



Apache Knox - Hadoop Security Swiss Knife

Krishna Pandey, CISSP , CCSP

Staff Software Engineer (Platform Security)

Larry McCay

Senior Manager (Security Architecture) &
Knox PMC chair, Ranger, Metron and Hadoop committer

I know what happened, since last summer...

- Over 53,000 Incidents [1]
- 2,216 Confirmed Data Breaches [2]x
- Formjacking – 48,000 unique websites on average/month [3]
- Crypto-jacking [reduced by 52% in 2018] [4]
- Penalties for non-compliance – GDPR
- More CVEs to patch – CVE-2019-5736, CVE-2018-8009, ...
- Meltdown, Spectre, Foreshadow, ..., Spoiler

Source: [1] [2] <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

[3] [4]: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en-apj.pdf>



What This Means to Big Data Landscape?

← → C https://www.shodan.io/search?query=port%3A"50070"+org%3A"amazon.com"

SHODAN port:"50070" org:"amazon.com" Explore Downloads Reports Developer Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 966

TOP COUNTRIES

United States 786
Germany 35
Japan 34
Brazil 31
Australia 25

TOP ORGANIZATIONS

Amazon.com 966

TOP OPERATING SYSTEMS

Linux 3.x 1

TOP PRODUCTS

HDFS NameNode 18
osiris host IDS agent 3
OpenSSH 1

████████.155 ↗
ec2-████████.155.compute-1.amazonaws.com
Amazon.com
Added on 2019-02-18 08:00:35 GMT
United States, Ashburn
cloud

HTTP/1.1 200 OK
Server: miniupnpd/1.0 UPnP/1.0
Content-Type: text/xml
Content-Length: 828
Date: Mon, 18 Feb 2019 08:08:35

Namenode information ↗
████████.158 ec2-████████.158.us-west-2.compute.amazonaws.com
Amazon.com
Added on 2019-02-18 07:25:29 GMT
United States, Boardman
Technologies:
closed

HTTP/1.1 200 OK
Cache-Control: no-cache
Expires: Mon, 18 Feb 2019 07:26:28 GMT
Date: Mon, 18 Feb 2019 07:26:28 GMT
Pragma: no-cache
Expires: Mon, 18 Feb 2019 07:26:28 GMT
Date: Mon, 18 Feb 2019 07:26:28 GMT
Pragma: no-cache
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIG...

████████.172 ↗
ec2-████████.172.ap-northeast-1.compute.amazonaws.com
Amazon.com
Added on 2019-02-18 07:39:42 GMT
Japan, Tokyo
cloud

████████.75 ↗
ec2-████████.75.compute-1.amazonaws.com
Amazon.com
Added on 2019-02-18 08:34:01 GMT
United States, Ashburn
cloud

HTTP/1.1 200 Ok
Server: miniupnpd/1.0 UPnP/1.0
Content-Type: text/xml
Content-Length: 828
Date: Mon, 18 Feb 2019 08:34:01

Hadoop NameNode&nbspip-████████.1.us-west-1.compute.internal:8020 ↗

Fig.2 Publicly accessible WebHDFS cluster

Not Secure | ce98.le535.le557.le573.50070.nl4.gsr.awhoer.net/dfshealth.html#tab-overview

Hadoop Overview Datanodes Datanode Volume Failures Snapshot Show Startup Progress Utilities

Overview

ceig6-98-535-557-573.jeyw-aiwx-6.pegsqtyxi.jeeqedsreaw.legsq.900
(active)

Started:	Sat Jan 26 21:27:12 +0530 2019
Version:	2.9.1, re30710aea4e6e55e69372929106cf119af06fd0e
Compiled:	Mon Apr 16 15:03:00 +0530 2018 by root from branch-2.9.1
Cluster ID:	CID-dfa2961c-f121-491a-aecc-406c31a7ad7f
Block Pool ID:	BP-933667155-le516.ce75.ce78.ce86.nl4.gsr.awhoer.net-1540811254633

Summary

Security is off.

Safemode is off.

1,915,667 files and directories, 1,100,923 blocks = 3,016,590 total filesystem object(s).

Heap Memory used 415.13 MB of 448 MB Heap Memory. Max Heap Memory is 889 MB.

Non Heap Memory used 86.43 MB of 87.94 MB Committed Non Heap Memory. Max Non Heap Memory is <unbounded>.

Configured Capacity:	2.88 TB
DFS Used:	1.89 TB (65.55%)
Non DFS Used:	51.39 GB
DFS Remaining:	965.41 GB (32.7%)
Block Pool Used:	1.89 TB (65.55%)
DataNodes usages% (Min/Median/Max/stdDev):	65.55% / 65.55% / 65.55% / 0.00%
Live Nodes	3 (Decommissioned: 0, In Maintenance: 0)
Dead Nodes	0 (Decommissioned: 0, In Maintenance: 0)
Decommissioning Nodes	0

Upload File

Choose Files No file chosen

Close Upload

Go!

Search:

Show 25 entries

Permission Owner Group Size Last Modified Replication Block Size Name

drwxr-x-x ec2-user supergroup 0 B Jan 16 19:21 app

-rw-r--r-- panusr supergroup 9.36 KB Jan 08 11:23 data

drwxr-x-x panusr supergroup 0 B Jan 16 19:21 home

drwxr-x-x panusr supergroup 0 B Jan 08 11:12 test

drwxrwx-wx panusr supergroup 0 B Dec 20 00:36 tmp

drwxr-x-x panusr supergroup 0 B Jan 24 17:11 user

drwxr-x-x panusr supergroup 0 B Dec 05 13:22 user

Showing 1 to 7 of 7 entries

Previous 1 Next

Hadoop, 2018.

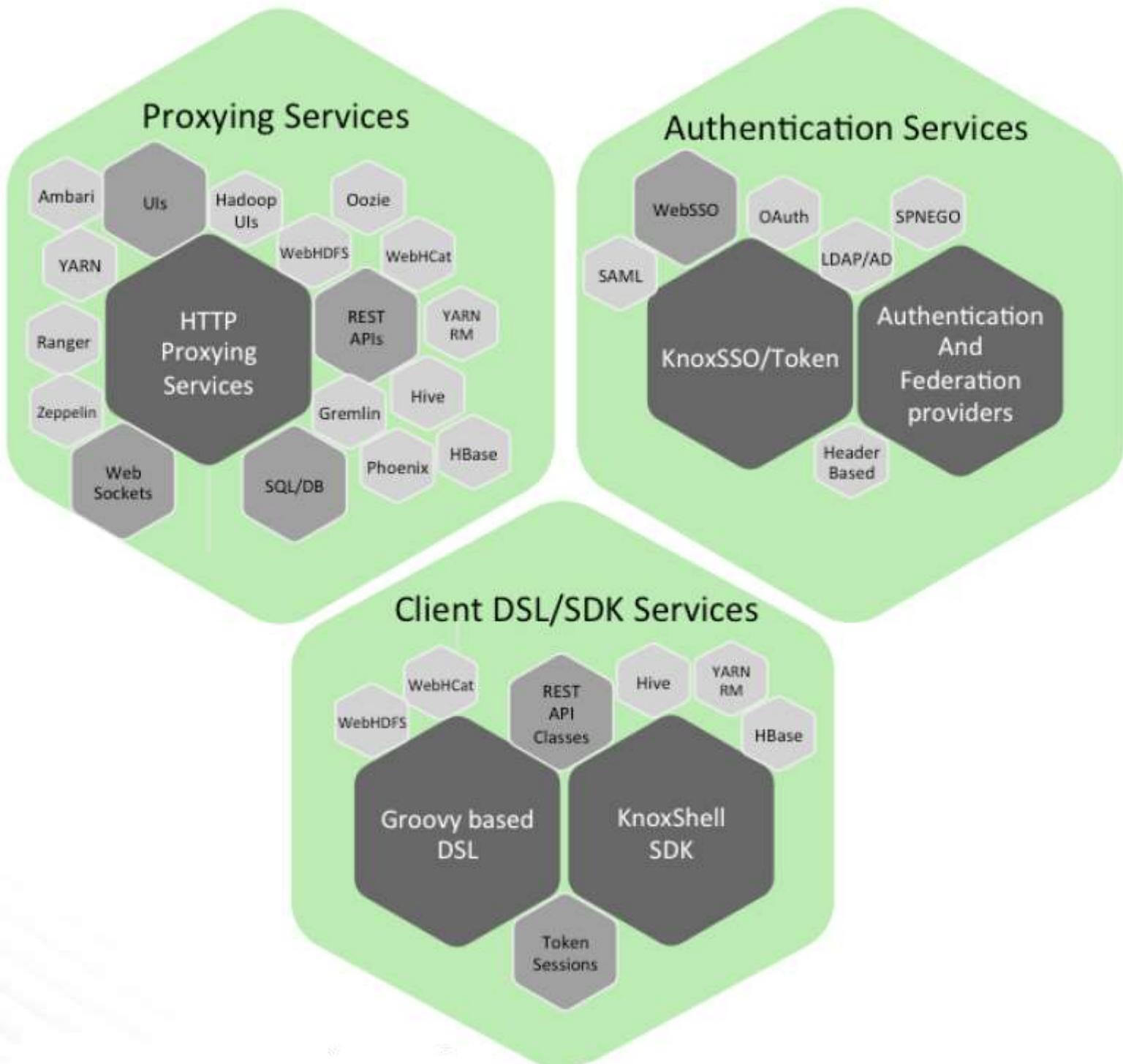


Apache Knox



- Knox Gateway is a reverse proxy for the Hadoop Ecosystem
- A trusted proxy within Hadoop platform deployments
- Proxies HTTP APIs and UIs
- Encapsulates and minimizes the burden of Kerberos on HTTP clients
- Highly flexible with pluggable provider chains

Apache Knox – What is it?



3 Primary Sets of Services from Knox:

- **Proxied Services**
 - Protected Access to Platform Resources
 - Pluggable Provider Pipeline
- **Authentication Services**
 - KnoxSSO
 - KnoxToken
- **Client Services**
 - SDK Client Classes
 - Groovy based DSL for Scripting
 - Knox Token Sessions
 - Credential Collectors

Why Knox?

Enhanced Security

- Proxy to abstract network details
- TLS Termination for non-SSL services

Centralized Control

- Auditing
- Service-level authorization
- Knox Admin UI
- Service Discovery and Topology Generation Framework

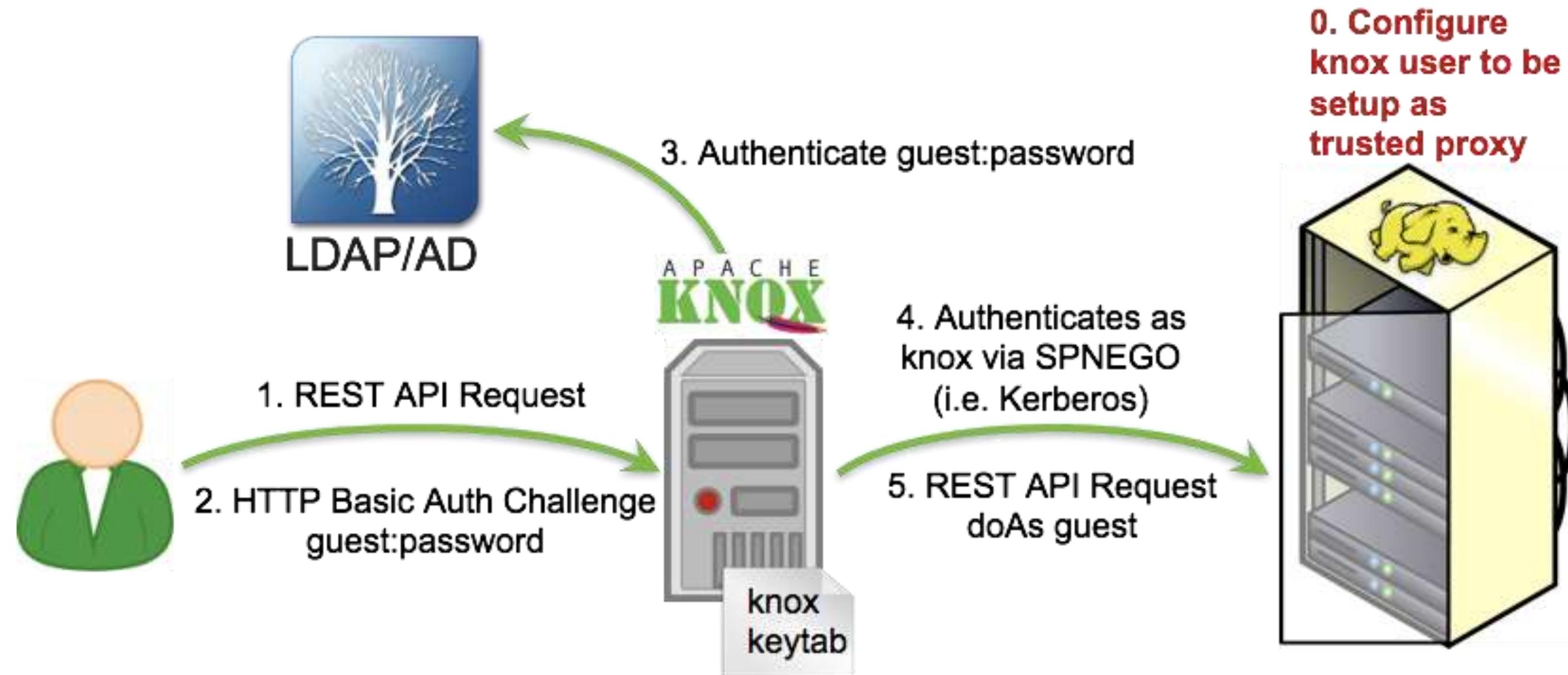
Simplified Access

- Kerberos encapsulation
- Extends API reach
- Single access point
- Single SSL certificate
- Multi-cluster support

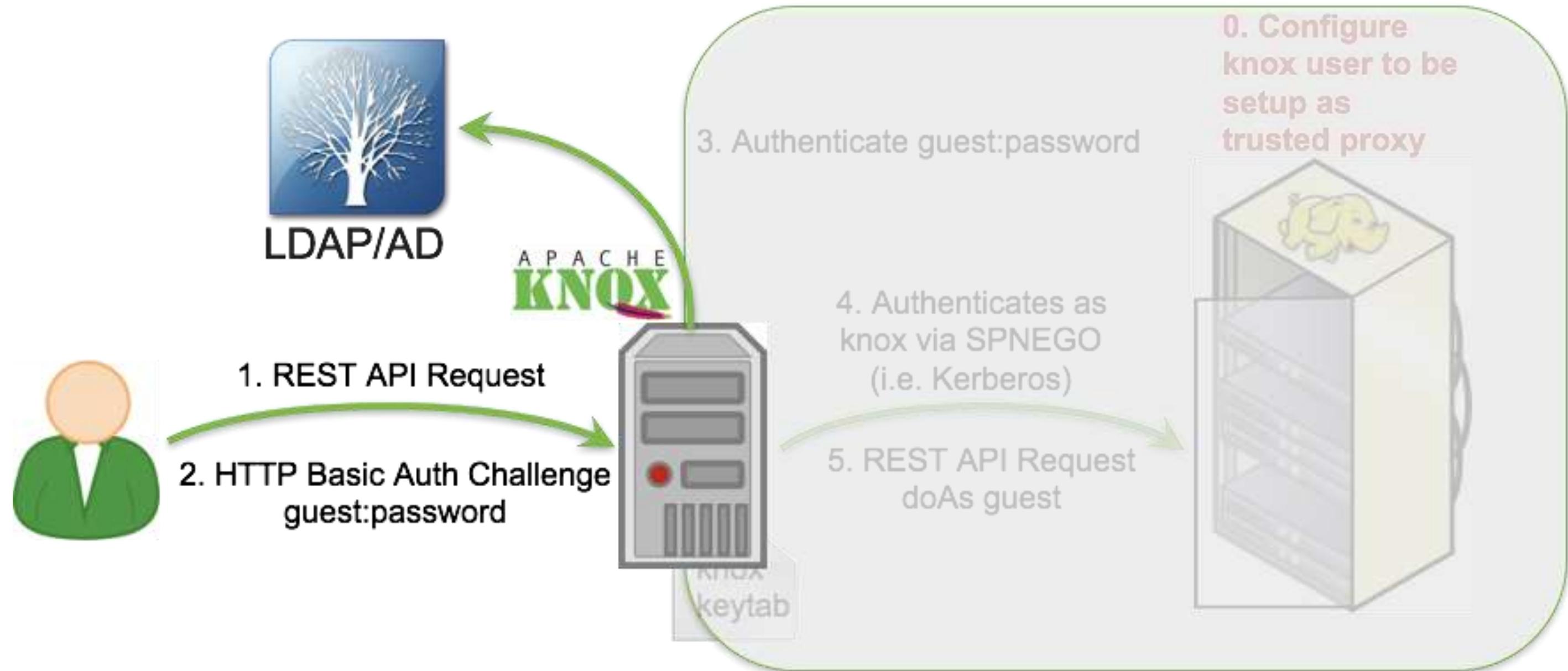
Enterprise Integration

- LDAP/AD integration
- Support for SAMLv2, OAuth and related IdPs: eg. Okta
- SSO integration

Knox - Hadoop Trusted Proxy & Authn Service



Encapsulation of Kerberos



Apache Knox Providers

Web App Security	Protections against common web application vulnerabilities
Authentication / Federation	Authenticate a user's credentials or federate an external authentication event
Authorization	Verify that the authenticated user has access to requested resources
Audit	Detailed accounting of resource access

Web Application Security

Web App Security Provider

- Knox is a Web API (REST) and UI Gateway for Hadoop. The fact that REST interactions are HTTP based means that they are vulnerable to a number of web application security vulnerabilities.
 - CSRF
 - CORS
 - X-Frame-Options
 - X-Content-Type-Options
 - HTTP Strict Transport Security
 - X-XSS-Protection

Authentication Mechanisms

Apache Knox - Supported Authentication Mechanisms

- PAM based Authentication
 - provide the ability to use the configuration provided by existing PAM modules
 - remove limitations with the KnoxLdapRealm
 - Supported for nested OUs and nested groups
 - Faster lookups
 - Support more complex LDAP queries
 - Reduce load on the LDAP/AD server (caching by SSSD)
- HadoopAuth Authentication Provider
 - allows clients to use the strong authentication and SSO capabilities of Kerberos.
 - integrates the use of the Apache Hadoop module for SPNEGO and delegation token based authentication

Supported Authentication Mechanisms (Contd.)

- Header based Preauthenticated SSO Provider
 - This provider was designed for use with identity solutions such as those provided by CA's SiteMinder and IBM's Tivoli Access Manager.
 - **CAUTION:** *The use of this provider requires that proper network security and identity provider configuration and deployment does not allow requests directly to the Knox gateway. Otherwise, this provider will leave the gateway exposed to identity spoofing.*
- Pac4j Provider
 - used as a federation provider to support the OAuth, CAS, SAML and OpenID Connect protocols.
 - It must be used for SSO, in association with the KnoxSSO service and optionally with the SSOCookieProvider for access to REST APIs.

Supported Authentication Mechanisms (Contd.)

- SSO Cookie Provider
 - a typical SP initiated websso mechanism that sets a cookie to be presented by browsers to participating applications and cryptographically verified.
 - enables the federation of the authentication event that occurred through KnoxSSO
- KnoxSSO Service
 - Provides WebSSO capabilities to the Hadoop cluster*
- KnoxToken Service
 - Using the acquired token, a client is able to access REST APIs that are protected with the JWTProvider federation provider.
- TLS Client Certificate Provider
 - enables establishing the user based on the client provided TLS certificate.
 - The user will be the DN from the certificate.

* not all components are supported

Authorization

Authorization Support in Knox

- Service Level Authorization
- Service based ACL definition – simple Knox authorization
- Apache Ranger Integration
 - for enterprise/centralized authorization policies
 - for finer grained policies on services across the platform (service level for Knox)

Apache Ranger Centralized Policy Management

The screenshot shows the Apache Ranger web interface for centralized policy management. The top navigation bar includes links for 'Ranger', 'Access Manager', 'Audit', 'Settings', and 'admin'. The main content area is titled 'Service Manager' and displays a grid of service resources:

Service	Resource	Actions
HDFS	hungergames_hadoop	(eye, checkmark, trash)
HBASE	hungergames_hbase	(eye, checkmark, trash)
HIVE	hungergames_hive	(eye, checkmark, trash)
YARN	hungergames_yarn	(eye, checkmark, trash)
KNOX	hungergames_knox	(eye, checkmark, trash)
STORM		(eye, checkmark, trash)
SOLR		(eye, checkmark, trash)
KAFKA		(eye, checkmark, trash)
NIFI-REGISTRY		(eye, checkmark, trash)
ATLAS	hungergames_atlas	(eye, checkmark, trash)

Buttons for 'Import' and 'Export' are located in the top right corner of the main content area. At the bottom left, there is a link to the Apache License, Version 2.0. The bottom right corner features the Hortonworks logo.

Audit



3号航站楼 Terminal 3
机场快线 Airport Express Train

Audit – Centralized Logging

- All Service access through the Knox Gateway is Audited with detailed Entries for:
 - Original Access Request
 - Authentication Event
 - Identity Assertion: principal mapping, group lookup
 - Authorization Event
 - Dispatch to backend service



Apache Knox to the Rescue...

Knox defense against Web Attack Vectors

- Which category Knox has protection against?
 - Security headers
 - XFS
 - CSRF (limited to REST APIs)
 - SSL Downgrade
 - MIME Sniffing
 - XSS
 - Open Redirect – validated redirect & forwards
 - Whitelisting

Let's Protect with Apache Knox

The screenshot shows the Hortonworks Data Studio interface with the 'Overview' tab selected. The top bar includes links for 'Hadoop', 'Overview', 'Datanodes', 'Datanode Volume Failures', 'Snapshot', 'Show', 'Startup Progress', and 'Utilities'. The main content area displays an 'Overview' section with a long URL and a table of system statistics.

Started:	Sat Jan 26 21:27:12 +0530 2019
Version:	2.9.1, re30710aea4e6e55e69372929106cf119af06fd0e
Compiled:	Mon Apr 16 15:03:00 +0530 2018 by root from branch-2.9.1
Cluster ID:	CID-dfa2961c-f121-491a-aecc-406c31a7ad7f
Block Pool ID:	BP-933667155-le516.ce75.ce86.nl4.gsr.awhoer.net-1540811254633

The screenshot shows the Hortonworks Data Studio interface with the 'Utilities' tab selected. A modal dialog titled 'Upload File' is open, prompting for a file to choose. Below it, the 'Browse Directory' section shows a list of files and directories with columns for Permission, Owner, Group, Size, Last Modified, Replication, Block Size, and Name. The bottom of the screen shows a summary of cluster usage.

Permission	Owner	Group	Size	Last Modified	Replication	Block Size	Name
drwxr-xr-x	ec2-user	supergroup	0 B	Jan 16 19:21	0	0 B	app
-rw-r--r--	pamusr	supergroup	9.36 KB	Jan 08 11:23	3	128 MB	data
drwxr-xr-x	pamusr	supergroup	0 B	Jan 16 19:21	0	0 B	home
drwxr-xr-x	pamusr	supergroup	0 B	Jan 08 11:12	0	0 B	test
drwxrwxrwx	pamusr	supergroup	0 B	Dec 20 00:36	0	0 B	tmp
drwxr-xr-x	pamusr	supergroup	0 B	Jan 24 17:11	0	0 B	user
drwxr-xr-x	pamusr	supergroup	0 B	Dec 05 13:22	0	0 B	user

Summary:
Security is off.
Safemode is off.
1,915,667 files and directories, 1,100,923 blocks = 3,016,590 total filesystem object(s).
Heap Memory used 415.13 MB of 448 MB Heap Memory. Max Heap Memory is 889 MB.
Non Heap Memory used 86.43 MB of 87.94 MB Committed Non Heap Memory. Max Non Heap Memory is <unbounded>.
Configured Capacity: 2.88 TB
DFS Used: 1.89 TB (65.55%)
Non DFS Used: 51.39 GB
DFS Remaining: 965.41 GB (32.7%)
Block Pool Used: 1.89 TB (65.55%)
DataNodes usages% (Min/Median/Max/stdDev): 65.55% / 65.55% / 65.55% / 0.00%
Live Nodes: 3 (Decommissioned: 0, In Maintenance: 0)
Dead Nodes: 0 (Decommissioned: 0, In Maintenance: 0)
Decommissioning Nodes: 0

Limit Attack Surface

- Only expose Knox Port through Cloud VPC
- All other Service Access goes through Knox

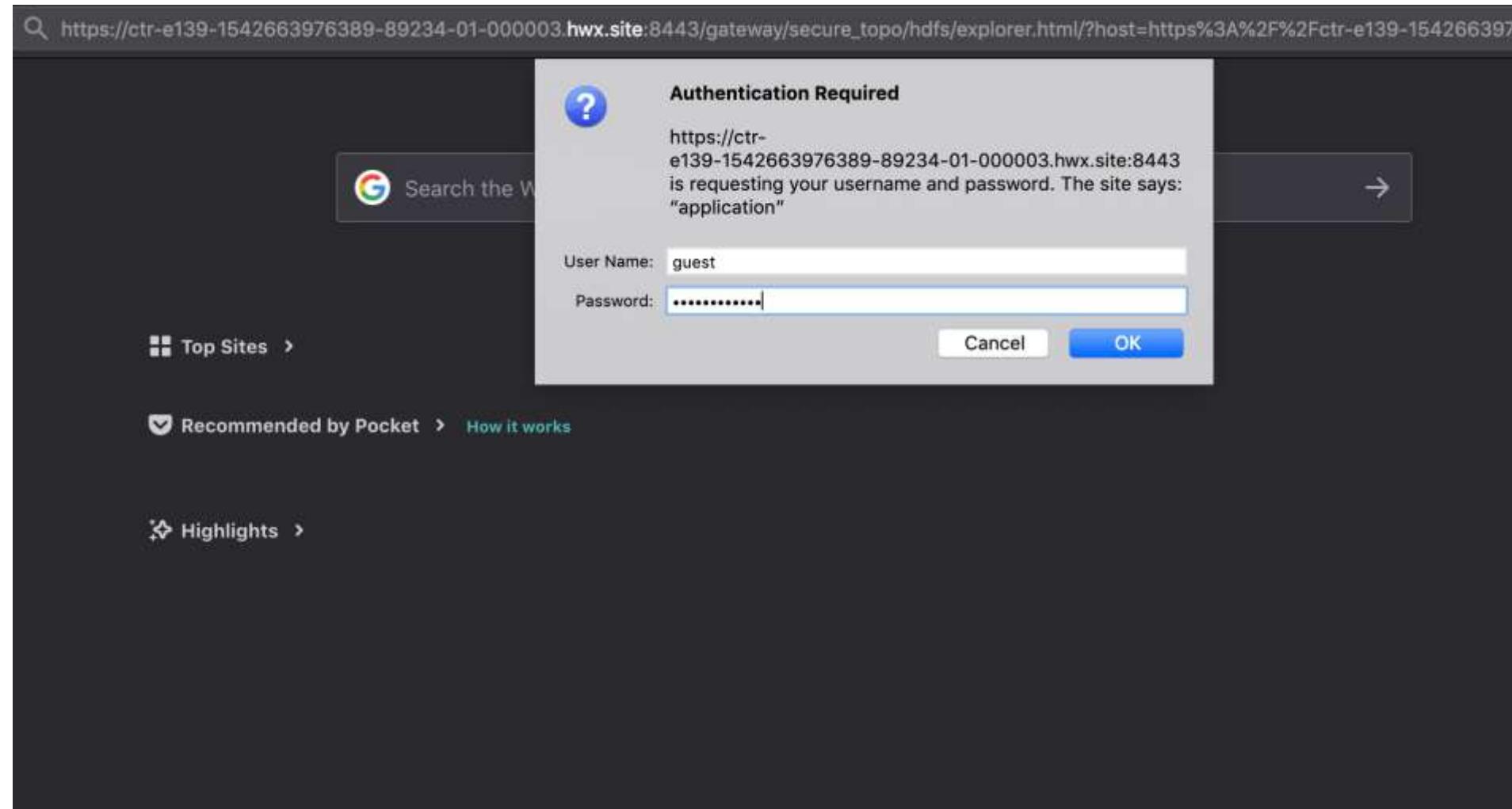
Add Authenticated Access

- Without Knox or Kerberos enablement, there is no Authentication.
- Proxy Access to the UI through Knox Gateway require HTTP BASIC Auth against LDAP/AD
- Calls to WebHDFS URLs will include the Authenticated User as a user.name Query Param
- Only Authorized Users will have access.

Add Service Level Authorization

- Enable Authorization Providers e.g. Ranger
- Restrict Access to WebHDFS to Users in certain LDAP groups
- Only a subset of your Authenticated Users will have Access to WebHDFS

End Result - Authentication



End Result - Authorization

The screenshot shows a browser window for the Hortonworks HDFS Explorer at https://ctr-e139-1542663976389-89234-01-000003.hwx.site:8443/gateway/secure_topo/hdfs/explorer.html?host=https%3A%2F%2Fctr-e139-1542663976389-89234-01-000003.hwx.site:8443. The navigation bar includes links for Hadoop, Overview, Datanodes, Datanode Volume Failures, Snapshot, Startup Progress, and Utilities.

The main area is titled "Browse Directory" and shows a directory listing for "/app-logs". A red error message box displays the text: "Permission denied: user=guest, access=READ_EXECUTE, inode="/app-logs/hive":hive:hadoop:drwxrwx---". Below the message is a search bar containing "/app-logs" and a "Go!" button. To the right are three small preview icons labeled "1", "2", and "3".

The table below the search bar lists two entries:

Permission	Owner	Group	Size	Last Modified	Replication	Block Size	Name
drwxrwx---	hive	hadoop	0 B	Mar 18 09:20	0	0 B	hive
drwxrwx---	spark	hadoop	0 B	Mar 18 09:20	0	0 B	spark

Below the table, it says "Showing 1 to 2 of 2 entries" and has "Previous" and "Next" buttons. The page footer contains the text "Hadoop, 2018."

Security Controls - Apache Knox

	Issue Categories (OWASP Top 10 – 2017)	Apache Knox
A1	Injection	No
A2	Broken Authentication	Yes
A3	Sensitive Data Exposure	Yes (Encrypts params & locations)
A4	XML External Entities (XXE)	No
A5	Broken Access Control	Partially (Service level ACLs)
A6	Security Misconfiguration	Partially (Less exposed Services)
A7	XSS	Partially*
A8	Insecure Deserialization	No
A9	Using Components with Known Vulnerabilities	Partially
A10	Insufficient Logging and Monitoring	Partially**

What else you can do?

- Security around your Perimeter
 - Web Application Firewall
 - Intrusion Detection & Prevention System
 - Network (Packet filtering) Firewall
 - API Gateway
- Hardening everything you can
 - O/S - Secure PAM Configuration, SELinux, remove unused packages, disable unused services, etc.
 - Application Server – Jetty, Tomcat, etc.
 - Database Server – enable SSL, restrict IP addresses, etc.
 - KDC Server – master_key_type, supported_enctypes, ticket_lifetime, etc.
 - Set ***.proxyuser.*.hosts/groups** only to needed hosts/groups

Take Away

- Kerberos Encapsulation – Web Browser friendly.
- Knox - Eliminates need for developing central Authentication solution for Hadoop ecosystem
- Provides ready integration with Enterprise Authentication mechanisms like AD, Okta, etc.
- Prevents against several OWASP Top 10 threats



Questions?



Thank you