

Applicatif / Langage

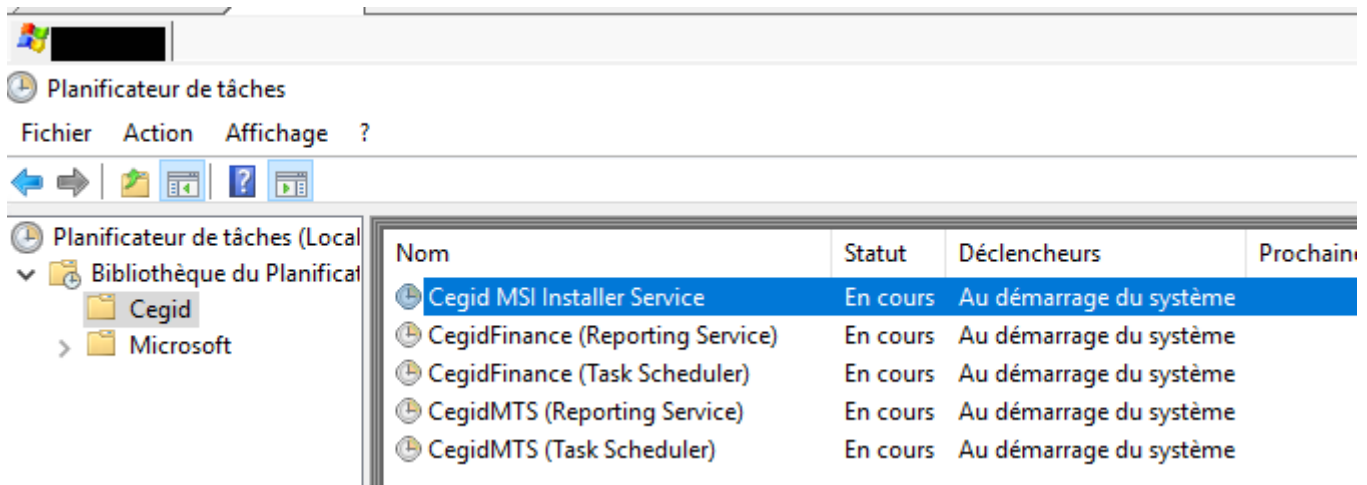
- Applications
 - CEGID Y2 notes d'Incident
- BASTION
 - Incident - Session Probe Drive of Session Probe is not ready yet
 - Bastion TMA
 - Incident - TLS CERTIFICATE CHANGED
- CITRIX
 - Ajouter une application depuis Citrix Cloud
 - Citrix AppCenter
- Supervision
 - Elastic Search Installation
- WEB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

Applications

CEGID Y2 notes d'Incident

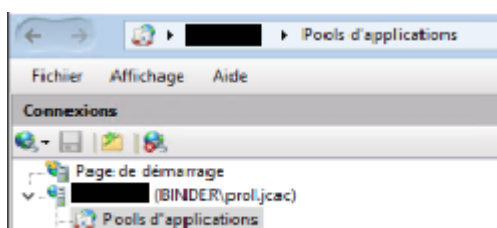
En cas d'incident CEGID où plusieurs modules ne fonctionnent pas comme attendu il faut procéder à la vérification ci-dessous:

Les tâches planifiées CEGID doivent être 'en cours d'exécution' sur le SRVY2RT :

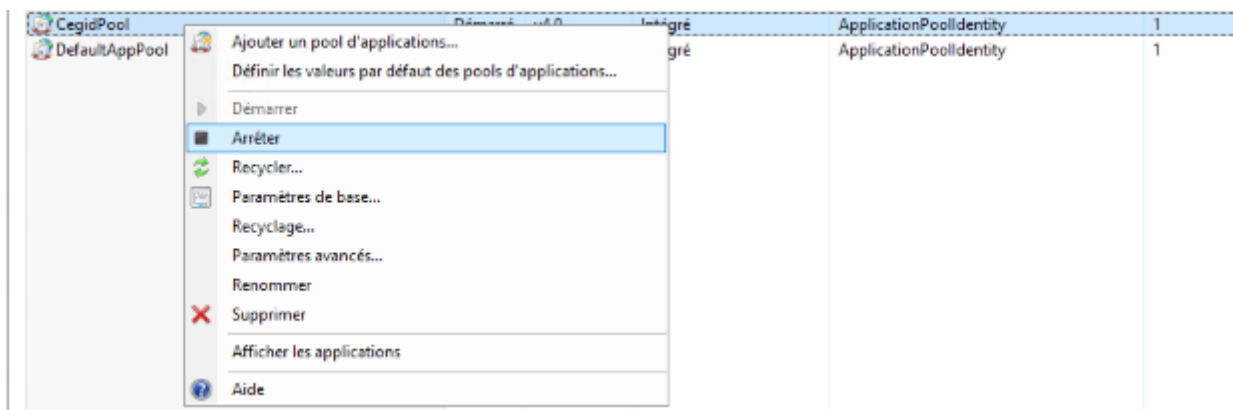


Si ce n'est pas le cas, il faut les démarrer manuellement.
Elles doivent rester "en cours"

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

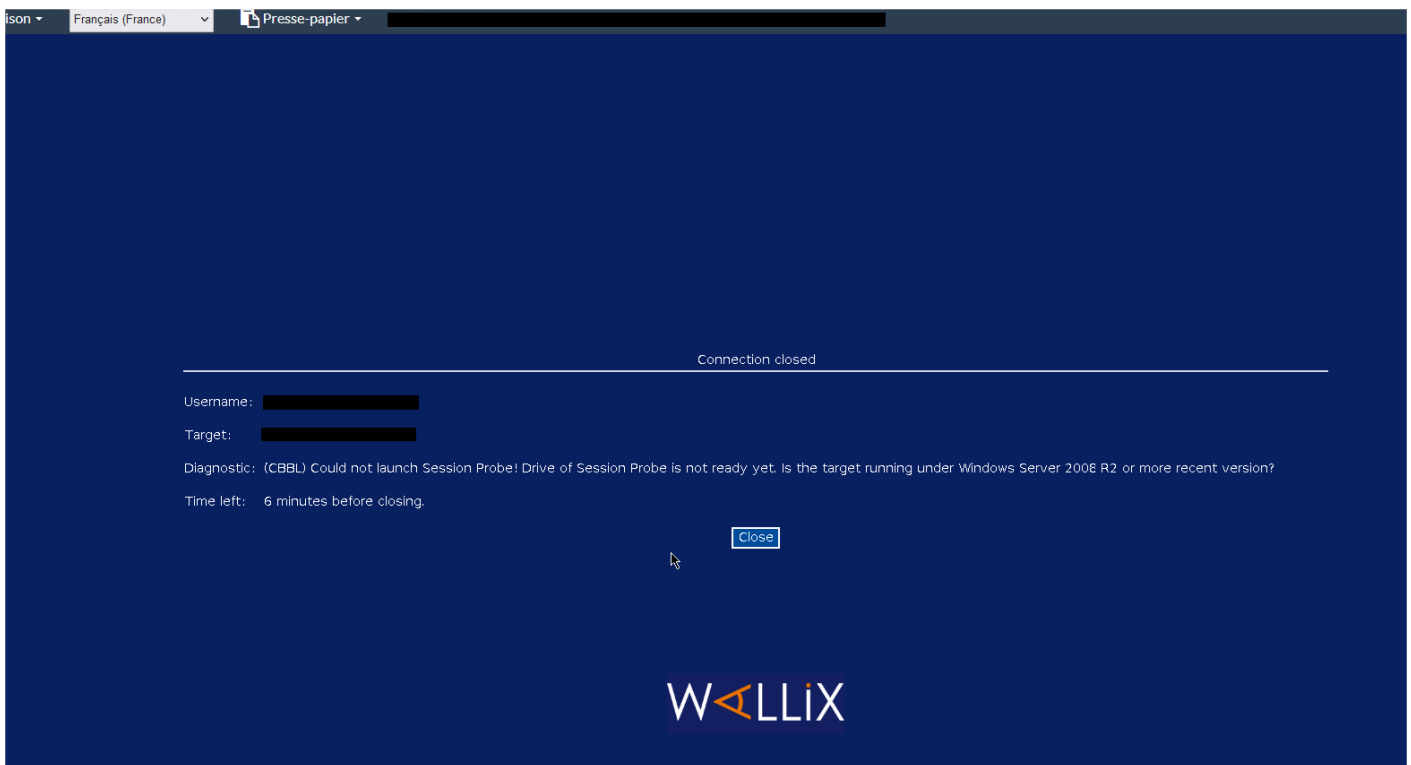


demander au client si les users peuvent se reconnecter

BASTION

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?
```

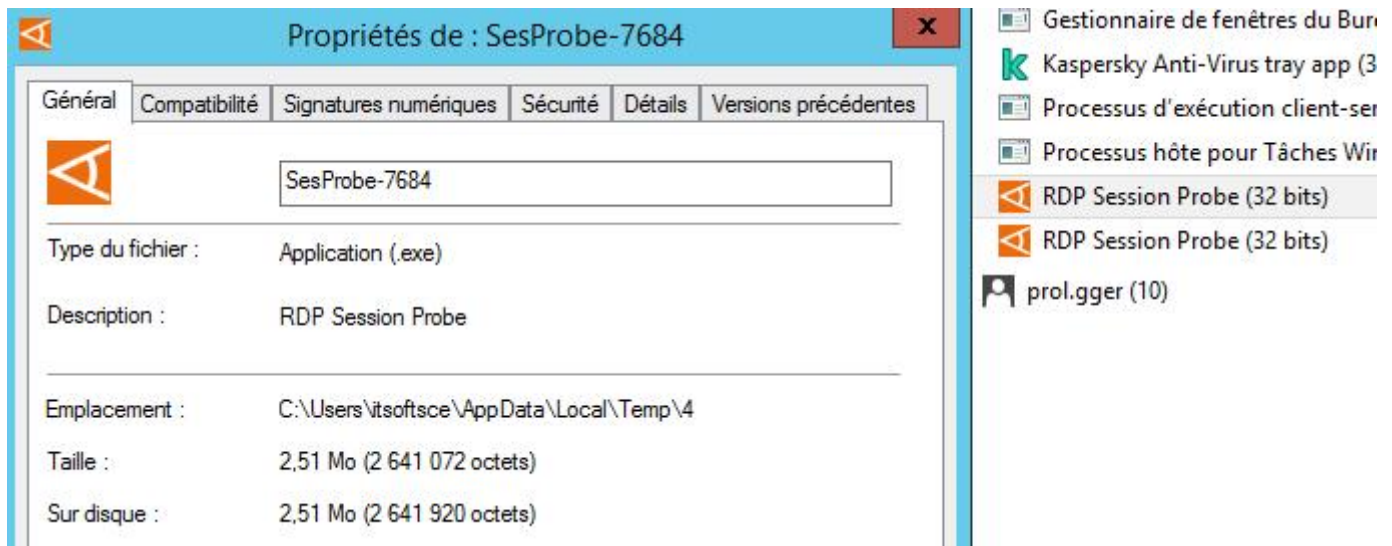
```
Aug 25 13:27:37 bastion1 rdpproxy[24076]: ERR (24076/24076) --  
SessionProbeVirtualChannel::process_event_launch: Session Probe is not ready yet!
```

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 TMA

Interface d'admin :

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

Ajout des serveurs:

Targets --> Devices --> Add

The screenshot shows the Bastion TMA admin interface. At the top, there is a breadcrumb navigation: [Home](#) > [Targets](#) > [Devices](#) > [New](#) > **General**. Below this is a tabbed interface with tabs: **General**, [Services](#), [Local domains](#), [Local accounts](#), [Groups](#), [Certificates](#), and [Tags](#). The 'General' tab is active. It contains three text input fields: 'Name *' (with a red asterisk), 'Alias', and 'IP address or FQDN *' (with a red asterisk). Below these fields is a section titled 'Description' with a play button icon. At the bottom left of the form is an orange 'Apply' button.

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)

New service RDP

Device

PRD

Service name *

RDP

This name is already used

Port *

3389

Connection policy *

RDP

Global domains

A global domain is required to create targets for applications and clusters

Enter a global domain name

Proxy options

☒ RDP_CLIPBOARD_UP
 ☒ RDP_CLIPBOARD_DOWN
 ☒ RDP_CLIPBOARD_FILE
 ☒ RDP_PRINTER
 ☒ RDP_COM_PORT
 ☒ RDP_DRIVE
 ☒ RDP_SMARTCARD
 ☒ RDP_AUDIO_OUTPUT
 ☒ RDP_AUDIO_INPUT

Close

Apply and close

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:

Add interactive login targets for session management

Group

From *

A device and related services

Device *

Services *

Select at least one available entry

☐ Service name
 ☐ RDP

☒ Already in group

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

Add

<input type="checkbox"/>	Application	Device	Service
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP

Attribution des accès aux users:

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

User group *

Target group *

Name *

Description:

Accès aux nouveaux serveurs Exchange 2019

Critical targets:
☐

Enable sessions:
☒

Protocols/subprotocols *

Available Protocols/subprotocols

Q

RAWTCPIP

RLOGIN

SSH_SHELL_SESSION

SSH_REMOTE_COMMAND

SSH_SCP_UP

SSH_SCP_DOWN

SSH_X11

SFTP_SESSION

SSH_DIRECT_TCPIP

SSH_REVERSE_TCPIP

SSH_AUTH_AGENT

Select all

Selected Protocols/subprotocols

Q

RDP

RDP_AUDIO_INPUT

RDP_AUDIO_OUTPUT

RDP_CLIPBOARD_DOWN

RDP_CLIPBOARD_FILE

RDP_CLIPBOARD_UP

RDP_COM_PORT

RDP_DRIVE

RDP_PRINTER

RDP_SMARTCARD

Delete all

Enable session recording:
☒

Enable password checkout:
☐

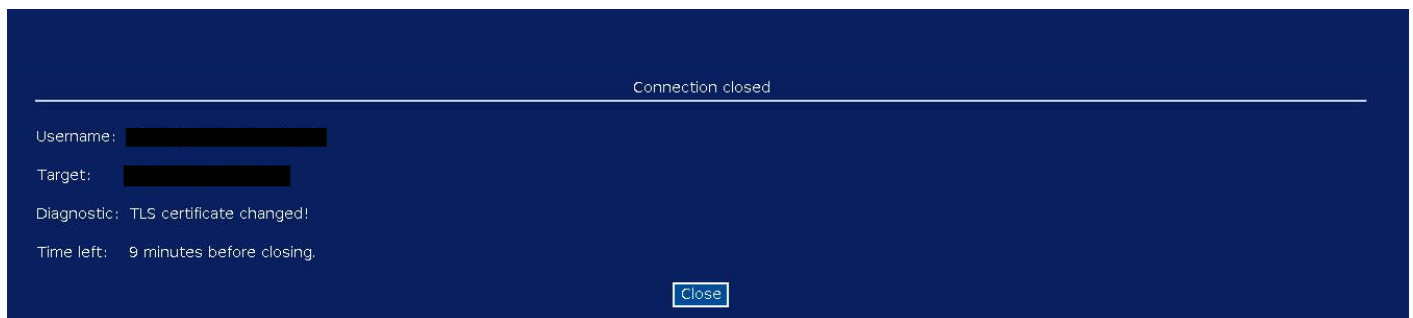
Enable approval workflow:
☐

Demander de tester les accès.

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

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.

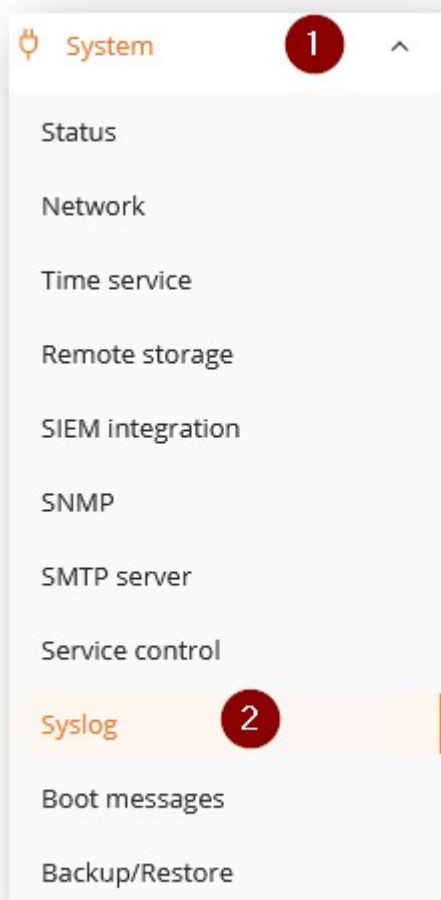
Le renouvellement est possible en supprimant en premier lieu le certificat dans le bastion et se reconnecter au serveur cible depuis l'accès utilisateur pour que le bastion récupère le nouveau certificat.

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/

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 :

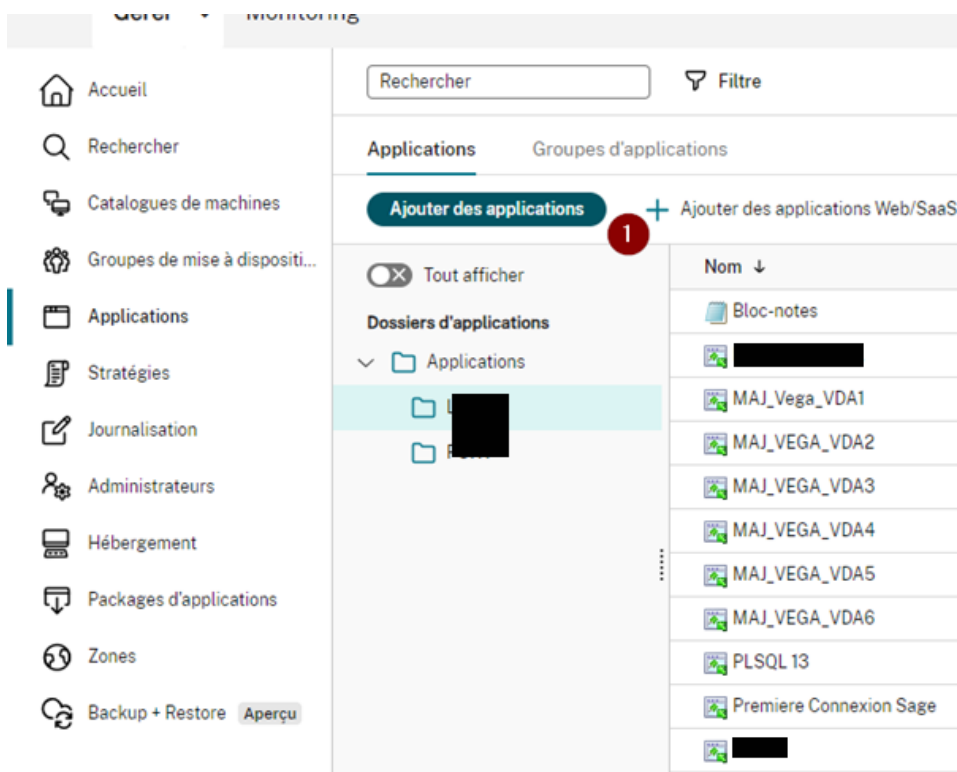
```
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- SSL_get_peer_certificate()
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate directory is:
'/var/wab/cert/18074c309afb7897005056a2a787'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate 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

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 des applications



1 Introduction

2 Groupes

3 Applications

4 Résumé

Introduction aux applications

Pour mettre des applications à la disposition de vos utilisateurs, sélectionnez un ou plusieurs groupes d'applications ou de mise à disposition, puis sélectionnez des applications disponibles. Les groupes de mise à disposition peuvent également être associés à des groupes d'applications.

Ajouter manuellement l'application en renseignant les différents champs.

Ajouter des applications

- ✓ Introduction
- ✓ Groupes
- ③ Applications
- ④ Résumé

Applications

Pour ajouter des applications, cliquez sur Ajouter, sélectionnez une source, puis sélectionnez des applications à partir de cette source. Si vous ne souhaitez pas placer ces applications dans le dossier défaut, cliquez sur Modifier pour sélectionner un autre dossier.

Aucune application n'existe actuellement.

Ajouter ▾

Depuis le menu Démarrer...

Manuellement...

Packages d'applications...

Existantes...

Groupe d'applications...

Placer les applications dans le dossier suivant

Applications\

Modifier

Ajouter des applications manuellement



Vous pouvez ajouter des applications à partir d'une machine virtuelle figurant dans ce groupe de mise à disposition où depuis un emplacement réseau différent.

Chemin d'accès au fichier exécutable :

Exemple : %ProgramFiles(x86)%\Internet Explorer\iexplore.exe

Argument de ligne de commande (facultatif) :

Exemple : https://www.exemple.com

Répertoire de travail :

Exemple : %ProgramFiles(x86)%\Internet Explorer

Nom de l'application (pour l'utilisateur) :

Exemple : Exemple de site Web

Nom de l'application (pour l'administrateur) :

Exemple : Internet Explorer - exemple de site Web

Voici un exemple d'application :

Le nom de l'application a été renseigné.

Paramètres de l'application

TEST VEGA OCI



Identification

Mise à disposition

Emplacement

Groupes

Limiter la visibilité

Association de type de fichier

Zone

Identification

Identifiez cette application.

Nom de l'application (pour l'administrateur) :

TEST VEGA OCI

Nom de l'application (pour l'utilisateur) :

TEST VEGA OCI

Description et mots-clés :

Description que l'utilisateur verra. Vous pouvez également utiliser ce champ pour entrer des mots-clés pour StoreFront.

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

Paramètres de l'application

TEST VEGA OCI

Identification

Mise à disposition

Emplacement

Groupes

Limiter la visibilité

Association de type de fichier

Zone

Mise à disposition

Spécifiez comment cette application sera mise à la disposition de vos utilisateurs.

Icône d'application :

Changer...

Catégorie d'application (facultatif) :

Exemple : CatégorieApplication\Sous-Catégorie\Sous-Catégorie

Catégorie dans l'application Citrix Workspace dans laquelle l'application apparaît.

☐

 Ajouter un raccourci sur le bureau de l'utilisateur

Comment souhaitez-vous contrôler l'utilisation de cette application ?

☒

 Autoriser l'utilisation illimitée

☐

 Limiter le nombre d'instances exécutées en même temps à :

0

☐

 Limiter à une instance par utilisateur

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).

Paramètres de l'application

TEST VEGA OCI

Identification

Mise à disposition

Emplacement

Groupes

Limiter la visibilité

Association de type de fichier

Zone

Emplacement

Entrez les informations d'emplacement ci-dessous.

Chemin d'accès au fichier exécutable :

C:\winegax64_TESTOCI\hydra2.exe

Accédez aux applications sur la machine locale ou entrez le chemin d'accès manuellement.

Argument de ligne de commande (facultatif) :

L1=FR

Répertoire de travail :

C:\winegax64_TESTOCI

Paramètres de l'application

TEST VEGA OCI



Identification

Mise à disposition

Emplacement

Groupes

Limiter la visibilité

Association de type de fichier

Zone

Groupes

Ajoutez, supprimez ou modifiez la priorité des groupes de mise à disposition ou d'applications sur lesquels l'application sera disponible.

Nom ↓	Machines	Priorité
▼ Groupes de mise à disposition (1)		
██████████	6	0

[Ajouter ▼](#) [Modifier la priorité...](#) [Supprimer](#)

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.

Paramètres de l'application

TEST VEGA OCI



Identification

Mise à disposition

Emplacement

Groupes

Limiter la visibilité

Association de type de fichier

Zone

Limiter la visibilité

Par défaut, tous les utilisateurs appartenant à un groupe de mise à disposition peuvent voir les applications, mais vous pouvez restreindre cette visibilité dans l'application Citrix Workspace. Étant donné que tous les utilisateurs peuvent démarrer ces applications, si vous voulez qu'elles ne soient plus accessibles, plutôt que de les masquer, placez-les dans un autre groupe de mise à disposition.

- ☐ Afficher cette application au groupe de mise à disposition
- ☒ Limiter la visibilité de cette application aux utilisateurs répertoriés ci-dessous

Nom ↓
COMSER ██████████

[Ajouter](#) [Supprimer](#)

Paramètres de l'application

TEST VEGA OCI



Identification

Mise à disposition

Emplacement

Groupes

Limiter la visibilité

Association de type de fichier

Zone

Zone

Dans les sites disposant de plus d'une zone, les paramètres suivants spécifient si les zones affectent le lancement d'applications.

☐ Utiliser la zone sélectionnée pour déterminer l'emplacement à partir duquel lancer cette application.

Horizon Cloud Workspace



☐ Lancer l'application uniquement dans la zone sélectionnée.

☒ Ne pas configurer de zone d'accueil pour cette application.

☐ Ne pas tenir compte de la zone d'accueil d'un utilisateur lors du lancement de cette application.


A la fin l'application sera visible ici :

Applications		Groupes d'applications		
Ajouter des applications		+ Ajouter des applications Web/SaaS	Propriétés	Supprimer
+++ Plus				
Tout afficher	Nom	Description	Source	État
	ENV TEST VEGA	-	Image principale	Activée
	MAJ_VEGA_VDA1	L'application met à jour uniquement le VDA1	Image principale	Activée
	MAJ_VEGA_VDA2	L'application met à jour uniquement le VDA2	Image principale	Activée
	MAJ_VEGA_VDA3	L'application met à jour uniquement le VDA3	Image principale	Activée
	MAJ_VEGA_VDA4	L'application met à jour uniquement le VDA4	Image principale	Activée
	MAJ_VEGA_VDA5	L'application met à jour uniquement le VDA5	Image principale	Activée
	MAJ_VEGA_VDA6	L'application met à jour uniquement le VDA6	Image principale	Activée
	PLSQL 13	-	Image principale	Activée
	Première Connexion Sage	-	Image principale	Activée
		-	Image principale	Activée
	TEST VEGA OCI	-	Image principale	Activée
	User admin VEGA	-	Image principale	Activée
		-	Image principale	Activée

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.

Gérer les balises pour le application 'TEST VEGA OCI'

Sélectionnez les balises que vous souhaitez appliquer à l'élément sélectionné. Pour ajouter une balise, cliquez sur Créer. Pour modifier une balise, sélectionnez-la et cliquez sur Modifier. Pour supprimer une balise, sélectionnez-la et cliquez sur Supprimer.

 Balise ↓	Description
<input checked="" type="checkbox"/> VDA1	Cible MAJ Vega
<input type="checkbox"/> VDA2	Cible Vega MAJ
<input type="checkbox"/> VDA3	Cible MAJ Vega
<input type="checkbox"/> VDA4	Cible MAJ Vega
<input type="checkbox"/> VDA5	Cible MAJ Vega
<input type="checkbox"/> VDA6	Cible MAJ Vega

[Créer](#)[Modifier](#)[Supprimer](#)

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.

Search

Filter

Applications

Application Groups

Create Application Group

+ Add Applications

⚙ Properties

🗑 Delete

⋮ More

View all

Application group folders

Application Groups

MAJ_Vega_VDA1

MAJ_Vega_VDA2

MAJ_Vega_VDA3

MAJ_Vega_VDA4

MAJ_Vega_VDA5

MAJ_Vega_VDA6

Name ↓

MAJ_Vega_VDA1

TEST VEGA OCI

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

Modifier groupe d'applications

×

MAJ_Vega_VDA1

Utilisateurs

Groupe de mise à disposition

Paramètres

Statistiques

Groupe de mise à disposition

Éventuellement, sélectionnez un ou plusieurs groupes de mise à disposition à associer à ce groupe d'applications.

☒ Restreindre les lancements aux machines dotées de balises :

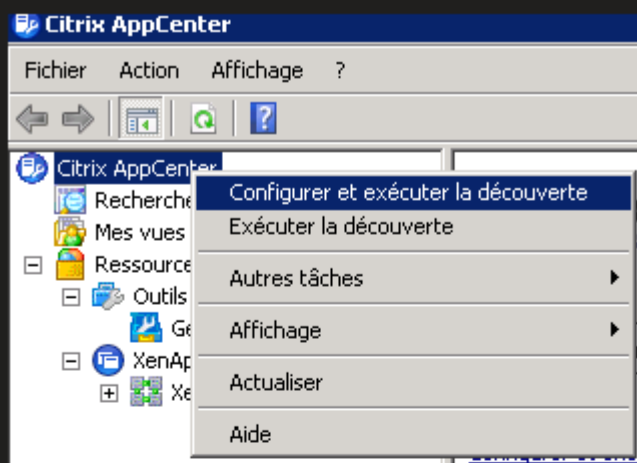
VDA1

Nom ↓	Machines	Priorité
LYOV-SBCA	1 sur 6	0

CITRIX

Citrix AppCenter

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



Configurer et exécuter la découverte



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



Bienvenue

Étapes

► Bienvenue

Ceci est l'assistant de découverte de la console AppCenter. Il vous guidera au travers du processus de découverte.

Avant d'utiliser AppCenter, vous devez exécuter la découverte pour établir le contact entre les

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](#)

Download the APM agent

Download the agent jar from [Maven Central](#). Do not add the agent as a dependency to your application.

Start your application with the javaagent flag

Add the `-javaagent` flag and configure the agent with system properties.

- Set the required service name (allowed characters: a-z, A-Z, 0-9, -, _, and space)
- Set the custom APM Server URL (default: `http://localhost:8200`)
- Set the APM Server secret token
- Set the service environment
- Set the base package of your application


Configuration setting	Configuration value
-----------------------	---------------------

Configuration setting	Configuration value
Delastic.apm.service_name	my-service-name
Delastic.apm.secret_token	nv32xNSLMjK80VI793
Delastic.apm.server_url	https://3608c6cb2bb74c299668d92e02aeef8.lo gaas.idfm-ob.fr:9243
Delastic.apm.environment	my-environment

```
1 | java -javaagent:/path/to/elastic-apm-agent-<version>.jar \  
2 | -Delastic.apm.service_name=my-service-name \  
3 | -Delastic.apm.secret_token=nv32xNSLMjK80VI793 \  
4 | -Delastic.apm.server_url=https://3608c6cb2bb74c299668d92e02aeef8.logaas.idfm-  
  | ob.fr:9243 \  
5 | -Delastic.apm.environment=my-environment \  
6 | -Delastic.apm.application_packages=org.example \  
7 | -jar my-service-name.jar
```

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

✓




Ruby on Rails
Configure instrumentation for Ruby on Rails applications.

Install the APM agent

Add the agent to your Gemfile.

```
gem 'elastic-apm'
```



Configure the agent

APM is automatically started when your app boots. Configure the agent, by creating the config file
`config/elastic_apm.yml`

Configuration setting	Configuration value
service_name	my-service-name
secret_token	nv32xNSLMjK80VI793
server_url	https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243
environment	my-environment

```
1 | # config/elastic_apm.yml:
2 |
3 | i service_name: 'my-service-name'
4 |
5 | i secret_token: 'nv32xNSLMjK80VI793'
6 |
7 | i server_url: 'https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243'
8 |
9 | i environment: 'my-environment'
```



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

2 Edit the configuration

If you're using an X-Pack secured version of Elastic Stack, you must specify credentials in the `apm-server.yml` config file.

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: <username>
  password: <password>
```



3 Start APM Server

The server processes and stores application performance metrics in Elasticsearch.

```
Start-Service apm-server
```



4 APM Server status

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



.NET

.NET

Configure instrumentation for .NET applications.

Download the APM agent

Add the the agent package(s) from [NuGet](#) to your .NET application. There are multiple NuGet packages available for different use cases.

For an ASP.NET Core application with Entity Framework Core download the [Elastic.Apm.NetCoreAll](#) package. This package will automatically add every agent component to your application.

In case you would like to minimize the dependencies, you can use the [Elastic.Apm.AspNetCore](#) package for just ASP.NET Core monitoring or the [Elastic.Apm.EfCore](#) package for just Entity Framework Core monitoring.

In case you only want to use the public Agent API for manual instrumentation use the [Elastic.Apm](#) package.

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://3608c6cb2bb74c299668d92e02aeef8.logaas.idfm-ob.fr:9243
Environment	my-environment

```
1 {
2   "ElasticApm": {
3     "ServiceName": "my-service-name",
4     "SecretToken": "nv32xNSLMjK80VI793",
5     "ServerUrl": "https://3608c6cb2bb74c299668d92e02aeef8.logaas.idfm-ob.fr:9243",
6     "Environment": "my-environment",
7   }
8 }
```



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

```
1 // Add this to the very top of the first file loaded in your app
2 var apm = require('elastic-apm-node').start({
3   serviceName: 'my-service-name',
4
5   secretToken: 'nv32xNSLMjK80VI793',
6
7   serverUrl: 'https://3608c6cb2bb74c299668d92e02aeeef8.logaas.idfm-ob.fr:9243',
8
9   environment: 'my-environment'
10 })
```



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
```

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
```

```
$ /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  
// Clearing the cache for the prod environment with debug false  
// Removing old cache directory...  
// Finished  
[OK] Cache for the "prod" environment (debug=false) was successfully cleared.  
// Clearing cache pool: cache.redis  
[OK] Cache was successfully cleared.
```

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](#)