Contents

[1. Onboard Administrator Modules 2](#_Toc472678406)

[1.1 IP Addresses 2](#_Toc472678407)

[2. Cisco Catalyst Blade Switch 3020 2](#_Toc472678408)

[2.1 IP Addresses 2](#_Toc472678409)

[2.2 Management interfaces 2](#_Toc472678410)

[2.3 Management Methods 3](#_Toc472678411)

[2.3.1 Device Manager 3](#_Toc472678412)

[2.3.2 telnet 4](#_Toc472678413)

[2.4 Enabling the crossover connects 4](#_Toc472678414)

[2.4.1 Disabled by default 5](#_Toc472678415)

[2.4.2 Disabled by default (text) 5](#_Toc472678416)

[3. Bl460c G1, Bay 1 6](#_Toc472678417)

[3.1 Resource information 6](#_Toc472678418)

[3.2 iLO 6](#_Toc472678419)

[3.3 Boot order 6](#_Toc472678420)

[3.4 HBA: Local storage 6](#_Toc472678421)

[3.5 Intel VT-x 7](#_Toc472678422)

[4. Brocade 4/12 SAN Switch for HP c-class BladeSystem 7](#_Toc472678423)

[4.1 IP Addresses 8](#_Toc472678424)

[4.2 Management Console security 8](#_Toc472678425)

[4.3 Fix 9](#_Toc472678426)

[4.4 Credentials 9](#_Toc472678427)

[5. Browsers 9](#_Toc472678428)

[5.1 OA Web App Requirements 9](#_Toc472678429)

[5.1.1 Browser: Chrome 10](#_Toc472678430)

[5.1.2 Browser: Internet Explorer 10](#_Toc472678431)

[5.1.3 Browser: Firefox 11](#_Toc472678432)

[5.2 iLO Remote Console Requirements 11](#_Toc472678433)

[5.2.1 Using the Java iLO Remote Console 11](#_Toc472678434)

[5.2.2 Remote Console security 12](#_Toc472678435)

[5.2.3 Updated: Remote Console Security 14](#_Toc472678436)

[5.2.4 Trace: Correct Operation 14](#_Toc472678437)

[5.2.5 Trace: Operation with TLS 1.2 only 18](#_Toc472678438)

[5.2.6 Trace: Operation without any TLS selected 21](#_Toc472678439)

# 1. Onboard Administrator Modules

## 1.1 IP Addresses

Machine generated alternative text:
bicOO 
the settings are applied you will have to sign in to the Onboard Administrator again using the new settings 
Changing the Onboard Administrator's DNS Name could cause a hostname mismatch on the SSL certificate You may have to update the certificate 
Information on any Onboard Administrator whose DNS Name is changed 
Active Onboard Administrator Network Settings 
O DHCP 
Enable Dynamic DNS 
Standby Onboard Administrator Network Settings 
O DHCP 
Enable Dynamic DNS 
@ Static IP Settings 
Required Field • 
DNS Host Name • 
M AC Address 
IP Address • 
Subnet Mask • 
DNS server 1 
DNS server 2 
oaO 
OO IF:29EC 7C:ED 
0001 
2SS2SS2ss 192 
@ Static IP Settings 
Required Field • 
DNS Host Name • 
M AC Address 
Subnet Mask • 
DNS server 1 
DNS server 2 
cal 
0002 
2SS2SS2ss 192 

# 2. Cisco Catalyst Blade Switch 3020

## 2.1 IP Addresses

* + <http://10.0.0.31> (fa0 interface for switch in bay 1)
  + <http://10.0.0.32> (fa0 interface for switch in bay 2)

## 2.2 Management interfaces

**Management interfaces**

* fa0
  + Internal connection to OA
  + **This is used in my configuration**
* VLAN 1
  + External connection, accessible through switch ports
  + **This is not used in my configuration**

**Procedure**

* Set up fa0 by resetting each Catalyst Blade Switch.
* This prompted the switch to claim an IP address through the enclosure's bay IP addressing system.
* The "Cisco Catalyst Blade Switch 3020 for HP Getting Started Guide" refers to EBIPA as "Onboard Administrator is configured to run as a DHCP server"

## 2.3 Management Methods

### 2.3.1 Device Manager

In order to access the Device Manager, use a browser to launch the Device Manager by entering the address, as follows:

<http://10.0.0.31>

<http://10.0.0.32>

Entering the address alone will not launch the Device Manager(!).

Express setup was run for both switches in order to provide telnet access. It was also necessary to set up the interface to the switches' management VLAN and to use a different network number, as shown in the screen snips.

Device Manager Express Setup of switch at 10.0.0.31

Passwords hidden below are JUXAV9V2 in every case.

Machine generated alternative text:
Contents 
Dashboard 
Configure 
Smartports 
Port Settings 
Express Setup 
Restart / Reset 
Monitor 
• Trends 
Port Status 
• Port Statistics 
Maintenance 
• Telnet 
Software Upgrade 
• Network Assistant 
Network Settings 
Management Interface (VLAN 
IP Address: 
Default Gateway: 
Switch Password: 
Optional Settings 
Host Name: 
Telnet Access: 
Telnet Password: 
SNMP: 
SNMP Read Community: 
10 
10 
bayl 
@Enable 
o 
Enable 
31 
62 
o 
Disable 
• Disable 
Submit 
Subnet Mask: 
Confirm Switch Password: 
Confirm Telnet Password: 
SNMP Write Community: 
Cancel 
255255255192 v 

Device Manager Express Setup of switch at 10.0.0.32

Machine generated alternative text:
Contents 
• Dashboard 
Configure 
Smartports 
Port Settings 
Express Setup 
Restart / Reset 
Monitor 
Maintenance 
• Network Assistant 
Express Setup 
Network Settings 
Management Interface (VLAN 
IP Address: 
Default Gateway: 
Switch Password: 
Optional Settings 
Host Name: 
Telnet Access: 
Telnet Password: 
SNMP: 
10 
10 
bay2 
• Enable 
o 
Enable 
32 
62 
o 
Disable 
• Disable 
Submit 
Subnet Mask: 
Confirm Switch Password: 
Confirm Telnet Password: 
Cancel 
255255255192 v 

Immediately after express setup, a password prompt is shown and JUXAV9V2 is entered.

Machine generated alternative text:
Authentication Required 
A username and password are being requested by http://IO.O.OB2.The site says: "level 15 access" 
Confirm Switch Password: 
User Name: 
Passwo rd: 
iwitch Password: 

### 2.3.2 telnet

Once Express Setup has been run to configure telnet access, this can be used to connect to the CLI.

## 2.4 Enabling the crossover connects

Machine generated alternative text:
1 V' S 
「 凵 「 凵 「 凵 「 凵 「 凵 「 凵 「 凵 「 凵 
「 凵 「 凵 「 凵 「 凵 「 凵 「 凵 「 凵 
SM 

Each Ethernet switch provides eight external Ethernet ports for connecting the blade enclosure to the external network.

Ports 17-20: Four Small Form-Factor Pluggable (SFP) ports provide 1000BASE-SX interfaces and are shared with four of the copper Gigabit Ethernet links.

Ports 23-24: Two additional copper Gigabit Ethernet ports are shared with two internal crossover interfaces connecting the pair of switches (labeled X-Crossovers in Figures 2 and 3). All of these ports can be grouped to support the IEEE 802.3ad LACP.

Ports 1-16: Each blade server is connected to the backplane using the available Gigabit Ethernet network interface cards (NICs). The number of NICs on each blade server varies. Each server, whether it is full- or half-height, supports an additional Ethernet interface providing Integrated Lights Out (iLO) support

### 2.4.1 Disabled by default

Machine generated alternative text:
8 uplink ports: 2 copper only, 4 shared copper or SFP, and 2 shared with X-crossover connects 
16 
Downlink 
10/100/1000T 
X Connects 
(Disabled by Default) 
HP ProLiant BL460c/ 
HP ProLiant BL465c 
NIC NIC 
gof 16 
NIC NIC 
16 
Downlink 
Ports 
Cisco 24-Port 
Switching 
ASICS 
Switch B 
Gigabit Ethernet 
Cisco 24-Port 
Switching 
ASICS 
Switch A 
High Density Backplane 

### 2.4.2 Disabled by default (text)

bay1#show interfaces gigabitEthernet 0/23

GigabitEthernet0/23 is down, line protocol is down (notconnect)

# 3. Bl460c G1, Bay 1

## 3.1 Resource information

Machine generated alternative text:
HP ProLiant BL46Bc Gl 
Product ID : 
HP BIOS 115 85/82/2811 
Backup Version 18/25/2818 
Bootb lock 81/89/208 
8192MB Menory Conf igured 
Proc 1: lntel 2.66CHz ,12MB L2 Cache 
Proc 2: Intel 2.66CHz,12MB L2 Cache 
MAC address for NIC 1 : 
iSCS1 MRC address : 
MRC address for NIC 2: 
iSCSI MRC address : 
881F29CRFDF8 
ØØIF29CRFDF1 
ØØIF29CRFDEØ 
ØØIF29CRFDE1 

## 3.2 iLO

Firmware updated to version 2.25 using software at page <http://h20564.www2.hp.com/hpsc/swd/public/readIndex?sp4ts.oid=1842756&swLangOid=8&swEnvOid=4022>

 iLO "Administrator" password modified to be the same as the password of the OA.

## 3.3 Boot order

Machine generated alternative text:
IPL . 
.1 
2 
IPL : 
IPL 
.4 
IPL . 
IPL . 
.5 
CD-ROM 
F loppy Drive 
USB DriveKeg 
Hard Drive C: 
PCI Enbedded 
(See Boot Contro I ler Order) 
HP NC3?3i Mu Itifunction Cigabit Adapter Port 1 

## 3.4 HBA: Local storage

Machine generated alternative text:
tlr:l 
PCI Enbedded 
HP Snart Array E2BØi Control ler 

## 3.5 Intel VT-x

Machine generated alternative text:
HA Prefetcher 
Adjacent Sector Prefetch 
No-Execute Menory Protection 
Intel (R) Virtua lization Techno logg 
Lou Power Halt State (Intel CIE) 
Intel Core C3 State 
Processor Core Disab le 
nab led 
l' Disabled 
ons.. 
ing Sequence 

Intel Virtualization Technology was found disabled. It was enabled on 10th January 2015 at 15:31

# 4. Brocade 4/12 SAN Switch for HP c-class BladeSystem

Add exceptions in Java control panel for:

* <http://10.0.0.33>
* <http://10.0.0.34>

Without the exception, the certificate (which is expired) causes the Web Tools application to be blocked:

Machine generated alternative text:
plicati 
Application Blocked by Java Security 
For security, applicatons must now meet the requirements for the High or Very High security 
settings, or be part of the Excepton Site List, to be allowed to run. More Informaton. 
Your security settings have blocked an application signed with an expired or 
not-yet-valid certficate from running 

## 4.1 IP Addresses

* + <http://10.0.0.33>
  + <http://10.0.0.34>

## 4.2 Management Console security

Machine generated alternative text:
pplication Blocked f 
Failed to validate certificate. 
The application will not be executed. 
Securi 
More Information 
Publisher: 
53.0 

sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: algorithm constraints check failed

at sun.security.validator.PKIXValidator.doValidate(Unknown Source)

at sun.security.validator.PKIXValidator.engineValidate(Unknown Source)

at sun.security.validator.Validator.validate(Unknown Source)

at sun.security.validator.Validator.validate(Unknown Source)

at sun.security.validator.Validator.validate(Unknown Source)

at com.sun.deploy.security.TrustDecider.getValidationState(Unknown Source)

at com.sun.deploy.security.TrustDecider.validateChain(Unknown Source)

at com.sun.deploy.security.TrustDecider.isAllPermissionGranted(Unknown Source)

at com.sun.javaws.security.AppPolicy.grantUnrestrictedAccess(Unknown Source)

at com.sun.javaws.security.JNLPSignedResourcesHelper.checkSignedResourcesHelper(Unknown Source)

at com.sun.javaws.security.JNLPSignedResourcesHelper.checkSignedResources(Unknown Source)

at com.sun.javaws.Launcher.prepareResources(Unknown Source)

at com.sun.javaws.Launcher.prepareAllResources(Unknown Source)

at com.sun.javaws.Launcher.prepareToLaunch(Unknown Source)

at com.sun.javaws.Launcher.prepareToLaunch(Unknown Source)

at com.sun.javaws.Launcher.launch(Unknown Source)

at com.sun.javaws.Main.launchApp(Unknown Source)

at com.sun.javaws.Main.continueInSecureThread(Unknown Source)

at com.sun.javaws.Main.access$000(Unknown Source)

at com.sun.javaws.Main$1.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

Caused by: java.security.cert.CertPathValidatorException: algorithm constraints check failed

at sun.security.provider.certpath.PKIXMasterCertPathValidator.validate(Unknown Source)

at sun.security.provider.certpath.PKIXCertPathValidator.validate(Unknown Source)

at sun.security.provider.certpath.PKIXCertPathValidator.validate(Unknown Source)

at sun.security.provider.certpath.PKIXCertPathValidator.engineValidate(Unknown Source)

at java.security.cert.CertPathValidator.validate(Unknown Source)

... 21 more

## 4.3 Fix

In java.security, modified the key length for MD2 to >=256 from >=1024

This was a setting of the property jdk.certpath.disabledAlgorithms

## 4.4 Credentials

For both Brocade SAN switches:

**User/password**

admin/adminadmin

root/rootroot

factory/factoryfactory

user/useruser

# 5. Browsers

## 5.1 OA Web App Requirements

**Requirements**

The HP BladeSystem Onboard Administrator Web interface requires an XSLT enabled browser with support for JavaScript® 1.3 or equivalent.

The following browsers are officially supported:

* + Microsoft® Internet Explorer 6.0, 7.0, and 8.0
  + Mozilla™ Firefox® 2.0, 3.0, and 3.5

Browsers that provide the required functionality but do not appear in the above list will not be prevented from running the application, but no support is offered for unlisted browsers.

If you received a notice that your browser does not have the required functionality, examine your browser settings to see if they meet the requirements below or contact your administrator.

Please note: If you are using Internet Explorer 8.0 or above, you may have to add the Onboard Administrator's domain to your trusted sites for the application to work properly. The Onboard Administrator web interface is only supported when running Internet Explorer 8.0 in compatibility mode. Consult Internet Explorer Help for information on these topics.

**Javascript**

Client-side javascript is used extensively by this application. Check your browser settings to make sure javascript *is* enabled before running the application.

**ActiveX**

When using Microsoft® Internet Explorer with this application, ActiveX must be enabled. Check your browser settings to make sure ActiveX *is* enabled before running the application.

**Popup Windows**

Popup windows must be allowed for certain features to function correctly. Check your browser settings to make sure popup blockers are *not* enabled before running the application.

**Cookies**

Cookies must be enabled for certain features to function correctly. Check your browser settings to make sure cookies *are* enabled before running the application.

From <[*https://10.0.0.1/082411-150555/html/loginBody.var*](https://10.0.0.1/082411-150555/html/loginBody.var)>

### 5.1.1 Browser: Chrome

Chrome does not load the OA web application properly.

Machine generated alternative text:
About 
Google Chrome 
A web browser built for speed, simplicity, and security 
Get help with using Chrome Report an issue 
Version 39.0.2171.95 m 
Google Chrome is up to date. 

### 5.1.2 Browser: Internet Explorer

Did not load the sign-in page, despite:

(a) Verification that JavaScript was enabled

(b) Exemption of <https://10.0.0.1> and <https://10.0.0.2> from the list of pages that are blocked from presenting popups.

(c) Addition of <https://10.0.0.1> and <https://10.0.0.2> to the list of trusted sites as well as <http://10.0.0.1> and <http://10.0.0.2>

Machine generated alternative text:
About Internet Explorer 
Internet 
Explorerll 
Version: 11.0.9600.17498 
Update Versions: 11.0.15 
Product ID: DOI 
Install new versions automatically 
g: 2013 Microsoft Corporation. All rights reserved. 
Close 

### 5.1.3 Browser: Firefox

Worked without need for configuration

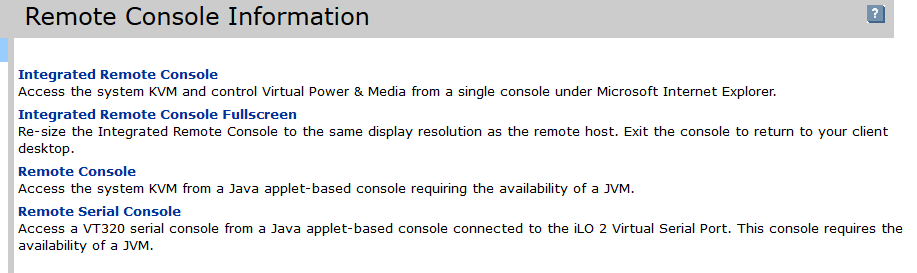
## 5.2 iLO Remote Console Requirements

This requires the Java plugin for the browser used to launch it.

In this case, only Firefox successfully launched the Remote Console and therefore the plugin for Firefox was required.

### 5.2.1 Using the Java iLO Remote Console

* 1. After selecting "Remote Console" from the iLO2 web interface (Fig. 1), a separate browser window opens and attempts to run the Java applet on Firefox's browser plugin. The result of this operation is shown in Fig. 2. Fig. 3 shows context information: the JRE version and the browser's Java plug-in version.



**Fig. 1**

Machine generated alternative text:
ClassNotFoundException 
com.hp.102.remcons.remcons.class 
De tails 

**Fig. 2**

* 1. The problem is caused by deviation from ***any one*** of the following two conditions:
     1. You are required to sign all RIAs (Applets and Web Start applications).
     2. You are required to set the "Permissions" attribute within the Manifest.

From <[*https://blogs.oracle.com/java-platform-group/entry/new\_security\_requirements\_for\_rias*](https://blogs.oracle.com/java-platform-group/entry/new_security_requirements_for_rias)>

* 1. Signature of the applet may be avoided by adding the URL of the RIA to Java's exception site list in the Java Control Panel. In this case, the URL is
  2. The Permissions attribute is set in the jar file that is part of iLO2 firmware version 2.23:

*Java 7u51 was released today and I can say that even* ***with the fix for the manifest file we did for iLO2 v2.23,*** *iLO3 v1.65 and iLO4 v1.32 and adding a trusted SSL certificate to each iLO, users could still experience issues opening the remote console and the virtual media applets.*

*The best solution so far is adding all your iLOs to the Java exception site list.*

From <[*http://h30499.www3.hp.com/t5/HP-BladeSystem-Management/iLO-Java-Remote-Console-Upcoming-JRE-1-7u51/td-p/6250401#.VLED\_MmGPrN*](http://h30499.www3.hp.com/t5/HP-BladeSystem-Management/iLO-Java-Remote-Console-Upcoming-JRE-1-7u51/td-p/6250401#.VLED_MmGPrN)>

As indicated [here](onenote:Configuration.one#Bl460c%20G1&section-id={F381359B-A0AF-4BAB-A023-D20360DCD175}&page-id={36AE80FF-39E0-469C-AB93-521B4F34F265}&base-path=https://d.docs.live.net/c9b0b7fc55b7317f/Documents/CCE3020 Practice 2015/c7000), iLO2 firmware version 2.25 and therefore the permissions attribute issue has been resolved.

* 1. The pending issue appears to be the authentication of the remote console RIA. This may be effected either through digital signature or through whitelisting.

Java Plug-in 11.25.2.18

Using JRE version 1.8.0\_25-b18 Java HotSpot(TM) Client VM

User home directory = C:\Users\edepa

----------------------------------------------------

c: clear console window

f: finalize objects on finalization queue

g: garbage collect

h: display this help message

l: dump classloader list

m: print memory usage

o: trigger logging

q: hide console

r: reload policy configuration

s: dump system and deployment properties

t: dump thread list

v: dump thread stack

x: clear classloader cache

0-5: set trace level to <n>

----------------------------------------------------

**Fig. 3**

### 5.2.2 Remote Console security

The last statement in [this](onenote:Configuration.one#Using%20the%20Java%20iLO%20Remote%20Console&section-id={F381359B-A0AF-4BAB-A023-D20360DCD175}&page-id={1F908CF6-D828-44B3-AB7A-4FBFCEFFF4CE}&base-path=https://d.docs.live.net/c9b0b7fc55b7317f/Documents/CCE3020 Practice 2015/c7000) page regards authentication of the remote console RIA:

"*The pending issue appears to be the authentication of the remote console RIA. This may be effected either through digital signature or through whitelisting*."

Whitelisting has not changed the outcome. The popup in Fig. 2 in [this](onenote:Configuration.one#Using%20the%20Java%20iLO%20Remote%20Console&section-id={F381359B-A0AF-4BAB-A023-D20360DCD175}&page-id={1F908CF6-D828-44B3-AB7A-4FBFCEFFF4CE}&base-path=https://d.docs.live.net/c9b0b7fc55b7317f/Documents/CCE3020 Practice 2015/c7000) page is still returned, despite:

(a) The exception list shown in Fig. 1

(b) Clearing temporary Internet files and preventing Java from caching applets

(c) Storing a security exception permanently in Firefox for the certificate presented by the blade server's iLO.

Machine generated alternative text:
Excepton Site List 
Applications launched from the sites listed below will be allowed to run after the appropriate security 
prompts. 
ttps://lo.o.o.ll/ 
ttps : //ILO 
Edit Site List... 

**Fig. 1**

The solution was found with the help of two pointers:

1. Machine generated alternative text:
   Debugging 
   VI Enable tracing 
   Enable logging 
   Show applet lifecycle exceptions 
   Java console 
   @ Show console 
   Hide console 
   Co not start console Using the Java console to debug the fault:

**Re: iLO Java Remote Console: Upcoming JRE 1.7u51**

[Post options](http://h30499.www3.hp.com/t5/HP-BladeSystem-Management/iLO-Java-Remote-Console-Upcoming-JRE-1-7u51/td-p/6250401)

‎01-29-2014 01:21 PM

Do you have the debug output from the java console?

From <[*http://h30499.www3.hp.com/t5/HP-BladeSystem-Management/iLO-Java-Remote-Console-Upcoming-JRE-1-7u51/td-p/6250401#.VLEuocmGMRR*](http://h30499.www3.hp.com/t5/HP-BladeSystem-Management/iLO-Java-Remote-Console-Upcoming-JRE-1-7u51/td-p/6250401#.VLEuocmGMRR)>

This revealed the exception to be:

security: Checking if SSL certificate is in Deployment permanent certificate store

javax.net.ssl.SSLException: Received fatal alert: bad\_record\_mac

1. Searching for solutions to the javax.net.ssl.SSLException revealed:

Ok, here is what I have found.

* On Java 1.7.0\_45 things should work without any change. However, if SSLv3 is enabled, there is exception, due to java bug (i suppose).
* On Java 1.7.0\_51 it's opposite: you **must** enable the SSLv3 as described above.

From <[*https://github.com/oblac/jodd/issues/110*](https://github.com/oblac/jodd/issues/110)>

Machine generated alternative text:
Advanced Security Settings 
use certficates and keys in browser keystore 
Enable blacklist revcn:ation check 
Enable caching password for authenbcation 
use SSL 2. O compatible ClienYeIIo format 
VI use ssL 3.0 
a Use TLS 1.0 
TLS 1.1 
a Use TLS 1.2 Since JRE v1.8.0\_25-b18 is installed, SSL3 must be enabled. The Java Control Panel revealed that it was enabled but not exclusively. By disabling all transport layer security protocols but SSL3, the issue was resolved!

### 5.2.3 Updated: Remote Console Security

With installation of JRE 1.8.0\_31, SSL 3 is no longer available. The embedded Java server supports TLS v1; this must be selected in the Java Control Panel.

### 5.2.4 Trace: Correct Operation

Java Plug-in 11.31.2.13

Using JRE version 1.8.0\_31-b13 Java HotSpot(TM) Client VM

User home directory = C:\Users\edepa

----------------------------------------------------

c: clear console window

f: finalize objects on finalization queue

g: garbage collect

h: display this help message

l: dump classloader list

m: print memory usage

o: trigger logging

q: hide console

r: reload policy configuration

s: dump system and deployment properties

t: dump thread list

v: dump thread stack

x: clear classloader cache

0-5: set trace level to <n>

----------------------------------------------------

basic: Added progress listener: sun.plugin.util.ProgressMonitorAdapter@bb1f41

security: Expected Main URL: <https://10.0.0.11/rc175p08.jar>

basic: Plugin2ClassLoader.addURL parent called for <https://10.0.0.11/rc175p08.jar>

security: Accessing keys and certificate in Mozilla user profile: null

security: JSS is not configured

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

security: Loading SSL Root CA certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecacerts

security: Loaded SSL Root CA certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecacerts

security: Loading SSL Root CA certificates from C:\Program Files\Java\jre1.8.0\_31\lib\security\cacerts

security: Loaded SSL Root CA certificates from C:\Program Files\Java\jre1.8.0\_31\lib\security\cacerts

security: Obtain certificate collection in SSL Root CA certificate store

security: Obtain certificate collection in SSL Root CA certificate store

security: Loading Deployment SSL certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecerts

security: Loaded Deployment SSL certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecerts

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: Loaded blacklisted.certs file: C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\blacklisted.certs

security: SHA-256Certificate finger print: 94B916AB7285827A0A98F88FC47CBF5D978BC7AFD87ABCEEE924CD022506FBD1

security: Checking if SSL certificate is in Deployment permanent certificate store

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

network: Connecting <https://10.0.0.11/rc175p08.jar> with cookie "hp-iLO-Session=00000003:::GIUFZYSUBIVSJZIFOFPJJDHTEIKXXIIMMTLQRRIL"

network: ResponseCode for <https://10.0.0.11/rc175p08.jar> : 200

network: Encoding for <https://10.0.0.11/rc175p08.jar> : null

network: Server response: (length: 56077, lastModified: Thu Jan 01 01:00:00 CET 1970, downloadVersion: null, mimeType: application/octet-stream)

network: Downloading resource: <https://10.0.0.11/rc175p08.jar>

Content-Length: 56,077

Content-Encoding: null

network: Wrote URL <https://10.0.0.11/rc175p08.jar> to File C:\Users\edepa\AppData\Local\Temp\jar\_cache4920698707700012195.tmp

security: Blacklist revocation check is enabled

security: blacklist: created: NEED\_LOAD, lastModified: 1422434408287

security: blacklist: check contains 5v/V87+cFlb2so+2R40JueDnltQ=, state now NEED\_LOAD

security: blacklist: loadCache

security: blacklist: not found in cache

security: Trusted libraries list check is enabled

security: Trusted libraries list file not found

security: blacklist: check contains 5v/V87+cFlb2so+2R40JueDnltQ=, state now IN\_MEMORY

security: blacklist: not found in cache

network: Disconnect connection to <https://10.0.0.11/rc175p08.jar>

network: Downloaded <https://10.0.0.11/rc175p08.jar>: C:\Users\edepa\AppData\Local\Temp\jar\_cache4920698707700012195.tmp

cache: Adding MemoryCache entry: <https://10.0.0.11/rc175p08.jar>

cache: registerReference: com.sun.deploy.cache.MemoryCache$CachedResourceReference@f34eafba: 1

security: Missing Application-Library-Allowable-Codebase manifest attribute for: <https://10.0.0.11/rc175p08.jar>

security: Loading Deployment certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.certs

security: Loaded Deployment certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.certs

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: Validate the certificate chain using CertPath API

security: The certificate has expired, need to check timestamping info

security: No timestamping info available

security: Loading Root CA certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.cacerts

security: Loaded Root CA certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.cacerts

security: Loading Root CA certificates from C:\Program Files\Java\jre1.8.0\_31\lib\security\cacerts

security: Loaded Root CA certificates from C:\Program Files\Java\jre1.8.0\_31\lib\security\cacerts

security: Obtain certificate collection in Root CA certificate store

security: Obtain certificate collection in Root CA certificate store

security: Obtain certificate collection in Root CA certificate store

security: Obtain certificate collection in Root CA certificate store

security: SHA-256Certificate finger print: A400B8815DBEAFB2725A7CFAC09998FE22F88DFD4ACA2947038B3602FEEA33EE

security: SHA-256Certificate finger print: 0CFC19DB681B014BFE3F23CB3A78B67208B4E3D8D7B6A7B1807F7CD6ECB2A54E

security: The OCSP support is enabled

security: The CRL support is enabled

network: Connecting <http://ocsp.verisign.com/> with proxy=DIRECT

network: Connecting <http://ocsp.verisign.com:80/> with proxy=DIRECT

security: OCSP Response: GOOD

network: Connecting <http://ocsp.verisign.com/> with proxy=DIRECT

security: OCSP Response: GOOD

security: Certificate validation succeeded using OCSP/CRL

security: Saving certificates in Deployment session certificate store

security: Saved certificates in Deployment session certificate store

security: Saving certificates in Deployment session certificate store

security: Saved certificates in Deployment session certificate store

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <https://10.0.0.11/rc175p08.jar> with cookie "hp-iLO-Session=00000003:::GIUFZYSUBIVSJZIFOFPJJDHTEIKXXIIMMTLQRRIL"

security: Grant connect perm for <https://10.0.0.11/rc175p08.jar> : java.security.Permissions@14c64bd (

("java.net.URLPermission" "<https://10.0.0.11:443/->" "\*:\*")

("java.net.URLPermission" "<https://10.0.0.11:443>" "\*:\*")

)

security: Missing Application-Library-Allowable-Codebase manifest attribute for: <https://10.0.0.11/rc175p08.jar>

security: Validate the certificate chain using CertPath API

security: The certificate has expired, need to check timestamping info

security: No timestamping info available

basic: Plugin2ClassLoader.getPermissions CeilingPolicy allPerms

security: The certificate has expired, need to check timestamping info

security: No timestamping info available

security: Missing Application-Library-Allowable-Codebase manifest attribute for: <https://10.0.0.11/rc175p08.jar>

security: Validate the certificate chain using CertPath API

security: The certificate has expired, need to check timestamping info

security: No timestamping info available

security: SSV validation:

running: 1.8.0\_31

requested: null

range: null

javaVersionParam: null

Rule Set version: null

network: Created version ID: 1.8.0.31

network: Created version ID: 1.8.0.31

security: continue with running version

network: Created version ID: 1.8.0.31

network: Created version ID: 1.8

network: Created version ID: 8.0.31

Exception: java.io.FileNotFoundException: C:\Users\edepa\.java\hp.properties (The system cannot find the path specified)

Trying to select locale: en\_GB

basic: Applet loaded.

basic: Applet resized and added to parent container

basic: PERF: AppletExecutionRunnable - applet.init() BEGIN ; jvmLaunch dt 918872 us, pluginInit dt 5250279 us, TotalTime: 6169151 us

Trying to select locale: en\_GB

Applet initialized...

basic: Applet initialized

basic: Starting applet

basic: completed perf rollup

Applet started...

network: Connecting <http://10.0.0.11:23/> with proxy=DIRECT

Remote Console inactivity timeout = 30 minutes.

basic: Applet made visible

basic: Applet started

basic: Told clients applet is started

Version 20050808154652

security: Grant liveconnect connect perm for <https://10.0.0.11/drc2fram.htm?restart=0> : java.security.Permissions@c6efcb (

("java.lang.RuntimePermission" "accessClassInPackage.sun.audio")

("java.lang.RuntimePermission" "stopThread")

("java.util.PropertyPermission" "java.specification.version" "read")

("java.util.PropertyPermission" "path.separator" "read")

("java.util.PropertyPermission" "java.vm.vendor" "read")

("java.util.PropertyPermission" "os.version" "read")

("java.util.PropertyPermission" "browser.version" "read")

("java.util.PropertyPermission" "java.vendor.url" "read")

("java.util.PropertyPermission" "browser" "read")

("java.util.PropertyPermission" "browser.vendor" "read")

("java.util.PropertyPermission" "os.name" "read")

("java.util.PropertyPermission" "java.vm.specification.version" "read")

("java.util.PropertyPermission" "java.vm.name" "read")

("java.util.PropertyPermission" "javaws.\*" "read,write")

("java.util.PropertyPermission" "javaplugin.vm.options" "read")

("java.util.PropertyPermission" "mrj.version" "read")

("java.util.PropertyPermission" "java.version" "read")

("java.util.PropertyPermission" "jnlp.\*" "read,write")

("java.util.PropertyPermission" "javaplugin.version" "read")

("java.util.PropertyPermission" "os.arch" "read")

("java.util.PropertyPermission" "java.specification.vendor" "read")

("java.util.PropertyPermission" "java.vm.specification.name" "read")

("java.util.PropertyPermission" "file.separator" "read")

("java.util.PropertyPermission" "line.separator" "read")

("java.util.PropertyPermission" "java.vendor" "read")

("java.util.PropertyPermission" "java.specification.name" "read")

("java.util.PropertyPermission" "java.vm.specification.vendor" "read")

("java.util.PropertyPermission" "java.vm.version" "read")

("java.util.PropertyPermission" "javapi.\*" "read,write")

("java.util.PropertyPermission" "java.class.version" "read")

("java.util.PropertyPermission" "http.agent" "read")

("java.net.URLPermission" "<https://10.0.0.11:443/->" "\*:\*")

("java.net.URLPermission" "<https://10.0.0.11:443>" "\*:\*")

("com.sun.deploy.security.SecureCookiePermission" "origin.https://10.0.0.11:443")

("java.net.SocketPermission" "localhost:0" "listen,resolve")

)

### 5.2.5 Trace: Operation with TLS 1.2 only

Java Plug-in 11.31.2.13

Using JRE version 1.8.0\_31-b13 Java HotSpot(TM) Client VM

User home directory = C:\Users\edepa

----------------------------------------------------

c: clear console window

f: finalize objects on finalization queue

g: garbage collect

h: display this help message

l: dump classloader list

m: print memory usage

o: trigger logging

q: hide console

r: reload policy configuration

s: dump system and deployment properties

t: dump thread list

v: dump thread stack

x: clear classloader cache

0-5: set trace level to <n>

----------------------------------------------------

basic: Added progress listener: sun.plugin.util.ProgressMonitorAdapter@124ccf

security: Expected Main URL: <https://10.0.0.11/rc175p08.jar>

basic: Plugin2ClassLoader.addURL parent called for <https://10.0.0.11/rc175p08.jar>

security: Accessing keys and certificate in Mozilla user profile: null

security: JSS is not configured

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

**javax.net.ssl.SSLHandshakeException: Server chose TLSv1, but that protocol version is not enabled or not supported by the client.**

at sun.security.ssl.ClientHandshaker.serverHello(Unknown Source)

at sun.security.ssl.ClientHandshaker.processMessage(Unknown Source)

at sun.security.ssl.Handshaker.processLoop(Unknown Source)

at sun.security.ssl.Handshaker.process\_record(Unknown Source)

at sun.security.ssl.SSLSocketImpl.readRecord(Unknown Source)

at sun.security.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)

at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)

at sun.net.www.protocol.https.HttpsURLConnectionImpl.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.getJarFile(Unknown Source)

at sun.net.www.protocol.jar.JarFileFactory.get(Unknown Source)

at sun.net.www.protocol.jar.JarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFileInternal(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.access$800(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader$1.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.ensureOpen(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.<init>(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$3.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getResource(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at sun.plugin2.applet.Plugin2ClassLoader.findClassHelper(Unknown Source)

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

javax.net.ssl.SSLHandshakeException: Server chose TLSv1, but that protocol version is not enabled or not supported by the client.

at sun.security.ssl.ClientHandshaker.serverHello(Unknown Source)

at sun.security.ssl.ClientHandshaker.processMessage(Unknown Source)

at sun.security.ssl.Handshaker.processLoop(Unknown Source)

at sun.security.ssl.Handshaker.process\_record(Unknown Source)

at sun.security.ssl.SSLSocketImpl.readRecord(Unknown Source)

at sun.security.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)

at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)

at sun.net.www.protocol.https.HttpsURLConnectionImpl.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.getJarFile(Unknown Source)

at sun.net.www.protocol.jar.JarFileFactory.get(Unknown Source)

at sun.net.www.protocol.jar.JarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFileInternal(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.access$800(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader$1.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.ensureOpen(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.<init>(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$3.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getResource(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at sun.plugin2.applet.Plugin2ClassLoader.findClassHelper(Unknown Source)

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

network: Connecting <https://10.0.0.11/com/hp/ilo2/remcons/remcons.class> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

network: Connecting <https://10.0.0.11/com/hp/ilo2/remcons/remcons/class.class> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

java.lang.ClassNotFoundException: com.hp.ilo2.remcons.remcons.class

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

basic: load: class com.hp.ilo2.remcons.remcons.class not found.

java.lang.ClassNotFoundException: com.hp.ilo2.remcons.remcons.class

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

security: Reset deny session certificate store

basic: Removed progress listener: sun.plugin.util.ProgressMonitorAdapter@124ccf

security: Reset deny session certificate store

### 5.2.6 Trace: Operation without any TLS selected

Java Plug-in 11.31.2.13

Using JRE version 1.8.0\_31-b13 Java HotSpot(TM) Client VM

User home directory = C:\Users\edepa

----------------------------------------------------

c: clear console window

f: finalize objects on finalization queue

g: garbage collect

h: display this help message

l: dump classloader list

m: print memory usage

o: trigger logging

q: hide console

r: reload policy configuration

s: dump system and deployment properties

t: dump thread list

v: dump thread stack

x: clear classloader cache

0-5: set trace level to <n>

----------------------------------------------------

basic: Added progress listener: sun.plugin.util.ProgressMonitorAdapter@11e4a38

security: Expected Main URL: <https://10.0.0.11/rc175p08.jar>

basic: Plugin2ClassLoader.addURL parent called for <https://10.0.0.11/rc175p08.jar>

security: Accessing keys and certificate in Mozilla user profile: null

security: JSS is not configured

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

security: Loading SSL Root CA certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecacerts

security: Loaded SSL Root CA certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecacerts

security: Loading SSL Root CA certificates from C:\Program Files\Java\jre1.8.0\_31\lib\security\cacerts

security: Loaded SSL Root CA certificates from C:\Program Files\Java\jre1.8.0\_31\lib\security\cacerts

security: Obtain certificate collection in SSL Root CA certificate store

security: Obtain certificate collection in SSL Root CA certificate store

security: Loading Deployment SSL certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecerts

security: Loaded Deployment SSL certificates from C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\trusted.jssecerts

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: Loaded blacklisted.certs file: C:\Users\edepa\AppData\LocalLow\Sun\Java\Deployment\security\blacklisted.certs

security: SHA-256Certificate finger print: 94B916AB7285827A0A98F88FC47CBF5D978BC7AFD87ABCEEE924CD022506FBD1

**security: Checking if SSL certificate is in Deployment permanent certificate store**

**javax.net.ssl.SSLException: Received fatal alert: bad\_record\_mac**

at sun.security.ssl.Alerts.getSSLException(Unknown Source)

at sun.security.ssl.Alerts.getSSLException(Unknown Source)

at sun.security.ssl.SSLSocketImpl.recvAlert(Unknown Source)

at sun.security.ssl.SSLSocketImpl.readRecord(Unknown Source)

at sun.security.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)

at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)

at sun.net.www.protocol.https.HttpsURLConnectionImpl.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.getJarFile(Unknown Source)

at sun.net.www.protocol.jar.JarFileFactory.get(Unknown Source)

at sun.net.www.protocol.jar.JarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFileInternal(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.access$800(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader$1.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.ensureOpen(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.<init>(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$3.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getResource(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at sun.plugin2.applet.Plugin2ClassLoader.findClassHelper(Unknown Source)

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

network: Connecting <https://10.0.0.11/rc175p08.jar> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

security: Obtain certificate collection in SSL Root CA certificate store

security: Obtain certificate collection in SSL Root CA certificate store

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: SHA-256Certificate finger print: 94B916AB7285827A0A98F88FC47CBF5D978BC7AFD87ABCEEE924CD022506FBD1

security: Checking if SSL certificate is in Deployment permanent certificate store

javax.net.ssl.SSLException: Received fatal alert: bad\_record\_mac

at sun.security.ssl.Alerts.getSSLException(Unknown Source)

at sun.security.ssl.Alerts.getSSLException(Unknown Source)

at sun.security.ssl.SSLSocketImpl.recvAlert(Unknown Source)

at sun.security.ssl.SSLSocketImpl.readRecord(Unknown Source)

at sun.security.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)

at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)

at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)

at sun.net.www.protocol.https.HttpsURLConnectionImpl.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.connect(Unknown Source)

at sun.plugin.PluginURLJarFileCallBack.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.retrieve(Unknown Source)

at sun.net.www.protocol.jar.URLJarFile.getJarFile(Unknown Source)

at sun.net.www.protocol.jar.JarFileFactory.get(Unknown Source)

at sun.net.www.protocol.jar.JarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.connect(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFileInternal(Unknown Source)

at sun.plugin.net.protocol.jar.CachedJarURLConnection.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.getJarFile(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.access$800(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader$1.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.ensureOpen(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$JarLoader.<init>(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath$3.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getLoader(Unknown Source)

at com.sun.deploy.security.DeployURLClassPath.getResource(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader$2.run(Unknown Source)

at java.security.AccessController.doPrivileged(Native Method)

at sun.plugin2.applet.Plugin2ClassLoader.findClassHelper(Unknown Source)

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

network: Connecting <https://10.0.0.11/com/hp/ilo2/remcons/remcons.class> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

security: Obtain certificate collection in SSL Root CA certificate store

security: Obtain certificate collection in SSL Root CA certificate store

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: SHA-256Certificate finger print: 94B916AB7285827A0A98F88FC47CBF5D978BC7AFD87ABCEEE924CD022506FBD1

security: Checking if SSL certificate is in Deployment permanent certificate store

network: Connecting <https://10.0.0.11/com/hp/ilo2/remcons/remcons/class.class> with proxy=DIRECT

network: Connecting <http://10.0.0.11:443/> with proxy=DIRECT

security: Obtain certificate collection in SSL Root CA certificate store

security: Obtain certificate collection in SSL Root CA certificate store

security: Loading certificates from Deployment session certificate store

security: Loaded certificates from Deployment session certificate store

security: SHA-256Certificate finger print: 94B916AB7285827A0A98F88FC47CBF5D978BC7AFD87ABCEEE924CD022506FBD1

security: Checking if SSL certificate is in Deployment permanent certificate store

java.lang.ClassNotFoundException: com.hp.ilo2.remcons.remcons.class

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

basic: load: class com.hp.ilo2.remcons.remcons.class not found.

java.lang.ClassNotFoundException: com.hp.ilo2.remcons.remcons.class

at sun.plugin2.applet.Applet2ClassLoader.findClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass0(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)

at sun.plugin2.applet.Plugin2ClassLoader.loadCode(Unknown Source)

at sun.plugin2.applet.Plugin2Manager.initAppletAdapter(Unknown Source)

at sun.plugin2.applet.Plugin2Manager$AppletExecutionRunnable.run(Unknown Source)

at java.lang.Thread.run(Unknown Source)

security: Reset deny session certificate store

basic: Removed progress listener: sun.plugin.util.ProgressMonitorAdapter@11e4a38

security: Reset deny session certificate store

Logging set to : true ... completed.

Reload policy configuration ... completed.