Applicatif / Langage

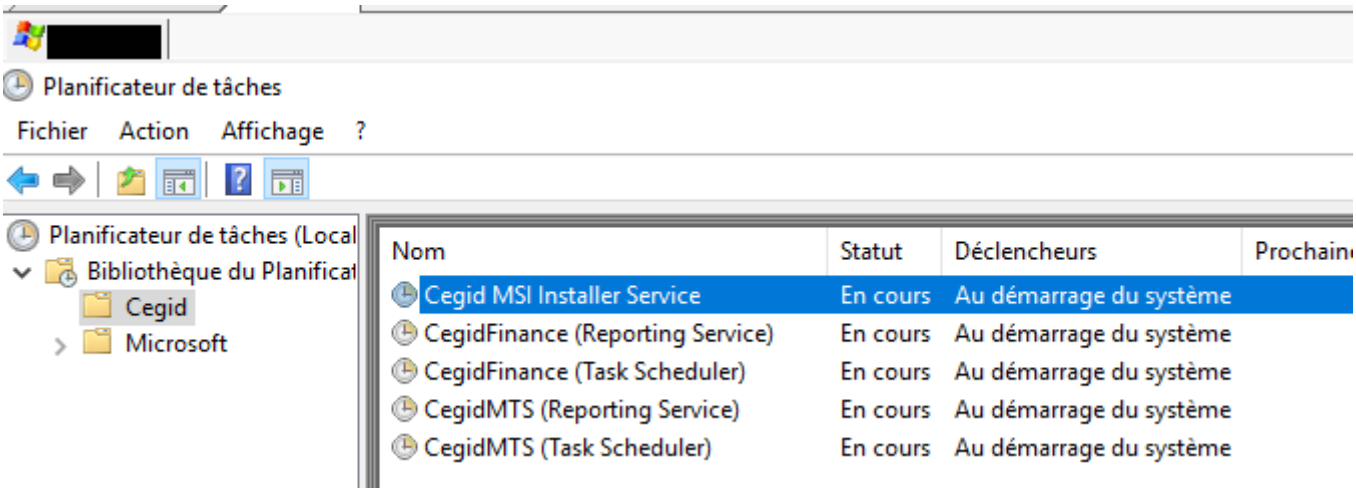
- Applications
  - CEGID Y2 notes d'Incident
- BASTION
  - Incident - Session Probe Drive of Session Probe is not ready yet
  - Bastion TMA
  - Incident - TLS CERTIFICATE CHANGED
- CITRIX
  - Ajouter une application depuis Citrix Cloud
  - Citrix AppCenter
- Supervision
  - Elastic Search Installation
- WEB
  - Clear Cache REDIS
  - Varnish clean cache
  - Error PHP
  - PHP-FPM

Applications

Applications

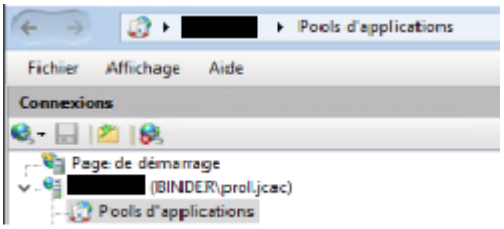
CEGID Y2 notes d'Incident

En cas d'incident CEGID où plusieurs modules ne fonctionnent pas comme attendu il faut procéder à la vérification ci-dessous:
Les tâches planifiées CEGID doivent être 'en cours d'exécution' sur le SRVY2RT :

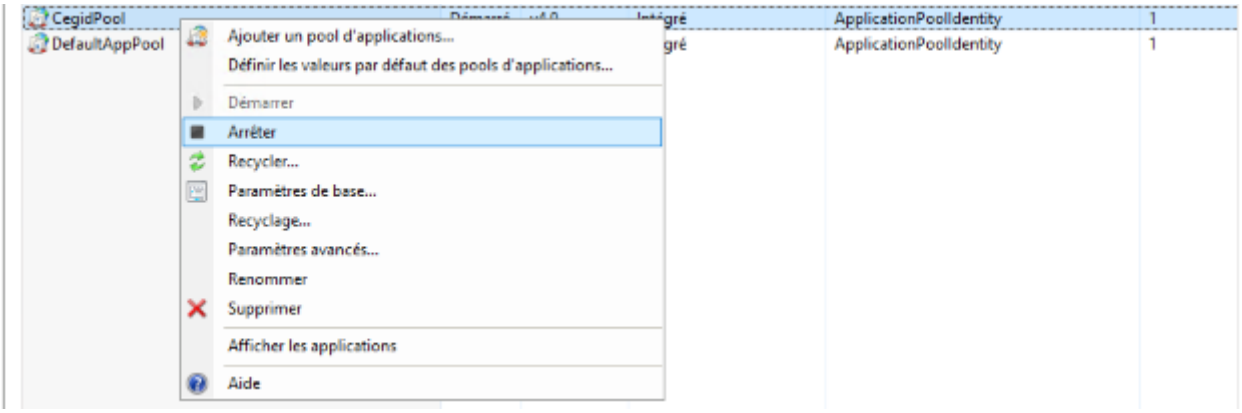


Si ce n'est pas le cas, il faut les démarrer manuellement.
Elles doivent rester "en cours"

En cas d'incident CEGID, Si aucun utilisateur arrive à se connecter veuillez en premier lieu reset l'application POOL dans IIS : Ouvrir IIS > clique Pools Application



Aller sur CegidPool > Clique droit > Arrêter > Démarrer

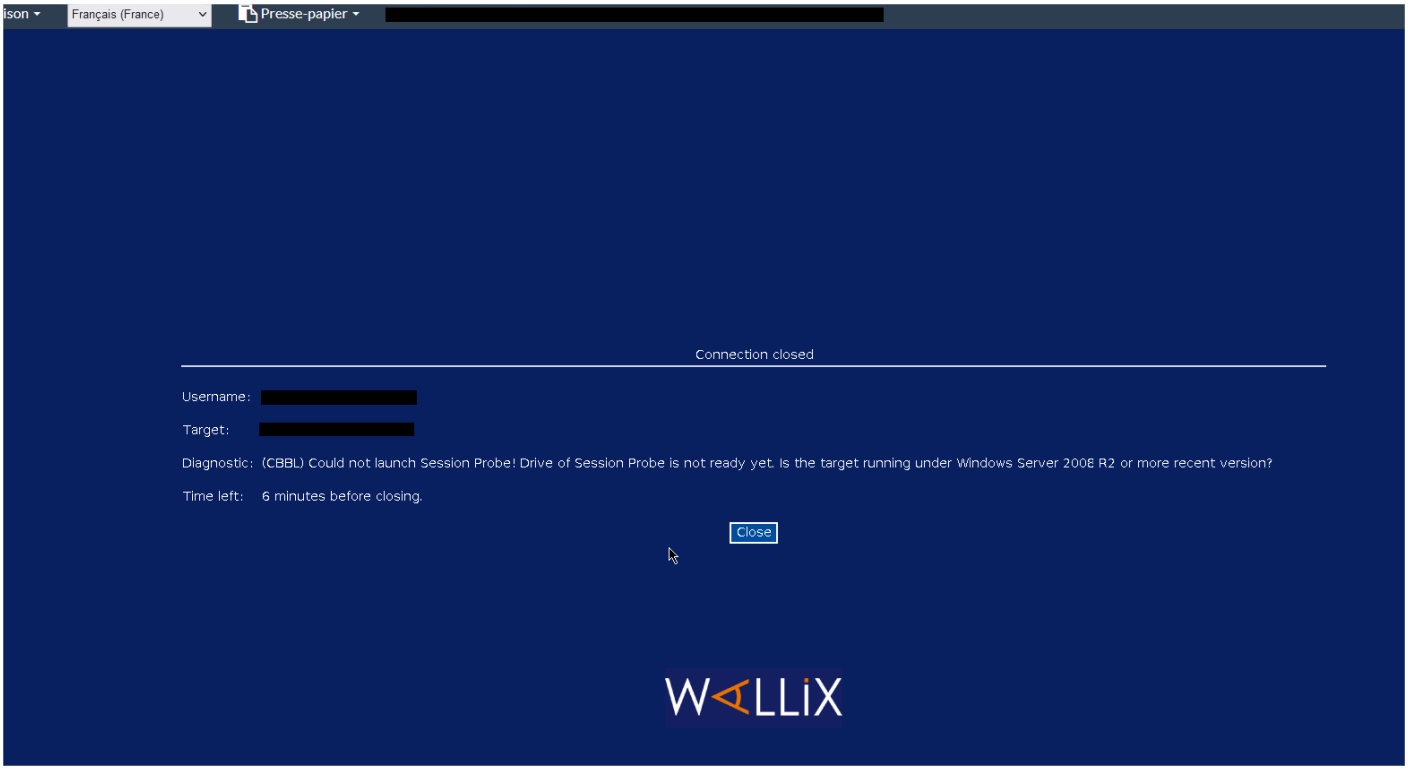


demander au client si les users peuvent se reconnecter

BASTION

BASTION

Incident - Session Probe Drive of Session Probe is not ready yet



Erreur dans les logs :

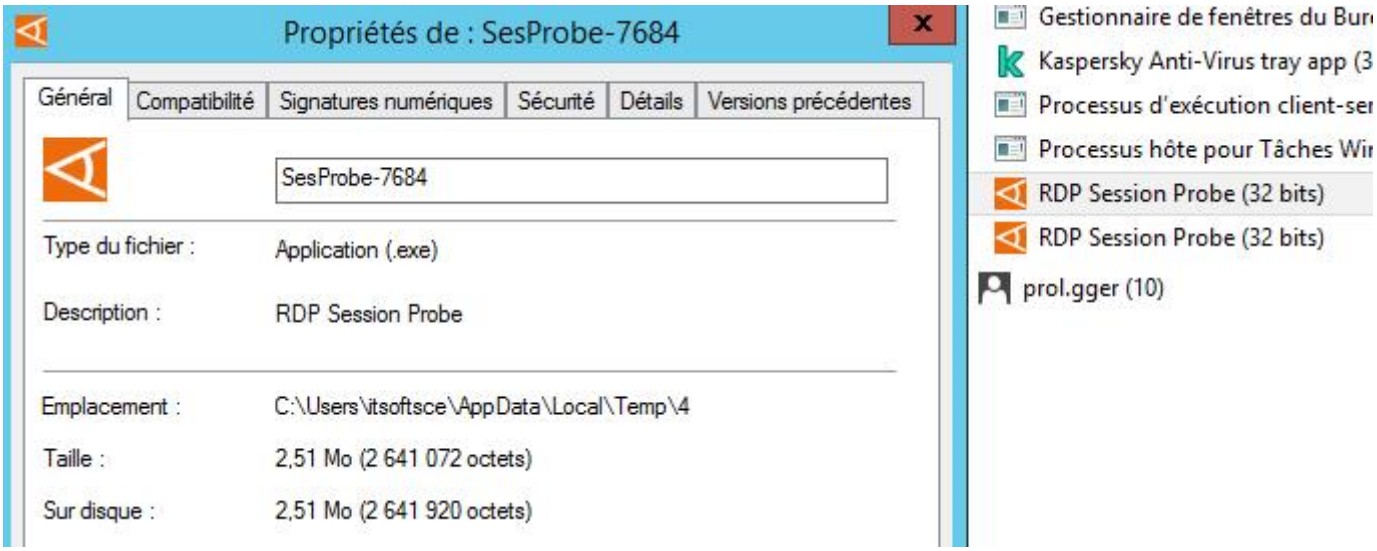
> Aug 25 13:27:37 bastion1 rdpproxy[24076]: ERR (24076/24076) -- SessionProbeClipboardBasedLauncher :=> Drive of Session Probe is not ready yet. Is the target running under Windows Server 2008 R2 or more recent version?

> Aug 25 13:27:37 bastion1 rdpproxy[24076]: ERR (24076/24076) -- SessionProbeVirtualChannel::process_event_launch: Session Probe is not ready yet!

Pour l'erreur lié à la Session Probe, il y'avait une session "fantôme" itsoftsce en doublon avec peu 5 processus ouverts.
J'ai juste déconnecter l'utilisateur puis je me suis reconnecté depuis l'accès manager sans

problème.

Quand, la session est ouverte depuis l'accès manager, cela ouvre deux processus SesProbe pour la session en cours comme sur la capture d'écran :



Note depuis le guide d'administration :

The session probe is loaded by a batch script. Without WALLIX Bastion, this script will cause the display of a non-user friendly black console window in the RDP session.
Moreover, the user may interact with it and disrupt the loading process.

Enabling the launch mask can block the display as well as mouse and keyboard inputs during the loading of the session probe loading phase. As a consequence, the console window becomes invisible.

redirection of clipboard must be enabled by Terminal Services to be able to use the smart launcher (this is enabled by default).

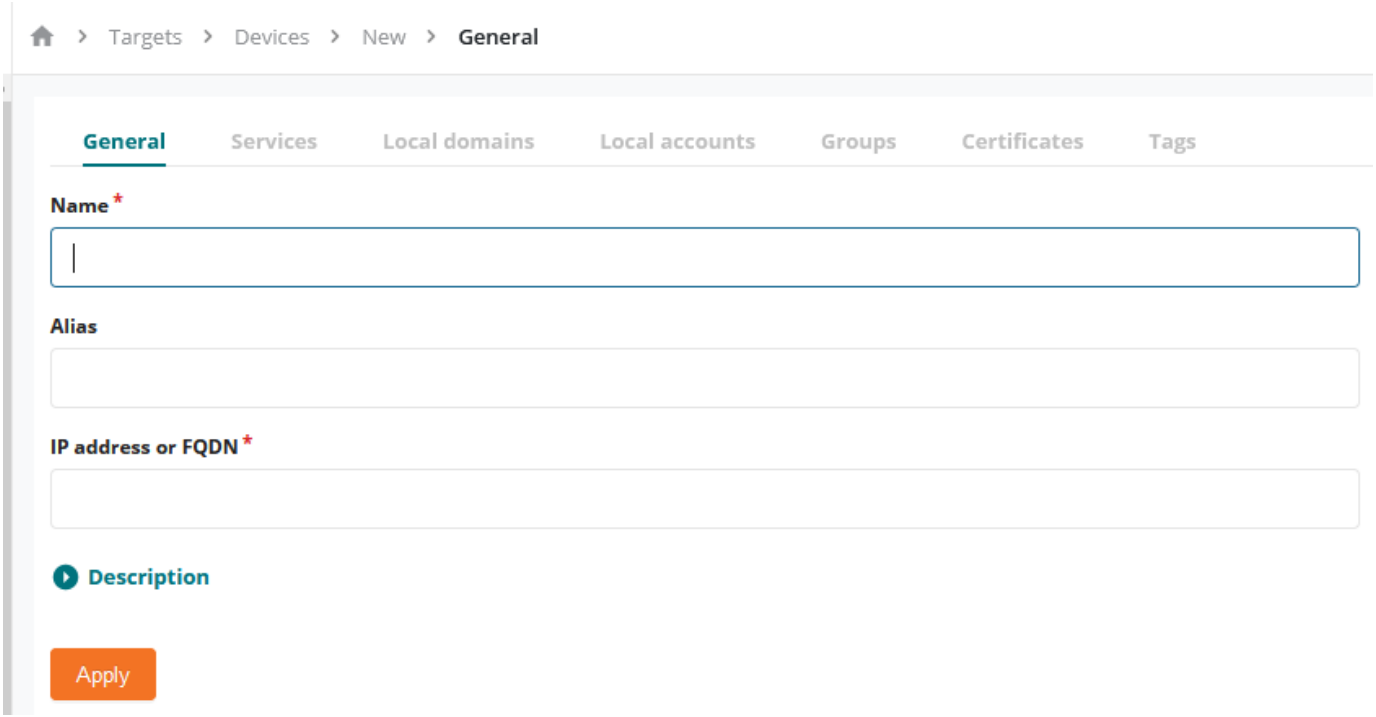
BASTION

Bastion TMA

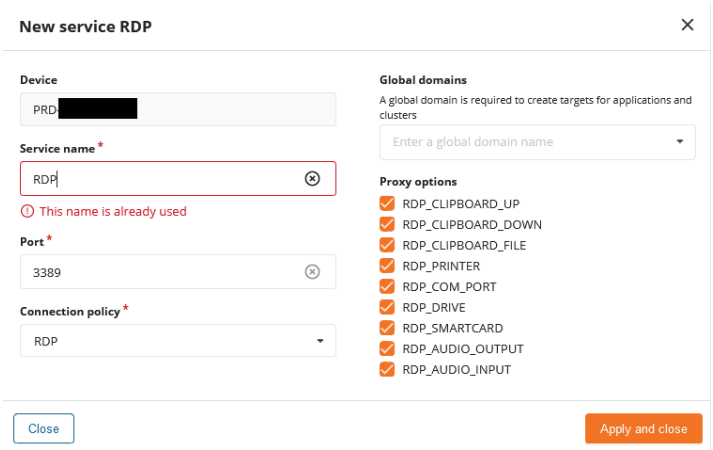
Interface d'admin :

Ajout des accès à des users à des serveurs non existants dans le bastion.

Ajout des serveurs:
Targets --> Devices --> Add



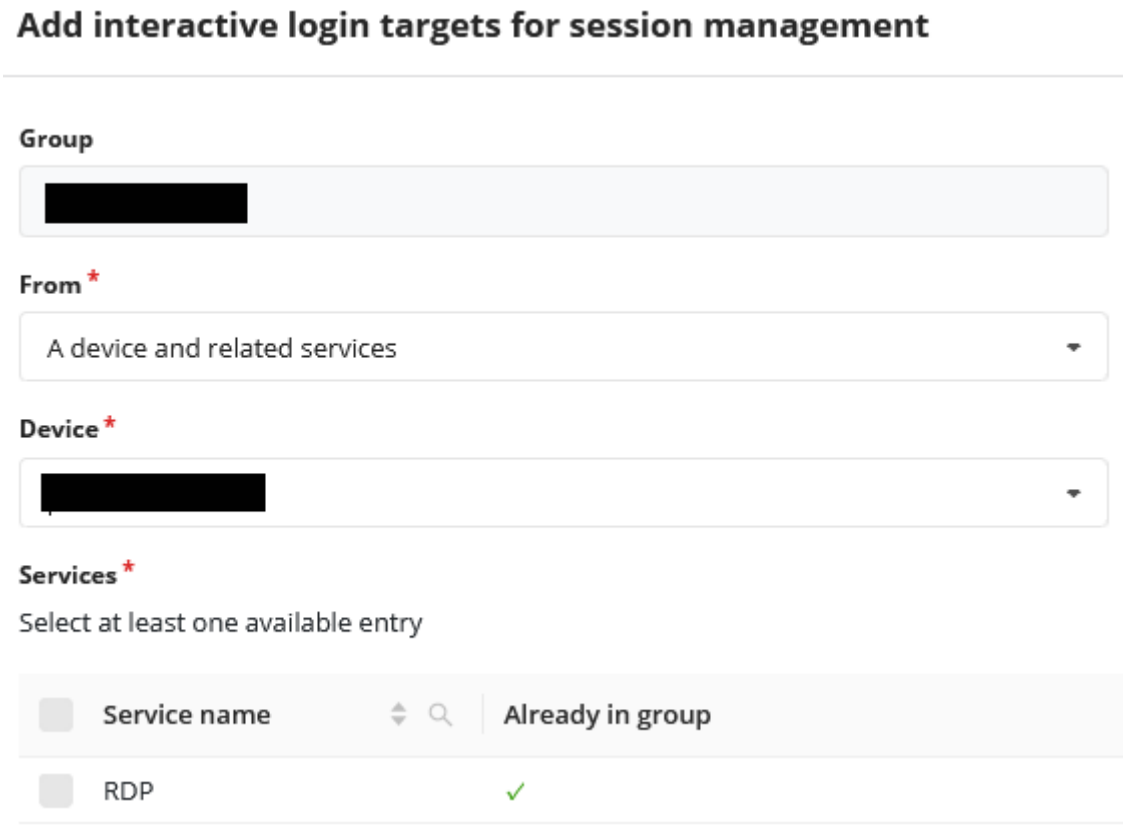
Mettre le nom du serveur et son IP puis cliquer sur apply.
Ensuite aller sur l'onglet services et cliquer sur ADD puis RDP pour serveurs Windows (SSH pour serveurs Linux)



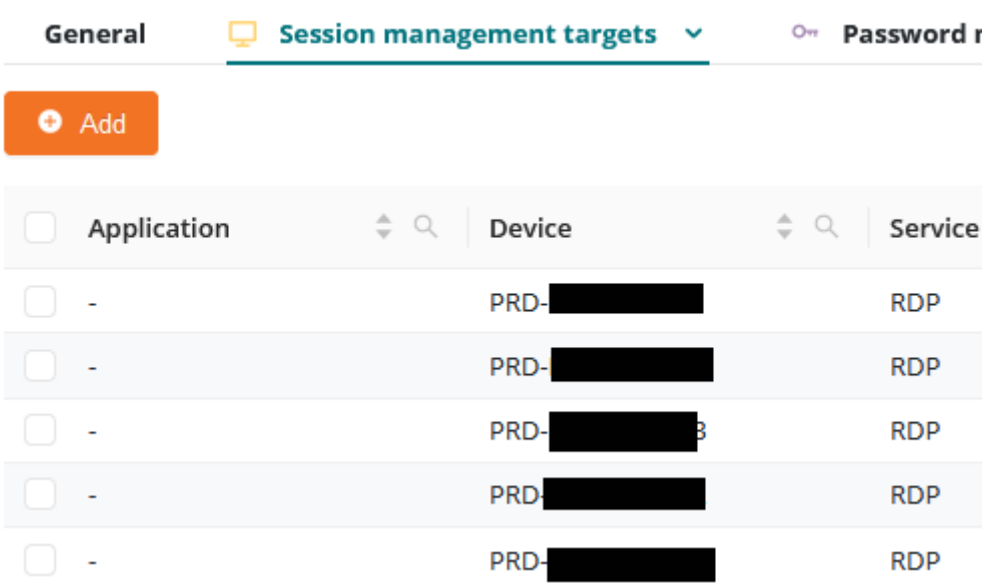
Faire apply and close. Ne pas prendre en compte l'erreur dans la PJ. La conf est déjà en place pour le serveur.

Création groupe de device :
Se rendre dans Targets --> Groups --> Add
Lui donner un nom puis apply

Aller sur l'onglet Session Management Targets puis interactive login:

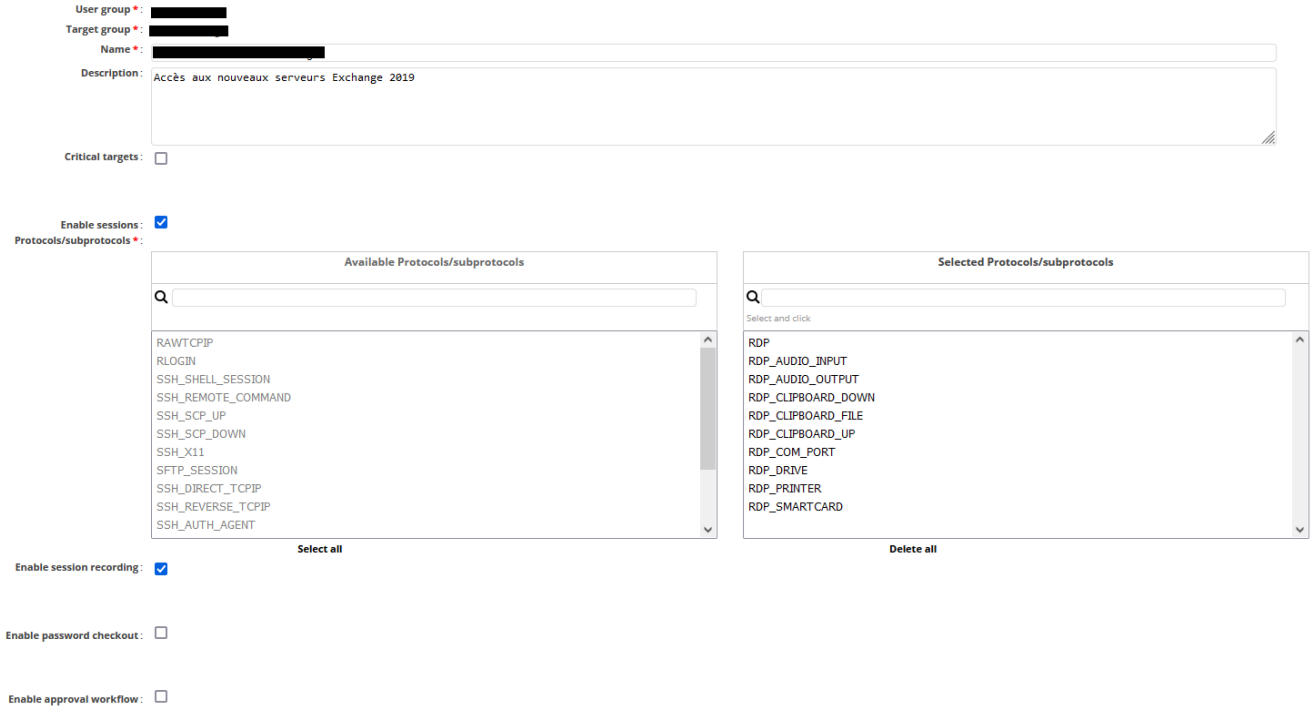


Penser à cocher RDP à chaque fois pour tous les serveurs.
Résultat final:



Attribution des accès aux users:

Aller dans Authorizations --> Manage authorizations --> + Add an autorisation



Demander de tester les accès.
Attention il faut que le port RDP 3389 soit ouvert entre les serveurs et le bastion TMA.

BASTION

Incident - TLS CERTIFICATE CHANGED

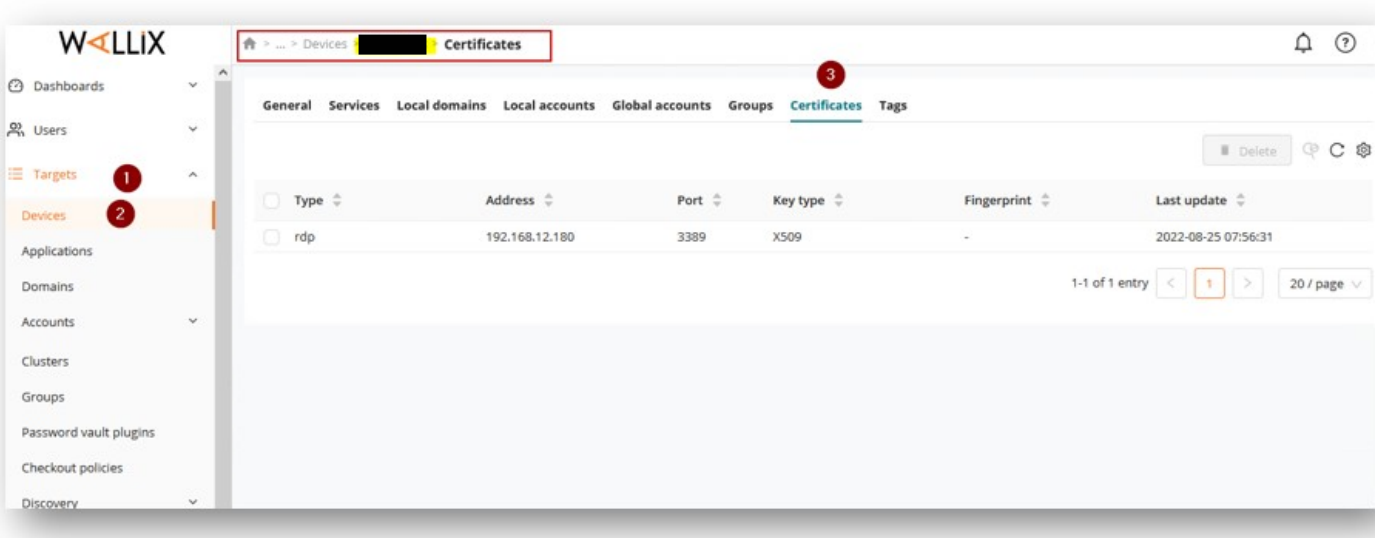
Type d'erreur :



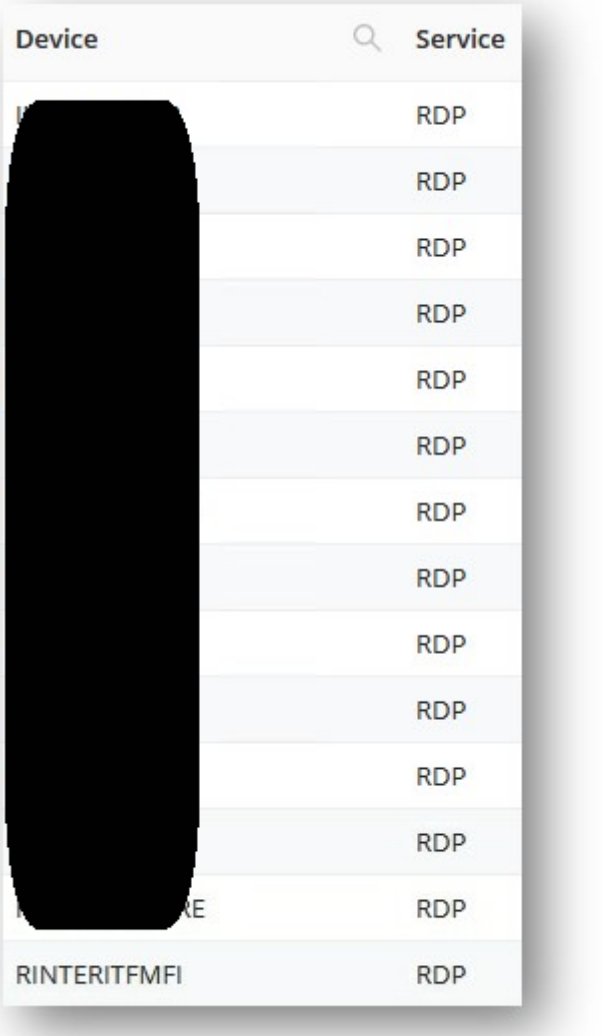
Suite à nos investigations et à l’appel auprès du support Wallix, les erreurs TLS_CERTIFICATE_CHANGED surviennent lorsque le serveur cible renouvelle son certificat de bureau à distance (RDP).
Le bastion ne remplace pas le certificat obsolète existant par le nouveau de la machine cible.

Le renouvellement est possible en supprimant en premier lieu le certificat dans le bastion et se reconnecter au serveur cible depuis l’accès utilisateur pour que le bastion récupère le nouveau certificat.
Il n’y a pas de réplication pour cette partie du certificat RDP pour la machine cible donc l’action de renouvellement du certificat RDP doit être effectuée sur les deux bastions.

Note : Les certificats sont stockés localement sur les bastions à l’emplacement : /var/wab/cert/

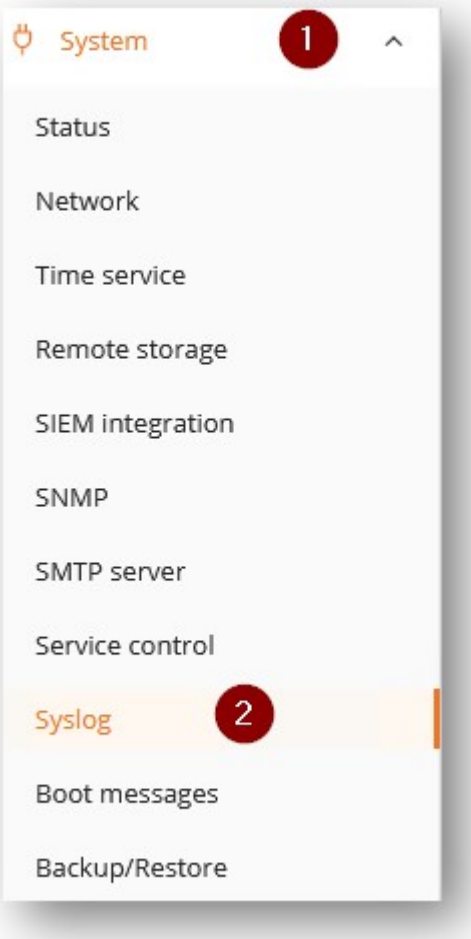


J’ai vérifié et renouvelé sur les deux bastions lorsque cela a été nécessaire pour toutes les machines cibles du groupe AUTORISATION :



La connexion devrait être possible désormais pour les utilisateurs et le message

TLS_CERTIFICATE_CHANGED ne devrait plus apparaître.
En complément, les détails de l’erreur apparaissent dans les logs du bastion dans System\Syslog.



Exemple de l’erreur :

Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- SSL_get_peer_certificate()
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate directory is: '/var/wab/cert/18074c309afb7897005056a2a787'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate file is: '/var/wab/cert/18074c309afb7897005056a2a787/rdp,192.168.12.100,3389,X509.pem'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- nb1=1107 nb2=1107
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509 existing::issuer=CN = INTER
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509 existing::subject=CN = INTER
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509

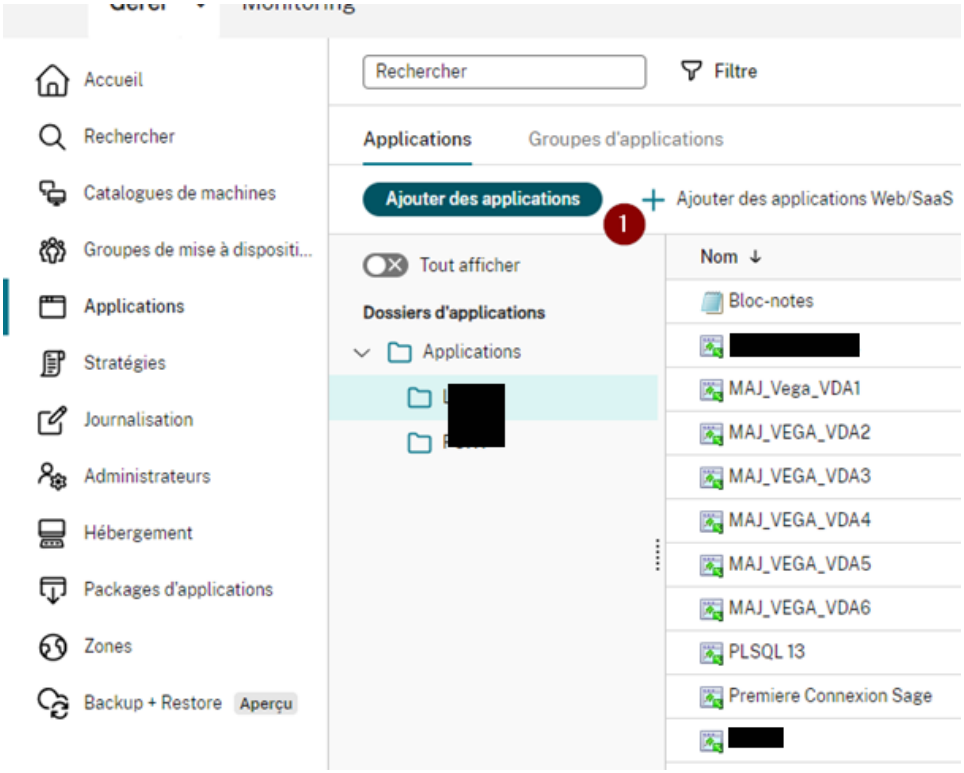
CITRIX

CITRIX

Ajouter une application depuis Citrix Cloud

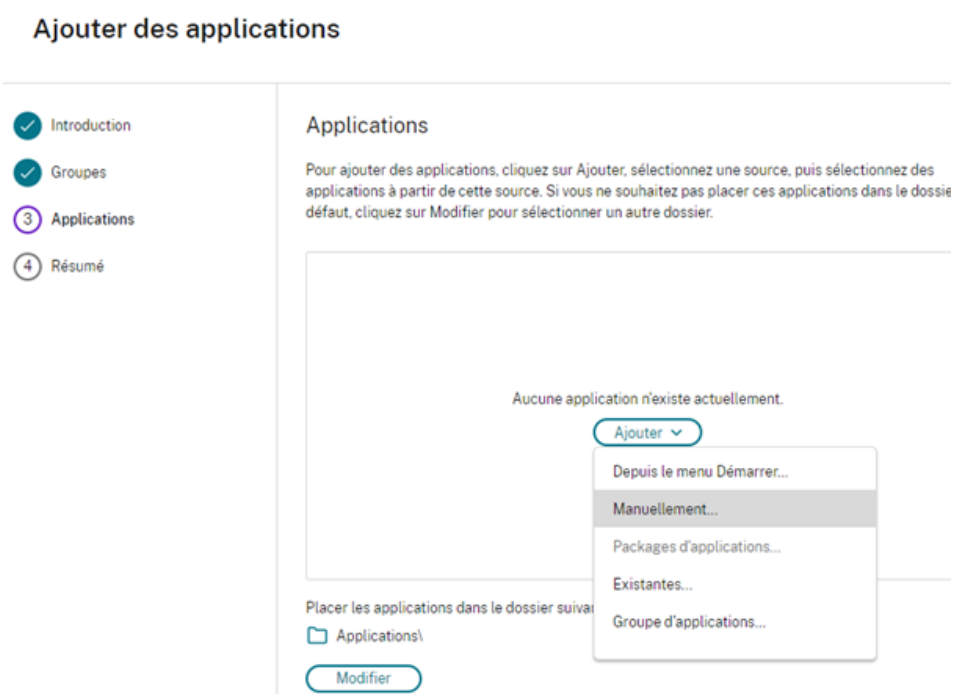
Procédure :

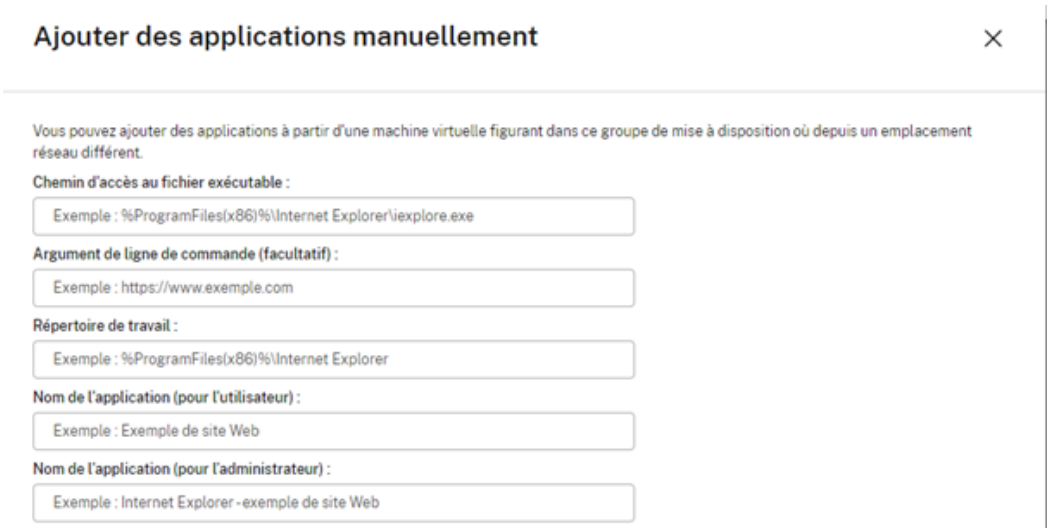
Se rendre sur la partie DaaS Advanced en s'authentifiant sur le site https://adm.cloud.com/
Dans la partie applications, cliquez sur "Ajouter des applications" dans le dossier





Ajouter manuellement l'application en renseignant les différents champs.

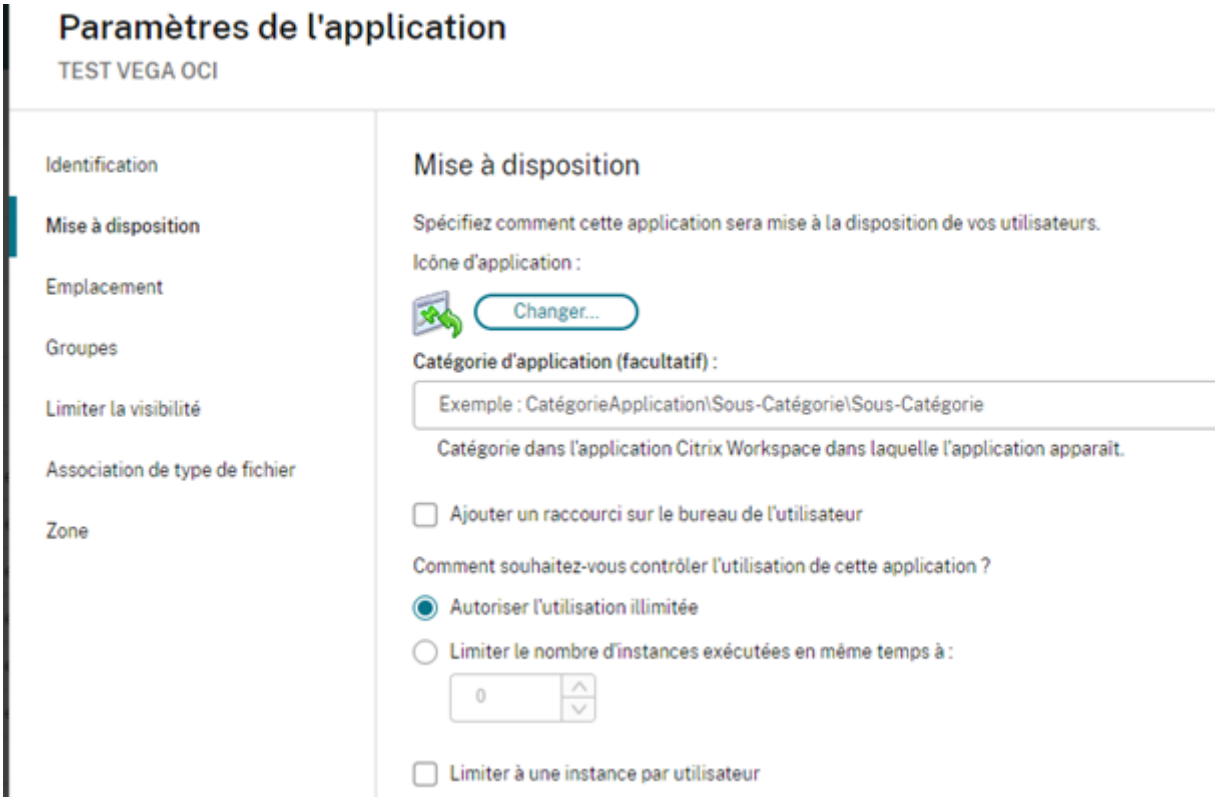




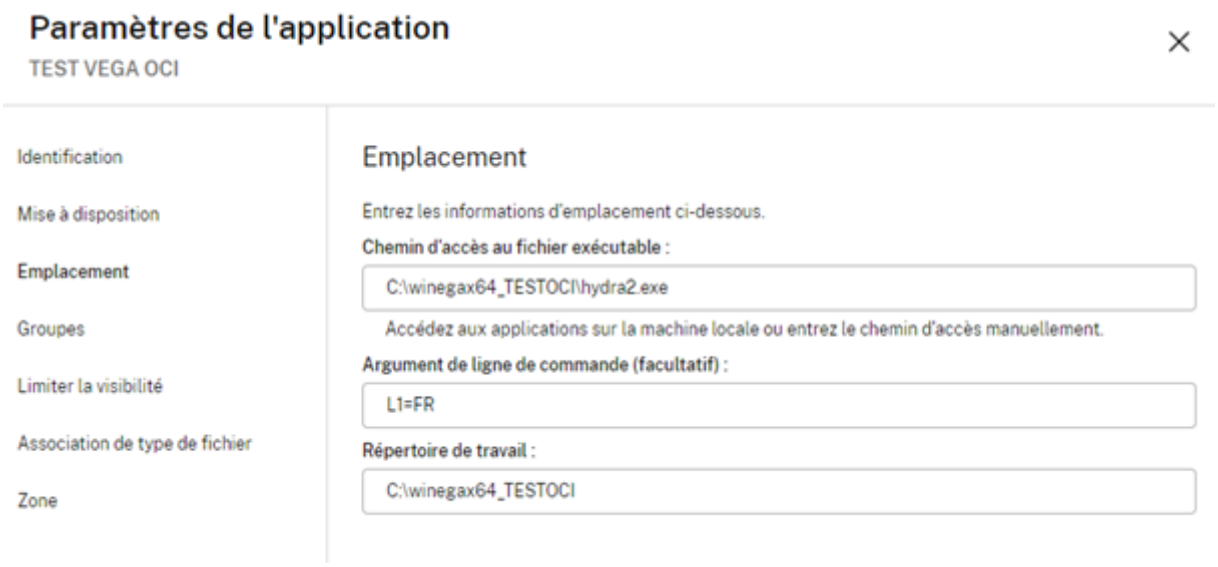
Voici un exemple d'application :
Le nom de l'application a été renseigné.

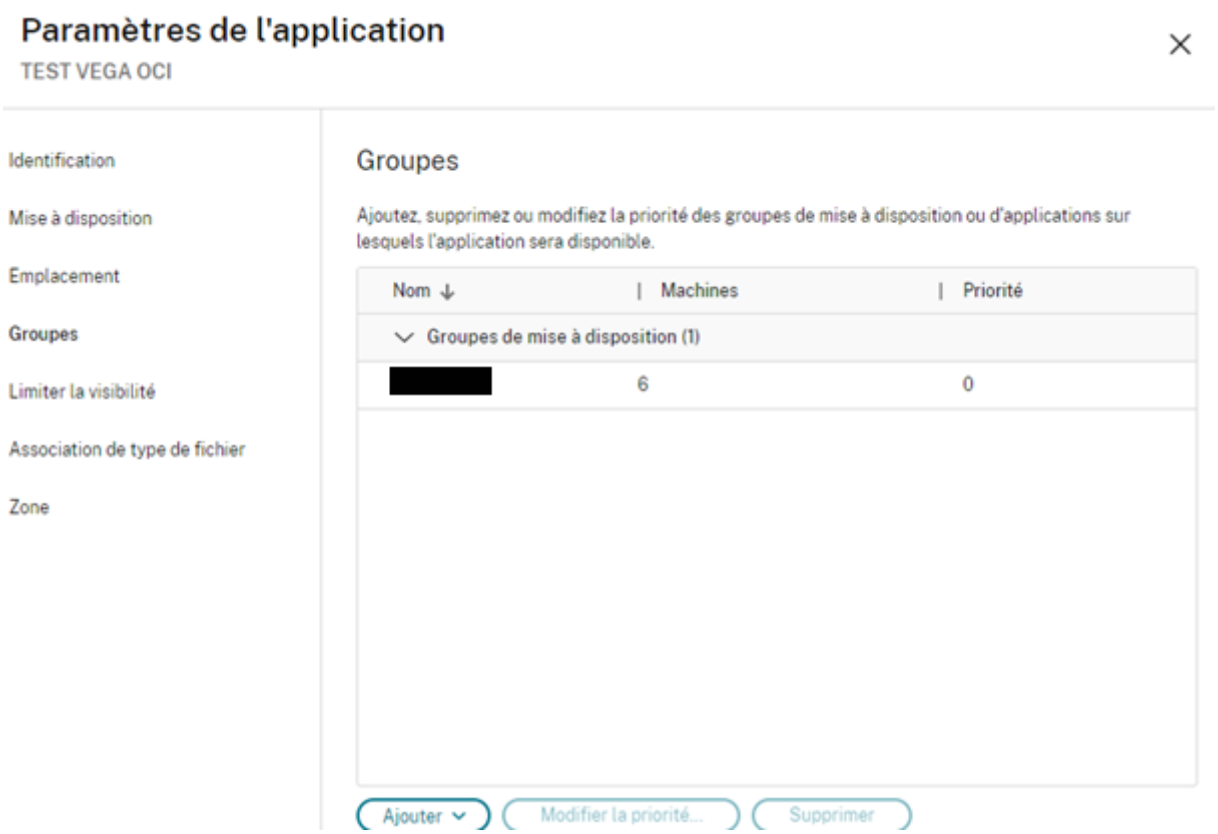


Possibilité de changer l'icône d'application et de limiter le nombre d'instances. (laisser les paramètres par défaut)

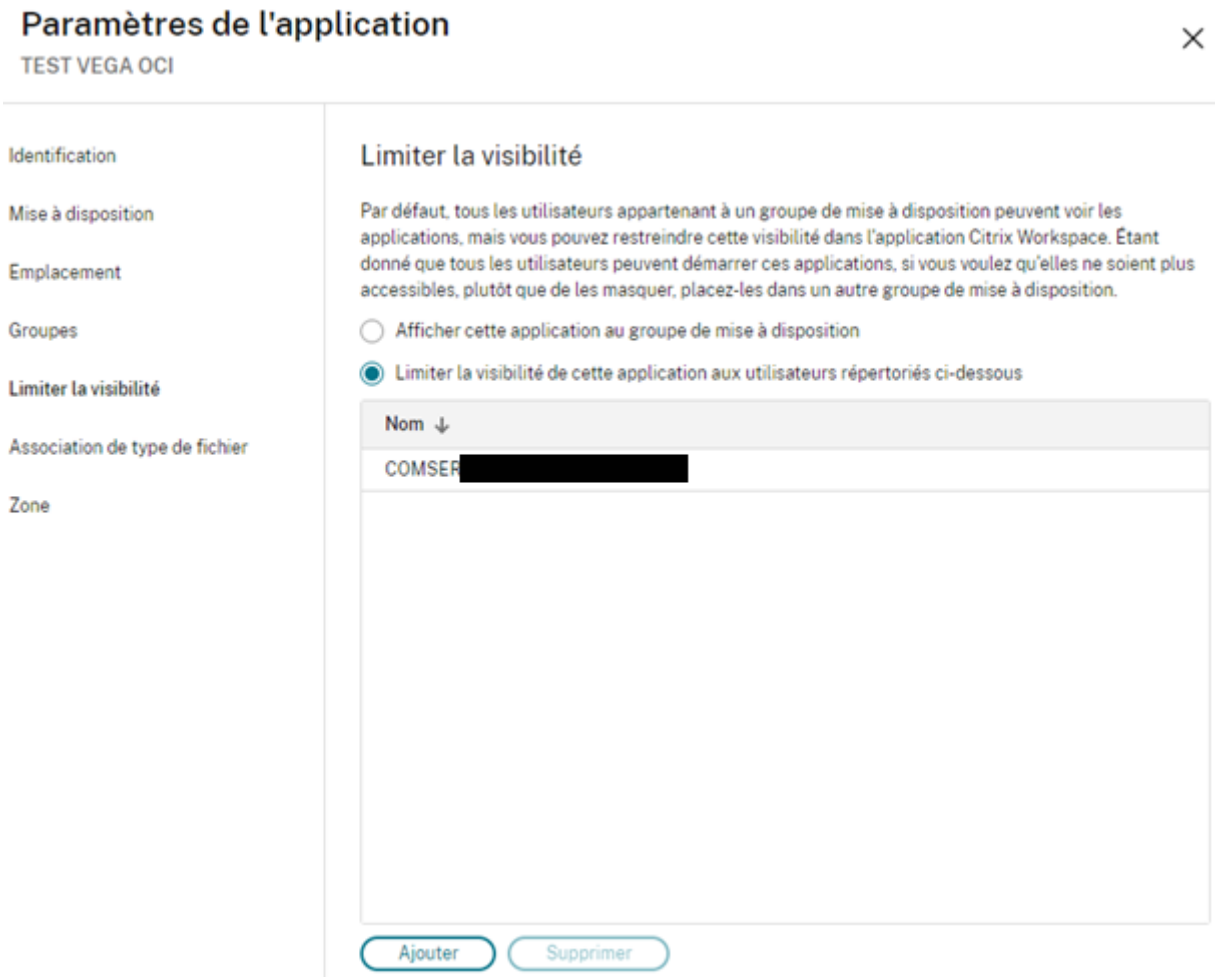


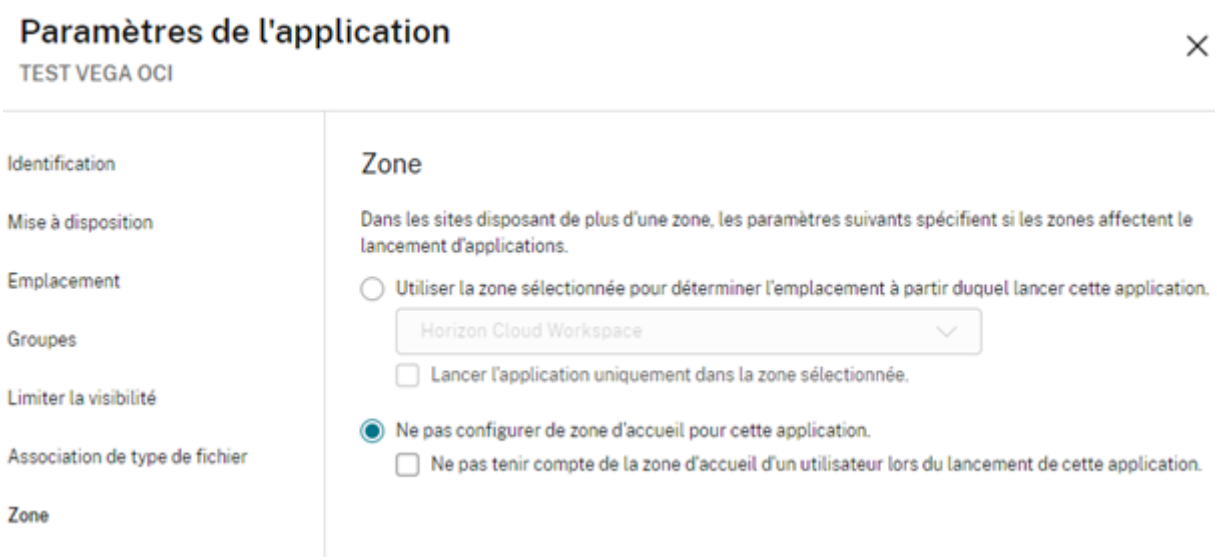
Chemin d'accès au fichier exécutable (emplacement avec le chemin exact de l'exécutable)
Argument de ligne de commande pour indiquer les options d'exécution.
Indiquer le répertoire de travail (emplacement/dossier du fichier à exécuter).



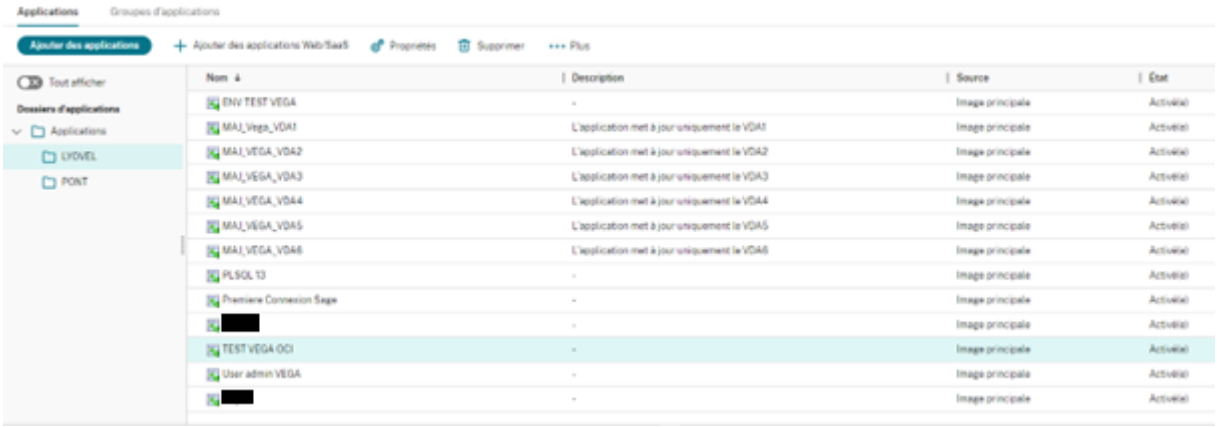


Pour limiter l'accès et la visibilité de l'application selon la demande, il faut au préalable créer un groupe de sécurité AD (exemple XenApp_NomApplication) et y insérer les membres/comptes AD qui devront avoir les autorisations pour accéder à l'application.

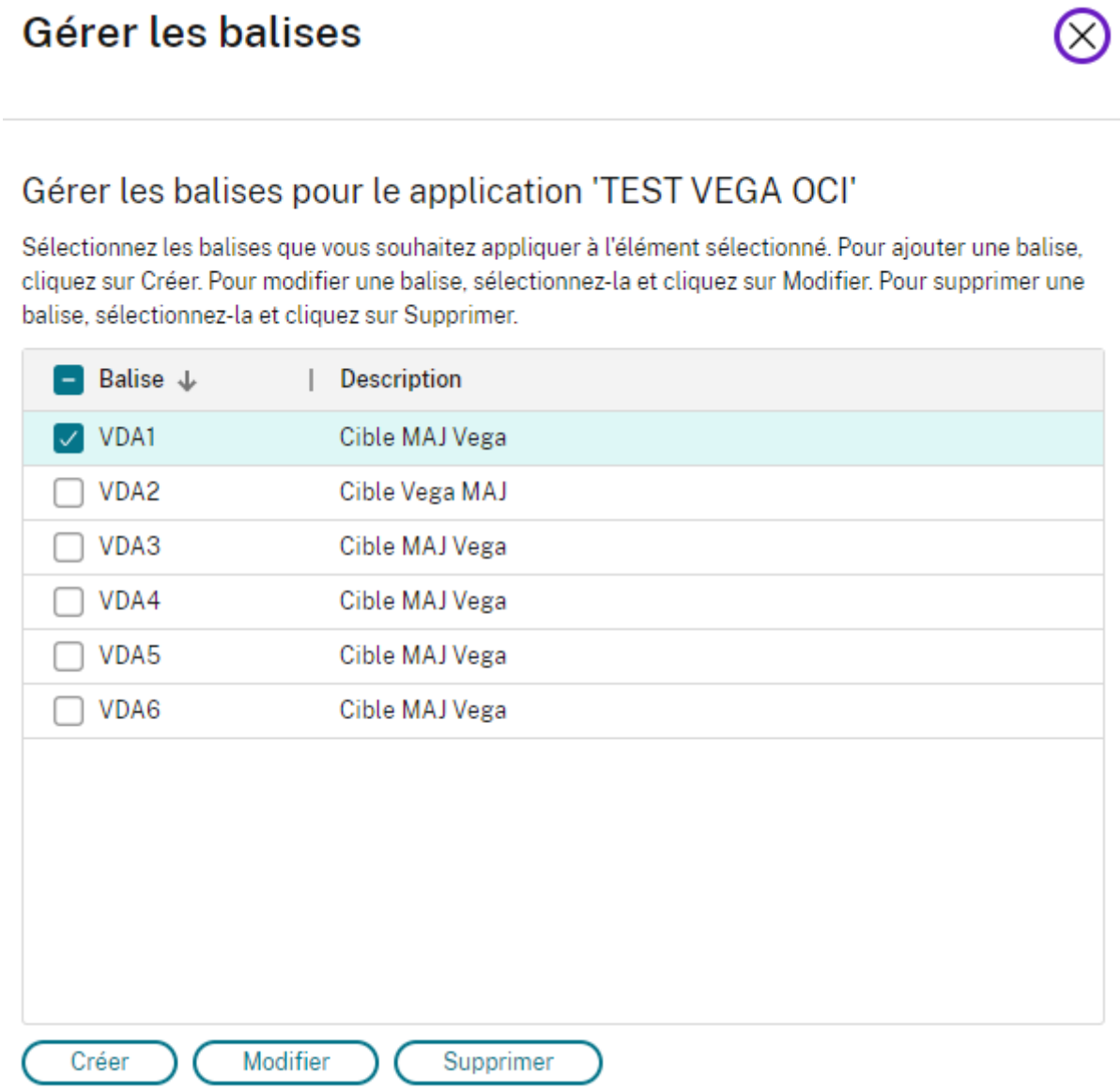




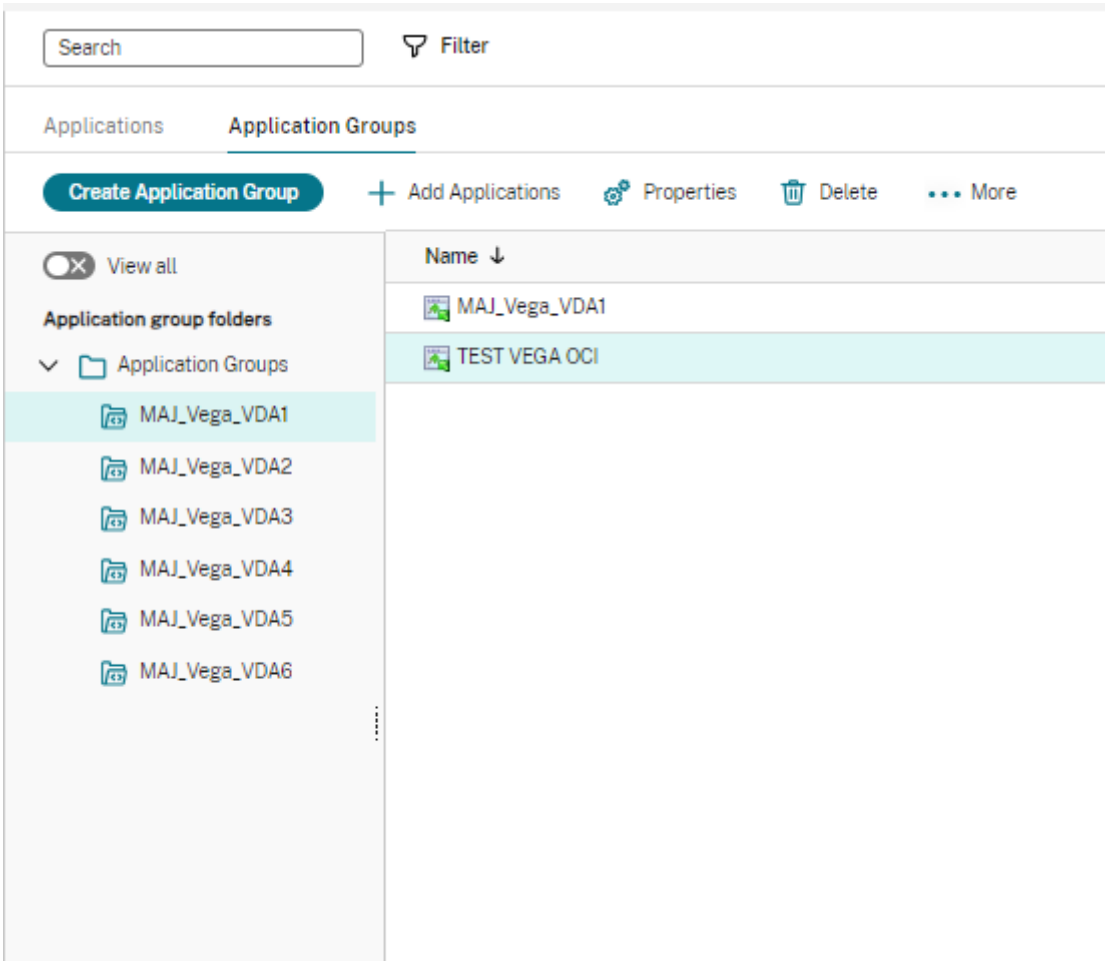
A la fin l'application sera visible ici :



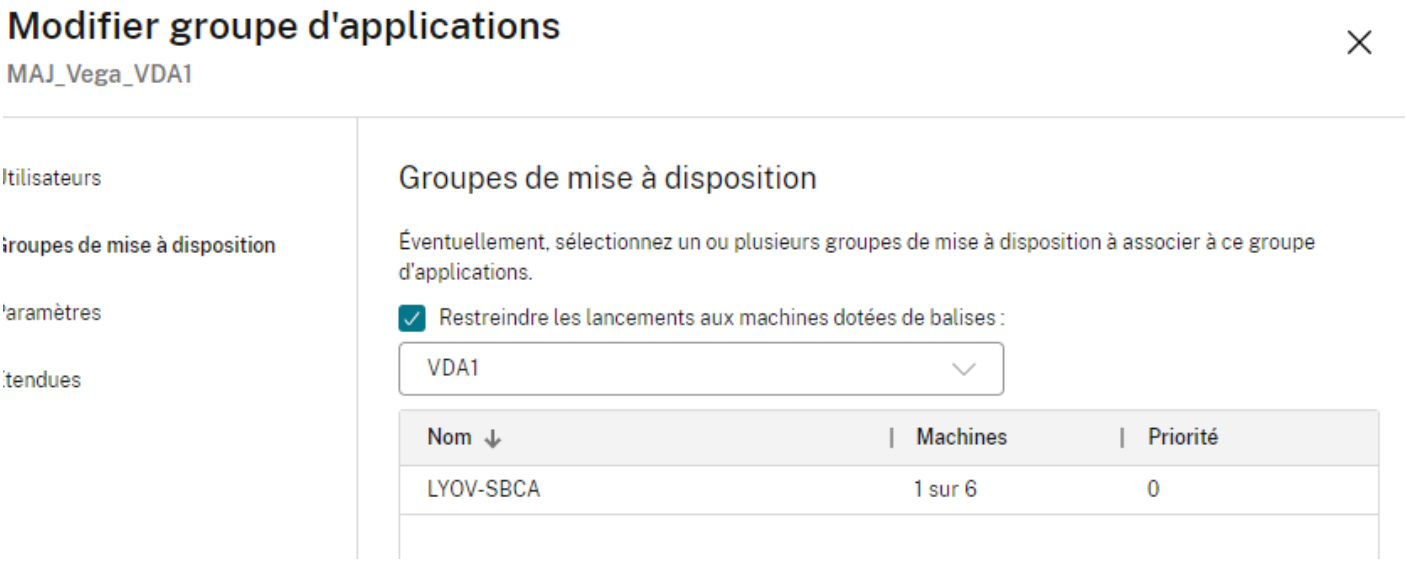
Si le client spécifie que l'application doit être accessible uniquement depuis un serveur VDA, il faut effectuer un clic droit sur l'application et lui appliquer une balise/tag correspond à la machine VDA.



Ensuite, il faut se rendre dans Application Groups ou Groupe d'applications et dans le " dossier " correspond, il faut ajouter une application existante.
Voir l'exemple ci-dessous : L'application existante TEST VEGA OCI a été ajoutée dans le groupe d'application MAJ_VEGA_VDA1.
Tous les utilisateurs qui seront dans le groupe AD XenApp_TEST_VEGA_OCI pourront se connecter à l'application depuis VDA1 uniquement.



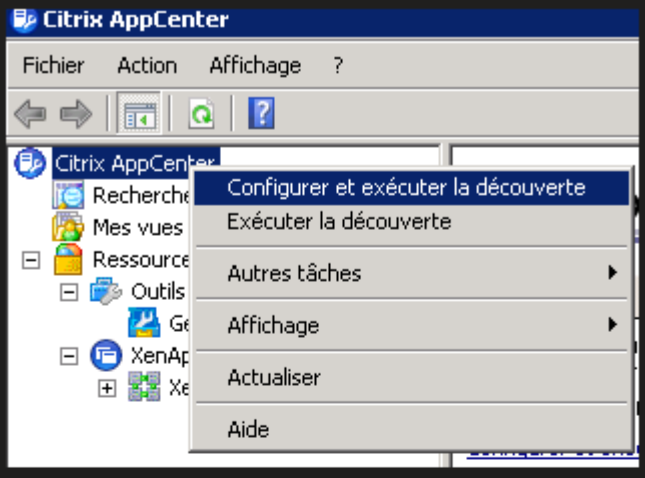
Note : Dans les paramètres du groupe d'applications, la restriction de lancement des applications sur une machine spécifique est indiquée.

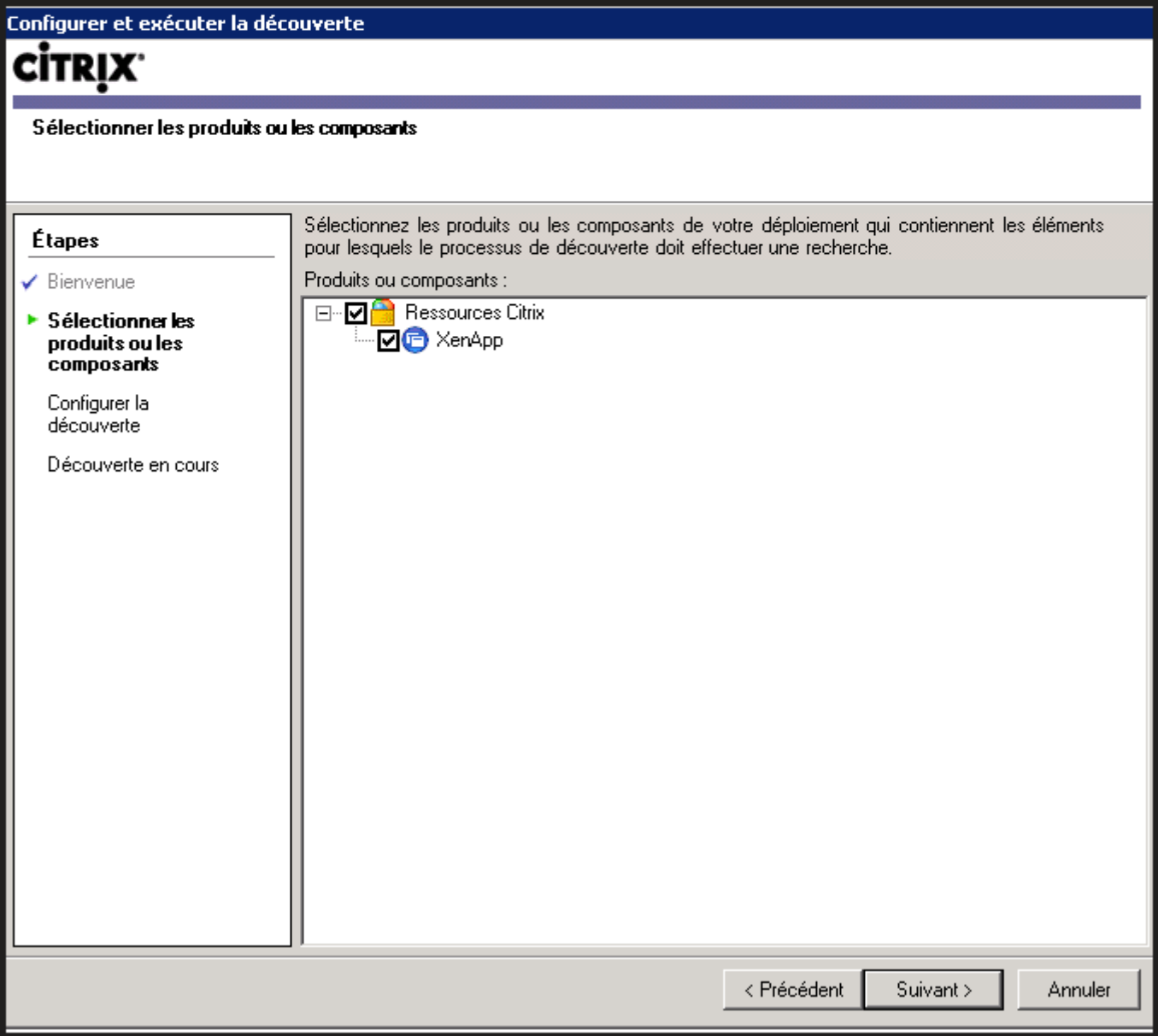


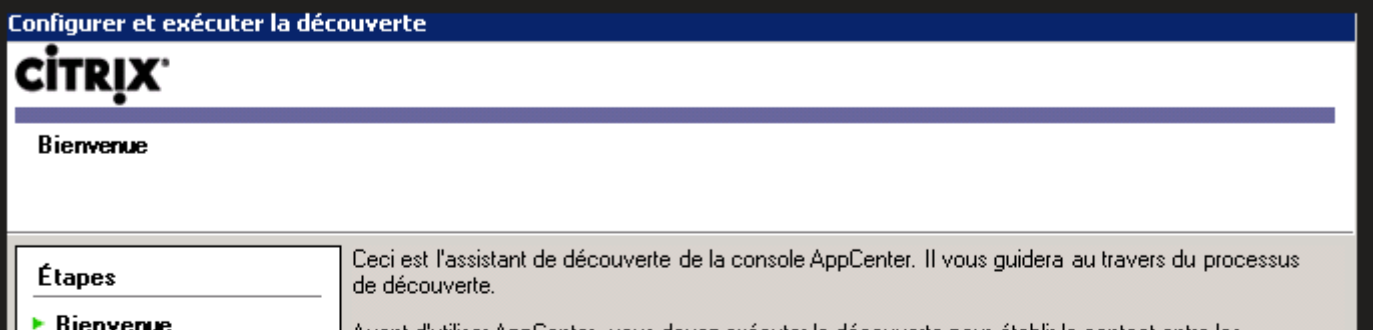
CITRIX

Citrix AppCenter

Pour accéder à la gestion du déploiement XenApp, il faut d'abord ajouter le serveur via "Configurer et exécuter la découverte" :


Citrix AppCenter
Fichier
Action
Affichage
?
Citrix AppCenter
Recherche
Mes vues
Ressource
Outils
XenAp
Configurer et exécuter la découverte
Exécuter la découverte
Autres tâches
Affichage
Actualiser
Aide


Configurer et exécuter la découverte
CITRIX
Sélectionner les produits ou les composants
Étapes
Bienvenue
Sélectionner les produits ou les composants
Configurer la découverte
Découverte en cours
Sélectionnez les produits ou les composants de votre déploiement qui contiennent les éléments pour lesquels le processus de découverte doit effectuer une recherche.
Produits ou composants :
Ressources Citrix
XenApp
< Précédent
Suivant >
Annuler


Configurer et exécuter la découverte
CITRIX
Bienvenue
Étapes
Bienvenue
Ceci est l'assistant de découverte de la console AppCenter. Il vous guidera au travers du processus de découverte.

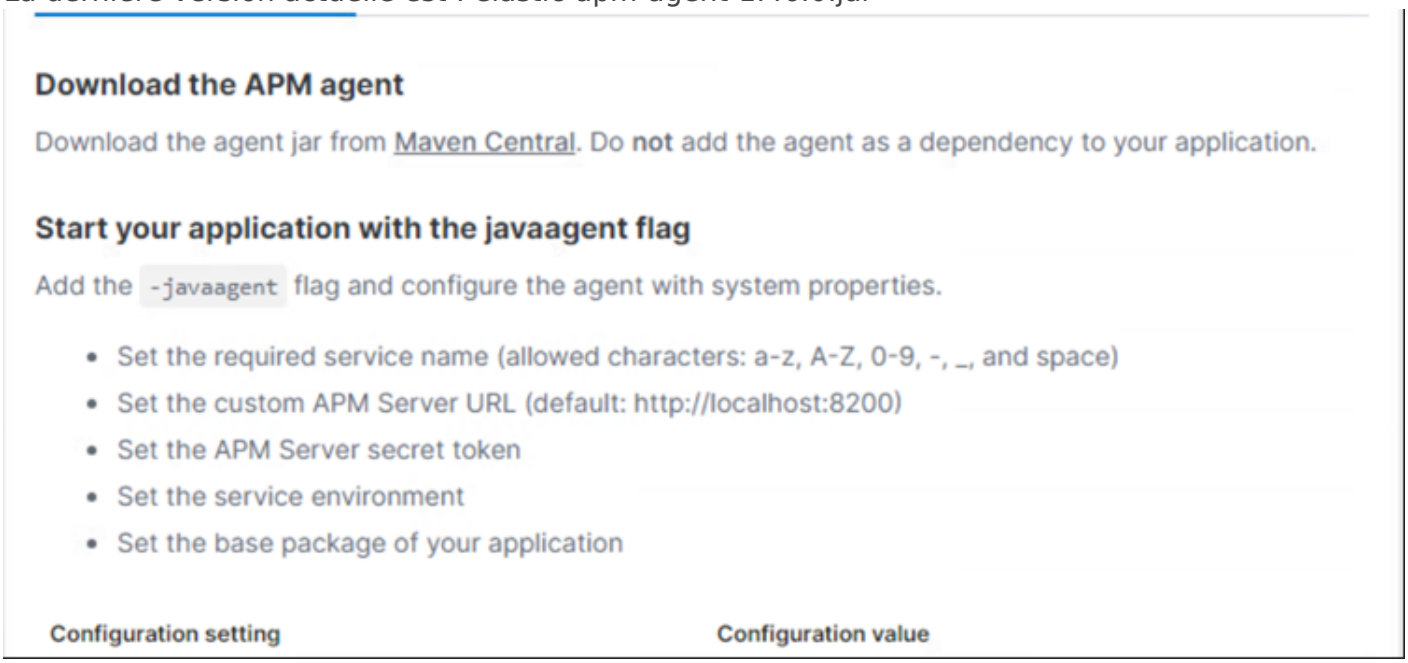
Supervision

Supervision

Elastic Search Installation

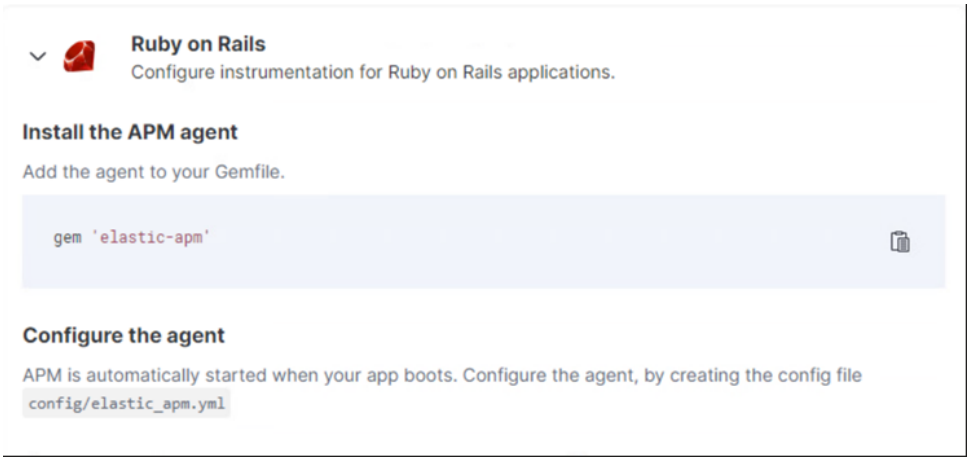
Voici la procédure pour installer l’agent APM pour TOMCAT Linux.

La dernière version actuelle est : elastic-apm-agent-1.46.0.jar



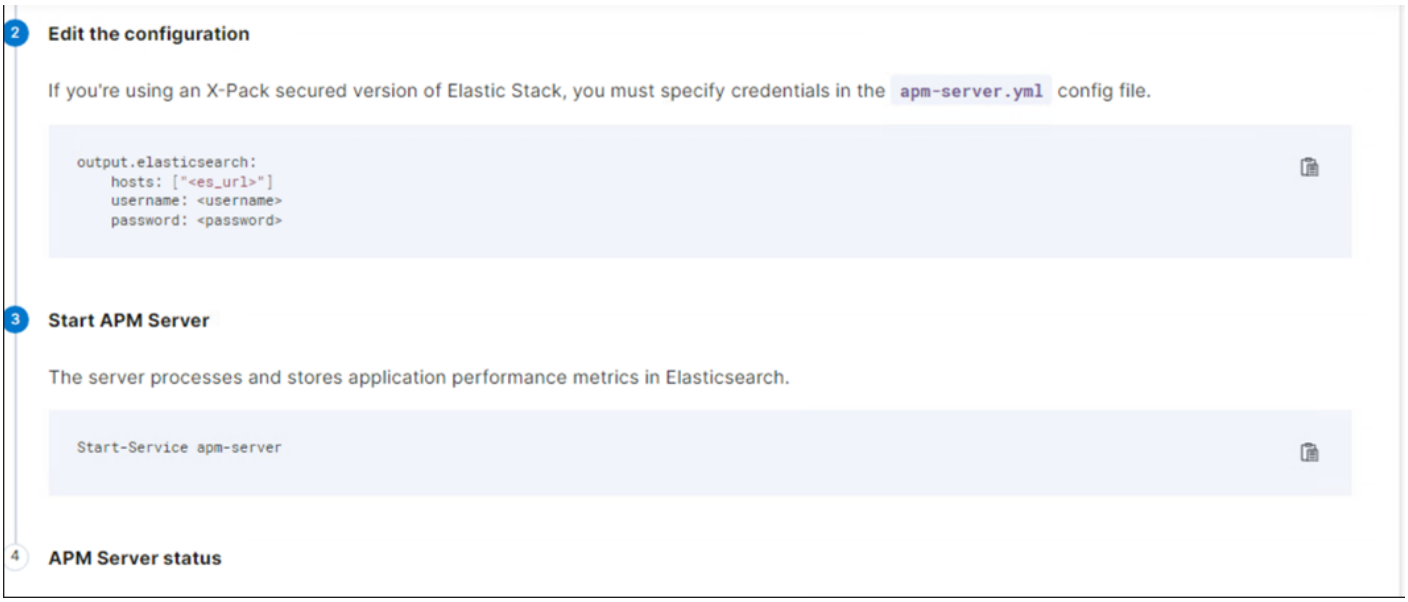


Voici la procédure pour installer l’agent APM pour Ruby on Rails Linux.

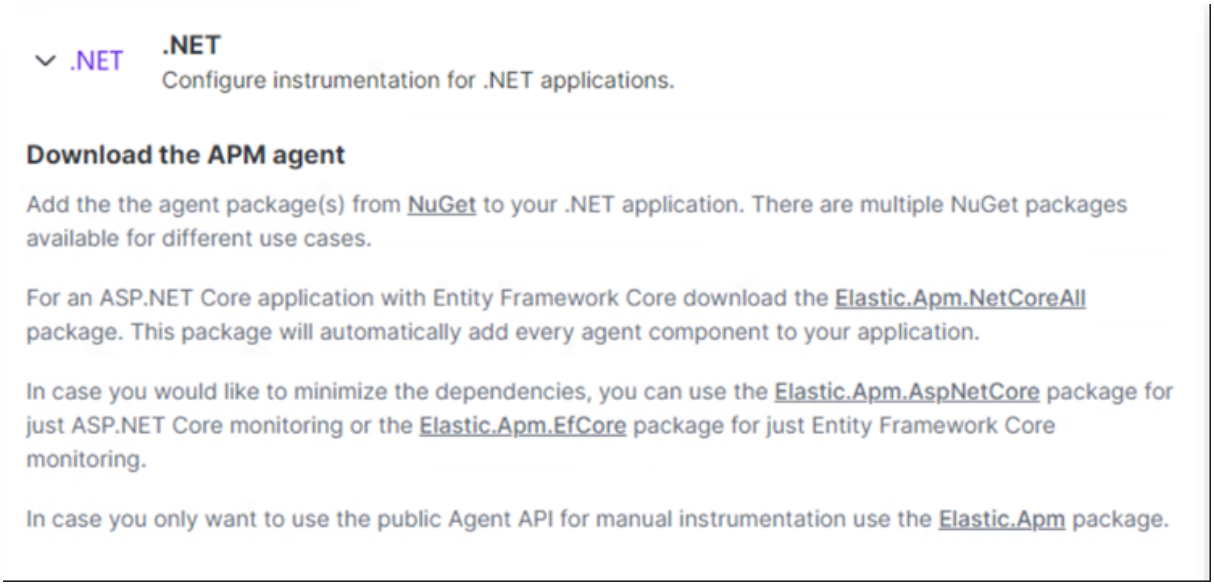




Voici la procédure pour installer l’agent APM pour TOMCAT Windows.



Voici la procédure pour installer l’agent APM pour ASP.net.



Add the agent to the application

In case of ASP.NET Core with the `Elastic.Apm.NetCoreAll` package, call the `UseAllElasticApm` method in the `Configure` method within the `Startup.cs` file.

```
public class Startup

  public void Configure(IApplicationBuilder app, IHostingEnvironment env)

    app.UseAllElasticApm(Configuration);
    //…rest of the method

  //…rest of the class
```

Passing an `IConfiguration` instance is optional and by doing so, the agent will read config settings through this `IConfiguration` instance (e.g. from the `appsettings.json` file).

Configuration setting	Configuration value
ServiceName	my-service-name
SecretToken	nv32xNSLMjK80VI793
ServerUrl	https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243
Environment	my-environment

```
{
  "ElasticApm": {
    "ServiceName": "my-service-name",
    "SecretToken": "nv32xNSLMjK80VI793",
    "ServerUrl": "https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243",
    "Environment": "my-environment",
  }
}
```

Voici la procédure pour installer l’agent APM pour Node.js

Node.js

Configure instrumentation for Node.js applications.

Install the APM agent

Install the APM agent for Node.js as a dependency to your application.

```
npm install elastic-apm-node --save
```

Configure the agent

Agents are libraries that run inside of your application process. APM services are created programmatically based on the `serviceName`. This agent supports a variety of frameworks but can also be used with your custom stack.

Configuration setting	Configuration value
serviceName	my-service-name
secretToken	nv32xNSLMjK80VI793
serverUrl	https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243
environment	my-environment

```
// Add this to the very top of the first file loaded in your app
var apm = require('elastic-apm-node').start({
  serviceName: 'my-service-name',

  secretToken: 'nv32xNSLMjK80VI793',

  serverUrl: 'https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243',

  environment: 'my-environment'
})
```

WEB

WEB

Clear Cache REDIS

La commande suivante est à lancer pour chaque site dans le répertoire du site, et sur chacun des 3 serveurs web en tant que l'utilisateur apache (ou www-data ou admin-apache)

Exemple comment exécuter la commande :

```
sudo -u login  php bin/console cache:clear --env=prod && php bin/console cache:pool:clear cache.redis --env=prod

cd /production/questions
php bin/console cache:clear --env=prod && php bin/console cache:pool:clear cache.redis --env=prod
cd /production/ezplatform
php bin/console cache:clear --env=prod && php bin/console cache:pool:clear cache.redis --env=prod
cd /production/ezplatform
php bin/console cache:clear --env=prod && php bin/console cache:pool:clear cache.redis --env=prod
cd /production/ezplatform
php bin/console cache:clear --env=prod && php bin/console cache:pool:clear cache.redis --env=prod
cd /production/ezplatform
php bin/console cache:clear --env=prod && php bin/console cache:pool:clear cache.redis --env=prod
```

WEB

Varnish clean cache

```
rm -rf /production/www/var/cache/* && systemctl restart rh-varnish5-varnish && systemctl restart httpd && systemctl restart rh-php73-php-fpm.service && systemctl restart rh-redis5-redis
```

```
su - LOGIN
```

```
cd /production/www/current/docroot
/opt/rh/rh-php73/root/bin/php bin/console cache:clear --no-warmup --env=prod -vvv && /opt/rh/rh-php73/root/bin/php bin/console cache:pool:clear cache.redis --env=prod -vvv
```



WEB

Error PHP

> PHP Fatal error: Uncaught RuntimeException: Failed to start the session

Open the Varnish configuration file:
/etc/varnish/default.vcl or /etc/varnish/varnish.params

You should see a line similar to the following in your configuration file:

# set the size of the cache in MB
set max_cache_size = 256M;

Increase the cache size:

set max_cache_size = 512M;

Save the configuration file and restart Varnish

WEB

PHP-FPM

Ajustement de la sonde Centreon :
Lin_Process_php-fpm_pool
- Min : 24
○ Car dans le fichier de configuration c'est le nombre de process lancé au démarrage
- Max : 200
○ Car le maximum dans le fichier de configuration est 256

Fichier de conf : /etc/php/7.4/fpm/pool.d/www.conf