IIS Reverse Proxy Implementation
for OXI/OEDS Servers

VERSION: 1.1 | MAY 29, 2015
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended Audience</td>
<td>3</td>
</tr>
<tr>
<td>About this Document</td>
<td>3</td>
</tr>
<tr>
<td>Advisories and Known Issues</td>
<td>3</td>
</tr>
<tr>
<td>Additional Considerations</td>
<td>4</td>
</tr>
<tr>
<td>SSL Overview</td>
<td>5</td>
</tr>
<tr>
<td>IIS Reverse Proxy Installation Overview for OPERA OXI/OEDS Servers</td>
<td>6</td>
</tr>
<tr>
<td>Components</td>
<td>6</td>
</tr>
<tr>
<td>Implementing the IIS Reverse Proxy Solution</td>
<td>7</td>
</tr>
<tr>
<td>Troubleshooting Tips</td>
<td>25</td>
</tr>
</tbody>
</table>
Intended Audience
Oracle Implementation Resources and IT Personnel involved in installing SSL certificates on an OPERA OXI/OEDS Server. This solution is intended for externally facing OPERA OXI/OEDS Servers within a segmented DMZ. It is only supported for Windows 7 and Windows 2008 Server R2 and for OPERA Versions 5.0.x.x.

About this Document
The SSL Installation and Overview for OPERA section provides a high level overview of the Implementation process for an OPERA Application Server without providing step by step details.

The provided Troubleshooting Tips will likely be helpful to anyone troubleshooting issues that may have arisen during an IIS Reverse Proxy Implementation.

Advisories and Known Issues

- The installation described in this document was designed to handle most standard OXI/OEDS installations. For complex installations including Data Center environments or installations, Oracle strongly recommends consultation with a knowledgeable resource prior to implementation.

- Oracle strongly recommends that an OPERA OXI server be segmented within a DMZ if it is presented to externally located interface communication. For example, an OPERA OXI server that functions as an endpoint for SynXis or Travelclick postings should be in a segmented DMZ.

- Oracle strongly recommends that a backup of the system be taken prior to and after implementation.
Additional Considerations

This solution leverages Microsoft Internet Information Services as a reverse proxy in order to account for the following:

- The POODLE vulnerability (CVE-2014-3566 and CVE-2014-8730) affects protocols currently required for OPERA communication. Legacy V5 application servers (OPERA version 5.0.04.02 and below) are affected. In order to properly mitigate POODLE, SSLv3 and TLS 1.0 support should be disabled in favor of TLS 1.2 instead. This can be completed via the updates to SCHannel registry settings for IIS.

- SSL certificates issued by a public Certificate Authority must be issued using a SHA-2 cipher after January 1, 2016. The Legacy V5 application server (OPERA version 5.0.04.02 and below) cannot support this cipher. IIS 7.5 allows for SHA-2 support.
SSL Overview

Secure Sockets Layer (SSL) communications have become an internet standard when securing sensitive data transmissions across a network. When making a connection via this protocol, the connection is validated in three steps:

1 – The name of the server to which the certificate is issued must match the URL requested.
2 – The Certificate Signing Authority that issue the certificate must be known to the client machine or there must be a chain of certificates provided that point to a CA that is known to the client.
3 – The certificate must not be expired.
4 – The name of the server to which the certificate is issued must be a Fully Qualified Domain Name and Domain validation must be confirmed by the Certificate Signing Authority.

The first step of validation ensures that the website hasn't been hijacked by an unknown entity. There are scenarios where this can pose some challenges for an OPERA installation, however. In most cases, the OPERA server may be configured to use the application server name in the URL, but a user may request a connection to OPERA using the machine’s IP Address. In this case, the client machine will see that it has been redirected to https://appservername when the original request was made for https://ipaddress. In such a case, the two URL’s don’t match, so the client machine does (and should) display an error message that the site name is mismatched. In order to resolve this, the client request can be modified to request https://appservername.

In the second step of validation, the server passes an SSL certificate to the client machine requesting a connection. The client is then able to view the signature of the Certificate Signing Authority that issued the certificate to the server and determine whether the server can be trusted. In some cases, the Certificate Signing Authority that issued the certificate to the server and the Certificate Signing Authority that signed the server certificate may not be directly trusted by the client, but the Certificate Signing Authority that issued the certificate for the signer is trusted. Visually, this could look something like this:

As long as the Certificate Signing Authority of one of the certificates in the certificate path of the server’s certificate is trusted by the client, the connection is validated.

The third step of validation simply checks for the expiration date on the SSL certificate itself. In the event that an expired certificate is encountered, the client browser will still allow the connection (i.e., the system remains functional) and displays a message indicating the certificate is expired. Once the certificate is replaced with a new copy that expires at a later date, the message will stop.

In order to secure incoming communications to an HTTP server, an SSL certificate ensures that all messages between client and server are encrypted during transmission.
IIS Reverse Proxy Installation Overview for OPERA OXI/OEDS Servers

For OXI / OEDS Servers, installing an SSL certificate requires the following high level steps:

1. Install Windows Internet Information Services (IIS) 7.5
2. Install additional IIS feature required for reverse proxy functionality
3. Generate a Certificate Signing Request from within IIS
4. Obtain a signed certificate from certificate provider
5. Install the signed (previously requested) certificate into IIS
6. Update the 10g Application Server configuration to account for the IIS redirect
7. Update the IIS configuration to proxy requests to the 10g Application Server

Components

The following components are required for IIS Reverse Proxy:

- Windows 7 x32 bit
  - webfarm_v1.1_x86_en_us.msi
  - ExternalDiskCache_x86_en-US.msi
  - rewrite_x86_en-US.msi
  - requestRouter_x86

- Windows 7 x64 bit and Windows 2008 R2
  - webfarm_v1.1_amd64_en_us.msi
  - ExternalDiskCache_amd64_en-US.msi
  - rewrite_amd64_en-US.msi
  - requestRouter_x64

Currently, the files are available using the links below. Be aware the difference between x86 and x64 versions of the files.

- [Download](http://download.microsoft.com/download/5/4/7/5477b52e-7cc8-433c-aa26-74732b485857/webfarm_v1.1_x86_en_us.msi)
- [Download](http://download.microsoft.com/download/4/D/F/4DFDA851-515F-474E-BA7A-5802B3C95101/ExternalDiskCache_x86_en-US.msi)
- [Download](http://download.microsoft.com/download/6/9/C/69C1195A-123E-4BE8-8EDF-371C0C4CEC5C/rewrite_x86_en-US.msi)
- [Download](http://download.microsoft.com/download/6/3/D/63D67918-483E-4507-939D-7F8C077F889E/requestRouter_x86.msi)

- [Download](http://download.microsoft.com/download/5/7/0/57065640-4665-4980-a2f1-4d5940b577b0/webfarm_v1.1_amd64_en_us.msi)
- [Download](http://download.microsoft.com/download/3/4/1/3415F3F9-5698-44FE-A072-D4ACF0972B39/ExternalDiskCache_amd64_en-US.msi)
- [Download](http://download.microsoft.com/download/6/7/0/6780164-7DD0-48AF-86E3-D7A182D6815/rewrite_amd64_en-US.msi)
- [Download](http://download.microsoft.com/download/6/3/3/63D67918-483E-4507-939D-7F8C077F889E/requestRouter_x64.msi)
Implementing the IIS Reverse Proxy Solution

1. Ensure that the OXIServlets page is up and functional.

2. Update OPERA configuration via OAppCfgEd
   - Read Only Mode = NO
   - Turn off Redirect
   - Turn off SSL
   - Change default port to 8081
3. Ensure that the OXIServlets page is up and functional on port 8081
4. Ensure that IIS is installed
   - NOTE: IIS may already be setup and in use with OEDS services
     i. If so, decisions will have to be made about what ports IIS will be using
     ii. Documented steps present both OXI and OEDS services on port 443 using a single SSL certificate
   - Windows 7 - Control Panel >> Programs and Features >> Turn Windows Features On or Off >> Ensure Internet Information Services is checked
   - Windows 2008 – Admin Tools >> Server Manager >> Roles >> Add Roles >> Web Server (IIS)
   - Helpful script to install necessary IIS components
     i. CMD – Run as Admin
5. Install additional IIS add-on features
   - Double click on each to begin the straightforward installation, continue by clicking NEXT
   - It is of utmost importance that they are installed in the correct order
     
     Windows 7 x32 bit
     i. webfarm_v1.1_x86_en_us.msi
     ii. ExternalDiskCache_x86_en-US.msi
     iii. rewrite_x86_en-US.msi
     iv. requestRouter_x86

     Windows 7 x64 bit and Windows 2008 R2
     i. webfarm_v1.1_amd64_en_us.msi
     ii. ExternalDiskCache_amd64_en-US.msi
     iii. rewrite_amd64_en-US.msi
     iv. requestRouter_x64.msi

6. Configure IIS for SSL – Issue Certificate Request
   - Start >> Control Panel >> Administrative Tools >> Internet Information Services Manager
   - Double click on the Server Certificates option
   - NOTE – If the server is already functioning with OEDS, an SSL Certificate may already exist within IIS. This certificate can be used for both OXI and OEDS. Please skip to step 8 in order to update the port binding. Also be aware that external vendors will likely need to update the URLs for posting after implementation is completed.
• Create Certificate Request

• Enter all pertinent information regarding the request
• Enter Bit Length of 2048 or higher – 2048 is the minimum suggested value

• Save the Certificate Request to a convenient location

• Select FINISH
7. Configure IIS for SSL - Obtain certificate from Trusted Certificate Authority
8. Configure IIS for SSL – Complete Certificate Request
   - Complete Certificate Request
     - Select the .cer or .pfx file returned by the Certificate Authority
     - Issue a Friendly Name for the certificate
   - The certificate will show up within the Server Certificates listing
9. Configure IIS for SSL – Bind certificate to Default Web Page on Port 443
   - Start >> Control Panel >> Administrative Tools >> Internet Information Services Manager
   - Sites >> Default Web Sites
   - Bindings option on the right hand side
Select the Add option

- Select HTTPS, the IPv4 address, Port 443 and the correct SSL certificate
10. Start the Default Web Site and test that port 443 is bound with the SSL certificate.
- Select Default Web Site in left panel
- Select the Start or Restart option in the right panel

![Image of IIS Configuration]

- Test the following URL – https://172.36.200.215 – replacing the IP with that of your server
- IIS7 default page should show as follows

![Image of IIS Default Page]

11. Configure IIS for Reverse Proxy of Operajserv (OXI Requests)
- Start >> Control Panel >> Administrative Tools >> Internet Information Services Manager
- Select the server name in the left panel
- Double click Application Request Routing Cache in middle panel

- Select Server Proxy Settings in right panel

- Ensure the following options are selected / configured
i. Enable proxy should be checked
ii. Leave the rest of the default options alone as seen in screenshot below

Application Request Routing

Use this feature to configure proxy settings for Application Request Routing.

- Enable proxy

  **Proxy Setting**

  HTTP version:
  Pass through

  Keep alive

  Time-out (seconds): 120

- Reverse rewrite host in response headers

  Custom Headers

  Preserve client IP in the following headers:
  Forwarded-For

  Include TCP port from client IP

  Forwarding proxy header value:

- Cache Setting

  Memory cache duration (seconds):
  60

  Enable disk cache
  Enable request consolidation

  Query string support:
  Ignore query string

- Scroll down

  i. Check option for USE URL REWRITE TO INSPECT INCOMING REQUESTS
  ii. Enter value for Reverse Proxy – **localhost:8081**
- Buffer Setting
  Response buffer (KB):
  4385
  Response buffer threshold (KB):
  256

- Proxy Chain
  Proxy server:
  Example: proxy.contoso.com:8888

- Proxy Type
  - Use URL Rewrite to inspect incoming requests
  - Enable SSL offloading
  Reverse proxy:
  [localhost:8081]

- Select the APPLY option in right panel
- Select the URL Rewrite option in the right panel

- Highlight the ARR_server_proxy URL Rewrite Inbound Rule and select Edit in right panel
- Change the Pattern value from * to "Operajserv" and select Apply in right panel.

- Select Back to Rules and confirm that the ARR_server_proxy Inbound Rule shows the updated pattern.

- This change ensures that all URL requests containing Operajserv are proxied to port 8081 on the localhost.

- Restart IIS to ensure the change is in place.
12. Ensure that the OXIServlets page is up and accessible
   - Update the URL below with the proper FQDN or server name

13. Restrict the protocols are utilized by IIS
   - This requires updating registry so please be cautious and take a backup if you are unsure of the changes
   - The following registry keys will need to be created
     - These values can be customized as needed.
     - DisabledByDefault is set to 1 – the protocol will NOT be used/accepted.
     - DisabledByDefault is set to 0 – the protocol is active and acceptable.
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server"
       - REG_DWORD named DisabledByDefault with value of 0x00000001
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client"
       - REG_DWORD named DisabledByDefault with value of 0x00000001
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server"
       - REG_DWORD named DisabledByDefault with value of 0x00000000
       - This was set to 0 in order to account for external vendors still posting using SSLv3
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client"
       - REG_DWORD named DisabledByDefault with value of 0x00000001
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server"
       - REG_DWORD named DisabledByDefault with value of 0x00000000
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client"
       - REG_DWORD named DisabledByDefault with value of 0x00000000
       - Be aware setting TLS 1.0 values to 1 will disable RDP connectivity for the machine
     - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server"
       - REG_DWORD named DisabledByDefault with value of 0x00000000
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client
  o REG_DWORD named DisabledByDefault with value of 0x00000000
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
  o REG_DWORD named DisabledByDefault with value of 0x00000000
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
  o REG_DWORD named DisabledByDefault with value of 0x00000000
- The following REG file can be used to quickly update the settings above

14. Restart the Default Web Page
- From a CMD prompt
- net start "World Wide Web Publishing Service"

15. Test and ensure that the OXIServlets are still produced – same as step 11

16. Test and ensure that the OEDS service is produced
- The example URL may differ depending on the OEDS installation … this is an example for HTNG
  - https://reservations.ogtslab.com/HTNG/ActivityService.asmx

17. Ensure that all external vendors have the new URLs for posting if they were changed. Test with the external vendors and ensure that the interfaces are working properly.
Troubleshooting Tips

1. Please review the Windows Event Logs for an IIS errors if the solution is not behaving as expected.

2. If the reverse proxy is not functioning, please ensure that the ARR_Reverse_Proxy rule in Step 10 is not greyed out. If it is, please delete the rule, uncheck the option to Enable Proxy, save configuration, restart IIS and complete Step 10 again.
IIS Reverse Proxy for OXI/OEDS
May 12, 2015
Author: Devin Mills