IBM Z Workload Scheduler Agent

10.2.4 pour MS Windows

**CAGIP**

**GEA/OPS/XPR**

**01.57.72.12.03**

**02/09/2025**

STEVE FREMOND

Mode opératoire d’installation d’IBM Z Workload Scheduler Agent 10.2.4 sous OS MS Windows

Sommaire

[1 Prérequis 2](#_Toc209710497)

[2 Certificat et clé privé 2](#_Toc209710498)

[3 Installation 2](#_Toc209710499)

[4 Firewall 3](#_Toc209710500)

Lien documentation IBM en ligne :

<https://www.ibm.com/docs/fr/workload-automation/10.2.4?topic=ssf-customizing-ssl-connection-z-controller-when-using-your-certificates-saf>

<https://www.ibm.com/docs/en/workload-automation/10.2.4?topic=twsinst->

# Prérequis

Déposer l’archive contenant les binaires d’installation (10.2.4-IWS-ZAGENT-WINDOWS.zip) sur la VM cible dans l’arborescence de votre choix.  
Dans ce document nous utiliserons comme arborescence source « D:\Zinstall\IBM »

Depuis la version 10.2.3, l’agent nécessite la mise en œuvre d’un magasin de clé de sécurité même dans le cas d’usage d’une communication non sécurisé entre l’ordonnanceur et l’agent.

Dans de document nous allons utiliser une clé autosigné (voir [Chapitre 2](#_Certificat_et_clé)), il est pour cela nécessaire de disposer d’openssl sur la VM cible.

Il est possible d’utiliser openssl fournit par l’agent, mais il nécessitera une première tentative d’installation de l’agent qui échouera, et devra être relancé par la suite .

# Certificat et clé privé

1. Ouvrir une fenêtre de commande
2. Exécuter :

set ZcRootDir=d:\apps\IBM\TWA

mkdir "%ZcRootDir%\TWS\ssl\depot

cd "%ZcRootDir%\TWS\ssl\depot

# Si utilisation d’openssl fournit par l’agent

set openssl=%ZcRootDir%\TWS\bin\openssl.exe

set OPENSSL\_CONF=%ZcRootDir%\TWS\ssl\openssl.cnf

# Si utilisation d’openssl fournit par l’agent remplacer « openssl » par « %openssl% » dans toutes les commandes ci-dessous.

openssl genrsa -out ca.key 4096

openssl req -x509 -new -nodes –key ca.key -subj "/CN=ZcentricAgent" -days 3650 -out ca.crt

openssl genrsa -des3 -out tls.key 4096

# Repondre et confirmer la pass phrase celle-ci sera à utiliser comme valeur de l’argument -sslpassword à l’installation

openssl req -new -key tls.key -out tls.csr

# Repondre et confirmer la Pass Phrase identique à celle utilisée ci-dessus

# Repondre Country (FR)

# Repondre State (FRANCE)

# Repondre City (PARIS)

# Repondre Organization (CAGIP)

# Repondre Organization Unit Name (nom de l’équipe responsable)

# Repondre Common Name (fqdn du serveur)

# Repondre Email Address (\*\*\*\*\*@ca-gip.fr)

# Repondre Password ()

# Repondre Optionnal Company Name ()

openssl x509 -req -in tls.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out tls.crt -extfile %OPENSSL\_CONF% -extensions v3\_req

# Installation

1. Ouvrir une fenêtre de commande
2. Exécuter :

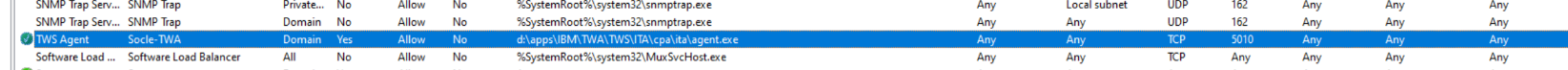
set ZcRootDir=d:\apps\IBM\TWA

cd /D D:\Zinstall\IBM\10.2.4-IWS-ZAGENT-WINDOWS\TWS\WINDOWS\_X86\_64

# Remplacer les astérisques ci-dessous par les mots de passe correspondant

cscript twsinst.vbs -new -skipcheckprereq -uname CAA01\00svczc1 -password \*\*\*\*\*\*\* -acceptlicense yes -addjruntime false -hostname %COMPUTERNAME% -displayname %COMPUTERNAME% -jmport 5010 -jmportssl false -inst\_dir "%ZcRootDir%" -sslkeysfolder "%ZcRootDir%\TWS\ssl\depot" -sslpassword \*\*\*\*\*\*\*

# Firewall

Une règle, au niveau du firewall de la VM, doit être ajoutée comme suit :

Via une fenêtre powershell en tant qu’administrateur, executer:  
*New-NetFirewallRule -DisplayName "TWS Agent" -Direction Inbound -Program "D:\Apps\IBM\TWA\TWS\ITA\cpa\ita\agent.exe" -RemoteAddress Any -Profile Domain -Action Allow -Protocol TCP -LocalPort 5010*

**FIN DE DOCUMENT**

**\*\*\*\*\*\*\*\*\*\***