

Splunk4Admins

Agent Management



Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words "will," "believes," "plans," "anticipates," "expects," "estimates," "strives," "goal," "intends," "may," "endeavors," "continues," "projects," "seeks," or "targets," or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management's beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management's control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk's and Cisco's complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco's current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk's market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco's ability to implement its plans, forecasts and other expectations with respect to Splunk's business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the "Risk Factors" section of Cisco's most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the "Risk Factors" section of Splunk's most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

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. We undertake no 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.

Splunk, Splunk> and Turn Data Into Doing 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.

© 2025 SPLUNK LLC All rights reserved.



Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



Workshop Agenda

- Expectations
- What is an agent?
 - Types
- What is Agent Management?
- App management via Agent Manager?
- Agent Management & Deployment Labs
- Agent Image Lab (Extra Credit)
- Summary

Audience

Who is this Workshop for?

- Splunk Admins
- “Required”: Power User Certified
- “Preferred”: Splunk Admin enabled (at least started ...), Certified

Expectations for Workshop

- Last roughly 60-90 minutes
- Understand the Forwarder types
- Understand how data moves to be searchable
- See and experience managing Forwarders
- Know the ways to install/upgrade Forwarders
- Understand the Deployment Server
- Experience configuring a Deployment Server
- Experience setting up an app and push to a Forwarder
- Experience creating and leveraging a universal forwarder tarball image
- Experience using an intermediate forwarder



REGISTRATION



5 MINS

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://splunk.show/<uniqueID>>
3. Download the hands-on lab guide:
<https://splk.it/S4A-AM-Lab-Guide>

Contains step-by-step instructions
for all of today's exercises!

4. Download a copy of today's slide deck.
<https://splk.it/S4A-AM-Attendee>

Goal



PLATFORM

Splunk4Admins - Agent Management

⌚ 10/12 12:52 - 10/12 19:52

💻 Enterprise

📅 Splunk4Admins - Forwarder M...

🕒 STARTING SOON

Actions ▾

+ Enroll event

Enroll in today's event

Workshop Agenda

- Expectations
- What is an agent?
 - Types
- What is Agent Management?
- App management via Agent Manager?
- Agent Management & Deployment Labs
- Agent Image Lab (Extra Credit)
- Summary

Splunk Components and Processes (RECAP)

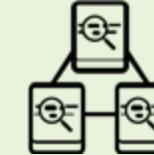
- Allow users to submit search requests using SPL
- Distribute search requests to the indexers
- Consolidate results and render visualizations of results
- Store search-time knowledge objects (such as field extractions, alerts, and dashboards)

- Receive incoming data from forwarders
- Index and store data in Splunk indexes
- Search data in response to requests from search heads

- Monitor configured inputs and forward the data to the indexers (best practice data collection method)
- Requires minimal resources and typically installed on the machines that produce the data

- Centralizes configuration management for various functions including clustering, licensing, and clients
- Requires systems running Splunk Enterprise

Search Tier



Search Head Cluster

Indexing Tier



Indexer Cluster

Collection Tier



Universal
Forwarders

Heavy
Forwarders

Other
Inputs

Management

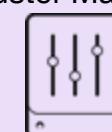
License Master



Monitor Console



Cluster Manager



SHC - Deployer



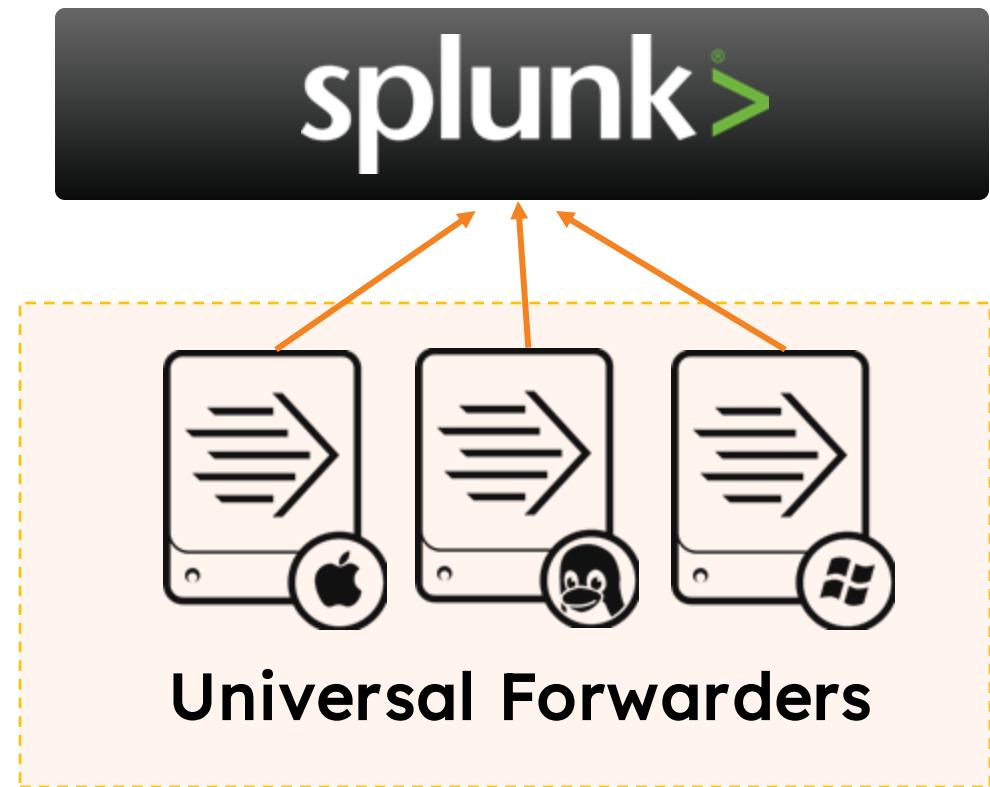
Agent Manager



Review: Universal Forwarders



- Gathers data from a host
- Sends data over network to receiving ports on receivers (usually an indexer)
- Provided as separate installation binary with a built-in license (no limits)
- Designed to run on production servers (minimal CPU / memory use, bandwidth constrained to 256 Kbps by default, no web interface, cannot search or index)

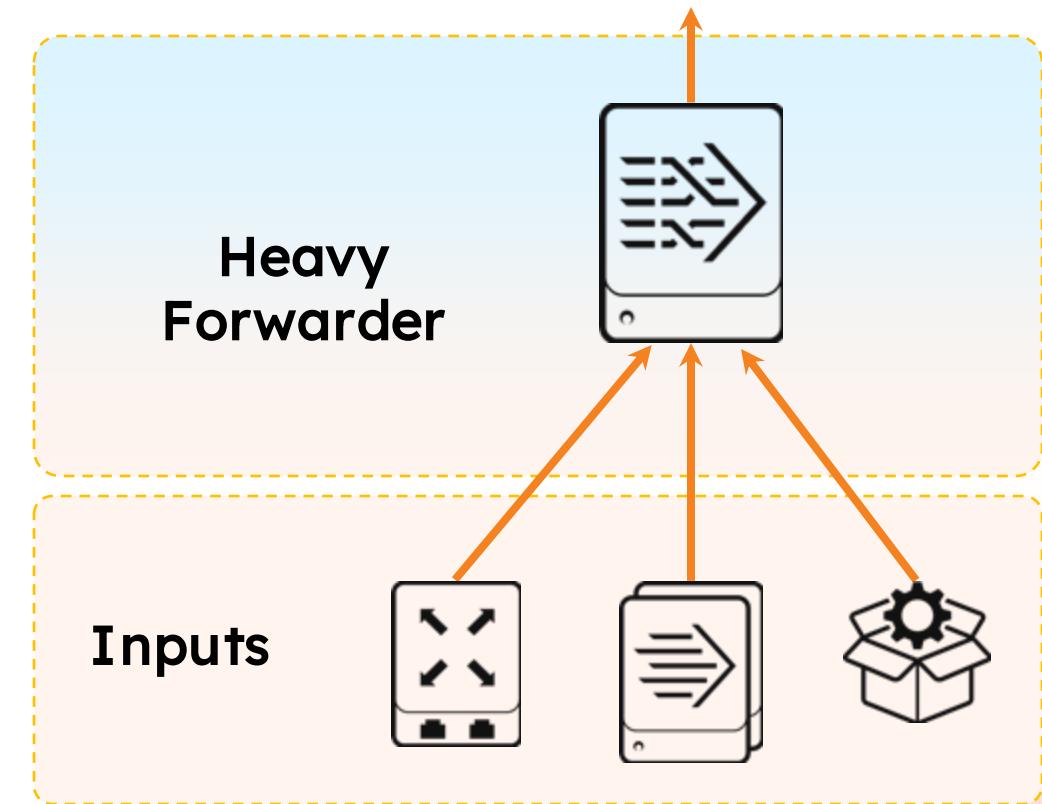


Review: Heavy Forwarders

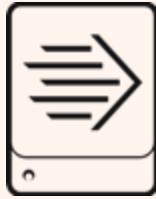


- Splunk Enterprise instance with the Forwarder License enabled
- Can parse data before forwarding it
- Can route data based on event criteria to different indexers or 3rd party receivers
- Supports complex use cases
- Cannot perform distributed searches

splunk>



Deciding Between UF and HF



Universal Forwarder



- Ideal for most circumstances, including collecting files or as intermediate forwarder
- Minimal footprint on production servers
- Generally requires less bandwidth and has faster processing than same data on HF
- Supports simple routing or cloning data to separate indexers
- Does not support filtering based on regular expressions*

* Except for Windows Event Logs on Windows

Heavy Forwarder

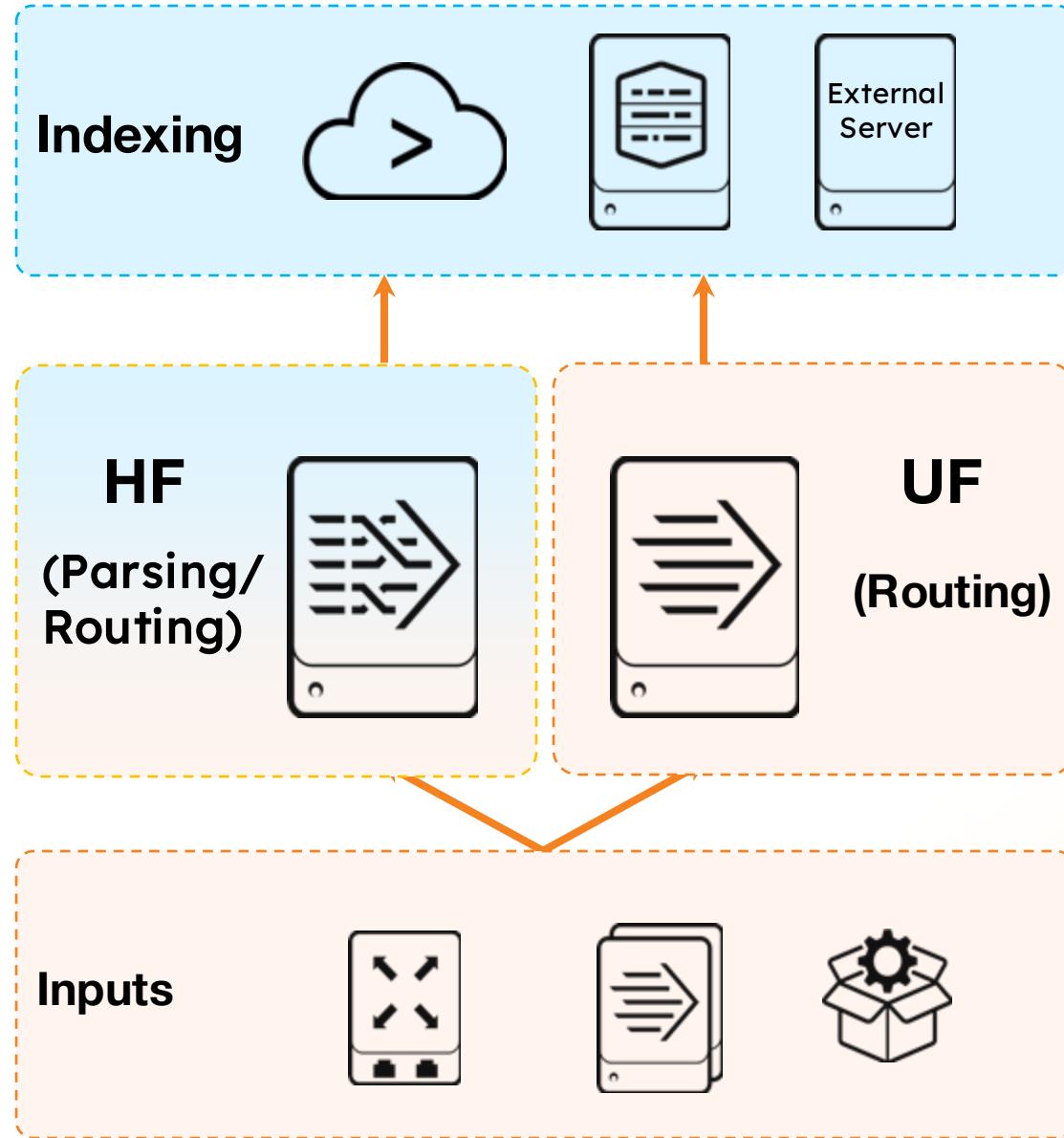


- Generally runs on dedicated servers
- Required by some apps, add-ons, or input types (such as HEC, DBconnect)
- Supports complex, event-level routing and filtering
- Can anonymize or mask data before forwarding to an indexer
- Provides Splunk Web and predictable version of Python, if needed
- May increase network traffic

Review: Intermediate Forwarders



- Often Heavy Forwarders
- Route data from inputs to indexers or other intermediate forwarders
- Can reduce or limit bandwidth on specific network segments
- Can limit security concerns (DMZ, firewalls)
- Can parse, filter or index data if a HF



Comparing Intermediate Forwarders

Universal Forwarders

- Smallest resource footprint
- Efficient network utilization profile
- Cannot process time zones (run all on UTC)

Heavy Forwarders

- Can parse and route data
- Can process time zones
- More network bandwidth
- More system resources
- Usually affected by blocking - not utilizing the indexing performance in Splunk Cloud for index time parsing

Agent Deployment Best Practices

- Update firewall rules to allow outbound connections on port 9997
- Secure data using SSL (default using Splunk Cloud)
- Use direct communication between forwarders and indexers
 - If not possible, use a combination of intermediate UFs and HFs
 - Maintain a minimum Forwarder:Indexer ratio of 2:1

> Best Practice

UF Best Practices: Improve Load Balancing

- Configure event breaker per sourcetype on UF
 - Controls how the forwarders package and send the data to receivers
 - Distributes data more evenly for indexers in a load-balanced target group
 - Can be enabled for any source type
 - Works with any kind of load balancing setup
 - Configured as `EVENT_BREAKER_ENABLE` and `EVENT_BREAKER` in `props.conf`
 - Single line event example:

```
[my_syslog]
EVENT_BREAKER_ENABLE = true
```

- Multi-line event example:

```
[my_log4j]
EVENT_BREAKER_ENABLE = true
EVENT_BREAKER = ([\r\n]+)\d\d\d\d-\d\d-
```

Installing a Universal Forwarder

	*NIX	Windows
Download	www.splunk.com/en_us/download/universal-forwarder.html	
Install	<ul style="list-style-type: none">• Un-compress .tgz, .rpm, or .deb file in the path Splunk will run from• Default SPLUNK_HOME is: <code>/opt/splunkforwarder</code>	<ul style="list-style-type: none">• Execute .msi installer (or use the CLI)• Default SPLUNK_HOME is: <code>C:\Program Files\SplunkUniversalForwarder</code>

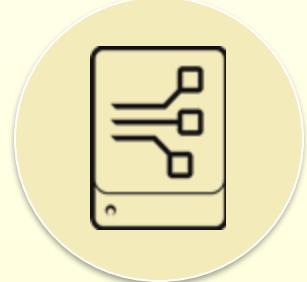
- Silent installation methods exist on all platforms
- Same splunk command-line interface in **SPLUNK_HOME/bin**
 - Same commands for start/stop, restart, etc.
 - An admin account and password are required

Install Linux UF	https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Installanixuniversalforwarder
Install Windows UF	https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/InstallaWindowsuniversalforwarderfromthecommandline

Workshop Agenda

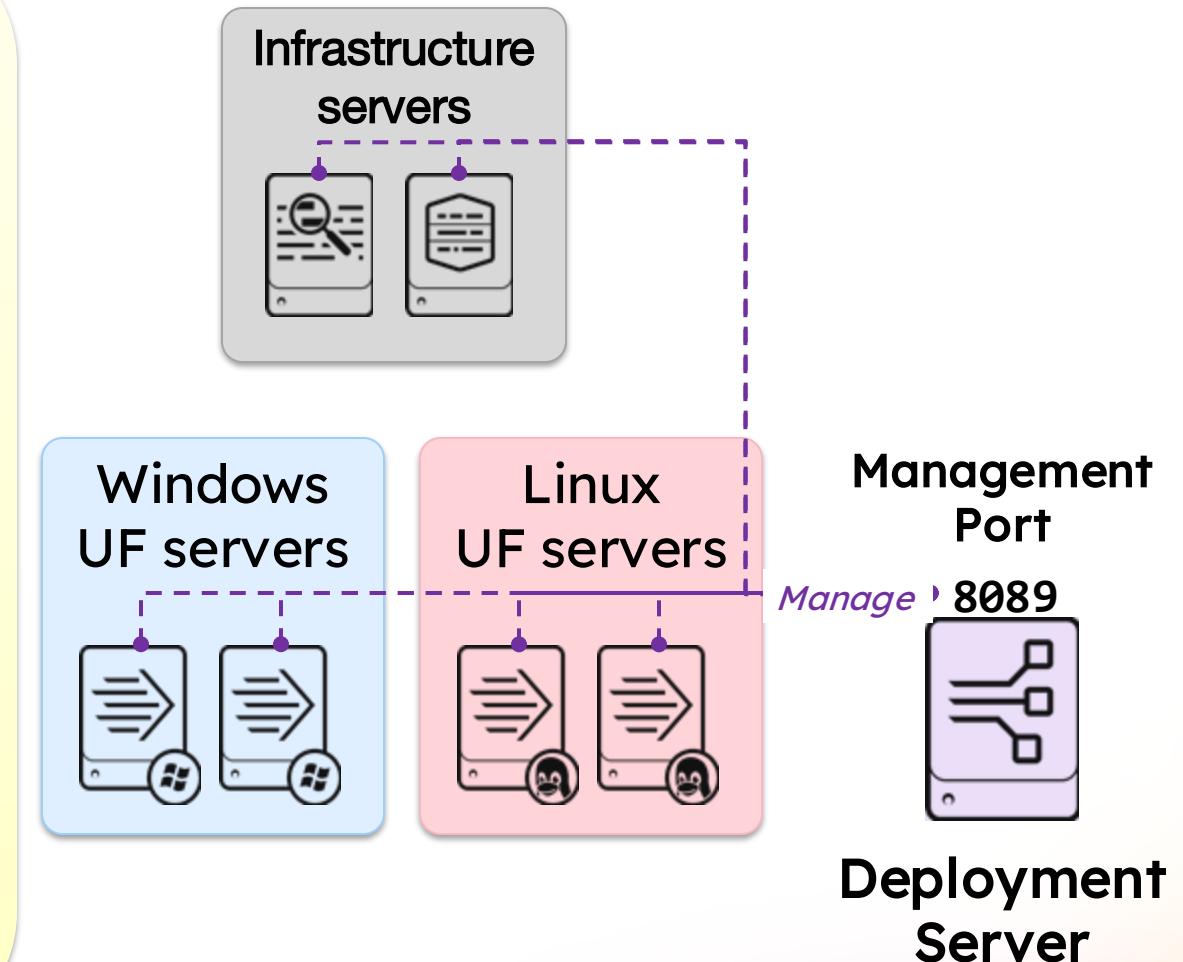
- Expectations
- What is an agent?
 - Types
- **What is Agent Management?**
- App management via Agent Manager?
- Agent Management & Deployment Labs
- Agent Image Lab (Extra Credit)
- Summary

Understanding the Deployment Server



Deployment Server (DS)

- Built-in tool for centrally managing configuration packages as apps for clients
- Includes Forwarder Management as the graphical user interface
- Can restart remote Splunk instances
- Requires an Enterprise license and should be on a dedicated server



Deployment Server Components

Deployment Apps

- Configuration files (such as `inputs.conf`) packaged as apps to be deployed to the deployment clients
- Reside in `SPLUNK_HOME/etc/deployment-apps/`

Deployment Clients

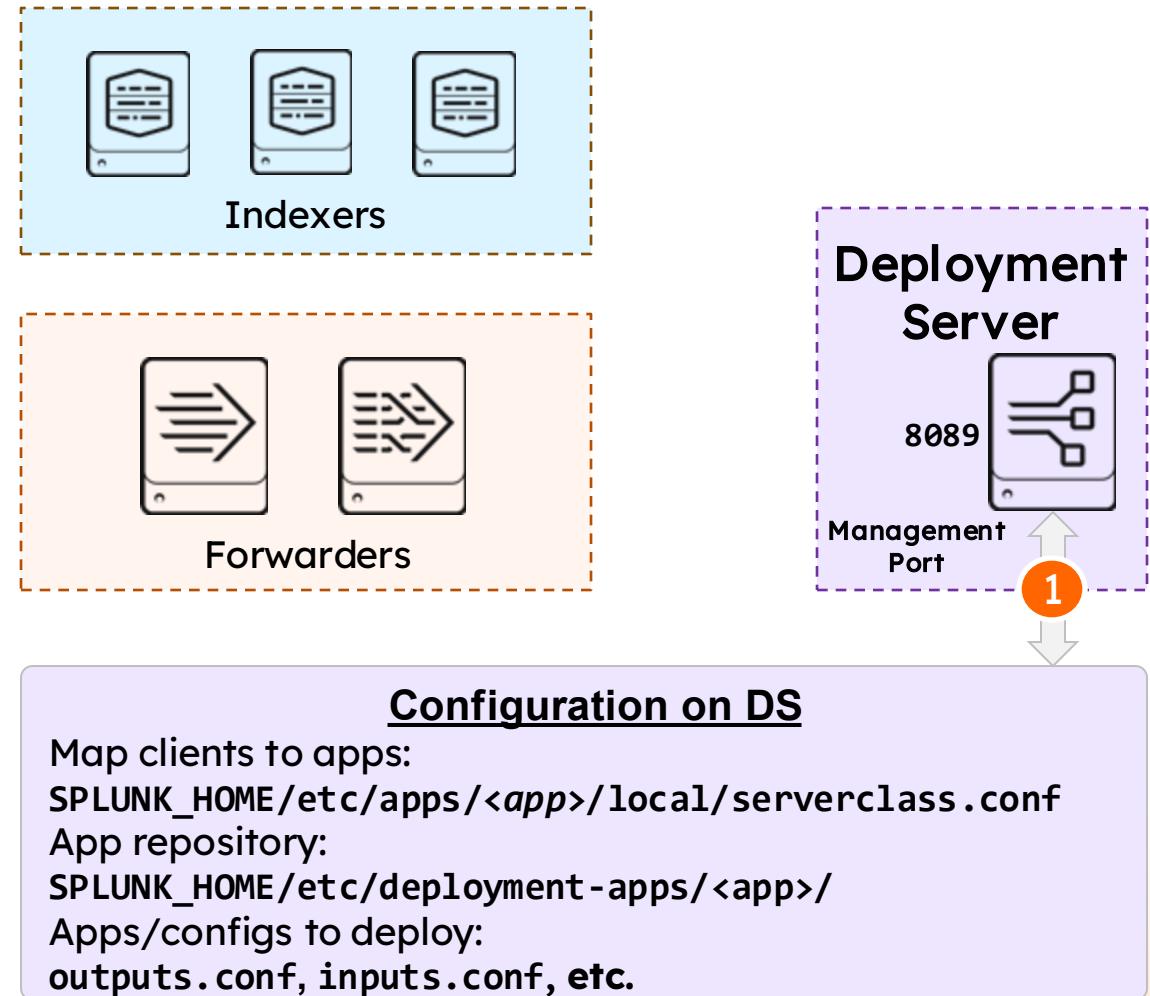
- Splunk instances (Enterprise or UF) that are connected to the Deployment Server (DS) and are phoning home
- Initiate the connection to the Deployment Server

Server Classes

- Groupings of deployment clients
- Define what apps should be deployed to which clients
- Saved in `serverclass.conf`

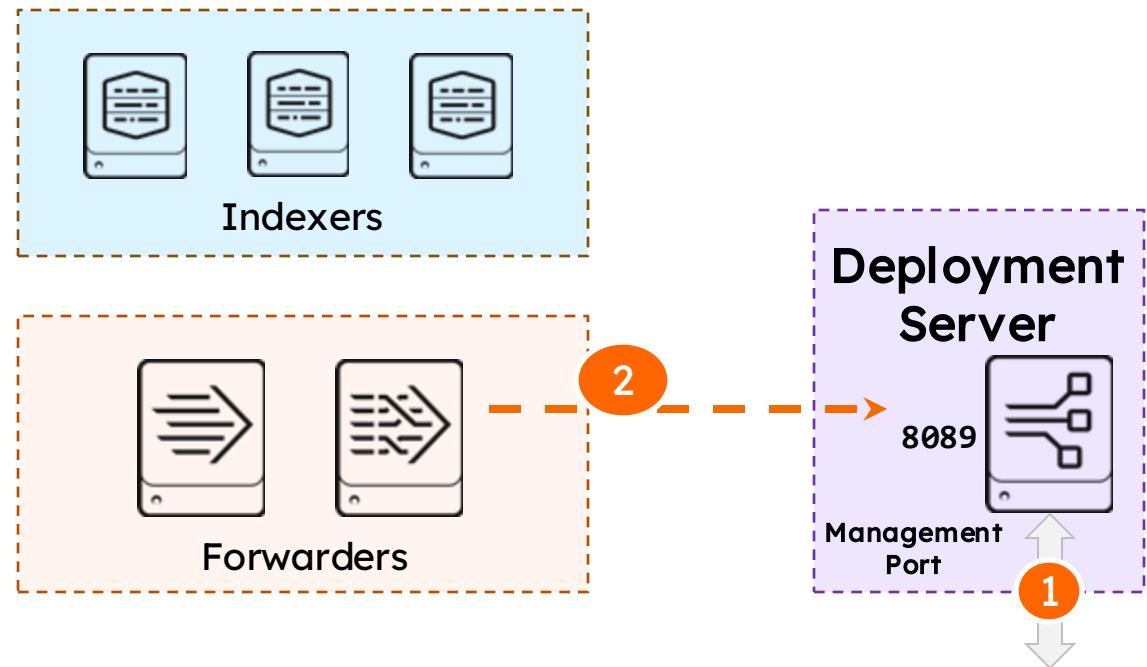
Deployment Server Configuration (1)

1. Configure DS, server classes, and app packages



Deployment Server Configuration (2)

1. Configure DS, server classes, and app packages
2. Configure instances as deployment clients with **deploymentclient.conf**
 - Client starts phone home to DS



Configuration on DS

Map clients to apps:

`SPLUNK_HOME/etc/apps/<app>/local/serverclass.conf`

App repository:

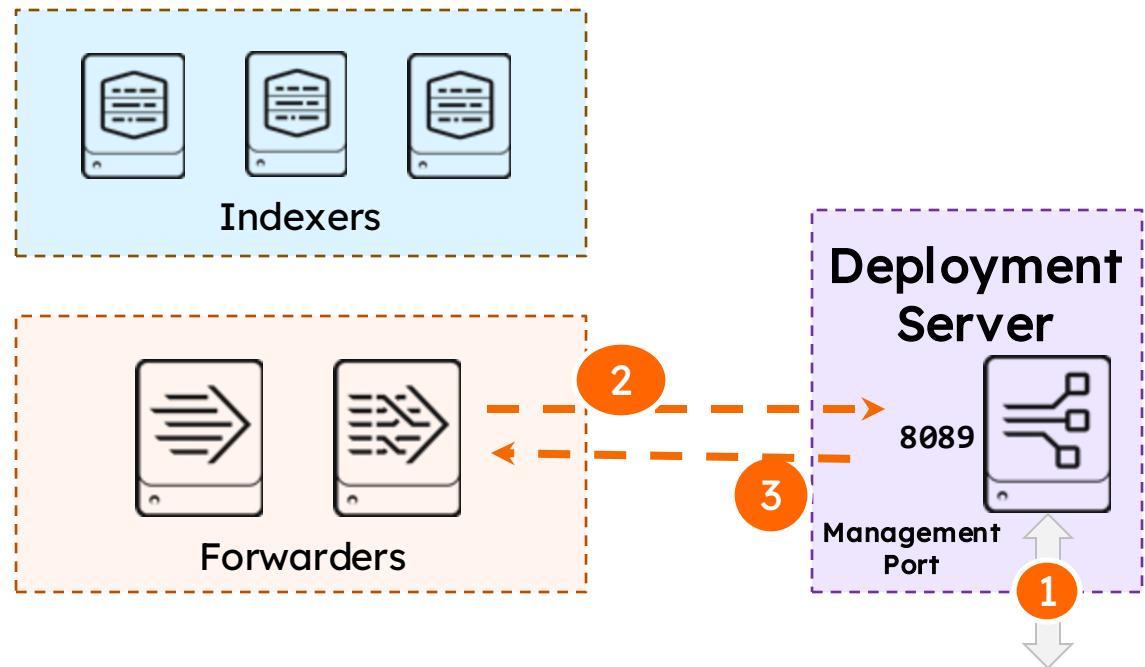
`SPLUNK_HOME/etc/deployment-apps/<app>/`

Apps/configs to deploy:

`outputs.conf, inputs.conf, etc.`

Deployment Server Configuration (3)

1. Configure DS, server classes, and app packages
2. Configure instances as deployment clients with **deploymentclient.conf**
 - Client starts phone home to DS
3. Client downloads subscribed apps
 - As directed by server classes on DS



Configuration on DS

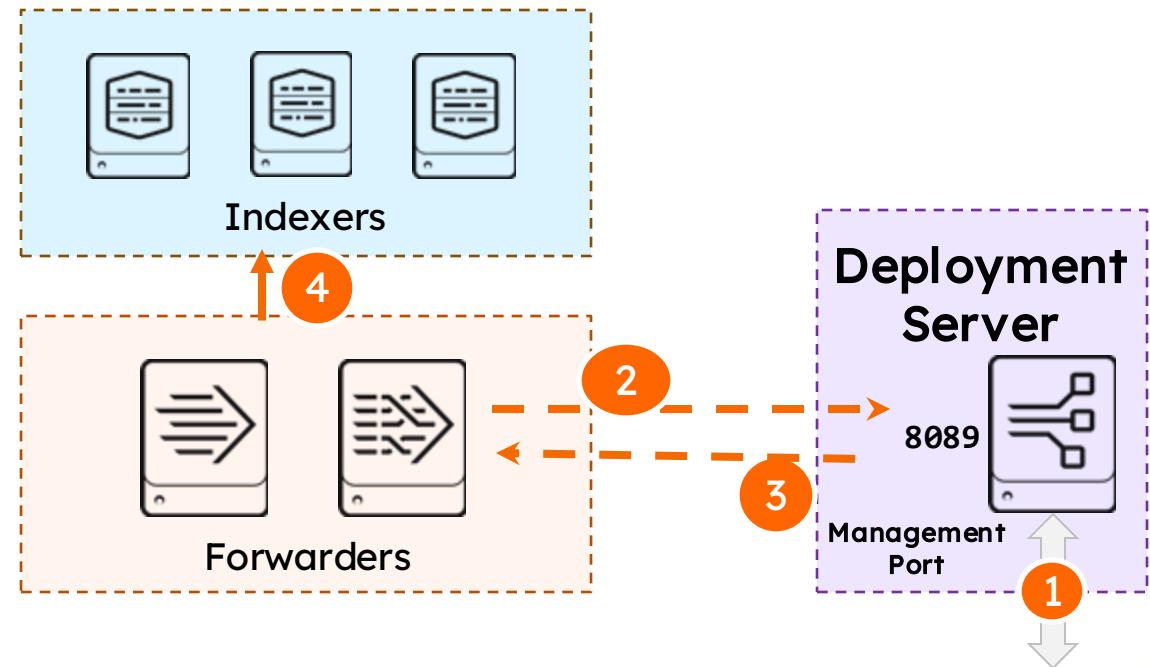
Map clients to apps:
`SPLUNK_HOME/etc/apps/<app>/local/serverclass.conf`

App repository:
`SPLUNK_HOME/etc/deployment-apps/<app>/`

Apps/configs to deploy:
`outputs.conf, inputs.conf, etc.`

Deployment Server Configuration (4)

1. Configure DS, server classes, and app packages
2. Configure instances as deployment clients with **deploymentclient.conf**
 - Client starts phone home to DS
3. Client downloads subscribed apps
 - As directed by server classes on DS
4. Client uses app configurations
 - For example: sending data to indexers



Configuration on DS

Map clients to apps:
`SPLUNK_HOME/etc/apps/<app>/local/serverclass.conf`
App repository:
`SPLUNK_HOME/etc/deployment-apps/<app>/`
Apps/configs to deploy:
`outputs.conf, inputs.conf, etc.`

Enabling Forwarder Management

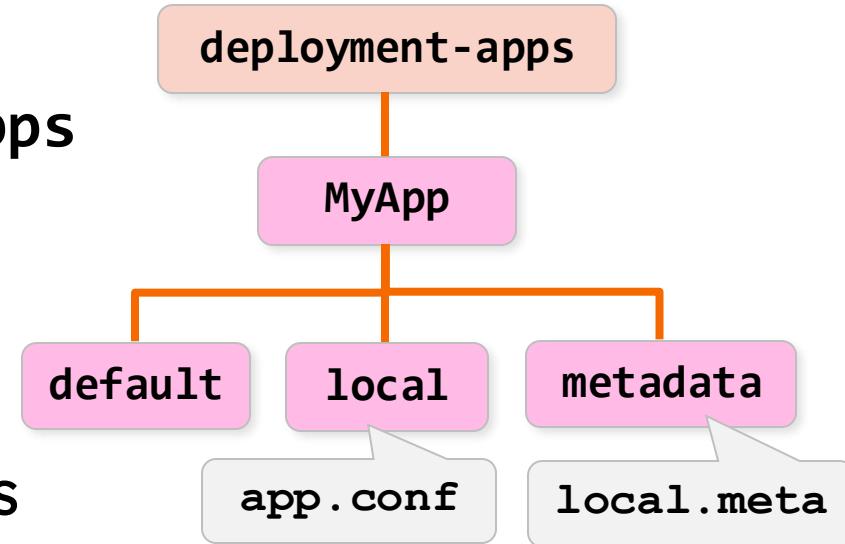
1. On deployment server:
 - Install an Enterprise license (to retain GUI)
 - Add one or more apps in **SPLUNK_HOME/etc/deployment-apps**
2. On forwarders: Set up the deployment client
 - Create **org_all_deploymentclient** base app with **deploymentclient.conf** file
 - Run **splunk restart**
3. On deployment server: Create one or more server classes
 - Use forwarder management in Splunk Web
 - Modify **serverclass.conf (Preferred)**

Workshop Agenda

- Expectations
- What is an agent?
 - Types
- What is Agent Management?
- App management via Agent Manager?
- Agent Management & Deployment Labs
- Agent Image Lab (Extra Credit)
- Summary

Configuring a Deployment App

- Follows app structure and rules
 - Place files in `SPLUNK_HOME/etc/deployment-apps`
 - Recommended files:
 - `app.conf` (in `default` or `local`)
 - `local.meta` (in `metadata`)
 - Add necessary configuration files, scripts, and other resources to appropriate directories
- Files are deployed to client's `SPLUNK_HOME/etc/apps` folder by default
- Best practice
 - Create small and discrete deployment apps
 - Take advantage of `.conf` file layering
 - Use a consistent naming convention



> **Best Practice**

Apps and Add-ons

- Can be downloaded from Splunkbase
- Installed on a Splunk instance:
 - Using the Deployment Server
 - Using CLI on the instance
 - Manually by extracting the app
- Deploy to **SPLUNK_HOME/etc/apps**
- Comes with documentation for details about settings for **inputs.conf**, and so on

The screenshot shows the Splunkbase interface with the 'Discover Apps' section. At the top, there are tabs for 'splunkbase', 'Collections', and 'Apps', along with a search bar. The main heading is 'Discover Apps'. Below it, there's a 'PLATFORM' filter section with a checked 'SPLUNK' checkbox and dropdown menus for 'PRODUCT' (Splunk Enterprise selected) and 'VERSION' (9.1 selected). To the right, a message says 'Showing 1-18 of 102 Results' and 'Filtered by: Splunk, Product > Splunk Enterprise, Version > 9.1, IT Operations, Splunk'. There are four visible app cards:

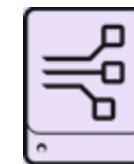
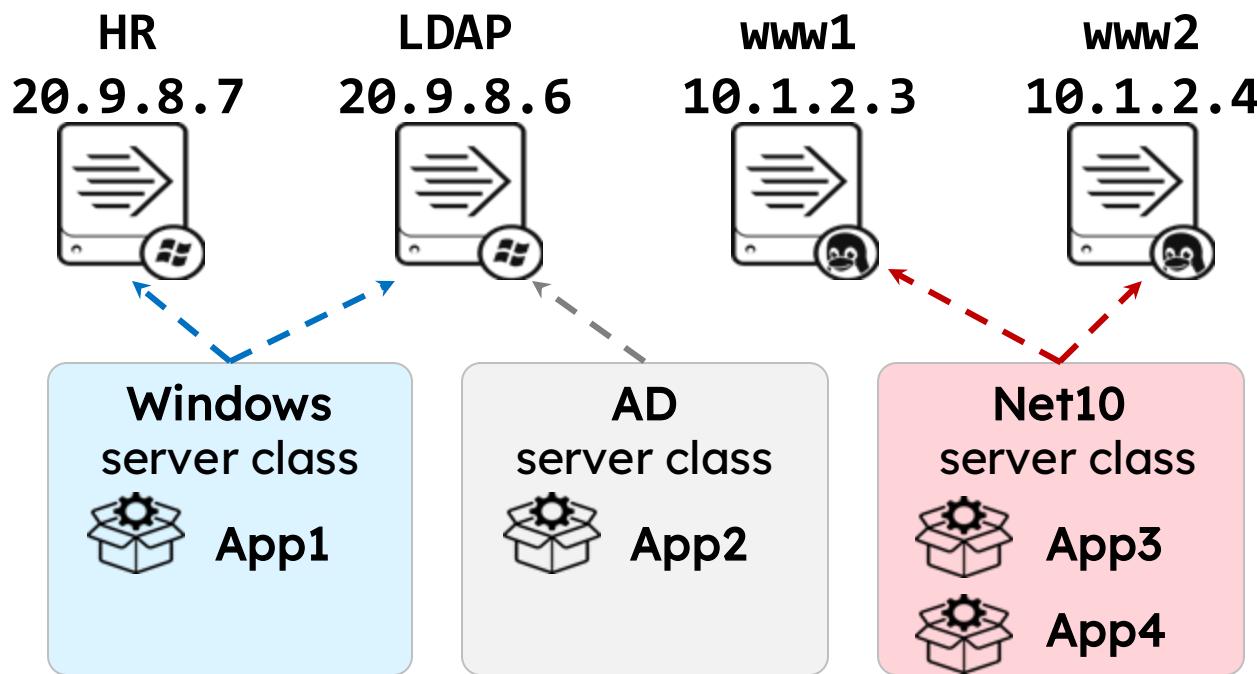
- Splunk Add-on for Microsoft Windows**: By Splunk Inc. (AddOn+), Splunk Enterprise, Splunk Cloud, 4.0 stars (40 reviews)
- Splunk Add-on for Unix and Linux**: By Splunk Inc. (AddOn+), Splunk Enterprise, Splunk Cloud, 4.9 stars (49 reviews)
- SPLUNK SUPPORTED ADDON**: SPLUNK SUPPORTED ADDON
- Splunk Supporting Add-on for Active Directory**: By Splunk Inc. (AddOn+), Splunk Enterprise, Splunk Cloud, 4.0 stars (40 reviews)

Configuring Deployment Clients

- On prospective deployment clients (usually forwarders):
 1. Create `deploymentclient.conf` manually or using a software management tool
 2. Run: `splunk set deploy-poll <deployment_server:splunkd_port>`
 - Creates `deploymentclient.conf` in `SPLUNK_HOME/etc/system/local`
 - **Don't do this**
 3. Restart the deployment clients:
`splunk restart`
 - Edit `[deployment-client]` stanza to override defaults
 - Can be part of initial deployment app
 - Contains phone home setting (default: 60 seconds)
- 
- ```
deploymentclient.conf
[target-broker:deploymentServer]
targetUri = splunk_server:8089
...
[deployment-client]
clientName = webserver_1
phoneHomeIntervalInSecs = 300
```

# What's a Server Class?

- Maps groups of clients to deployment apps
  - Can be based on client name, host name, IP address, DNS name, or machine types



**Deployment Server**

| Server class | Rules                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Windows      | <ul style="list-style-type: none"><li>Assigned to Windows systems</li><li>Installs <b>App1</b></li></ul>                                 |
| AD           | <ul style="list-style-type: none"><li>Assigned to Active Directory servers</li><li>Installs <b>App2</b></li></ul>                        |
| Net10        | <ul style="list-style-type: none"><li>Assigned to hosts on <b>10.1.2.*</b> subnet</li><li>Installs <b>App3</b> and <b>App4</b></li></ul> |

# Adding a Server Class

The screenshot illustrates the process of adding a new server class in the Splunk Forwarder Management interface.

**Initial State:** The main interface shows "Forwarder Management" with a repository location of "\$SPLUNK\_HOME/etc/deployment-apps". It displays 0 Clients phoned home in the last 24 hours and 0 Deployment Errors. Under "Server Classes", there is 1 Server Class (uf\_base) listed. A message indicates "No server classes. Learn more. Or create one".

**Action 1:** The "Server Classes (0)" link is highlighted with a red box and circled with a red number 1.

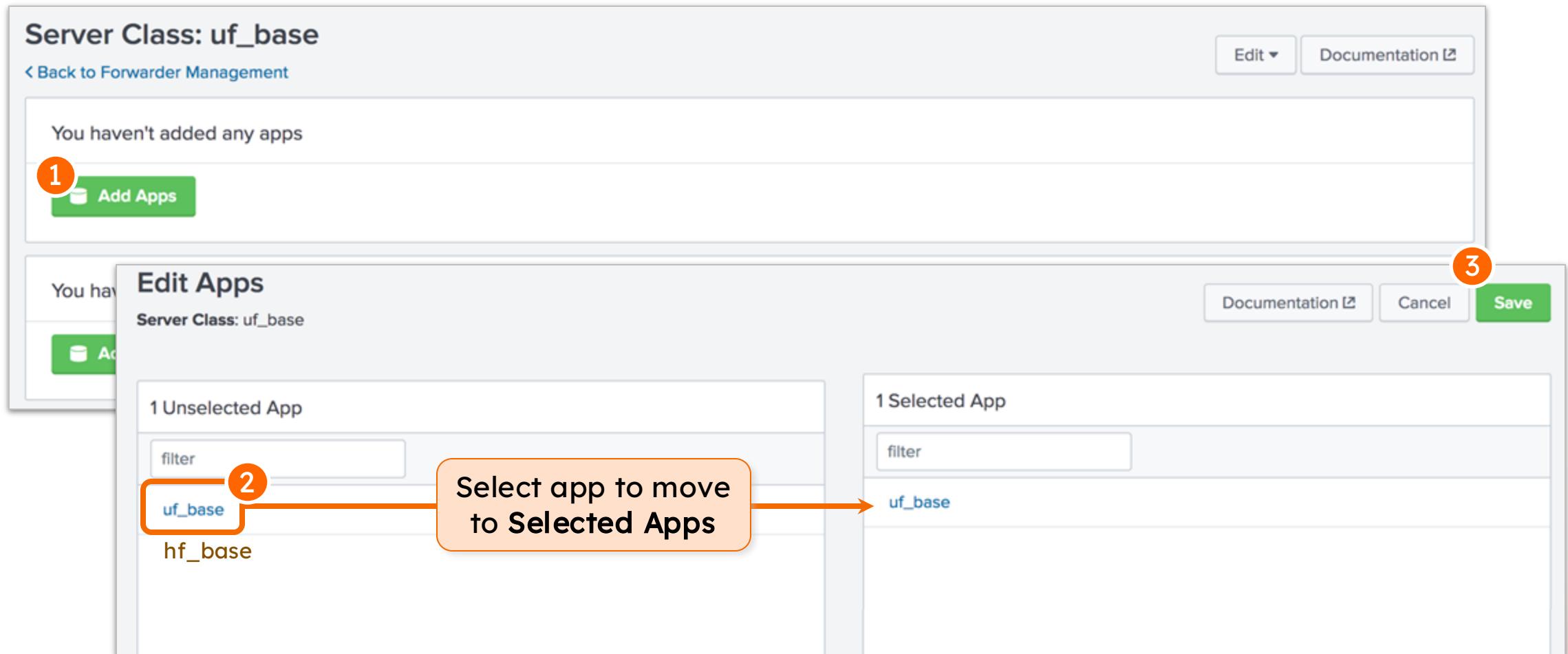
**Action 2:** A red arrow points from the "Create one" link in the message to the "New Server Class" dialog box.

**Dialog Box:** The "New Server Class" dialog box is open, prompting the user to "Enter a name for the new server class". The "Name" field is empty and highlighted with a blue border. The dialog also includes "Cancel" and "Save" buttons.

**Action 3:** A red box highlights the "Name" input field in the dialog, and a red number 3 is circled around it.

**Final State:** The main interface now shows 1 Client phoned home in the last 24 hours. The "Server Classes" section shows 1 Server Class (uf\_base) listed. A red box highlights the "New Server Class" button in the bottom right corner, and a red number 2 is circled around it.

# Selecting Apps for the Server Class



# Post Deployment Behavior Setting

The screenshot shows the Splunk Forwarder Management interface for a server class named "uf\_base".

**Top Panel:** Shows the "Server Class: uf\_base" header, a "Deployed Successfully" dropdown, a "filter" input, and pagination controls (1 Apps, 10 Per Page). A red box labeled "1" highlights the "Edit" button for the "uf\_base" row.

**Bottom Panel (Edit App: uf\_base):** Shows the "Edit App: uf\_base" title, "Server Classes" section (with "uf\_base" selected), and an "After Installation" section. In the "After Installation" section, two checkboxes are present: "Enable App" (checked) and "Restart Splunkd" (unchecked). A callout bubble with the text "Ensure Restart Splunkd is enabled" points to the "Restart Splunkd" checkbox. A red box labeled "2" highlights the "Restart Splunkd" checkbox. A red box labeled "3" highlights the "Save" button at the bottom right.

# Selecting Clients for the Server Class

The screenshot shows the 'Edit Clients' page for a 'Server Class: uf\_base'. The 'Include (whitelist)' field contains 'ip-10\*'. A callout box labeled '2' points to this field with the text: 'Enter Include, Exclude, and/or Machine Type filters'. Another callout box labeled '2' points to the 'Exclude (blacklist)' field, which is currently empty, with the text: '• Supports wildcards  
• Exclude takes precedence over Include'. A third callout box labeled '3' points to the 'Save' button at the bottom right with the text: '• In addition to include/exclude, you can further filter based on machine types  
• The list is based on the clients that have connected to this deployment server'. The table at the bottom shows one client entry: 'ip-10-0-0-100' with host name '10.0.0.100', DNS name 'E9DB9FFE-589E-4158-8B2F-77F26B4418A4', instance name 'engdev203', IP address '10.0.0.100', machine type 'linux-x86\_64', and a timestamp 'a few seconds ago'.

Server Class: uf\_base

Back to Forwarder Manager

Edit Clients

Server Class: uf\_base

Documentation

Apps Edit

Deployed Successfully

1 Apps 10 Per Page

Name

uf\_base

You haven't added any clients yet.

Add Clients

1

2

3

Include (whitelist)

ip-10\*

Can be client name or IP address. Examples: 185.2.3.\*, fwdr-\*

Learn more

Exclude (blacklist)

Optional

Examples: ronnie, rarity

Learn more

Filter by Machine Type (machineTypesFilter)

+ Optional

All Matched Unmatched filter

1 10 Per Page

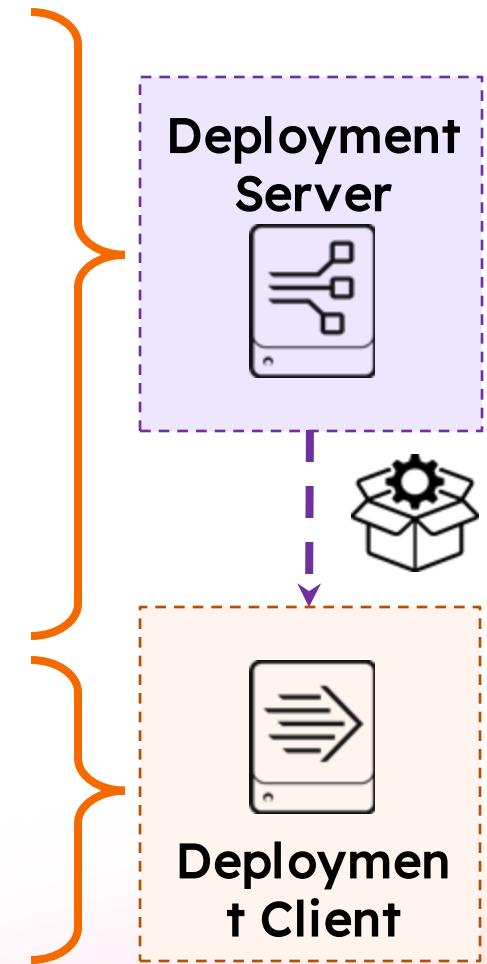
| Matched       | Host Name  | DNS Name                             | Client Name | Instance Name | IP Address | Machine Type | Phone Home        |
|---------------|------------|--------------------------------------|-------------|---------------|------------|--------------|-------------------|
| ip-10-0-0-100 | 10.0.0.100 | E9DB9FFE-589E-4158-8B2F-77F26B4418A4 |             | engdev203     | 10.0.0.100 | linux-x86_64 | a few seconds ago |

# Verify Forwarder Management

- On the deployment client:
  - Display the deployment server and management port:  
`splunk show deploy-poll`
  - Confirm expected app directories and contents in  
`SPLUNK_HOME/etc/apps/app_name`
    - Occurs at the next phone home interval
- On the deployment server:
  - Display information about the deployment clients:  
`splunk list deploy-clients`

# Updating Deployed Apps

1. Add new apps or change existing app in **deployment-apps**
2. Run **splunk reload deploy-server**
  - Detects changes to deployment apps on DS
    - Re-caches list of deployment apps
    - Re-calculates checksums used to uniquely identify apps by their contents
  - Eliminates need to restart Splunk
3. Verify the client downloads new/changed apps after next phone-home
  - Client downloads apps when checksums have changed

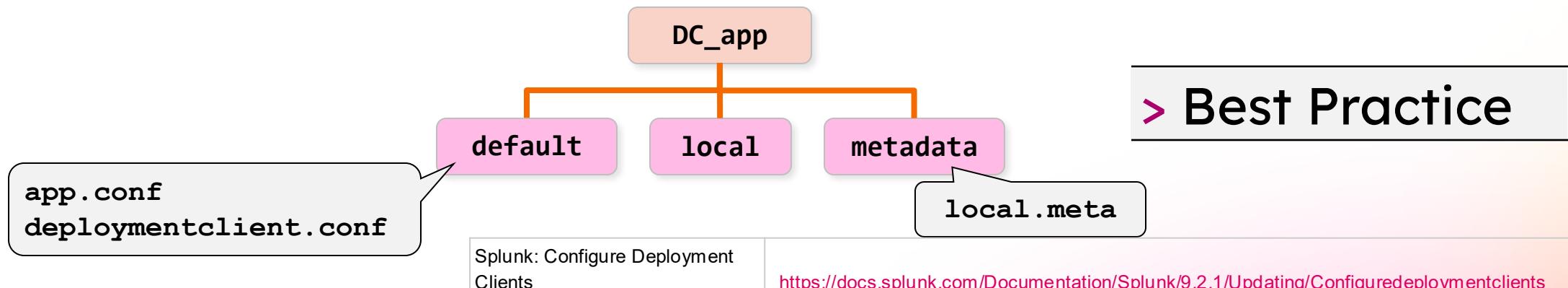


# Workshop Agenda

- Expectations
- What is an agent?
  - Types
- What is Agent Management?
- App management via Agent Manager?
- **Agent Management & Deployment Labs**
- Agent Image Lab (Extra Credit)
- Summary

# Manage Deployment Client Settings Centrally

- Must configure client to phone home to DS first
- Use an app to manage deployment client settings
  - Create a deployment client settings app (example: DC\_app)
  - Move `deploymentclient.conf` settings from `etc/system/local/` to `etc/apps/DC_app/local/`
  - Deploy DC\_app to clients using a dedicated server class



# Forwarder Management & Deployment Labs

1. Access the Web UI and CLI of your Deployment Server
2. Retrieve Splunk settings from your deployment server using the CLI
3. Examine Splunk configuration file documentation and basic .conf files
4. Create the outputs base app
5. Create the deployment client base app
6. Create the serverclass.conf file

# Workshop Agenda

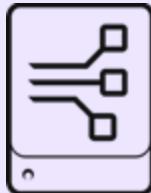
- Expectations
- What is an agent?
  - Types
- What is Agent Management?
- App management via Agent Manager?
- Agent Management & Deployment Labs
- Agent Image Lab (Extra Credit)
- Summary

# Forwarder Image Lab (Extra Credit)

1. Preparation for Cloning
2. Creating a Tarball
3. Optional Secure Copy (SCP)

# Useful Commands

**Deployment Server**



**Deployment Client**

| Command                                   | Operation                                                                                   |
|-------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>From the Deployment Server (DS):</b>   |                                                                                             |
| <code>splunk reload deploy-server</code>  | Checks all apps for changes and notifies the relevant clients the next time they phone home |
| <code>splunk list deploy-clients</code>   | Displays information about the deployment clients                                           |
| <b>From the Deployment Client:</b>        |                                                                                             |
| <code>splunk set deploy-poll</code>       | Connects the client to the deployment server and management port                            |
| <code>splunk show deploy-poll</code>      | Displays the current deployment server and management port                                  |
| <code>splunk list forward-server</code>   | Displays the current forward server configuration                                           |
| <code>splunk disable deploy-client</code> | Disables the deployment client                                                              |

# Workshop Agenda

- Expectations
- What is an agent?
  - Types
- What is Agent Management?
- App management via Agent Manager?
- Agent Management & Deployment Labs
- Agent Image Lab (Extra Credit)
- Summary

# Key Takeaways

1. Understanding Universal Forwarders:
  - a. Learn the role of Splunk Universal Forwarders in collecting and forwarding data from various sources to Splunk indexers.
  - b. Understand the difference between Universal Forwarders and Heavy Forwarders.
2. Deployment Server Configuration:
  - a. Setup and configuration of a Splunk Deployment Server.
  - b. Create and manage server classes to define groups of deployment clients.
  - c. Assign apps to server classes for efficient distribution of configurations and updates.
3. Creating Serverclass.conf:
  - a. Gain hands-on experience in creating and configuring the serverclass.conf file.
  - b. Learn to define whitelist and blacklist criteria to include or exclude forwarders from server classes.
4. Managing Forwarders:
  - a. Develop skills to manage and monitor forwarders effectively.
  - b. Learn to troubleshoot common issues with forwarder deployment and communication.

# Thank you