WEBADM SAML IDENTITY PROVIDER

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved. http://www.rcdevs.com

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

B WebADM SAML Identity Provider

Web-Service SSO Federation

Configuration of WebADM as a SAML Identity Provider

1. Configuration of the Identity Provider

First, we need a WebADM server with *MFA Authentication Server* and *OpenID & SAML Provider*. We can use the <u>appliance</u> or <u>install</u> a new server.

We need also a DNS name for the server. If we can not change the DNS, we can also add the name in /etc/hosts or c:\WINDOWS\system32\drivers\etc\hosts for testing purpose:

Once the server is up and running, we can configure it as a SAML Identity Provider (IdP).

We connect to the WebADM GUI > Applications tab > Singe Sign-On > OpenID & SAML Provider > REGISTER:

| ome Admin | Create | Search Import Databases Applications About Logout |
|------------------|--------|---|
| | | Registered Applications and Services |
| Categories | | Web Applications |
| Authentication | (2) | OpenID & SAML Provider 1.2.2-6 (Freeware) |
| SMS Relay | (1) | |
| Self-Service | (3) | SAML2, OpenID-Connect and OAuth2. |
| Signature | (1) | Latest Version: 1.2.2-6 (Ok) |
| / Single Sign-Or | ı (2) | Status: Not Registered [REGISTER] |
| | | Available Languages: FR |

We click on **CONFIGURE**:

| | | Registered Applications and Services |
|------------------|-----|---|
| Categories | | Web Applications |
| Authentication | (2) | OpenID & SAML Provider 1.2.2-6 (Freeware) |
| SMS Relay | (1) | OpenID & SAMI single sign-on service (Identity Provider) supporting |
| Self-Service | (3) | SAML2, OpenID-Connect and OAuth2. |
| Signature | (1) | Latest Version: 1.2.2-6 (Ok) |
| ✓ Single Sign-On | (2) | Status: Not Configured [CHECK] [CONFIGURE] [REMOVE] |
| | | Available Languages: FR |
| | | WebApp URL: https://webadm.local/webapps/openid/ |
| | | SAML Metadata: https://webadm.local/ws/saml/ |

We add the url of the server in **Issuer URL**:

| Common Features | | | | | |
|--|----------------------|--|--|--|--|
| ✓ Issuer URL | https://webadm.local | | | | |
| This is your IdP EntityID or issuer name, and it must be a valid URL | | | | | |

At Server Certificate, we click on Edit:

| \checkmark | Server Certificate | | Edit |
|--------------|--|---|------|
| | Paste here the public certifiate The PEM certificate block star | e (in PEM format) for your IdP server. rts withBEGIN CERTIFICATE | |
| \checkmark | Server Private Key | | |
| | Paste here the private key (in The PEM private key block sta | PEM format) for your IdP server. arts withBEGIN RSA PRIVATE KEY | |

We click on Generate:

| X.509 Certificate Generator | | | | | | |
|--|---|--|--|--|--|--|
| Common Name: WebADM Certificate RSA Key Size: 2048 Bits \$ |] | | | | | |
| Generate | | | | | | |

| X.509 Certificate Generator | |
|---|---|
| Generating 2048 bits private key Success Creating a certificate request Success Calling WebADM CA for certificate request signing Success | |
| Certificate | |
| BEGIN CERTIFICATE MIICujCCAaKgAwIBAgIBAjANBgkqhkiG9w0BAQsFADAkMRIwEAYDVQQDD/ RE0gQ0EXDJAMBgNVBA0MBUxYY2FSMB4XDTE3MTIyMTA5MzEzM1oXDTE MzEzM1owHTEbMBkGA1UEAwwSV2ViQURNIENIcnRpZmIjYXRIMIBIjANBgk 9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt50Qdornq&TzHj8hjAScG0vxVeZIf +cwGgRV7wo3LYKigqMF8aEb1i4yzM7MB6o058apWTBR5Jff0F9Ng+bFzxv XzobKblp1THmEhCyTZj54u2mO94+wW5pS0Yff8Q5CMrPcN32i3X/ZyLjTlic gFyzIazvs+PDEHGMJ93JPV+zAf7d02cKE78E8z+eJhVibdJjeJtSK0aBw90T paoesjk1tX+IrY3L0tJapLd1TbBIZ3wgqmXosPf672q1erRljxccNpK582p5m5T SIIHXIMoJpadW+MIJWA6W6gc0PwIlatmoHcyxRNFEMjsnC+ZNQIDAQABM/ SIb3DQEBCwUAA4IBAQAKzn7PZqpQRdG+M62on6g4En2h9bxRcLYKREzH q6wNg0LsQwZiI0KGGERpJ1SSkdeBzW72VVmEmDZxrrigMacgJaaK7K0DU 0ZHyc8Madt70jTAsDfJA/c3A754q37/BMXYEqZ/1Rkb8dnK42IZmT6MW0f SF03/T2pYWc/xMEByxbtVg1NT80DKNkYDtNfC1GCGGRRibzrGFORXGNTKcf | AIXZWJB i4MTIyMTA5 qhkiG Ske0Fh WV6bBR qRcUW '3zOW 'e AOGCSqG 8LEebHAo Gj6nxAf GAdxC Dibgo5n +rIS3 |
| Private Key | |
| BEGIN PRIVATE KEY MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAolBAQC3nRB2iud ePyGMBJwY6/FV5mV9KR7QWH5zAaBFXvCjctgqKCowXxoRvWLjLMzswHq FHki9/QX02D5sXPG9ZXpsFF0hspsinVMeYSELJNmPni7aY73j7BbmlLRitBF ys9w3f0Ldf9nluNMiWpFxRaAXLMhrO+z48MQCYwn3ck9X7MB/t3TZwoTvv FWJt0mN4m1lo5oHD05PfM5alqh6y0TW1f4itjcs60lqkt3VNsGVnfCCqZeiw3 arV6tGWPFxw2mTnzanmblN5lggdcgygmlp1b4yUIVDpbqBzQ/AiVq2ag4zE yOycL5k1AgMBAAECggEAek3u12dzJJNA9uRolOllhkCApozRSyeoIEnO/1s9v i+ZzYDEywvY07k7F5GyWOYu1bQ0hWa5CyW6hu/7L4sr0P55KJm8TqD09U z7LrM4FXo4SQfu4Z2qsRVjs7e96DvKSj0Q123BGb1nuE4qhEi4JE9zBu6pXU L4JAe014A5NLof500hYJJb09brfzoXI4Oevuf0/5uiaYqJcFR2Z6KFfVgWJJ67 tO4uIAXdaFx9ceaef8fBYNa0CVipB+/Mb3fFJOs9X406YPhitvONd8x9lkfT9 8f+GYKEB1Smw5yAnwa6yOcvbPX99F24q4pvrIUD4yQKBgQDkXeAcFXcilff A4BN118qjvWcArZkgl7MsWps6PL0UVdumVZ/bSuWsiuZCbxZKEi52HYNpv DKHDT6cNW9N/LBD27vXfJGJ1ymkRG24JONPX386pFxK3GAo2vtkyTqatR | epzxPM jTnxqlZM ·Dkl wTzP54m 9/rv EOUQ welT wBauXTnF 5Epy 'ZU 6Sh Dhak0+ lub93j /w23nKm |
| Apply Cancel | |

We can add some extra attributes, for example **mail** and **mobile**, and click on Apply:



That's all, WebADM is now able to work as an Identity Provider (IdP).

We can check metadata, go to WebADM GUI > Applications > Single Sign-On > OpenID & SAML Provider > SAML Metadata and open the link in a new tab:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://webadm.local">
<IdPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>
MIICujCCAaKgAwIBAgIBAzANBgkqhkiG9w0BAQsFADAkMRIwEAYDVQQDDAlXZWJBRE0gQ0ExDjAMBgNVBAoMBUxv)
</X509Certificate>
<!--
Cert Fingerprint (SHA1): 802b0a629dfc11a686306a73f8b11b272e1b9ca2
- ->
<! - -
Cert Fingerprint (MD5): a0480b3a54a7ea7e2da2d6b9e27fbfbf
- ->
</X509Data>
</KeyInfo>
</KeyDescriptor>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"</pre>
Location="https://webadm.local/webapps/openid/"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"</pre>
Location="https://webadm.local/webapps/openid/"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"</pre>
Location="https://webadm.local/webapps/openid/"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"</pre>
Location="https://webadm.local/webapps/openid/"/>
</IdPSSODescriptor>
</EntityDescriptor>
```

2. Configuration of a Service Provider: SP Initiated

For this test, we are using simplesamplphp.

We install it on another *CentOS* 7 server.

We open http port:

firewall-cmd --permanent --add-service http
firewall-cmd --reload

We disable selinux:

setenforce 0
vi /etc/selinux/config

We install required packages:

```
yum install wget php php-mbstring php-xml httpd
```

We install simplesamlphp:

```
wget "https://simplesamlphp.org/download?latest" -0 ssp.tgz
tar xzf ssp.tgz
mv simplesamlphp* /var/simplesamlphp
```

We add a virtual host to Apache (replace sp.local with the right DNS name who point to this server):

vi /etc/httpd/conf.d/saml.conf

```
<VirtualHost *>
   ServerName sp.local
   DocumentRoot /var/www/sp.local
   SetEnv SIMPLESAMLPHP_CONFIG_DIR /var/simplesamlphp/config
   Alias /simplesaml /var/simplesamlphp/www

   Coirectory /var/simplesamlphp/www>
    Require all granted
   </Directory>
</VirtualHost>
```

We add the Identity Provider. All these values should correspond to the content of metadata from SAML configuration in WebADM:

- > \$metadata[] corresponds to entityID
- > SingleSignOnService corresponds to SingleSignOnService Location=
- > SingleLogoutService corresponds to SingleLogoutService Location=
- > certFingerprint corresponds to Cert Fingerprint (SHA1)

vi /var/simplesamlphp/metadata/saml20-IdP-remote.php

```
<?php
$metadata['https://webadm.local'] = array(
    'SingleSignOnService' => 'https://webadm.local/webapps/openid/',
    'SingleLogoutService' => 'https://webadm.local/webapps/openid/',
    'certFingerprint' => '802b0a629dfc11a686306a73f8b11b272e1b9ca2',
);
```

We enable SAML in /var/simplesamlphp/config/config.php:

vi /var/simplesamlphp/config/config.php

enable.saml20-IdP' => true

We start Apache:

systemctl start httpd
systemctl enable httpd

We open http://sp.local/simplesaml in a browser:

| 20 |) sp.local/si | mplesaml/module. | php/core/frontpa | ge_welcome.ph | ηp | | | | ☆ | | G 8 |
|---------------------------------|---|--|--|--|--|--|--|---|------------------------------|-------------------|------------|
| | | | | | | | | | | | |
| s | impleSAM | Lphp installatio | n page | | | | | | | | |
| Eng Lëtz 简 [/] | l lish B okmål zebuergesch 体中文 繁體 [,] | Nynorsk Sámegi Čeština Slovenšč 中文 русский язык | ella Dansk Deuts ina Lietuvių kalba עברית eesti keel ע | sch Svenska S Hrvatski Mag Bahasa Indone | Suomeksi E yar Język p esia Srpski | spañol Fran oolski Portug Latviešu R | çais Italiano luês Portugi comânește E | o Nederlands uês brasileiro Euskara ελλην | Türkç νικά <i>Ι</i> | e 日∶ \frikaa | 本語 ans |
| | Welcome | Configuration | Authentication | Federation | | | | | | | |
| | Congratula installation, documentat | tions, you have sur where you will find ion. entation | ccessfully installed links to test exampl | SimpleSAMLph _l les, diagnostics, | p. This is the metadata ar | e start page of nd even links | ^f your to relevant | Login as ad | Iminis | trator | |
| | About Si | mpleSAMLphp | | | | | | | | | |
| | This Simple SimpleSAM | SAMLphp thing is p Lphp web page ove | pretty cool, where car ar at <u>UNINETT</u> . | an I read more a | ibout it? You | can find more | e information | about it at the | | | |
| C | opyright © 20 | 07-2017 UNINETT | AS | | | | | | ((| ŝ | °°° |

We click on Authentication:

| SimpleSAMLphp installation page | |
|---|--|
| English Bokmål Nynorsk Sámegiella Dansk Deutsch Svenska Lëtzebuergesch Čeština Slovenščina Lietuvių kalba Hrvatski Ма 简体中文 繁體中文 русский язык eesti keel עַבְרִית Bahasa Indor | Suomeksi Español Français Italiano Nederlands gyar Język polski Português Português brasileiro Türkçe 日本語 nesia Srpski Latviešu Româneşte Euskara ελληνικά Afrikaans |
| Welcome Configuration Authentication Federation | |
| Test configured authentication sources | Login as administrator |
| Copyright © 2007-2017 UNINETT AS | |

We click on Test configured authentication sources:

| Test authentication sources | |
|--|---|
| nglish Bokmål Nynorsk Sámegiella Dansk Deutsch Svenska Suomeksi Español Français Italiano ovenščina Lietuvių kalba Hrvatski Magyar Język polski Português Português brasileiro Türkçe 日本 אַרָרַיָּרָ Bahasa Indonesia Srpski Latviešu Românește Euskara ελληνικά Afrikaans | Nederlands Lёtzebuergesch Čeština 语 简体中文 繁體中文 русский язык еез |
| Test authentication sources | |
| admin default-sp | |
| Copyright © 2007-2017 UNINETT AS | |

We click on default - sp:

| 0-14- | | |
|--------|-------------------------|----------|
| Select | <i>v</i> oi ir identity | provider |
| | | |

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomeksi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עַבְרִית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara | ελληνικά | Afrikaans

Please select the identity provider where you want to authenticate:

not translated (idpname_https://webadm.local) ᅌ Select

Remember my choice

Copyright © 2007-2017 UNINETT AS

| We c | lick on | Sel | ect | : |
|------|---------|-----|-----|---|
|------|---------|-----|-----|---|

| OpenID & SAML Provider | | | | | | |
|---|-----------------------------------|---------------------------------------|--|--|--|--|
| Welcome to the Identity Provider Portal at <i>webadm.local</i> . Please enter the required information to login at <i>sp.local</i> . | | | | | | |
| Login with PKI 3 | Username: Password: Domain: | john •••••• Default \$ Login | | | | |
| × | Provided by | RCDevs Security Solutions | | | | |

We authenticate with an activated user through WebADM IdP:



It's done, we are authenticated:

| SAML 2.0 SP Demo Example | • |
|--------------------------|---|
|--------------------------|---|

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomeksi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עַרְרִית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara | ελληνικά | Afrikaans

SAML 2.0 SP Demo Example

Hi, this is the status page of SimpleSAMLphp. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that are attached to your session.

Your attributes

| User ID uid | john |
|----------------|-------------------|
| domain | Default |
| Mail mail | john.doe@acme.com |
| Mobile | 123 456 789 |

SAML Subject

| | NameId | 7fc7212c35c7c2e2cb5d820044469055 | |
|-----------|-----------|--|--|
| | Format | urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | |
| Logout | | | |
| Copyright | © 2007-20 | 17 UNINETT AS | |

We can check the log in /opt/webadm/logs/webadm.log:

```
[2017-12-21 11:16:31] [192.168.1.220] [OpenID:Y84I9XHY] User not authenticated
(entering login form)
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] New login request (OpenOTP)
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] > Username: john
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] > Domain: Default
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] > ANY Password: xxxxxx
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] Sending openotpSimpleLogin
request
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] New openotpSimpleLogin SOAP
request
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] > Username: john
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] > Domain: Default
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] > Password: xxxxxxx
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] > Client ID: OpenID
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] > Source IP: 192.168.1.220
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] > Context ID:
5cf415099b146265083580f7098f5717
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Registered openotpSimpleLogin
request
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Resolved LDAP user: cn=john,o=Root
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Started transaction lock for user
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Found 1 user mobiles: 123 456 789
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Found 1 user emails:
john.doe@acme.com
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Found 37 user settings:
LoginMode=LDAP, OTPType=TOKEN, OTPLength=6, ChallengeMode=Yes, ChallengeTimeout=90, MobileTime
1:HOTP-SHA1-6:QN06-
T1M, SMSType=Normal, SMSMode=Ondemand, MailMode=Ondemand, LastOTPTime=300, ListChallengeMode=
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Found 1 user data: LoginCount
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Requested login factors: LDAP
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] LDAP password Ok
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Updated user data
[2017-12-21 11:16:36] [127.0.0.1] [OpenOTP:CADTGBMD] Sent success response
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] OpenOTP authentication success
[2017-12-21 11:16:36] [192.168.1.220] [OpenID:7TWF4J4E] Resolved LDAP user:
cn=john,o=Root (cached)
[2017-12-21 11:16:37] [192.168.1.220] [OpenID:7TWF4J4E] Login session started for
cn=john,o=Root
[2017-12-21 11:16:37] [192.168.1.220] [OpenID:7TWF4J4E] Sent SAML success response
```

3. Configuration of a Service Provider: IdP Initiated

In this case, the authentication will be started directly from *OpenID & SAML Provider* web application. We will configure WebADM to manage authentications with Amazon Web Service (AWS). Other Service providers are available but not shown in this HowTo: GSuite, SalesForce, SugarCRM, Zimbra, GoToMeeting, GoToWebinar, GoToTraining and GoToAssist.

First, we save the SAML metadata in a file. For our IdP server, we find it in https://webadm.local/ws/saml/.

We open AWS console > IAM > Identity providers > reate Provider:

| Search IAM | Create | Provider Delete Pro | viders | | | 2 🌣 |
|-------------------|--------|---------------------|--------|--------|-----------------|----------------|
| Dashboard | Filter | |) | | | Showing 5 resu |
| Groups | | | | | | |
| Users | F | Provider Name 🗢 | | Туре 🗢 | Creation Time 🗢 | |
| Roles | | | | | | |
| Policies | | | | | | |
| dentity providers | | | | | | |
| Account settings | | | | | | |
| Credential report | | | | | | |
| | | | | | | |
| Encryption keys | | | | | | |

We select **SAML**, add a name, insert the metadata file and click on **Next** Step:

| Create Provider | Configure Prov | vider | |
|--|---|---|------------------|
| Step 1 : Configure Provider Step 2 : Verify | Choose a provider type. Provider Type* | SAML | |
| | Provider Name* | webadm Maximum 128 characters. Use alphanumeric and '' characters. | |
| | Metadata Document* | C:\fakepath\saml_metadata.xml Choose File | |
| | * Required | | Cancel Next Step |

We click on Create:

| Create Provider | Verify Provider Information |
|---|--|
| Step 1 : Configure Provider Step 2 : Verify | Verify the following provider information. Click Create to finish. Provider Name webadm Type SAML |
| | Cancel Previous Create |

Now, our IdP is added to AWS. We select **Roles**:

| Search IAM | | You have finished crea To use this provider, you mus | ting a SAML provider. | vider in the role's trust policy. Do t | his now. | × |
|--------------------|------|---|------------------------------|--|-------------|------|
| Dashboard | | Learn more about creating ro | bles for SAML providers. | ····· | | |
| Groups | | | | | | |
| Users | Crea | ate Provider Delete Provid | lers | | 0 0 | G |
| Roles | web | adm | | s | howing 1 re | sult |
| Policies | | | | | | |
| Identity providers | | Provider Name \$ | Туре 🗢 | Creation Time \$ | | |
| Account settings | | webadm | SAML | 2017-12-22 10:11 UT | C+0100 | |
| Credential report | | | | | | |
| | | | | | | |
| | | | | | | |

We click on Create Role:

| Dashboard | | |
|-------------------|---|--|
| Groups | What are IAM roles? | |
| aroups | IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following: | |
| Jsers | • IAM user in another account | |
| Roles | Application code running on an EC2 instance that needs to perform actions on AWS resources | |
| Policies | Application code running on an Eoz instance that needs to perform actions on Awo resources | |
| dentity providers | Users from a corporate directory who use identity federation with SAML | |
| Account settings | IAM roles issue keys that are valid for short durations, making them a more secure way to grant access | |
| Credential report | | |
| | Additional resources: | |
| | IAM Roles FAQ | |
| Encryption keys | IAM Roles Documentation | |
| | Tutorial: Setting Up Cross Account Access | |
| | Common Scenarios for Roles | |
| | | |

We click on **SAML**:



We select our SAML provider, select AWS Management Console access and click on Next Permission:

| | - | | | | | | |
|--|-------------------|------------------------------------|---|-------------------|--|--|--|
| AWS service EC2, Lambda and others | Another AWS accou | unt Cognito or any OpenID provider | SAML Saml 2.0 federation Your corporate directory | | | | |
| Allows users that are federated with SAML 2.0 to assume this role to perform actions in your account. Learn more Choose a SAML 2.0 provider If you're creating a role for API access, choose an Attribute and then type a Value to include in the role. This restricts access to users with the specified attributes. | | | | | | | |
| SAML provider webadm Create new provider Create new provider Refresh Allow programmatic access only Allow programmatic and AWS Management Console access | | | | | | | |
| | Attribute SA | AML:aud | • | | | | |
| | Value* htt | tps://signin.aws.amazon.com/saml | | | | | |
| | Condition C | Add condition (optional) | | | | | |
| equired | | | Cancel | Next: Permissions | | | |

We select a permission policy and click on **Next**: **Review**.

| Filter: P | olicy type V Q Search | Showing 345 results |
|-----------|-------------------------------------|--|
| | Policy name | Attachments - Description |
| | AmazonEC2FullAccess | 0 Provides full access to Amazon EC2 via the AWS Manageme |
| | AmazonEC2ReadOnlyAccess | 3 Provides read only access to Amazon EC2 via the AWS Man |
| | AmazonEC2ReportsAccess | 0 Provides full access to all Amazon EC2 reports via the AWS |
| | Final AmazonEC2RoleforAWSCodeDeploy | 0 Provides EC2 access to S3 bucket to download revision. Thi |
| | AmazonEC2RoleforDataPipelineRole | 0 Default policy for the Amazon EC2 Role for Data Pipeline ser |
| | AmazonEC2RoleforSSM | 0 Default policy for Amazon EC2 Role for Simple Systems Man |
| | AmazonEC2SpotFleetAutoscaleRole | 0 Policy to enable Autoscaling for Amazon EC2 Spot Fleet |
| | AmazonEC2SpotFleetRole | 0 Allows EC2 Spot Fleet to request and terminate Spot Instanc |

We add a name and click on Create role:

| Create role | 1 | 2 | | 3 |
|--|--|---------------------|----------|-------------|
| | Trust | Permiss | sions | Review |
| Review | | | | |
| Provide the required information below | and review this role before you create | it. | | |
| Role name* | test_role | | | |
| | Maximum 64 characters. Use alphanumeric and '+=,.@ | _' characters. | | |
| Role description | | | | |
| | | | | 10 |
| | Maximum 1000 characters. Use alphanumeric and '+=, | @' characters. | | |
| Trusted entities | The identity provider(s) arn:aws:iam::407291384 | 368:saml-provider/\ | webadm | |
| Policies | AmazonEC2ReadOnlyAccess | | | |
| * Required | | Cancel | Previous | Create role |

The role is now created, we can select it to see more details.

| Search IAM | Create role Delete role | <i>C</i> * 0 |
|---|---|---------------------|
| Dashboard | Q test_role | Showing 1 result |
| Groups | Role name 👻 Description Trusted entities | |
| Roles | test_role Identity Provider: arn:aws:iam::40 | 72913843 |
| Policies | | |
| Identity providers | | |
| Account settings | | |
| Credential report | | |
| | | |
| Encryption keys | | |
| Search IAM Dashboard Groups Users Roles Policies | Summary Role ARN arn:aws:iarn::407291384368:role/test_role Role description Instance Profile ARNs Path / Creating time 2017_12_22_10:22 UTC+0100 | Delete rol |
| Identity providers | | |
| Account settings | Permissions Trust relationships Access Advisor Revoke sessions | |
| Credential report | Attach policy Attached policies: 1 | |
| Encryption keys | Policy name • Policy type • | |
| | AmazonEC2ReadOnlyAccess AWS managed policy | × |
| | | • Add inline policy |

3.2 Configuration of WebADM

We need to activate IdP initiated authentication for AWS.

We open the configuration in WebADM GUI > Applications > Single Sign-on > CONFIGURE :

| | | Registered Applications and Services |
|------------------|-----|---|
| Categories | | Web Applications |
| Authentication | (2) | OpenID & SAML Provider 1.2.2-6 (Freeware) |
| SMS Relay | (1) | OpenID & SAMI single sign-on service (Identity Provider) supporting |
| Self-Service | (3) | SAML2, OpenID-Connect and OAuth2. |
| Signature | (1) | Latest Version: 1.2.2-6 (Ok) |
| 🗸 Single Sign-Or | (2) | Status: Enabled [CONFIGURE] [REMOVE] |
| | | Available Languages: FR |
| | | WebApp URL: https://webadm.local/webapps/openid/ |
| | | SAML Metadata: https://webadm.local/ws/saml/ |

We check Enable Application SSO and AmazonWS, we add AWS Account Number (a numerical value that you can find in the ARN of the AWS role) and AWS Provider Name and apply:

| | | Application SSO Portal |
|---|---|---|
| | | AmazonWS |
| | | GSuite |
| | | SalesForce |
| | | SugarCRM |
| | Enable Application SSO | Zimbra |
| | Litable Application 350 | GoToMeeting |
| | | GoToWebinar |
| | | GoToTraining |
| | | GoToAssist |
| | | [None] |
| | Allow IdP-initialited login for | the following Cloud applications. |
| | AWS Account Number | 407291384368 |
| | Required if you use Amazon You can optionally set multip | Web Services (numeric value). le accounts in the form 'alias1:account1,alias2:account2'. |
| | AWS Provider Name | webadm |
| SAML provider name in your AWS IAM configuration. | | |

We select the test user and click on WebADM settings: [CONFIGURE]:

| | | Object cn=john,o=Root 🧃 |) | | |
|---|--|--|--|----|-------|
| LDAP Actions | (| Dbject Details | Application Actions | | |
| Delete this object Copy this object Export to LDIF Change password Create certificate Inlock WebApp access Advanced edit mode | Object class(es): Account is unique: WebADM settings: WebADM data: User activated: Logs and inventory | webadmAccount, person Yes (in o=root) 1 settings [CONFIGURE] 3 data [EDIT] Yes Deactivate ① : WebApp, WebSry, Inventory | MFA Authentication Server (12 actions) | | |
| Object Name | јо | hn | | Re | ename |
| Add Attribute (7) | | escription / Note | | \$ | Add |
| Add Extension (1) | L | INIX Account | | \$ | Add |
| Email Address [add values] [delete attribute] | jo | hn.doe@acme.com | | | |
| Mobile Phone Number () [add values] [delete attribute] | 12 | 23 456 789 | | | |
| Last Name [add values] | jo | hn | | | |
| Login Name [add values] | јо | hn | | | |

We select OpenID, add AWS Role Names and Apply. We can also add the AWS role to an LDAP group:

| | | Application SSO Portal | | |
|--|---|--|--|--|
| | | ✓ AmazonWS (Default) | | |
| | | GSuite | | |
| | | SalesForce | | |
| | | SugarCRM | | |
| | Frahla Analization 000 | Zimbra | | |
| | Enable Application 550 | GoToMeeting | | |
| | | GoToWebinar | | |
| | | GoToTraining | | |
| | | GoToAssist | | |
| | | [None] | | |
| | Allow IdP-initialited login for the following Cloud applications. | | | |
| | AWS Role Names | test_role | | |
| | Comma-separated list of You can optionally filter re | role names in your AWS IAM configuration. oles per AWS account number like 'account1:role1,account2:role2'. | | |
| | | Apply Cancel Reset | | |

3.3 Testing

We open the web application in https://webadm.local/webapps/openid/ and Login with the user:

| Openll | D & SAML I | Provider |
|--|------------------------------------|---|
| Welcome to the Identii Please enter the requi | ty Provider Por red information | tal at <i>webadm.local.</i> n to continue. |
| | Username: Password: Domain: | john ••••• Default \$ |
| Login with PKI | Provided by F | RCDevs Security Solutions |

We select Application SSO:

| OpenID & SAML Provider | | | |
|-----------------------------------|---|--|--|
| A Home | Application SSO Logout | | |
| You Web | You are authenticated with account Default\john . Web-based single sign-on is enabled for your account. | | |
| SSO Config | jurations | | |
| Enable SAM | Enable SAML usage: 💿 Yes 🔵 No 🕚 | | |
| Enable OpenID usage: 💿 Yes 🔵 No 📵 | | | |
| SSO Session Time: 1 Hour 💠 📵 | | | |
| | | | |
| ₩ | Provided by RCDevs Security Solutions | | |

We click on Amazon WS:



That's it, we are now connected to AWS:



We can check the log in /opt/webadm/logs/webadm.log:

```
[2017-12-22 09:35:17] [192.168.1.220] [OpenID:4JGOGCOT] New login request (OpenOTP)
[2017-12-22 09:35:17] [192.168.1.220] [OpenID:4JGOGCOT] > Username: john
[2017-12-22 09:35:17] [192.168.1.220] [OpenID:4JG0GCOT] > Domain: Default
[2017-12-22 09:35:17] [192.168.1.220] [OpenID:4JGOGCOT] > ANY Password: xxxxxxx
[2017-12-22 09:35:17] [192.168.1.220] [OpenID:4JGOGCOT] Sending openotpSimpleLogin
request
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] New openotpSimpleLogin SOAP
request
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] > Username: john
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] > Domain: Default
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] > Password: xxxxxx
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] > Client ID: OpenID
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] > Source IP: 192.168.1.220
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] > Context ID:
5cf415099b146265083580f7098f5717
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] Registered openotpSimpleLogin
request
[2017-12-22 09:35:17] [127.0.0.1] [OpenOTP:FFYIGQ6S] Resolved LDAP user: cn=john,o=Root
(cached)
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Started transaction lock for user
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Found 1 user mobiles: 123 456 789
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Found 1 user emails:
john.doe@acme.com
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Found 37 user settings:
LoginMode=LDAP,OTPType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,MobileTime
1:HOTP-SHA1-6:QN06-
T1M, SMSType=Normal, SMSMode=Ondemand, MailMode=Ondemand, LastOTPTime=300, ListChallengeMode=
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Found 2 user data:
LoginCount, RejectCount
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Requested login factors: LDAP
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] LDAP password 0k
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Updated user data
[2017-12-22 09:35:18] [127.0.0.1] [OpenOTP:FFYIGQ6S] Sent success response
[2017-12-22 09:35:18] [192.168.1.220] [OpenID:4JGOGCOT] OpenOTP authentication success
[2017-12-22 09:35:18] [192.168.1.220] [OpenID:4JG0GC0T] Resolved LDAP user:
cn=john,o=Root (cached)
[2017-12-22 09:35:18] [192.168.1.220] [OpenID:4JGOGCOT] Login session started for
cn=john,o=Root
[2017-12-22 09:36:50] [192.168.1.220] [OpenID:4JG0GC0T] Sent SAML success response
```

4. How to create a Client Policy per Service Provider (SP)

Since the WebADM 1.6.9-x and OpenID/SAML provider 1.3.0, it is possible to create WebADM client policies per Service Provider. That will allow you to return attributes, nameID, attributes mappings, or use a different certificate per client (SP) and not only globally. This feature makes the IDP much more powerful.

To create a client policy for your SP, log in on the WebADM Admin GUI, click on Admin tab, Client Policy and click on

Give a name to your Client Policy and then click Proceed and Create Object.

| Confirm object creation fo | or cn=My_SP,dc=Clients,dc=WebAD |
|----------------------------|---------------------------------|
| Attribute | Value |
| DN | cn=My_SP,dc=Clients,dc=We |
| Common Name | My_SP |
| WebADM Object Type | Client |
| | |

We will now configure the client policy. Many settings can be applied here like which users/groups/networks the client policy will be applied, allowed/excluded hours, which domain... An important setting on this page is the Client Name Aliases which will allow us to do the matching between the client policy and the SP. For this, the client policy must be created with the SP issuer URL (Entity ID) as Client Name Aliases.

| Object Settings for cn=sp_saml_ff-bak,dc=Clients,dc=WebADM | | |
|--|--|---|
| | Disable Client When disabled, client requests | Yes No (default) Using this client policy will be refused. |
| | <u>Default Domain</u> This domain is automatically se | AD |
| | Friendly Name Friendly client name or short de | escription to be used for %CLIENT% in user messages. |
| | Client Name Aliases | https://192.168.3.187/simplesaml/module.php/saml/sp/metadata.php/defa ult-sp |
| | Comma-separated list of alternation | ative client IDs. |

The matching is done, we will now configure the SP policy.

If you scroll down a little bit, you will find the setting named Forced Application Policies, click on the Edit button and select OpenID application in the left box.

| Application Settings | | | | | |
|----------------------|---|--|--|--|--|
| | | SAMI Sanica | | | |
| | Name Identifier | Email (Default) | | | |
| | Persistent (default): A persistent N Transient: A new NameID is gene Email: The user email address is X509: The LDAP DN is used and Windows: Uses Windows Domain UserID: The user login name is us | NameID is generated per domain user for the Issuer URL. rated for the time of the user session on the IdP. used and NameID format is set to emailAddress. NameID format is set to X509SubjectName. NUID and NameID format is set to WindowsDomainQualifiedName. sed (does not work with more than one WebADM Domain). | | | |
| | UserID Mapping | uid | | | |
| | SAML attribute to be used to return | the user ID. | | | |
| | Domain Mapping | domain | | | |
| | Attribute to be used to return the us | ser domain. | | | |
| | Group Mapping | groups | | | |
| | Attribute to be used to return the us | ser group memberships. | | | |
| | Return Attributes | | | | |
| | Comma-separated list of LDAP attr Attribute name mappings can be sp Example: fullname,mail,mobile,lang | ibutes to be returned in SAML assertions. becified in the form name1=attr1,name2=attr2. guage=preferredLanguage | | | |
| | Holder of Key | Yes (default) No | | | |
| | Include the user certificate and use If not enabled or the user does not | 'holder-of-key' assertion confirmation method. have a certificate, the method defaults to 'bearer'. | | | |
| | Sign Entire SAML Response | Yes No (default) | | | |
| | By default the IdP signs the XML A Enable this option if you need to sig | ssersion and Subject. gn the entire SAML Response too. | | | |
| | Encrypt SAML Response | ─ Yes ● No (default) | | | |
| | | | | | |
| You | u need to set the client SP certific | cate below for SAML encryption. | | | |
| Client Certificate | | | | | |
| Pa | ste here the public certifiate (in P | EM format) for your SP server. | | | |
| Ass | sertion Consumer Service URL | | | | |
| Re If n | direction URL for the signed logir ot set, the AssertionConsumerSe | n assertion response. erviceURL is taken from the SAML assertion request. | | | |
| Log | gout Consumer Service URL | | | | |
| lf s | et, the user is redirected to the U | IRL after successful logout. | | | |
| | | Apply Cancel Reset | | | |

Configure your client policy with every setting you need for your SP and then save your configuration.

| | Application Settings | | | | | |
|---|---|---|--|--|--|--|
| | | | | | | |
| | SAML Service | | | | | |
| Image: A start of the start of | Name Identifier | Email (Default) 🕈 | | | | |
| | Persistent (default): A persistent NameID is generated per domain user for the Issuer URL. Transient: A new NameID is generated for the time of the user session on the IdP. Email: The user email address is used and NameID format is set to emailAddress. X509: The LDAP DN is used and NameID format is set to X509SubjectName. Windows: Uses Windows Domain\UID and NameID format is set to WindowsDomainQualifiedName. UserID: The user login name is used (does not work with more than one WebADM Domain). | | | | | |
| | UserID Mapping | uid | | | | |
| | SAML attribute to be used to return | the user ID. | | | | |
| | Domain Mapping | domain | | | | |
| | Attribute to be used to return the us | er domain. | | | | |
| | Group Mapping | groups | | | | |
| | Attribute to be used to return the us | er group memberships. | | | | |
| | Return Attributes | webadmdata, xxx=webadmsettings | | | | |
| | Comma-separated list of LDAP attributes to be returned in SAML assertions. Attribute name mappings can be specified in the form name1=attr1,name2=attr2. Example: fullname,mail,mobile,language=preferredLanguage | | | | | |
| | Holder of Key | Yes (default) No | | | | |
| | Include the user certificate and use 'holder-of-key' assertion confirmation method. If not enabled or the user does not have a certificate, the method defaults to 'bearer'. | | | | | |
| | Sign Entire SAML Response | ◯ Yes ● No (default) | | | | |
| | By default the IdP signs the XML As Enable this option if you need to sig | ssersion and Subject. gn the entire SAML Response too. | | | | |
| | Encrypt SAML Response | ◯ Yes ● No (default) | | | | |
| | | | | | | |
| | You need to set the client SP certifi | icate below for SAML encryption. | | | | |
| | Client Certificate | BEGIN CERTIFICATE MIIFizCCA30gAwIBAgIJAKmCPqWZZduvMA0GCSqGSIb3DQEBCwUAMFwx BAYTAIVTMQ8wDQYDVQQIDAZEZW5pYWwxFDASBgNVBAcMC1NwcmluZ2 CgYDVQQKDANEaXMxGDAWBgNVBAMMD3d3dy5leGFtcGxILmNvbTAeFw0 NDA5MTRaFw0xOTEyMDUxNDA5MTRaMFwxCzAJBgNVBAYTAIVTMQ8wDC ZW5pYWwxFDASBgNVBACMC1NwcmluZ2ZpZWxkMQwwCgYDVQQKDANEa BAMMD3d3dy5leGFtcGxILmNvbTCCAilwDQYJKoZIhvcNAQEBBQADggIPAD | | | | |
| | Paste here the public certifiate (in F | PEM format) for your SP server. | | | | |
| | Assertion Consumer Service URL | | | | | |
| | Redirection URL for the signed logi If not set, the AssertionConsumerS | in assertion response. erviceURL is taken from the SAML assertion request. | | | | |
| | Logout Consumer Service URL | | | | | |
| | If set, the user is redirected to the L | JRL after successful logout. | | | | |
| | | | | | | |
| | | Apply Cancel Reset | | | | |

Your client policy for your SP is now configured. Try an authentication from your SP and check the WebADM logs to be sure that your policy is applied correctly.

Note

You can not yet apply any OpenOTP settings in the same OpenID/SAML client policy. That part is in the RCDevs roadmap and will be added in the future.

This manual was prepared with great care. However, RCDevs S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs S.A. The latter especially applies for data processing systems. RCDevs S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs S.A. @ 2019 RCDevs S.A, All Rights Reserved