Hewlett Packard Enterprise

Cloud Service Automation

Global Search for Service Consumers

Software version: 4.70

Document release date: September 2017

Software release date: July 2016

Contents

Introduction

This document helps you understand the integration between GlobalSearch/ElasticSearch and Cloud Service Automation (CSA). This will help you find answers to the questions that you might have on the usage of Search Service feature in CSA.

Supported versions

CSA software and hardware requirements are documented in Cloud Service Automation Platform Support Matrix. You can find this documents on the Software Support Portal at https://softwaresupport.hpe.com.

Global Search, CSA Search Service and Elastic Search

CSA is integrated with elastic search service to store catalog, subscriptions, and service instances information. Service consumers can search for Service Offerings, Service Subscriptions, and Service Instances using the embedded search. The search indexes are kept up-to-date by the background service.

Marketplace Portal (MPP) dashboard provides Global search box where consumers can search for specific information from ES database. You can do wildcard search and specific text based search, and also use various supported search patterns like *, %, logical operations (and, or, not) etc.

CSA search service helps user to find a certain service offering, service instance, or subscription by a meaningful keyword. For service offerings, global search finds the keyword in the name, description, option sets, options, and properties. For service instances and subscriptions, global search finds the keyword in the name, description, and instance properties (name and value).

Elastic Search (ES) is a database for searching text. It stores structured text and indexes on filesystem. ES itself does not have any security model, but there is plugin to ES named SearchGuard that provides security features.

In CSA use case, SearchGuard is configured to protect ES and to allow connection from CSA search service on its `http` transport only with client certificate authentication. Logic what results are to be displayed to a consumer user who uses search (to avoid returning information that user does not have access to) is driven by accessible catalog ids encoded into ES query. There is also an ES port used for inter-node communication in cluster - that one is protected by a key stored on filesystem that other node has to know.

Rest API Usage

Use wildcard in the search term for exact match.

For example, consider the following hostname and IP address of the VM as search terms.

Host Name : See0806f0

Management IP Address : 10.2.12.8

The expected search term will be `*See0806f0* and *10.2.12.8*`

Instead of the above search term, if you use `See0806f0 and 10.2.12.8`, then the results may not always be appropriate. The reason is that Elastic search does pattern matching by analyzing the search where it could be tokenized for possible match.

The string given in the global search text box is converted to a rest call and given to the ES Server.

Example:

1. Search for service offering with string "`Service Offering for Elastic Search TA`" should return offering name and subscription associated with that offering.

   ```
   https://<csa server>:8089/api/search?count=10&keyword=%22Service+Offering+for+Elastic+Search+TA%22&offset=0
   ```

   Response:


   ```
   [{"id":"8a818fad55a551700155e91928cf14dc","title":"Service Offering for Elastic Search TA","description":null,"iconUrl":"/csa/images/library/ccueVersion-cloudlinux.png","type":"SERVICE_OFFERING","catalogId":"8a818eb15230cd9d015230d936db27cf","catalogName":"QAINT_320 Catalog
   ```


```
1","categoryName":"CRM","categoryDisplayName":"CRM","version":"1.0.0","hideInitialPrice":fals
e,"hideRecurringPrice":false,"base":0,"recurring":0,"recurringPeriod":"YEAR","currency":"USD"
},{"id":"8a818fad55a551700155e91a6a431534","title":"Subscription for Elastic Search
TA","description":"Service Offering for Elastic Search
TA","iconUrl":"/csa/images/library/ccueVersion-
cloudlinux.png","type":"SUBSCRIPTION","catalogId":"8a818eb15230cd9d015230d936db27cf","catalog
Name":"QAINT_320 Catalog 1","status":"ACTIVE"}]
```


2. Search for the subscription with string "`Subscription for Elastic Search TA`" should return subscription.

   ```
   https://<csa
   server>:8089/api/search?count=10&keyword=%22Subscription+for+Elastic+Search+TA%22&offset=0
   ```

   Response:


   ```
   [{"id":"8a818fad55a551700155e91a6a431534","title":"Subscription for Elastic Search
   TA","description":"Service Offering for Elastic Search
   TA","iconUrl":"/csa/images/library/ccueVersion-
   cloudlinux.png","type":"SUBSCRIPTION","catalogId":"8a818eb15230cd9d015230d936db27cf","catalog
   Name":"QAINT_320 Catalog 1","status":"ACTIVE"}]
   ```


3. Search for the string name "`SearchHostnameProperty`" should return subscription associated with that hostname.

   ```
   https://<csa server>:8089/api/search?count=10&keyword=SearchHostnameProperty&offset=0
   ```

   Response:


   ```
   [{"id":"8a818fad55a551700155e91a6a431534","title":"Subscription for Elastic Search
   TA","description":"Service Offering for Elastic Search
   TA","iconUrl":"/csa/images/library/ccueVersion-
   cloudlinux.png","type":"SUBSCRIPTION","catalogId":"8a818eb15230cd9d015230d936db27cf","catalog
   Name":"QAINT_320 Catalog 1","status":"ACTIVE"}]
   ```


For more information on various values that the search string can take, visit the following URL.

https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html#query-string-syntax

Configurations in CSA

Generally elasticsearch works without any specific configuration changes. However, in the following situations, you need to configure certain parameters for elastic search.

- CSA is installed on cluster and you want all the nodes to be in sync for elastic search.
- The certificate expires or a new certificate is generated.

In the above situations you need to change the configurations. The required configuration changes are given below.

Task	Description
Edit `csa.properties`	Configure the property `csa.provider.es.exists` for elasticsearch integration. By default the value of this property is set to **True**. If you do not want to use elasticsearch, Set the value to **False**. `csa.provider.es.exists=true`

Edit `app.json`	You can find this file in `csa_home\csa-search-service`. Edit this file and make sure that the properties and their values are as shown in below sample configuration:
	`{`
	`---`
	`---`
	`"ccue-basic-server": {`

Task	Description

	"host": "<CSA_NODE1>",
	"port": 9000,
	},
	"pfx": ".keystore_test", keystore should be valid node keystore and should be in PKCS12 format. Make sure this keystore exists under csa-search-service folder.
	--- 	
	--- 	
	"msvc-basic-search": {
	"searchEngineURL": "https://<CSA_NODE1>:9201", CSA search engine should be pointing the CSA local node.
	"searchEngineUser": "admin",
	"searchEnginePassword": "ENC(YQmH6ucZ0gUJ71nLBl9uKw\u003d\u003d)",
	"idmURL": "https://<CSA IDM URL or CSA Load Balancer>:9444/idm-service",
	"idmUser": "idmTransportUser",
	"idmPassword": "ENC(pzl9bdHkceriGilPyhsV5A\u003d\u003d)",
	"pfx": ".keystore_test", keystore should be valid node keystore and should be in PKCS12 format.
	"passphrase": "ENC(lCmcjnJRVPVcjbUen6H+xw\u003d\u003d)",
	"ca": "C:/Program Files/HPE/CSA/jboss-as/standalone/configuration/apache_csa.crt", CSA server certificate or Load balancer certificate
	"strictSSL": true, Make it false, if you are using self-signed certificate
	--- 	
	--- 	
	}

Edit elasticSearch.yml	You can find elasticSearch.yml under <CSA_HOME>/elasticsearch-1.6.1/config. Edit this file and make sure that the highlighted properties and their values are correct as shown in the sample configuration below. cluster.name: "elasticsearch" → To identify cluster name when running multiple clusters on the same network. Uncomment and set it to unique so that all nodes in this cluster should share same unique name. node.name: "node1" → To identity unique node in cluster node.master: true → uncomment this property and set it to true, note: Each node in the cluster must be a master node. node.data: true → optionally, uncomment this property to allow this node to store data #node.local: true → Comment this property if nodes want to run in cluster, ignore or uncomment if you are running CSA on standalone mode. When you disable this property, global search can find and communicate with other nodes on the network. If this property is left enabled, global search will

Task	Description
	not discover other nodes and will isolate itself from the network. transport.tcp.port: 9300 → Customer Port for node to node communication http.port: 9201 → Custom Port on which Elastic Search will be listening http.enabled: true discovery.zen.ping.timeout: 5s discovery.zen.ping.unicast.hosts Set this property to the IP addresses of the master nodes that perform discovery when new master or data nodes are started. Since all nodes in the cluster are master nodes, set this property to all IP addresses of the nodes in the cluster For example, discovery.zen.ping.unicast.hosts: ["111.222.333.444","111.222.333.445","111.222.333.446"] **searchguard.enabled: true** → Enables SSL communication between CSA search service to ElasticSearch. Locate the Transport layer SSL section and verify the following: searchguard.ssl.transport.node.keystore_password: changeit → keystore password searchguard.ssl.transport.node.truststore_password: changeit → truststore password Windows Location of the CSA keystore and CSA truststore: searchguard.ssl.transport.node.keystore_filepath: C:\Program Files\HPE\CSA\jboss-as/standalone/configuration/.keystore searchguard.ssl.transport.node.truststore_filepath: C:\Program Files\HPE\CSA/openjre/lib/security/cacert Linux location of the CSA keystore and CSA truststore : searchguard.ssl.transport.node.keystore_filepath: /usr/local/hpe/csa/jboss-as/standalone/configuration/.keystore searchguard.ssl.transport.node.truststore_filepath: /usr/local/hpe/csa/openjre/lib/security/cacerts Locate the REST layer SSL section and verify the following: searchguard.ssl.transport.http.keystore_password: changeit → keystore password searchguard.ssl.transport.http.truststore_password: changeit → truststore password Windows Location of the CSA keystore and CSA truststore: searchguard.ssl.transport.http.keystore_filepath: C:\Program Files\HPE\CSA/jboss-as/standalone/configuration/.keystore searchguard.ssl.transport.http.truststore_filepath: C:\Program Files\HPE\CSA/openjre/lib/security/cacerts Linux location of the CSA keystore and CSA truststore: searchguard.ssl.transport.http.keystore_filepath: /usr/local/hpe/csa/jboss-as/standalone/configuration/.keystore searchguard.ssl.transport.http.truststore_filepath: /usr/local/hpe/csa/openjre/lib/security/cacerts

Task	Description
Create security key	Create a security key for authenticating communication between the nodes in the cluster when sharing shards and replicas of the inventory index. Creation of security key involves the following steps: **1. Stop elasticsearch service on CSA node1** Windows - Navigate to **Services** screen, select **ElasticSearch 1.6.1 service** and restart the service Linux - Run the following command: `csa_home/scripts/elasticsearch restart` **2. Copy searchguard node key to all nodes** Copy the searchguard node key (CSA_HOME/elasticsearch-1.6.1/searchgurad_node_key.key) file from CSA node1 to all other nodes in the cluster. Copy the file to the same directory in all the nodes without changing the file name. **3. Restart the services** Restart the services as explained in step 1.

Troubleshooting

Problem	Global search unable to retrieve any details.
Primary software component	CSA search service and Elastic Search
Failure message	For failure messages check for the logs in the locations. You will see exceptions related to SSL handshake and/or TLS communication: Error: Request error, retrying -- self-signed certificate in certificate chain On Windows, CSA_HOME\csa-search-service\bin\daemon\hpesearchservice.err.log and CSA_HOME\elasticsearch-1.6.1\logs On Linux, CSA_HOME/csa-search-service/bin/.msvc/msvc.log and CSA_HOME/elasticsearch-1.6.1/logs To debug the logs, Enable logging level to debug in logging.yml under CSA_HOME\elasticsearch-1.6.1\config
Probable cause	Certificate may not be valid CA signed

Solution	Edit `app.json` and check if following properties are configured to false:
	`"strictSSL": false,`
	`"rejectUnauthorized": false`
	Also verify and make sure that the certificate and keystore are not expired. If they are expired, then you must update `app.json` and `elasticsearch.yml` with the details of new keystore and Certificate.
	Check for the above properties under Configuration section to update the keystore and Certificate.

Global search is not working after Certificate change or after Certificate expired.

Problem	Global search doesn’t work after certificate change.
Primary software component	CSA search service and Elastic Search

Failure message	For failure messages check for the logs from the following location, you will see exceptions related to SSL handshake and/or TLS communication. On Windows, CSA_HOME\csa-search-service\bin\daemon\hpesearchservice.err.log and CSA_HOME\elasticsearch-1.6.1\logs On Linux, CSA_HOME/csa-search-service/bin/.msvc/msvc.log and CSA_HOME/elasticsearch-1.6.1/logs To debug the logs, Enable logging level to debug in logging.yml under CSA_HOME\elasticsearch-1.6.1\config Also check the logs under CSA_HOME/csa-search-service/logs/server.log
Probable cause	SSL communication is broken between CSA search service and Elastic search
Solution	If Certificate expired or Certificate changed then make sure you update app.json and elasticsearch.yml with new keystore and Certificate. Check for the highlighted properties under Configuration section to update the keystore and Certificate.

Global search is not working when CSA installed on Linux platform

Problem	Global search function is not working on Linux setup
Failure message	For failure messages check for the logs from the following location, you will see exceptions like : Error: 140527461144352:error:0B07C065:x509 certificate routines:X509_STORE_add_cert:cert already in hash table:../deps/openssl/openssl/crypto/x509/x509_lu.c:348: . On Windows, CSA_HOME\csa-search-service\bin\daemon\hpesearchservice.err.log On Linux, CSA_HOME/csa-search-service/bin/.msvc/msvc.log Also check the logs under CSA_HOME/csa-search-service/logs/server.log
Probable cause	SSL communication is broken between CSA search service and Elastic search
Solution	1. Go to `CSA_HOME/scripts` 2. `./msvc stop` 3. Go to `CSA_HOME/csa-search-service/bin` 4. Edit `start-msvc.sh` and replace `start-msvc.js` with `msvc-server.js` as shown below. `${NODEJS_HOME}/bin/node ${SEARCH_SERVICE_HOME}/bin/msvc-server.js &` 5. `./msvc start` 6. Create new offering and subscription. 7. Go to MPP and verify search patterns returning for subscriptions.

How to move Global Search data from one CSA instance to another CSA instance

Problem	In an upgraded or migrated CSA environment, Global Search service results appear for new offerings and subscriptions when elasticsearch is configured, but the results do not appear for offerings and subscriptions that already exist.
Solution	If global search is enabled, it should find existing subscriptions. If global search is not working, you need to re-enable global search when you restart CSA services, which allows you to see all offerings/subscriptions. If an existing CSA database is to be attached to a new node (for example, to recover from a node crash or because of machine migration), perform the following steps to repopulate existing information to the global search in the new node. It is assumed that we have a CSA instance (source server) that has elasticsearch indices used for global

	search. If elasticsearch was never enabled in this instance, these indices will be empty, and this migration step is not needed. If it is enabled currently or was enabled previously, the indices exist, and you need to perform this migration. 1. Stop all services in <target instance>, and rename the existing folder "elasticsearch" to say "elasticsearch_old." This folder can be deleted once the migration is completed. 2. Copy the elasticsearch folder from instance <source instance> to instance <target instance>. 3. Restart all services. 4. Log in to Marketplace Portal and perform a global search. All offerings, subscriptions and service instances created in <source instance> are searchable. If any are created in the <target instance>, they are not searchable. 5. Any offerings, subscriptions, and service instances created from now on will be globally searchable, because they will be indexed into elasticsearch as they are created.

Workaround: Disable SSL between CSA search service and Elastic Search

Problem	SSL Communication between CSA search service and Elastic Search may not work due to wrong certificates or due to some other security reason
Failure message	For failure messages check for the logs from the following location, you will see exceptions like : Error: 140527461144352:error:0B07C065:x509 certificate routines:X509_STORE_add_cert:cert already in hash table:../deps/openssl/openssl/crypto/x509/x509_lu.c:348: . On Windows, CSA_HOME\csa-search-service\bin\daemon\hpesearchservice.err.log On Linux, CSA_HOME/csa-search-service/bin/.msvc/msvc.log Also check the logs under CSA_HOME/csa-search-service/logs/server.log
Probable cause	SSL communication is broken between CSA search service and Elastic search

Solution	Disable SSL communication between CSA search service and Elastic search:
	Edit `app.json` under `csa_home\csa-search-service`, search for searchEngine URL and replace https with http as shown below.
	`"searchEngineURL": "http://<CSA_NODE1>:9201",`
	Edit `elasticSearch.yml` under `CSA_HOME/elasticsearch-1.6.1/config`, search for searchguard.enabled and replace true to false as shown below
	`searchguard.enabled: false`
	Restart Search service and ElasticSearch service

Known Issues

1. The version of ElasticSearch used in CSA is 1.6.1. There is a plan to upgrade to newer version.
2. Once a subscription is canceled or expired, the service instance properties will be empty upon search. But global search will still list the canceled and expired subscriptions.
3. Elastic search log files fill up the disk space, each being larger than 5-6 GB.
   Edit `/elasticsearch/config/logging.yml` and change `es.logger.level` from debug to error.

For any other issues check the logs from the following location:

On Windows, `CSA_HOME\csa-search-service\bin\daemon\hpesearchservice.err.log` and `CSA_HOME\elasticsearch-1.6.1\logs`.

On Linux, `CSA_HOME/csa-search-service/bin/.msvc/msvc.log` and `CSA_HOME/elasticsearch-1.6.1/logs`

To debug the logs, enable logging level to debug in `logging.yml` under `CSA_HOME\elasticsearch-1.6.1\config`.

Send documentation feedback

If you have comments about this document, you can send them to clouddocs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hpe.com.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hpe.com.