Prime Service Catalog and UCS Director Integration

Creating a New Certificate

March 23, 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 UCSD 4

TRADEMARKS AND DISCLAIMERS 8

1 Introduction

1.1 Preface

This document is a set of best practices and guidelines regarding Prime Service Catalog and UCS Director 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 ONE Enterprise Cloud Suite products where applicable.

1.3 Related Documents

You can find related documentation by going to the following:

- Prime Service Catalog documentation
- UCS Director documentation

2 Self-Signed Certificate Validation Fails

The UCS Director (UCSD) - or Cisco Intercloud Fabric for Business (ICFB) - Virtual Appliance includes a built-in self-signed certificate that is hardcoded with the common name = “Cisco, Inc.”. When integrating UCSD with Prime Service Catalog (PSC), in order for the SSL handshake to work correctly (i.e. for the PSC server to connect to the UCSD server in https mode), the common name of the certificate used by the UCSD server must match with the hostname or server name of the UCSD server. Since the certificate has a hardcoded common name of “Cisco, Inc.”, the SSL handshake fails, resulting in an error message stating that the hostname does not match.

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

2.1 Create a new Self-signed Certificate for UCSD

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

Note: *Replace the values highlighted in red with the actual values appropriate for your own environment.*

1. Log in as shelladmin to the UCSD machine.
2. Stop all UCSD services.
3. Log in as root to the UCSD machine.
4. CD to the /opt/infra/web_cloudmgr/apache-tomcat/keystore directory.
5. Execute the following command to generate a Java keystore and key pair:

```
/opt/bin/jre/bin/keytool -genkey -alias qa -validity 360 -keyalg RSA -
keysize 2048 -keystore qa.jks -storepass Cisco1234 -keypass Cisco1234
```

6. The keytool command presents a series of prompts. Ensure that for the first prompt (eg. *What is your first and last name?*), enter either the FQDN hostname or the IP address of your UCSD server. In the example below, I entered the IP address of my UCSD server. This will become the common name in my self-signed certificate.

```
What is your first and last name?
  [Unknown]:  172.23.14.100
What is the name of your organizational unit?
  [Unknown]:  QA
What is the name of your organization?
  [Unknown]:  Cisco
What is the name of your City or Locality?
  [Unknown]:  San Jose
What is the name of your State or Province?
  [Unknown]:  California
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=172.23.14.100, OU=QA, O=Cisco, L=San Jose, ST=California, C=US correct?
  [no]:
```

7. **<u>If you decide to use self-signed certificate:</u>**

   a) Execute the following command to export the root certificate for your self-signed certificate:

   ```
   /opt/bin/jre/bin/keytool -export -rfc -alias qa -keystore qa.jks -
   storepass Cisco1234 -keypass Cisco1234 -file root.cer
   ```

8. **<u>If you decide to use a signed certificate:</u>**

   a) Execute the following command to generate a certificate signing request (CSR):

   ```
   /opt/bin/jre/bin/keytool -certreq -alias qa -keystore qa.jks -storepass
   Cisco1234 -file qa.csr
   ```

   b) Follow the instructions on the following wiki page to submit your CSR for signing by the Microsoft Active Directory Certificate Services that I set up for our celosis.com lab:

   http://wikicentral.cisco.com/display/GROUP/Microsoft+Active+Directory+Certificate+Services

   c) Once you download both the signed certificate and the CA root certificate, copy both files (for example, mycert.cer and CAcert.cer) to your UCSD machine, under the /opt/infra/web_cloudmgr/apache-tomcat/keystore directory.

   d) Execute the following command to import the CA root certificate into the same keystore file that you created in Step 5:

   ```
   /opt/bin/jre/bin/keytool -import -trustcacerts -alias root -file
   CAcert.cer -keystore qa.jks -storepass Cisco1234
   ```

   e) Import the signed certificate into the same keystore file:

   ```
   /opt/bin/jre/bin/keytool -import -alias qa -file mycert.cer -keystore
   qa.jks -storepass Cisco1234
   ```

9. Modify file “opt/infra/web_cloudmgr/apache-tomcat/conf/server.xml” as follows:

   Search for the following line:

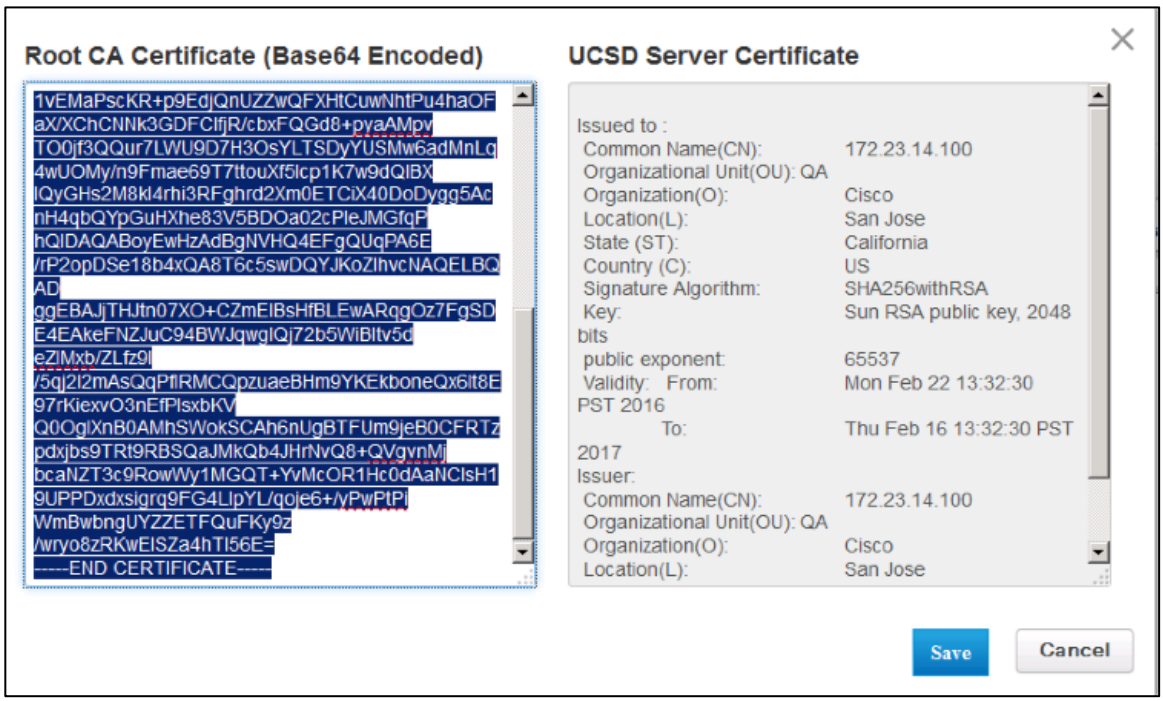
```
<Connector port=”443” protocol=”HTTP/1.1” SSLEnabled=”true”
  maxThreads=”150” scheme=”https” secure=”true”
  keystoreFile=”keystore/.keystore” keystorePass=”cloupiaadmin”
```

   Replace with the following values:

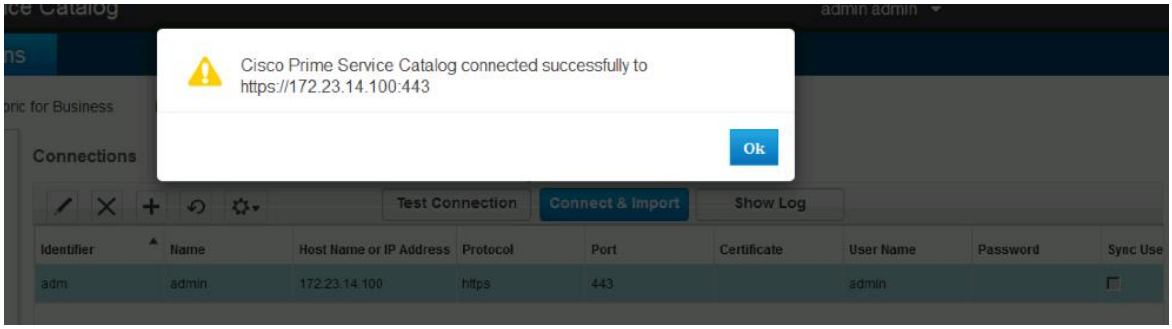
```
<Connector port=”443” protocol=”HTTP/1.1” SSLEnabled=”true”
  maxThreads=”150” scheme=”https” secure=”true”
  keystoreFile=”keystore/qa.jks” keystorePass=”Cisco1234” alias=”qa”
```

10. Start the UCSD services.

11. On the PSC side, when you add a connection to this UCSD 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 either root.cer (if you use self-signed certificate) or CAcert.cer (if you use the certificate signed by the Microsoft Active Directory Certificate Service) into the Root CA Certificate (Base64 Encoded) panel on the left hand side. Click **Save**.



12. Verify that the connection to your UCSD 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.

© 2017 Cisco Systems, Inc. All rights reserved.