

.conf2015

Simplified Forwarder Deployment and Deployment Server Techniques

Cary Petterborg

Sr. Monitoring Eng., LDS Church

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

My Disclaimer

During the course of this presentation, I may make references to my employer, the Church of Jesus Christ of Latter-day Saints. This should not be taken as an endorsement of Splunk or Splunk products by the LDS Church.

In addition, software referenced in this presentation may be made available for download. This software may not be suitable for your environment. No warranty or claim of suitability is made on this software, and any damages incurred are not my responsibility (you take full responsibility for any damages). Care should be taken when installing any software.



.conf2015

Scope and Audience

splunk>

Scope

- Simplified universal forwarder (UF) installation
- By anyone with root/admin access
- No need to edit files
- Finds “standard inputs” automatically
- Installation conforms to a known standard

When is this method useful?

Including, but not limited to, the following criteria:

- Many indexes (e.g. departmental indexes)
- Ad hoc deployment (non-ubiquitous forwarders or slow migration)
- Allow non-admin installation of UF
- Multiple data centers or offices
- Secure facility installations of UF
- Add a UF to search heads and indexers to monitor local data

Audience: Who should be here?

- Splunk administrators
- Infrastructure operations personnel
- Splunk personnel in charge of new Splunk features. 😊



.conf2015

About Me

splunk>

Who is Cary Petterborg?

- Splunk user and administrator for 3.5 years
- Monitoring Engineer for 8 years
- Web developer for 21 years
- Software engineer for 35 years
- Many languages from assembly to Ruby
- Works for the LDS Church in Salt Lake City



.conf2015

My Employer

splunk>

The Church of Jesus Christ of Latter-day Saints

- Based in Salt Lake City, Utah
- Established 1830
- 16 million members worldwide
- 9,000 servers (Family Search – additional 12,000 servers)
- 2,300 UFs, 8 indexers, 6 search heads, deployment server, 2 syslog servers



.conf2015

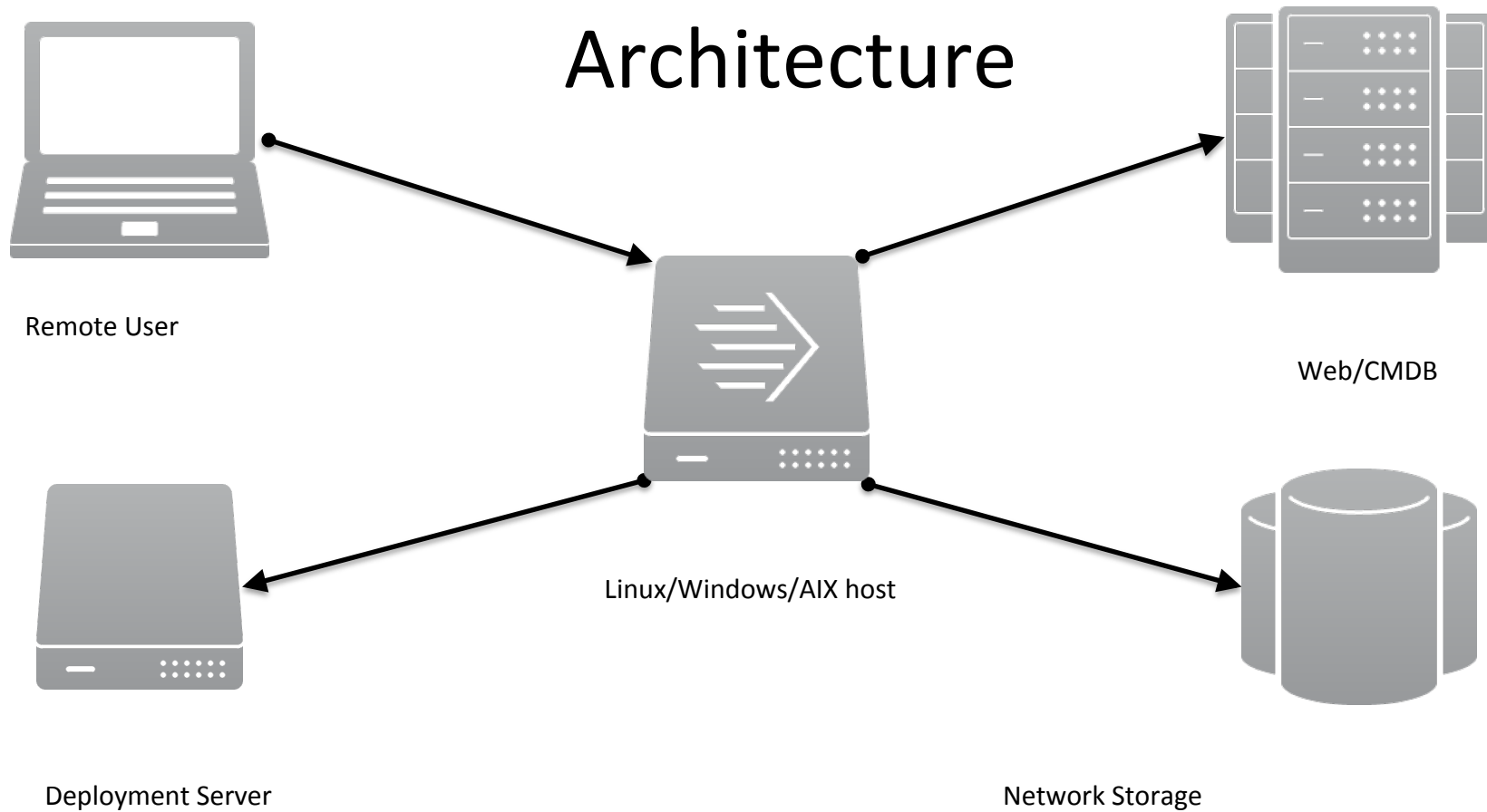
Requirements & Assumptions

splunk>

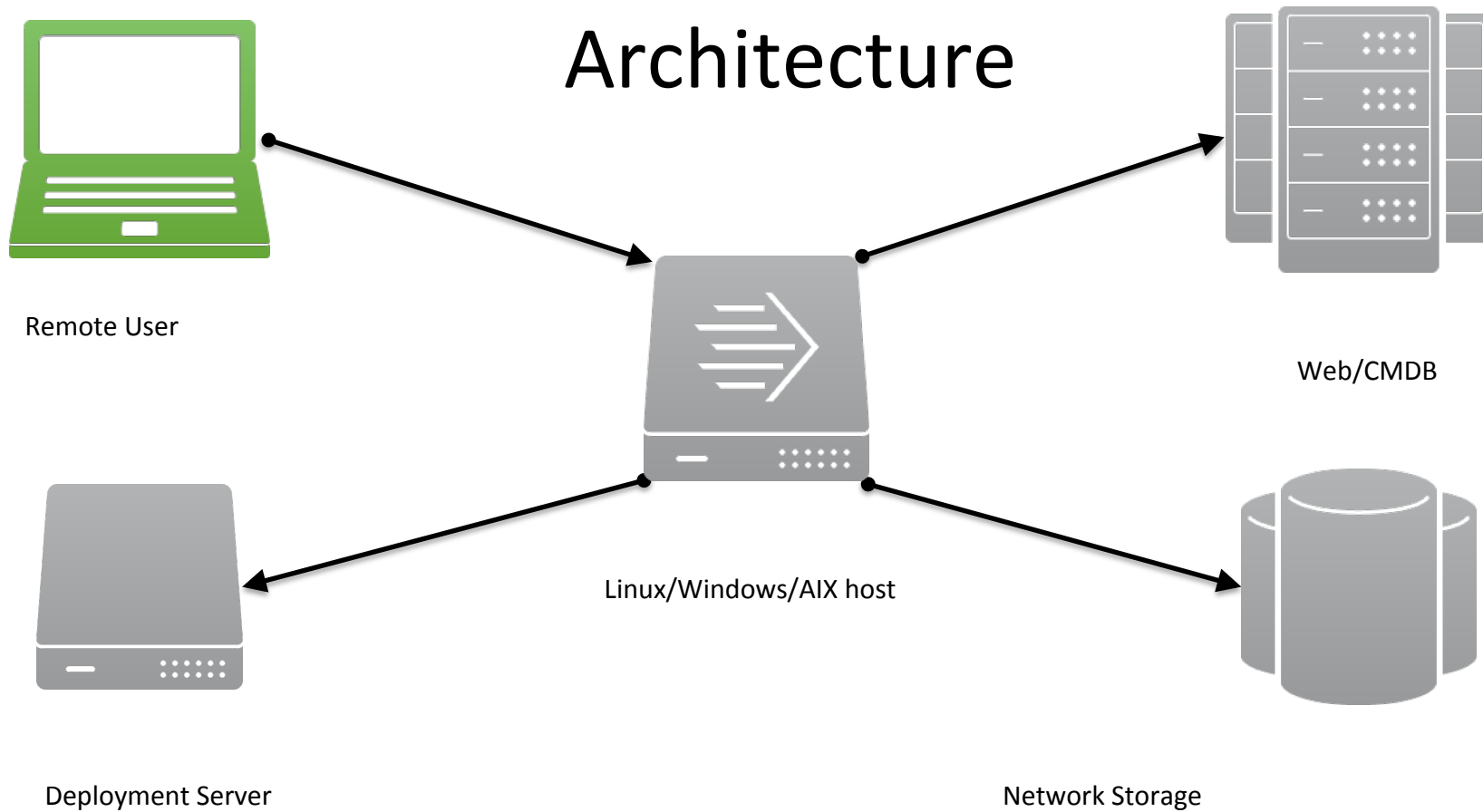
Requirements

- Root access for Linux and AIX (bash)
- Administrator access for Windows (PowerShell)
- Web server for remote file access
- Splunk deployment server
- Firewalls configured properly

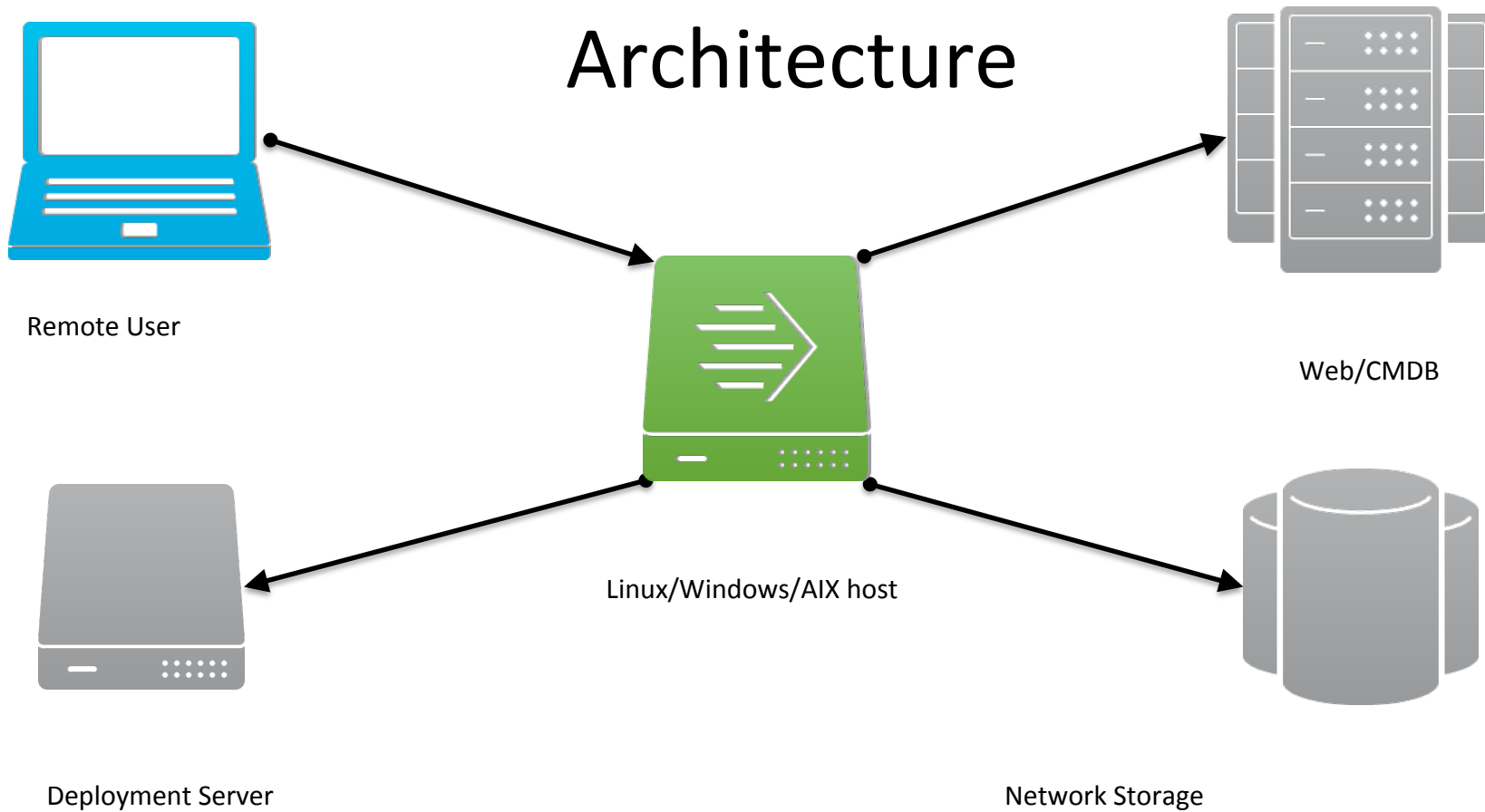
Architecture



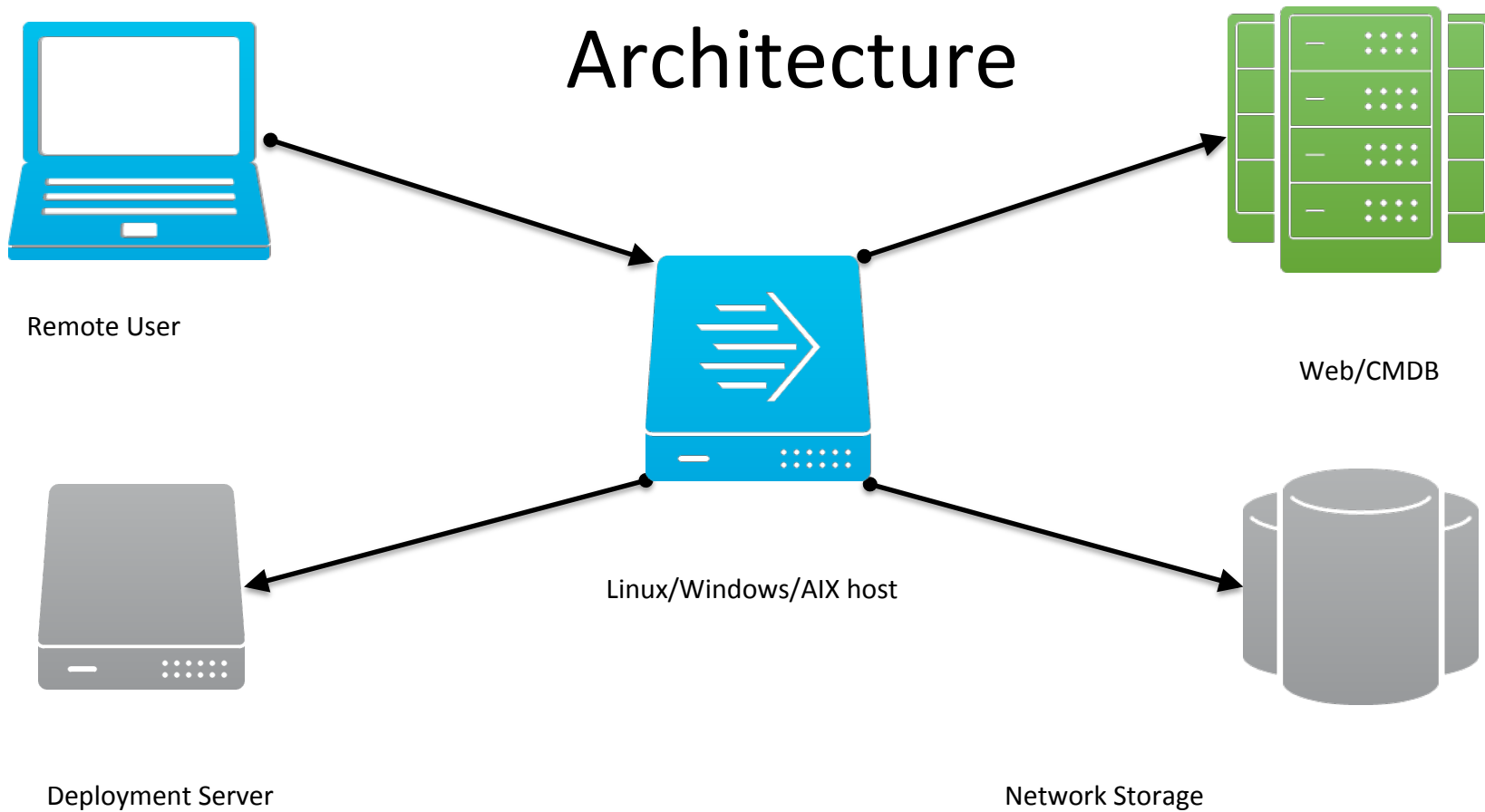
Architecture



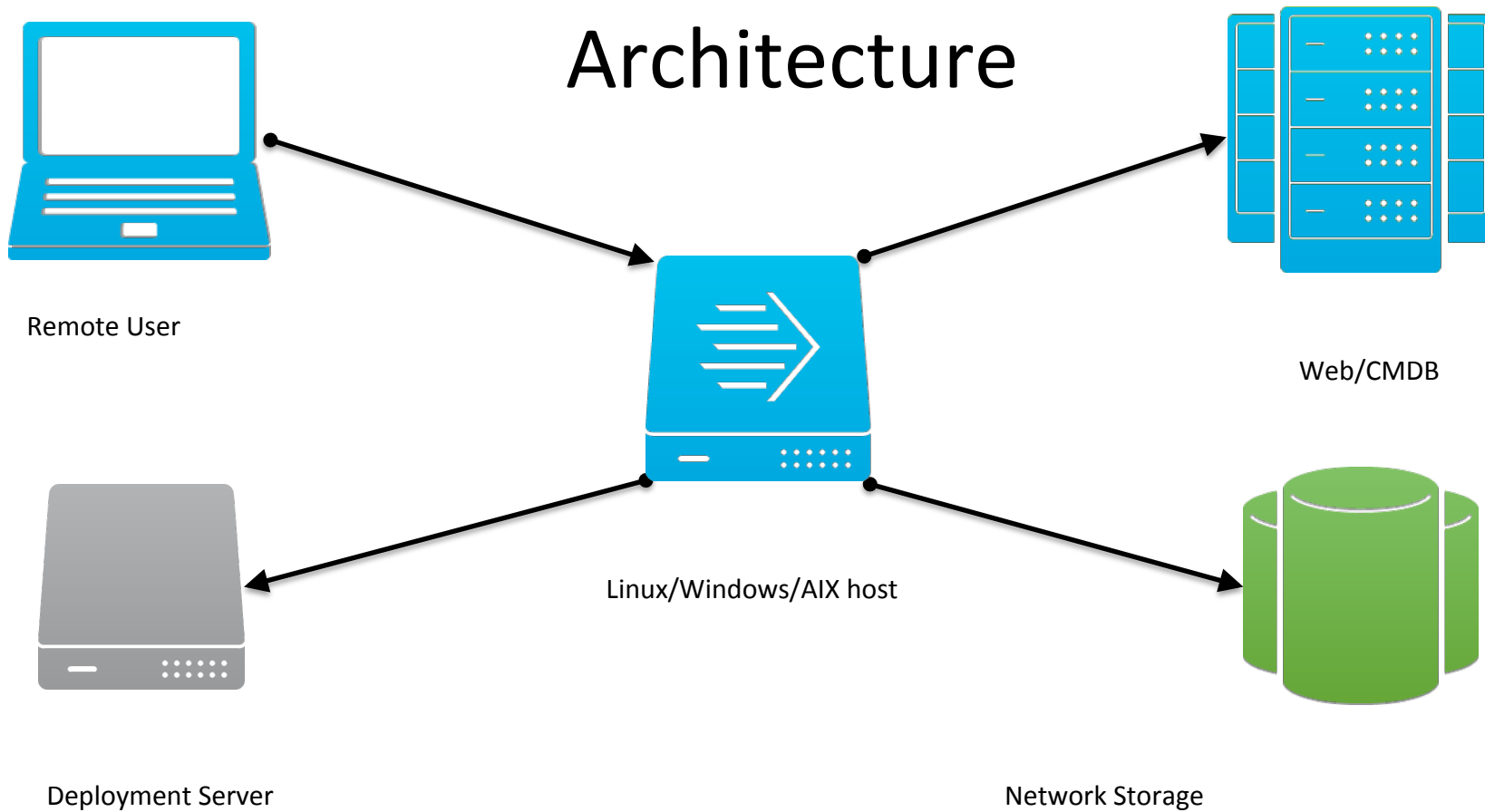
Architecture



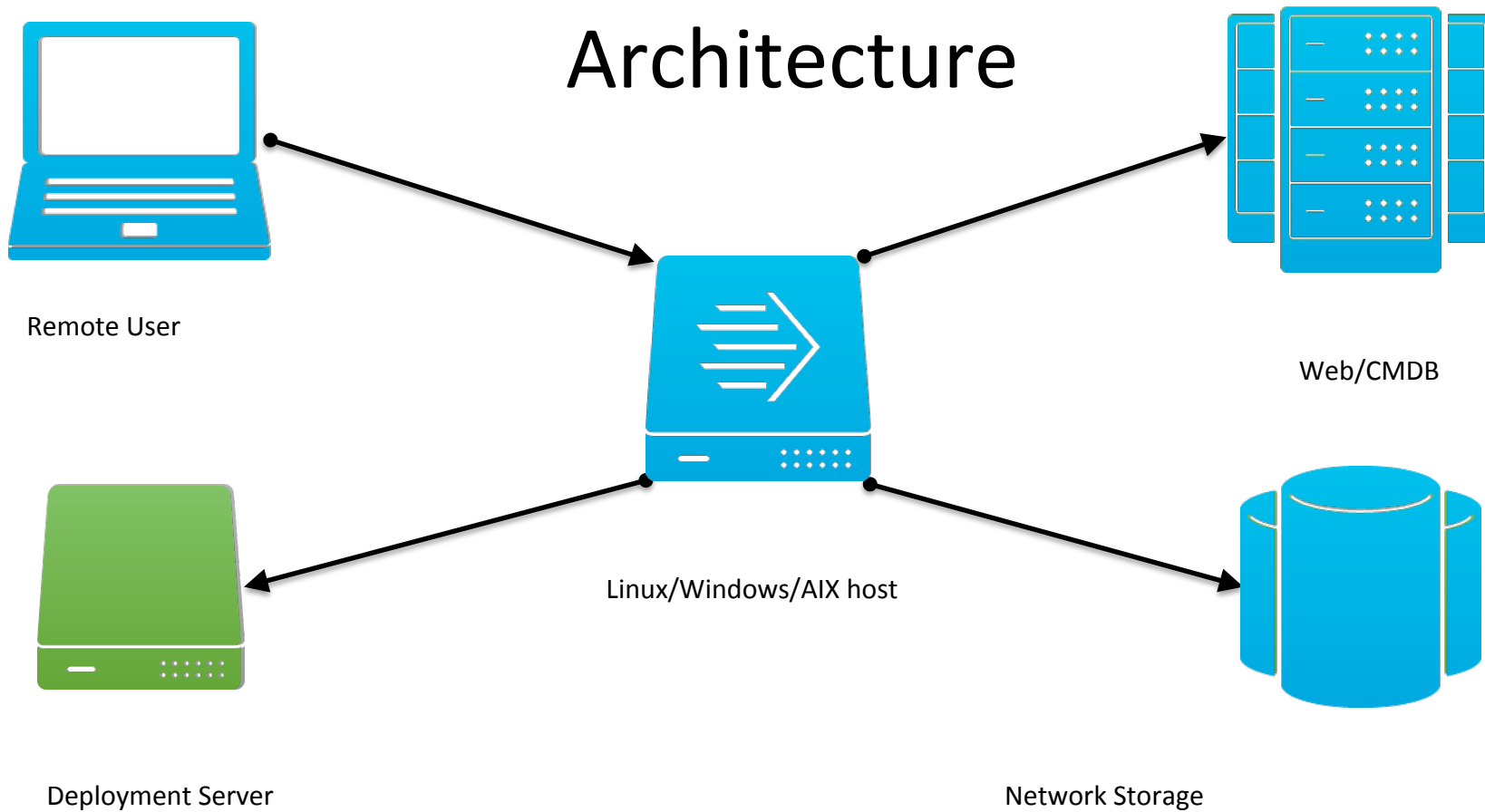
Architecture



Architecture



Architecture



Optional Tools

- Recommended: Universal mount point for Linux and AIX (i.e., NFS mount)
- CMDB
- **wget** for Linux and AIX
- Access to web service to validate Configuration Items (CI)



.conf2015

About the Scripts

splunk>

Script Functionality

1. Checks for new installation or update
2. Verifies host as valid CI in CMDB
3. Sets the default index
4. Auto-discovers applications
5. Installs UF from .tar or .msi file
6. Creates the deployment server configuration
7. Restarts UF



.conf2015

Make Your
Deployment Server
Do the Work

splunk>

Set Up the Deployment Server

- **clientName** from *deploymentclient.conf* file determines:
 - Default index
 - Application inputs
 - Hostname
- Use a standardized deployment configuration file instead of using the Splunk installation archive (tar, .msi, etc.) to set the deployment server – Interactive: Windows will complain that you are not providing inputs and outputs, but this is really fine.

Result of install to deploymentclient.conf

- etc/system/local/deploymentclient.conf:

```
[deployment-client]
```

```
clientName=prod_cs_apache_lnx12345
```

Key:

Production-splunk _index _application1 _applicationZ _hostname

Example serverclass.conf

```
...  
# apache  
[serverClass:forwarders_apache]  
whitelist.O = *_apache_  
[serverClass:forwarders_apache:app:test_apache]  
appFile=empty_app  
[serverClass:forwarders_apache:app:all_apache_inputs]  
...
```


Example Apache inputs configuration

- Set up a normal deployment app (all_apache_inputs/local/inputs.conf) for apache, like:

these are the apache log files to monitor:

```
[monitor:///var/log/httpd/*access*log]
```

```
sourcetype=apache
```

```
[monitor:///var/log/httpd/*error*log]
```

```
sourcetype=apache_error
```

...

Example serverclass.conf

...

indexZ default index

[serverClass:Z_forwards]

restartSplunkd=true

whitelist.0=*_indexZ_*

[serverClass:Z_forwards:app:indexZ_default_inputs]

...

Example default index definition

- etc/deployment-apps/indexZ_default_inputs/local/inputs.conf:

```
# default indexZ  
[default]  
index=indexZ
```



.conf2015

Standardized Deployment Configuration

splunk>

Deployment Zip or Tar file contents

```
splunkforwarder/  
splunkforwarder/etc/  
splunkforwarder/etc/apps/  
splunkforwarder/etc/apps/all_deploymentclient/  
splunkforwarder/etc/apps/all_deploymentclient/local/  
splunkforwarder/etc/apps/all_deploymentclient/local/app.conf  
splunkforwarder/etc/apps/all_deploymentclient/local/deploymentclient.conf  
splunkforwarder/etc/apps/all_deploymentclient/metadata/  
splunkforwarder/etc/apps/all_deploymentclient/metadata/local.meta
```

etc/apps/all_deploymentclient/local/deploymentclient.conf

example deployment config (set your host and port)

[deployment-client]

phoneHomeIntervalInSecs = 300

[target-broker:deploymentServer]

targetUri= splunk-deploy.YOUR.ORG:9089

Deploying This Configuration

- Distribute the archive file to the installing host (part of the script)
- Untar or unzip the archive into the etc/apps directory
- On startup of Splunk this file is read in, then the deployment server is contacted for the rest of the configuration files, including the outputs.conf, etc.
- The deployment server can be identified by DNS or IP address, just make sure it is reachable in the same way by all hosts



.conf2015

Integrating with CMDB

splunk>

What Is Involved?

- Required: CMDB API or Database with Configuration Items
- Custom web page that calls API or Database query
- Can be very simple (see the example)
- On Linux/AIX it can be accessed with **wget**
- On Windows – not currently supported in script – looking for options

Example script: cmdb.php?host=hostname

```
<?PHP
$hostname = $_GET['host'];
$cmd = sprintf("echo \"select count(*) from cmdb_itsm_config_item
where ci_name = '%s'\" | mysql -h cmdb-host -u user -ppassword cmdb",
$hostname);
exec ($cmd,$output);
echo $output[1];
?>
```



.conf2015

Upgrading Via the Installation Scripts

splunk>

Updating configurations

An upgrade to using this method can be performed using this same script.

- Symlink the installation script on Linux/AIX and it will do an update:

```
ln -s forwarderInstall6.sh forwarderUpdate6.sh
```

- Will not install a new forwarder, just update the configuration
- Useful when the forwarder is already installed, but you want to get the configuration set up the same way.



.conf2015

Helpful suggestions

splunk>

Suggestions, Part 1

If you want to make the fewest changes to the scripts:

- Make applications with dashes in names – NOT underscores
my-app instead of *my_app*
- Don't use underscores in hostnames or index names
fin-legal instead of *fin_legal*
- powershell -ExecutionPolicy ByPass -File splunkinstall.ps1

Suggestions, Part 2

- Set up firewall rules so that you can include all hosts accesses as widely as possible
- Firewall ports:
 - To deployment server (ours is 9089)
 - To indexers (default: 9997)
 - To web server for files access (ours is 80)

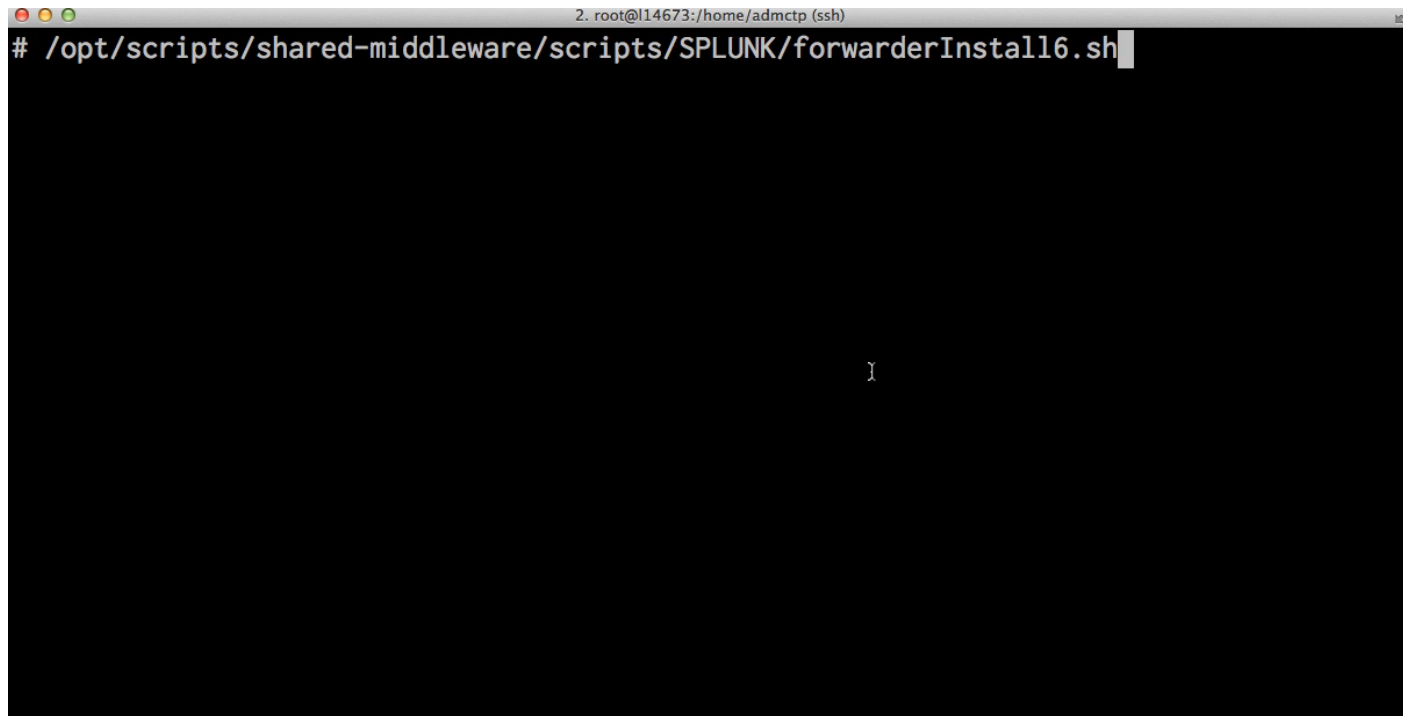


.conf2015

Watch the install

splunk>

The Linux Installation in Action!



A terminal window with a title bar showing '2. root@l14673:/home/admctp (ssh)'. The command prompt is '# /opt/scripts/shared-middlew.../scripts/SPLUNK/forwarderInstall6.sh'. The terminal area is mostly black with a cursor visible in the center.

```
2. root@l14673:/home/admctp (ssh)
# /opt/scripts/shared-middlew.../scripts/SPLUNK/forwarderInstall6.sh
```



.conf2015

Example Install Files

splunk>

Where Are the Files and What Next?

- <https://app.box.com/splunkufinstallscripts>
- The script files are going to be uploaded soon, with updates following
- A personal email: splunkinstaller@petterb.org



.conf2015

Questions?

splunk>



.conf2015

THANK YOU

splunk>