PeopleSoft and ElasticSearch Security Examined

July 16, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications

Oracle E-Business Suite
and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database
Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Firewall
for Oracle E-Business Suite
and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Why Do Elasticsearch Databases Keep Getting Hacked?

“The cause of the problem? A poor understanding of Elasticsearch security and how the software works.”

Mike Paquette, security product director at Elastic
Infosecurity Magazine – February 2019

Source: https://www.infosecurity-magazine.com/infosec/why-do-elasticsearch-databases-1-1/

Terminology

Elasticsearch	Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents
Kibana	Kibana is an open source data visualization dashboard for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data.
Logstash	Logstash is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to Elasticsearch.
Elastic.co	The company that develops open source Elasticsearch, Kibana, and Logstash and commercial add-ons to those products.

PeopleSoft Elasticsearch Security Challenges

- **Fixed Elasticsearch versions (2.3.2, 6.1.2, or 7.0) for PeopleSoft**
  - Unable to upgrade – Oracle must release a new version or patch
  - No Elastic.co security patches – Oracle provides security patches
  - Think “Oracle fork” of Elasticsearch

- **Elastic.co and third-party plugins not supported**
  - Elastic.co security plugins in X-Pack
  - Open Distro (Amazon) security plugins
  - Search Guard plugin

PeopleSoft Elasticsearch References – Manuals

- **PeopleSoft Deployment Packages for Elasticsearch Installation**
  - PeopleTools 8.56 – October 2019
  - PeopleTools 8.57 – January 2019
  - PeopleTools 8.58 – December 2019
- **PeopleSoft PeopleTools 8.55 Installing or Upgrading the Elastic Search DPK**
- **PeopleSoft PeopleTools Search Technology**
  - PeopleTools 8.55 – November 2016
  - PeopleTools 8.56 – June 2017
  - PeopleTools 8.57 – September 2018
- **PeopleSoft PeopleTools Kibana SSL Configuration**

PeopleSoft Elasticsearch References – My Oracle Support

General

- Elasticsearch Home Page (Doc ID 2205540.2)
- FAQ: E-ES: Elasticsearch FAQ (Doc ID 2500023.1)
- How To: E-ES: Is It Supported To Use PeopleTools And A Standalone, Opensource Instance Of Elasticsearch? (Doc ID 2566690.1)
- How To: E-ES: Can We Use Elasticsearch Version 6.5 or 7.0? (Doc ID 2482862.1)
- Reference: Tech Update – PeopleTools Upgrades Elasticsearch in Current Releases (Doc ID 2513903.1)

Installation and Configuration

- How To: E-ES: What are the hardware and software requirements for Elasticsearch, and which resources/roles are required to configure, install, and maintain Elasticsearch? (Doc ID 2412549.1)
- How To: E-ES: How To use a Single Elasticsearch Cluster with Multiple PeopleSoft Environments? (Doc ID 2209311.1)
- How To: E-ES: How to Check that Full Direct Transfer is being Used in Elasticsearch? (Doc ID 2511117.1)

Logging and Auditing

- How To: E-ES: Locating Elasticsearch Logs (Doc ID 2235926.1)
- How To: Does Elastic Search have an auditing functionality to monitor logins in PeopleSoft? (Doc ID 2359227.1)
- How To: E-ES: Elasticsearch: Capture User Search Strings In Global Search In PeopleSoft (Doc ID 2539584.1)

Security

- How To: E-ES: Security Patches For Elastic Search And Kibana (Doc ID 2552045.1)
- How To: E-ES: Can the elasticsearch.yml File Work With Multiple Root And Trust Certificates ? (Doc ID 2427952.1)
- E-ES: ES 232_xx: ES 612_xx: How to configure SSL in Search Framework implementations using Elasticsearch? (Doc ID 2217683.1)

Elasticsearch Security References

- **Open Distro Security Guide**
  - https://opendistro.github.io/for-elasticsearch-docs/docs/security-configuration/
- **Elasticsearch Vulnerabilities**
  - https://www.cvedetails.com/vulnerability-list.php?vendor_id=13554
- **psadmin.io Deploy and Configure Elasticsearch**
  - https://psadmin.io/2016/11/08/deploy-and-configure-elasticsearch/

PeopleTools and Elasticsearch

PeopleTools	Elasticsearch Versions Supported	Elastic Components
~~8.55~~	**~~2.3.2~~** (8.55.11-25) **6.1.2** (8.55.26+)	▪ Elasticsearch
8.56	**~~2.3.2~~** (8.56.00-11) **6.1.2** (8.56.12+)	▪ Elasticsearch
8.57	**6.1.2**	▪ Elasticsearch ▪ Kibana (search-index, server)
8.58	**7.0**	▪ Elasticsearch ▪ Kibana (application) ▪ Logstash (Health Center)

MOS Document *Lifetime Support Summary for PeopleSoft Releases* (Doc ID 2238983.2)
MOS Document *Elasticsearch Home Page* (Doc ID 2205540.2)

PeopleSoft Elasticsearch Components

Elasticsearch Version	Release Date	PeopleTools Versions	Oracle Support End-Date
~~**2.3.2**~~	April 21, 2016	8.55, 8.56	October 11, 2019
6.1.2	January 16, 2018	8.55, 8.56, 8.57	TBA
7.0	April 10, 2019	8.58	TBA

PeopleSoft Elasticsearch Plugins Installed

- **Oracle PeopleSoft Security Plugin (orcl-security-plugin)**
  - Integration with PeopleSoft security
  - PSCipher support
  - SSL network encryption

- **Elastic.co Phonetic Analysis plugin**
- **Elastic.co Ingest Attachment plugin**
  - Extract text from attachments including PDF, Word, Excel, PowerPoint, etc.
- **Oracle PeopleSoft File and Web Crawler Plugin (orcl-crawl-plugin)**
- **Oracle PeopleSoft System Monitoring Plugin (orcl-monitor-plugin)**

PeopleSoft Elasticsearch Security Vulnerabilities

- **January 2020**
  - CVE-2020-2600 (8.56, 8.57)
  - CVE-2020-2687 (8.56, 8.57)
  - Upgrade to PeopleTools 8.56.21 or 8.57.12
  - Upgrades Elasticsearch JRE to 1.8.0_231

- **October 2018**
  - CVE-2018-3164 (8.55, 8.56)
  - Upgrade to PeopleTools 8.55.26 or 8.56.12

PeopleSoft Elasticsearch Java Version

- **PeopleSoft Elasticsearch is bundled with Java JRE 1.8**
  - Version is fixed and can not be independently updated
  - See MOS Note ID 2632008.1

- **JRE is updated through Elasticsearch DPK**
  - Updated quarterly as part of Critical Patch Updates

Encryption at Rest

- **Elasticsearch does not have built-in encryption by default**
  - Plugins for encryption are not supported by Oracle
- **Use dm-crypt**
  - Transparent data encryption for Linux
  - Elastic.co only officially supports for Platinum license customers
  - Oracle does not support dm-crypt

PeopleSoft Elasticsearch Network Configuration

Elasticsearch Component	PeopleTools Versions	Protocol	TCP/IP Default Port
Client "REST"	All	HTTP/REST	9200
Internode "Transport"	All	Proprietary	9300
Kibana Client	8.57 8.58	HTTP	5601

Network Encryption

- **Encryption is disabled by default**
- **Three different parts to network encryption**
  1. PeopleSoft application server ← → Elasticsearch nodes
  2. Elasticsearch node ← → node communication
  3. User ← → Kibana (8.57, 8.58) – see PeopleTools Kibana SSL Configuration

See PeopleTools Search Technology	See PeopleTools Kibana SSL Configuration
elasticsearch.yml	**kibana.yml**
1 **orclssl.http.ssl: true**	3 **server.ssl.enabled: true**
2 **orclssl.transport.ssl: true**	server.ssl.certificate: …
orclssl.keystore=…	server.ssl.key: …
orclssl.keystore_password=…	elasticsearch.ssl.certificateauthorities: …
orclssl.truststore=…	
orclssl.truststore_password=…	
orclssl.callback: false	

Masking of Sensitive Data in Search Results

- **PeopleTools 8.58 introduces masking of sensitive data search results**
- **Search results on classic and fluid search pages**
  - component keyword search results
  - component real-time search results
  - classic and fluid prompt page search results
- **If list view of the keyword search results page contains sensitive data**
  - the list view is removed and if a facet contains sensitive data, the facet is removed
- **Data masking is done in the SearchInit event any SearchKey field**
  - Use SetDisplayMask, CopyDisplayMast, SetFacetNamestoRemove, and SetRemovelistView

Elasticsearch Auditing and Logging

- **Security event auditing part of x-pack**
  - Not included due to Elastic.co licensing
- **Log files in $ES_HOME/logs**
  - ESCLUSTER.log = per cluster log file
  - ESCLUSTER_server.log = per server log file
  - Failed logins captured


```
{"type": "server", "timestamp": "2020-06-
01T15:20:16,369+0000", "level": "ERROR", "component":
"c.p.p.e.s.o.r.OrclAuthPluginRestFilter", "cluster.name":
"ESCLUSTER", "node.name": "ps4.integrigy.com",
"cluster.uuid": "Q8q9YPMBQA-8sQj7py8Xuw", "node.id":
"PYqs3ELlSZqhW9KQouIZow",  "message":
"[OrclAuthPluginRestFilter] Invalid password for user
esadmin"}
```

Elasticsearch Auditing and Logging

- **Elasticsearch logging uses standard Java logging framework**
  - Framework is Log4j
  - 6.1.2/7.0 = Configuration is in $ES_HOME/config/log4j2.properties
  - 2.3.2 = Configuration is in $ES_HOME/config/logging.yml

- **Unlimited log files are saved and roll over every 128MB**

PeopleSoft Elasticsearch Users

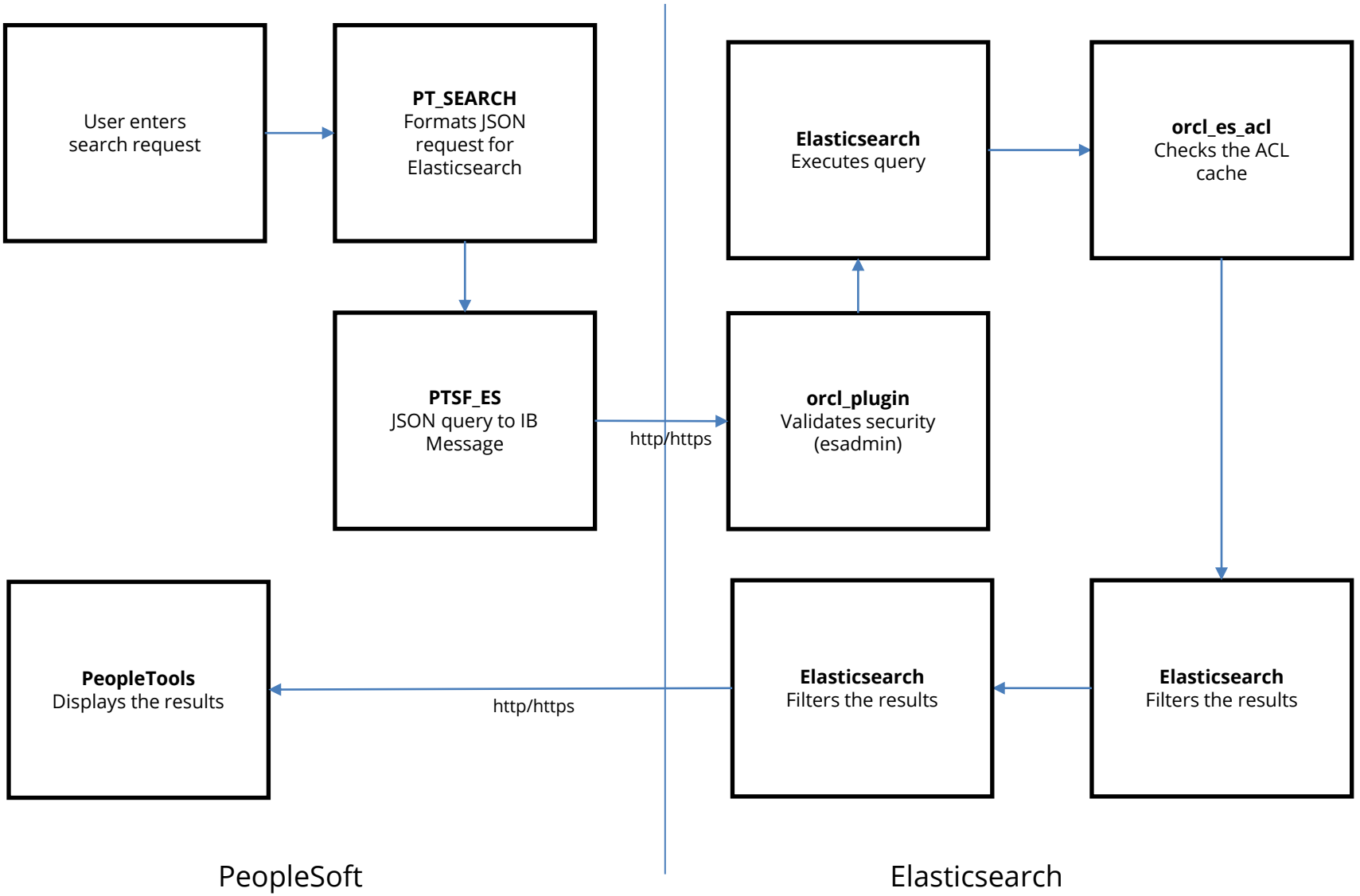
Elasticsearch User	Description	Roles
esadmin	▪ Elasticsearch administrative user ▪ Password set during DPK installation ▪ Default password is “esadmin” or “Esadmin1”	admin read security
people	▪ PeopleSoft Elasticsearch proxy user ▪ Password set during DPK installation ▪ Default password is “peop1e” ▪ Not the same user as PeopleSoft Connect ID	read

- Use the Elasticsearch $ES_HOME/bin/elasticsearchuser utility to change passwords, add users, etc.
- Use elasticsearchuser adduser to change passwords
- Users and passwords controlled by the Oracle security plugin and stored in plugins/orcl-security-plugin/config/properties
- Password encrypted using PSCipher

PeopleSoft Elasticsearch Roles

PeopleSoft Role	Description
Search Administrator	▪ Search definitions and search categories ▪ Scheduling index builds ▪ Monitoring indexes
Search Developer	▪ Search queries ▪ Search definitions ▪ Search categories
Search Server	▪ Search engine search instance

PeopleSoft and Elasticsearch Flow



Kibana Security

- **8.57 – Limited to only the esadmin user**
  - Limited functionality in terms of Elasticsearch information
- **8.58 – Application and Health Center Dashboards**
  - esadmin user allowed – no data authorization
  - Any PeopleSoft user with “Search Administrator” role or create/edit dashboard
  - User data authorization is based on the search definition for the visualization or dashboard
  - Dashboard privileges defined under Kibana Privileges (PeopleTools > Search Framework > Administration > Kibana Privileges)

Additional Security Considerations

- **Elasticsearch cluster may be shared between PeopleSoft environments (Prod, Demo, Dev, Test, etc.)**
  - Security is based on PeopleSoft user id, which does not include environment or database information
  - Production should always be a separate Elasticsearch cluster
  - Only share between environments with no or same sensitive data

- **PeopleSoft security credentials and ACLs are cached in Elasticsearch**
  - Refresh interval is 2 hours
  - Security changes will take up to the interval to update
  - To change the interval see PeopleTools > Search Framework > Administration > Search Options
  - To refresh the cache see PeopleTools > Search Framework > Utilities > Search Test Page

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**