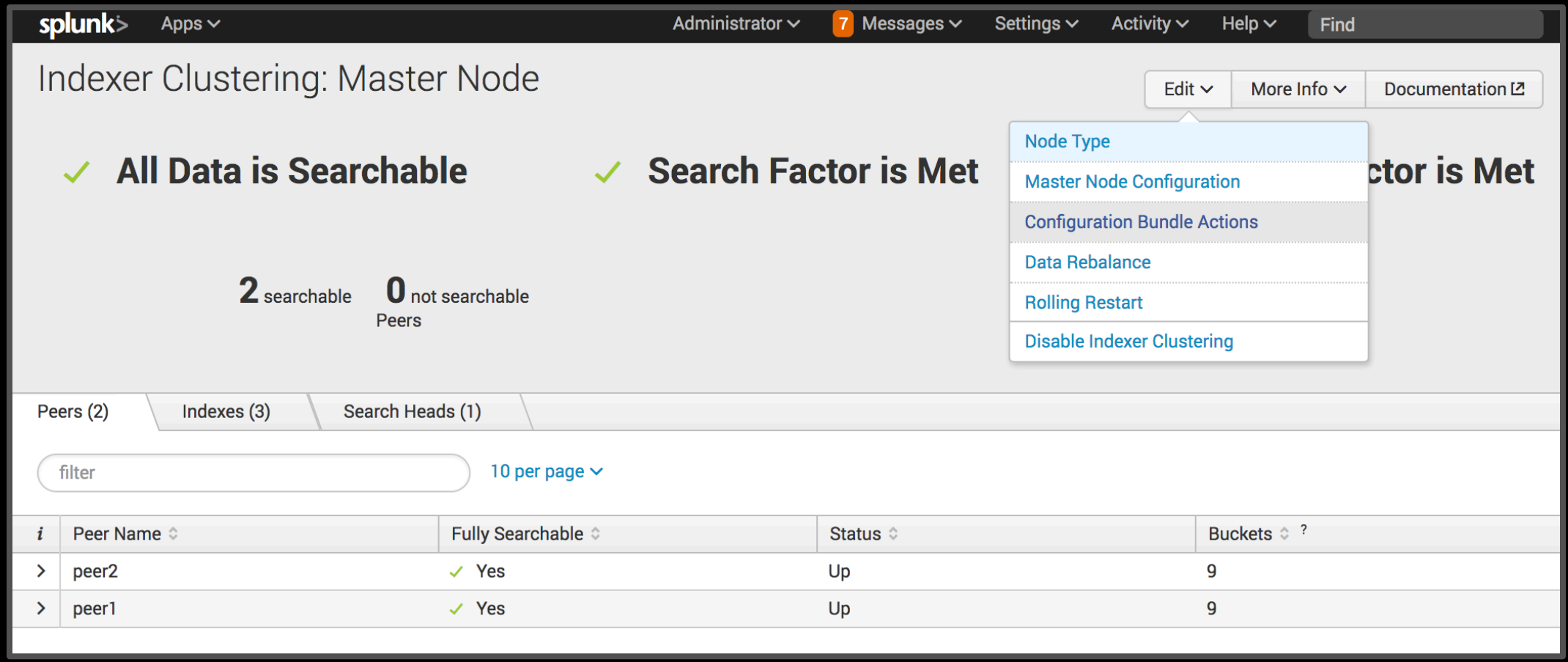


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Configuration Bundle Actions

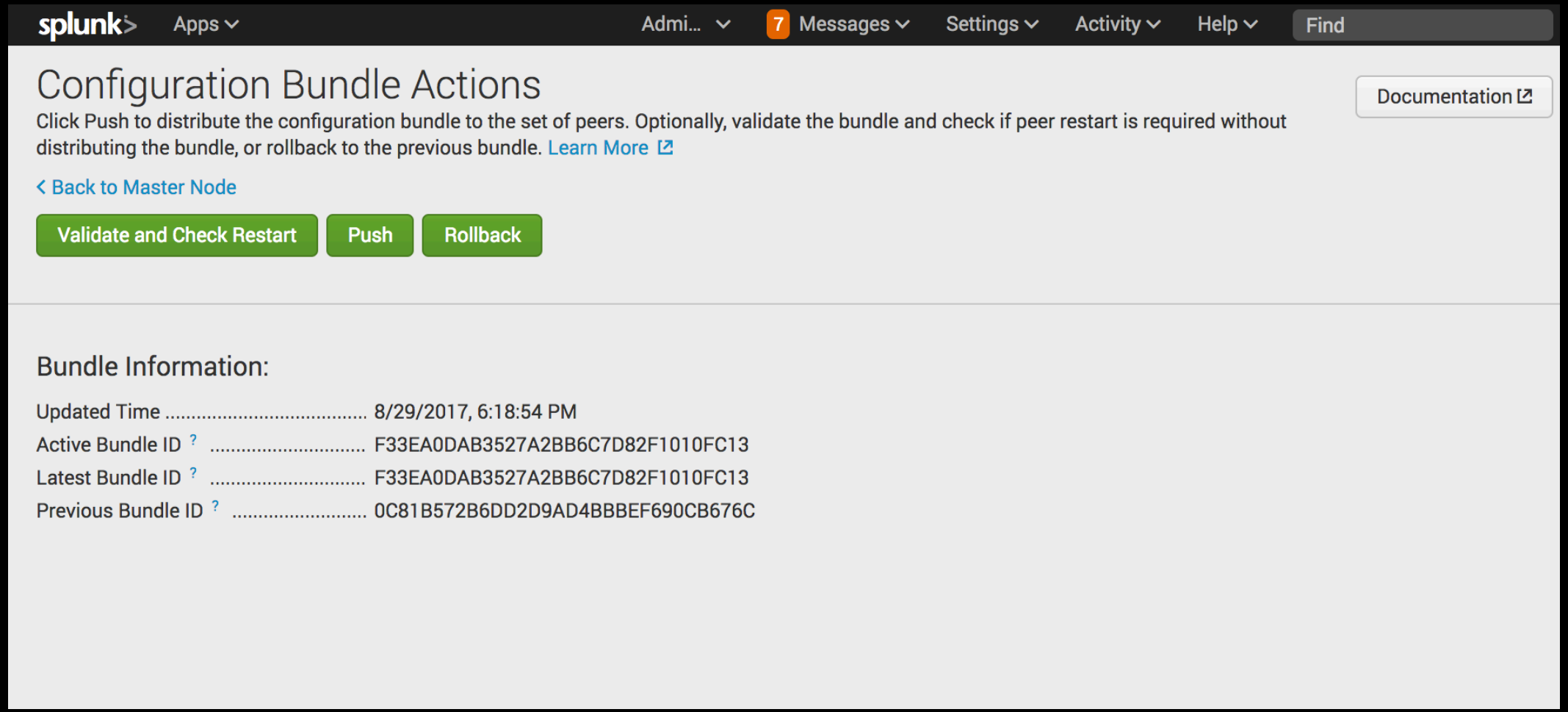


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Configuration Bundle Actions



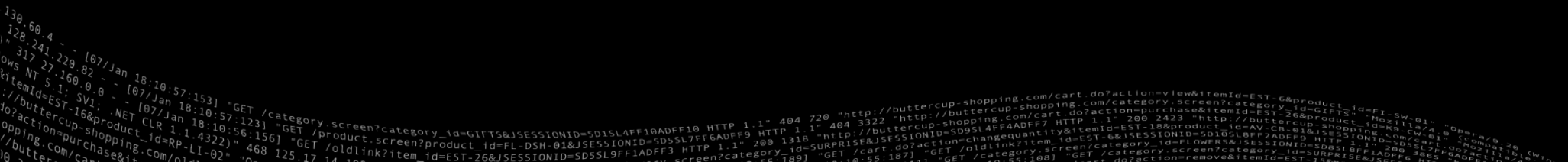
splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Configuration change to effect bundle push

```
kkolla@kkolla-HP:~/Work/instances/master/etc/master-apps/_cluster/local$ cat inputs.conf
[splunktcp://13452]
disabled=0
kkolla@kkolla-HP:~/Work/instances/master/etc/master-apps/_cluster/local$
```

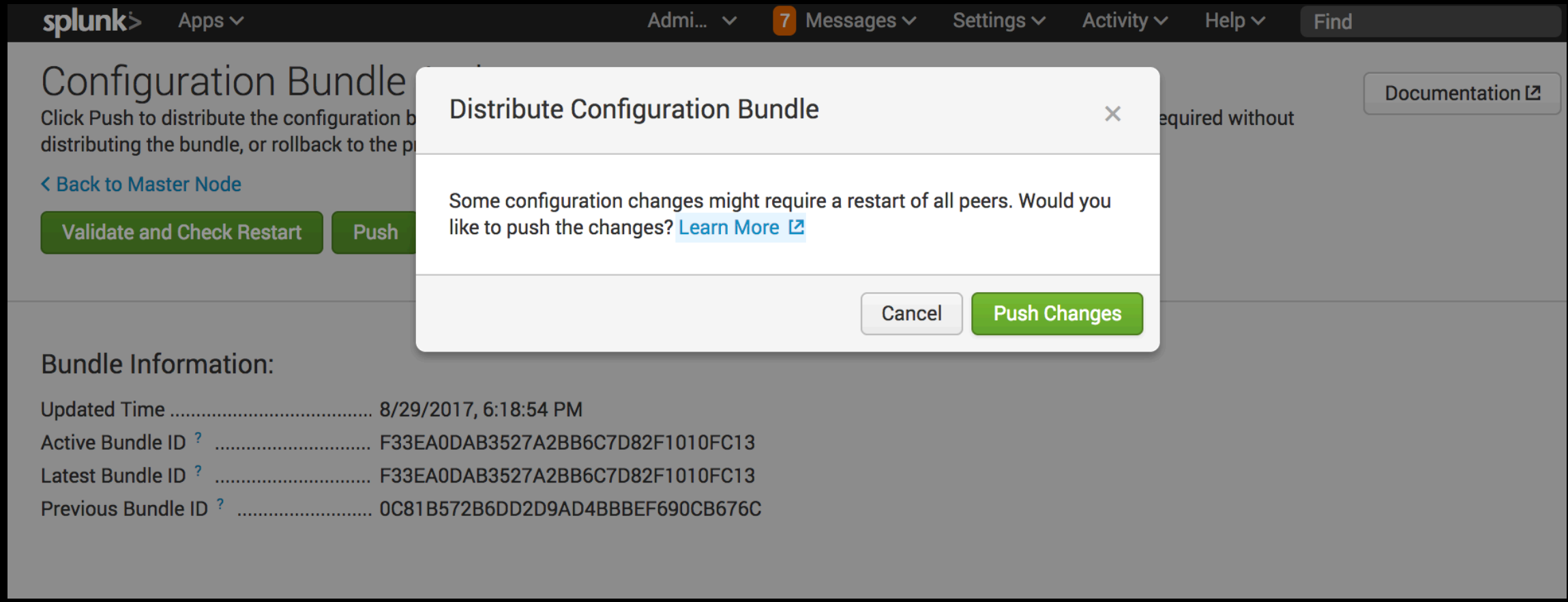


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Bundle Push from the UI

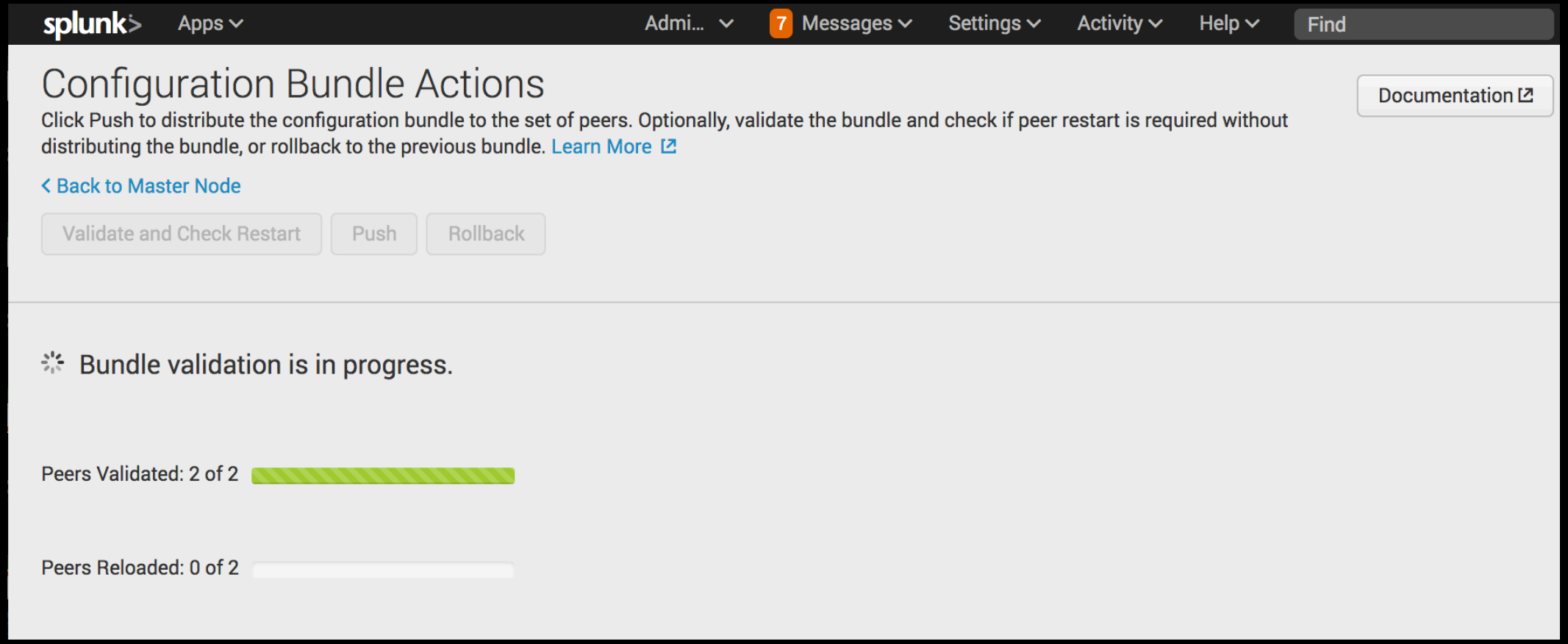


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Bundle Push from the UI - Stages

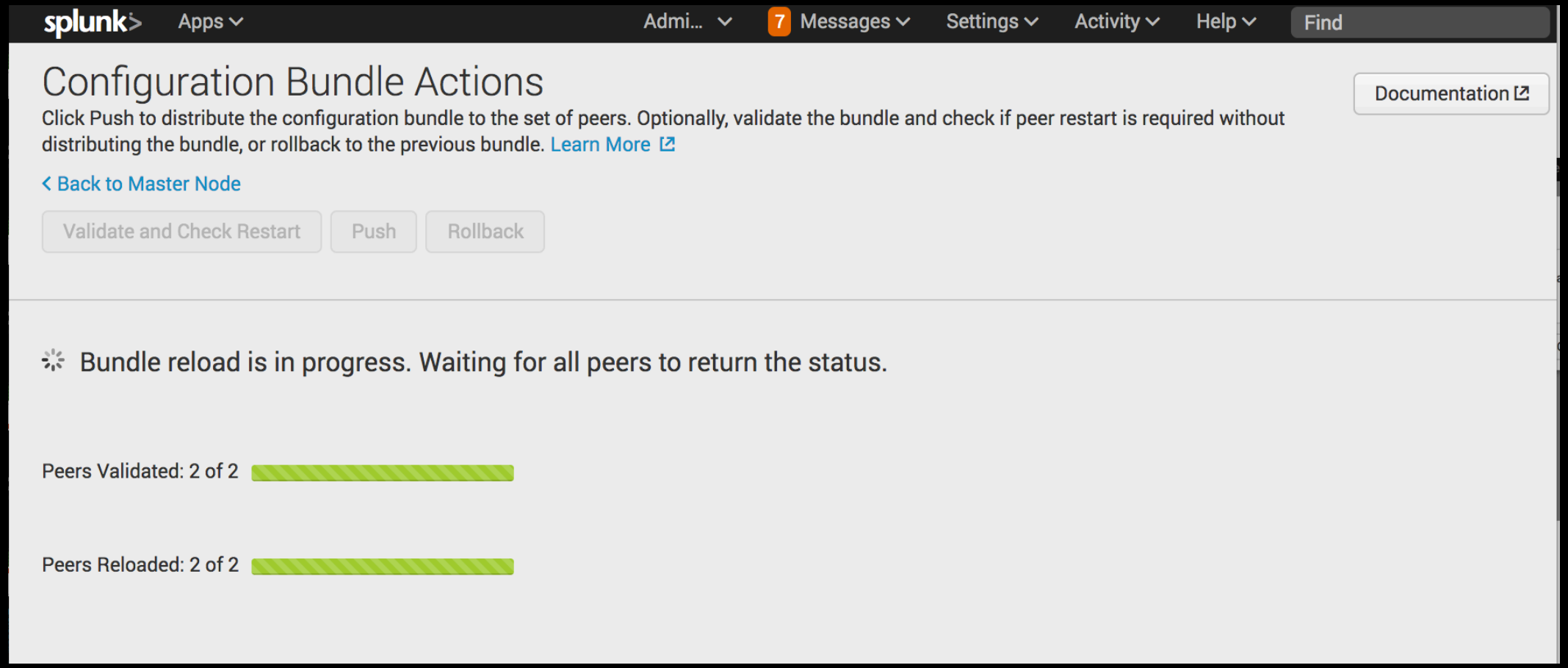


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Bundle Push from the UI - Stages

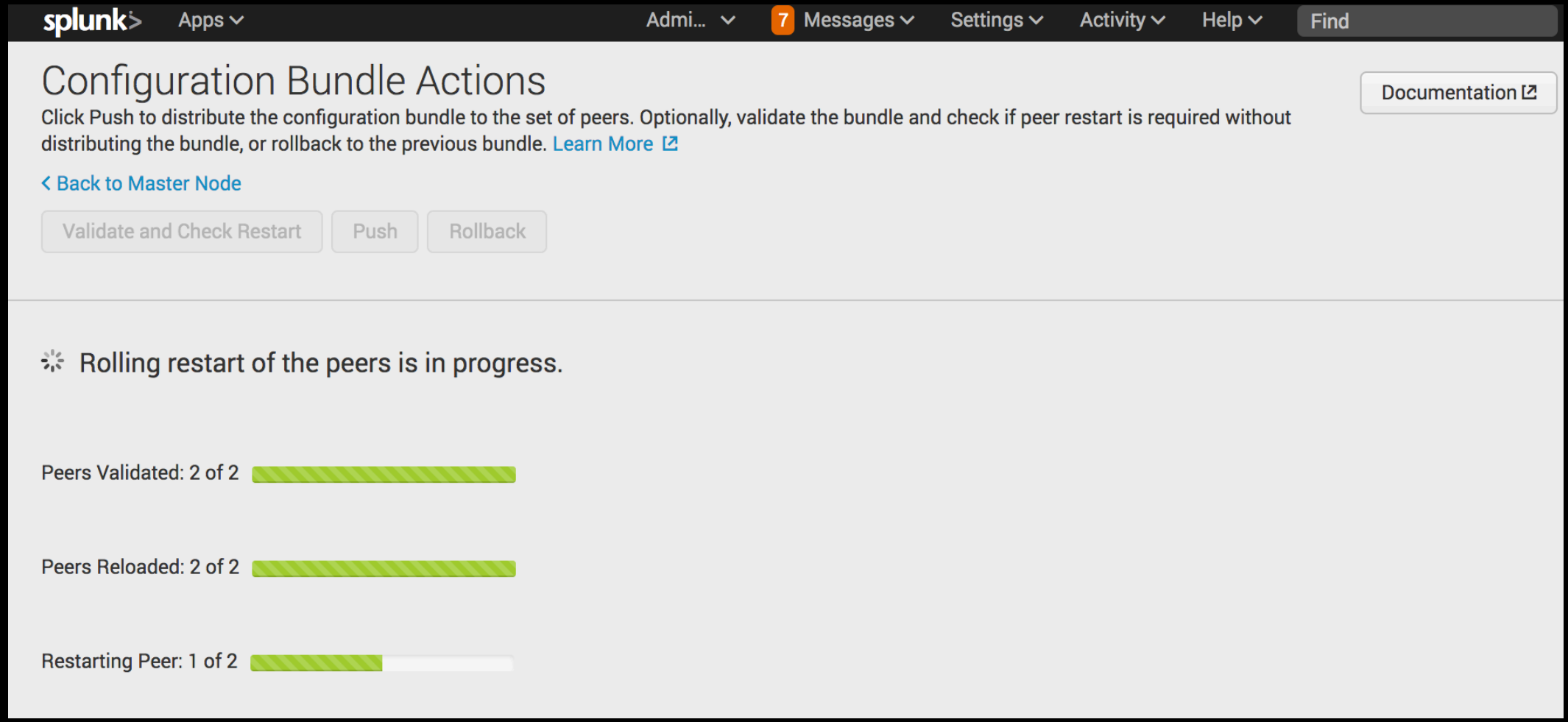


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Bundle Push from the UI - Stages

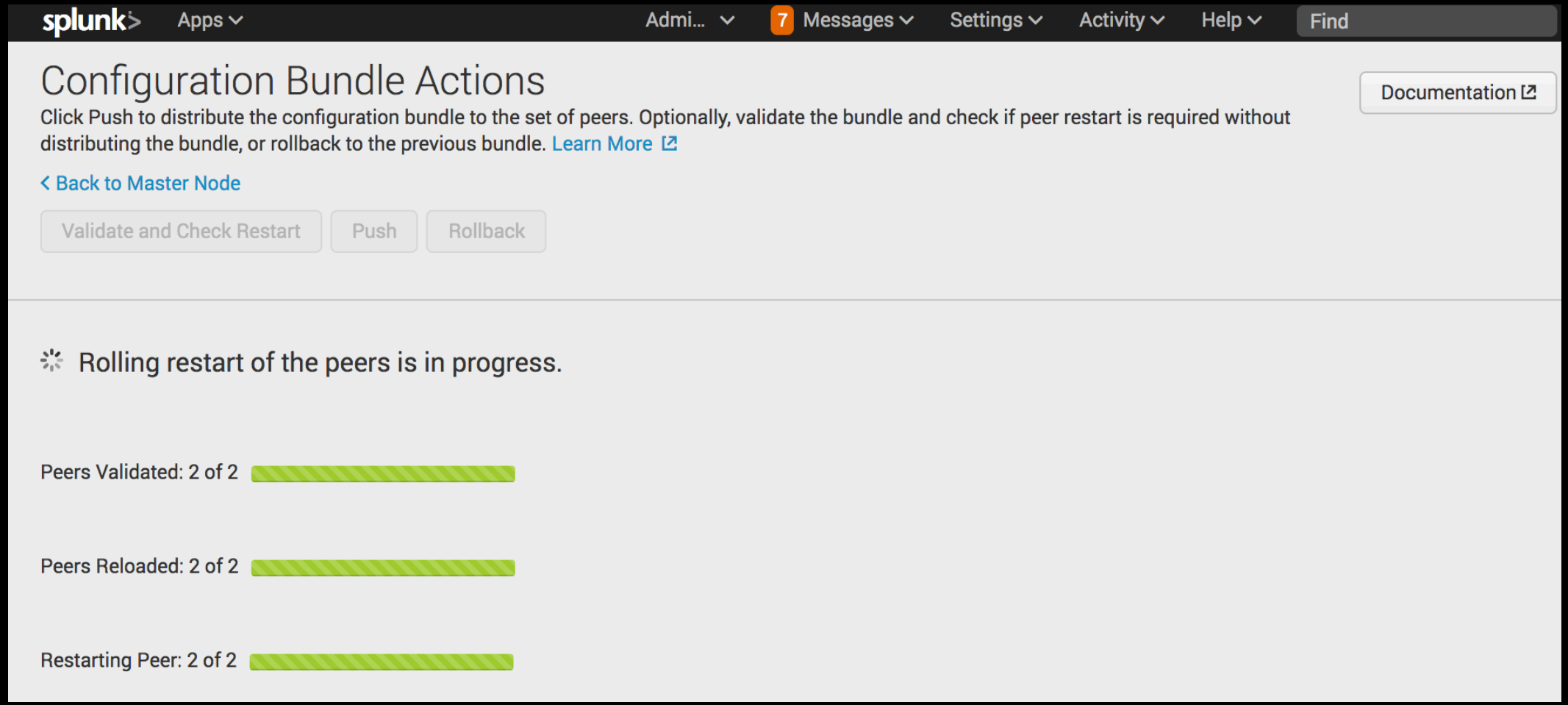


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Bundle Push from the UI - Stages

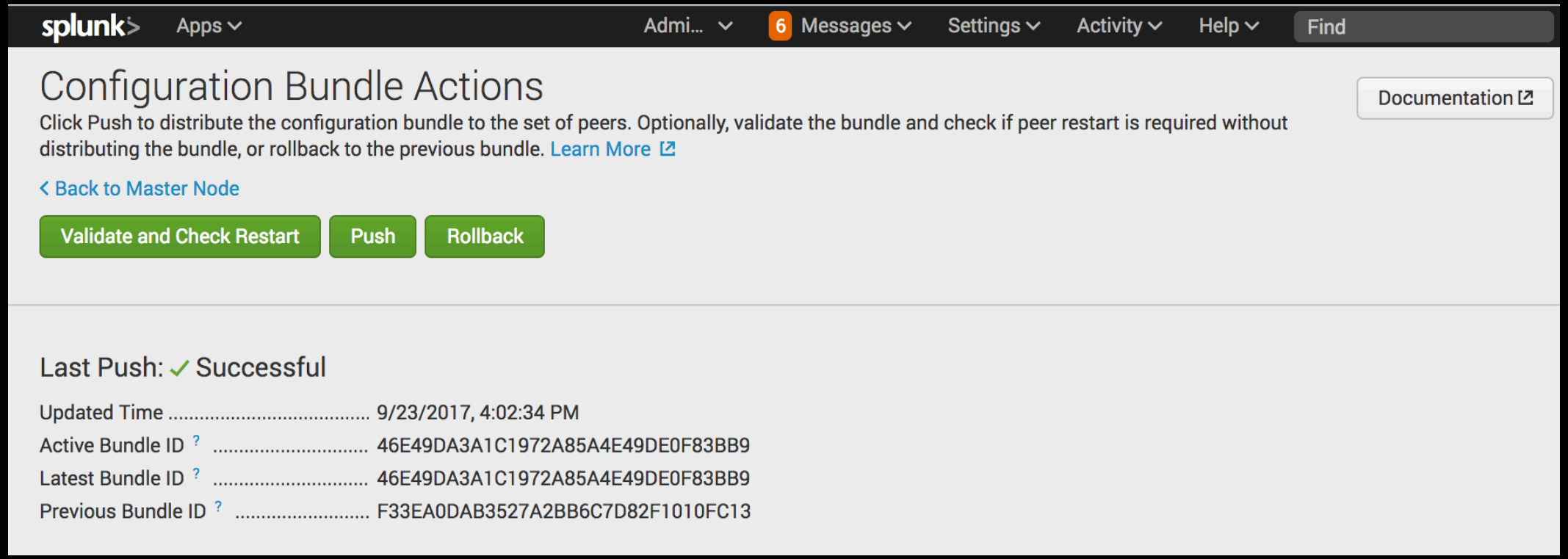


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Bundle Push from the UI - Complete

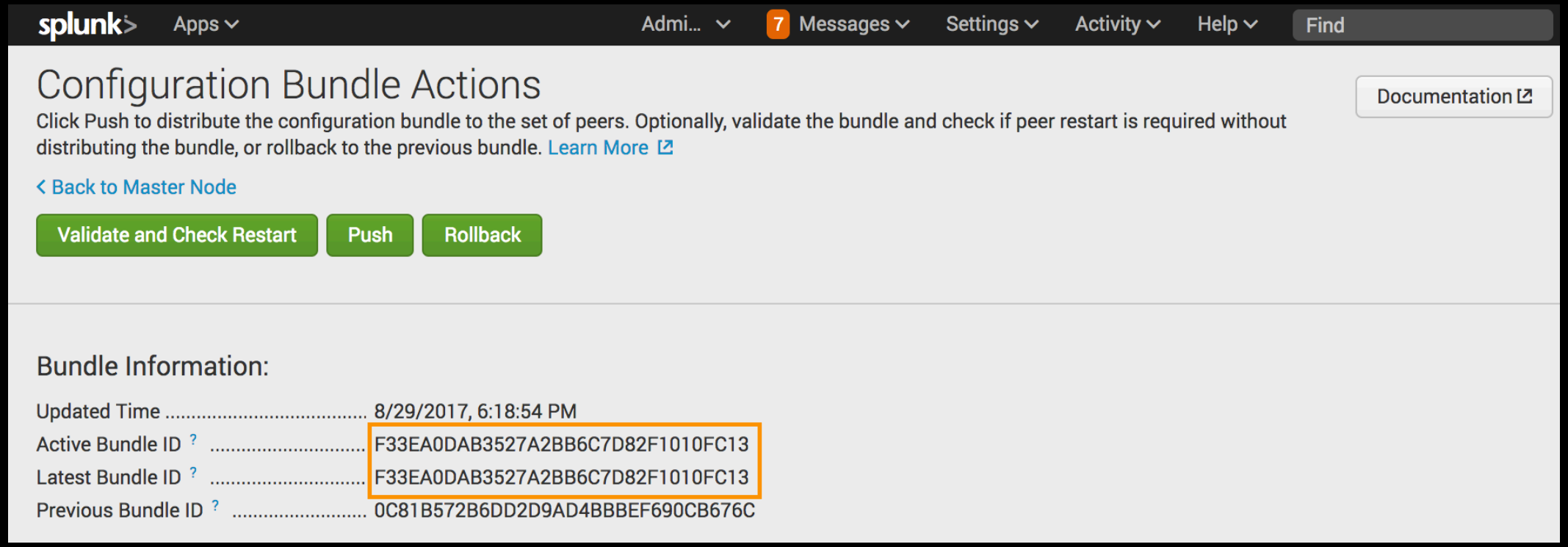


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

UI – Before Bundle Push

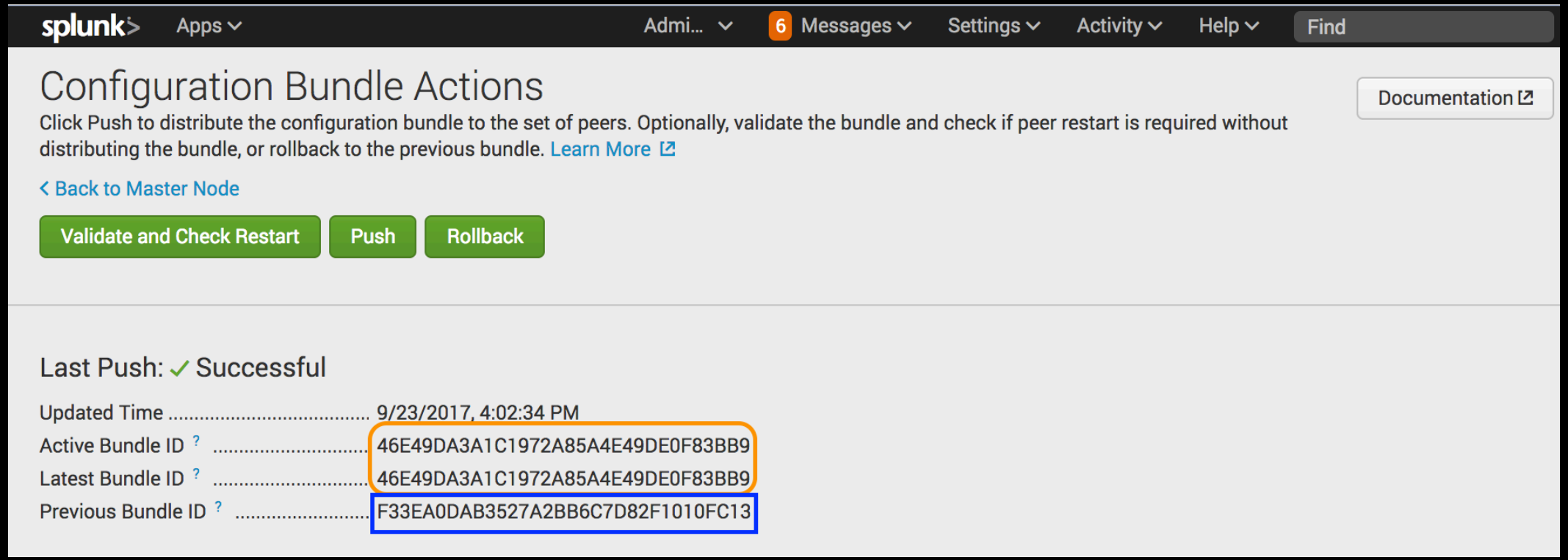


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

UI – After Bundle Push

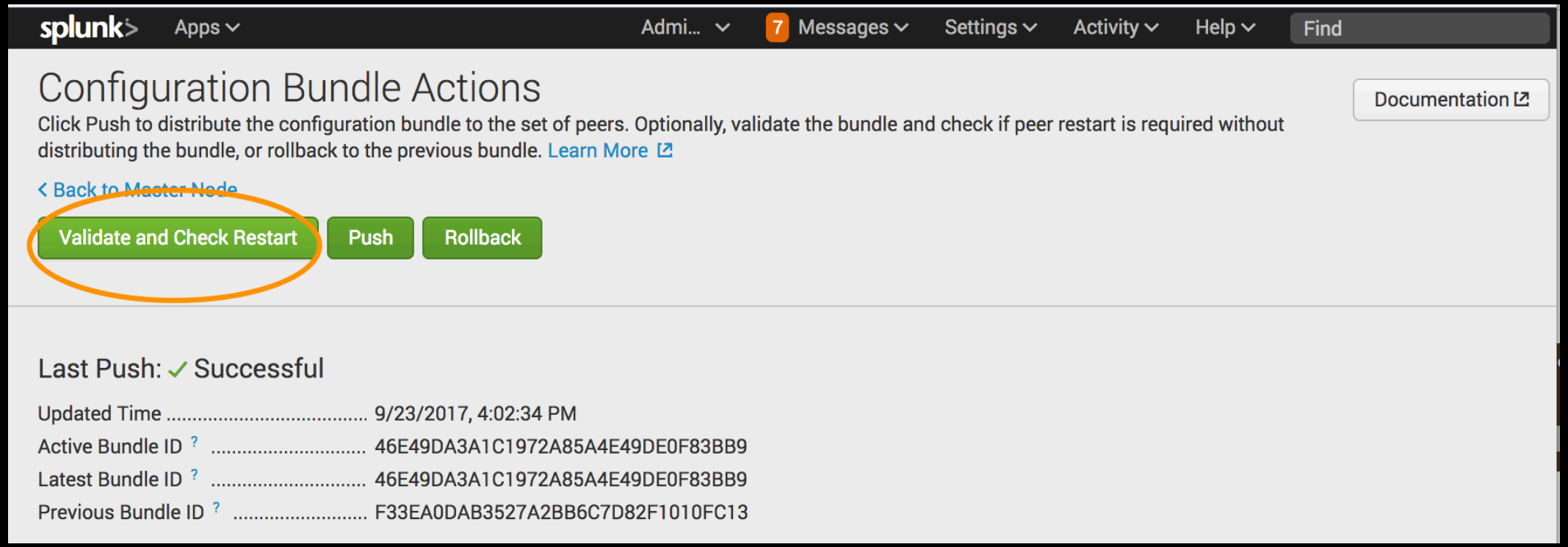


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

UI – Validate and Check Restart



splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Configuration change to effect bundle Check Restart

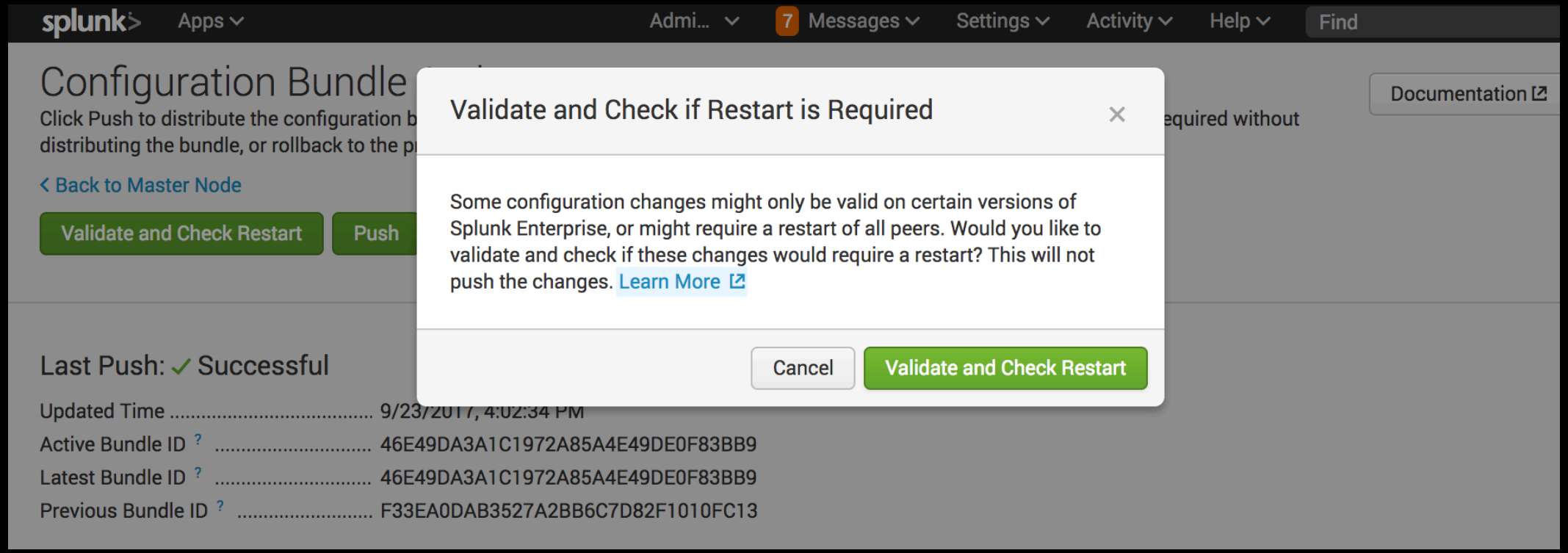
```
kkolla@kkolla-HP:~/Work/instances/master/etc/master-apps/_cluster/local$ cat inputs.conf
[splunktcp://33452]
disabled=0
kkolla@kkolla-HP:~/Work/instances/master/etc/master-apps/_cluster/local$
```

splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Validate and Check Restart from the UI

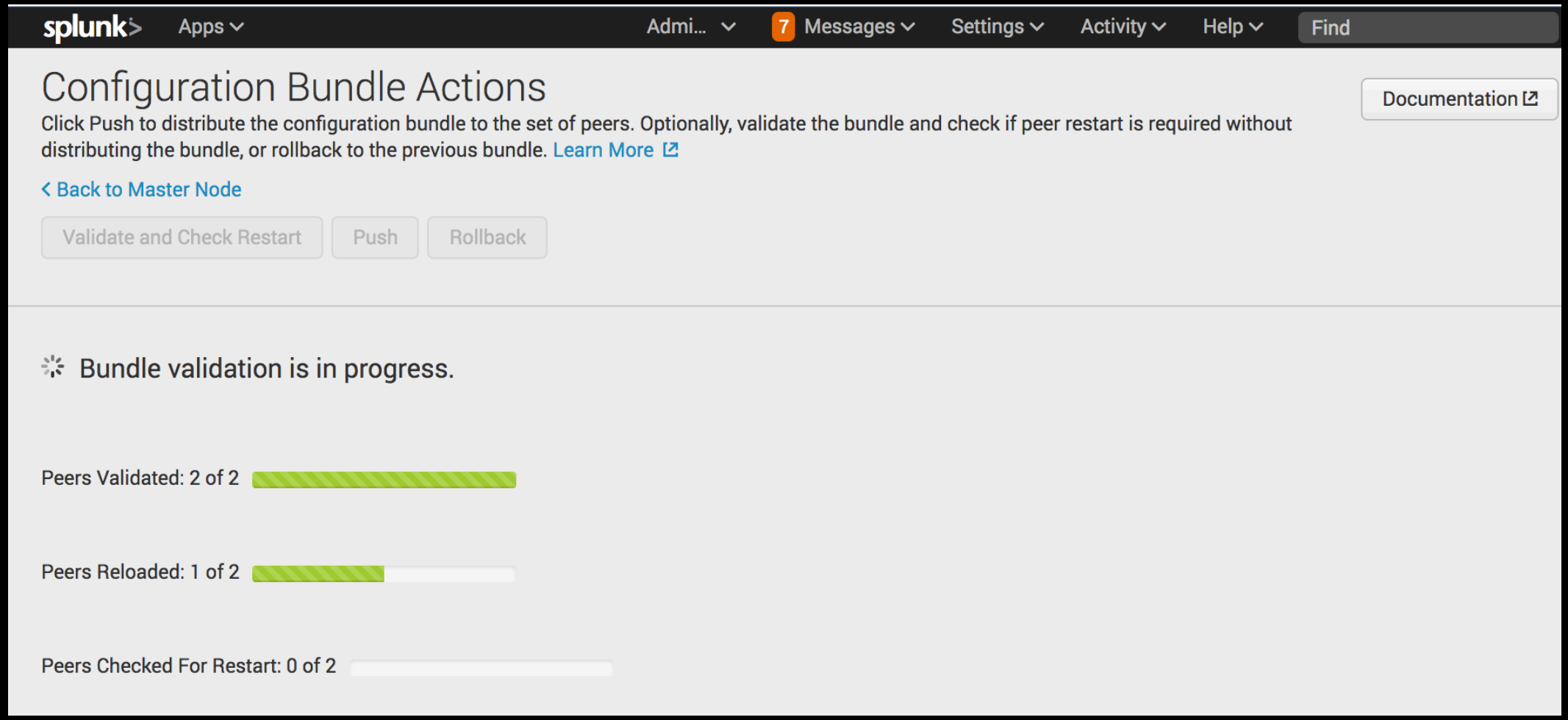


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Validate and Check Restart from the UI

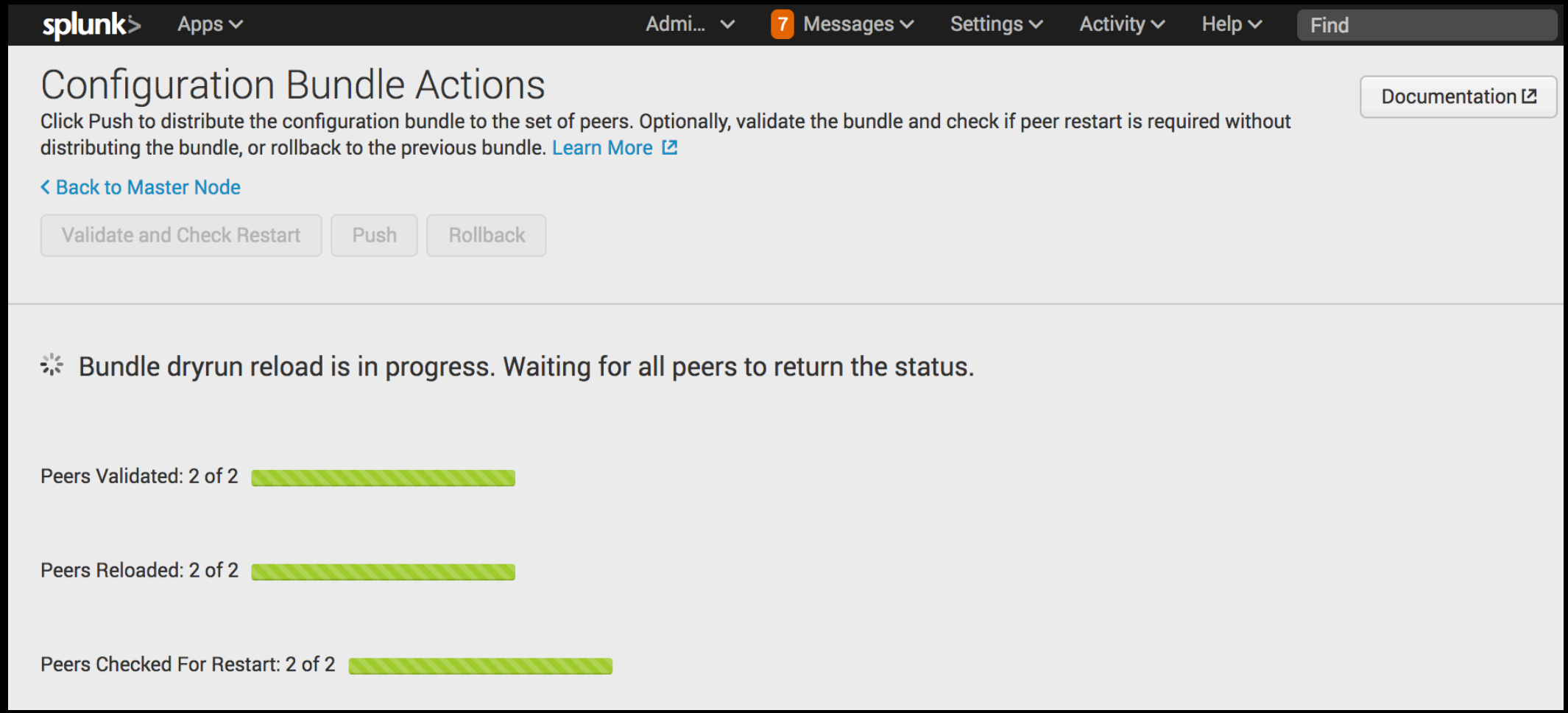


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Validate and Check Restart from the UI

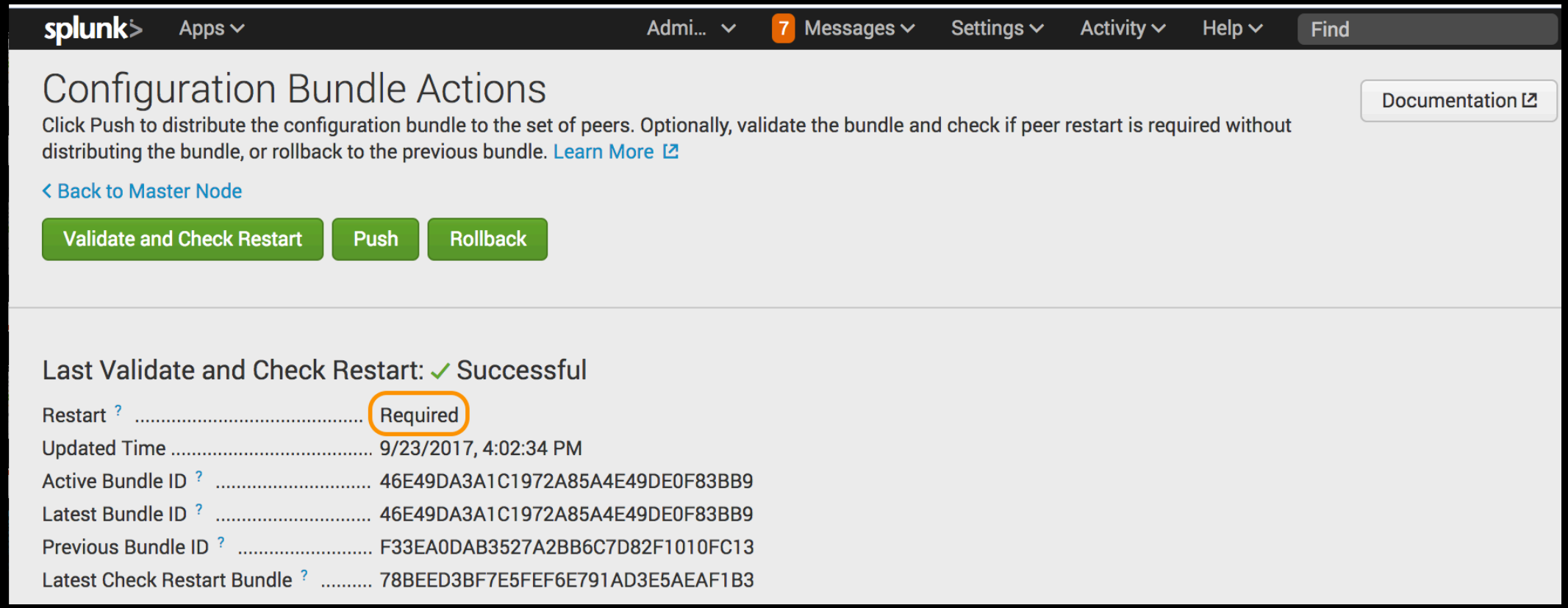


splunk> .conf2017

© 2017 SPLUNK INC.

Bundle Operations

Validate and Check Restart from the UI



splunk> .conf2017

© 2017 SPLUNK INC.

Troubleshooting and Best Practices

Pushing Configuration Bundles in an Indexer Cluster

splunk> .conf2017

© 2017 SPLUNK INC.

Apply Bundle

Cluster Master – splunkd.log

```
INFO  CMBundleMgr - apply bundle status transitioning from='None', to='Bundle Creation is in progress.

INFO  CMMaster - Creating a new bundle on the master.

INFO CMBundleMgr - apply bundle status transitioning from='None', to='Bundle validation is in progress.'

INFO  CMMaster - Bundle validation is in progress for peers=8A0E551F-227C-48DC-9018-515A63F971E8,F78272B2-24DC-43BD-A402-A101123F2B4F.

Bundle validation success reported by [F78272B2-24DC-43BD-A402-A101123F2B4F peer_name=peer1] successful for bundleid=1E704E11131BC274111CD8991E0DE621

INFO  CMPeer - Bundle validation success reported by [8A0E551F-227C-48DC-9018-515A63F971E8 peer_name=peer2] successful for bundleid=1E704E11131BC274111CD8991E0DE621
```

splunk> .conf2017

© 2017 SPLUNK INC.

Apply Bundle

Cluster Master – splunkd.log

```
INFO  CMBundleMgr - apply bundle status transitioning from='Bundle validation is in progress.', to='Bundle reload is in progress. Waiting for all peers to return the status.'

INFO  CMMaster - Peers have indicated they are reload capable, issuing bundle reload.

INFO  CMPeer - Bundle reload status peer=8A0E551F-227C-48DC-9018-515A63F971E8 peer_name=peer2 restart_required=1 rolling_restart=1 dryrun=0 reasons=[One or more configs require a restart to take effect. Configs=inputs]

INFO  CMPeer - Bundle reload status peer=F78272B2-24DC-43BD-A402-A101123F2B4F peer_name=peer1 restart_required=1 rolling_restart=1 dryrun=0 reasons=[One or more configs require a restart to take effect. Configs=inputs]

INFO  CMMaster - Restart required to apply the bundle.

INFO  CMBundleMgr - apply bundle status transitioning from='Bundle reload is in progress. Waiting for all peers to return the status.', to='Rolling restart of the peers is in progress.'

INFO  CMMaster - Starting a rolling restart of the peers.
```

splunk> .conf2017

© 2017 SPLUNK INC.

Apply Bundle

Viewing the cluster bundle

- $ ./bin/splunk show cluster-bundle-status

```
17:03 $ splunk show cluster-bundle-status

master
        cluster_status=None
        active_bundle
               checksum=ED4C6043FBF5345DBDCD3DD304636F9C
               timestamp=1501714888 (in localtime=Wed Aug  2 16:01:28 2017)
        latest_bundle
               checksum=ED4C6043FBF5345DBDCD3DD304636F9C
               timestamp=1501714888 (in localtime=Wed Aug  2 16:01:28 2017)
        last_validated_bundle
               checksum=ED4C6043FBF5345DBDCD3DD304636F9C
               last_validation_succeeded=1
               timestamp=1501714888 (in localtime=Wed Aug  2 16:01:28 2017)

 peer2   8A0E551F-227C-48DC-9018-515A63F971E8    default
        active_bundle=ED4C6043FBF5345DBDCD3DD304636F9C
        latest_bundle=ED4C6043FBF5345DBDCD3DD304636F9C
        last_validated_bundle=ED4C6043FBF5345DBDCD3DD304636F9C
        last_bundle_validation_status=success
        restart_required_apply_bundle=0
        status=Up
```

splunk> .conf2017

© 2017 SPLUNK INC.

Check Restart

Cluster Master – splunkd.log

```
INFO  CMMaster - Changing the dryrun bundle on the master,
dryrun='815D4F439CA468F282164B7E456154E7'.

CMBundleMgr - apply bundle status transitioning from='None', to='Bundle validation is in
progress.'

CMMaster - Tracking bundle validation status for peers=F78272B2-24DC-43BD-A402-
A101123F2B4F,8A0E551F-227C-48DC-9018-515A63F971E8

INFO  CMPeer - Bundle validation success reported by [F78272B2-24DC-43BD-A402-
A101123F2B4F peer_name=peer1] successful for bundleid=815D4F439CA468F282164B7E456154E7

INFO  CMPeer - Bundle validation success reported by [8A0E551F-227C-48DC-9018-
515A63F971E8 peer_name=peer2] successful for bundleid=815D4F439CA468F282164B7E456154E7

INFO  CMMaster - CMMaster issuing a dry run of bundle push
```

splunk> .conf2017

© 2017 SPLUNK INC.

Check Restart

Cluster Master – splunkd.log

```
INFO  CMBundleMgr - apply bundle status
transitioning from='Bundle validation is
in progress.', to='Bundle dryrun reload
is in progress. Waiting for all peers to
return the status.'


INFO  CMMaster - Dry Run Complete
```

```
16:58 $ splunk show cluster-bundle-status

master
        cluster_status=None
        active_bundle
               checksum=1E704E11131BC274111CD8991E0DE621
               timestamp=1501715122 (in localtime=Wed Aug  2 16:05:22 2017)
        latest_bundle
               checksum=1E704E11131BC274111CD8991E0DE621
               timestamp=1501715122 (in localtime=Wed Aug  2 16:05:22 2017)
        last_validated_bundle
               checksum=815D4F439CA468F282164B7E456154E7
               last_validation_succeeded=1
               timestamp=1501716951 (in localtime=Wed Aug  2 16:35:51 2017)

 peer2  8A0E551F-227C-48DC-9018-515A63F971E8    default
        active_bundle=1E704E11131BC274111CD8991E0DE621
        latest_bundle=1E704E11131BC274111CD8991E0DE621
        last_validated_bundle=815D4F439CA468F282164B7E456154E7
        last_bundle_validation_status=success
        last_bundle_checked_for_restart=815D4F439CA468F282164B7E456154E7
        last_check_restart_result=restart required
        restart_required_apply_bundle=0
        status=Up
```

splunk> .conf2017

© 2017 SPLUNK INC.

Rollback

Cluster Master – splunkd.log

```
INFO  CMBundleMgr - apply bundle status transitioning from='None', to='Bundle Creation is in progress.'

INFO  CMMaster - Initiating rollback bundle process

INFO  CMBundleMgr - Rolling back bundle on the master to previousActive bundle=ED4C6043FBF5345DBDCD3DD304636F9C previousActive bundlePath=/Users/kkolla/Work/instances/master/var/run/splunk/cluster/remote-bundle/971e64c31b6bbb0c0e7479cf500e0647-1501714888.bundle

CMMaster - Tracking bundle validation status for peers=F78272B2-24DC-43BD-A402-A101123F2B4F,8A0E551F-227C-48DC-9018-515A63F971E8

INFO  CMBundleMgr - setting previousActive bundle=ED4C6043FBF5345DBDCD3DD304636F9C to active bundle=1E704E11131BC274111CD8991E0DE621

INFO  CMMaster - Peers have indicated they are reload capable, issuing bundle reload.

INFO  CMMaster - Starting a rolling restart of the peers.
```

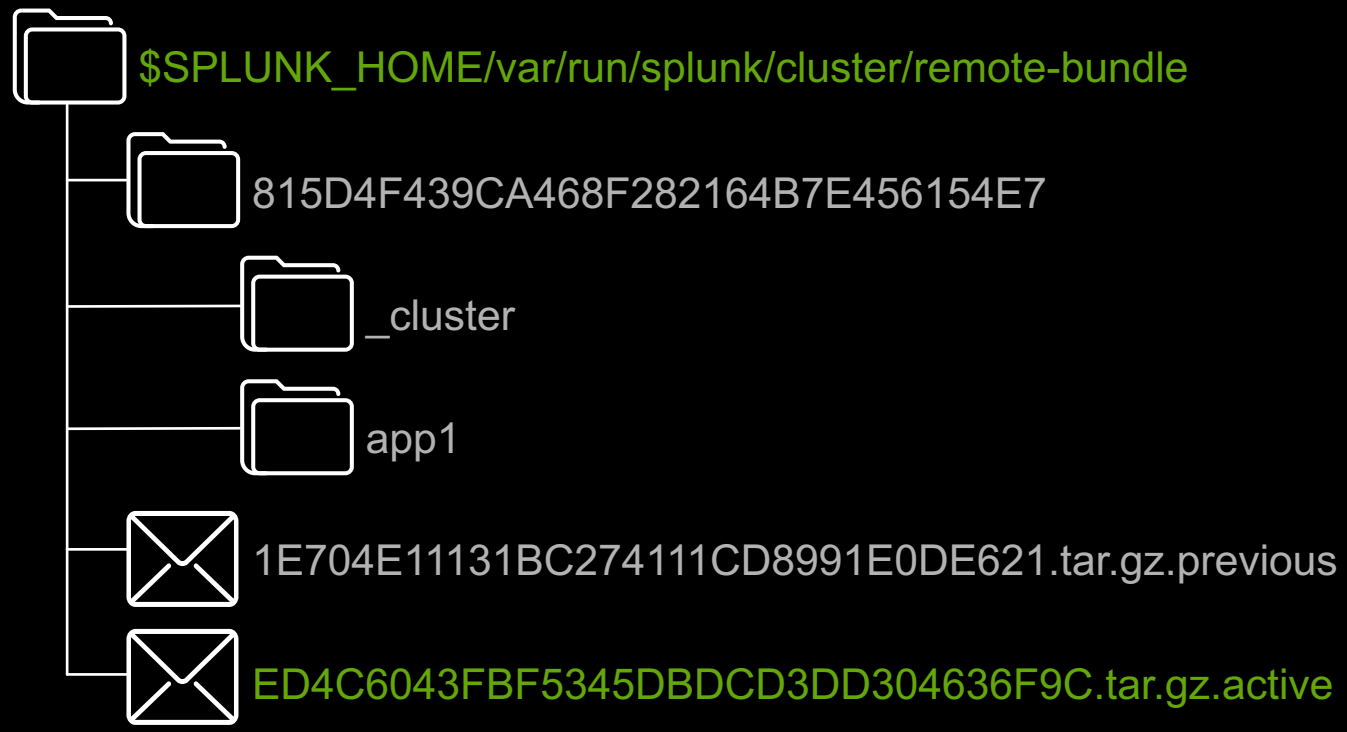
splunk> .conf2017

© 2017 SPLUNK INC.

Keeping Track of Bundles

which bundle again?

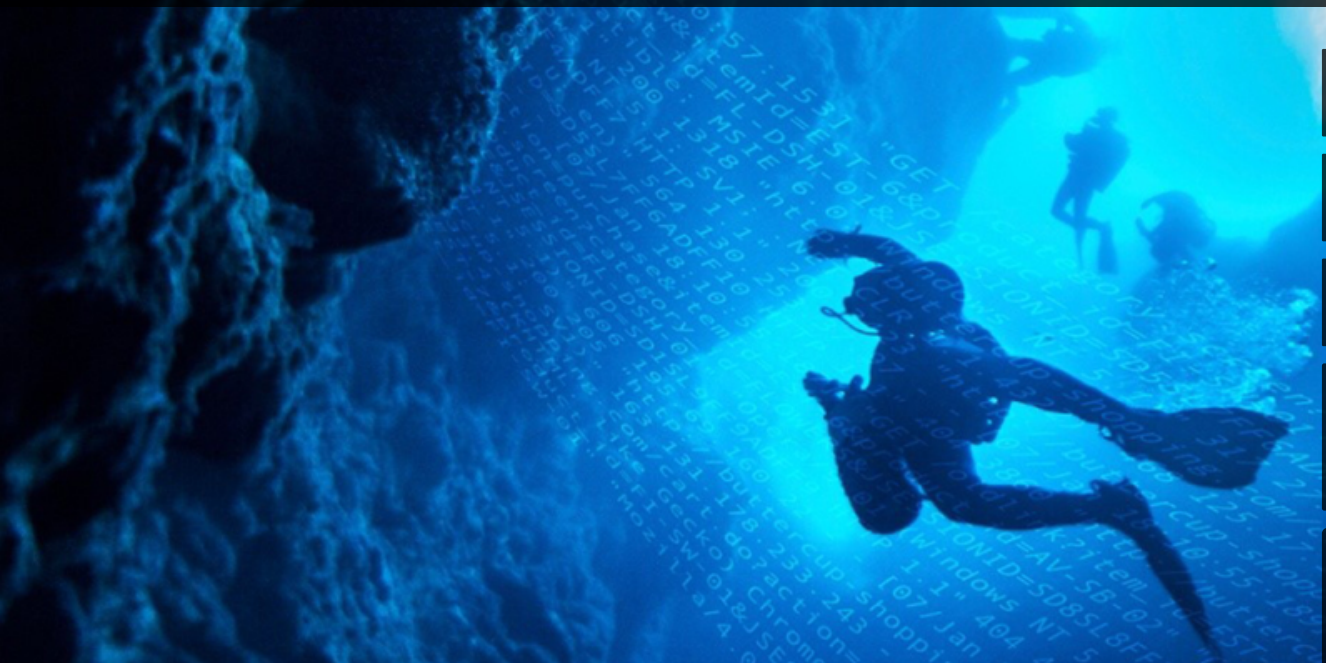
- The bundles folder



splunk> .conf2017

© 2017 SPLUNK INC.

Best Practices



1. Find a reasonable time to do your bundle push
2. Do NOT change slave configurations locally
3. When in doubt, use “—check-restart”
4. Enable phased bundle downloads for large bundles or large clusters

URLs:

https://docs.splunk.com/Documentation/Splunk/6.6.3/Indexer/Managecommonconfigurations

https://docs.splunk.com/Documentation/Splunk/6.6.3/Indexer/Configurationbundleissues

© 2017 SPLUNK INC.

Thank You

Don't forget to rate this session in the .conf2017 mobile app