Prime Service Catalog and CloudCenter Integration

Creating a New Self-Signed Certificate

March 22, 2017

Version 1.0

Cisco Systems, Inc.
Corporate Headquarters
170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel: 408 526-4000 Toll Free: 800 553-NETS (6387)
Fax: 408 526-4100

Contents

1 INTRODUCTION 3

1.1 PREFACE 3
1.2 ASSUMPTIONS 3
1.3 RELATED DOCUMENTS 3

2 SELF-SIGNED CERTIFICATE VALIDATION FAILS 4

2.1 CREATE A NEW SELF-SIGNED CERTIFICATE FOR CLOUDCENTER 4

TRADEMARKS AND DISCLAIMERS 7

1 Introduction

1.1 Preface

This document is a set of best practices and guidelines regarding Prime Service Catalog and CloudCenter integration.

This publication IS NOT a comprehensive deployment guide and Engineers should consult other Cisco documentation as appropriate for deployment against Cisco best practices.

1.2 Assumptions

Readers of this guide must be knowledgeable of Prime Service Catalog concepts and modules, and other Cisco products, such as USC Director and CloudCenter where applicable.

1.3 Related Documents

You can find related documentation by going to the following:

- Prime Service Catalog documentation
- CloudCenter documentation

2 Self-Signed Certificate Validation Fails

The CloudCenter Virtual Appliance includes a built-in self-signed certificate that is hardcoded with the CN = “example.com”. When integrating with Prime Service Catalog (PSC) with CloudCenter, PSC connects to CloudCenter in https mode, attempts to retrieve the certificate (eg. public key) of the CloudCenter server and tries to validate (eg. trust) the certificate. The certificate validation fails because the CN in the self-signed certificate does not match with the hostname or IP address of your CloudCenter server.

The remedy for this issue is to create a new self-signed certificate for your CloudCenter server and set the common name for the certificate to match either the FQDN hostname or the IP address of your CloudCenter server. When you add a CloudCenter server on the Manage Connections UI in PSC, make sure you enter either the FQDN hostname or the IP address of your CloudCenter server, depending on what you used as the common name in the self-signed certificate.

2.1 Create a new Self-signed Certificate for CloudCenter

Do the following to create and configure a new certificate for the CloudCenter server.

1. Log in the CloudCenter machine as “root”.

2. CD to the /usr/local/tomcat/conf/ssl directory.

3. Execute the following command to generate an RSA Private Key:

   ```
   openssl genrsa -out qa.key 2048
   ```

4. Execute the following command to create a self-signed certificate:

   ```
   openssl req -new -x509 -days 365 -key qa.key -out qa.crt
   ```

   A series of prompts display. The values highlighted in red below are examples of the type of input you can enter. The most important one is the Common Name. Make sure that for Common Name, enter either the FQDN hostname or the IP address of your CloudCenter server:

   Country Name (2 letter code) [XX]:US
   State or Province Name (full name) []:California
   Locality Name (eg, city) [Default City]:San Jose
   Organization Name (eg, company) [Default Company Ltd]:Cisco
   Organizational Unit Name (eg, section) []:QA
   Common Name (eg, your name or your server's hostname) []:**172.21.36.130**
   Email Address []:khangngu@cisco.com

5. Change the ownership of the certificate files: chown cliqruser:cliqruser qa.*

6. Stop the tomcat server: /etc/init.d/tomcat stop

7. Modify file “/usr/local/tomcat/conf/server.xml” as follows:

   Search for the following line:

```
<Connector port="10443" maxHttpHeaderSize="8192"
  maxThreads="150"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  SSLEnabled="true"
  SSLCertificateFile="${catalina.base}/conf/ssl/example.com.crt"
  SSLCertificateKeyFile="${catalina.base}/conf/ssl/example.com.key"
```

   Replace with the following values:

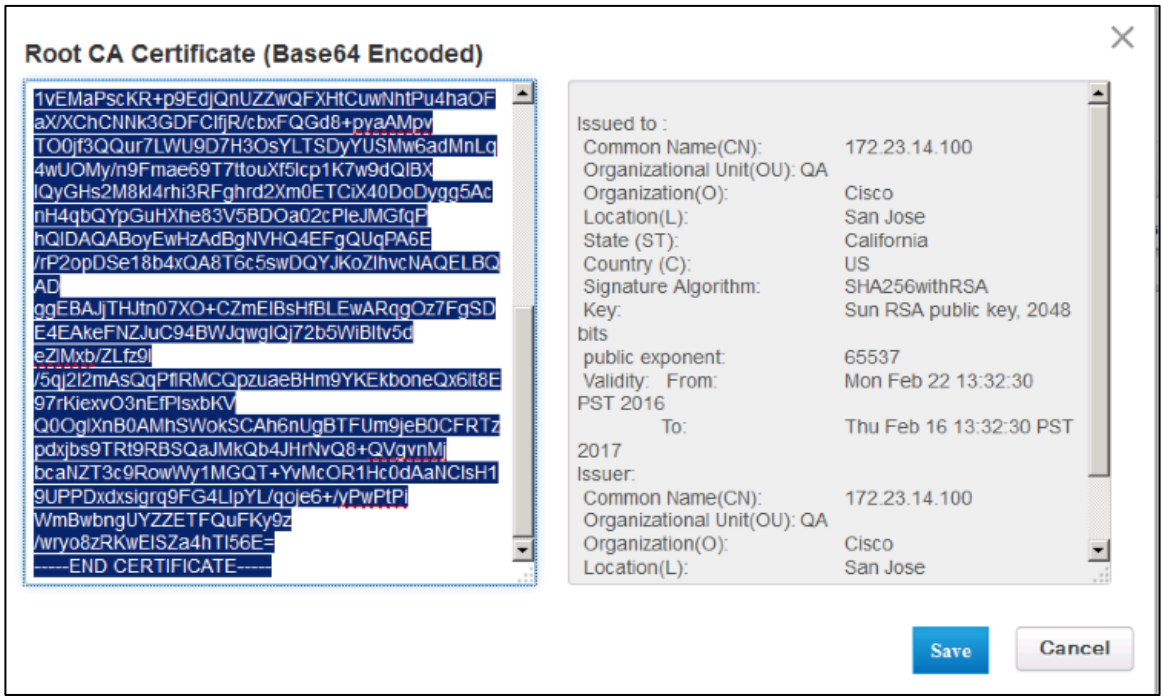
```
<Connector port="10443" maxHttpHeaderSize="8192"
  maxThreads="150"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  SSLEnabled="true"
  SSLCertificateFile="${catalina.base}/conf/ssl/qa.crt"
  SSLCertificateKeyFile="${catalina.base}/conf/ssl/qa.key"
```

8. Start the tomcat server: /etc/init.d/tomcat start

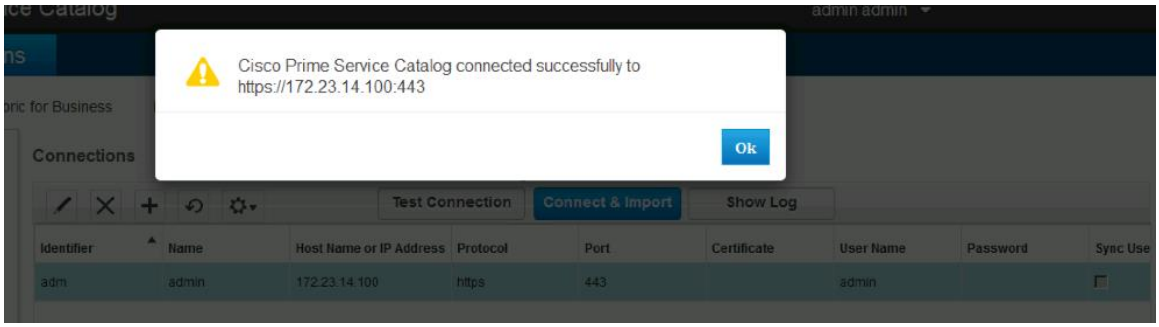
9. Tail the following log files to ensure that the CloudCenter server is started up correctly:

   tail -f /usr/local/tomcat/logs/catalina.<*current-date*>.log
   tail -f /usr/local/tomcat/logs/osmosix.log

10. On the PSC side, when you add a connection to this CloudCenter server in the Manage Connections UI, set the protocol to https, port number to 433, enter the username and password, then click the certificate button. On the popup window, copy/paste the content of the **qa.crt** file into the Root CA Certificate (Base64 Encoded) panel on the left hand side. Click **Save**. See below



11. Verify that the connection to your CloudCenter server in https mode is successful:



Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THIRD PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.