Hewlett Packard
Enterprise

Cloud Service Automation

Deployment Architectures

Software version: 4.80

Document release date: January 2017

Software release date: January 2017

Contents

Purpose

HP CSA is part of a larger cloud solution required by the customer to provide private cloud, public cloud or hybrid cloud for their end users. HP CSA itself has three (3) components that have dependencies and constraints to deploy them in different parts of the overall solution. The components of CSA are CSA-Controller (CSA-C), Identity Management (IDM) and Marketplace Portal (MPP). The complexity has increased between CSA3.2 and CSA4.0 due to the technology involved with MPP and IDM. The MPP is developed using Node.js and IDM is based on JBoss. Node.js doesn't have support for two-token authentication as required by CAC. This has resulted in using IDM as a login form provider. Since the login page is provided by IDM, there is a requirement to have some access to IDM from the MPP for user login.

This document tries to capture a few deployment architectures to help field teams understand the options available. The deployment architectures can be classified broadly into two categories

- Enterprise deployment
- Service provider deployment

The main difference between these deployments is the end users. Enterprise cloud deployments are majorly used to provide a self-service facility for the employees to obtain services with minimal involvement by IT. The cloud deployment can be independent for different groups. Cloud deployments are potentially simpler by which giving IT a greater chance to focus on services rather than building infrastructure elements like VM, DNS updates, AD updates, etc. In the service provider deployment, the end users are not part of the same organization or enterprise. End users may belong to different organizations and it is necessary for the service provider to maintain data, network and services security for each of the consumer organizations. Service providers have to provide more personalized portals for each consumer organization and maintain a separate set of authentication data. With all these put together, the deployment can be complicated and expanded.

There is no reason not to use an enterprise architecture in a service provider and vice versa.

Enterprise Deployment

The following are deployment architectures that are used in the enterprise environment:

1. All-in-One CSA deployment:

   When the enterprise IT is the main user who is trying to standardize the service creation, eliminate user errors and optimize the time taken to provide IT services, the CSA deployment can be very simple. All IT engineers will have access to the end user portal (MPP) and admin portal. With limited business users, the co-located MPP is ideal. All three components are installed on a single server, are rightfully sized, and all end users access the portal on the server.

2. All-in-One with remote MPP:

   The enterprise has multiple departments or groups that need access to the MPP for obtaining standardized services offered by the IT department. The departments/groups are geographically distributed. Though the groups have network connectivity, due to geographic separation, they may see a slow response with the 'all-in- one' CSA deployment. The MPP can be remotely located near the departments/groups, giving a better response to users.

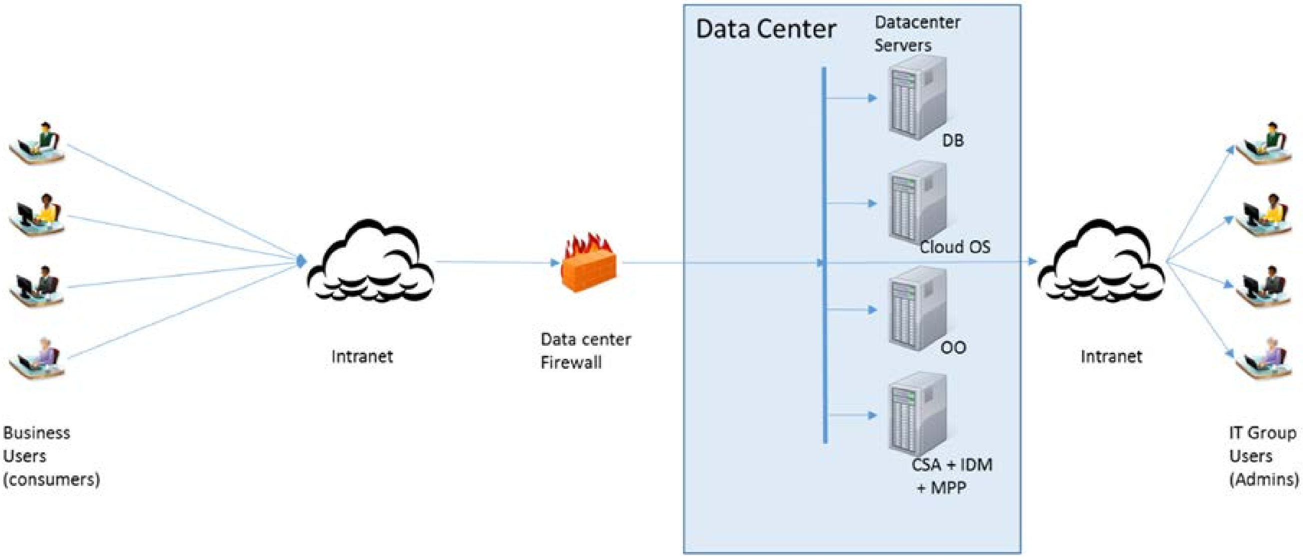
3. Remote MPP only with CSA:

   Enterprise IT wants to separate the MPP from the CSA-C and IDM server. This is an architecture where MPP is not installed on the CSA-C and IDM server. There may be more than one remote MPP instance installed, used by IT as well as business users.

All-in-One CSA

In this setup, all components (CSA-C, IDM and MPP) are installed on the same server. This is the default installation option for CSA. CSA include JBoss and Node.js.

Figure 1 All-in-One CSA architecture



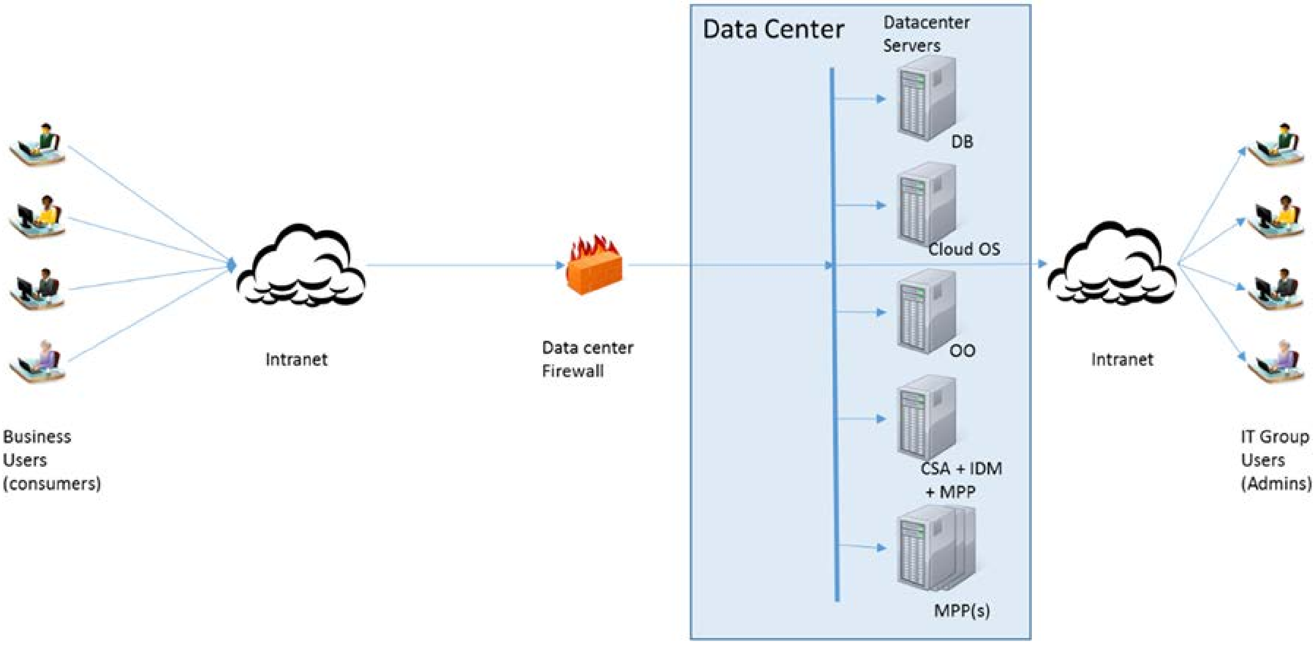
Customers interested in setting up a cluster using this approach can follow the cluster configuration guide provided as part of the product manuals. The CSA-Controller and IDM are set up inside a JBoss cluster where Infinispan is used as a federated store for tokens by IDM. The MPP can run independently or in a Node.js cluster environment.

The Apache proxy server may be installed on one of the cluster nodes as described in the cluster configuration guide or on a separate server.

All-in-One CSA with remote MPP

This will be very similar to the all-in-one CSA with additional MPP servers supporting different user groups. In CSA4.00, the MPP needs access to the CSA database for validation. To install a remote MPP, follow the documented procedure to remove certain components and leave only the MPP on the server. It is important to make sure the SSL certificates are properly imported between the remote MPP and IDM.

Figure 2 All-in-one CSA with remote MPP

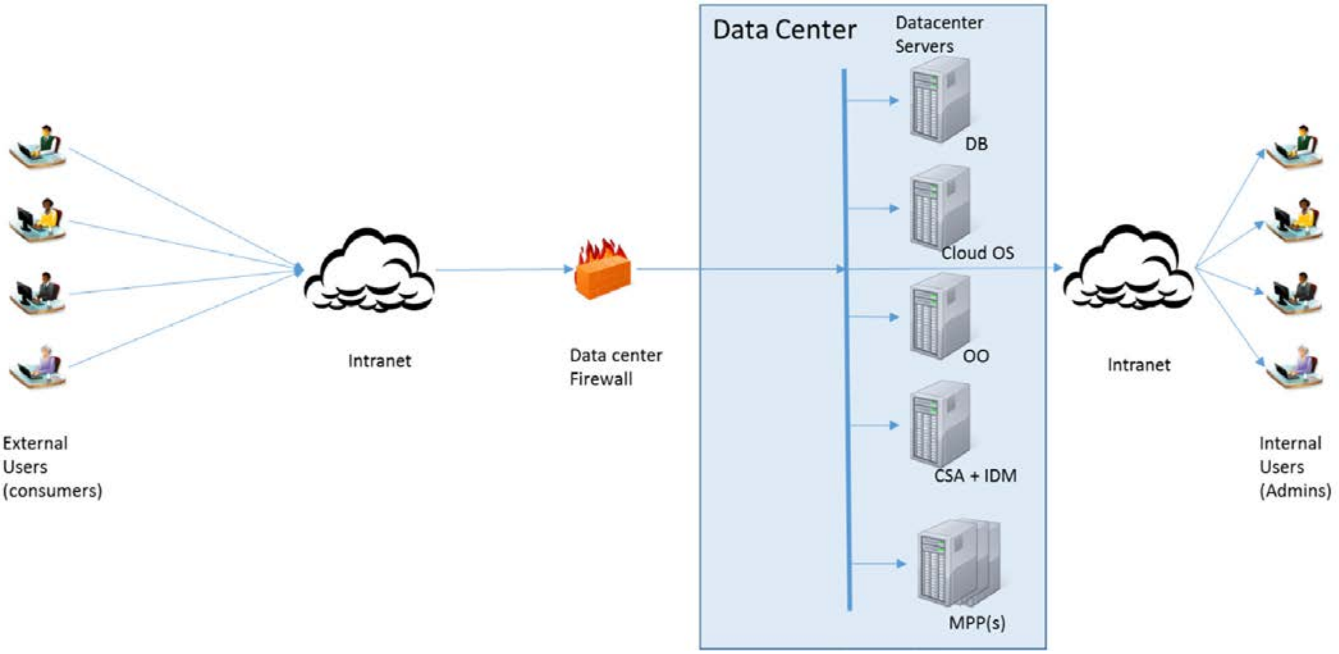


Customers requiring cluster setup with this architecture should set up the JBoss cluster as detailed in the cluster configuration guide, with an Apache proxy server to access the CSA-Controller and IDM and a proxy server with a load balancer to balance the load between one or more remote MPP installations.

Remote MPP only with CSA

This setup is the same as an 'all-in-one CSA with remote MPP' except that the MPP installed with CSA on the CSA-C and IDM server will be removed/deactivated. MPP access is always through the remote MPP. Access to the CSA-C system will be eliminated for end user operation except for the login process. The remote MPP installation is the same as in the 'all-in-one CSA with remote MPP' architecture.

Figure 3 Remote MPP only with CSA



Customers requiring a clustered environment with this architecture can set up a JBoss cluster for CSA-C and IDM with an Apache proxy. The JBoss cluster will be a standard setup and steps are available in the cluster configuration guide. MPPs can be set up as a Node.js cluster or independent MPP sessions.

Service Provider Deployment

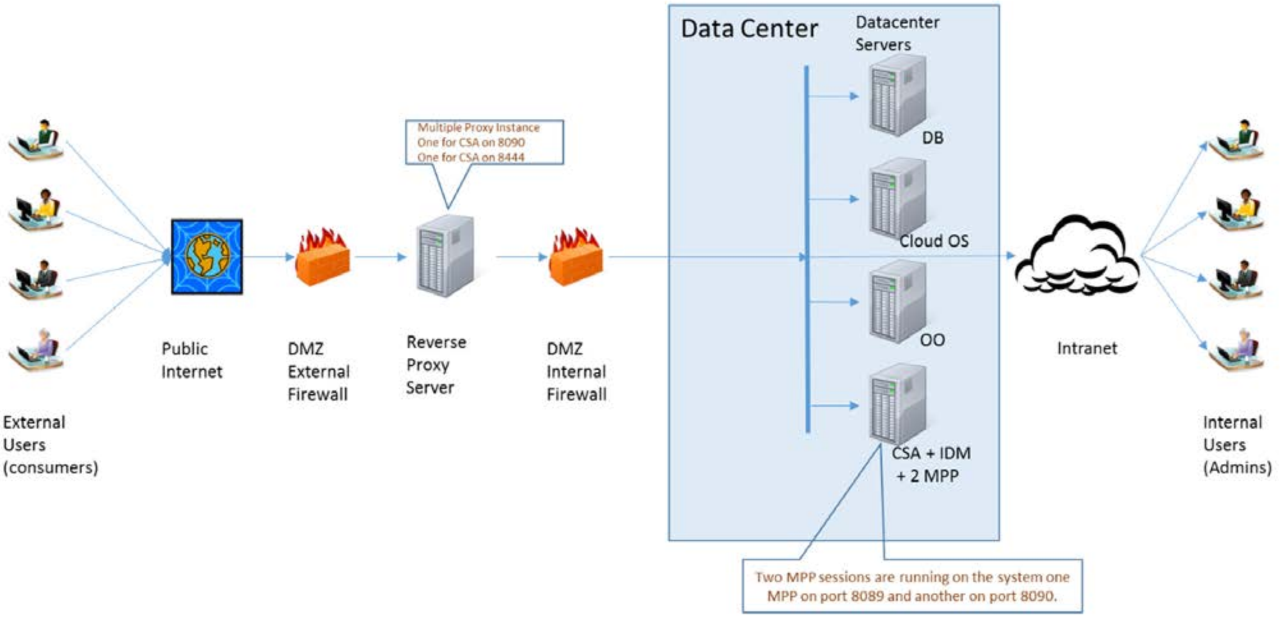
The following are the architectures for the Service Provider environment with restrictions on the consumer accessing the servers in the datacenter. The Reverse-Proxy servers are deployed in the DMZ and the end users only have access to the Reverse-Proxy server in the DMZ through a firewall.

1. All-in-One Secure CSA
2. Remote MPP with IDM
3. Reverse Proxy Cascading

All-in-One Secure CSA

From an installation process perspective, this is identical to an all-in-one CSA installation. Once the installation is complete, a second instance of the MPP is set up on the CSA system.

Figure 4 All-in-one Secure CSA



The procedure to set up a second MPP on the CSA server is as follows:

```
cd <CSAHOME>\

         copy portal folder; paste as portalexternal
cd  <CSAHOME>\portalexternal\bin

         edit install_mpp.js - change 'HP Marketplace Portal' to add the
string 'external'

         'HP Marketplace Portal' => 'HP Marketplace Portal external'
cd  <CSAHOME>\portalexternal\nodemodules\mppserver\conf\

         edit mpp.json
         replace port with 8090

         replace IDM url with right port and proxy server name
```

The above procedure will register a second MPP service with the name ‘HP Marketplace Portal external’.

Now it is necessary to set up the Apache proxy with multiple virtual hosts to allow users to access CSA through a proxy server. The Apache proxy server configuration will be as follows (ssl.conf). The procedure to set up multiple Apache proxy servers on a single server can be reviewed at http://wiki.apache.org/httpd/RunningMultipleApacheInstances. Update the highlighted values to match the environment.

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443 https

Listen 8090

Listen 8444

ServerName <ReverseProxyHost>

SSLPassPhraseDialog  builtin

SSLSessionCache         shmcb:/var/cache/mod_ssl/scache(512000)
SSLSessionCacheTimeout  300

SSLMutex default

SSLRandomSeed startup file:/dev/urandom  256
SSLRandomSeed connect builtin
SSLCryptoDevice builtin

<VirtualHost <ReverseProxyHost>:8444>
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
```

```
SSLCertificateFile /etc/pki/tls/certs/revproxy-01.crt
SSLCertificateKeyFile /etc/pki/tls/private/revproxy-01.key
SetEnvIf User-Agent ".*MSIE.*" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<Proxy *>
  Order deny,allow
  Allow from all
</Proxy>
ProxyPass /  https://<CSAHOST>:8444/
ProxyPassReverse  / https:// <CSAHOST>:8444/
</VirtualHost>
<VirtualHost <ReverseProxyHost>:8090>
SSLEngine on
SSLProxyEngine on
ProxyPreserveHost on
SSLProtocol all -SSLv2
SSLCertificateFile /etc/pki/tls/certs/revproxy-01.crt
SSLCertificateKeyFile /etc/pki/tls/private/revproxy-01.key
<Proxy *>
  Order deny,allow
  Allow from all
</Proxy>
RewriteEngine on
ProxyPass / https:// <CSAHOST>:8090/
ProxyPassReverse  / https:// <CSAHOST>:8090/
Header edit Location <CSAHOST> <ReverseProxyHost>
</VirtualHost>
```

This architecture in a cluster mode will be very complex to maintain. It is recommended to migrate to another architecture if clustering is a requirement from the customer.

Remote MPP with IDM

This architecture includes a remote MPP installed with the IDM service. The IDM service is independent of the IDM service running on other MPP servers and on the CSA server. IDM will communicate with the CSA-Controller for all LDAP details and communicate with the LDAP potentially inside the firewall.

Following will be the process of setting up this architecture:

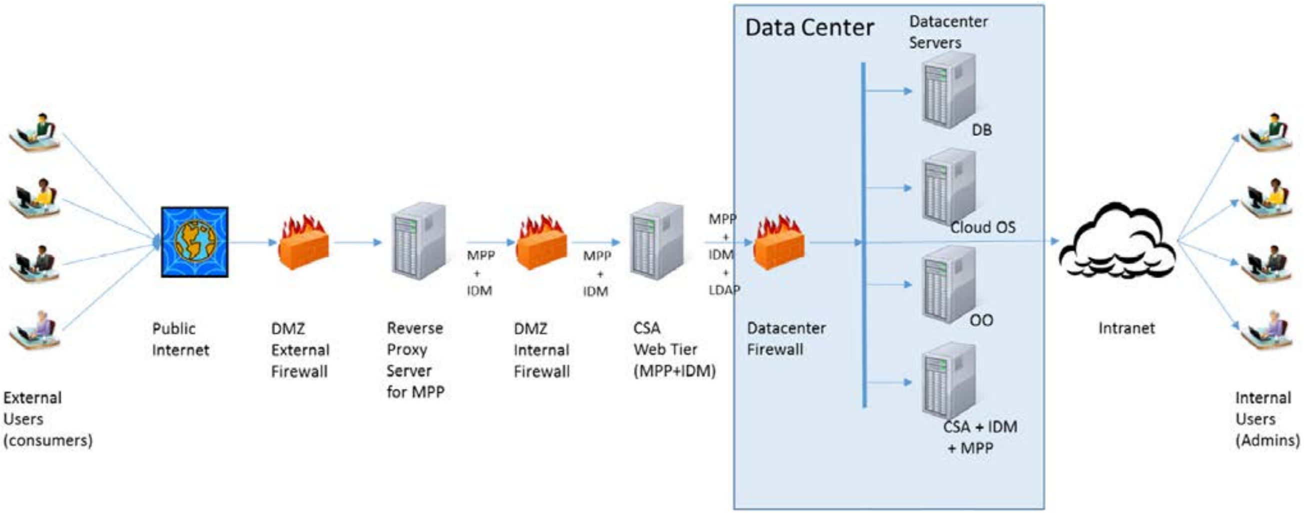
1. Install CSA 4.0 on **server1**
2. Install CSA 4.0 on **server2**
3. Remove the csa.war and csa-provider-help.war from the second installation (**server2**)
4. Rename jboss.crt on the server2 to jboss2.crt
5. Copy jboss.crt from server1 to server2 and name it jboss1.crt
6. Edited mpp.json on **server2** to look like: "provider": {

   ```
       "url": "https://<server1_FQDN>:8444", "contextPath":
       "/csa/api/mpp", "strictSSL": true,

       "secureProtocol": "SSLv23_method",
       "ca": "C:/Program Files/Hewlett-Packard/CSA/jboss-as-
   7.1.1.Final/standalone/configuration/jboss1.crt"
     },
     "idmProvider": {
       "url": "https://<server2_FQDN>:8444", "returnUrl":
       "https://<server2_FQDN>:8089",
       "contextPath": "/idm-service", "username":
       "idmTransportUser",

       "password": "ENC(UjHqZNQwz3aV5fESqx4Zx5xlcPOWh1JyR7huf9spJDo=)", "strictSSL":
       true,

       "secureProtocol": "SSLv23_method",
       "ca": "C:/Program Files/Hewlett-Packard/CSA/jboss-as-
   7.1.1.Final/standalone/configuration/jboss2.crt"
     },
   ```

   *Jboss1.crt is the certificate for server1 and jboss2.crt is the certificate for server2
7. Edit <csa_home>\jboss-as-7.1.1.Final\standalone\deployments\idm-service.war\WEB-INF\spring\applicationContext.properties on **server2** to look like:

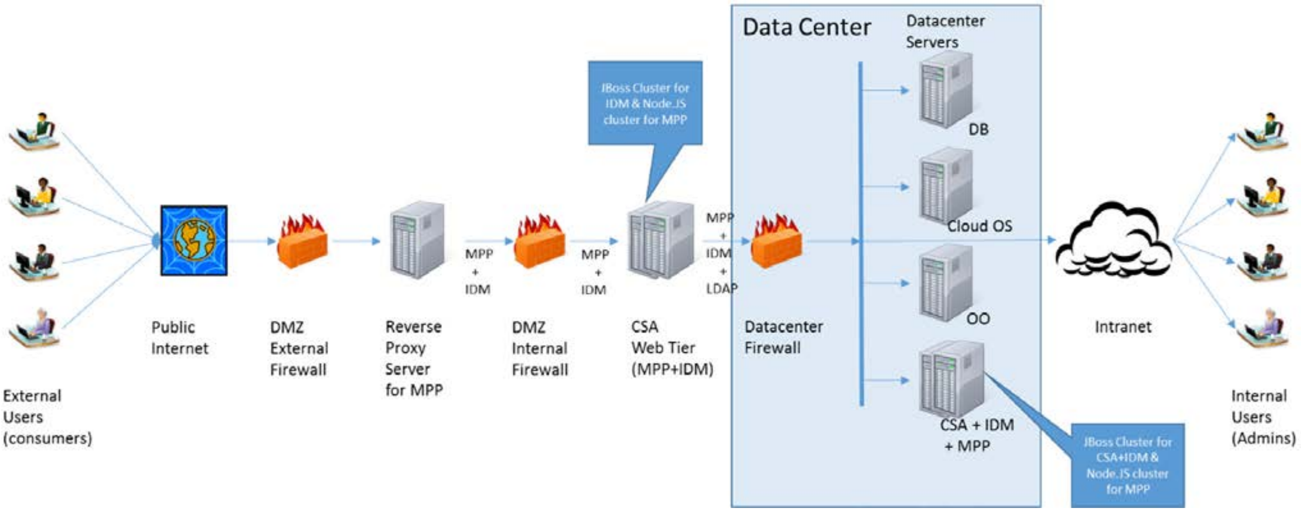
   ```
   idm.ssl.requireValidCertificate = true
   # Properties of CSA server that manages organization LDAP configurations idm.csa.protocol
   = https

   idm.csa.hostname = server1
   idm.csa.port = 8444
   ```
8. Import the server1 certificate (jboss1.crt) into the server2 cacerts file from the java used by CSA (<jre_used_by_csa >\lib\security)
9. Restart the CSA/MPP services on **server2**
10. Open the browser and type https://<server2_fqdn>:8444/mpp/ to access CSA on server1

Figure 5 Remote MPP with IDM



Clustering can be achieved at different levels. It is recommended to have the CSA-controller, IDM and MPP installed in the datacenter to follow the clustering setup as detailed in the cluster configuration guide. Depending on the consumer organization contract, MPP and IDM in the web tier may be clustered using a JBoss cluster and Node.js cluster.

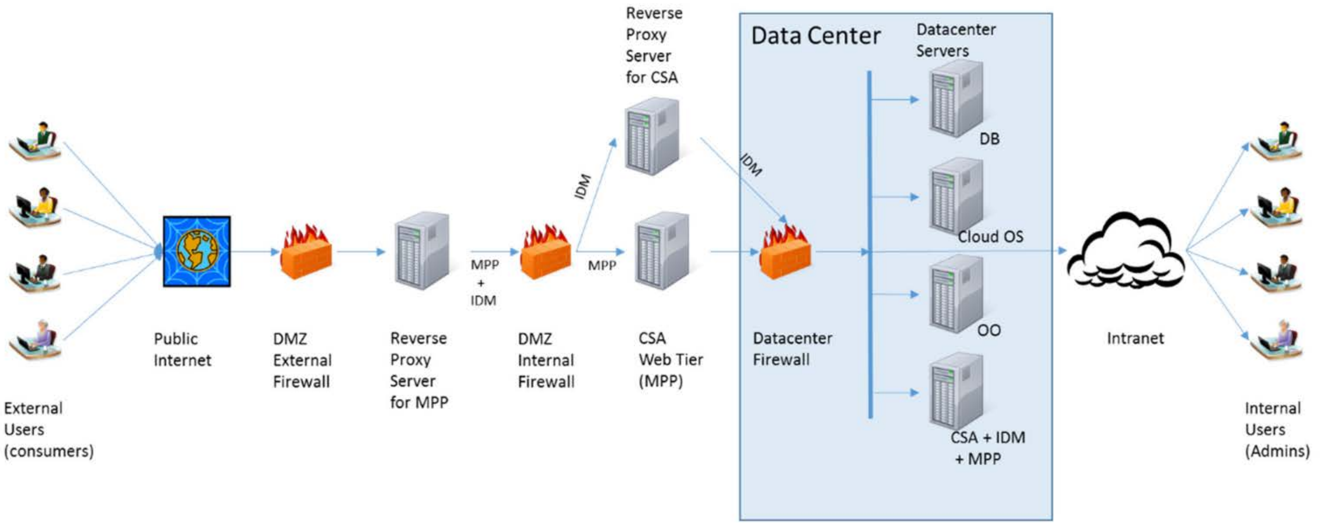
Figure 6 Remote MPP with IDM in a cluster setup



Reverse Proxy Cascading

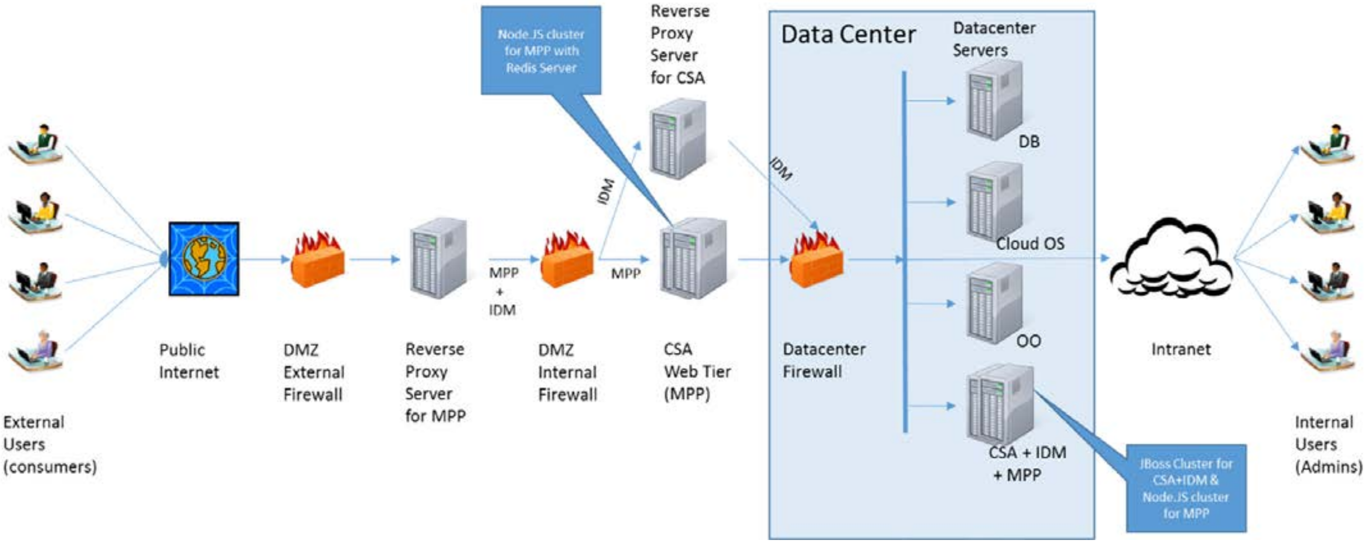
This architecture will represent a central IDM setup where the remote MPP depends on IDM running on the CSA server inside the datacenter. Access to IDM for the login form is achieved through the reverse proxy. The reverse proxy setup for MPP will in turn connect to the reverse proxy setup for IDM. This isolates the CSA server running CSA-Controller, IDM and possibly another session of MPP. The servers in the DMZ or a server communicating with the servers in DMZ are not in the datacenter. This ensures that end users have no access to perform any malicious activity on the datacenter server.

Figure 7 Reverse Proxy Cascading



The cluster setup of this architecture will follow details in the Cluster configuration guide. The reverse proxy may also be set up in an Apache cluster environment.

Figure 8 Reverse Proxy Cascading in Cluster

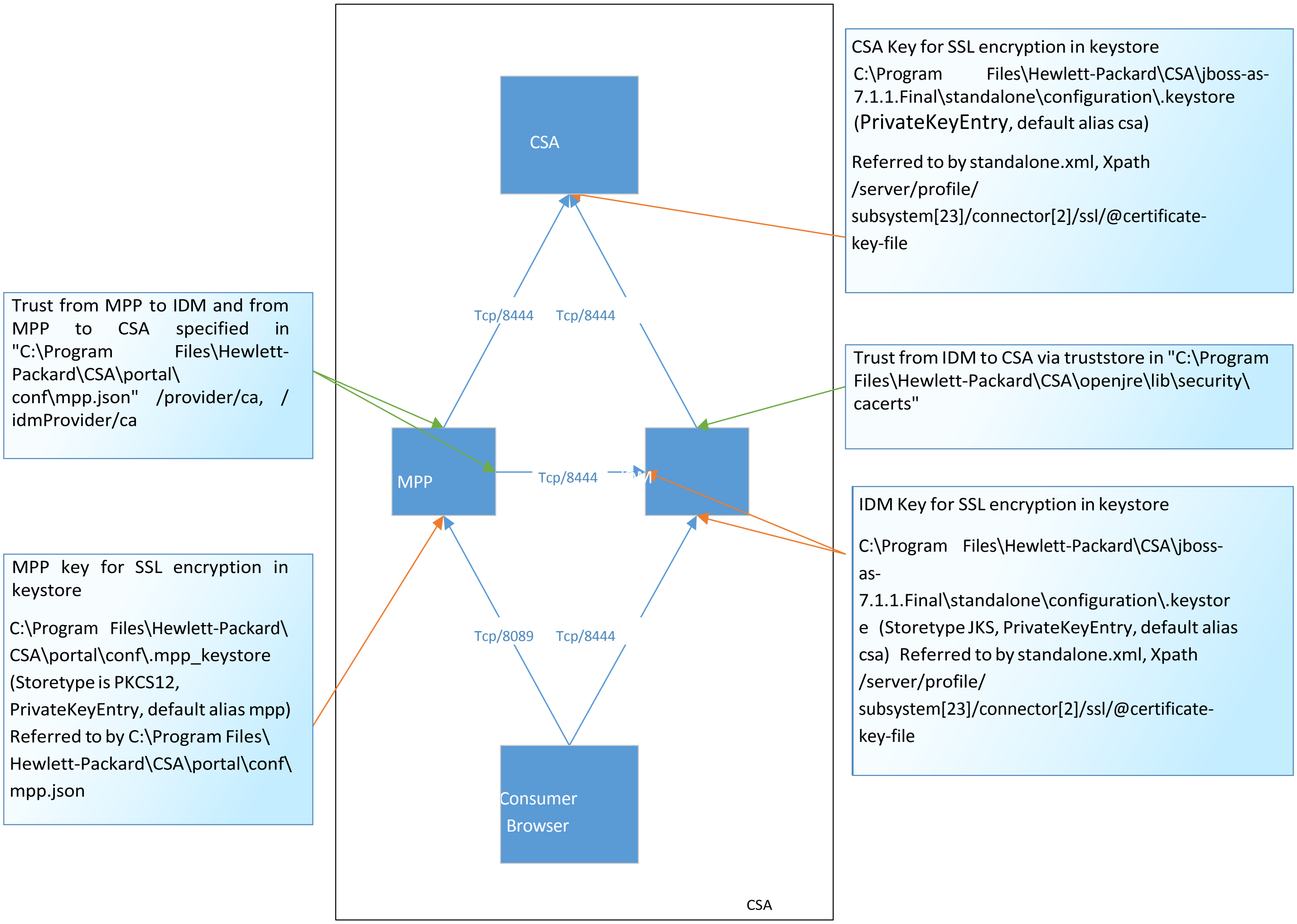


Communication between CSA Modules

SSL Certificates

The communication between the CSA modules is configurable to be secure or not. The following figure indicates how to set up the communication between the CSA modules (CSA-Controller, IDM, MPP and consumer browser) to use certificates for secure communication.

Figure 9 Certificates and trust setting



CSA Key for SSL encryption in keystore C:\Program Files\Hewlett-Packard\CSA\jboss-as-7.1.1.Final\standalone\configuration\.keystore (PrivateKeyEntry, default alias csa)

Referred to by standalone.xml, Xpath /server/profile/ subsystem[23]/connector[2]/ssl/@certificate-key-file

Trust from MPP to IDM and from MPP to CSA specified in "C:\Program Files\Hewlett-Packard\CSA\portal\conf\mpp.json" /provider/ca, / idmProvider/ca

Trust from IDM to CSA via truststore in "C:\Program Files\Hewlett-Packard\CSA\openjre\lib\security\cacerts"

IDM Key for SSL encryption in keystore

C:\Program Files\Hewlett-Packard\CSA\jboss-as-7.1.1.Final\standalone\configuration\.keystore (Storetype JKS, PrivateKeyEntry, default alias csa) Referred to by standalone.xml, Xpath /server/profile/ subsystem[23]/connector[2]/ssl/@certificate-key-file

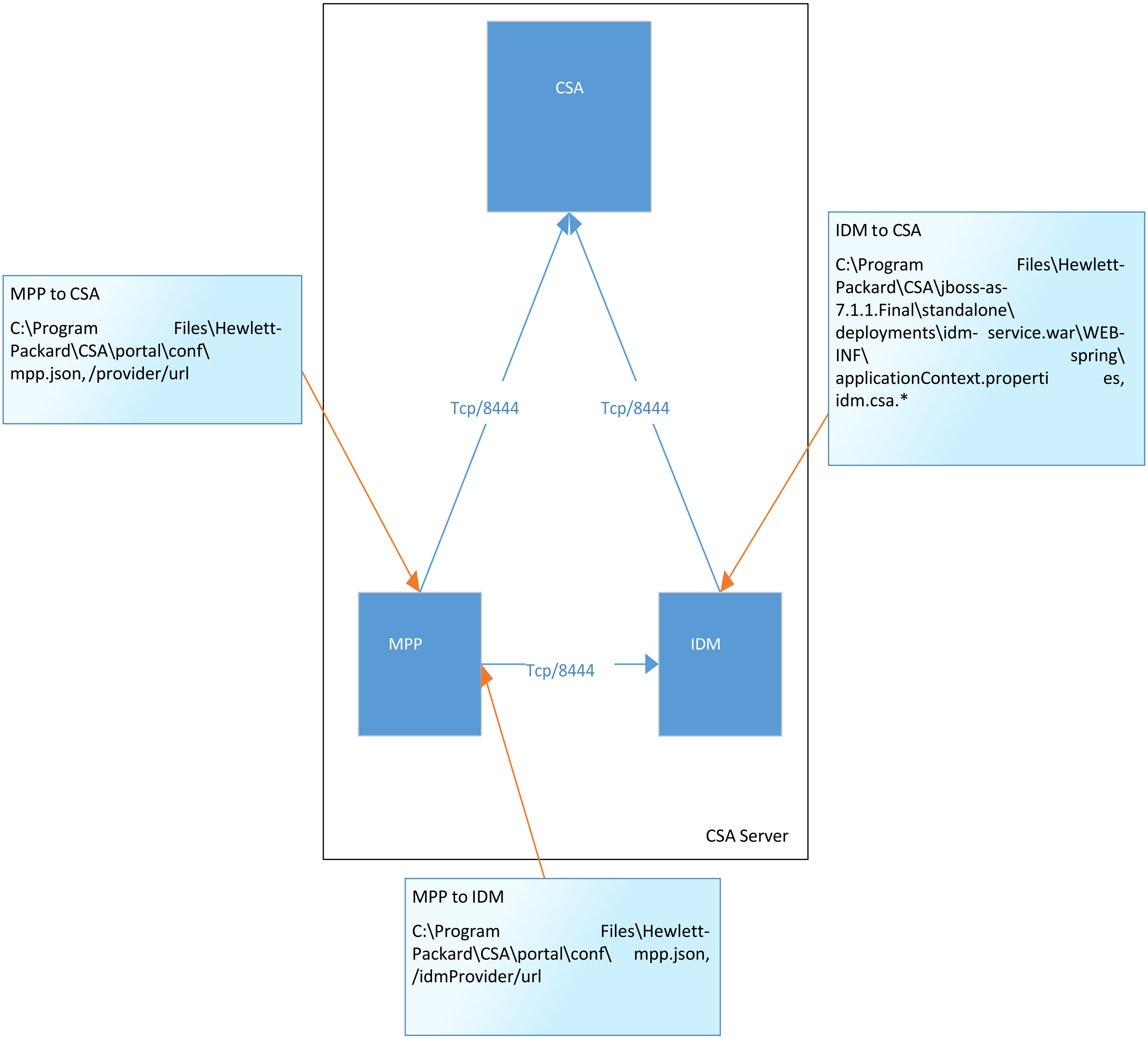
MPP key for SSL encryption in keystore

C:\Program Files\Hewlett-Packard\CSA\portal\conf\.mpp_keystore (Storetype is PKCS12, PrivateKeyEntry, default alias mpp) Referred to by C:\Program Files\Hewlett-Packard\CSA\portal\conf\mpp.json

Configuration files

The following figure indicates the files that are important in the SSL configuration. It is important to validate the values in these files for proper communication between modules as well as user communication.

Figure 10 Configuration files



MPP to CSA

C:\Program Files\Hewlett-Packard\CSA\portal\conf\mpp.json, /provider/url

IDM to CSA

C:\Program Files\Hewlett-Packard\CSA\jboss-as-7.1.1.Final\standalone\deployments\idm-service.war\WEB-INF\spring\applicationContext.properties, idm.csa.*

MPP to IDM

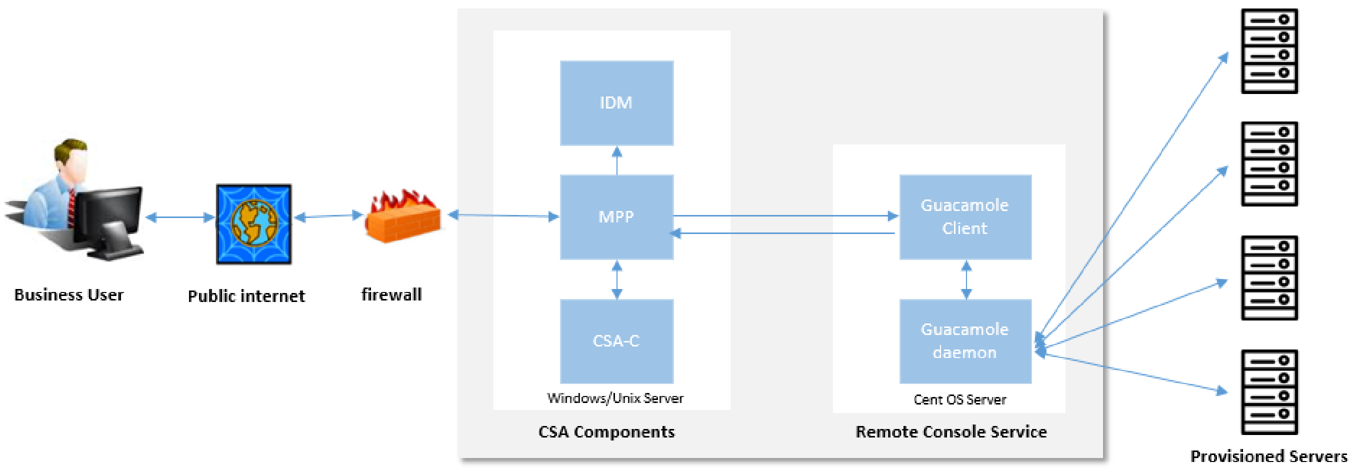
C:\Program Files\Hewlett-Packard\CSA\portal\conf\ mpp.json, /idmProvider/url

Remote Console Deployment Options

The remote console feature is introduced in CSA 4.8. This feature brings a new component RCS (Remote Console Service) into CSA Deployment model. The CSA components are CSA-Controller (CSA-C), Identity Management (IDM), Marketplace Portal (MPP) and Remote Console Service (RCS).

MPP provides access to remote console of the provisioned servers. Every server component in the service instance details page will have an Open Console button that connects directly to the server through Web Browser. Remote console service is running on a separate CentOS server. RCS needs to be installed separately and is not part of core CSA installation. RCS contains 2 components, a customized guacamole client and guacamole daemon.

Block diagram of CSA components



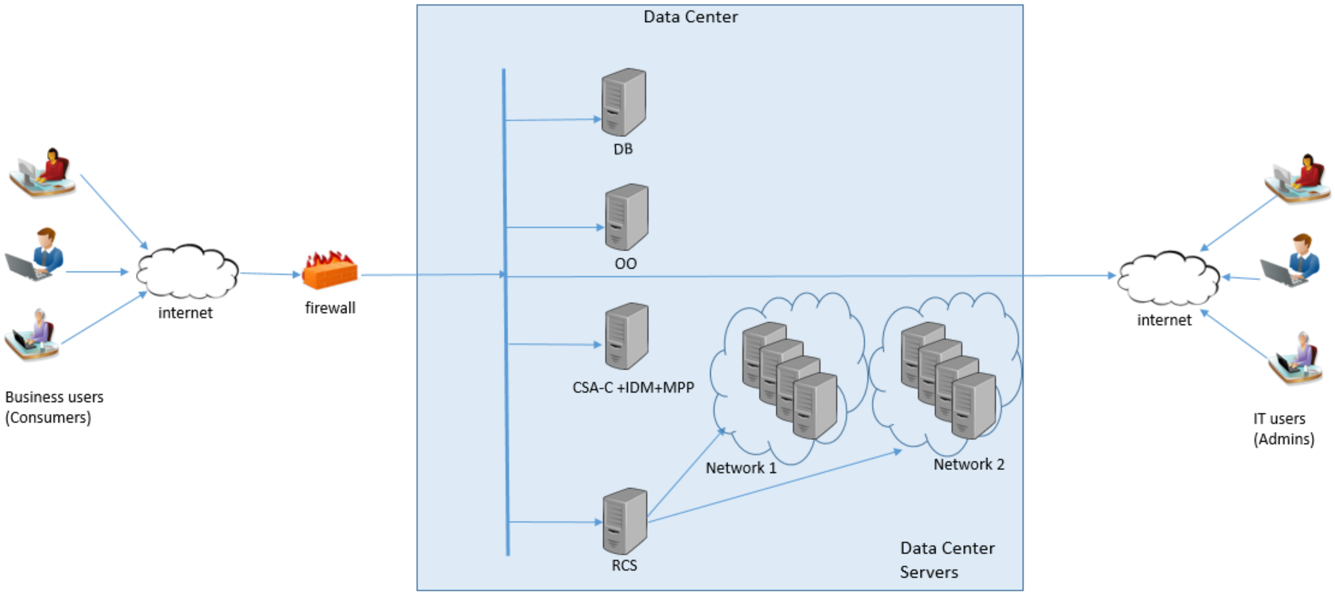
Below examples can help field teams in configuring Remote Console for customers. Remote console can support 2 types of deployment architectures.

- Single RCS
- Multiple RCS’s

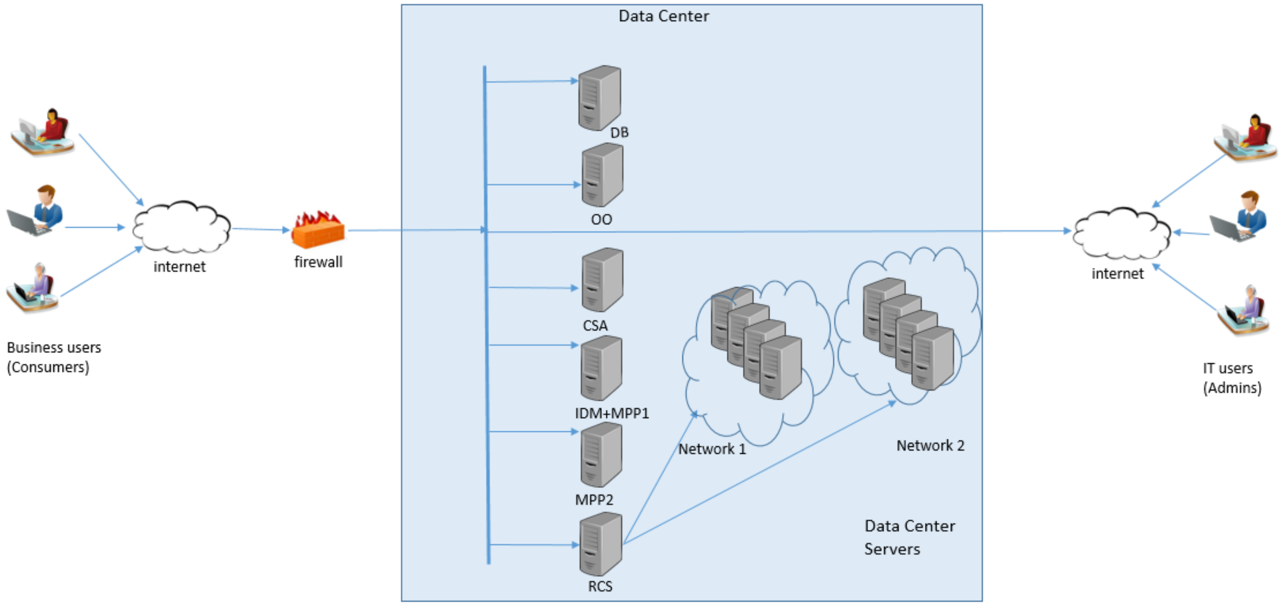
In both the deployment options, there can be always only one RCS mapped to one MPP.

Single RCS

In this deployment architecture, there will be a single instance of RCS installed on a CentOS server. RCS should have network access to MPP. Also, RCS should be in the same network as provisioned servers so that it can establish a remote connection with them. The remaining CSA components CSA-C, MPP and IDM can be installed on the same server or can be distributed across different servers. Single RCS can be supported for Enterprise Deployment Architectures mentioned above in this document. Below example depicts the RCS deployment in an “All in one CSA” enterprise architecture



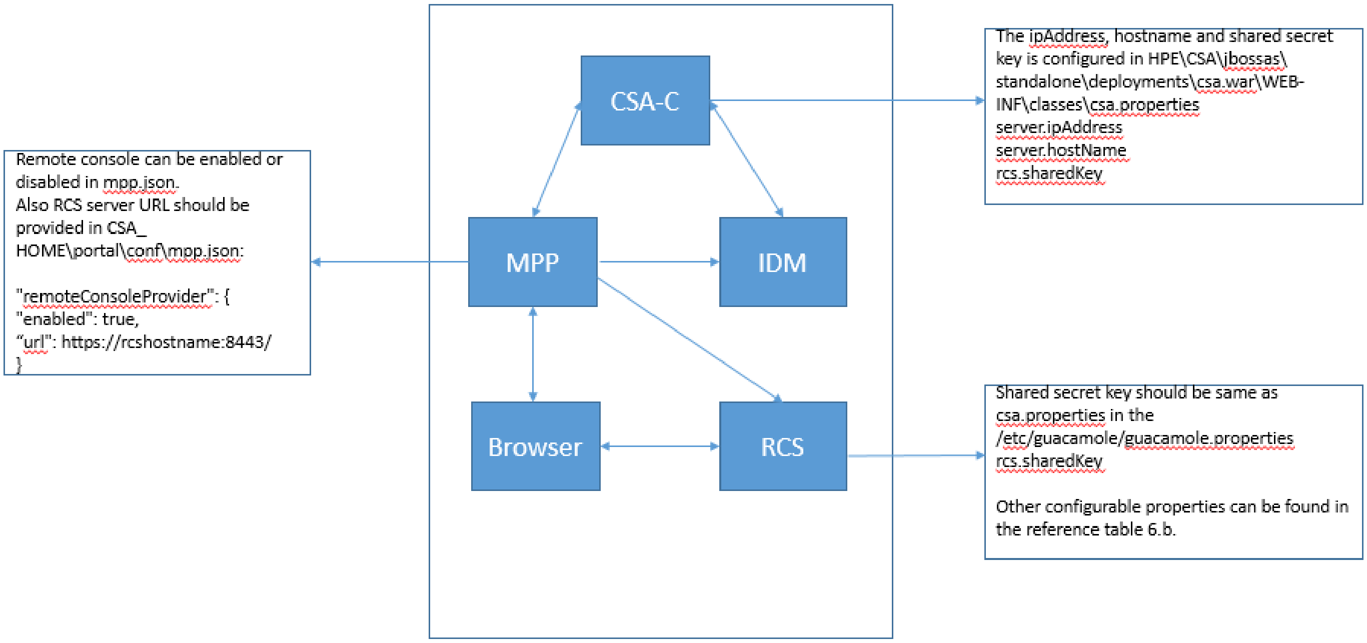
Below example describes the single RCS deployment in a distributed CSA architecture (With remote MPPs).



In the above CSA setup, multiple MPP instances are installed remotely. However, there is only a single instance of RCS that can connect to all the MPP instances and provisioned servers that are distributed across networks.

Configuration of the single RCS

Below diagram briefly explains on the components to be configured for single RCS.



Remote console can be enabled or disabled in mpp.json.
Also RCS server URL should be provided in CSA_ HOME\portal\conf\mpp.json:

"remoteConsoleProvider": {
"enabled": true,
“url": https://rcshostname:8443/
}

The ipAddress, hostname and shared secret key is configured in HPE\CSA\jbossas\ standalone\deployments\csa.war\WEB-INF\classes\csa.properties
server.ipAddress
server.hostName
rcs.sharedKey

Shared secret key should be same as csa.properties in the /etc/guacamole/guacamole.properties
rcs.sharedKey

Other configurable properties can be found in the reference table 6.b.

Configure MPP

In single RCS model, all MPP instances will point to the same RCS server. The file CSA_HOME\portal\conf\mpp.json has new entries for remote console –

"remoteConsoleProvider": {

"enabled": true,

“url": https://rcshostname:8443/

}

The enabled field is used to enable/disable the remote console feature. When the value for enabled field is false, the Open Console button does not appear in the MPP portal. By default, out of the box installation will have remote console enabled.

The url field needs to be configured post RCS installation. The hostname and port of the RCS server should be provided. When there are multiple instances of MPP, all the MPP instances are configured with the same url.

Configure CSA-C

In the file HPE\CSA\jbossas\standalone\deployments\csa.war\WEB-INF\classes\csa.properties, 3 properties have to be configured for remote console.

1. *server.ipAddress*

   This property should map to the IP Address field names used in the customized service designs. Example: ipAddress, primary_ip_address, ipAddress_1 etc.

2. *server.hostName*

   This property should map to the Hostname field name used in the customized service designs.

   Example: hostname, host, fqdn etc.

3. *rcs.sharedKey*

   This is a secret shared key between RCS and CSA-C and should have same value for the field rcs.sharedKey in guacamole.properties and csa.properties. A unique value will be generate at the time of RCS installation for the field rcs.shareKey which needs to be copied to csa.properties.

   It is recommended not to use the same shared key for a longer duration. Shared key can be changed to any value and when the key is changed, care should be taken to have same value in CSA-C and RCS, else remote console authentication will fail.

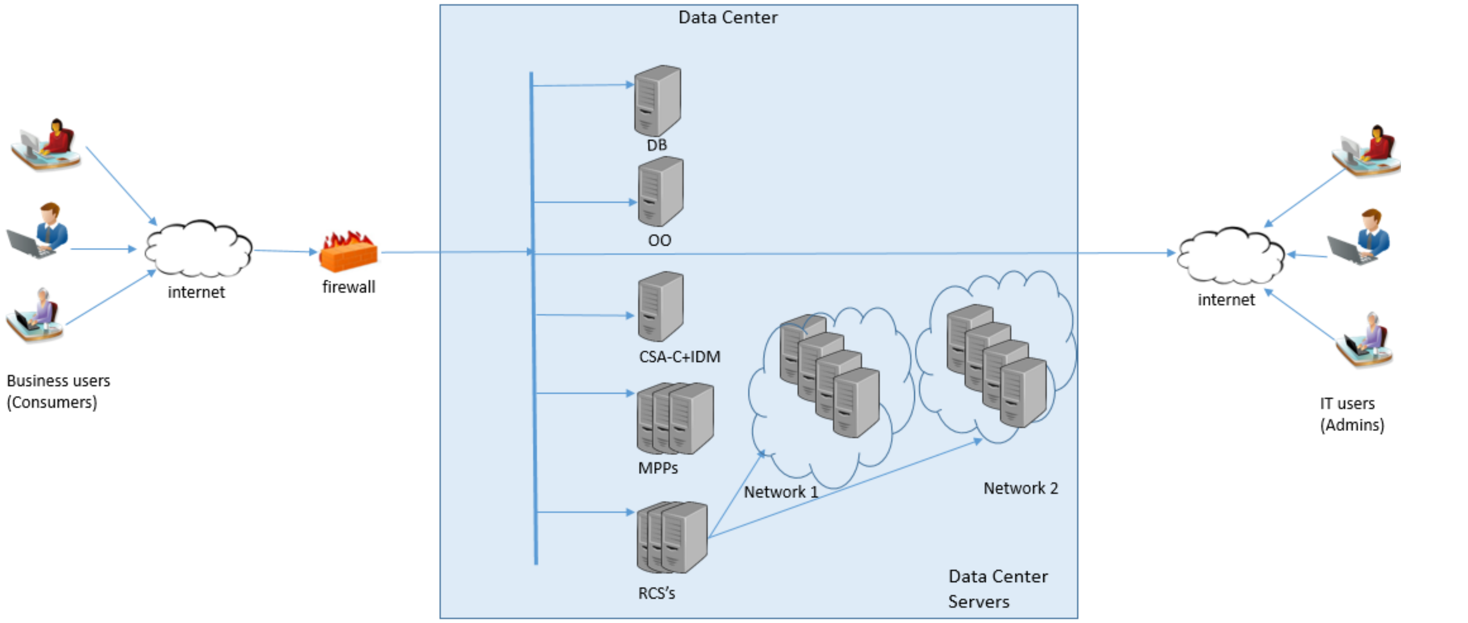
Configure RCS

Refer to section Install and Configure Remote Console Service in the CSA installation guide. It provides detailed procedure of installing RCS, configuring SSL and modifying the RCS configuration post installation.

Multiple RCS's

Multiple RCS's Architecture is mostly used when there are multiple remote MPP installations. Service provider architecture is an example where there can be a restriction of having separate networks in the data center for different organizations. In such cases, MPP and RCS instances should be running on the same network for each organization. The provisioned servers in the data center exist on separate network for every organization.

Below is an example that represents Multiple RCS's deployment architecture –



In multiple RCS's deployment architecture, there should be always a one-one mapping between MPP and RCS i.e. every MPP can support only one RCS.

Configuration of Multiple RCS's

Configure MPP

In Multiple RCS's model, each instance of MPP instances will point to different RCS server.

The file CSA_HOME\portal\conf\mpp.json on MPP1 should be configured –

```
"remoteConsoleProvider": {
"enabled": true,
“url": https://rcshostname-1:8443/
}
```

The file CSA_HOME\portal\conf\mpp.json on MPP2 should be configured –

```
"remoteConsoleProvider": {
"enabled": true,
“url": https://rcshostname-2:8443/
}
```

The enabled field is used to enable/disable the remote console feature. When the value for enabled field is false, the Open Console button does not appear in the MPP portal. By default, out of the box installation will have remote console enabled.

The url field needs to be configured post RCS installation on the MPP server. The hostname and port of the RCS server should be provided. When there are multiple instances of MPP, all the MPP instances are configured with corresponding RCS url.

There can be few remote MPP nodes with remote console feature enabled and few with this feature disabled.

Configure CSA-C

The configuration on CSA-C for remote console is the same as single RCS except for the rcs.sharedKey field. The shared key between all RCS servers and CSA-C should be same.

Configure RCS

Refer to section Install and Configure Remote Console Service in the CSA installation guide. It provides detailed procedure of installing RCS, configuring SSL and modifying the RCS configuration post installation.

For Multiple RCS deployment model, every RCS instance should have the same rcs.sharedKey in guacamole.properties.

For more information

To access other toolkits to design and extend cloud services running on HPE CloudSystem, go to hpe.com/go/csdevelopers. For more information on HPE CloudSystem, visit hpe.com/go/cloudsystem.

The HPE Live Network Portal can be found at https://hpln.hp.com/solutions.

HPE software product manuals and documentation for the following products can be found at h20230.www2.hp.com/selfsolve/manuals. You will need an HP Passport to sign in and gain access.

- HPE Cloud Service Automation
- HPE ArcSight
- HPE Operations Orchestration
- HPE Server Automation
- HPE SiteScope
- HPE Universal CMDB

To help us improve our documents, please send feedback to CSAdocs@hpe.com.

Learn more at hpe.com/go/CSA

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.