Integrating Oracle Access Manager with Citrix NetScaler as SAML SP

This guide focuses on defining the process for deploying Oracle Access Manager as an IdP, with NetScaler acting as the SAML SP.
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

NetScaler’s SAML integration capabilities allow current Oracle Access Manager (OAM) users to enable authentication for applications deployed on NetScaler through OAM, thus avoiding having to configure an additional authentication source.

**Introduction**

This solution allows the integration of Oracle Access Manager with NetScaler, enabling the use of OAM as an authentication source for applications deployed on NetScaler.

Oracle Access Management provides traditional access management capabilities along with some advanced identity management capabilities such as adaptive authentication, federated single-sign on (SSO), risk analysis, and fine-grained authorization which can also be extended to mobile clients and mobile applications. OAM is an integral part of the authentication and authorization framework that facilitates access to the Oracle enterprise software suite.

In this deployment, we will configure a content switching virtual server on NetScaler to enable multiple domain access with different FQDNs on a single IP address.

**Configuration**

Successful integration of a NetScaler appliance with OAM requires an appliance running NetScaler software release 11.1 or later, with an Enterprise or Platinum license.

**NetScaler features to be enabled**

The following feature must be enabled to use single sign-on with OAM: **Authentication, authorization and auditing (AAA)**

The AAA feature controls NetScaler authentication, authorization, and auditing policies. These policies include definition and management of various authentication schemas. NetScaler supports a wide range of authentication protocols.
Solution Description

Enabling SSO for OAM with NetScaler has two parts: configuring the OAM portal and configuring the NetScaler appliance. OAM should be configured to use NetScaler as a third party SAML SP (Service Provider). The NetScaler appliance is configured as a SAML SP by creating the AAA Virtual Server that will host the SAML SP policy.

The following instructions assume that you have already created the appropriate external and/or internal DNS entries to route authentication requests to a NetScaler-monitored IP address, and that an SSL certificate has already been created and installed on the appliance for the SSL/HTTPS communication. This document also assumes that user accounts and the required user directories have been created and configured on OAM.

Before proceeding, you will require the certificate that the NetScaler appliance and OAM will use to verify the SAML request and response. To get the verification certificate from the NetScaler appliance, follow these steps:

- Log on to your NetScaler appliance, and then select the Configuration tab.
- Select Traffic Management > SSL
- On the right, under Tools, select Manage Certificates / Keys / CSR's

From the Manage Certificates window, browse to the certificate you will be using for your AAA Virtual Server. Select the certificate and choose the Download button. Save the certificate to a location of your choice.
Part 1: Configure OAM

To configure OAM, log on to your OAM account with administrator credentials, and then do the following:

1. On the main configuration page, click the Federation button in the top right corner of the screen.
2. On the Federation page, in the Federation section, click the Identity Provider Management link. (In the OAM console, the Identity Provider Management section manages SPs (Service providers) bound to OAM, and the Service Provider Management section manages IDPs (Identity Providers) bound to OAM).
3. On the Identity Provider Management screen, click the Create Service Provider Partner button.
4. On the configuration screen, set the parameters listed under the following screen shot.

In the General section:
Name. An indicative name for the SP Partner configuration. (The above example uses NSSAML_SP)
Description. A description of the SP Partner configuration.
Enable Partner. Select this check box.

In the Service Information section:
Protocol. Choose SAML 2.0.
Service Details. Select Enter Manually.
Provider ID. Enter the same name as the value that will be entered in the NetScaler Appliance.
Assertion Consumer URL. <FQDN of the AAA virtual server>/cgi/samlauth

In the Signing Certificate section:
Load signing Certificate. Browse to the signing certificate that is specified as the Identity Provider (IdP) certificate on the NetScaler appliance.
Extracting the IDP certificate for NetScaler

To extract the IDP certificate, navigate to http://public-oam-host:public-oam-port/oamfed/idp/metadata (http://10.105.157.147:14100/oamfed/sp/metadata in our setup), and then download the metadata XML file. In the file, look for the X.509 certificate tag, and copy the contents of the tag into a Notepad file. Add BEGIN and END certificate tags at the beginning and end of the file as shown below.

-----BEGIN CERTIFICATE-----
MIITkjcCBXqqAwIBAgIQ9Q9a7ev11PafwDCfR62Z7FzANBkgqhkiG9wBAQsFADB3MQswC
EyJvUzEdMBsGAIUChMU3t1tY50ZMgQ29ycG9yYXRpb24hAdBgnVBAstF1N5bwFue
xN8IE51dHdvcmxskDAM伯NgBAMTH1N5bwFudGyjIENsYXNzIDMgRVgU1MNIEFICGR
MTUvNTIxMDAvMDAwUhctNMTYwNTI2MjM1OTU5WjcCAR1yizAARBgr8gRgEAEY1PAIAbM
xMCBgrBEEAY1PAIAbgwRIGwSyYdhcnUxHTAbBgNHAB8TFFByaXZhdGUgT33nY5w5pemF0e
DgYDVQQIEIwczN0MdwgQswCQYDVQQGEwJHVzEOMAwGA1UEAQUWObFMbMTcexEzARBgNf
bGlmb3JuaW8dANBgnVABAcMBkdvbGBVPYTEeMBwGA1UECwNYNzQxMCBIb2xsaXNzZGIgC
MRoWAmYDVQQKDBFDaXNyYxqjGT2s5aAw5I1ExmQzETMBEAgEAIUEwWklTBIcmF0aW9uczEJ
AwNhY29ub4Yu1210cm14b25saN51NmNvTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCw
AkJjY1vQ8/dXye4xY1ciYpiSx56A6Aa1M+ZPYVxmbtdqQ9a9FwWtsrj5jM7SqsGe
8qoJIsV9nZ0UAh4SSLcancNCCdQpX7HgPnw10E6ZDjgjhvfJzjZQpekYFFFF+5X9awQHLA
k+xh7/t/my0sm/tiKeA+3escTEmCqjQpxWkD4wScAQCDJG+a4kC/kIzuNRNyiakRPpYoC
TbkA4AZ19Guv5xSxvqX+rW8C9kmFqsFb21GBkHUMOTAXfsNvjMOzTN1bhm61a/mjYcou5
YbMmbjBOPk/bodxvaHL+bJTePM1tWHfEAoeRCaWEA0CancvngJzMCEAgEAlQaM
Z2iuLMnpdhJpeG9ubGluZS5jb20wCQYDVQR0TBAiWaDAOBgnVHQ88Af8EBAMC8aAmrWHYDV
FAYIKuYBBQQUHawEhGcGEAAQnQF8WmCMNgyA1udlARMFm6wwYLYZIAYb4RQEOFHwYwTDAjE
BQcCARYXhHR8cHM6Ly9kLmN5bWlLmNvS9jCHMwQJIKutYBBQUHAgwRoXaHR0cDHE6Lm
bWlLmNvS9ycGEwHwYDVQRjB3gwFoAUAVmr59cMCPznyAHV9WRR20zowYDR0F0
oB6giHYaHR0cDovL3nyLmN5bWlLmNvS9zi5jcmwVwYIkYWBQQUAEQESzBMBjBBG
BZAbBhNcdHRwOl8vc31uc31tyZQyZ9tMCYCCcGAQUBFzAChcqbodHRwOi8vc31uc31y
L3tNyLmYdDCAoCAQMEGcIgAQQB1nkCAJBIEgFqEgFgE7wA82AK5S5CZ0CFhU7s4sncn8
uON3zQ7IdwQQAABAATXcAGNUYAAAAQDACEcwrQRHIALVY1QmveDa2R6k1jKyc+c0L8we+duH+X
ngzA1iBbVbckcGy8HlIv5gy6N XKpkoBAnEoOxXQxsioZ5ahFwDQ81AYFbUpov18sL00
xhdrm88Fw70c+UnFXWidDdAAABTAxBgNtUEAIAQQALEVwR1RgdRvCsZ7CQ2KR1p97Tk6G6u6
yFJxJdMrM17iClEX1vDwRadow+3xrneIS/hFEPsyfjw+Eh3G3p81La+aMA86GCgS9I3b3
A4IBAQCDoPfK1Kztvsd/0LEZNcP94G4Z8C6RXmYzpxp/z906pGiTo+qA1ohy8skipWiAe
KaHe7c7rn1z2tU1B7MLvN8Lkoy5zkqIf164v1jci1zKw78EB20XUCXoEOTY/r/m9/yY
V30AbE02AKnhmHE0u12ZYd46yr/rrvdf1EBoFJhtAp51p6m/ZyGwC4wv+7kzb+/.XOFlzJF
ZXktM9aNPszyZ5406iuRt88FmU+kC8tqv3/UYlYsZdIWNc9Shho5X79yXN1HKB80HRz6
pRWzAYY5vdU38Erv8KUTe0DPybFRzmnnoOyoRgjU70a
-----END CERTIFICATE-----

To make sure the certificate can be added in NetScaler, place an Enter character after every 64th character.

Add the certificate to the NetScaler appliance in the Traffic Management > SSL > Manage Certificates section.
Part 2: Configure the NetScaler Appliance

The following configuration is required on the NetScaler appliance for it to be supported as a SAML service provider for OAM:

- SSL certificate with external and internal DNS configured for the FQDN presented by the certificate (Wildcard certificates are supported).
- AAA virtual server
- SAML policy and profile

This guide covers the configuration described above. The SSL certificate and DNS configurations should be in place prior to setup.

To Configure your AAA Virtual Server

An employee trying to log in to OAM is redirected to a NetScaler AAA virtual server that validates the employee’s corporate credentials. This virtual server listens on port 443, which requires an SSL certificate. External and/or internal DNS resolution of the virtual server’s IP address (which is on the NetScaler appliance) is also required.

The following steps require a preexisting virtual server to be in place. In addition, they assume that DNS name resolution is already in place, and that the SSL certificate is already installed on your NetScaler appliance.

1. On the NetScaler Configuration tab, navigate to Security > AAA – Application Traffic > Virtual Servers and click the Add button.
2. In the Authentication Virtual Server window, enter the virtual server’s name and IP address.
3. Scroll down and make sure that the Authentication and State check boxes are selected.
4. Click Continue.
5. In the Certificates section, select No Server Certificate.
6. In the Server Cert Key window, click Bind.
7. Under SSL Certificates, choose your AAA SSL Certificate and select Insert. (Note – This is the certificate that you provided as the signing certificate in the Service Provider setup in OAM.)
8. Click Save, and then click Continue.

Configuring the SAML policy

Click the plus (+) icon next to authentication. Then, on the Choose Type screen, select SAML and Primary.
On the next screen, enter a name for the policy. Then, click the plus (+) icon (or, if a SAML server has already been added, the pencil icon) next to the server name. Enter `ns_true` as the expression, because this policy is to be used for all authentication.

### Create Authentication SAML Policy

<table>
<thead>
<tr>
<th>Name*</th>
<th>oam_saml</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>SAML</td>
</tr>
<tr>
<td>Server*</td>
<td>Oam</td>
</tr>
<tr>
<td>Expression*</td>
<td><code>ns_true</code></td>
</tr>
</tbody>
</table>

This next screen requires you to provide configuration settings. Here, for IDP certificate name, you will be required to provide the certificate used by OAM to sign assertions sent to NetScaler.


The signing certificate should be the NetScaler server certificate, and the issuer name should be set to the same name set in the OAM configuration. For basic configuration used as an example in this article, Reject Unsigned Assertion is set to OFF. The IDP certificate is the certificate that was added earlier to the NetScaler appliance during OAM configuration.

Now click More. In the additional settings that appear, confirm that the signature algorithm and digest method are set to SHA1.

This completes configuration for SAML.
Conclusion

NetScaler provides a secure and seamless experience with OAM by enabling single sign-on to OAM accounts, avoiding the need for users to remember multiple passwords and user IDs, while reducing the administrative overhead involved in maintaining these deployments.