

splunk>

.conf2017

© 2017 SPLUNK INC.

# Cisco and Splunk

Innovation through the Power of Innovation

Douglas Hurd	Cisco Security Technical Alliances PM
Colin Lowenberg	Cisco Meraki Platform Partnerships PM
Karthik Karupasamy	Cisco UCS Technical Marketing Engineer
Robert Novak	Cisco Big Data Technical Solutions Architect

September 28, 2017 | Washington, DC

# 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.

# Eight Years of Integration and Innovation

---

A brief history of Cisco and Splunk together  
With Robert Novak



# Why Does Hardware Still Matter?

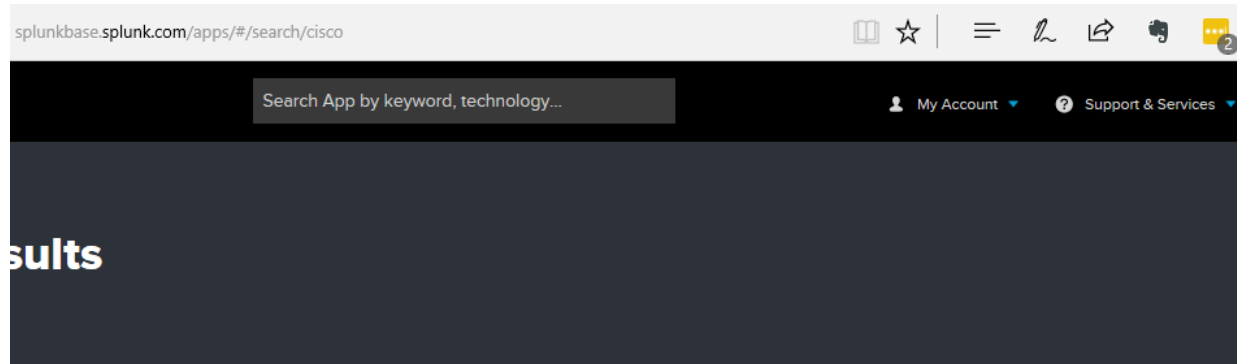
- ▶ Cisco customer big data pools tend to grow 2-3x/year
- ▶ Cisco customer IT staff doesn't grow as fast
- ▶ The Cisco Unified Computing System (UCS) provides scalable, repeatable, predictable, and manageable deployments across dozens to thousands of servers for any application deployment
- ▶ Pallet to production in hours, not days or weeks
- ▶ Deep engineering integration between Cisco and Splunk with tested and proven configurations

More on this later...













# Dozens Of Apps And Add-ons At Splunkbase



Search: cisco x

Showing 1-20 of 47 results

Best Match v

 <b>Cisco Security Suite</b> 2064 Installs	 <b>Cisco Networks App for Splunk</b> 1839 Installs	 <b>Cisco Networks Add-on for Splunk</b> 2974 Installs	 <b>Cisco ACI App for Splunk Enterprise</b> 103 Installs
 <b>Cisco ACI Add-on for Splunk</b> 107 Installs	 <b>Splunk Add-on for Cisco ASA</b> 5249 Installs	 <b>Splunk Add-on for Cisco FireSIGHT</b> 5306 Installs	 <b>Splunk Add-on for Cisco IPS</b> 563 Installs

Always more being added and updated, by Cisco, Splunk, partners, third party developers, and end users!








# Splunk and Cisco API-based Integrations

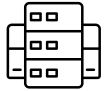




Programmable Operational Analytics at Scale





### Security

-  Identity Services (ISE/pxGrid)
-  FirePOWER Next Gen Firewall
-  Umbrella (DNS)
-  CloudLock
-  ThreatGrid\*

### Infrastructure

-  Cisco UCS
-  ACI / APIC
-  Nexus 9k
-  Meraki Wireless / CMX
-  Tetration

### Collaboration Business Analytics

-  Call Manager
-  Spark

and many more here <https://splunkbase.splunk.com/apps/#/search/Cisco/>

# Cisco Security Integrations

---

Making sense of a broad security platform using Cisco and Splunk technologies

With Douglas Hurd

# Splunk & Cisco Security – “Better Together”



## Security Breadth, Customer Reach, Infrastructure for Automation

- Largest security footprint in the industry
- Produces broad range of security telemetry across most security technologies
- Ubiquitous network footprint enables bi-directional integration for executing security automation
- High investment in Splunk apps for serving joint customers



## Analytics Efficacy, Ability to Automate, Committed Customers

- Voluminous, context-rich Cisco data sources drive license volumes while enabling improved security & compliance, more effective SIEM use cases and new use cases beyond security
- Automated actions in Cisco network environs
- Proven, supported integrations accelerate time to value



# Cisco Splunk Integrations

### Security

- IPS
- Identity Services Engine/pxGrid
- FireSIGHT (including AMP)
- ASA/PIX/FWSM Firewalls
- Web Security Appliance (WSA)
- Email Security Appliance (ESA)
- Stealthwatch
- Umbrella Investigate
- Cloud Web Security (CWS)
- AnyConnect
- CloudLock
- ThreatGrid

Cisco Security Suite App

### Data Center / ACI

- Cisco UCS
- UCS Director Express for Big Data
- Application Centric Infrastructure (ACI - APIC)
- Nexus 9K
- Tetration (planned)

### Enterprise Networking

- Nexus and Catalyst Switches
- Nexus 1000V
- NGN Routers (CRS, ASR, ISR)
- Meraki Wireless
- Open SDN Network Controller
- CMX Wireless
- Network Data Platform (planned)

Cisco Networks App

### Collaboration

- Call Manager
- Spark
- AppDynamics

- ✓ Inaugural SIEM & Threat Defense Partner
- ✓ Inaugural pxGrid partner
- ✓ Inaugural member of Cisco Security Tech Alliances program
- ✓ Inaugural ACI Partner
- ✓ Inaugural Data Analytics Partner

- ✓ **CVD: Cisco UCS Integrated Infrastructure for Splunk Enterprise (Distributed Deployment, High Capacity)** ([link](#))
- ✓ **CVD: Cisco Application Centric Infrastructure with Splunk** ([link](#))
- ✓ Splunk on UCS Reference Architecture ([link](#))
- ✓ Cisco Cloud Security for VMDC 1.0 Design Guide ([link](#))



# Cisco Firepower & Splunk

---

Douglas Hurd / Cisco Security Technical Alliances





# Threat Defense Security

## Summary Dashboard (6.2.0)

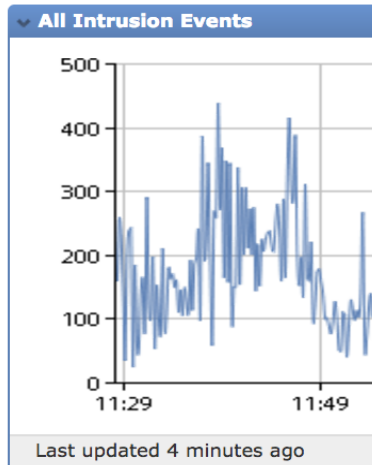
Provides a summary of activity on the appliance

Show the Last 1 hour

**Top Attackers**

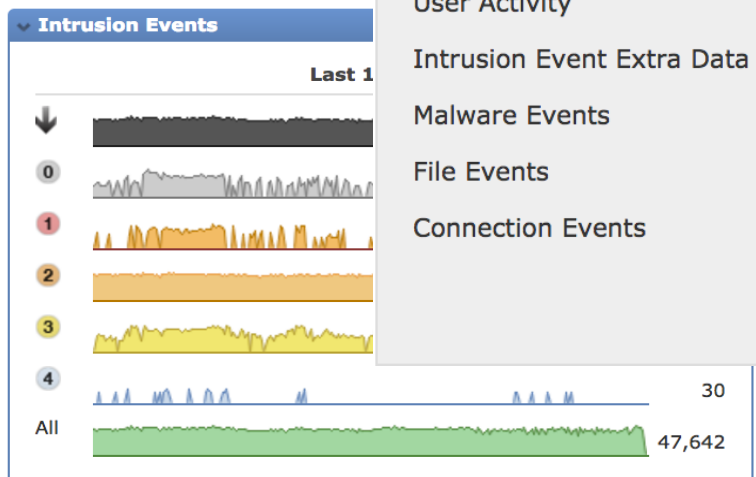
Source IP	Count
192.168.199.132	20,722
192.168.199.133	7,643
220.231.10.124	3,965
186.107.10.124	1,723
172.149.41.1	1,453
172.91.41.1	1,441
12.100.10.50	1,263
220.231.10.75	1,102
220.231.10.21	1,068
192.168.199.254	1,020

Last updated 4 minutes ago



**Top Targets**

Destination IP	Count
224.0.0.22	26,122
192.168.199.133	2,312
10.0.10.124	2,164
10.0.10.21	1,937
10.0.10.75	1,741
10.110.10.12	1,723
192.38.41.133	1,453
192.89.41.133	1,441
10.0.10.122	1,266
192.168.199.132	1,020



### eStreamer Event Configuration

Select the types of events that will be sent to connected eStreamer clients

- Discovery Events
- Correlation and White List Events
- Impact Flag Alerts
- Intrusion Events
- Intrusion Event Packet Data
- User Activity
- Intrusion Event Extra Data
- Malware Events
- File Events
- Connection Events

**Save**

+ Add Widgets

**by Application Protocol**

Application	Total Events
...	52,114
...	23,070
...	12,248
...	386
for IPv6	204
...	16
...	16
...	12
...	12
...	10

minutes ago

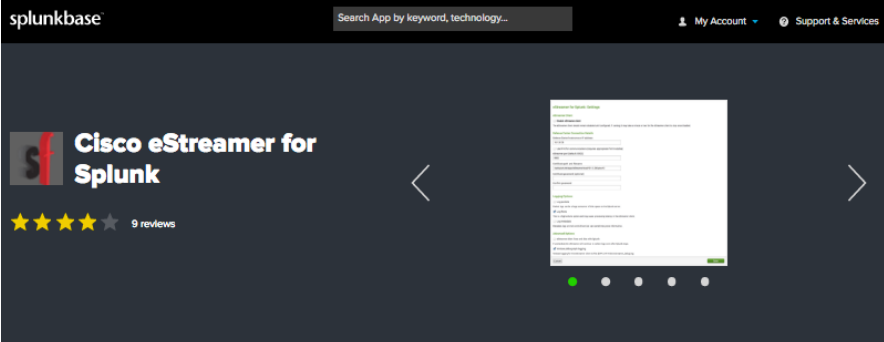
**Events by Application Protocol**

Application	Impact 1 Events
...	2,346
...	10



# Background on Firepower and Splunk

- ▶ Firepower-Splunk mutual customer base expanding
  - ASA to Firepower Threat Defense – More FMCs
- ▶ Add-Ons for Firepower available on Splunkbase
- ▶ Cisco's Firepower TA & App built in 2014, based on v.5.4
  - Over 6000 downloads
  - *Not recommended with FMC V6.x*
- ▶ 'Community Supported' model facing challenges
- ▶ Focused on new business model for this critical integration
- ▶ Resources directed at Firepower 6.x customers



The screenshot shows the Splunkbase interface for the 'Cisco eStreamer for Splunk' app. The app title is prominently displayed with a 4-star rating and 9 reviews. Below the title, there are statistics for 435 installs and 4,275 downloads, along with a 'LOGIN TO DOWNLOAD' button. The 'Overview' tab is selected, showing a description of the app's functionality: 'Sourcefire eStreamer log collection and comprehensive selection of dashboards optimized for Sourcefire System 5.2+ and Splunk 6.' It lists supported Sourcefire event types such as Intrusion Events, Malware Events, and File Events. A 'Release Notes' section is visible, detailing the 'Version: 2.2.2' released on Sept. 23, 2016, at 6:07 p.m., which is platform independent and compatible with Splunk versions 6.4, 6.1, and 6.0. The page also includes metadata like category (Security, Fraud & Compliance), product support (Splunk Enterprise), and content type (App).

**Overview** Details

Sourcefire eStreamer log collection and comprehensive selection of dashboards optimized for Sourcefire System 5.2+ and Splunk 6.

The supported Sourcefire event types are:

- Intrusion Events
- Intrusion Event Packet Data (optional)
- Intrusion Event Extra Data
- Malware Events
- File Events
- Connection Logs and Security Intelligence Events (optional)
- Correlation and White List Events
- Impact Flag Alerts
- Connection Events (optional)

Please note this app was developed for, and tested on, Unix platforms only. Windows support is not currently available.

This app is written and maintained by Sourcefire, now part of Cisco, but is only community supported – no official support is available. Be sure to visit the Documentation tab for initial assistance with setup, configuration, important notes, and a version change log.

eStreamer for Splunk is copyright © 2013-2014 Cisco and/or its affiliates. All rights reserved. Sourcefire is now part of Cisco.

**Release Notes** Version 2.2.2 ⌵

**Version: 2.2.2**

Sept. 23, 2016, 6:07 p.m.  
Platform Independent  
6.4, 6.1, 6.0

435 Installs 4,275 Downloads

[LOGIN TO DOWNLOAD](#)

VERSION  
2.2.2

CATEGORY  
Security, Fraud & Compliance

PRODUCT SUPPORT  
Splunk Enterprise

CONTENT TYPE  
App

SPLUNK VERSIONS  
6.4  
6.1  
6.0

LICENSING  
[Cisco eStreamer End User License Agreement](#)

PLATFORMS  
Platform Independent

COMMUNITY SUPPORTED  
[Questions on SplunkAnswers](#)  
[File a case](#)  
[Flag as inappropriate](#)

BUILT BY  
**douglas hurd**

[Subscribe](#) [Share](#)

# Background on Firepower and Splunk

- ▶ Firepower-Splunk mutual customer base expanding
  - ASA to Firepower Threat Defense – More FMCs
- ▶ Add-Ons for Firepower available on Splunkbase
- ▶ Cisco's Firepower TA & App built in 2014, based on v.5.4
  - Over 6000 downloads
  - *Not recommended with FMC V6.x*
- ▶ 'Community Supported' model facing challenges
- ▶ Focused on new business model for this critical integration
- ▶ Resources directed at Firepower 6.x customers

The screenshot shows the Splunkbase interface for the Cisco eStreamer eNCore Add-on for Splunk. The top navigation bar includes the Splunkbase logo, a search bar, and links for 'My Account', 'My Splunk', and 'Support & Services'. The main content area features the Cisco logo, the app name, and a 2-star rating. Below this is a blue bar with 'ADMINISTRATOR TOOLS: Manage App | View App | View Analytics'. The 'Overview' tab is active, displaying a description of the app as an eStreamer client with a Splunk plugin for event forwarding. It lists supported event types such as Discovery Events, Correlation and White List Events, Impact Flag Alerts, Intrusion Events, and Malware Events. A note states that the app is for Linux platforms only. On the right, there are statistics for 105 installs and 324 downloads, along with 'Download' and 'Rate this App' buttons. Further down, it shows the version (3.0.0), the developer (douglas hurd), and compatibility information for Splunk Enterprise products and versions (6.6, 6.5).





# New Cisco eStreamer 'eNcore' for Splunk

- ▶ Scalable app with major improvements
- ▶ TAC Support option will be offered
  - Free for customers that do not want TAC support
  - Chargeable for customers that want TAC support
- ▶ Official GA Release: End of June
- ▶ Beta II underway during May thru June 2017
- ▶ PID: FP-SPLUNK-SW-K9
- ▶ Description: "Cisco eStreamer eNcore for Splunk"
  - Software downloads: [software.cisco.com](http://software.cisco.com)

	Free Version	Pay Version
App Cost	Free	\$\$\$
Community Support	Yes	Yes
TAC Support	No	Yes
App Updates	Yes	Yes

# Improvements and Enhancements

Feature	Benefit
Built from scratch in Python	<ul style="list-style-type: none"> <li>No Perl dependencies</li> <li>Python very popular</li> <li>Completely up to date with entire 6.2 API schema</li> </ul>
Multi-process	<ul style="list-style-type: none"> <li>Highly scalable</li> </ul>
Multi-FMC Support	<ul style="list-style-type: none"> <li>Connect multiple FMCs to one instance</li> <li>Reduce complexity</li> </ul>
Fully Qualified Event Output	<ul style="list-style-type: none"> <li>Encoded event info is written out in text</li> </ul>
Event de-duplication (Future)	<ul style="list-style-type: none"> <li>Avoid paying Splunk for redundant event data</li> <li>Gives Firepower HA configurations more flexibility</li> </ul>
TAC Supported option available	<ul style="list-style-type: none"> <li>End to End support for Firepower Splunk customers</li> </ul>
Forward Compatible	<ul style="list-style-type: none"> <li>Ongoing maintenance to support new eStreamer API versions</li> </ul>



# Cisco Cloud Security and Splunk

---

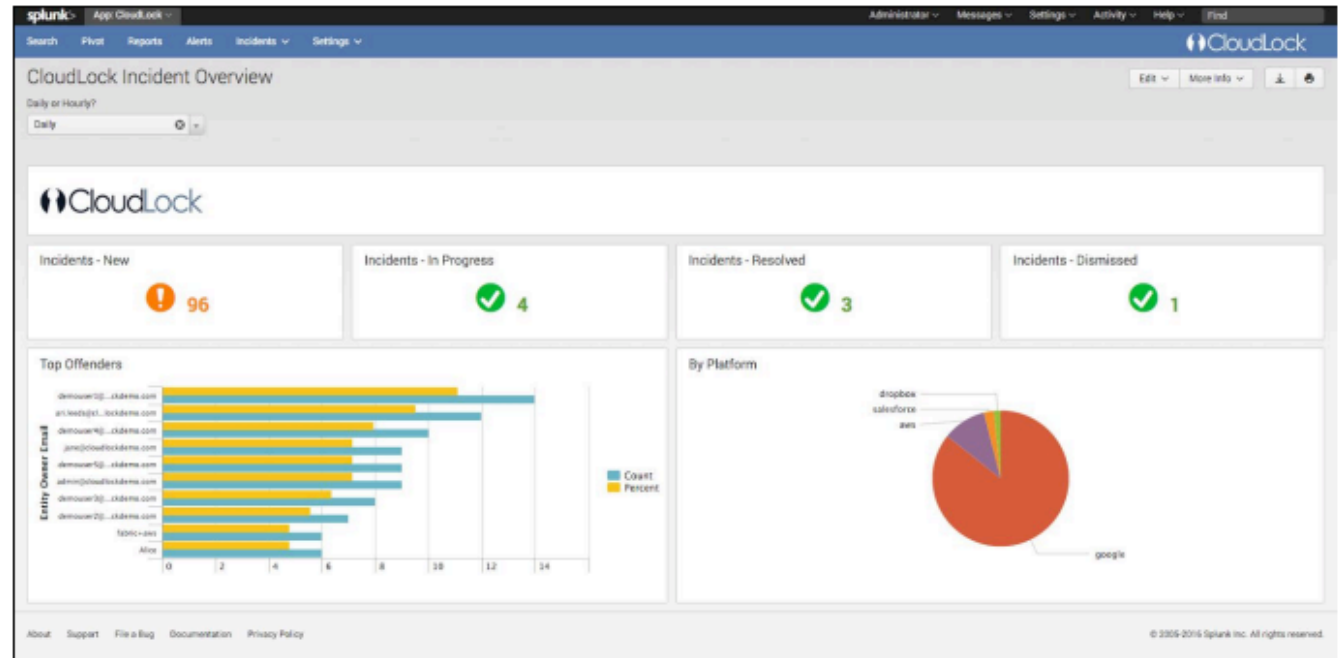




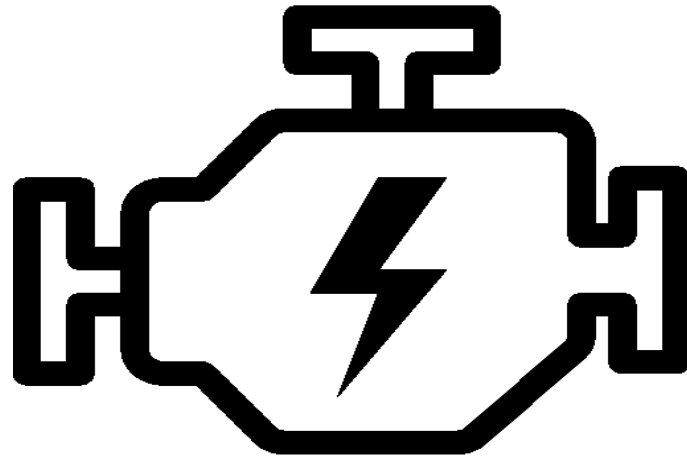


# Splunk App for Cisco Cloudlock

- ▶ Manage Cloud Security incidents within Splunk
- ▶ Seamless extend Security Operations to cloud environments while maintaining existing workflows
- ▶ Leverage Splunk's rich data visualization, alerting and reporting functionality
- ▶ Two leaders - Partnership Strength

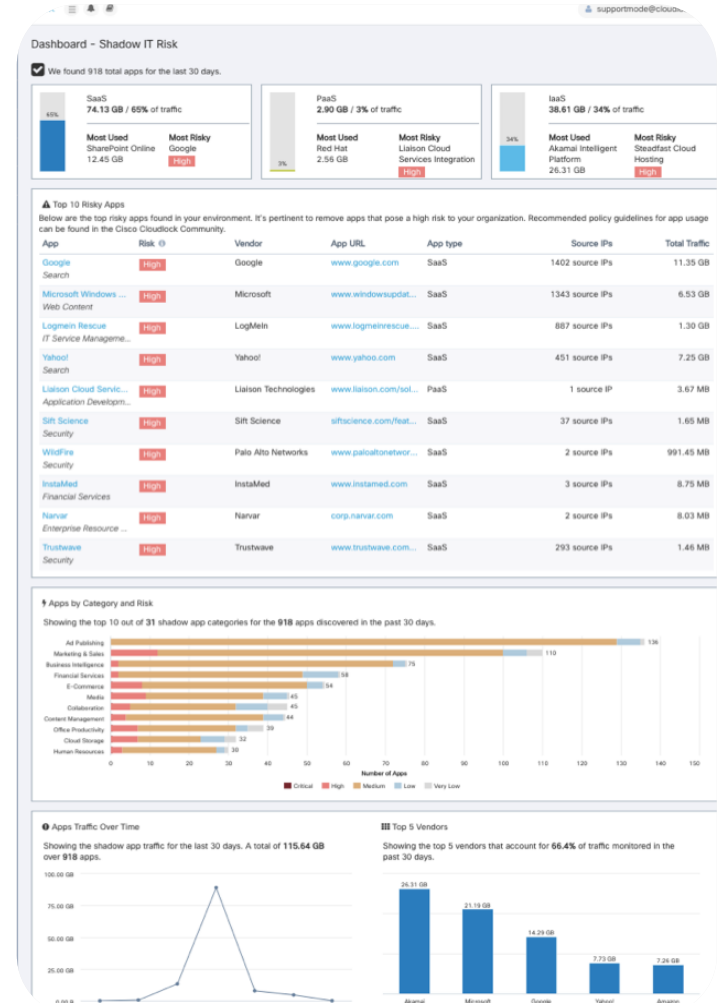


# ShadowIT for Cisco FP and Splunk Customers



SIEM: **splunk**>

**DESIGNED TO SUPPORT ANY DATA SOURCE**



# Correlating Network And Infrastructure Data Around The World

Using open APIs monitor and manage connectivity and security for the largest Latin American country

Colin Lowenberg







### Resumen del Mes

Presenta Indicadores de Usabilidad tales como: Cuántos Usuarios (dispositivos) utilizan México Conectado, Cuánto Ancho de Banda consumen, Qué tipo de Aplicaciones utilizan, Qué páginas visitan. Se presenta el resumen del Mes en curso. Universo de Sitios: 40,100

Cuántos Usuarios se Conectan en Total:

# 3,841,279 Usuarios Únicos

El número representa la suma de los dispositivos únicos en el periodo de tiempo especificado. Se realiza el supuesto de que un dispositivo es igual a un usuario.

Cuánto Ancho de Banda se Consumió de Internet:

# 172.8 TeraBytes

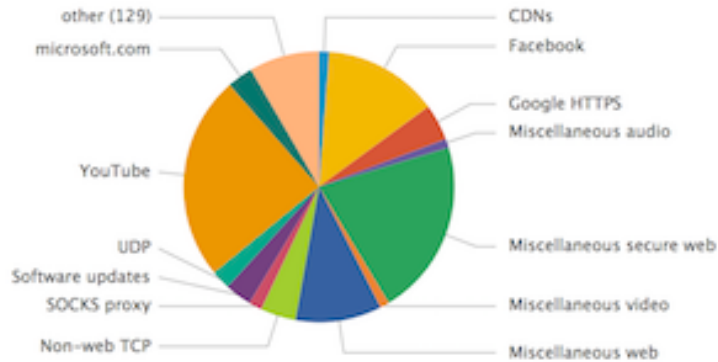
Suma del Tráfico Recibido en el periodo de tiempo.

Cuánto Ancho de Banda se Generó hacia Internet:

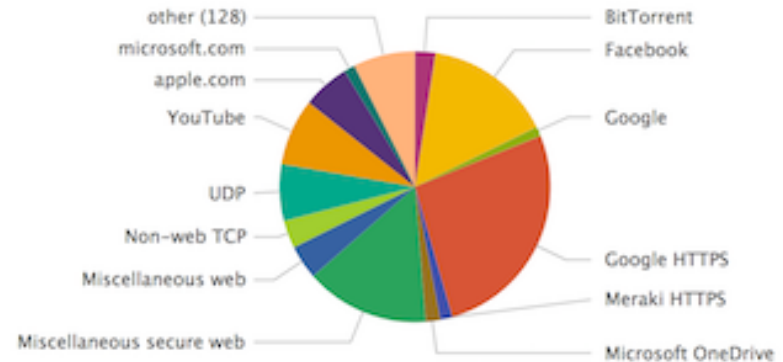
# 20.2 TeraBytes

Suma del Tráfico Enviado en el periodo de tiempo.

Cuánto Tráfico se Recibe por Tipo de Aplicación:



Cuánto Tráfico se Envía por Tipo de Aplicación:



# Smart Cities & Government Analytics

## The Mexico Conectado Project

### Country Digitization Analytics Platform

### CDAP

(powered by Splunk)



# Your Splunk Environment: Better on Cisco UCS

---

Automate deployment, correlate with your entire datacenter, and optimize for management and scalability

With Karthik Karupasamy

# Cisco UCS Add-On for Splunk Enterprise

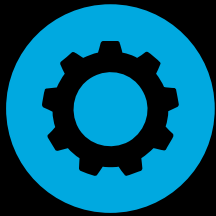
---





# Cisco Unified Computing System

A differentiated, revolutionary approach



## Simplified Architecture

---

- ▶ Networking with fewer components
- ▶ Lower cost and easier scaling
- ▶ Fewer management touch points
- ▶ Stateless: any resource, any time
- ▶ Better TCO/ROI



## Unified Management

---

- ▶ Faster deploy/provision
- ▶ Unification leads to reduced complexity
- ▶ Management via a single interface



## Higher Performance

---

- ▶ Brings out the best of x86 architecture
- ▶ Optimized resource utilization for compute, networking, and management

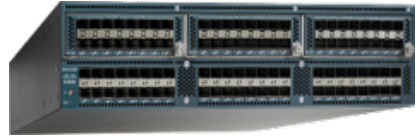


## Scale

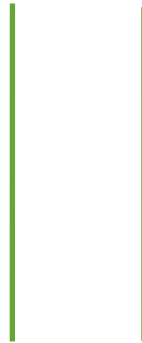
---

- ▶ Ultimate Scalability  
Enhanced design capability
- ▶ Designed for the future, today

# Cisco UCS Integrated Infrastructure for Big Data Topology



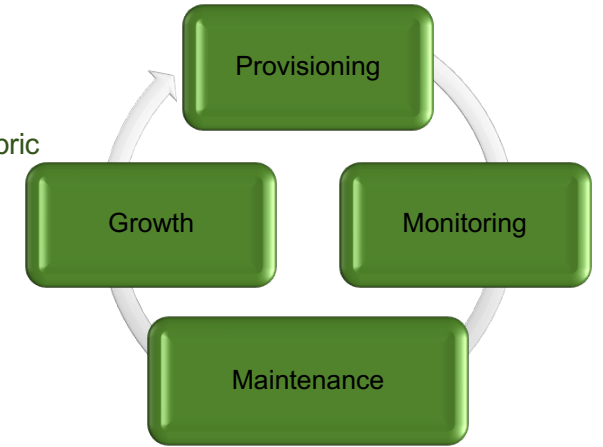
Support for direct connectivity to Fabric Interconnects



SingleConnect: LAN, SAN and Management




UCS 6200 and 6300 Series Fabric Interconnects, Installed in pairs, active-active. UCS Manager is embedded



Pre-tested and pre-validated configuration

Fabric-based infrastructure integrates computing, networking, and storage resources

Designed for high performance and availability



# Cisco UCS Director Express for Big Data

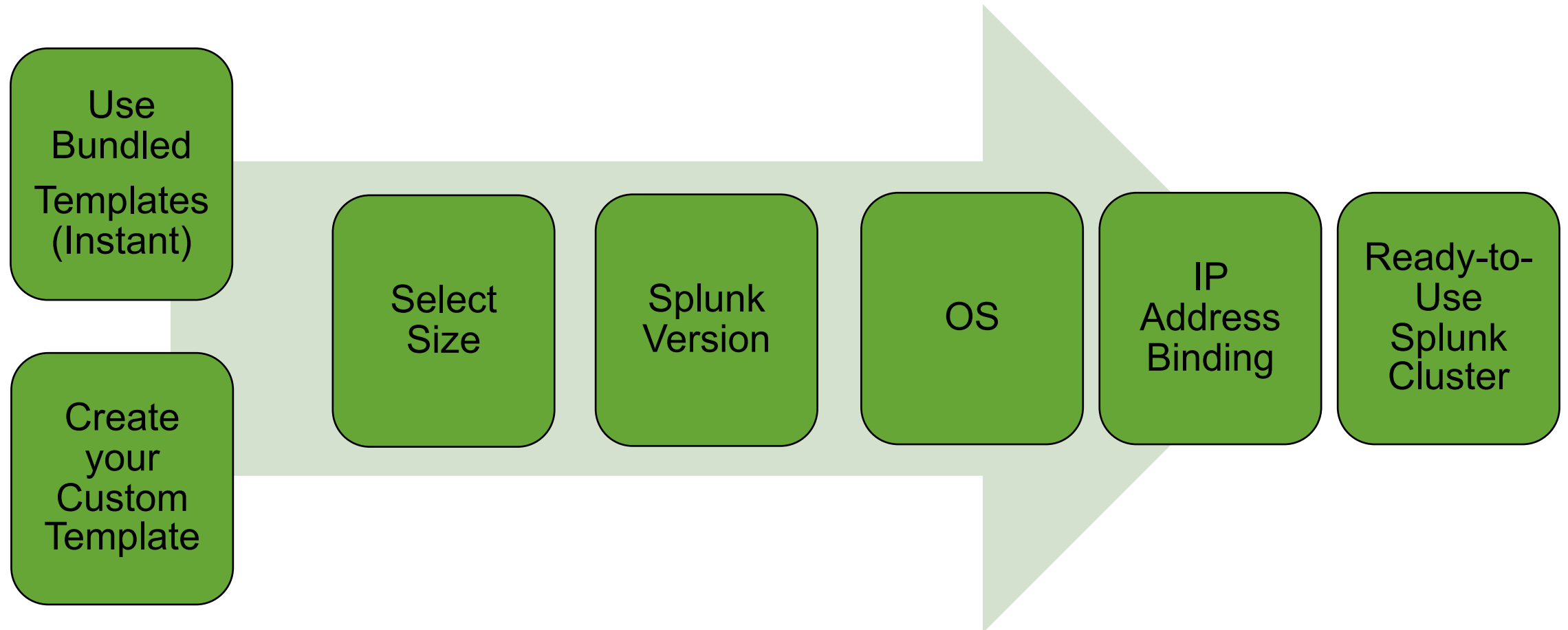
---





# UCSD Express For Big Data – Two Ways to Create

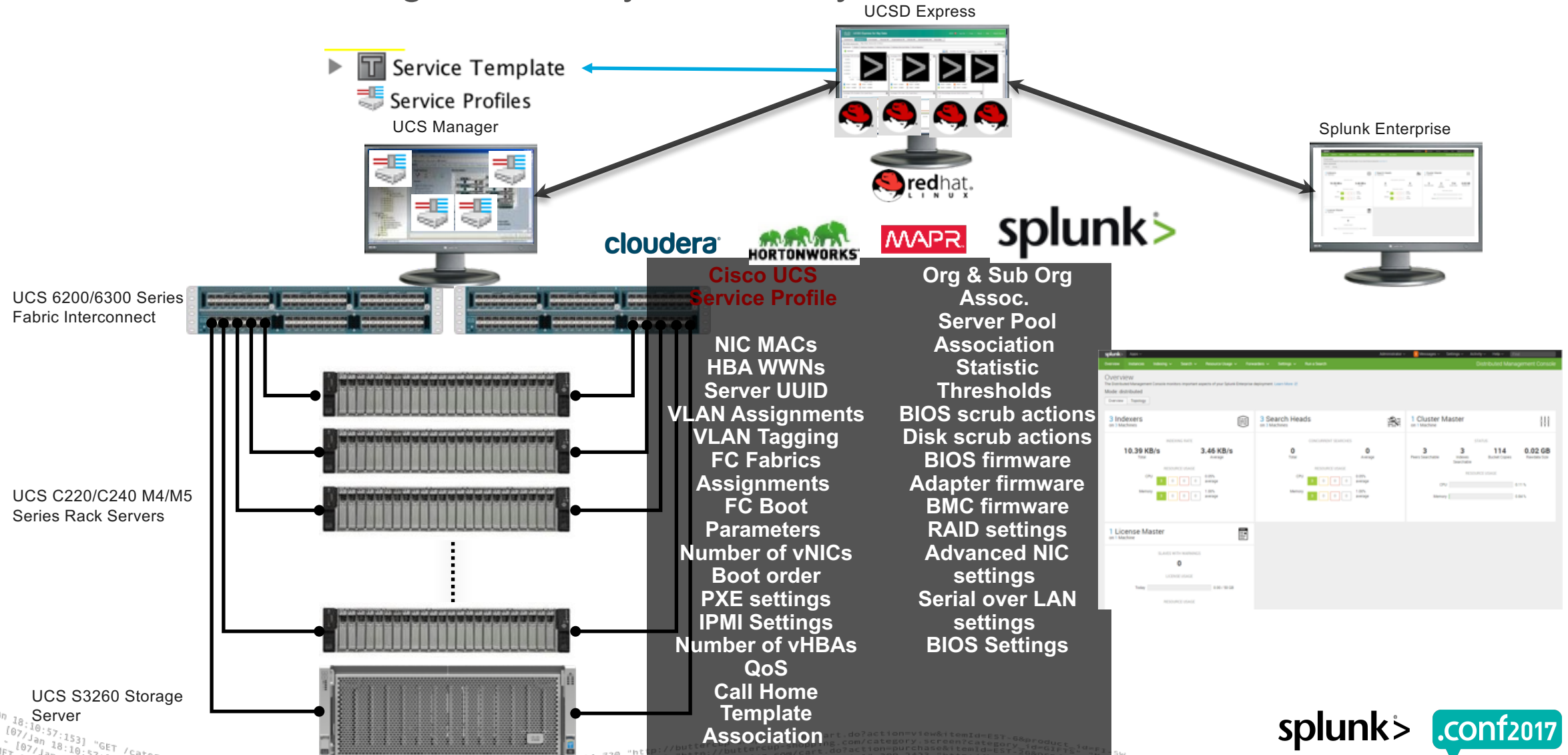
Unified Management Platform for Highly Available Distributed Splunk Clusters





# Unified Management with UCS Director Express for Big Data

## Programmability, Scalability and Automation





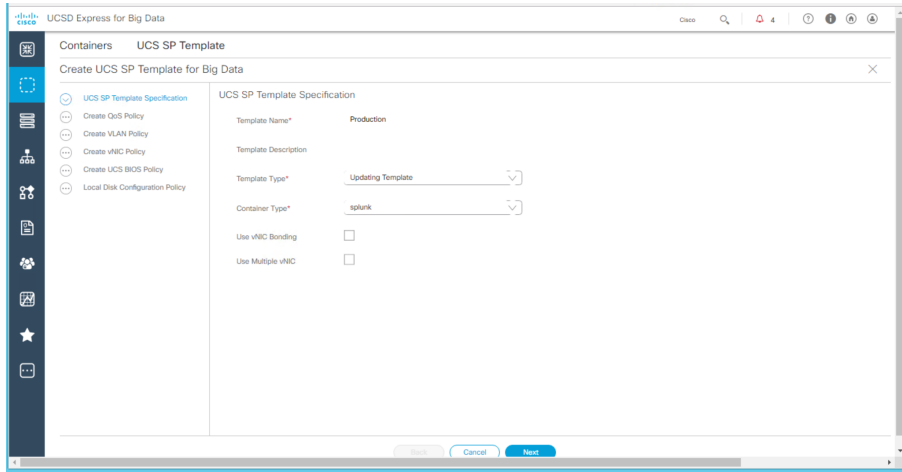


# Creating and Managing Splunk clusters

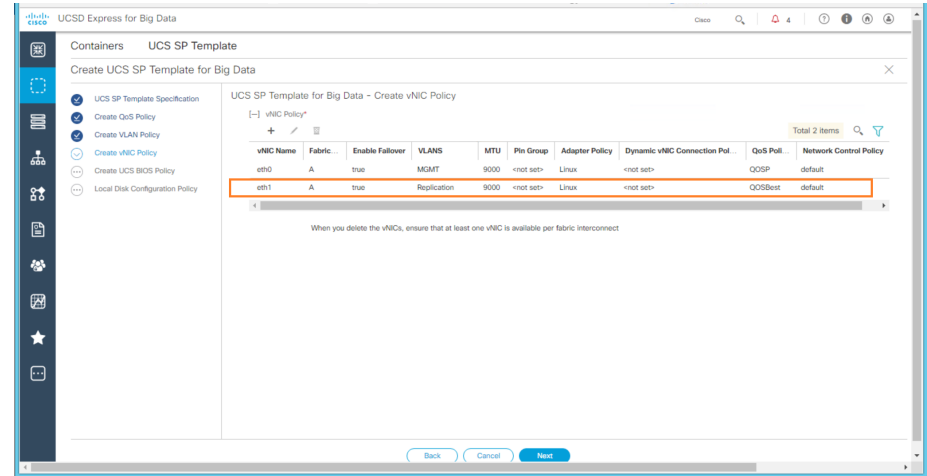
---

# Splunk Cluster customizations

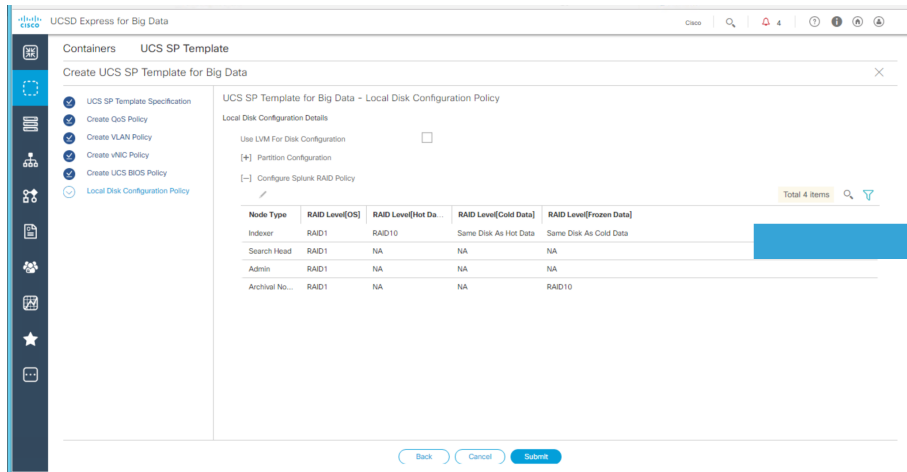
## Select physical infrastructure options



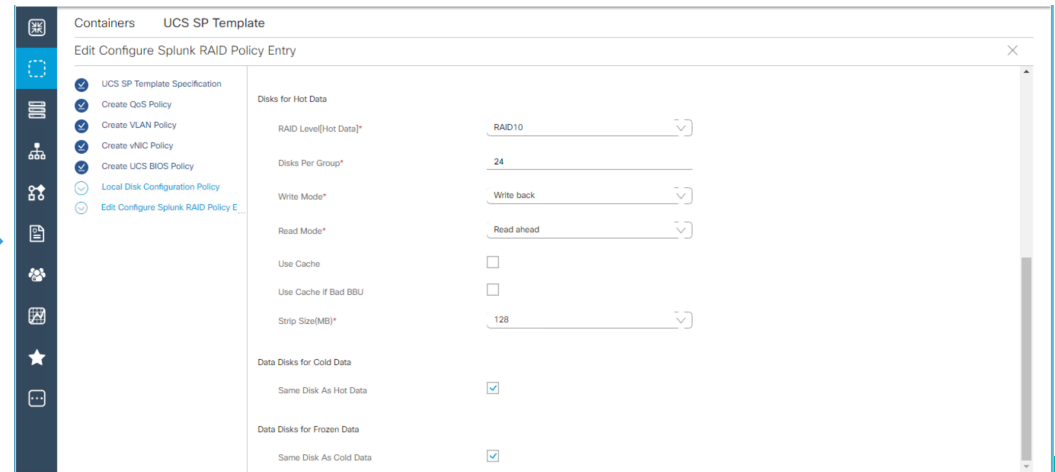
## Optionally add another NIC for Replication Traffic



## Select custom RAID policy for each Role



## Customize Storage Tiers



# Creating a Splunk cluster

- ▶ Cluster Name
- ▶ OS (RHEL)
- ▶ Splunk version
- ▶ UCS Manager
- ▶ Organization

The screenshot displays the 'Customized Splunk Cluster Creation' form within the Cisco UCS Express for Big Data interface. The form includes the following fields and options:

- Big Data Account Name\***: prod1 (Note: Enter Big Data Account Name with atmost 10 alphanumeric characters)
- UCSM Policy Name Prefix\***: prod1 (Note: Enter UCSM Policy Name Prefix with atmost 5 alphanumeric characters)
- SSH (root) Password\***: .....
- Confirm SSH Password\***: .....
- Splunk Manager Password\***: .....
- Confirm Splunk Manager Password\***: .....
- OS Version\***: RHEL7.2 (Note: Choose RHEL6.5 or later for M4 servers)
- Splunk Distribution Version\***: splunk-6.5.2
- Multi UCSM**:
- UCS Manager Account\***: UCSM1
- Organization\***: root

At the bottom of the form, there are buttons for 'Cancel' and 'Submit', and a link for '[+] UCS SP Template'.



# Creating a Splunk Cluster

- ▶ Server-pools (per role)
- ▶ Map vNIC to IP-Pools.
  - Mgmt, (and ingest)
  - Data1 for Replication (optional),

▶ Click **Submit**

Replication  
Factor,  
Search  
Factor

PXE VLAN

Server  
Pools

Networking

UCSD Express for Big Data

Containers Cluster Deploy Templates

Customized Splunk Cluster Creation

UCS Manager Account\* UCSM1

Organization\* root

[+] UCS SP Template

PXE VLAN ID\* 104  
[4048-4093],[1-3967]

Replication Factor\* 2

Search Factor\* 2

[-] Splunk Server Roles\*

Node Type	Node Count	Host Name Pre...	Validate Page	SSD Boot Drives Available for ...	Search Head to be part of clus...	Deploy
Indexer	4	prod-idx	false	false	true	true
Search Head	3	prod-srch	false	false	true	true
Admin	1	prod-admin	true	false	true	true
Archival No...			false	false	false	true

[-] vNIC Template\*

vNIC Name	IP Pool	MAC Address Pool	VLAN ID
eth0	Pool1:50.1.1.1	Mgmt	101
eth1	Pool2:0.0.0.0	Data1	220

When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool and VLAN ID to the first vNIC in the vNIC Template table.

Cancel Submit

# Creating a Splunk Cluster -- Server Pool Selection

Server Count

Server Pools

Hostname Prefix

Containers Cluster Deploy Templates

Edit Splunk Server Roles Entry

Node Type Indexer

Node Count\* 4

Host Name Prefix\* prod-idx

[ - ] Server Pool\* (UCSM1;org-root/compute-pool-Indexer;5)

ID	Server Pool	Server Pool Policy Qualificati...	Assign...	Size
<input type="checkbox"/> UCSM1;org-root/compute-pool-default;0	default		1	1
<input type="checkbox"/> UCSM1;org-root/compute-pool-ucs;8	ucs		3	11
<input type="checkbox"/> UCSM1;org-root/compute-pool-960gb-ssd;0	960gb-ssd		1	1
<input checked="" type="checkbox"/> UCSM1;org-root/compute-pool-Indexer;5	Indexer		2	7
<input type="checkbox"/> UCSM1;org-root/compute-pool-Search;4	Search		2	6
<input type="checkbox"/> UCSM1;org-root/compute-pool-Admin;1	Admin		1	2
<input type="checkbox"/> UCSM1;org-root/compute-pool-C220;3	C220		2	5
<input type="checkbox"/> UCSM1;org-root/compute-pool-Admin1;1	Admin1		0	1
<input type="checkbox"/> UCSM1;org-root/compute-pool-rack6-13;7	rack6-13		1	8

Total 15 items

Cancel Submit

# Creating a Splunk Cluster -- vNIC configuration

- ▶ Map vNIC to IP-Pools.

**NOTE:** eth0 → MGMT pool binding shown.

- ▶ Click **Submit**

Containers Cluster Deploy Templates

Edit vNIC Template Entry

vNIC Name eth0

IP Pool\* Pool1(50.1.1.150 - 50.1.1.180)

MAC Address Pool\* Mgmt (503)

VLAN ID\* 101

[4048-4093],[1-3967]

(MGMT VLAN)

Cancel Submit

UCSD Express for Big Data

Containers Cluster Deploy Templates

Customized Splunk Cluster Creation

UCS Manager Account\* UCSM1

Organization\* root

[+] UCS SP Template

PXE VLAN ID\* 104

[4048-4093],[1-3967]

Replication Factor\* 2

Search Factor\* 2

[-] Splunk Server Roles\*

Node Type	Node Count	Host Name Pre...	Validate Page	SSD Boot Drives Available for ...	Search Head to be part of clus...	Deploy
Indexer	4	prod-idx	false	false	true	true
Search Head	3	prod-srch	false	false	true	true
Admin	1	prod-admin	true	false	true	true
Archival No...			false	false	false	true

Total 4 items

[-] vNIC Template\*

vNIC Name	IP Pool	MAC Address Pool	VLAN ID
eth0	Pool1:50.1.1.1	Mgmt	101
eth1	Pool2:0.0.0.0	Data1	220

When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool and VLAN ID to the first vNIC in the vNIC Template table.

Cancel Submit



# Splunk UCS HW Template – RAID Policy

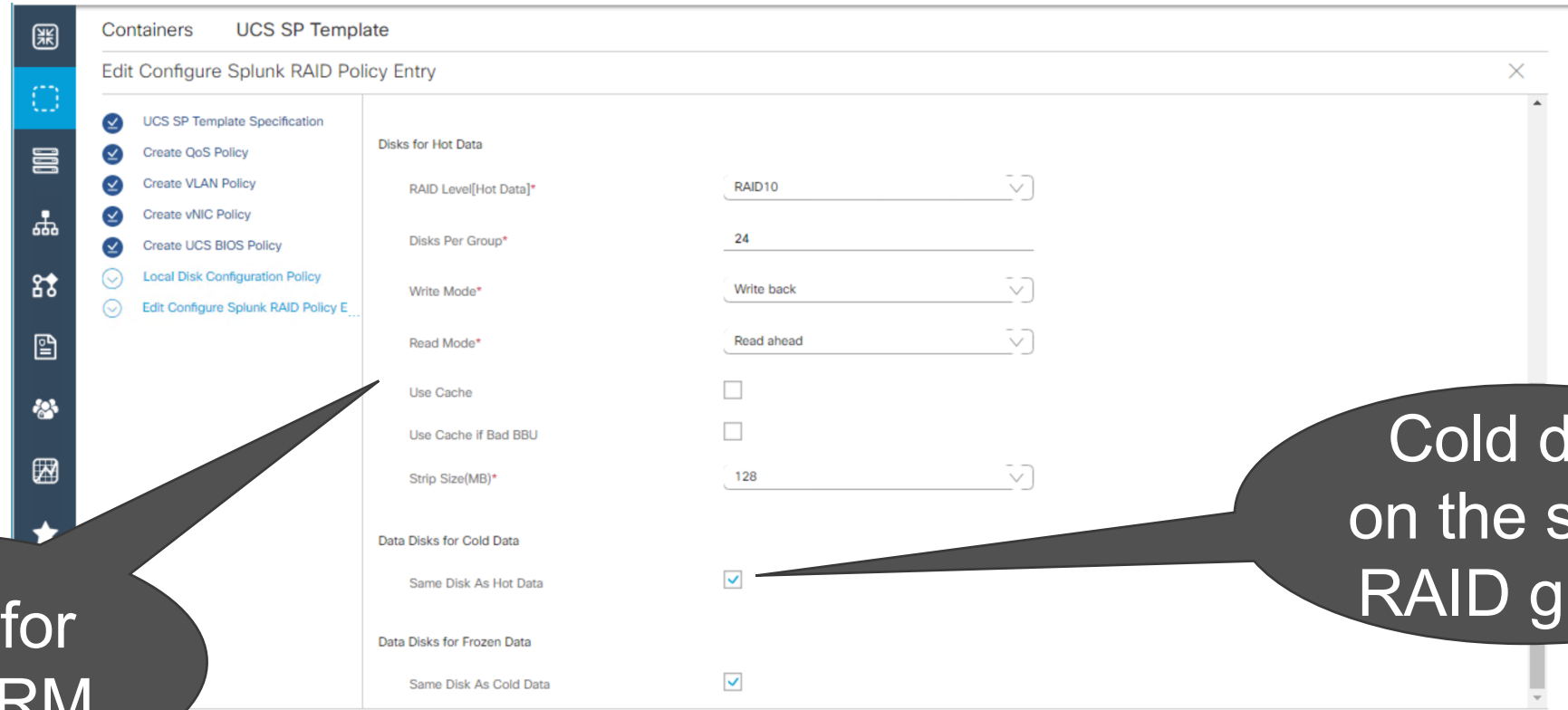
The screenshot shows the 'UCS SP Template' configuration page in Splunk. The main heading is 'Modify UCS SP Template for Big Data'. The left sidebar contains a list of configuration options, with 'Local Disk Configurati...' selected. The main content area is titled 'UCS SP Template for Big Data - Local Disk Configuration Policy' and shows 'Local Disk Configuration Details'. A checkbox for 'Use LVM For Disk Configuration' is present. Below it is a 'Partition Configuration' section with a table of mount points and sizes. At the bottom, there is a section for 'Configure Splunk RAID Policy' with 'Back', 'Cancel', and 'Submit' buttons.

Mount Po...	Size(GB)
/boot	1
/	1 with grow
/tmp	5
/var/tmp	5
swap	2
/home	5

Custom Partitions

RAID Policy

# Splunk UCS HW Template – Inside the RAID Policy



RAID10 for HOT/WARM

Cold data on the same RAID group

# Splunk UCS HW Template – Inside the RAID Policy

The screenshot shows the 'Edit Configure Splunk RAID Policy Entry' window in the UCS SP Template configuration tool. The interface is divided into three sections for different data states: 'Hot Data', 'Cold Data', and 'Frozen Data'. Each section has a 'RAID Level' dropdown menu, a 'Disks Per Group' input field, and 'Write Mode' and 'Read Mode' dropdown menus. There are also checkboxes for 'Use Cache' and 'Use Cache If Bad BBU', and a 'Strip Size(MB)' input field. The 'Same Disk As Cold Data' checkbox is checked, and the 'Same Disk As Cold Data' checkbox is also checked.

Section	RAID Level	Disks Per Group	Write Mode	Read Mode	Use Cache	Use Cache If Bad BBU	Strip Size(MB)	Same Disk As [Data State]
Hot Data	RAID10	16	Write back	Read ahead	<input type="checkbox"/>	<input type="checkbox"/>	128	
Cold Data	RAID5	8	Write back	Read ahead	<input type="checkbox"/>	<input type="checkbox"/>	128	
Frozen Data								<input checked="" type="checkbox"/>

RAID10 for HOT/WARM

RAID5 for COLD



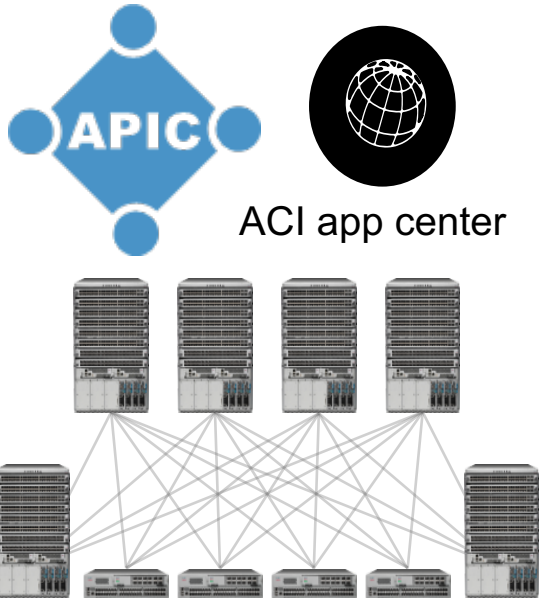


# ACI and Tetration

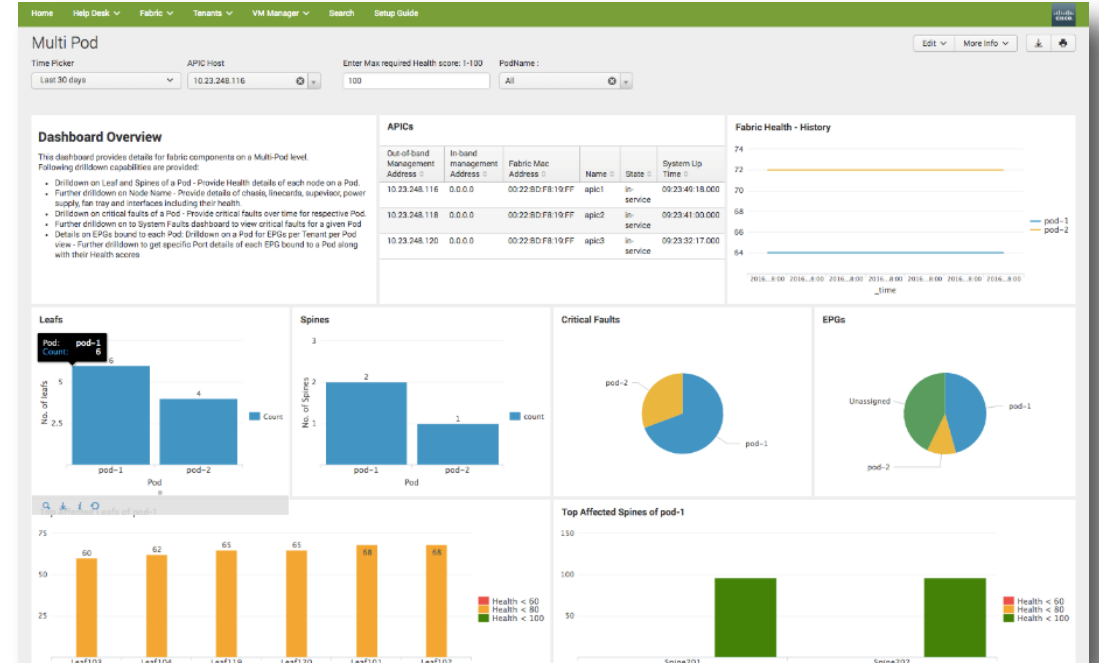
---

# Aci-splunk: What Is New?

## Cisco ACI App & Add-on for Splunk Enterprise version 4.0 – Splunk Certified



**Splunk Certified**  
Available on splunkbase



Supported on APIC 1.3 and higher

Compatible with Splunk 6.4 & above

Multiple APIC monitoring

Multi-Pod visibility

Micro-Segmentation support

Enhanced user interface with drill down capabilities

ACI App Center integration

# Tetration Analytics App for Splunk

Cisco Tetration App & Add-on for Splunk Enterprise version 1.0



Tetration App for Splunk V1.0

Use Tetration APIs to receive ADM, Endpoints, Inventory data



Cisco Tetration Analytics

Send Configuration data, health & performance metrics, syslog and fault information

Enforce policies using Tetration sensors

Real-time Application Monitoring

Accelerated RCA & deeper visibility

Policy Enforcement



# Why You Never See Tacos Mounted On Drones In The Real World

Wrapping up the Cisco and Splunk innovation story  
With Robert Novak

# Thank You

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

splunk> .conf2017

# Supplemental Information



Cisco Technology	Description	SplunkBase URL
<b>Cisco Security Suite</b>	The Cisco Security Suite provides a single pane of glass interface into Cisco security data.	<a href="https://splunkbase.splunk.com/app/525/">https://splunkbase.splunk.com/app/525/</a>
<b>Cisco Firepower™ Management Center</b>	Splunk Add-on for Cisco FirePower Management Center leverages data collected via Cisco eStreamer to allow a Splunk Admin to analyze and correlate reports from Cisco through the Splunk Common Information Model.	<a href="https://splunkbase.splunk.com/app/1808">https://splunkbase.splunk.com/app/1808</a>
<b>Cisco eNcore for Splunk</b>	Comprehensive eStreamer ‘Client’ or Splunk ‘TA’ that collects all ten event types in their entirety from Firepower Management Center 6.x	<a href="https://splunkbase.splunk.com/app/3662/">https://splunkbase.splunk.com/app/3662/</a>
<b>Cisco Umbrella</b>	Automatically enrich security alerts inside Splunk, allowing analysts to discover the connections between the domains, IPs, and file hashes in an attacker’s infrastructure	<a href="https://splunkbase.splunk.com/app/3324/">https://splunkbase.splunk.com/app/3324/</a>
<b>Cisco ISE</b>	Splunk App for Cisco ISE. Collects data from ISE via Syslog and provides Adaptive Network Control (ANC) Mitigation Actions via pxGrid.	<a href="https://splunkbase.splunk.com/app/1589/">https://splunkbase.splunk.com/app/1589/</a> <a href="https://splunkbase.splunk.com/app/1915/">https://splunkbase.splunk.com/app/1915/</a>
<b>Cisco CloudLock</b>	The CloudLock Cloud Access Security Broker harnesses crowd-sourced, actionable cybersecurity intelligence to enable enterprises to securely leverage the cloud.	<a href="https://splunkbase.splunk.com/app/3043/">https://splunkbase.splunk.com/app/3043/</a> <a href="https://www.cloudlock.com/blog/tag/cloudlock-for-splunk/">https://www.cloudlock.com/blog/tag/cloudlock-for-splunk/</a>
<b>Cisco eStreamer</b>	eStreamer log collection and comprehensive selection of dashboards optimized for Sourcefire System 5.2+ and Splunk 6.	<a href="https://splunkbase.splunk.com/app/1629/">https://splunkbase.splunk.com/app/1629/</a>
<b>Cisco IPS</b>	The Splunk Add-on for Cisco IPS allows a Splunk software administrator to consume, analyze, and report on Cisco IPS data that conforms to the Security Device Event Exchange (SDEE) standard.	<a href="https://splunkbase.splunk.com/app/1903">https://splunkbase.splunk.com/app/1903</a>
<b>Cisco CWS</b>	The Cisco Cloud Web Security (CWS) Add-on for Splunk allows a Splunk administrator to analyze and correlate Cisco Cloud Web Security (CWS) log data through the Common Information Model in Splunk Enterprise	<a href="https://splunkbase.splunk.com/app/2791">https://splunkbase.splunk.com/app/2791</a>
<b>Cisco ESA</b>	The Splunk Add-on for Cisco ESA allows a the Splunk software administrator to leverage Textmail, HTTP, and Authentication logs of Cisco ESA.	<a href="https://splunkbase.splunk.com/app/1761">https://splunkbase.splunk.com/app/1761</a>
<b>Cisco AnyConnect</b>	The Cisco AnyConnect Network Visibility (NVM) App for Splunk allows IT administrators to analyze and correlate user and endpoint behavior in Splunk Enterprise.	<a href="https://splunkbase.splunk.com/app/2992/">https://splunkbase.splunk.com/app/2992/</a>
<b>Cisco ASA</b>	The Splunk Add-on for Cisco ASA allows a Splunk software administrator to map Cisco ASA devices, Cisco PIX, and Cisco FWSM events to the Splunk CIM.	<a href="https://splunkbase.splunk.com/app/1620">https://splunkbase.splunk.com/app/1620</a>