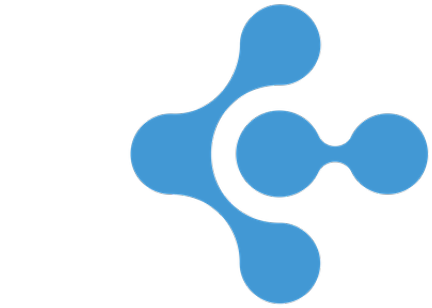


cockpit
IT Service Manager

Administration - Services d'authentification

Document FAQ

Table des matières

Introduction 3
I.Objectif 3
II.Définitions 3
Azure AD 4
I.Configuration du serveur Azure AD 4
II.Configuration de Cockpit IT Service Manager 9
Configuration LDAP 10
I.Configuration du serveur LDAP 10
II.Configuration de Cockpit IT Service Manager 11
A.Ajout du serveur 11
B.Test de connexion 12
Configuration Google 13
I.Configuration SSO Google 13
II.Configuration de Cockpit IT Service Manager 15
Cockpit 16
Administration 17
I.Paramétrer les modes de connexions des utilisateurs 17
A.Fonctionnement du menu 17
B.Fonctionnement connexion SSO 17
II.Droits des utilisateurs 17

Introduction

I. Objectif

Le but du document est de présenter le fonctionnement et la configuration des différents types de connexion à Cockpit IT Service Manager.

II. Définitions

SSO (Single Sign-On) : Permet aux utilisateurs d'accéder directement à Cockpit IT Service Manager lorsqu'ils sont déjà authentifiés auprès d'une application tierce se chargeant de la vérification de l'identité (exemples : Google, Azure AD, etc.).

LDAP : Permet de se connecter à Cockpit IT Service Manager via des utilisateurs gérés par un annuaire externe à Cockpit (exemples : openLDAP, ActiveDirectory, etc.).

Azure AD

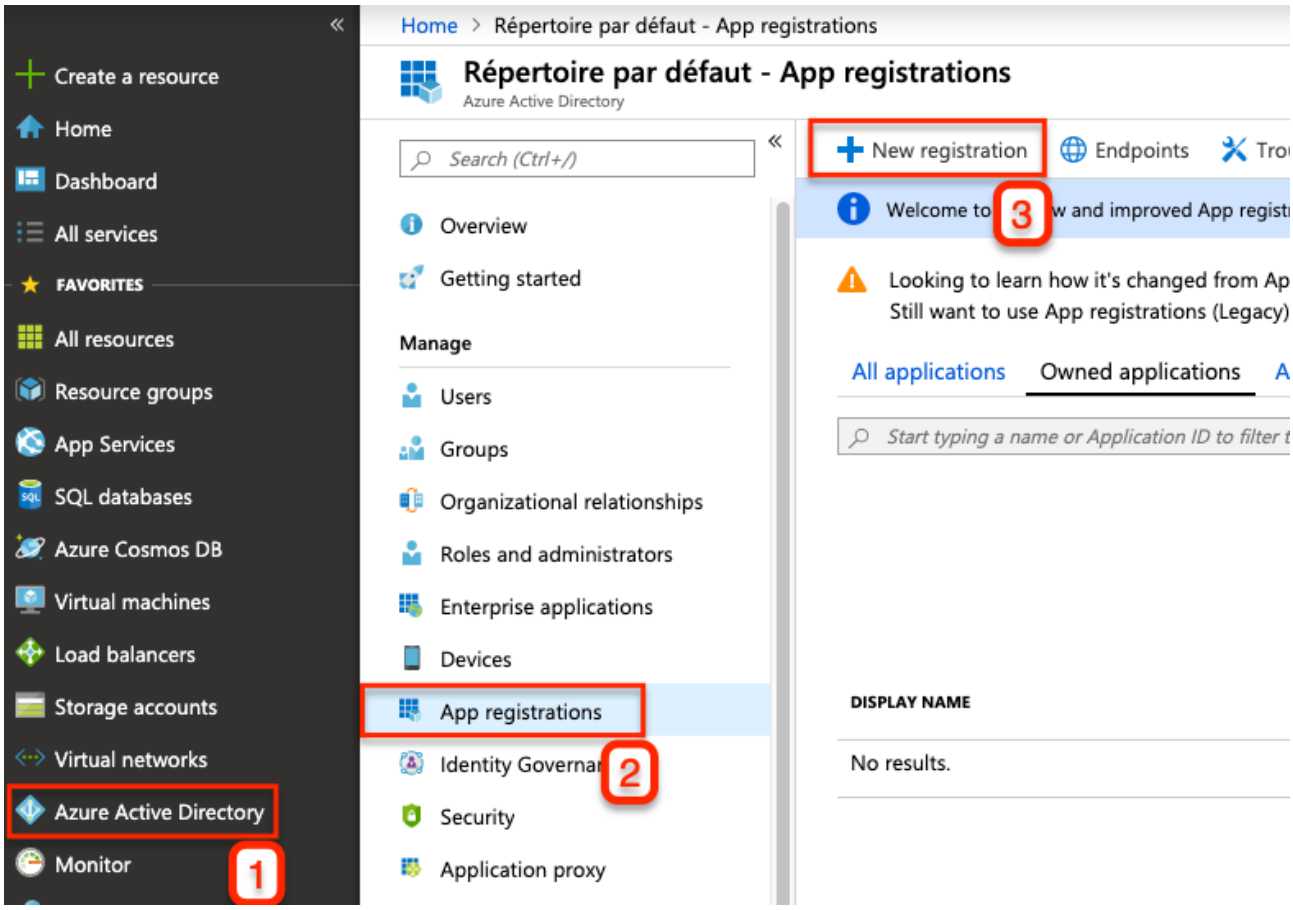
Objectif : Permettre aux utilisateurs connectés à leur portail Azure AD d'accéder directement au portail Cockpit IT Service Manager.

> Important : Un seul service d'authentification de type Azure AD peut être créé.

I. Configuration du serveur Azure AD

1. Créer une application

Depuis le portail Microsoft Azure AD aller dans « Azure Active Directory » puis cliquer sur « Inscriptions des applications », cliquer sur « Nouvelle inscription d'application » :



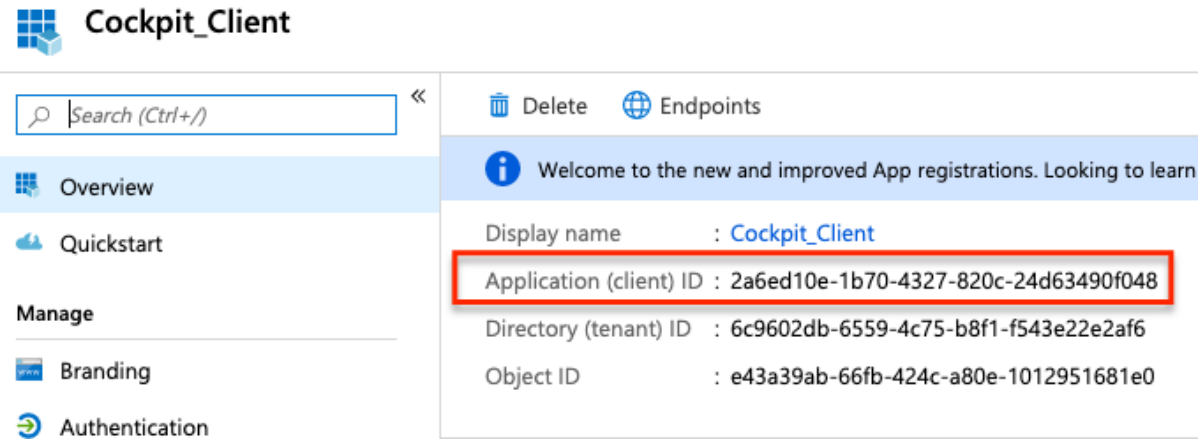
Renseigner les champs suivants :

- Nom : Cockpit_Client (texte libre)
- Supported account types : Sélectionner le type de compte adéquat. Dans la plupart des cas « Accounts in this organizational directory only »

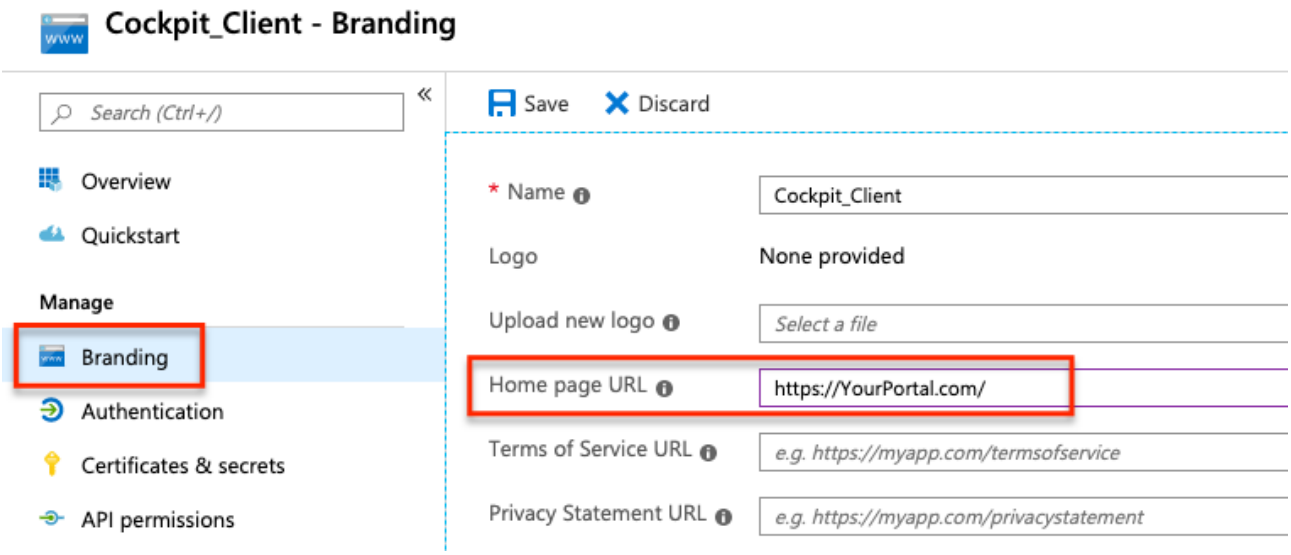
Cliquer sur « Register ».

2. Configurer l'application

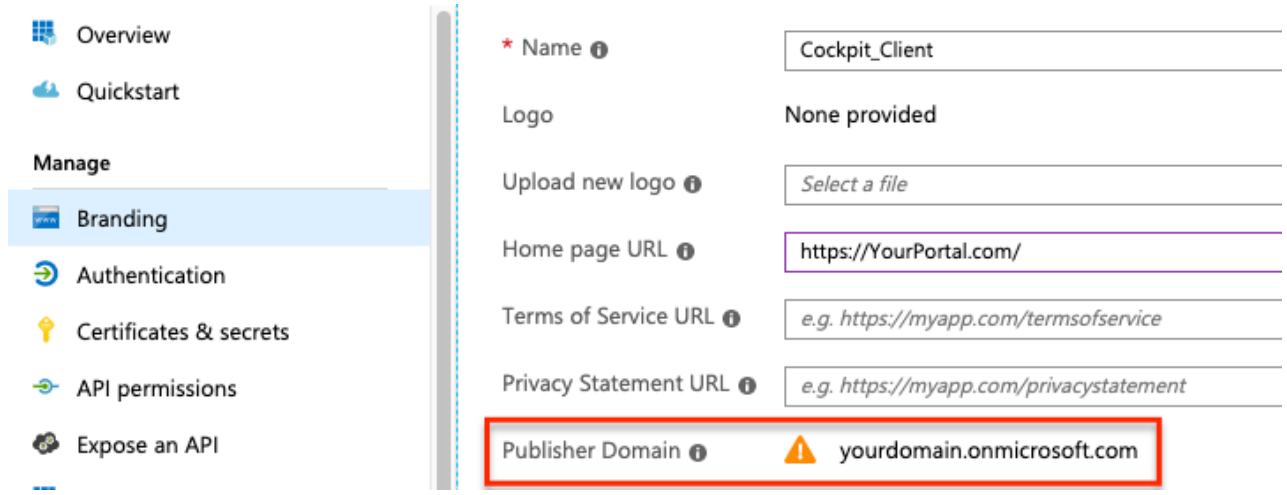
Cliquer sur l'application, relever le contenu du champ « Application (client) ID » qui sera utiliser dans le paramétrage de Cockpit IT Service Manager :



Puis aller dans le menu « Manage > Branding » et renseigner le champ « Home page URL » avec l'URL de votre portail :

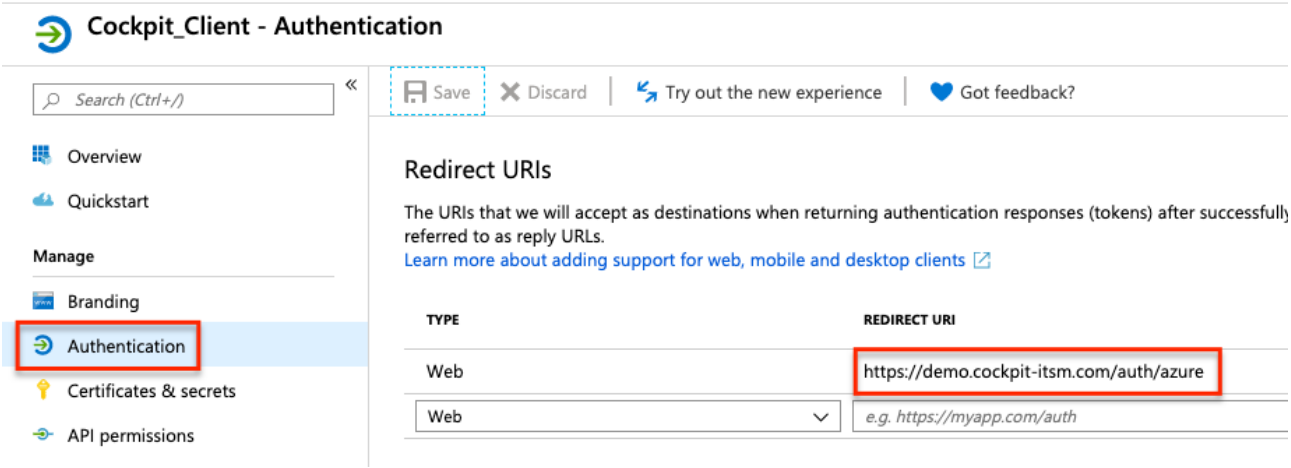


Toujours dans le menu « Manage > Branding », relever la valeur du champ « Publisher Domain », il pourra être demandé dans la partie Cockpit ITSM de la configuration :



Cliquer sur « Sauvegarder ».

Aller ensuite dans le menu « Manage > Authentication » et renseigner un champ « Redirect URIs » avec l'URL de votre portail au format suivant : « https://yourportal.cockpit-itsm.com/auth/azure »



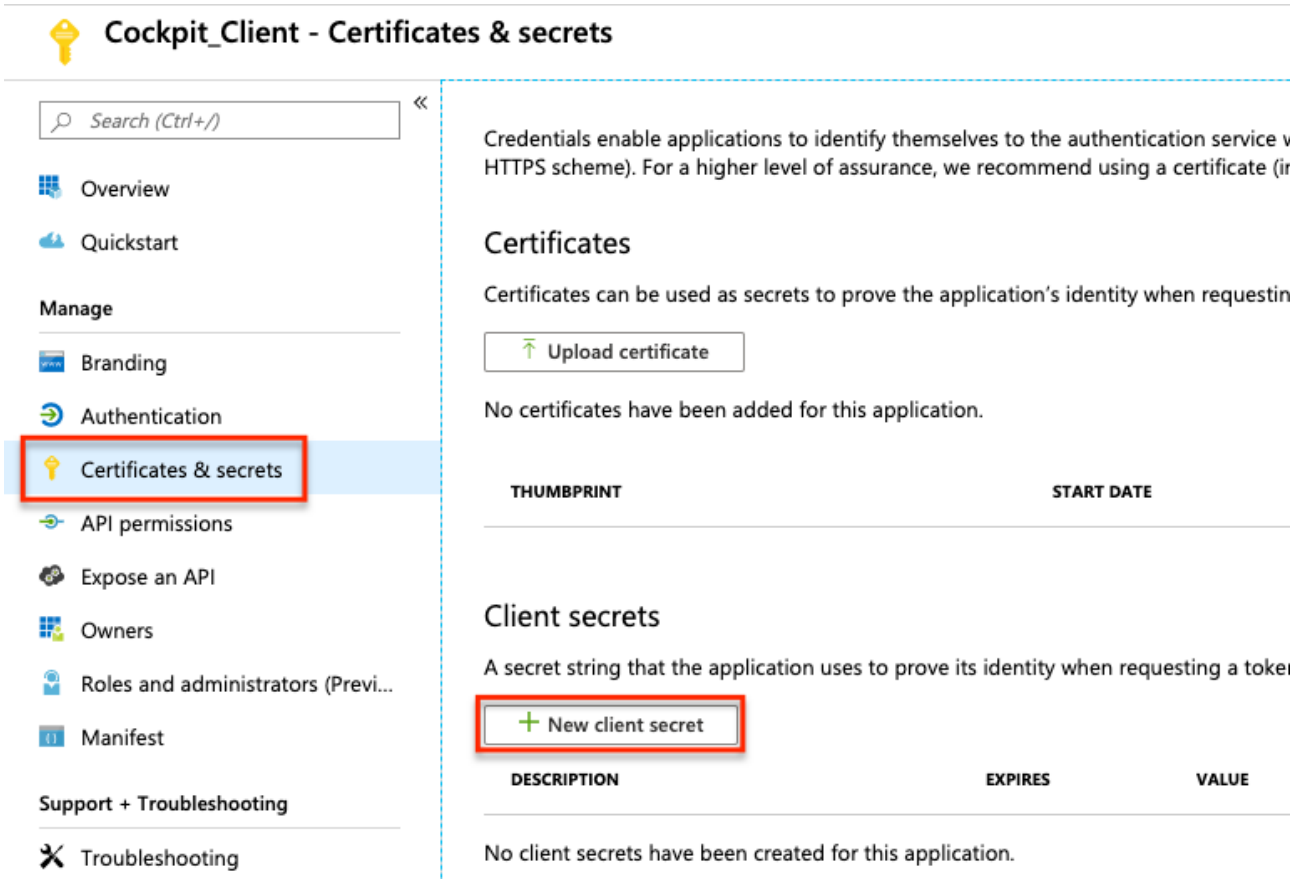
Dans la partie « Advanced settings » de ce menu, paramétrer la partie « Supported account types » en sélectionnant une des options ci-dessous :

- « Accounts in this organizational directory only (*Your AD Directory* only – Single tenant) » : Seuls les utilisateurs se trouvant dans l'Azure AD peuvent se connecter à l'application
- « Accounts in any organizational directory (Any Azure AD directory – Multitenant) » : Vous autorisez les utilisateurs d'autres Azure AD à se connecter à l'application

> Important : Selon l'option choisie le paramétrage côté Cockpit IT Service Manager sera différent.

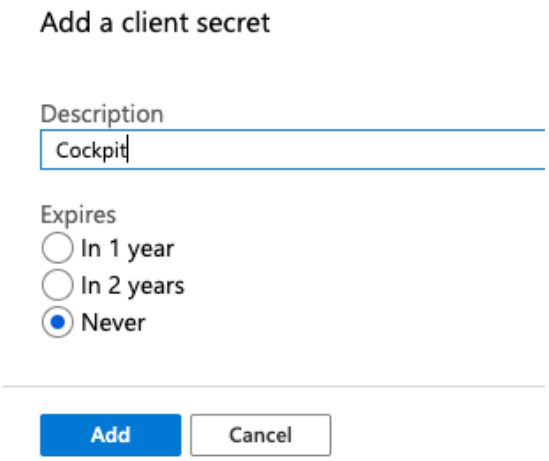
Cliquer sur « Sauvegarder ».

Aller ensuite dans le menu « Manage > Certificates & Secrets », ajouter un secret client en cliquant sur « New client secret » :

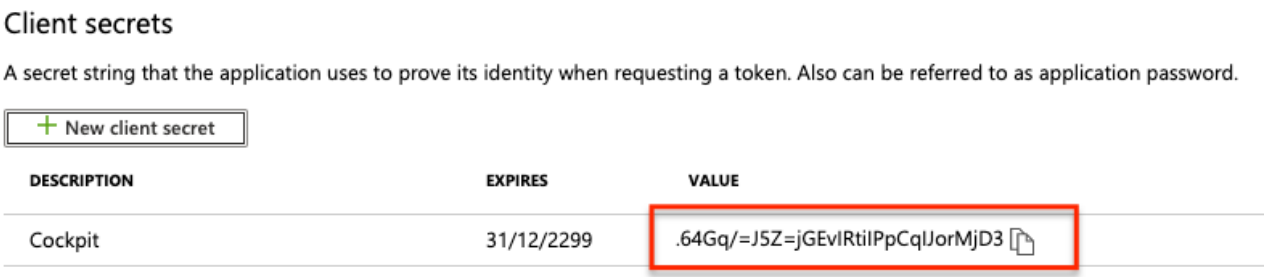


Renseigner les éléments suivants :

- Description : texte libre
- Expire : Jamais



Le secret client apparaît, relever le champ « Value », il sera demandé lors de la configuration côté portail Cockpit ITSM :



> Important: Il faut conserver le secret client car il sera demandé dans la configuration côté Cockpit IT Service Manager et ne sera plus visible en clair dans Azure AD. Il est toutefois possible d'en créer un autre en cas de besoin.

II. Configuration de Cockpit IT Service Manager

Menu : Administration > Connectivité > Authentification

Cliquer sur « Nouveau », renseigner les éléments suivants :

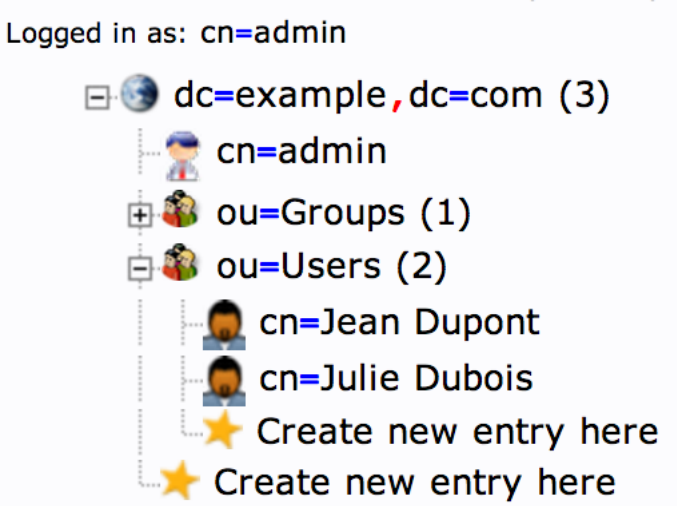
Champs	Valeurs
Type	Azure AD
Nom	Description du service d'authentification
Statut	Actif / Inactif Quand le statut est inactif la connexion via le service n'est plus possible ni proposée
Client	Ce champ fait référence à ce qui a été renseigné dans la partie « Supported account types » du menu « Manage > Branding ». Option « Accounts in this organizational directory only (*Your AD Directory* only – Single tenant) : indiquer le nom de votre tenant relevé précédemment (valeur du champ « Publisher Domain ») : « VotreNom.onmicrosoft.com » Option « Accounts in any organizational directory (Any Azure AD directory - Multitenant » : indiquer « common »
ID client	ID de l'application Depuis le portail Azure AD aller dans le menu « Azure Active Directory », cliquer sur « App registrations », relever « Application (client) ID » dans l'application créée pour Cockpit IT Service Manager.
Clé client	ID Clé client Indiquer le secret client relevé pendant la configuration du serveur Azure AD.

Configuration LDAP

I. Configuration du serveur LDAP

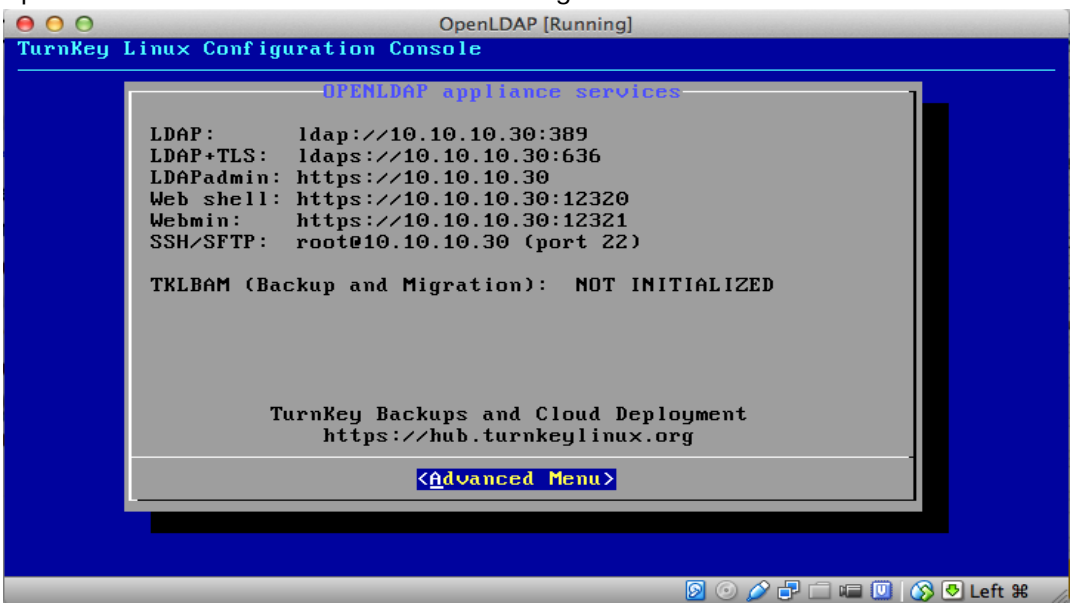
Les captures d'écran proviennent d'une installation « openLDAP » de test, mise à disposition par Turnkey linux.

La racine est « example.com » et les utilisateurs sont placés dans une unité organisationnelle (OU) nommée « Users » :



Chaque utilisateur possède pour « uid » son login Koaly EXP.

Le serveur possède l'adresse IP 10.10.10.30 et est configuré comme suit :



II. Configuration de Cockpit IT Service Manager

A. Ajout du serveur

1. Détail des éléments de configuration

Modèle	La valeur choisie permet de pré-remplir la configuration avec les valeurs standard mais n'influence pas la connexion au serveur
Description	Texte libre permettant d'identifier le serveur
Serveur	Adresse IP ou nom d'hôte utilisé pour se connecter au serveur
Port	Port pour se connecter au serveur (les valeurs par défaut sont : 389 pour le port non sécurisé et 636 pour le port sécurisé)
Encryptage	À cocher si la connexion est sécurisée
Base DN	Il s'agit de l'identification du nœud racine
Format de principal	Il s'agit du format utilisé pour atteindre un nœud d'un utilisateur
Attribut utilisateur	Il s'agit du nom de l'attribut LDAP que porte l'objet utilisateur et qui sera comparé au login Koaly EXP
Pool de serveurs	Permet d'indiquer le nom d'un groupe de serveurs de sorte à assurer une disponibilité accrue (en cas d'indisponibilité d'un serveur, si ce dernier fait partie d'un groupe, l'application tente de se connecter à un second serveur du groupe)

2. Cas d'exemple

Quelques remarques sur les valeurs utilisée dans notre cas d'exemple :

Modèle	Autre
Description	Turnkey OpenLDAP
Serveur	10.10.10.30 Le serveur LDAP écoute cette IP)389 (nous utilisons la connexion non sécurisée)
Port	389 Nous utilisons la connexion non sécurisée
Encryptage	Option décochée Nous utilisons la connexion non sécurisée
Base DN	« DC=example,DC=com » La racine du LDAP
Format de principal	« CN=${firstName} ${lastName},DC=domain,DC=local,OU=Users » où « ${firstName} » Nous recherchons les utilisateurs Koaly EXP via une recherche de « CN=${firstName} ${lastName},DC=domain,DC=local,OU=Users » où « ${firstName} » sera remplacé par le prénom de l'utilisateur et « ${lastName} » par son nom de famille.

Attribut utilisateur	uid Dans notre cas (serveur openLDAP), l'identifiant unique de l'utilisateur est porté par l'attribut « uid ». Ainsi, avec cette configuration, une utilisateur Koaly EXP possédant pour pré-nom « Julie », pour nom de famille « Dubois » et pour login « jdubois » pourra se connecter à l'application si : - L'utilisateur peut se connecter au serveur LDAP avec comme identifiant « CN=Julie Dubois,DC=domain,DC=local,OU=Users » son mot de passe Koaly EXP. - L'objet LDAP « CN=Julie Dubois,DC=domain,DC=local,OU=Users » possède un attribut « uid » ayant pour valeur « jdubois ».
Pool de serveurs	Vide

B. Test de connexion

1. Détail des éléments

Pour effectuer un test de connexion de « Julie Dubois », il convient de remplir comme suit :

Principal	Le principal utilisé pour se connecter au serveur LDAP, qu'il faut déduire du « format » de principal de la configuration.
Mot de passe	Mot de passe utilisé pour se connecter au serveur LDAP.
Valeur de l'attribut	Le login Koaly EXP à utiliser pour le test.

2. Cas d'exemple

Pour effectuer un test de connexion de « Julie Dubois », il convient de remplir comme suit :

Principal	CN=Julie Dubois,OU=Users,DC=example,DC=com
Mot de passe	*******
Valeur de l'attribut	jdubois

Configuration Google

Objectif : Permettre aux utilisateurs connectés à leur compte Google d'accéder au portail Cockpit IT Service Manager sans s'authentifier une deuxième fois.

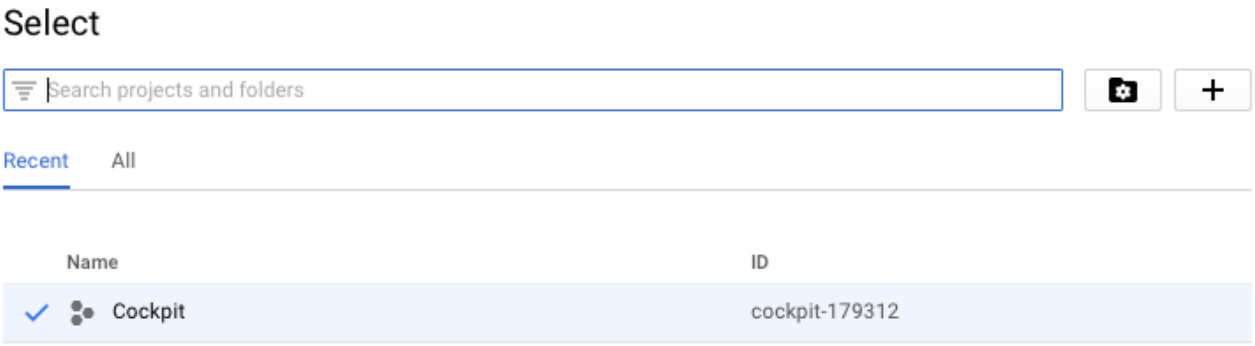
> Important : Un seul service d'authentification de type Google peut être créé.

I. Configuration SSO Google

Aller dans la console de développement Google :

https://console.developers.google.com/

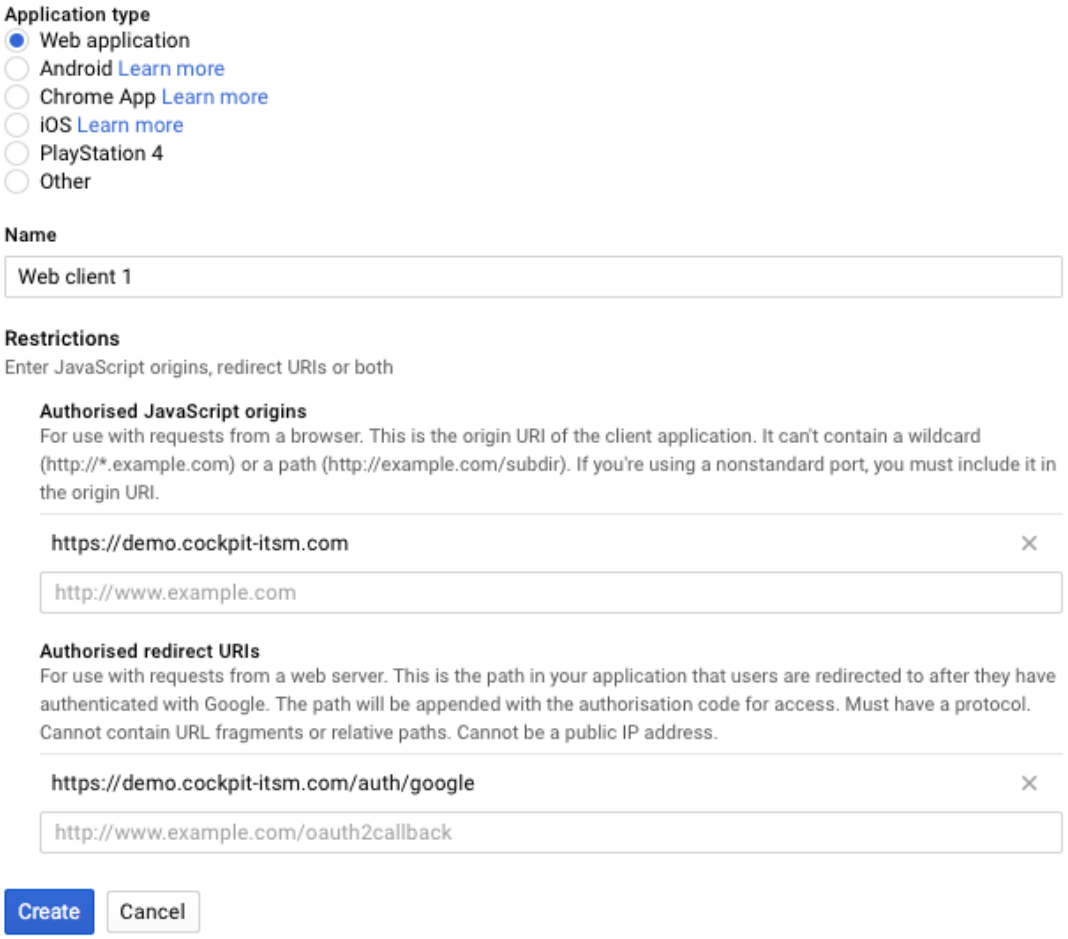
Créer un nouveau projet et le nommer « Cockpit » :



Aller dans le menu « Identifiants », sélectionner le projet « Cockpit » nouvellement créé.

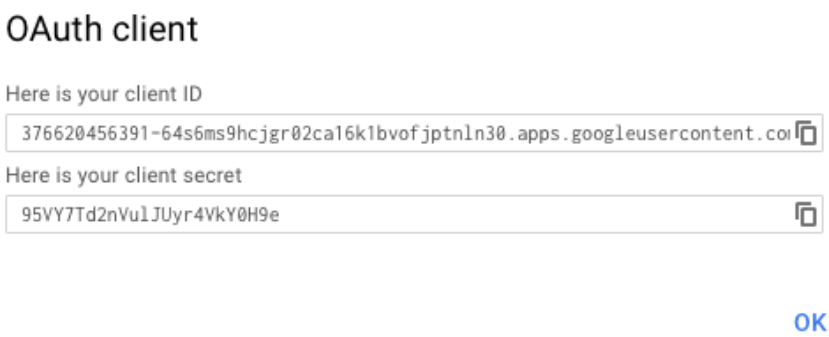
Créer un identifiant de type « ID client OAuth » :

- Type d'application : « Application Web »
- Origines JavaScript autorisées : <URL de base du portail> sans « / » à la fin
  Exemple : https://demo.cockpit-itsm.com
- URI de redirection autorisés : <URL de base du portail>/auth/google sans « / » à la fin
  Exemple : https://demo.cockpit-itsm.com/auth/google



Google renvoie dans une fenêtre popup :

- ID client
- Code secret client



Notez ces 2 éléments qui seront utilisées dans le paramétrage de Cockpit IT Service Manager puis cliquer sur « OK ».

II. Configuration de Cockpit IT Service Manager

Menu : Administration > Paramétrage > Services d'authentification

Cliquer sur « Nouveau », renseigner les éléments suivants :

Champs	Valeurs
Type	Google
Nom	Description du service d'authentification
Statut	Actif / Inactif Quand le statut est inactif la connexion via le service n'est plus possible ni proposée
ID client	ID client assigné au projet Google « Cockpit »
Secret client	Code secret client assigné au projet Google « Cockpit »

Cockpit

Connexion basée sur l'identifiant et le mot de passe de l'utilisateur renseignés dans la fiche de l'utilisateur, ces éléments sont gérés dans Cockpit IT Service Manager par :

- Les administrateurs Cockpit IT Service Manager pour les données personnelles et la politique de sécurité.
- Les utilisateurs pour le mot de passe et l'authentification forte.

I. Paramétrer les modes de connexions des utilisateurs

Objectif : Paramétrer les modes de connexion des utilisateurs

Menu : Administration > Application > Opérateurs / Contacts

A. Fonctionnement du menu

L'administrateur Cockpit IT Service Manager définit le mode de connexion (Cockpit, LDAP ou SSO) pour les utilisateurs (opérateurs ou contacts) :

- Individuellement en éditant un compte utilisateur, aller dans l'onglet « Accès au portail ».
- Massivement depuis la liste des opérateurs / utilisateurs, sélectionner les utilisateurs et cliquer sur le bouton « Modifier ».

B. Fonctionnement connexion SSO

Quand un mode de connexion de type SSO est sélectionné :

- Un email avec un lien est automatiquement envoyés aux utilisateurs, les utilisateurs doivent cliquer sur le lien pour valider leur connexion SSO. Le lien est valable 24 heures.
  L'email utilisé est celui renseigné dans les fiches utilisateurs.
- Dans les menus listant les Opérateurs / Contacts, le champ « Authentification » indique « Google / Azure – En cours de validation » et le champ « Utilisateur » est vide tant que l'utilisateur n'a pas validé sa connexion.
- Quand vous modifiez massivement le mode de connexion SSO des utilisateurs pour revenir au mode « Cockpit » ou « LDAP » le champ « Identifiant » est automatiquement composé avec les prénoms et noms de l'utilisateur : « Prénom Nom ».
  Un mot de passe est demandé et sera appliqué à tous les utilisateurs.
- Si vous éditez unitairement une fiche utilisateur pour affecter un mode de connexion de type « Cockpit » vous pouvez renseigner l'identifiant et le mot de passe.

II. Droits des utilisateurs

Objectif : Définir les droits des utilisateurs

Menu : Administration > Application > Profils opérateurs / Profils contacts

Fonctionnement : Dans les profils, onglet « Paramètres », il est possible de bloquer ou de donner la possibilité à l'utilisateur de choisir son mode de connexion.

Fin du document