

Raphael Beauregard, Robin Boucher, François-Xavier Leclerc, Cirelle Precelle

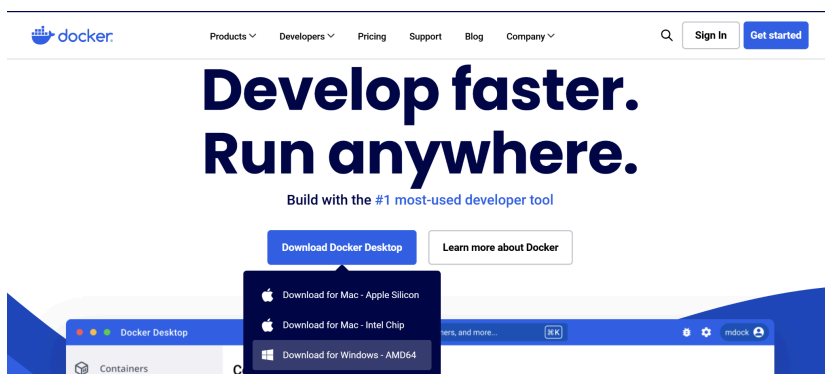
420-3DA-CB IDEN - Gestion Des Identifiants

31 Mars 2025

Installation et configuration d'OpenAM avec Docker

1. *Installation de Docker et OpenAM*

- Installer [Docker](#) pour votre système

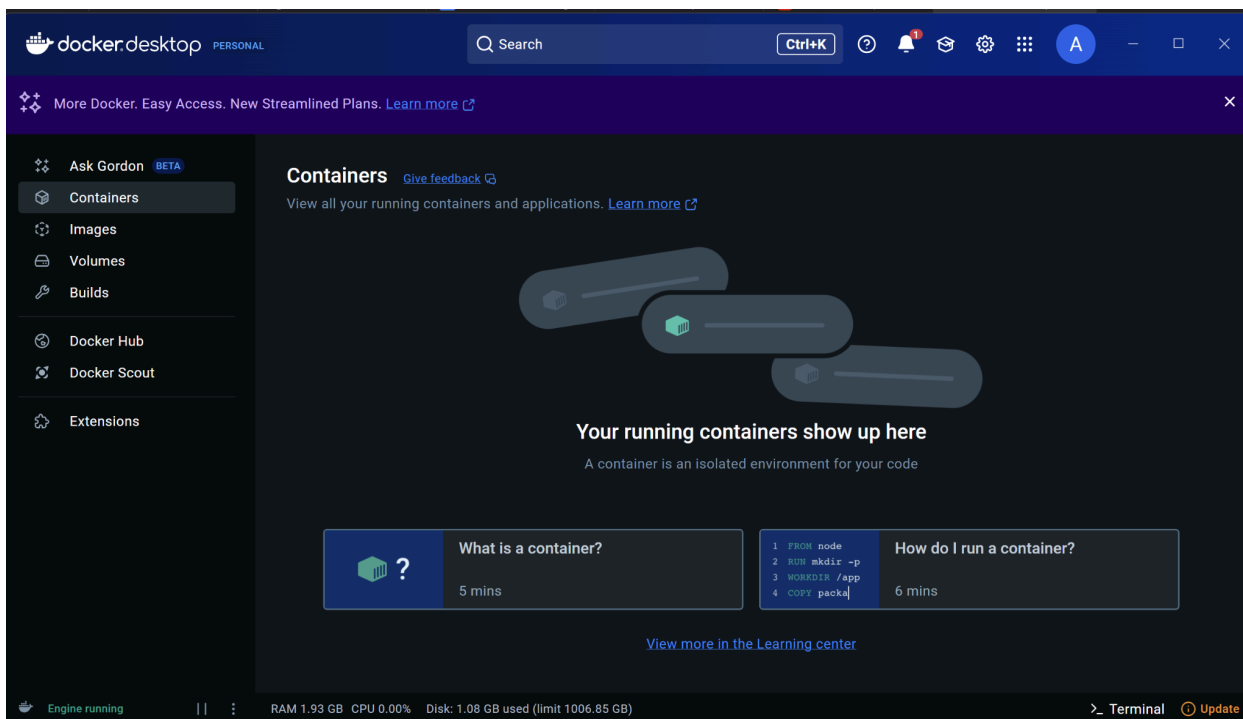
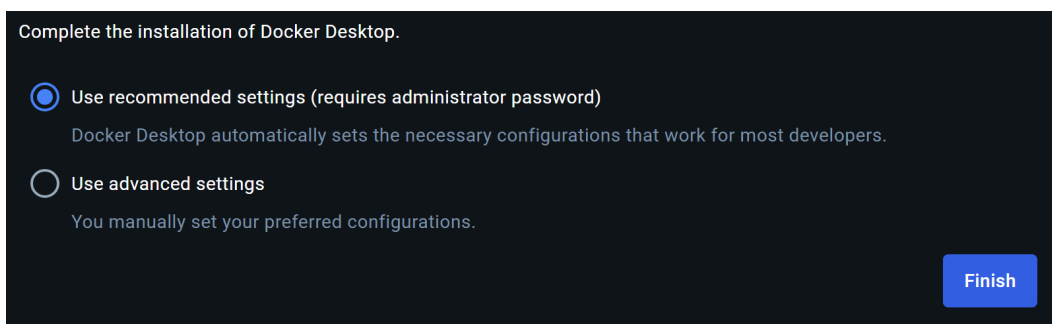


Docker Desktop 4.39.0

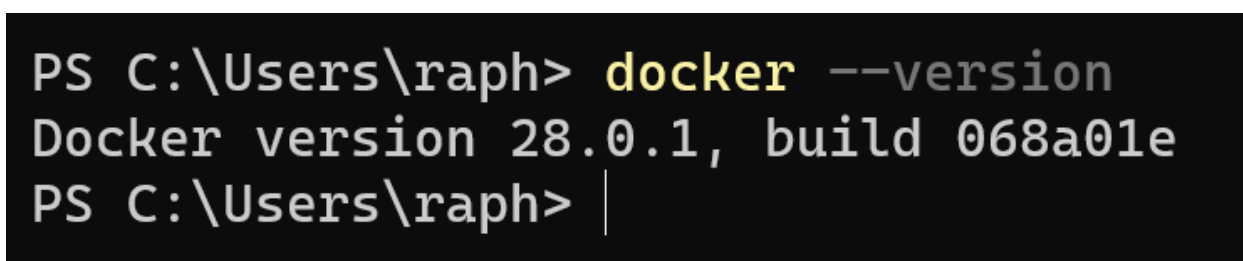
Unpacking files...

```
Unpacking file: resources/docker-desktop.iso
Unpacking file: resources/ddvp.ico
Unpacking file: resources/config-options.json
Unpacking file: resources/componentsVersion.json
Unpacking file: resources/bin/docker-compose
Unpacking file: resources/bin/docker
Unpacking file: resources/.gitignore
Unpacking file: InstallerCli.pdb
Unpacking file: InstallerCli.exe.config
Unpacking file: frontend/vk_swiftshader_icd.json
Unpacking file: frontend/v8_context_snapshot.bin
Unpacking file: frontend/snapshot_blob.bin
Unpacking file: frontend/resources/regedit/vbs/wsRegReadListStream.wsf
Unpacking file: frontend/resources/regedit/vbs/wsRegReadList.wsf
```

- Redémarrez votre PC.



- Vérifier si l'installation a été un succès en tapant “docker --version” dans un terminal/CMD.



2. Installation d'OpenAM

- Télécharger l'image Docker OpenAM depuis le terminal avec “docker pull openidentityplatform/openam”

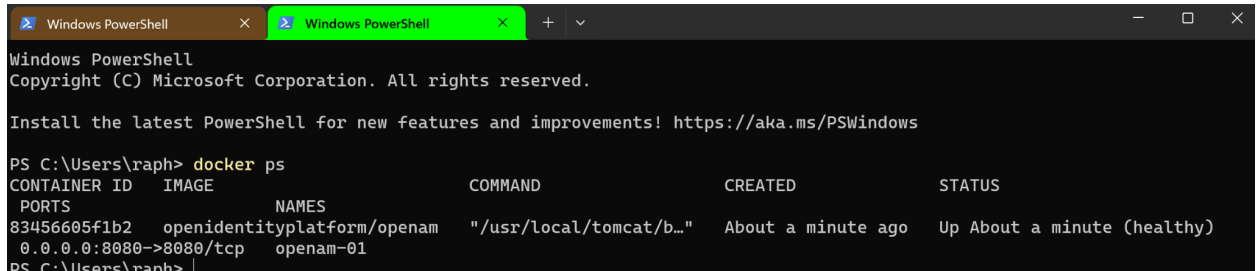
```
PS C:\Users\rpaph> docker pull openidentityplatform/openam
Using default tag: latest
latest: Pulling from openidentityplatform/openam
5a7813e071bf: Pull complete
4f4fb700ef54: Download complete
2f09a3412655: Download complete
24e1027cc04a: Downloading [=====>] 32.51MB/52.88MB
fea09db468e4: Downloading [==>] 32.51MB/478.5MB
08e6e358a2b7: Download complete
5354a9a4a846: Download complete
5ab21fde7f67: Downloading [=====>] 12.58MB/16.96MB
000d4b416c74: Download complete
eb109d1b0266: Download complete
```

- Lancer OpenAM avec la commande suivante:

```
docker run -h openam-01.domain.com -p 8080:8080 --name openam-01 openidentityplatform/openam
```

```
PS C:\Users\rpaph> docker run -h openam-01.domain.com -p 8080:8080 --name openam-01 openidentityplatform/openam
NOTE: Picked up JDK_JAVA_OPTIONS: --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.lang.invoke=ALL-UNNAMED --add-opens=java.base/java.lang.reflect=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport
```

- Vérifier (en utilisant une autre SHELL) que OpenAM est bien en marche

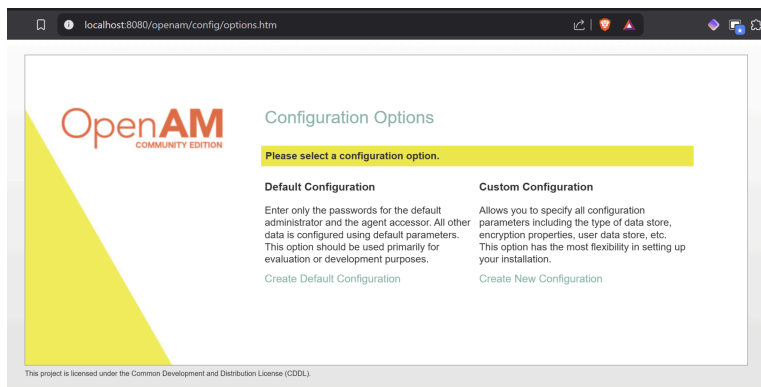


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rpaph> docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS
PORTS         NAMES
83456605f1b2   openidentityplatform/openam        "/usr/local/tomcat/b...  About a minute ago Up About a minute (healthy)
0.0.0.0:8080->8080/tcp   openam-01
```

- Accéder à OpenAM (<http://localhost:8080/openam>) en utilisant un navigateur.



3. Configuration d'OpenAM

- Utiliser la configuration par défaut

Default Configuration

Enter only the passwords for the default administrator and the agent accessor. All other data is configured using default parameters. This option should be used primarily for evaluation or development purposes.

Create Default Configuration

- Choisir une paire de mots de passe (“SuperAwesomeAdmin” et “SuperAwesomeAgent” pour mon cas) et se connecter en utilisant l'utilisateur “amAdmin”.

Provide Default User Passwords

Use this option for a quick setup. Only the passwords for the super user and agent user are required. All other configuration parameters are defaulted for you. The user and agent passwords must be different values.

* Indicates required field

Default User Password	
Default User [amAdmin]	
* Password	<input type="password"/> <input checked="" type="checkbox"/> OK
* Confirm Password	<input type="password"/>

Policy Agent User Password	
Default Policy Agent [UrlAccessAgent]	
* Password	<input type="password"/> <input checked="" type="checkbox"/> OK
* Confirm Password	<input type="password"/>

- Créer un Répertoire d'Utilisateurs (Realm)

Name	<input type="text" value="devrealm"/>		
Active	<input checked="" type="checkbox"/>		
Parent	<input type="text" value="/"/>		
Aliases	<input type="text"/>		
Use Stateless Sessions	<input type="checkbox"/>		

4. Ajout d'un utilisateur

- Dans le menu de gauche, sélectionnez mon-realm → Subjects → Users.
- Créez un utilisateur

New User

* ID:

First Name:	<input type="text" value="Yuri"/>
* Last Name:	<input type="text" value="Markov"/>
* Full Name:	<input type="text" value="Yuri Markov"/>
* Password:	<input type="password" value="....."/>
* Password (confirm):	<input type="password" value="....."/>
* User Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive

5. Configurer l'authentification

- Allez dans REALMNAME → Authentication

[Dashboard](#)
[Applications](#)
[Authentication](#)
 > [Settings](#)
 > [Chains](#)
 > [Modules](#)
[Services](#)
[Sessions](#)
[Data Stores](#)
☒ [Privileges](#)

New Module

Name	<input type="text" value="datastorage1"/>
Type	<input type="text" value="Data Store"/>
<input type="button" value="Cancel"/> <input type="button" value="Create"/>	

6. Configurer les Rôles et Permissions

- Créez un groupe sous Subjects - Groups

General Authentication Services Data Stores Privileges Policies Subjects Agents STS Scripts

User Group

/ (Top Level Realm) > devrealm

Group [Back to Access Control](#)

Group (0 Group)

Name	Universal Id
There are no entries.	

Group (1 Group)

<input checked="" type="checkbox"/> <input type="checkbox"/>	Name	Universal Id
<input type="checkbox"/>	imaginary	imaginary

- Allez dans REALMNAME → Privileges.
- Créez un nouveau rôle et associez des permissions spécifiques aux utilisateurs.

Privileges

- ☐ Read and write access to all realm and policy properties
- ☐ Read and write access to all log files
- ☒ Read access to all log files
- ☐ Write access to all log files
- ☒ Read and write access to all configured Agents
- ☒ Read and write access to all federation metadata configurations
- ☐ REST calls for reading realms
- ☐ Read and write access for policy administration (includes related REST endpoints)
- ☐ REST calls for policy evaluation
- ☐ REST calls for reading policies
- ☐ REST calls for managing policies
- ☐ REST calls for reading policy applications
- ☐ REST calls for modifying policy applications
- ☐ REST calls for reading policy resource types
- ☐ REST calls for modifying policy resource types
- ☐ REST calls for reading policy application types
- ☐ REST calls for reading environment conditions
- ☐ REST calls for reading subject conditions
- ☐ REST calls for reading decision combiners
- ☐ REST calls for reading subject attributes
- ☐ REST calls for modifying session properties.

7. Configurer une Politique de Mot de Passe

- Dans mon-realm, allez dans Authentication → Modules → HOTP/LDAP/OATH
- Vous pouvez définir des règles additionnelles ici pour les mots de passe

Overwrite User Name in sharedState upon Authentication Success	<input type="checkbox"/>	i
User Creation Attributes	<input type="text"/>	i
Minimum Password Length	<input type="text" value="8"/>	i
LDAP Behera Password Policy Support	<input checked="" type="checkbox"/>	i
Trust All Server Certificates	<input type="checkbox"/>	i
LDAP Connection Heartbeat Interval	<input type="text" value="10"/>	i

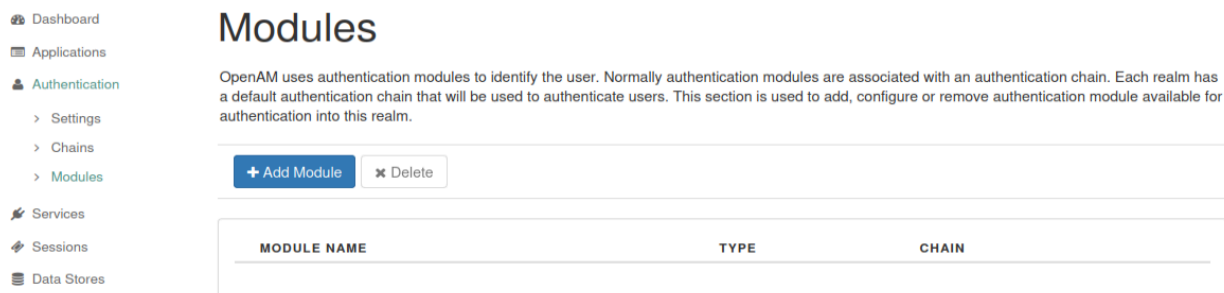
- Il y aussi des paramètres additionnels pour les administrateurs OpenAM sous
Authentication -> Settings -> Account Lockout

Core	User Profile	Account Lockout	General	Security	Post Authentication Processing
Login Failure Lockout Mode	<input type="checkbox"/>	i			
Login Failure Lockout Count	<input type="text" value="5"/>	i			
Login Failure Lockout Interval	<input type="text" value="300"/>	i			
Email Address to Send Lockout Notification	<input type="text"/>	i			
Warn User After N Failures	<input type="text" value="0"/>	i			
Login Failure Lockout Duration	<input type="text" value="0"/>	i			
Lockout Duration Multiplier	<input type="text" value="1"/>	i			
Lockout Attribute Name	<input type="text"/>	i			
Lockout Attribute Value	<input type="text"/>	i			
Invalid Attempts Data Attribute Name	<input type="text"/>	i			
Store Invalid Attempts in Data Store	<input checked="" type="checkbox"/>	i			

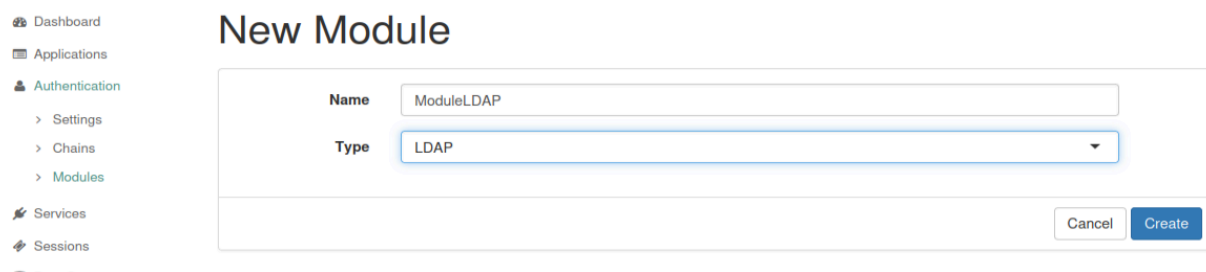
(Robin)

Intégration avec un Annuaire LDAP

1. Allez dans mon-realm → Authentication → Modules.



2. Ajoutez un nouveau module d'authentification de type LDAP.



3. Configurez la connexion avec votre serveur LDAP (exemple OpenLDAP ou Active Directory).

- Faire les configurations souhaitées puis enregistrer.

 LDAP

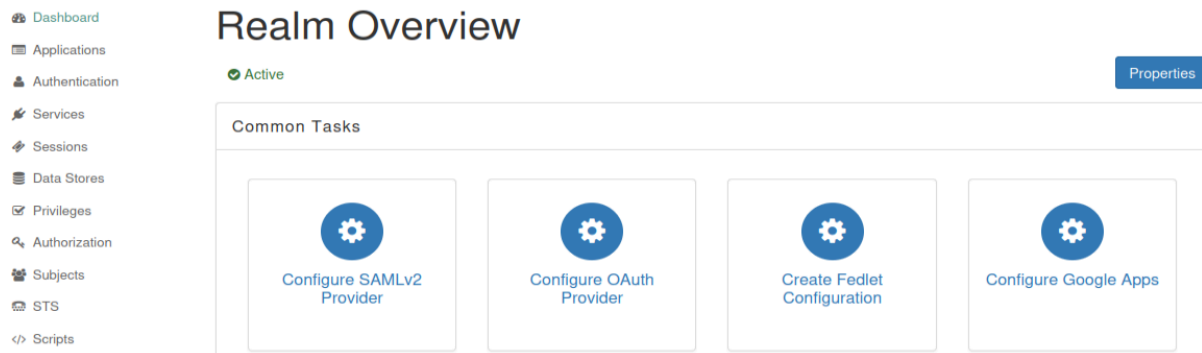
ModuleLDAP

Primary LDAP Server	<input type="text" value="localhost:50389"/>	i
Secondary LDAP Server	<input type="text"/>	i
DN to Start User Search	<input type="text" value="dc=openam,dc=openidentityplatform,dc=org"/>	i
Bind User DN	<input type="text" value="cn=Directory Manager"/>	i
Bind User Password	<input type="password" value="*****"/>	i
Attribute Used to Retrieve User Profile	<input type="text" value="uid"/>	i
Attributes Used to Search for a User to be Authenticated	<input type="text" value="uid"/>	i
User Search Filter	<input type="text"/>	i
Search Scope	<input type="text" value="SUBTREE"/>	i
LDAP Connection Mode	<input type="text" value="LDAP"/>	i
LDAPS Server Protocol Version	<input type="text" value="TLSv1"/>	i
Return User DN to DataStore	<input checked="" type="checkbox"/>	i
Overwrite User Name in sharedState upon Authentication Success	<input type="checkbox"/>	i
User Creation Attributes	<input type="text"/>	i
Minimum Password Length	<input type="text" value="8"/>	i
LDAP Behera Password Policy Support	<input checked="" type="checkbox"/>	i

Mise en Place du Single Sign-On (SSO)

1. Allez dans Federation → SAML Configuration.

- Aller dans Configuration SAMLv2 Provider



2. Ajoutez un fournisseur de services (SP) et un fournisseur d'identité (IdP).

- Aller dans Create Hosted Identity Provider
- Configurer le Circle of Trust

Create a SAMLv2 Identity Provider on this Server Configure Cancel

This page allows you to configure this instance of OpenAM server as an Identity Provider (IDP). You can provide a Name for the provider, Circle of Trust (COT), its metadata of the provider and optionally Signing Certificate. A COT is a group of IDPs and Service Providers (SPs) that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg SPs) in a COT. We shall generate the metadata if you do not have one. You are required to pick a realm for this provider if there are more than one realm in the system. Otherwise, this provider will be configured under the root realm.

Do you have metadata for this provider?: ☐ Yes ☒ No ?

metadata

* Realm: ?

* Name: ?

Signing Key: ?

Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.

* New Circle of Trust: ?

Attribute Mapping

Mapping attributes helps to ensure that both the Service Provider (SP) and the Identity Provider (IDP) can recognize the same attributes that may have unique names. For example, the SP may have an attribute called UserName but the IDP may call it UserID. Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed correctly.

Name in Assertion	Local Attribute Name
<input type="text"/>	<input type="text"/>

Delete Add

Select an attribute. ?

Configure puis,

- Aller dans Create Hosted Service Provider
- Configurer le New Circle of Trust:

Create a SAMLv2 Service Provider on this Server

Configure

Cancel

This page allows you to configure this instance of OpenAM server as a Service Provider (SP). You can provide a Name for the provider; Circle of Trust (COT), its metadata and its attribute mappings. A COT is a group of Identity Providers (IDPs) and SPs that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg IDPs) in a COT. We shall generate the metadata if you do not have one. You are required to pick a realm for this provider if there are more than one realm in the system. Otherwise, this provider will be configured under the root realm.

* Indicates required field

Do you have metadata for this provider?: ☐ Yes ☒ No

metadata

* Realm: /gestion1

* Name: http://localhost:8080/openam

Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this SP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.

* New Circle of Trust: http://localhost:8080/openam

Attribute Mapping

Use default attribute mapping from Identity Provider: ☒

- Entrer l’URL du metadata si possible et faire Configurer

(FX)

S  curisation avec HTTPS

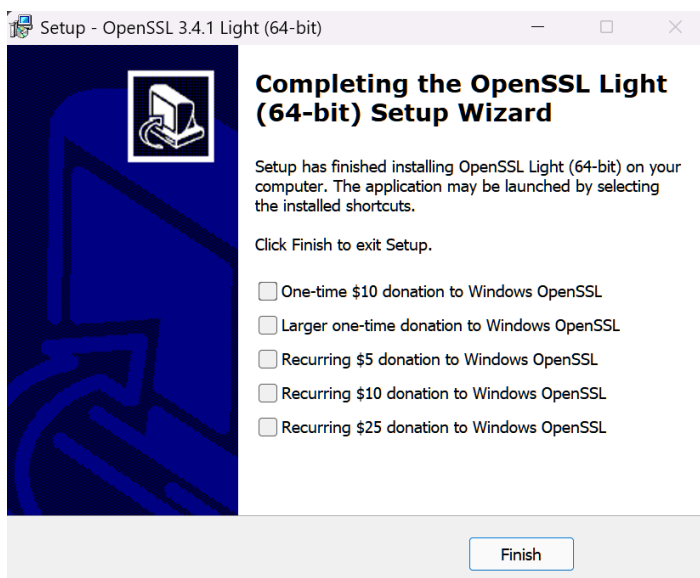
1. Installer un certificat SSL pour s  curiser OpenAM.

- T  l  charger et installer OpenSSL au lien suivant:

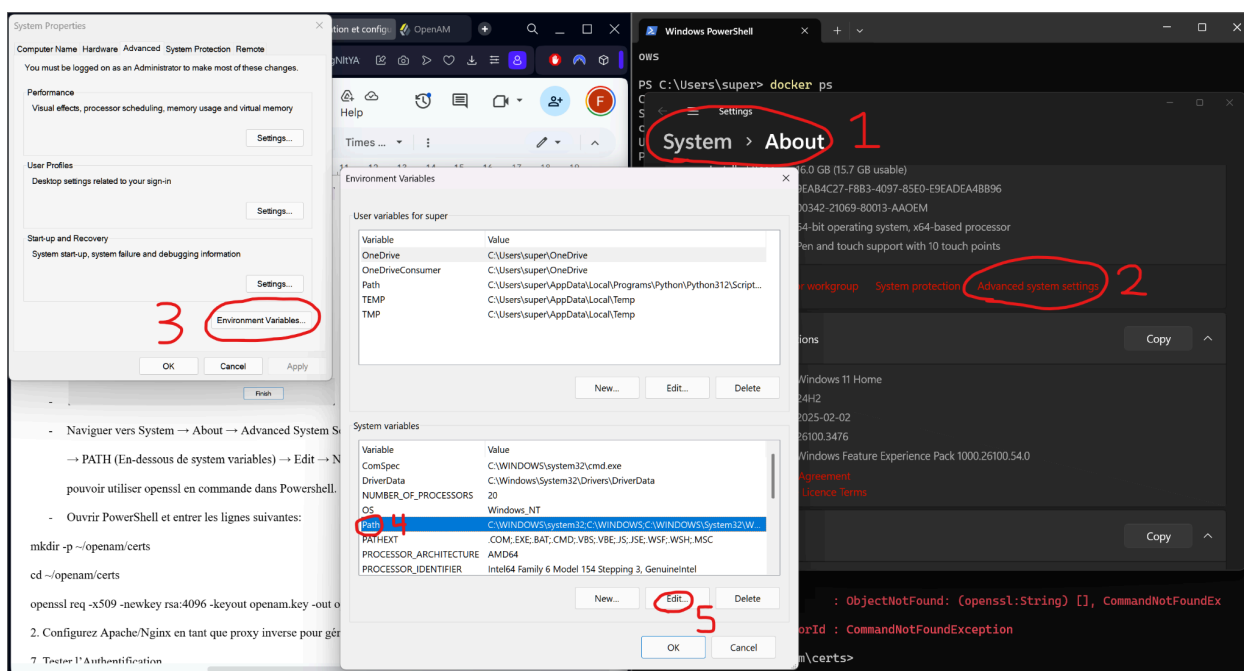
<https://slproweb.com/products/Win32OpenSSL.html>

File	Type	Description
Win64 OpenSSL v3.4.1 Light EXE MSI	SMB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.4.1 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

-



- Naviguer vers *System → About → Advanced System Settings → Environment Variables → Path (En-dessous de system variables) → Edit.*



- Faire New et entrer la ligne suivante, puis appliquer les changements:

C:\Program Files\OpenSSL-Win64\bin

- De cette façon nous allons pouvoir utiliser openssl en commande dans Powershell.

- Redémarrer le terminal Powershell et vérifier l'installation avec:

openssl version

- Créer un nouveau dossier pour le certificat:

mkdir -p ~/openam/certs

cd ~/openam/certs

- Générer votre certificat SSL avec:

openssl req -x509 -newkey rsa:4096 -keyout server.key -out server.crt -days 365 -nodes

- Répondre aux questions ou laisser vide.

2. Configurer Apache/Nginx en tant que proxy inverse pour gérer HTTPS.

- Télécharger Apache en .zip:

<https://www.apachelounge.com/download/>

Apache Lounge
Webmasters

Apache 2.4 VS17 Windows Binaries and Modules

Apache Lounge has provided up-to-date Windows binaries and popular third-party modules for more than 15 years. We have hundreds of thousands of satisfied users: small and big companies as well as home users. Always build with up to date dependencies and latest compilers, and tested thorough. The binaries are referenced by the ASF, Microsoft, PHP etc. and more and more software is packaged with our binaries and modules.

The binaries, are build with the sources from ASF at <http://httpd.apache.org>, contains the latest patches and latest dependencies like zlib, openssl etc. which makes the downloads here mostly more actual then downloads from other places. The binaries **do not run** on XP and 2003. Runs on: 7 SP1, Vista SP2, 8/8.1, 10, 11 Server 2008 SP2 / R2 SP1, Server 2012 / R2, Server 2016/2019/2022.

Build with the latest Windows Visual Studio C++ 2022 aka VS17. Has improvements, fixes and optimizations over VS16 in areas like Performance, MemoryManagement, New standard conformance features, Code generation and Stability. For example code quality tuning and improvements done across different code generation areas for "speed". And makes more use of latest processors and supported Windows editions (win7 and up) internal features.

VS17 is backward compatible, That means, a VS16/15/14 module can be used inside the VS17 binary.

Be sure you installed latest 14.42.34438.0 Visual C++ Redistributable Visual Studio 2015-2022 : vc_redist_x64 or vc_redist_x86 see Redistributable

Apache 2.4 binaries VS17
Info & Changelog

File Name	Size	Date
Apache 2.4.63-250207 Win64		
httpd-2.4.63-250207-win64-vs17.zip	07 Feb '25	11.728K
PGP Signature (Public PGP_key), SHA1-SHA512 Checksums		
Apache 2.4.63-250207 Win32		
httpd-2.4.63-250207-win32-vs17.zip	07 Feb '25	10.549K
PGP Signature (Public PGP_key), SHA1-SHA512 Checksums		

To be sure that a download is intact and has not been tampered with, use PGP, see PGP Signature

Apache 2.4 modules VS17

Mail for the PGP signatures and/or SHA checksums to verify the contents of a file.

Note: VS17 Win32 modules (like mod_fcgid) use VS16 ones at VS16 Win32 modules

Module Name	Size	Date
mod_jk Tomcat connector		
mod_jk-1.2.50-win64-VS17.zip	13 Aug '24	169K
mod_qos Quality Of Service module, is able to protect your server from various kinds of malicious access or attacks like slowlorts, DDoS		
mod_qos-11.74-win64-VS17.zip	03 Jun '23	1.894K

Keep Server Online

If you find the downloads useful, please express your satisfaction with a donation.

[Donate](#)

- Extraire le fichier .zip dans C:\Apache24

- Ouvrir un cmd en administrateur et naviguer au bin:

cd C:\Apache24\bin

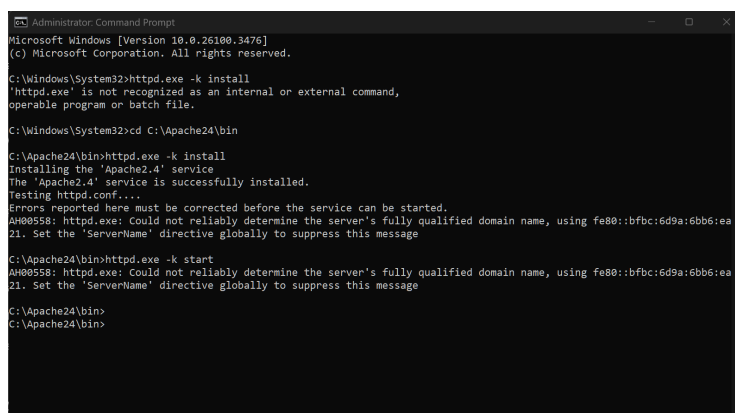
- Installer et démarrer le service Apache (garder le cmd ouvert pour plus tard):

httpd.exe -k install

httpd.exe -k start

- Note: l'erreur suivante n'est pas critique et peut être ignorée:

AH00558: httpd.exe: Could not reliably determine the server's fully qualified domain name, using fe80::bfb6:6d9a:6bb6:ea21. Set the 'ServerName' directive globally to suppress this message



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>httpd.exe -k install
'httpd.exe' is not recognized as an internal or external command,
operable program or batch file.

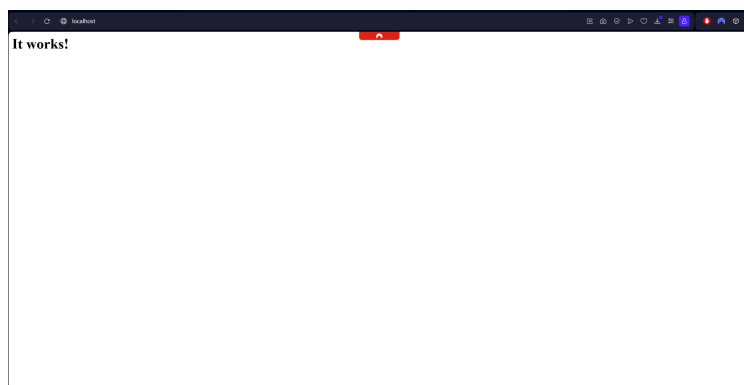
C:\Windows\System32>cd C:\Apache24\bin

C:\Apache24\bin>httpd.exe -k install
Installing the 'Apache2.4' service
The 'Apache2.4' service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
AH00558: httpd.exe: Could not reliably determine the server's fully qualified domain name, using fe80::bfb6:6d9a:6bb6:ea21. Set the 'ServerName' directive globally to suppress this message

C:\Apache24\bin>httpd.exe -k start
AH00558: httpd.exe: Could not reliably determine the server's fully qualified domain name, using fe80::bfb6:6d9a:6bb6:ea21. Set the 'ServerName' directive globally to suppress this message

C:\Apache24\bin>
C:\Apache24\bin>
```

- Ouvrir la page <http://localhost> et s'assurer que le message "It works!" est présent (la page de confirmation d'installation).



- Ouvrir le fichier de configuration d'Apache avec la commande suivante dans Powershell:

notepad C:\Apache24\conf\httpd.conf

- Enlever le # des lignes suivantes s'il est présent (utiliser ctrl + F pour chercher):

LoadModule ssl_module modules/mod_ssl.so

LoadModule proxy_module modules/mod_proxy.so

LoadModule proxy_http_module modules/mod_proxy_http.so

LoadModule socache_shmcb_module modules/mod_socache_shmcb.so

Include conf/extra/httpd-ssl.conf

- Ajouter ce paragraphe à la fin du fichier afin d'ajouter un serveur virtuel pour OpenAM
puis sauvegarder le fichier:

*<VirtualHost *:443>*

ServerName localhost

SSLEngine on

SSLCertificateFile "C:/Apache24/conf/server.crt"

SSLCertificateKeyFile "C:/Apache24/conf/server.key"

ProxyRequests Off

ProxyPass / http://localhost:8080/

ProxyPassReverse / http://localhost:8080/

</VirtualHost>

- Ouvrir le fichier:

notepad C:\Apache24\conf\extra\httpd-ssl.conf

- Ajouter les lignes suivantes en-dessous de Listen 443, puis sauvegarder:

*<VirtualHost *:443>*

ServerName localhost

DocumentRoot "C:/Apache24/htdocs"

SSLEngine on

SSLCertificateFile "C:/Apache24/conf/server.crt"

SSLCertificateKeyFile "C:/Apache24/conf/server.key"

ProxyRequests Off

ProxyPass /openam http://localhost:8080/openam

ProxyPassReverse /openam http://localhost:8080/openam

</VirtualHost>

- Naviguer vers:

C:\Users\<user>\openam\certs

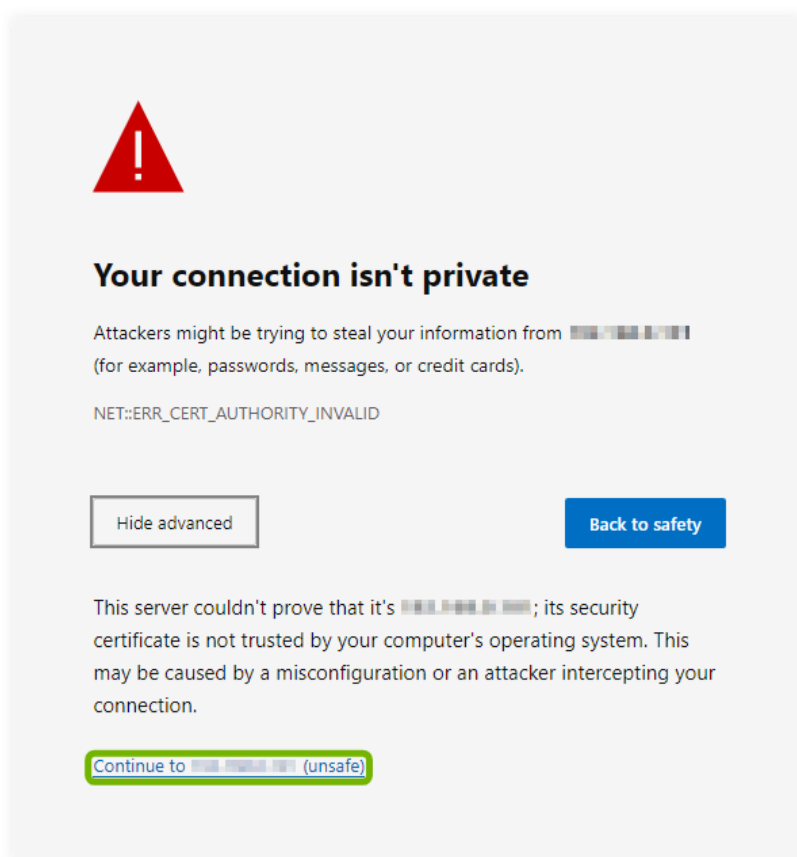
- Copier server.crt et server.key (les fichiers que nous avons créés avec le certificat ssl)
vers le dossier:

C:\Apache24\conf

- Redémarrer le service Apache pour que les changements prennent effet:

httpd.exe -k restart

- Maintenant, on devrait pouvoir accéder à OpenAM sur <https://localhost/openam> et non <http://localhost:8080/openam> (sécurisé par https).
- Si vous avez un message similaire, il faut cliquer sur avancé et continuer vers le site.



Tester l'Authentification

1. Déconnectez-vous de l'interface administrateur.
2. Allez sur <http://localhost:8080/openam/XUI/#login/>.
3. Essayez de vous connecter avec l'utilisateur utilisateur1.

Si la connexion réussit, l'utilisateur est bien géré par OpenAM!

Questions de Compréhension

1. Quelles sont les principales fonctionnalités d'OpenAM ?

OpenAM est une plateforme open source pour effectuer la gestion des identités et des accès pour différents types d'utilisateurs. OpenAM comporte différentes fonctionnalités tel que l'authentification centralisé, la gestion des sessions, le contrôle d'accès basé sur les rôles RBAC, la fédération d'identité (SAML, OAuth, OpenID Connect), la personnalisation des politiques d'accès, des audit et journalisation (suivre et auditer les activités des utilisateurs) et l'intégration avec des systèmes tiers.

2. Pourquoi utiliser Docker pour déployer OpenAM ?

Utiliser Docker nous permet de simplifier le déploiement de OpenAM, Docker nous offre des préconfigurations qui peuvent être exécutées sur n'importe quelle plateforme compatible avec Docker.

Il nous permet d'isoler chaque OpenAM dans son propre conteneur pour réduire les risques de conflits (ex: si OpenAM nécessite Java 11 pour fonctionner et qu'une autre application a besoin de Java 8 dans le même environnement, cela peut être évité).

Il nous permet d'avoir une scalabilité. Si l'environnement grandit en nombre d'utilisateurs, on peut ajouter des conteneurs Docker car il sont bien plus légers que des machines virtuelles et on peut gérer ces conteneurs avec Docker Compose ou Kubernetes.

Docker permet de créer des environnements isolés, reproductibles et faciles à gérer permettant des test rapide des nouvelles versions ou configurations sans affecter le système de production.

3. Quelle est la différence entre un utilisateur et un rôle dans OpenAM ?

Les rôles et les utilisateurs sont distincts mais complémentaires.

Un utilisateur représente une entité individuelle (ex: employé, client, admin), chaque utilisateur possède un id unique, des informations personnelles (mot de passe, attributs...) et les utilisateurs sont authentifiés par OpenAM pour accéder à des ressources.

Un rôle est un ensemble de permissions/d'autorisations regroupées sous une étiquette qui définit ce que les utilisateurs ayant ce rôle sont autorisés à faire dans le système. Les rôles permettent la simplification de la gestion des accès en attribuant des droits à des groupes d'utilisateurs plutôt qu'à des individus, géré laborieusement un à la fois.

4. Quel est l'avantage d'intégrer un annuaire LDAP avec OpenAM ?

Cela permet de centraliser et de gérer efficacement plusieurs utilisateurs, incluant leurs rôles et permissions. OpenAM se connecte directement à LDAP pour gérer l'authentification, ce qui simplifie la gestion et améliore la sécurité, en plus d'offrir une meilleure intégration avec de multiples systèmes d'entreprise et une synchronisation facile des données.

5. Comment activer le Single Sign-On (SSO) avec OpenAM ?

1. Allez dans Federation → SAML Configuration.

- Aller dans Configuration SAMLv2 Provider

2. Ajoutez un fournisseur de services (SP) et un fournisseur d'identité (IdP).

- Aller dans Create Hosted Identity Provider

- Configurer le Circle of Trust

Configure puis,

- Aller dans Create Hosted Service Provider
- Configurer le New Circle of Trust:
- Entrer l'URL du metadata si possible et faire Configure

6. Pourquoi est-il important d'utiliser HTTPS avec OpenAM ?

Parce que OpenAM traite des informations sensibles telles que des identifiants d'utilisateurs, il est donc nécessaire que la connexion soit encryptée afin de ne pas se faire voler ces données par attaque MITM par exemple.

7. Quels sont les principaux paramètres d'une politique de mot de passe sécurisée ?

- Une politique de mot de passe sécurisée repose sur plusieurs paramètres essentiels. Tout d'abord, la longueur minimale doit être d'au moins 12 à 16 caractères afin de limiter les attaques par force brute. La complexité est également primordiale : un mot de passe doit inclure des majuscules, des minuscules, des chiffres et des caractères spéciaux, tout en évitant les mots du dictionnaire et les suites évidentes. Il est recommandé de vérifier les mots de passe contre des bases de données de fuites connues et d'utiliser un algorithme de hachage robuste (comme bcrypt ou Argon2) pour leur stockage. Une politique efficace inclut également un verrouillage temporaire après plusieurs tentatives de connexion échouées afin de prévenir les attaques par essai systématique. L'utilisation d'un gestionnaire de mots de passe est encouragée pour éviter la réutilisation de mots de passe

faibles. Enfin, l'authentification multi-facteurs (MFA) constitue une protection supplémentaire en exigeant un second facteur d'identification, comme un code OTP ou un second appareil, comme un téléphone. Ces mesures combinées renforcent la sécurité des accès et limitent les risques de compromission.

8. Quelles sont les étapes pour créer un nouvel utilisateur dans OpenAM ?

- Dans le menu de gauche, sélectionnez mon-realm → Subjects → Users.
- Créez un utilisateur

New User

* ID:

First Name:	<input type="text" value="Yuri"/>
* Last Name:	<input type="text" value="Markov"/>
* Full Name:	<input type="text" value="Yuri Markov"/>
* Password:	<input type="password" value="....."/>
* Password (confirm):	<input type="password" value="....."/>
* User Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive

9. Comment vérifier que OpenAM est bien en cours d'exécution après son installation ?

- Vous pouvez essayer d'accéder OpenAM au <http://localhost:8080/openam>

10. Quels sont les avantages d'une solution IAM comme OpenAM pour une entreprise ?

- Elle permet une authentification centralisée et une gestion unifiée des identités, réduisant ainsi les risques liés aux mots de passe faibles ou réutilisés. Grâce à ses fonctionnalités de SSO, les utilisateurs peuvent accéder à plusieurs applications avec une seule authentification, améliorant la productivité et réduisant le nombre de demandes de réinitialisation de mot de passe. OpenAM prend également en charge l'authentification multi-facteurs, renforçant la protection contre les accès non autorisés. De plus, il facilite la mise en conformité avec les réglementations en matière de cybersécurité grâce à des journaux d'audit détaillés. De plus, étant une solution open-source, OpenAM offre une flexibilité et une personnalisation avancées tout en réduisant les coûts liés aux licences de solutions propriétaires.