

IBM Rational Developer for z Systems  
Version 9.5.1

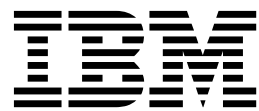
*Guide de référence de configuration de  
l'hôte*





IBM Rational Developer for z Systems  
Version 9.5.1

*Guide de référence de configuration de  
l'hôte*



**Remarque**

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 61.

**Première édition - novembre 2015**

Réf. US : SC27-8578-00

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.ibm.com/ca/fr> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France  
Direction Qualité  
17, avenue de l'Europe  
92275 Bois-Colombes Cedex*

| Cette édition concerne IBM Rational Developer for z Systems version 9.5 (numéro de logiciel 5724-T07 ou une partie  
| du numéro de programme 5697-CDT) et toutes les éditions et modifications ultérieures, sauf mention contraire dans  
| les nouvelles éditions.

Note to U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Copyright IBM Corporation 2015, 2015.

# Table des matières

<b>Figures</b> . . . . .	<b>v</b>
<b>Tableaux</b> . . . . .	<b>vii</b>
<b>Avis aux lecteurs canadiens.</b> . . . .	<b>ix</b>
<b>A propos de ce manuel</b> . . . . .	<b>xi</b>
A qui s'adresse ce guide . . . . .	xii
Récapitulatif des changements . . . . .	xii
Description du contenu du document . . . . .	xiv
Description de Developer for z Systems . . . . .	xiv
Remarques relatives à la sécurité . . . . .	xiv
Remarques relatives à TCP/IP . . . . .	xiv
Remarques relatives à WLM . . . . .	xiv
Remarques relatives à la fonction d'envoi au client . . . . .	xv
Remarques relatives à CICSTS . . . . .	xv
Configuration de AT-TLS . . . . .	xv

## IBM Rational Developer for System z - Guide de référence de configuration de l'hôte . . . . . 1

<b>Chapitre 1. Description de Developer for z Systems</b> . . . . .	<b>3</b>
Présentation du composant . . . . .	3
Propriétaires de tâches . . . . .	4
Débogueur intégré . . . . .	6
CARMA . . . . .	7
Fichiers de configuration CARMA . . . . .	8
CRASTART . . . . .	8
Soumission par lots . . . . .	8
Structure de répertoires z/OS UNIX . . . . .	9

<b>Chapitre 2. Remarques relatives à la sécurité</b> . . . . .	<b>11</b>
Méthodes d'authentification . . . . .	11
Authentification du gestionnaire de débogage . . . . .	11
Sécurité des connexions . . . . .	12
Communication chiffrée pour le débogueur intégré . . . . .	12
Sécurité du débogage . . . . .	13
CICSTS, sécurité . . . . .	13
SCLM, sécurité . . . . .	13
Définitions de sécurité . . . . .	14
Configuration requise et liste de contrôle . . . . .	14
Activation des paramètres et des classes de sécurité . . . . .	15
Définition d'un segment OMVS pour les utilisateurs Developer for z Systems . . . . .	16
Définition des tâches démarrées de Developer for z Systems . . . . .	16

Définition du gestionnaire de débogage en tant que serveur sécurisé z/OS UNIX . . . . .	16
Définition des bibliothèques contrôlées par un programme MVS pour le gestionnaire de débogage . . . . .	17
Définition de la prise en charge de passticket pour RSE . . . . .	18
Définition du droit d'accès aux fichiers z/OS UNIX pour RSE . . . . .	19
Définition de la protection des applications pour RSE . . . . .	19
Définition de fichiers contrôlés par programme z/OS UNIX pour RSE . . . . .	20
Définition de la sécurité des commandes JES . . . . .	20
Définition de l'accès au débogueur intégré . . . . .	22
Définition des profils de fichier . . . . .	22
Vérification des paramètres de sécurité . . . . .	23

<b>Chapitre 3. Remarques relatives à TCP/IP</b> . . . . .	<b>25</b>
Ports TCP/IP . . . . .	25
Communications externes . . . . .	25
Communication interne . . . . .	26
Réservation de port TCP/IP . . . . .	27
CARMA et TCP/IP . . . . .	27
CARMA et ports TCP/IP . . . . .	27
CARMA et affinité entre piles . . . . .	27
crastart*.conf . . . . .	28
CRASUB* . . . . .	28

<b>Chapitre 4. Remarques relatives à WLM</b> 29	
Classification des charges de travail . . . . .	29
Règles de classification . . . . .	30
Définition des objectifs . . . . .	31
Remarques relatives à la sélection des objectifs . . . . .	32
STC . . . . .	33
OMVS . . . . .	33
JES . . . . .	34

<b>Chapitre 5. Remarques relatives à la fonction d'envoi au client.</b> . . . .	<b>37</b>
Introduction . . . . .	37
Projets résidant sur l'hôte . . . . .	38

<b>Chapitre 6. Remarques relatives à CICSTS</b> . . . . .	<b>41</b>
Prise en charge de langues bidirectionnelles . . . . .	41
Messages IRZ de diagnostic pour Enterprise Service Tools . . . . .	41
Débogage de transactions CICS . . . . .	41

<b>Chapitre 7. Configuration de AT-TLS</b> ..	<b>43</b>
Configuration de syslogd . . . . .	44
Configuration AT-TLS dans PROFILE.TCPIP . . . . .	44

Tâche démarrée par l'agent de règles . . . . .	44
Configuration de l'agent de règles . . . . .	45
Règle AT-TLS. . . . .	45
Remarques relatives à TLS v1.2. . . . .	47
Mises à jour de sécurité AT-TLS . . . . .	48
Activation de la règle AT-TLS . . . . .	50

## **Bibliographie . . . . . 53**

Publications référencées . . . . .	53
Publications d'information . . . . .	54

## **Glossaire. . . . . 57**

## **Remarques . . . . . 61**

Documentation sur l'interface de programmation ..	63
---	----

Marques . . . . .	63
Conditions d'utilisation de la documentation du produit . . . . .	63
Licence de copyright . . . . .	64
Marques . . . . .	64

## **Index . . . . . 67**

---

## Figures

1.	Présentation du composant. . . . .	3		6.	Règle AT-TLS pour le gestionnaire de	
2.	Propriétaires de tâches . . . . .	5		débogage . . . . .		12
3.	Débogueur intégré . . . . .	6		7.	Ports TCP/IP . . . . .	25
4.	Flux CARMA . . . . .	7		8.	Classification WLM . . . . .	29
5.	Structure de répertoires z/OS UNIX . . . . .	9				





---

## Tableaux

1. Informations SAF pour les fonctions de débogage . . . . .	13		6. Qualificateurs de travaux WLM. . . . .	31
2. Variables de configuration de la sécurité . . . . .	14		7. Charges de travail WLM . . . . .	32
3. Commandes d'opérateur du moniteur de travaux JES2 . . . . .	21		8. Charges de travail et STC WLM. . . . .	33
4. Commandes d'opérateur du moniteur de travaux JES3 . . . . .	21		9. Charges de travail - OMVS WLM . . . . .	33
5. Sous-systèmes de point d'entrée WLM . . . . .	30		10. Charge de travail - JES WLM . . . . .	34
			11. Publications référencées . . . . .	53
			12. Sites Web référencés. . . . .	54
			13. Publications d'information . . . . .	54



---

## Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

### Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

### Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

### Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.








### OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

### Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Pos1)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

## Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

## Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

---

## A propos de ce manuel

Ce document fournit des informations de base sur les différentes tâches de configuration d'IBM® Rational Developer for z Systems, ainsi que d'autres composants et produits z/OS (tels que WLM et TCP/IP).

A partir de maintenant, les noms suivants sont utilisés dans le présent ouvrage :

- *IBM Explorer for z/OS* est appelé *z/OS Explorer*.
- *IBM Rational Developer for z Systems* a pour nom *Developer for z Systems*.
- *IBM Rational Developer for z Systems Integrated Debugger* est appelé *débogueur intégré*.
- L'abréviation utilisée pour *Common Access Repository Manager* est *CARMA*.
- *Software Configuration and Library Manager Developer Toolkit* est appelé *SCLM Developer Toolkit* et parfois abrégé en *SCLMDT*.
- *z/OS UNIX System Services* est appelé *z/OS UNIX*.
- *Customer Information Control System Transaction Server* est appelé *CICSTS*, abrégé en *CICS*.

Ce document fait partie d'un groupe de documents qui décrivent la configuration de l'hôte *Developer for z Systems*. Chacun de ces documents s'adresse à des utilisateurs spécifiques. Il est inutile de lire tous les documents pour configurer *Developer for z Systems*.

- Le manuel *IBM Rational Developer for z Systems - Guide de configuration hôte* (SC27-8577) décrit en détails toutes les tâches de planification, les tâches de configuration et les options (y compris les options facultatives) et offre des scénarios de remplacement.
- Le manuel *IBM Rational Developer for z Systems - Guide de référence de la configuration hôte* (SC43-2902) décrit la conception de *Developer for z Systems* et fournit des informations connexes sur les diverses tâches de configuration de *Developer for z Systems*, sur les composants z/OS et autres produits (tels que WLM et TCP/IP) associés à *Developer for z Systems*.
- Le manuel *IBM Rational Developer for z Systems - Guide de démarrage rapide de la configuration hôte* (GI11-9201) décrit la configuration minimale de *Developer for z Systems*.

Les informations contenues dans ce document s'appliquent à tous les modules IBM Rational Developer for z Systems version 9.5.1.

Vous trouverez les versions les plus à jour de ce document dans le manuel *IBM Rational Developer for z Systems - Guide de référence de la configuration hôte* (SC43-2902) disponible à l'adresse <http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss?CTY=US&FNC=SRX&PBL=SC27-8578>.

Les versions les plus récentes de la documentation complète, y compris les instructions d'installation, les livres blancs, les podcasts et les tutoriels, sont disponibles sur la page de la bibliothèque du site Web IBM Rational Developer for z Systems ([http://www-01.ibm.com/software/sw-library/en\\_US/products/Z964267S85716U24/](http://www-01.ibm.com/software/sw-library/en_US/products/Z964267S85716U24/)).

---

## A qui s'adresse ce guide

Ce document s'adresse aux programmeurs système chargés de configurer et d'optimiser IBM Rational Developer for z Systems version 9.5.1.

Bien que les étapes de configuration soient décrites dans une autre publication, ce document décrit en détail les sujets associés, tels que l'optimisation, la configuration de la sécurité etc. Avant d'utiliser le présent manuel, vous devez maîtriser les systèmes hôtes z/OS UNIX System Services et MVS.

---

## Récapitulatif des changements

Cette section récapitule les modifications apportées au manuel *IBM Rational Developer for z Systems version 9.5.1 - Guide de référence de la configuration hôte*, SC43-2902-00 (mis à jour en décembre 2015).

Les changements et ajouts techniques au texte et illustrations sont indiqués par un trait vertical situé à gauche du changement.

Nouvelles informations :

- Utilisation de nouveaux noms de fichiers MVS et de nouveaux chemins z/OS UNIX

Informations supprimées :

Dans la version 9.5.1, les fonctions liées à RSE et au moniteur de tâches JES ont été déplacées d'IBM Rational Developer for z Systems vers IBM Explorer for z/OS. Ce déplacement inclut la documentation connexe.

- Les données spécifiques de RSE sont supprimées de tous les chapitres
- Les données spécifiques du moniteur de travaux JES sont supprimées de tous les chapitres
- Les données spécifiques du service de commandes TSO sont supprimées de tous les chapitres
- Les données relatives à la fonction d'envoi au client par la commande push (Push-to-client) pour la gestion de la configuration et des versions sont supprimées de tous les chapitres
- La documentation sur la façon de configurer TCP/IP est supprimée

Ce document reprend des informations présentées précédemment dans le document *IBM Rational Developer for z Systems version 9.5 - Guide de référence de la configuration hôte*, SC14-7290-09.

Nouvelles informations :

- Documentation des vérifications de sécurité pour la nouvelle fonction d'envoi de messages. Voir Sécurité de l'envoi de messages
- Ajout de détails sur les commandes de l'opérateur JES utilisées. Voir Actions sur les travaux - Limitations liées à l'exécution
- Ajout d'informations sur les limitations relatives au nom de groupe d'envoi au client par commande push. Voir Limitations relatives aux noms de groupe
- Ajout d'informations sur les limitations relatives à SYSPLEX. Voir SYSPLEX
- Ajout d'informations sur la gestion des protocoles de chiffrement et des chiffrements. Voir Gestion des protocoles de chiffrement et des chiffrements

- Ajout d'instructions pour une configuration multiserveur simple. Voir Niveaux de logiciel identiques, fichiers de configuration différents

Informations supprimées :

- Le gestionnaire de déploiement d'application n'est plus mis à disposition ; par conséquent, toutes les informations le concernant ont été supprimées.

Ce document reprend des informations présentées précédemment dans le document *IBM Rational Developer for System z version 9.1.1 - Guide de référence de la configuration hôte*, SC14-7290-08.

Nouvelles informations :

- Mise à jour des profils de sécurité du débogueur intégré. Voir «Sécurité du débogage», à la page 13.
- Ajout d'informations sur la prise en charge de phrase de passe. Voir «Méthodes d'authentification», à la page 11.

Ce document reprend des informations présentées précédemment dans le manuel *IBM Rational Developer for System z version 9.1.1 - Guide de référence de configuration de l'hôte*, SC11-6869-07.

Nouvelles informations :

- Ajout d'informations sur la sécurité des fichiers journaux. Voir Sécurité des fichiers journaux.
- Ajout d'informations sur le support de groupe pour le rejet de mises à jour de la fonction d'envoi au client par commande push. Voir Groupes de développeurs multiples.
- Mise à jour des informations sur l'utilisation des ressources. Voir Remarques relatives à l'optimisation.
- Mise à jour des informations relatives aux fichiers journaux et à la fonction de trace. Voir Traitement des incidents de configuration.

Ce document reprend des informations présentées précédemment dans le document *IBM Rational Developer for System z Version 9.0.1 - Guide de référence de configuration de l'hôte*, SC11-6869-06.

Nouvelles informations :

- Ajout d'informations sur la configuration d'AT-TLS. Voir Chapitre 7, «Configuration de AT-TLS», à la page 43.

Ce document reprend des informations présentées précédemment dans le document *IBM Rational Developer for System z Version 9.0.1 - Guide de référence de configuration de l'hôte*, SC11-6869-06.

Nouvelles informations :

- Ajout d'informations sur les noms de fichier journal avec horodatage. Voir Fichiers journaux.
- Ajout d'informations sur de nouveaux événements auditable. Voir Données d'audit.

Ce document contient des informations présentées précédemment dans le manuel *IBM Rational Developer for System z version 9.0 - Guide de référence de la configuration hôte*, SC14-7290-04.

Nouvelles informations :

- Mise à jour de l'utilisation du port TCP/IP. Voir «Ports TCP/IP», à la page 25.
- Ajout d'un exemple pour la synchronisation automatique de 2 démons RSE. Voir Synchronisation automatique.
- Ajout d'informations sur de nouveaux fichiers journaux. Voir Fichiers journaux.

Ce document reprend des informations présentées précédemment dans le manuel *IBM Rational Developer for System z version 8.5.1 - Guide de référence de configuration de l'hôte*, SC11-6869-04.

Nouvelles informations :

- Ajout d'informations sur les profils SAF permettant de modifier les fonctions client. Voir Modification des fonctions client.
- Mise à jour des numéros d'utilisation des ressources. Voir Remarques relatives à l'optimisation
- Mise à jour de la valeur par défaut du nombre maximal d'utilisateurs par pool d'unités d'exécution. Voir Remarques relatives à l'optimisation.

Ce document reprend des informations présentées précédemment dans le document *IBM Rational Developer for System z Version 8.5 - Guide de référence de configuration de l'hôte*, SC11-6869-02.

Nouvelles informations :

- Mise à jour des informations relatives à la sécurité du gestionnaire de travaux JES. Voir Chapitre 2, «Remarques relatives à la sécurité», à la page 11.
- Informations supplémentaires sur les exits utilisateur. Voir Considérations relatives aux exits utilisateur.

---

## Description du contenu du document

Cette section récapitule les informations présentées dans ce document.

### Description de Developer for z Systems

Les différents composants de l'hôte Developer for z Systems interagissent pour offrir au client un accès à des services et des données d'hôte. En comprenant bien la conception de ces composants, vous pouvez prendre les bonnes décisions de configuration.

### Remarques relatives à la sécurité

Developer for z Systems interagit avec d'autres composants hôte, cela ayant des implications en matière de sécurité.

### Remarques relatives à TCP/IP

Developer for z Systems repose sur le protocole TCP/IP pour offrir l'accès au mainframe à des utilisateurs travaillant sur un poste de travail autre qu'un mainframe. TCP/IP sert également à assurer la communication entre les différents composants et les autres produits.

### Remarques relatives à WLM

Contrairement aux applications z/OS traditionnelles, Developer for z Systems n'est pas une application monolithique qui peut être identifiée facilement au niveau du Workload Manager (WLM). Les différents composants de Developer for z Systems



interagissent pour offrir au client un accès à des services et des données d'hôte. Certains de ces services sont actifs dans différents espaces adresse, ce qui se traduit par différentes classifications WLM.

## **Remarques relatives à la fonction d'envoi au client**

Developer for z Systems étend la fonction d'envoi au client via la commande push (push-to-client) z/OS Explorer ou le contrôle client basé sur l'hôte à l'aide des définitions de projet.

## **Remarques relatives à CICSTS**

Ce chapitre contient des informations utiles pour un administrateur CICS Transaction Server.

## **Configuration de AT-TLS**

Cette section vous aide à résoudre certains problèmes susceptibles de se produire lors de la configuration d'AT-TLS (Application Transparent Transport Layer Security) ou pendant la vérification ou la modification d'une configuration existante.



---

# **IBM Rational Developer for System z - Guide de référence de configuration de l'hôte**



---

## Chapitre 1. Description de Developer for z Systems

Les différents composants de l'hôte Developer for z Systems interagissent pour offrir au client un accès à des services et des données d'hôte. En comprenant bien la conception de ces composants, vous pouvez prendre les bonnes décisions de configuration.

Les rubriques suivantes sont traitées dans le présent chapitre :

- «Présentation du composant»
- «Propriétaires de tâches», à la page 4
- «Débogueur intégré», à la page 6
- «CARMA», à la page 7
- «Structure de répertoires z/OS UNIX», à la page 9

Developer for z Systems se construit par-dessus IBM Explorer for z/OS. Pour plus d'informations sur z/OS Explorer, voir la section concernant les remarques relatives à la sécurité dans le manuel *IBM Explorer for z/OS - Guide de référence de la configuration hôte* (SC27-8438).

---

### Présentation du composant

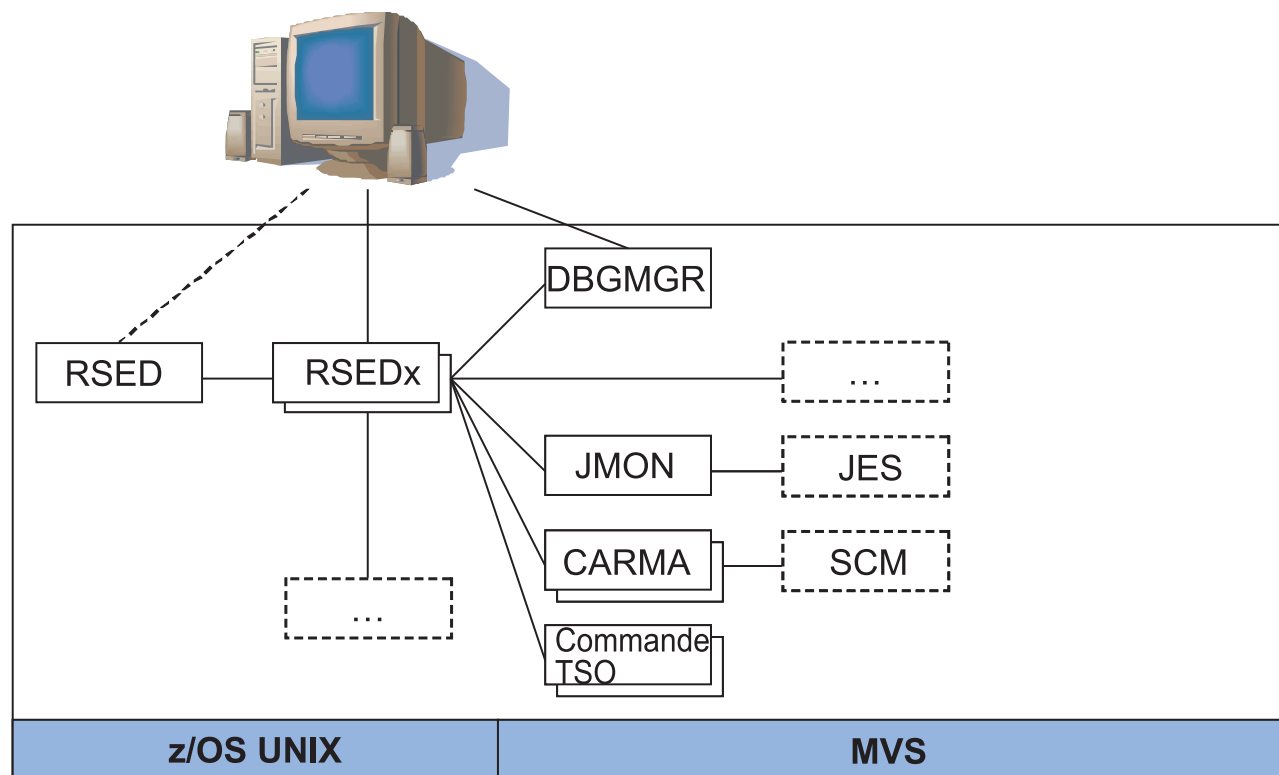


Figure 1. Présentation du composant

La figure 1 illustre une présentation générale de l'association z/OS Explorer et Developer for z Systems sur votre système hôte.

- L'Explorateur de systèmes distants (RSE) fournit des services de base, comme la connexion du client à l'hôte et le démarrage d'autres serveurs pour des services spécifiques. RSE se compose de deux entités logiques :
  - Le démon RSE (RSED), qui gère la configuration de la connexion. Il est également en charge de l'exécution en mode serveur unique. Pour se faire, le démon RSE crée un ou plusieurs processus enfants appelés pools d'unités d'exécution RSE (RSEDx).
  - Le serveur RSE qui gère les demandes client individuelles. Un serveur RSE est actif comme une unité d'exécution à l'intérieur d'un pool d'unités d'exécution RSE.
- Le gestionnaire de débogage (DBGMGR) coordonne l'activité du débogueur intégré.
- (z/OS Explorer) Le service de Commandes TSO (TSO cmd) offre une interface de type par lots pour les commandes TSO et ISPF.
- (z/OS Explorer) Le moniteur de travaux JES (JMON) fournit tous les services liés à JES.
- Common Access Repository Manager (CARMA) offre une interface permettant d'interagir avec les gestionnaires d'accès au référentiel (SCM), comme CA Endevor.
- Plusieurs services sont disponibles. Ils peuvent être fournis par Developer for z Systems ou par d'autres logiciels corequis.

La description du paragraphe et de la liste précédent illustre le rôle central attribué à RSE. A quelques exceptions près, toute la communication du client passe par RSE. Cela permet de faciliter la configuration du réseau liée à la sécurité, étant donné que seul un ensemble limité de ports est utilisé pour la communication hôte-client.

Pour gérer les connexions et charges de travail provenant des clients, RSE est composé d'un espace adresse de démon, qui permet de contrôler les espaces adresse du groupe d'unités d'exécution. Le démon agit comme un point focal pour la connexion et la gestion, alors que les pools d'unités d'exécution traitent les charges de travail du client. Selon les valeurs définies dans le fichier de configuration `rse.env` et la quantité de connexions client réelles, le démon peut démarrer plusieurs espaces adresse de pool d'unités d'exécution.

---

## Propriétaires de tâches

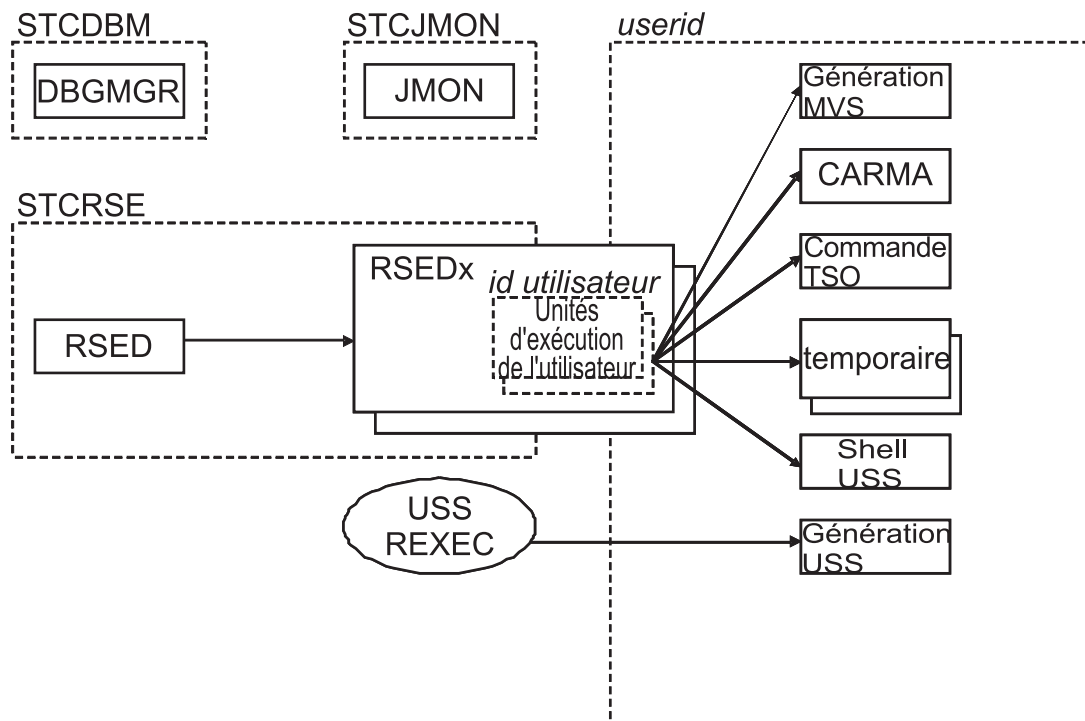


Figure 2. Propriétaires de tâches

La figure 2 offre une présentation de base du propriétaire des droits d'accès de sécurité utilisés pour les différentes tâches de z/OS Explorer et Developer for z Systems.

La propriété d'une tâche peut être divisée en deux sections. Les tâches démarrées appartiennent à l'ID utilisateur qui est attribué à la tâche démarrée dans le logiciel de sécurité. Toutes les autres tâches, avec les pools d'unités d'exécution RSE (RSEDx) comme exception, appartiennent à l'ID utilisateur du client.

La figure 2 présente les tâches démarrées de z/OS Explorer et Developer for z Systems (DBGMR, JMON et RSED), ainsi que des exemples de tâches démarrées et des services système avec lesquels Developer for z Systems communique. La balise USS REXEC représente le service z/OS UNIX REXEC (ou SSH).

Le démon RSE (RSED) crée un ou plusieurs espaces adresse de pools d'unités d'exécution (RSEDx) dédiés aux demandes des clients. Chaque pool d'unités d'exécution RSE prend en charge plusieurs clients et appartient au même utilisateur que celui du démon RSE. Chaque client possède sa propre unité d'exécution au sein d'un pool d'unités d'exécution et ces unités d'exécution appartiennent à l'ID utilisateur client.

Selon les actions menées par le client, un ou plusieurs espaces adresse supplémentaires peuvent être démarrés, tous appartenant à l'ID utilisateur du client, pour exécuter l'action demandée. Ces espaces adresse peuvent être un travail par lots MVS, une transaction APPC ou un processus enfant z/OS UNIX. Notez qu'un processus enfant z/OS UNIX est actif dans un initiateur z/OS UNIX (BPXAS) et le processus enfant apparaît comme une tâche démarrée dans JES.

La création de ces espaces adresse est le plus souvent déclenchée par une unité d'exécution d'utilisateur dans un pool d'unités d'exécution, soit directement soit à

l'aide d'un service système comme ISPF. L'espace adresse pourrait très bien être aussi créé par un tiers. Par exemple, REXEX ou SSH z/OS UNIX est impliqué lorsque un démarrage est généré dans z/OS UNIX.

Les espaces adresse spécifiques de l'utilisateur prennent fin à l'achèvement de la tâche ou à l'expiration d'un temps d'inactivité. Les tâches démarrées restent actives. Les espaces adresse répertoriés dans la figure 2, à la page 5 restent dans le système suffisamment longtemps pour être visibles. Toutefois, sachez qu'en raison de la conception de z/OS UNIX, il existe aussi des espaces adresses temporaires de durée de vie courte.

## Débogueur intégré

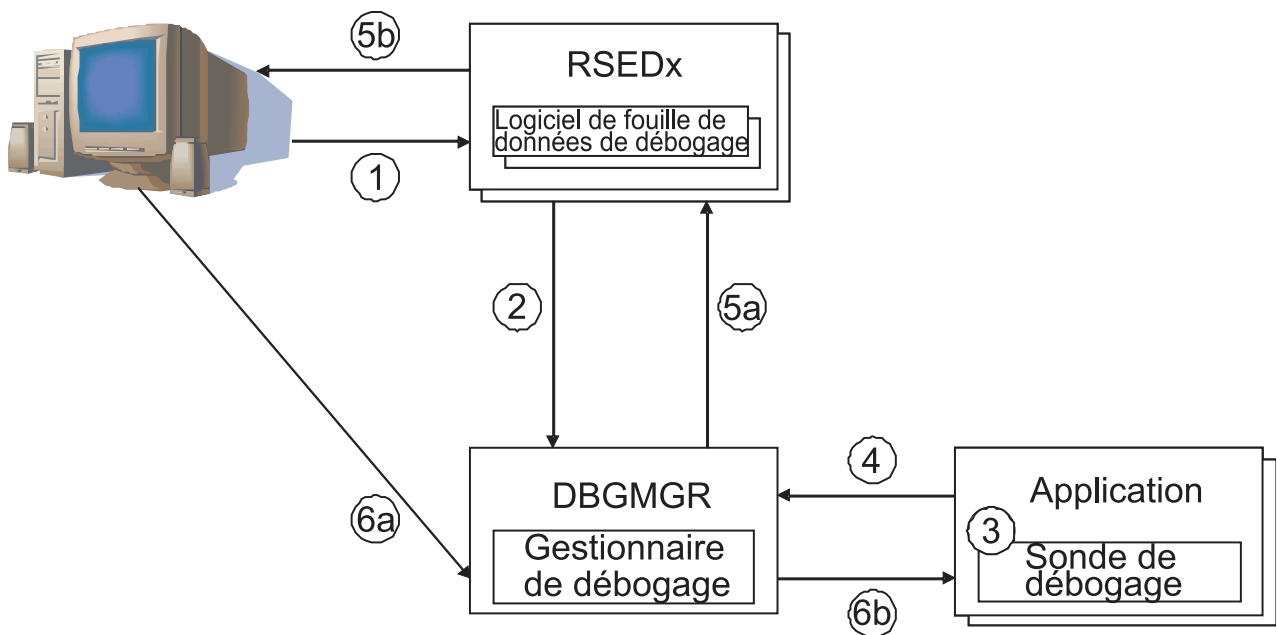


Figure 3. Débogueur intégré

Le débogueur intégré permet de déboguer différentes applications. La figure 5 montre une présentation schématique de la manière dont un client Developer for z Systems peut déboguer une application.

1. Le client se connecte à l'hôte à l'aide des informations de connexion Developer for z Systems normales.
2. Dans le cadre de la connexion, un logiciel de fouille de données de débogage enregistre l'utilisateur auprès du gestionnaire de débogage, qui est actif dans la tâche démarrée DBGMGR.
3. Lorsqu'une application est démarrée avec un indicateur signalant que celle-ci doit être déboguée, Language Environment (LE) appelle la sonde de débogage.
4. La sonde de débogage s'enregistre auprès du gestionnaire de débogage.



5. A l'aide du logiciel de fouille de données de débogage, le gestionnaire de débogage avertit le client Developer for z Systems de l'utilisateur qui reçoit cette session de débogage. Si l'utilisateur n'est pas enregistré à ce stade, la session de débogage se met en veille en attendant que l'utilisateur s'enregistre auprès du gestionnaire de débogage.
6. Le moteur de débogage dans le client contacte le gestionnaire de débogage qui à son tour transmet les données entre le moteur de débogage et la sonde de débogage dans les deux sens.

## CARMA

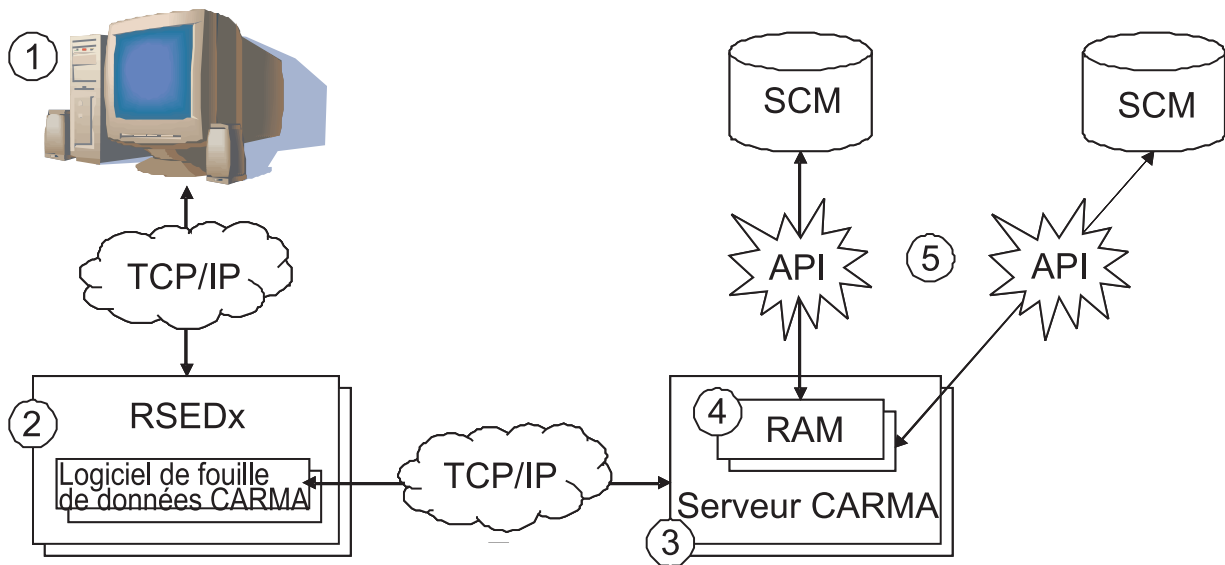


Figure 4. Flux CARMA

CARMA (Common Access Repository Manager) permet d'accéder à un SCM (Software Configuration Manager) basé sur un hôte, par exemple CA Endevor® SCM. La figure 4 explique schématiquement comment un client Developer for z Systems peut accéder à un SCM (Software Configuration Manager) de type hôte pris en charge.

1. Le client dispose d'un plug-in Common Access Repository Manager (CARMA).
2. Ce plug-in communique avec l'exploitant CARMA, actif comme unité d'exécution utilisateur dans le pool d'unités d'exécution RSE (RSEDx). Cette communication est établie par l'intermédiaire de la connexion RSE existante.
3. Lorsque le client demande l'accès à un SCM, l'exploitation CARMA se lie à un port TCP/IP et démarre un serveur CARMA utilisateur avec le numéro de port comme argument de démarrage. Le serveur CARMA se connecte ensuite à ce port et utilise ce chemin pour la communication avec le client. Notez que les SCM basés sur l'hôte s'attendent à ce que les espaces adresse d'utilisateur unique accèdent à leurs services, ce qui nécessite le démarrage par CARMA d'un serveur CARMA par utilisateur. Il n'est pas possible de créer un serveur unique prenant en charge plusieurs utilisateurs.
4. Le serveur CARMA charge le gestionnaire RAM (Repository Access Manager) qui prend en charge le SCM demandé.

5. Le gestionnaire RAM traite les informations techniques de l'interaction avec le SCM et présente une interface commune au client.

## Fichiers de configuration CARMA

Developer for z Systems prend en charge plusieurs méthodes pour démarrer un serveur CARMA. Chaque méthode offre des avantages, mais présente également des inconvénients. Developer for z Systems fournit également plusieurs RAM (Repository Access Managers) qui peuvent être divisés en deux groupes : RAM de production et RAM exemples. Diverses combinaisons de RAM et de méthodes de démarrage de serveur sont disponibles dans une installation préconfigurée.

Toutes les méthodes de démarrage de serveur ont un fichier de configuration commun, CRASRV.properties, qui définit, entre autres, la méthode de démarrage utilisée.

### CRASTART

La méthode "CRASTART" démarre le serveur CARMA sous la forme d'une sous-tâche dans RSE. Elle offre une configuration très flexible grâce à l'utilisation d'un fichier de configuration distinct qui définit les attributions de fichiers et les appels de programme nécessaires pour démarrer un serveur CARMA. Cette méthode offre les meilleures performances et utilise le moins de ressources mais requiert cependant que le module CRASTART se trouve dans LPA.

RSE appelle le module chargeable CRASTART qui utilise les définitions dans crastart\*.conf pour créer un environnement valide pour exécuter des commandes TSO et ISPF par lots. Developer for z Systems utilise cet environnement pour exécuter le serveur CARMA, CRASERV. Developer for z Systems fournit plusieurs fichiers crastart\*.conf, chaque fichier étant préconfiguré pour un gestionnaire donné.

### Soumission par lots

Cette méthode démarre le serveur CARMA en envoyant un travail. Il s'agit de la méthode par défaut utilisée dans les fichiers de configuration fournis. L'avantage de cette méthode est que les journaux CARMA sont facilement accessibles dans la sortie de travaux. Elle permet également d'utiliser un JCL de serveur personnalisé pour chaque développeur qui sera géré par le développeur lui-même. Toutefois, cette méthode utilise un initiateur JES pour chaque développeur qui démarre un serveur CARMA.

RSE appelle CLIST CRASUB\* qui envoie un document incorporé JCL pour créer un environnement valide pour exécuter des commandes TSO et ISPF par lots. Developer for z Systems utilise cet environnement pour exécuter le serveur CARMA, CRASERV. Developer for z Systems fournit plusieurs membres CRASUB\*, chaque membre étant préconfiguré pour un gestionnaire RAM donné.

## Structure de répertoires z/OS UNIX

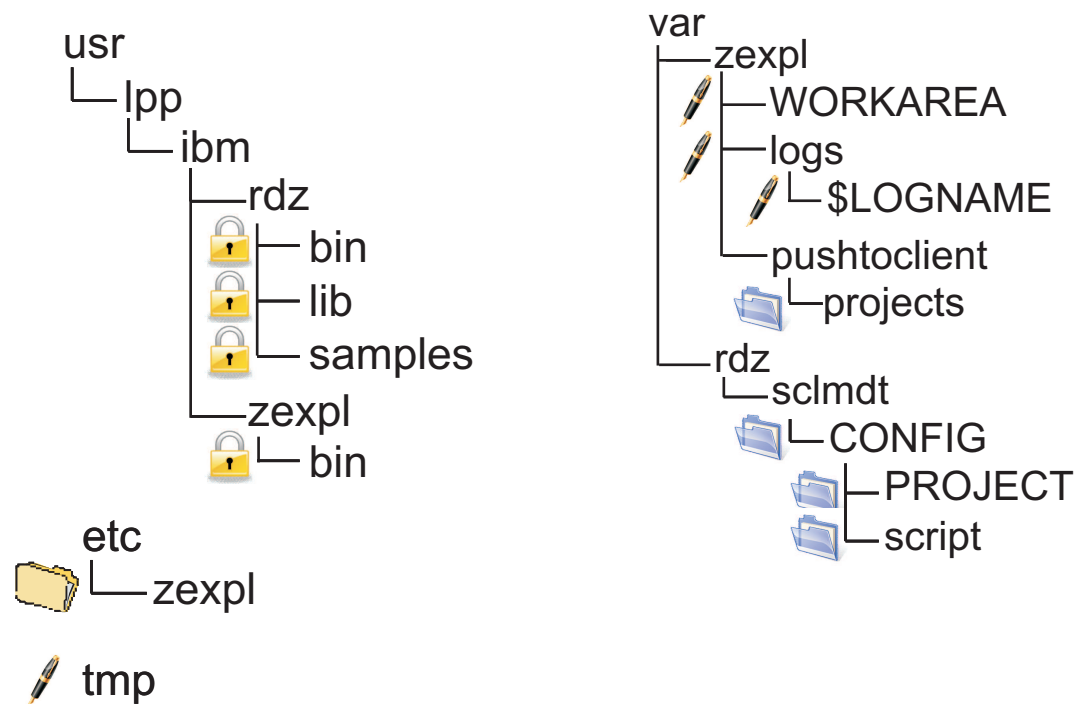


Figure 5. Structure de répertoires z/OS UNIX

La figure 5 présente les répertoires z/OS UNIX utilisés par Developer for z Systems. La liste suivante décrit chaque répertoire en contact avec Developer for z Systems, le mode de changement d'emplacement et qui gère les données qu'il contient.

- /usr/lpp/ibm/rdz/ est la racine du code produit Developer for z Systems. L'emplacement réel est spécifié dans le fichier de configuration rdz.env (variable RDZ\_HOME). Les fichiers sont gérés par SMP/E.
- Developer for z Systems place les fichiers dans /usr/lpp/ibm/zexpl/bin, le répertoire des fichiers binaires de z/OS Explorer. L'emplacement réel est spécifié dans la configuration z/OS Explorer. Les fichiers sont gérés par SMP/E.
- /etc/zexpl/ contient les fichiers de configuration z/OS Explorer et Developer for z Systems. L'emplacement réel est spécifié dans la tâche démarrée RSED (variable CNFG). Les fichiers sont gérés par le programmeur système.
- /tmp/ est utilisé par la passerelle ISPF existante pour stocker les données temporaires. Certains programmes de vérification de l'installation stockent leur sortie dans ce répertoire. Les fichiers qui s'y trouvent sont gérés par ISPF et les programmes IVP. L'emplacement peut être personnalisé à l'aide de la variable TMPDIR dans rse.env. Il s'agit également de l'emplacement par défaut des fichiers de vidage Java™, qui peuvent être personnalisés à l'aide de la variable \_CEE\_DUMPTARG de rse.env.

**Remarque :** /tmp/ requiert le masque de contrôle des données de droits 777 permettant à chaque client de créer des fichiers temporaires.

- /var/zexpl/WORKAREA/ est utilisé par la passerelle ISPF existante et par SCLMDT pour transférer des données entre z/OS UNIX et les espaces adresses basés sur MVS. L'emplacement réel est spécifié dans rse.env (variable CGI\_ISPWORK). Les fichiers sont gérés par ISPF et SCLMDT.

**Remarque :** /var/zexpl/WORKAREA/ requiert le masque de contrôle des bits de droit 777 permettant à chaque client de créer des fichiers temporaires. Developer for z Systems copie les messages de journal dans les fichiers journaux z/OS Explorer situés dans /var/zexpl/zexpl/logs/\$LOGNAME. L'emplacement réel est spécifié dans la configuration z/OS Explorer. Les fichiers qui s'y trouvent sont gérés par le code produit z/OS Explorer et Developer for z Systems.

- /var/rdz/sclmdt/CONFIG/ comporte les fichiers de configuration SCLMDT généraux. L'emplacement réel est spécifié dans rdz.env (variable SCLMDT\_CONF\_HOME). Les fichiers sont gérés par l'administrateur SCLM.
- /var/rdz/sclmdt/CONFIG/PROJECT/ comporte les fichiers de configuration du projet SCLMDT. L'emplacement réel est spécifié dans rdz.env (variable SCLMDT\_CONF\_HOME). Les fichiers sont gérés par l'administrateur SCLM.
- /var/rdz/sclmdt/CONFIG/script/ comporte les scripts associés à SCLMDT qui peuvent être utilisés par d'autres produits. L'emplacement réel n'est indiqué nulle part. Les fichiers sont gérés par l'administrateur SCLM.
- /var/rdz/pushtoclient/ contient les fichiers de configuration du client, les informations de mise à jour du produit client et les informations du projet résidant sur l'hôte envoyées au client lors de la connexion au système hôte. L'emplacement est défini dans pushtoclient.properties (variable pushtoclient.folder). Les fichiers qui s'y trouvent sont gérés par un administrateur de client Developer for z Systems.
- /var/rdz/pushtoclient/projects/ contient les fichiers de définition du projet résidant sur l'hôte. L'emplacement réel est spécifié dans le répertoire /var/rdz/pushtoclient/keymapping.xml, lequel est créé et géré par un administrateur de client Developer for z Systems. Les fichiers qui s'y trouvent sont gérés par un chef de projet ou un responsable du développement.

---

## Chapitre 2. Remarques relatives à la sécurité

Developer for z Systems étend les fonctionnalités de z/OS Explorer en fournissant des fonctions supplémentaires dont certaines interagissent avec d'autres composants et produits système (comme, par exemple, un gestionnaire SCM (Software Configuration Manager). Les définitions de sécurité propres à Developer for z Systems sont utilisées pour sécuriser les fonctions fournies.

Pour être efficaces, les mécanismes de sécurité utilisés par les serveurs et les services Developer for z Systems doivent reposer sur la sécurité des fichiers et systèmes de fichiers les contenant. Cela implique que seuls les administrateurs système habilités doivent pouvoir mettre à jour les bibliothèques de programmes et les fichiers de configuration.

Developer for z Systems se construit par-dessus IBM Explorer for z/OS. Pour plus d'informations sur z/OS Explorer, voir la section concernant les remarques relatives à la sécurité dans le manuel *IBM Explorer for z/OS - Guide de référence de la configuration hôte* (SC27-8438).

Les rubriques suivantes sont traitées dans le présent chapitre :

- «Méthodes d'authentification»
- «Sécurité des connexions», à la page 12
- «Sécurité du débogage», à la page 13
- «CICSTS, sécurité», à la page 13
- «SCLM, sécurité», à la page 13
- «Définitions de sécurité», à la page 14

---

### Méthodes d'authentification

#### Authentification de CARMA

L'authentification du client est effectuée par le démon RSE dans le cadre d'une demande de connexion client. CARMA est démarré à partir d'une unité d'exécution propre à l'utilisateur et hérite de l'environnement de sécurité de l'utilisateur en ignorant le besoin d'authentification supplémentaire.

#### Authentification SCLM Developer Toolkit

L'authentification du client est effectuée par le démon RSE dans le cadre d'une demande de connexion client. SCLMDT est démarré à partir d'une unité d'exécution propre à l'utilisateur et hérite de l'environnement de sécurité de l'utilisateur en ignorant le besoin d'authentification supplémentaire.

### Authentification du gestionnaire de débogage

L'authentification du client est effectuée par le démon RSE dans le cadre d'une demande de connexion client. Une fois que l'utilisateur est authentifié, des mots de passe PassTicket générés automatiquement sont utilisés pour toutes les demandes d'authentification ultérieures, y compris la connexion automatique au gestionnaire de débogage.

Pour que le gestionnaire de débogage puisse valider l'ID utilisateur et le mot de passe PassTicket présenté par RSE, il doit être autorisé à évaluer le mot de passe PassTicket. Cela implique que le module de chargement AQEZPCM, situé par défaut dans la bibliothèque de chargement FEL.SFEKAUTH, doit disposer d'une autorisation APF.

Lorsqu'un moteur de débogage basé client se connecte au gestionnaire de débogage, il doit présenter un jeton de sécurité valide pour son authentification.

## Sécurité des connexions

La plupart des communications entre le client et l'hôte Developer for z Systems s'effectuent via RSE ; elles utilisent donc la sécurité de connexion fournie par z/OS Explorer.

Certains services Developer for z Systems utilisent un chemin de communication (client-hôte) externe distinct :

- Le moteur de débogueur intégré sur le client se connecte au gestionnaire de débogage sur l'hôte. Les détails du chiffrement sont contrôlés par une règle AT-TLS (Application Transparent Transport Layer Security).
- Les actions à distance (basées sur l'hôte) dans les sous-projets z/OS UNIX utilisent un serveur REXEC ou SSH sur l'hôte. La communication SSH est toujours chiffrée.

## Communication chiffrée pour le débogueur intégré

Les communications (client-hôte) externes avec le gestionnaire de débogage facultatif peuvent également être chiffrées. Pour activer le chiffrement, créez une règle AT-TLS (Application Transparent TLS) pour le port utilisé par le gestionnaire de débogage pour la communication externe, par défaut 5335. Un exemple de règle est fourni dans la figure 6. Voir Chapitre 7, «Configuration de AT-TLS», à la page 43 pour des détails sur la configuration d'AT-TLS.

```

TTLRule                                RDz_Debug_Manager
{
  LocalPortRange                        5335
  Direction                            Inbound
  TLSGroupActionRef                    grp_Production
  TLSEnvironmentActionRef              RDz_Debug_Manager
}
TLSEnvironmentAction                  RDz_Debug_Manager
{
  HandshakeRole                        Server
  TLSKeyRingParms
  {
    Keyring dbgmgr.racf                # Keyring must be owned by the Debug Manager
  }
}
TLSGroupAction                        grp_Production
{
  TTLEnabled                           On
  Trace                                2
}

```

Figure 6. Règle AT-TLS pour le gestionnaire de débogage

**Remarque :** La méthode de communication utilisée par le débogage sur le client Developer for z Systems pour converser avec le gestionnaire de débogage sur l'hôte est liée par défaut à celle utilisée par le client Developer for z Systems pour converser avec le démon RSE. Ceci implique que si le chiffrement est activé pour

l'explorateur de systèmes distants RSE, il est supposé l'être également pour le gestionnaire de débogage. Un scénario alternatif est toutefois disponible pour d'autres configurations.

---

## Sécurité du débogage

Le débogueur intégré facultatif requiert que les utilisateurs disposent d'autorisations d'accès suffisantes aux profils de sécurité spécifiés. Si l'utilisateur ne dispose pas de l'autorisation requise, la session de débogage ne peut pas démarrer.

Developer for z Systems vérifie les droits d'accès aux profils répertoriés dans le tableau 1 afin de déterminer les autorisations de débogage accordées.

*Tableau 1. Informations SAF pour les fonctions de débogage*

Profil FACILITY	Droit d'accès requis	Résultat
AQE.AUTHDEBUG.STDPGM	READ	L'utilisateur est habilité à déboguer les applications à l'état problème
AQE.AUTHDEBUG.AUTHPGM	READ	L'utilisateur est habilité à déboguer les applications à l'état problème et les applications autorisées

### Remarque :

- Developer for z Systems suppose qu'un utilisateur ne dispose d'aucun droit d'accès lorsque votre logiciel de sécurité indique qu'il ne peut pas déterminer si un utilisateur dispose ou non des droits d'accès à un profil. Cela se produit par exemple lorsque le profil n'est pas défini.
- Les versions Developer for z Systems antérieures à la version 9.1.1 vérifiaient l'octroi de l'autorisation UPDATE au profil AQE.AUTHDEBUG.WRITEBUFFER pour permettre le débogage des transactions CICS en lecture seule. Ce profil n'est plus utilisé et peut être supprimé si votre système hôte utilise uniquement Developer for z Systems version 9.1.1, ou ultérieure.

Les exemples de définition de sécurité suivants autorisent tous les utilisateurs du groupe RDZDEBUG à déboguer des applications à l'état problème.

```
RDEFINE FACILITY (AQE.AUTHDEBUG.STDPGM) -  
  UACC(NONE) DATA('RATIONAL DEVELOPER FOR Z SYSTEMS – DEBUG PROBLEM-STATE')  
PERMIT AQE.AUTHDEBUG.STDPGM CLASS(FACILITY) -  
  ID(RDZDEBUG) ACCESS(READ)  
SETROPTS RACLIST(FACILITY) REFRESH
```

---

## CICSTS, sécurité

Le débogueur intégré facultatif peut déboguer des transactions CICS. Pour plus d'informations, voir «Débogage de transactions CICS», à la page 41.

---

## SCLM, sécurité

SCLM Developer Toolkit offre des fonctionnalités de sécurité facultatives pour les fonctions de génération, de promotion et de déploiement.

Si l'administrateur SCLM a activé la sécurité pour une fonction, des appels SAF sont effectués afin de vérifier l'autorité qui exécute la fonction protégée avec l'ID de l'appelant ou d'un utilisateur de substitution.

Pour de plus amples informations sur les définitions de sécurité SCLM requises, voir le document *SCLM Developer Toolkit - Guide d'administration* (SC11-6464).

## Définitions de sécurité

Personnalisez et soumettez l'exemple de travail FELRACF, comportant les exemples de commandes RACF, afin de créer les définitions de sécurité de base de Developer for z Systems. Personnalisez et soumettez l'exemple de travail AQERACF, comportant les exemples de commandes RACF, afin de créer les définitions de sécurité du débogueur intégré.

FELRACF et AQERACF se trouvent dans FEL.#CUST.JCL, sauf si vous avez indiqué un autre emplacement lorsque vous avez personnalisé et soumis le travail FEL.SFELSAMP(FELSETUP). Pour plus de détails, reportez-vous à "Configuration personnalisée" dans le manuel *Rational Developer for z Systems - Guide de configuration de l'hôte*.

Pour plus d'informations sur les commandes RACF, voir le document *RACF Command Language Reference* (SA22-7687).

## Configuration requise et liste de contrôle

Pour effectuer la configuration de la sécurité, l'administrateur de sécurité doit connaître les valeurs indiquées dans le tableau 2. Ces valeurs ont été définies dans les étapes précédentes d'installation et de personnalisation de Rational Developer for z Systems.

Tableau 2. Variables de configuration de la sécurité

Description	<ul style="list-style-type: none"> <li>Valeur par défaut</li> <li>Emplacement de la réponse</li> </ul>	Valeur
Qualificatif de haut niveau du produit Developer for z Systems	<ul style="list-style-type: none"> <li>FEL</li> <li>Installation SMP/E</li> </ul>	
Qualificatif de haut niveau de personnalisation de Developer for z Systems	<ul style="list-style-type: none"> <li>FEL.#CUST</li> <li>FEL.SFELSAMP(FELSETUP), comme indiqué dans la section sur la personnalisation de la configuration du manuel <i>Rational Developer for z Systems - Guide de configuration hôte</i>.</li> </ul>	



Tableau 2. Variables de configuration de la sécurité (suite)

Description	<ul style="list-style-type: none"> <li>• Valeur par défaut</li> <li>• Emplacement de la réponse</li> </ul>	Valeur
Nom de tâche démarrée du débogueur intégré	<ul style="list-style-type: none"> <li>• DBGMGR</li> <li>• FEL.#CUST.PROCLIB(DBGMGR), comme décrit dans le paragraphe sur les modifications de PROCLIB du manuel <i>Rational Developer for z Systems - Guide de configuration hôte</i></li> </ul>	

La liste ci-après présente les actions requises pour effectuer la configuration de sécurité de base de Developer for z Systems. Comme indiqué dans les sections ci-après, différentes méthodes peuvent répondre à vos exigences, en fonction du niveau de sécurité requis.

- «Activation des paramètres et des classes de sécurité»
- «Définition des tâches démarrées de Developer for z Systems», à la page 16
- «Définition du gestionnaire de débogage en tant que serveur sécurisé z/OS UNIX», à la page 16
- «Définition des bibliothèques contrôlées par un programme MVS pour le gestionnaire de débogage», à la page 17
- «Définition de l'accès au débogueur intégré», à la page 22
- «Définition des profils de fichier», à la page 22
- «Vérification des paramètres de sécurité», à la page 23

## Activation des paramètres et des classes de sécurité

Developer for z Systems utilise différents mécanismes de sécurité pour fournir au client un environnement de système hôte sécurisé et contrôlé. Pour ce faire, plusieurs classes et paramètres de sécurité doivent être actifs, comme indiqué par les exemples de commande RACF suivants :

- Affichage des paramètres en cours
  - SETROPTS LIST
- Activation de la classe de fonction pour le débogueur intégré
  - SETROPTS GENERIC(FACILITY)
  - SETROPTS CLASSACT(FACILITY) RACLIST(FACILITY)
- Activation des définitions de tâche démarrée pour le débogueur intégré
  - SETROPTS GENERIC(STARTED)
  - RDEFINE STARTED \*\* STDATA(USER(=MEMBER) GROUP(STCGROUP) TRACE(YES))
  - SETROPTS CLASSACT(STARTED) RACLIST(STARTED)
- Activation du contrôle de programme pour le débogueur intégré
  - RDEFINE PROGRAM \*\* ADDMEM('SYS1.CMDLIB'//NOPADCHK) UACC(READ)
  - SETROPTS WHEN(PROGRAM)

**Remarque :** Ne créez pas le profil \*\* si le profil \* existe déjà dans la classe PROGRAM. Cela occulterait et compliquerait le chemin de recherche utilisé par le logiciel de sécurité. Dans ce cas de figure, vous devez fusionner la définition

\* existante et la nouvelle définition \*\*. Utilisez le profil \*\*, comme indiqué dans la documentation *Security Server RACF Security Administrator's Guide* (SA22-7683).

**Attention :** Certains produits (FTP, par exemple) doivent être contrôlés par programme si "WHEN PROGRAM" est actif. Vous devez essayer ce contrôle de programmes avant de l'activer sur un système de production.

## Définition d'un segment OMVS pour les utilisateurs Developer for z Systems

Un segment OMVS RACF ou équivalent indiquant un ID utilisateur z/OS UNIX différent de zéro valide, un répertoire principal et une commande shell doivent être définis pour chaque utilisateur de Developer for z Systems. Leur groupe par défaut requiert également un segment OMVS avec un ID de groupe.

Lors de l'utilisation du débogueur intégré facultatif, l'ID utilisateur sous laquelle l'application déboguée est active et son groupe par défaut nécessitent également un segment OMVS RACF ou équivalent.

Dans les exemples de commandes RACF ci-dessous, remplacez les marques de réservation #userid, #user-identifiant, #group-name et #group-identifiant par les valeurs réelles :

- ALTUSER #userid  
OMVS(UID(#user-identifiant) HOME(/u/#userid) PROGRAM(/bin/sh) NOASSIZEMAX)
- ALTGROUP #group-name OMVS(GID(#group-identifiant))

## Définition des tâches démarrées de Developer for z Systems

L'exemple de commandes RACF ci-dessous crée la tâche démarrée DBGMR, avec un ID utilisateur protégé (STCDBM), ainsi que le groupe STCGROUP qui lui est affecté.

- ADDGROUP STCGROUP OMVS(AUTOUID)  
DATA('GROUP WITH OMVS SEGMENT FOR STARTED TASKS')
- ADDUSER STCDBM DFLTGRP(STCGROUP) NOPASSWORD NAME('DEBUG MANAGER')  
OMVS(AUTOUID HOME(/tmp) PROGRAM(/bin/sh) )  
DATA('Rational Developer for z Systems')
- RDEFINE STARTED DBGMR.\* DATA('DEBUG MANAGER')  
STDATA(USER(STCDBM) GROUP(STCGROUP) TRUSTED(NO))
- SETROPTS RACLIST(STARTED) REFRESH

### Remarque :

- Assurez-vous que les ID utilisateur des tâches démarrées sont protégés en indiquant le mot clé NOPASSWORD.
- La tâche démarrée du débogueur intégré (DBGMR) est utilisée uniquement par la fonction Débogueur intégré.

## Définition du gestionnaire de débogage en tant que serveur sécurisé z/OS UNIX

Le débogueur intégré requiert un accès UPDATE au profil BPX.SERVER pour créer ou supprimer l'environnement de sécurité de l'unité d'exécution. L'utilisation de

UID(0) pour contourner cette exigence n'est pas prise en charge. Cette autorisation est requise uniquement lorsque la fonction de débogueur intégrée facultative est utilisée.

- RDEFINE FACILITY BPX.SERVER UACC(NONE)
- PERMIT BPX.SERVER CLASS(FACILITY) ACCESS(UPDATE) ID(STCDBM)
- SETROPTS RACLIST(FACILITY) REFRESH

**Avertissement :** La définition du profil BPX.SERVER permet de configurer z/OS UNIX comme un commutateur global qui bascule de la sécurité de niveau UNIX à la sécurité plus étendue de z/OS UNIX. Ce basculement peut avoir une incidence sur d'autres applications et opérations z/OS UNIX. Vous devez tester la sécurité avant de l'activer sur un système de production. Pour plus d'informations sur les différents niveaux de sécurité, voir *UNIX System Services Planning* (GA22-7800).

## Définition des bibliothèques contrôlées par un programme MVS pour le gestionnaire de débogage

Les serveurs disposant des droits BPX.SERVER doivent être exécutés dans un environnement propre, contrôlé par un programme. Cette exigence signifie que tous les programmes appelés par le gestionnaire de débogage doivent également être contrôlés par programme. Pour les bibliothèques de chargement MVS, le contrôle par programme est géré par votre logiciel de sécurité.

Le gestionnaire de débogage utilise les bibliothèques système, l'environnement d'exécution Language Environment et la bibliothèque de chargement de Developer for z Systems (ISP.SISPLOAD).

- RALTER PROGRAM \*\* UACC(READ) ADDMEM('SYS1.LINKLIB'//NOPADCHK)
- RALTER PROGRAM \*\* UACC(READ) ADDMEM('SYS1.CSSLIB'//NOPADCHK)
- RALTER PROGRAM \*\* UACC(READ) ADDMEM('CEE.SCEERUN'//NOPADCHK)
- RALTER PROGRAM \*\* UACC(READ) ADDMEM('CEE.SCEERUN2'//NOPADCHK)
- RALTER PROGRAM \*\* UACC(READ) ADDMEM('FEL.SFELAUTH'//NOPADCHK)
- SETROPTS WHEN(PROGRAM) REFRESH

**Remarque :** N'utilisez pas le profil \*\* si le profil \* existe déjà dans la classe PROGRAM. Le profil occulte et complique le chemin de recherche utilisé par votre logiciel de sécurité. Dans ce cas de figure, vous devez fusionner la définition \* existante et la nouvelle définition \*\*. Utilisez le profil \*\*, comme indiqué dans le manuel dans *Security Server RACF Security Administrator's Guide* (SA22-7683).

Les bibliothèques prérequis suivantes doivent être contrôlées par un programme pour la prise en charge des services facultatifs. Cette liste n'inclut pas les fichiers spécifiques d'un produit avec lequel interagit Developer for z Systems (tels que IBM Explorer for z/OS).

- Autre bibliothèque d'exécution REXX, pour SCLM Developer Toolkit
  - REXX.\*.SEAGALT

**Remarque :** Les bibliothèques qui sont conçues pour le positionnement LSA requièrent également des autorisations de contrôle de programme si l'utilisateur y accède via LINKLIST ou STEPLIB. La présente publication concerne l'utilisation des bibliothèques LPA suivantes :

- Bibliothèque d'exécution REXX, pour SCLM Developer Toolkit
  - REXX.\*.SEAGLPA

- Developer for z Systems, pour CARMA
  - FEL.SFELLPA

## Définition de la prise en charge de passticket pour RSE

Le mot de passe du client ou toute autre méthode d'identification, telle qu'un certificat X.509, est utilisé uniquement pour vérifier l'identité lors de la connexion. Par la suite, les mots de passe passticket permettent de gérer la sécurité des unités d'exécution. Cette étape est requise pour la connexion des clients.

Les passtickets sont des mots de passe générés par le système pour un cycle de vie d'environ 10 minutes. Les passtickets générés se fondent sur une clé secrète. Cette clé est un numéro 64 bits (16 caractères hexadécimaux). Dans l'exemple suivant de commandes RACF, remplacez la marque de réservation key16 par une chaîne hexadécimale à 16 caractères fournie par l'utilisateur qui comporte les caractères 0 à 9 et A à F.

- RDEFINE PTKTDATA FEKAPPL UACC(NONE) SSIGNON(KEYMASKED(key16))  
APPLDATA('NO REPLAY PROTECTION – DO NOT CHANGE')  
DATA('RATIONAL DEVELOPER FOR Z SYSTEMS')
- RDEFINE PTKTDATA IRRPTAUTH.FEKAPPL.\* UACC(NONE)  
DATA('RATIONAL DEVELOPER FOR Z SYSTEMS')
- PERMIT IRRPTAUTH.FEKAPPL.\* CLASS(PTKTDATA) ACCESS(UPDATE) ID(STCRSE)
- SETROPTS RACLIST(PTKTDATA) REFRESH

RSE prend en charge l'utilisation d'un ID application autre que FEKAPPL. Supprimez la mise en commentaire et personnalisez l'option "APPLID=FEKAPPL" dans `rdz.env` pour l'activer, comme indiqué à la section "Définition de paramètres de démarrage Java supplémentaires avec `_RSE_JAVAOPTS`" du manuel *IBM Rational Developer for z Systems - Guide de configuration hôte*. Les définitions de classe PTKTDATA doivent correspondre à l'ID application réel utilisé par RSE.

Vous ne devez pas utiliser OMVSAPPL comme ID d'application, car il ouvrira la clé confidentielle de la plupart des applications z/OS UNIX. De la même manière, vous ne devez pas utiliser l'ID d'application par défaut MVS, qui est MVS suivi par l'ID SMF du système, car il ouvre la clé confidentielle de la plupart des applications MVS, y compris les travaux par lots des utilisateurs.

### Remarque :

- Si la classe PTKTDATA est déjà définie, vérifiez qu'elle est définie en tant que classe générique avant de créer les profils indiqués ci-dessus. La prise en charge de caractères génériques dans la classe PTKTDATA est une nouveauté disponible à partir de z/OS édition 1.7, avec l'introduction d'une interface Java pour les mots de passe passticket.
- Remplacez le caractère générique (\*) dans la définition IRRPTAUTH.FEKAPPL.\* par un masque d'ID utilisateur valide afin de limiter les ID utilisateur pour lesquels RSE peut générer un mot de passe passticket.
- En fonction des paramètres RACF configurés, l'utilisateur qui définit un profil peut également figurer dans la liste d'accès du profil. Supprimez ce droit pour les profils PTKTDATA.
- Le moniteur de travaux JES et RSE doivent posséder le même ID application pour permettre au gestionnaire d'évaluer les mots de passe passticket présentés par RSE. Pour le moniteur de travaux JES, l'ID d'application est défini dans le fichier de configuration FEJJCNGF avec la directive APPLID.
- Si un produit cryptographique est installé et disponible sur le système, vous pouvez chiffrer la clé de l'application de connexion sécurisée pour renforcer la

protection. Pour ce faire, utilisez le mot clé KEYENCRYPTED au lieu du mot clé KEYMASKED. Pour plus d'informations, voir la documentation *Security Server RACF Security Administrator's Guide (SA22-7683)*.

**Avertissement :** La demande de connexion client échoue si les passtickets ne sont pas correctement configurés.

## Définition du droit d'accès aux fichiers z/OS UNIX pour RSE

La commande de l'opérateur **MODIFY LOGS** utilise l'ID utilisateur de tâche démarrée RSED pour collecter des journaux hôte et des informations de configuration. Par défaut, les fichiers journaux d'utilisateur sont créés avec des droits d'accès aux fichiers sécurisés (seul le propriétaire y a accès). Pour pouvoir collecter des fichiers journaux d'utilisateur sécurisés, l'ID utilisateur de tâche démarrée RSED doit être autorisé à les lire.

L'argument OWNER de la commande de l'opérateur **MODIFY LOGS** a pour résultat que l'ID utilisateur spécifié devienne le propriétaire des données collectées. Pour modifier la propriété, l'ID utilisateur de tâche démarrée RSED doit être autorisé à utiliser le service z/OS UNIX CHOWN.

- RDEFINE UNIXPRIV SUPERUSER.FILESYS UACC(NONE) DATA('OVERRIDE UNIX FILE ACCESS RESTRICTIONS')
- RDEFINE UNIXPRIV SUPERUSER.FILESYS.CHOWN UACC(NONE) DATA('OVERRIDE UNIX CHANGE OWNER RESTRICTIONS')
- PERMIT SUPERUSER.FILESYS CLASS(UNIXPRIV) ACCESS(READ) ID(STCRSE)
- PERMIT SUPERUSER.FILESYS.CHOWN CLASS(UNIXPRIV) ACCESS(READ) ID(STCRSE)
- SETROPTS RACLIST(UNIXPRIV) REFRESH

Notez que lorsque le profil SUPERUSER.FILESYS.ACLOVERRIDE est défini, les droits d'accès configurés dans la liste de contrôle d'accès sont prioritaires sur les droits octroyés par le biais de SUPERUSER.FILESYS. L'ID utilisateur de tâche démarrée RSED aura besoin de l'autorisation d'accès en lecture (READ) au profil SUPERUSER.FILESYS.ACLOVERRIDE pour ignorer les définitions de la liste de contrôle d'accès.

## Définition de la protection des applications pour RSE

Lors de la connexion du client, le démon RSE vérifie que l'utilisateur est autorisé à utiliser l'application.

- RDEFINE APPL FEKAPPL UACC(READ) DATA('RATIONAL DEVELOPER FOR Z SYSTEMS')
- SETROPTS RACLIST(APPL) REFRESH

### Remarque :

- Comme indiqué plus en détails dans «Définition de la prise en charge de passticket pour RSE», à la page 18, RSE prend en charge l'utilisation d'un ID application autre que FEKAPPL. La définition de classe APPL doit correspondre à l'ID application réel utilisé par RSE.
- La demande de connexion client aboutit si l'ID application n'est pas défini dans la classe APPL.
- La demande de connexion client échoue uniquement si l'ID application est défini et si l'utilisateur ne bénéficie pas d'accès en lecture sur le profil.

## Définition de fichiers contrôlés par programme z/OS UNIX pour RSE

Les serveurs disposant des droits BPX.SERVER doivent être exécutés dans un environnement propre, contrôlé par un programme. Cette exigence signifie que tous les programmes appelés par RSE doivent également être contrôlés par programme. Pour les fichiers z/OS UNIX, le contrôle par programme est géré par la commande **extattr**. Pour exécuter cette commande vous devez disposer du droit d'accès en lecture (READ) sur BPX.FILEATTR.PROGCTL dans la classe FACILITY ou avoir l'ID utilisateur UID(0).

Le serveur RSE utilise la bibliothèque partagée Java de RACF (/usr/lib/libIRRRacf\*.so).

- `extattr +p /usr/lib/libIRRRacf*.so`

### Remarque :

- Depuis z/OS 1.9, /usr/lib/libIRRRacf\*.so est installé en mode de contrôle par programme lors de l'installation de SMP/E RACF.
- Depuis z/OS 1.10, /usr/lib/libIRRRacf\*.so fait partie de SAF, lequel est fourni avec la version z/OS de base ; par conséquent, il est également disponible pour les clients non RACF.
- La configuration peut varier si vous utilisez un produit de sécurité autre que RACF. Pour de plus amples informations, consultez la documentation de votre produit de sécurité.
- L'installation SMP/E de Developer for z Systems définit le bit de contrôle par programme pour les programmes RSE internes.
- Utilisez la commande **ls -Eog** z/OS UNIX pour afficher l'état en cours du bit de contrôle par programme. Le fichier est contrôlé par un programme si la lettre **p** apparaît dans la deuxième chaîne.

```
$ ls -Eog /usr/lib/libIRRRacf*.so
-rwxr-xr-x  aps-  2      69632 Oct  5  2007 /usr/lib/libIRRRacf.so
-rwxr-xr-x  aps-  2      69632 Oct  5  2007 /usr/lib/libIRRRacf64.so
```

## Définition de la sécurité des commandes JES

Le moniteur de travaux JES émet toutes les commandes d'opérateur JES demandées par un utilisateur via une console EMCS dont le nom est contrôlé à l'aide de la directive `CONSOLE_NAME`, comme indiqué dans la section "FEJJCNFG, fichier de configuration du moniteur de travaux JES" du document *Rational Developer for z Systems - Guide de configuration de l'hôte*.

Les exemples de commande RACF suivants donnent aux utilisateurs Developer for z Systems un accès conditionnel à un nombre limité de commandes JES, à savoir Mettre en attente, Libérer, Annuler et Purger. Les utilisateurs possèdent des droits d'exécution uniquement s'ils lancent les commandes via le moniteur de travaux JES. Remplacez la marque de réservation `#console` par le nom réel de la console.

- `RDEFINE OPERCMDS MVS.MCSOPER.#console UACC(READ)`  
`DATA('RATIONAL DEVELOPER FOR Z SYSTEMS')`
- `RDEFINE OPERCMDS JES%.** UACC(NONE)`
- `PERMIT JES%.** CLASS(OPERCMDS) ACCESS(UPDATE) WHEN(CONSOLE(JMON)) ID(*)`
- `SETROPTS RACLIST(OPERCMDS) REFRESH`

### Remarque :

- L'utilisation de la console est autorisé si aucun profil `MVS.MCSOPER.#console` n'a été défini.

- La classe CONSOLE doit être active pour permettre le fonctionnement de WHEN(CONSOLE(JMON)) mais il n'y a pas de vérification réelle du profil dans la classe CONSOLE pour les consoles EMCS.
- Ne remplacez pas JMON par le nom réel de la console dans la clause WHEN(CONSOLE(JMON)). Le mot clé JMON représente l'application de point d'entrée, pas le nom de la console.

**Avertissement :** La définition des commandes JES à l'aide de l'accès universel NONE dans votre logiciel de sécurité peut avoir une incidence sur les autres applications et opérations. Vous devez tester la sécurité avant de l'activer sur un système de production.

Le tableau 3 et le tableau 4 présentent des commandes d'opérateur soumises pour JES2 et JES3, et les profils de sécurité discrets qui peuvent être utilisés pour les protéger.

*Tableau 3. Commandes d'opérateur du moniteur de travaux JES2*

Action	Commande	Profil OPERCMDS	Droit d'accès requis
Mettre en attente	\$Hx(jobid) avec x = {J, S ou T}	jesname.MODIFYHOLD.BAT jesname.MODIFYHOLD.STC jesname.MODIFYHOLD.TSU	UPDATE
Libérer	\$Ax(jobid) avec x = {J, S ou T}	jesname.MODIFYRELEASE.BAT jesname.MODIFYRELEASE.STC jesname.MODIFYRELEASE.TSU	UPDATE
Annuler	\$Cx(jobid) avec x = {J, S ou T}	jesname.CANCEL.BAT jesname.CANCEL.STC jesname.CANCEL.TSU	UPDATE
Purger	\$Cx(jobid),P avec x = {J, S ou T}	jesname.CANCEL.BAT jesname.CANCEL.STC jesname.CANCEL.TSU	UPDATE

*Tableau 4. Commandes d'opérateur du moniteur de travaux JES3*

Action	Commande	Profil OPERCMDS	Droit d'accès requis
Mettre en attente	*F,J=jobid,H	jesname.MODIFY.JOB	UPDATE
Libérer	*F,J=jobid,R	jesname.MODIFY.JOB	UPDATE
Annuler	*F,J=jobid,C	jesname.MODIFY.JOB	UPDATE
Purger	*F,J=jobid,C	jesname.MODIFY.JOB	UPDATE

**Remarque :**

- Les commandes d'opérateur JES Mettre en attente, Libérer, Annuler et Purger, ainsi que la commande Afficher JCL, peuvent être exécutées uniquement sur des fichiers spoule appartenant à l'ID utilisateur du client, sauf si vous avez indiqué LIMIT\_COMMANDS= avec la valeur LIMITED ou NOLIMIT dans le fichier de configuration du moniteur de travaux JES. Pour plus d'informations, reportez-vous au tableau "Actions sur les travaux - Limitations sur les cibles" du manuel *Référence de configuration de l'hôte* (SC11-6869).

- Les utilisateurs peuvent parcourir n'importe quel fichier spoule, sauf si LIMIT\_VIEW=USERID est défini dans le fichier de configuration du moniteur de travaux JES. Pour plus d'informations, voir "Accès aux fichiers spoule" dans *Référence de configuration de l'hôte* (SC11-6869).
- Même si les utilisateurs n'ont pas d'autorisation pour ces commandes d'opérateur, ils peuvent toujours soumettre des travaux et lire les sorties de travaux via le moniteur de travaux JES s'ils disposent de droits d'accès suffisants à des profils qui protègent ces ressources, comme celles des classes JESINPUT, JESJOBS et JESSPOOL.

Supposons que l'accès à l'identité du serveur du moniteur de travaux JES lors de la création d'une console JMON à partir d'une session TSO est empêché par votre logiciel de sécurité. Même si la console peut être créée, le point d'entrée est différent ; par exemple, moniteur de travaux JES/TSO. Les commandes JES exécutées par cette console échouent lors du contrôle de sécurité si la sécurité est configurée comme indiqué dans cette publication et que l'utilisateur ne dispose pas de droits d'accès aux commandes JES via d'autres procédures.

## Définition de l'accès au débogueur intégré

Les utilisateurs doivent disposer du droit d'accès en lecture à l'un des profils AQE.AUTHDEBUG.\* répertoriés pour pouvoir utiliser le débogueur intégré afin de déboguer les programmes à l'état problème. Les utilisateurs autorisés à accéder au profil AQE.AUTHDEBUG.AUTHPGM peuvent également déboguer des programmes autorisés par APF. Remplacez la marque de réservation #apf par des ID utilisateur ou des noms de groupes RACF valides pour les utilisateurs pouvant déboguer des programmes autorisés.

- RDEFINE FACILITY AQE.AUTHDEBUG.STDPGM UACC(NONE)
- PERMIT AQE.AUTHDEBUG.STDPGM CLASS(FACILITY) ACCESS(READ) ID(\*)
- RDEFINE FACILITY AQE.AUTHDEBUG.AUTHPGM UACC(NONE)
- PERMIT AQE.AUTHDEBUG.AUTHPGM CLASS(FACILITY) ACCESS(READ) ID(#apf)
- SETROPTS RACLIST(FACILITY) REFRESH

**Remarque :** Les versions de IBM Rational Developer for System z antérieures à la version 9.1.1 utilisaient un autre profil de classe FACILITY, AQE.AUTHDEBUG.WRITEBUFFER, qui n'est plus utilisé. Il peut être supprimé si votre système hôte utilise uniquement IBM Rational Developer for System z version 9.1.1 ou une version ultérieure.

## Définition des profils de fichier

Un accès en lecture pour les utilisateurs et en modification pour les programmeurs système suffit pour la plupart des fichiers Developer for z Systems. Remplacez la marque de réservation #sysprog par des ID utilisateur ou des noms de groupes RACF. Demandez également au programmeur système qui a installé et configuré le produit de vous fournir les noms de fichier corrects. FEK est le qualificatif de haut niveau par défaut utilisé pendant l'installation et FEL.#CUST celui relatif aux fichiers créés pendant le processus de personnalisation.

- | ADDGROUP (FEL) OWNER(IBMUSER) SUPGROUP(SYS1)  
| DATA('IBM Rational Developer for z Systems - HLQ STUB')  
|  
•  
| ADDSD 'FEL.\*.\*\*\*' UACC(READ)  
| DATA('IBM Rational Developer for z Systems')  
|  
•  
|  
| PERMIT 'FEL.\*.\*\*\*' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)



- SETROPTS GENERIC(DATASET) REFRESH

#### Remarque :

- Protégez FEL.SFELAUTH des mises à jour car ce fichier dispose de droits APF.
- Les exemples de commande utilisés dans la présente publication et dans le travail FELRACF supposent que l'EGN (Enhanced Generic Naming) est activé. Dans ce cas, le qualificatif \*\* peut être utilisé pour représenter tout nombre de qualificatifs dans la classe DATASET. Remplacez \*\* par \* si l'EGN n'est pas activé dans votre système. Pour plus d'informations sur EGN, voir le manuel *Security Server RACF Security Administrator's Guide* (SA22-7683).

Certains des composants Developer for z Systems requièrent des profils de fichier de sécurité supplémentaires. Remplacez les marques de réservation #sysprog et #ram-developer par des ID utilisateur ou des noms de groupe RACF valides :

- Si la traduction des noms longs/abrégiés de SCLM Developer Toolkit est utilisée, les utilisateurs doivent disposer d'un accès en mise à jour (UPDATE) au mappage VSAM, FEL.#CUST.LSTRANS.FILE.

```

-
  ADDSD 'FEL.#CUST.LSTRANS.**' UACC(UPDATE)
  DATA('IBM Rational Developer for z Systems - SCLMDT')
-
  PERMIT 'FEL.#CUST.LSTRANS.**' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
-
  SETROPTS GENERIC(DATASET) REFRESH

```

- CARMA RAM (Repository Access Manager) developers require UPDATE access to the CARMA VSAMs, FEL.#CUST.CRA\*.

```

-
  ADDSD 'FEL.#CUST.CRA**' UACC(READ)
  DATA('IBM Rational Developer for z Systems - CARMA')
-
  PERMIT 'FEL.#CUST.CRA**' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
-
  PERMIT 'FEL.#CUST.CRA**' CLASS(DATASET) ACCESS(UPDATE) ID(#ram-developer)
-
  SETROPTS GENERIC(DATASET) REFRESH

```

## Vérification des paramètres de sécurité

Utilisez les exemples de commande ci-dessous pour afficher les résultats de vos personnalisations de la sécurité.

- Paramètres et classes de sécurité
  - SETROPTS LIST
- Tâches démarrées
  - LISTGRP STCGROUP OMVS
  - LISTUSER STCDBM OMVS
  - RLIST STARTED DBGMGR.\* ALL STDATA
- Gestionnaire de débogage en tant que serveur sécurisé z/OS UNIX
  - RLIST FACILITY BPX.SERVER ALL
- Bibliothèques contrôlées par un programme MVS pour le gestionnaire de débogage

```
|      - RLIST PROGRAM ** ALL
|
|      • Accès au débogueur intégré
|      - RLIST FACILITY AQE.** ALL
|
|      • Profils de fichier
|      - LISTGRP FEL
|
|      - LISTDSD PREFIX(FEL) ALL
```

## Chapitre 3. Remarques relatives à TCP/IP

Developer for z Systems repose sur le protocole TCP/IP pour offrir l'accès au mainframe à des utilisateurs travaillant sur un poste de travail autre qu'un mainframe. TCP/IP sert également à assurer la communication entre les différents composants et les autres produits.

Les rubriques suivantes sont traitées dans le présent chapitre :

- «Ports TCP/IP»
- «CARMA et ports TCP/IP», à la page 27

Developer for z Systems se construit par-dessus IBM Explorer for z/OS. Pour plus d'informations sur z/OS Explorer, voir la section concernant les remarques relatives à TCP/IP dans le manuel *IBM Explorer for z/OS - Guide de référence de la configuration hôte* (SC27-8438).

### Ports TCP/IP

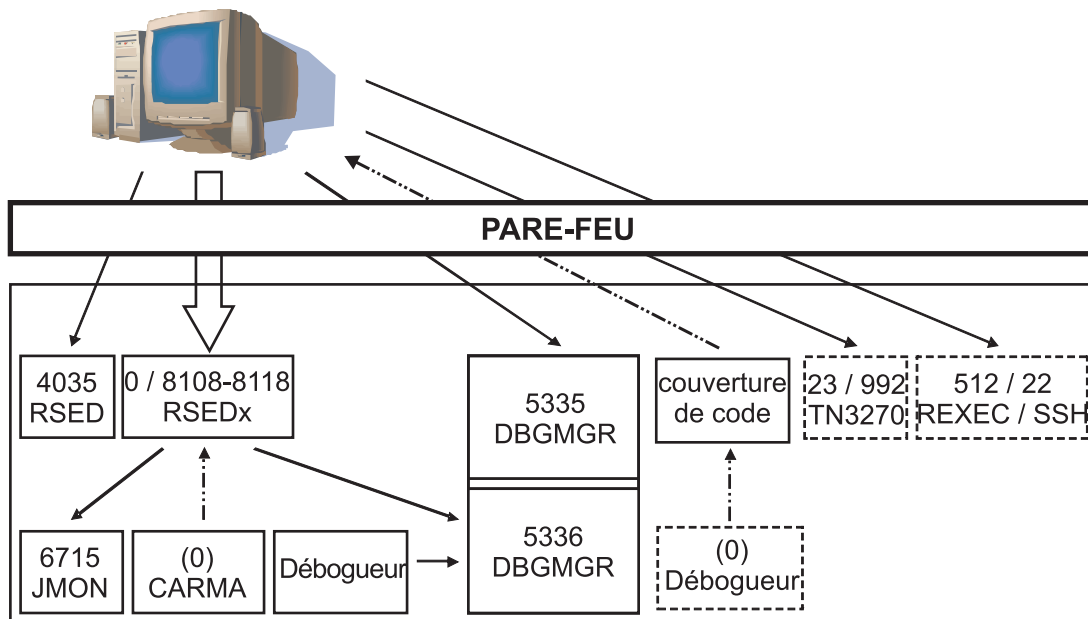


Figure 7. Ports TCP/IP

La figure 7 présente les ports TCP/IP pouvant être utilisés par z/OS Explorer et Developer for z Systems. Les flèches indiquent la partie qui assure la liaison (tête de flèche) et celle qui assure la connexion.

### Communications externes

Définissez les ports suivants sur le pare-feu qui protège l'hôte z/OS car ils sont utilisés pour les communications client-hôte (via le protocole tcp) :

- (z/OS Explorer) Démon RSE pour la configuration des communications client-hôte, port 4035 par défaut. Le port peut être défini dans le fichier de configuration `rse.env`. La communication sur ce port peut être chiffrée.

- (z/OS Explorer) Serveur RSE pour les communications client-hôte. Par défaut, tout port disponible est utilisé, mais une plage de ports peut être définie à l'aide de la définition `_RSE_PORTRANGE` dans le fichier `rse.env`. La plage de ports par défaut pour `_RSE_PORTRANGE` est comprise entre 8108 et 8118 (11 ports). La communication sur ce port peut être chiffrée.
- Gestionnaire de débogage pour les services de débogueur intégré, port par défaut 5335. Le port peut être défini dans le JCL de la tâche démarrée `DBGMGR`. La communication sur ce port peut être chiffrée.
- Service `INETD` pour les actions à distance (basées sur l'hôte) dans les sous-projets z/OS UNIX :
  - `REXEC` (version z/OS UNIX), port par défaut 512.
  - `SSH` (version z/OS UNIX), port par défaut 22. La communication sur ce port est chiffrée.
- (z/OS Explorer) Service Telnet `TN3270` pour l'émulateur de connexion à l'hôte, port par défaut 23. La communication externe peut être chiffrée (port par défaut 992). Le port par défaut affecté au service Telnet `TN3270` dépend de l'utilisation ou non du chiffrement par l'utilisateur.
- Vous pouvez indiquer à la fonction de couverture de code reposant sur l'hôte qu'elle doit se connecter au moteur du débogueur intégré d'un client `Developer for z Systems`. La communication sur ce port peut être chiffrée. Vous remarquerez que dans ce scénario, le collecteur de couverture de code reposant sur z/OS est un client pour TCP/IP et que le moteur du débogueur intégré sur l'ordinateur personnel de l'utilisateur est un serveur pour TCP/IP. Par défaut, `IBM Debug Tool` est utilisé localement sur le même hôte.

**Remarque :** Normalement, le client indique l'adresse TCP/IP utilisée pour se connecter à l'hôte. Cependant, pour s'assurer que les sessions de débogage communiquent avec l'hôte correct, le gestionnaire de débogage indique au client l'adresse TCP/IP à utiliser.

## Communication interne

Plusieurs services hôte `Developer for z Systems` s'exécutent dans des unités d'exécution ou espaces adresse séparés et utilisent des sockets TCP/IP comme mécanisme de communication, à l'aide de l'adresse de bouclage de votre système. Tous ces services utilisent RSE pour communiquer avec le client et limitent leur flux de données à l'hôte. Pour certains services, n'importe quel port est utilisé. Pour d'autres, le programmeur système peut sélectionner un port ou une plage de ports à utiliser :

- Moniteur de travaux `JES` pour les services associés à `JES`, port par défaut 6715. Le port peut être défini dans le membre de configuration `FEJJCNFG` et est répété dans le fichier de configuration `rse.env`.
- (Facultatif) La communication `CARMA` utilise par défaut un port temporaire, mais une plage de ports peut être définie dans le fichier de configuration `CRASRV.properties`.
- (Facultatif) Gestionnaire de débogage pour les services liés aux débogage, port par défaut 5336. Le port peut être défini dans le JCL de la tâche démarrée `DBGMGR`.
- La couverture de code basée sur l'hôte, qui est un travail par lots, alloue un port temporaire pour permettre à `IBM Debug Tool for z/OS` de communiquer avec celle-ci et de fournir les données nécessaires pour le rapport de couverture de code.

## Réservation de port TCP/IP

Si vous utilisez l'instruction PORT ou PORTRANGE dans PROFILE.TCPIP pour réserver les ports utilisés par z/OS Explorer et Developer for z Systems, notez que de nombreuses liaisons sont effectuées par les unités d'exécution actives dans le pool d'unités d'exécution RSE. Le nom de travail du pool d'unités d'exécution RSE est RSEDx, où RSED est le nom de la tâche démarrée RSE et x est un nombre à un chiffre aléatoire, si bien que la définition contient obligatoirement des caractères génériques.

```
PORT      4035      TCP RSED   ; z/OS Explorer - RSE daemon
PORT      6715      TCP JMON    ; z/OS Explorer - JES job monitor
PORT      5335      TCP DBGMR   ; Developer for z Systems - Integrated debugger
PORT      5336      TCP DBGMR   ; Developer for x Systems - Integrated debugger
PORTRange 8108 11   TCP RSED*   ; z/OS Explorer - RSE_PORTRANGE
;PORTRange 5227 100 TCP RSED*   ; Developer for z Systems - CARMA
```

---

## CARMA et TCP/IP

### CARMA et ports TCP/IP

CARMA (Common Access Repository Manager) permet d'accéder à un SCM (Software Configuration Manager) basé sur un hôte, par exemple CA Endevor® SCM. Dans la plupart des cas, comme pour le démon RSE, un serveur assure la liaison à un port et écoute les demandes de connexion. Toutefois, CARMA utilise une démarche différente, étant donné que le serveur CARMA n'est pas encore actif lorsque le client lance la demande de connexion.

Lorsque le client envoie une demande de connexion, l'exploitant CARMA, qui est actif comme une unité d'exécution utilisateur d'un pool d'unités d'exécution RSE, demande un port temporaire ou trouve un port libre dans la plage indiquée dans le fichier de configuration CRASRV.properties et procède à la liaison. L'exploitant démarre le serveur CARMA et transmet le numéro de port, de sorte que le serveur sache à quel port se connecter. Une fois le serveur connecté, le client peut envoyer les demandes au serveur et recevoir les résultats.

Du point de vue de TCP/IP, RSE (via le logiciel de fouille de données CARMA) constitue le serveur qui établit la liaison au port et le serveur CARMA représente le client qui s'y connecte.

Si vous utilisez l'instruction PORT ou PORTRANGE dans PROFILE.TCPIP pour réserver la plage de ports utilisée par CARMA, notez que le logiciel de fouille de données CARMA est actif dans un pool d'unités d'exécution RSE. Le nom de travail du pool d'unités d'exécution RSE est RSEDx, où RSED correspond au nom de la tâche RSE démarrée et x à un chiffre aléatoire unique, si bien que la définition contient obligatoirement des caractères génériques.

```
PORTRange 5227 100 RSED*           ; DEVELOPER FOR Z SYSTEMS - CARMA
```

**Remarque :** Le procédure de vérification d'installation de CARMA, fekfivpc, échoue si vous réservez les ports CARMA à une utilisation par des espaces adresse RSE. Ceci est à prévoir car la procédure de vérification d'installation s'exécute dans l'espace adresse de la personne qui lance cette procédure, pas dans l'espace adresse de RSE, et la demande de liaison de l'espace adresse TCP/IP va échouer.

### CARMA et affinité entre piles

CARMA (Common Access Repository Manager) permet d'accéder à un SCM (Software Configuration Manager) basé sur un hôte, par exemple CA Endevor®

SCM. Pour ce faire, CARMA démarre le serveur spécifique à un utilisateur qui doit être configuré pour une application de l'affinité entre piles.

A l'instar des tâches démarrées z/OS Explorer et Developer for z Systems, l'affinité entre piles d'un serveur CARMA est définie à l'aide de la variable `_BPXK_SETIBMOPT_TRANSPORT` qui doit être transmise à LE (Language Environment). Pour ce faire, réglez la commande de démarrage dans le fichier de configuration `crastart*.conf` ou `CRASUB*` actif.

**Remarque :**

- Le nom exact du fichier de configuration contenant la commande de démarrage dépend des différentes options sélectionnées par le programmeur-système qui a configuré CARMA. Voir le "Chapitre 3. (Facultatif) Common Access Repository Manager (CARMA)" dans le manuel *Guide de configuration de l'hôte* (SC27-8577) pour plus d'informations à ce sujet.
- `_BPXK_SETIBMOPT_TRANSPORT` spécifie le nom de la pile TCP/IP à utiliser, tel que défini dans l'instruction `TCPIPJOBNAME` dans le `TCPIP.DATA` correspondant.
- Le codage d'une instruction de définition de données `SYSTCPD` ne définit pas l'affinité entre piles demandée.
- Par défaut, CARMA n'utilise pas les piles TCP/IP normales. CARMA utilise l'adresse de bouclage pour la communication entre le logiciel de fouille de données CARMA et le serveur CARMA. Cela améliore la sécurité (seuls les processus locaux ont accès à l'adresse de bouclage) et peut éviter d'avoir à ajouter l'affinité entre piles à la communication CARMA.

**crastart\*.conf**

Remplacez le segment suivant :

```
... PARM(&CRAPRM1. &CRAPRM2.)
```

par celui-ci (où `TCPIP` représente la pile TCP/IP voulue) :

```
... PARM(ENVAR("_BPXK_SETIBMOPT_TRANSPORT=TCPIP") / &CRAPRM1. &CRAPRM2.)
```

**Remarque :** `CRASTART` ne prend pas en charge les continuations de ligne mais la longueur de ligne admise n'est soumise à aucune limite.

**CRASUB\***

Remplacez le segment suivant :

```
... PARM(&PORT &TIMEOUT)
```

par celui-ci (où `TCPIP` représente la pile TCP/IP voulue) :

```
... PARM(ENVAR("_BPXK_SETIBMOPT_TRANSPORT=TCPIP") / &PORT &TIMEOUT)
```

**Remarque :** La soumission de travail limite la longueur de ligne à 80 caractères. Pour concaténer deux lignes, vous pouvez couper une ligne trop longue à l'emplacement d'un blanc ( ) et utilisez un signe plus (+) à la fin de la première ligne.

## Chapitre 4. Remarques relatives à WLM

Contrairement aux applications z/OS traditionnelles, Rational Developer for z Systems n'est pas une application monolithique qui peut être identifiée facilement au niveau du Workload Manager (WLM). Les différents composants de Developer for z Systems interagissent pour offrir au client un accès à des services et des données d'hôte. Comme décrit au Chapitre 1, «Description de Developer for z Systems», à la page 3, certains de ces services sont actifs dans différents espaces adresse; ce qui se traduit par différentes classifications WLM.

Les rubriques suivantes sont traitées dans le présent chapitre :

- «Classification des charges de travail»
- «Définition des objectifs», à la page 31

Developer for z Systems se construit par-dessus IBM Explorer for z/OS. Pour plus d'informations sur z/OS Explorer, voir la section concernant les remarques relatives à WLM dans le manuel *IBM Explorer for z/OS - Guide de référence de la configuration hôte* (SC27-8438).

### Classification des charges de travail

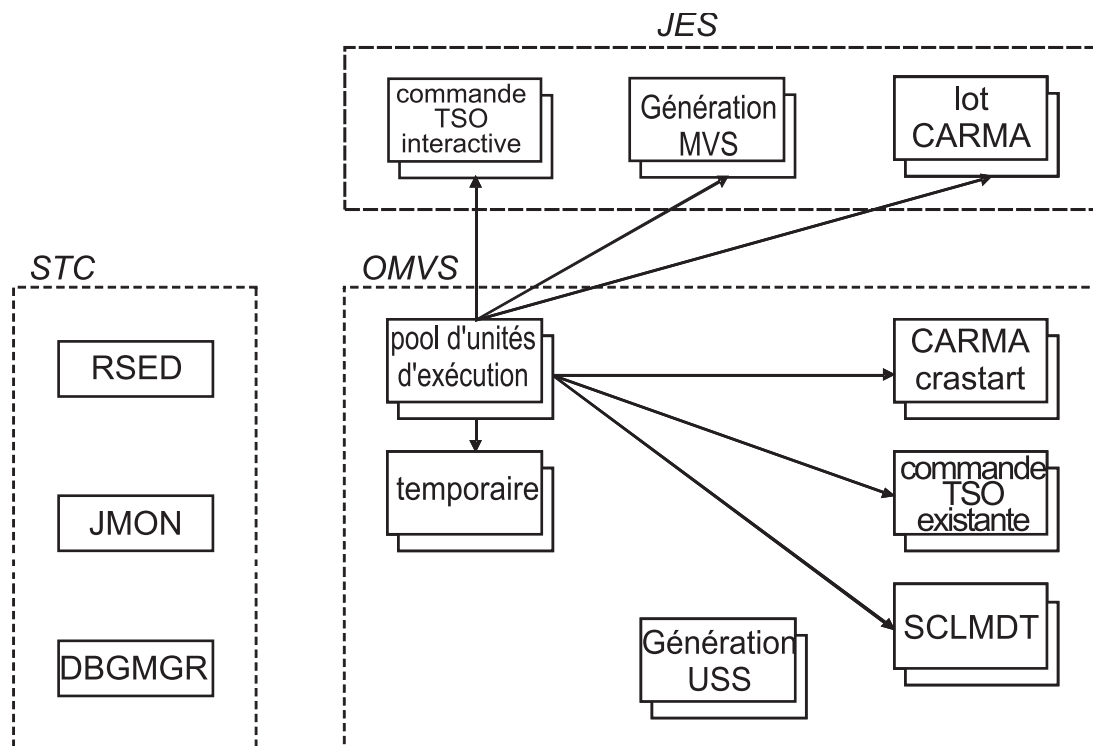


Figure 8. Classification WLM

La figure 8 contient une présentation de base des sous-systèmes par l'intermédiaire desquels les charges de travail de z/OS Explorer et Developer for z Systems sont présentées au gestionnaire WLM.

Le démon RSE (RSED), le gestionnaire de débogage (DBGMGR) et le moniteur de travaux JES (JMON) sont des tâches démarrées de z/OS Explorer et Developer for z Systems (ou des travaux par lots à exécution longue), chacun avec leur espace adresse individuel.

Le démon RSE génère un processus enfant pour chaque serveur de pools d'unités d'exécution RSE (qui prend en charge un nombre variable de clients). Chaque pool d'unités d'exécution est actif dans un espace adresse distinct (à l'aide d'un initiateur z/OS UNIX, BPXAS). Puisqu'il s'agit de processus générés, leur classification s'effectue d'après les règles de classification WLM OMVS, mais pas selon les règles de classification des tâches démarrées.

Les clients qui sont actifs dans un pool d'unités d'exécution peuvent créer une multitude d'autres espaces adresse, selon les actions menées par les utilisateurs. Selon la configuration de Developer for z Systems, certaines charges de travail, comme un service de Commandes TSO (TSO cmd) ou CARMA, peuvent s'exécuter dans des sous-systèmes différents.

Les espaces adresse répertoriés dans la figure 8, à la page 29 restent dans le système suffisamment longtemps pour être visibles, mais sachez qu'en raison de la conception de z/OS UNIX, il existe aussi des espaces adresses temporaires de durée de vie courte. Ces espaces adresse temporaires sont actifs dans le sous-système OMVS.

Notez que tandis que les pools d'unités d'exécution utilisent le même ID utilisateur et un nom de travail similaire au démon RSE, tous les espaces adresse démarrés par un pool d'unités d'exécution appartiennent à l'ID utilisateur du client ayant demandé l'action. L'ID utilisateur du client est aussi utilisé comme (partie du) nom de travail pour tous les espaces adresse basés sur OMVS et déclarés par le pool d'unités d'exécution.

D'autres espaces adresse sont créés par d'autres services qu'utilise Developer for z Systems, comme z/OS UNIX REXEC (génération USS).

## Règles de classification

WLM utilise des règles de classification pour mapper un travail entrant le système en une classe de service. Cette classification repose sur des qualificatifs de travaux. Le premier qualificatif (obligatoire) est le type de sous-système qui reçoit la demande de travail. Le tableau 5 répertorie les types de sous-systèmes qui peuvent recevoir des charges de travail de Developer for z Systems.

*Tableau 5. Sous-systèmes de point d'entrée WLM*

Type de sous-système	Description du travail
ASCH	Les demandes de travaux incluent tous les programmes de transactions APPC planifiés par le planificateur de transactions APPC/MVS fourni par IBM, ASCH.
JES	Les demandes de travaux incluent tous les travaux initiés par JES2 ou JES3.
OMVS	Les demandes de travaux incluent un travail traité dans des espaces adresse enfant en parallèle à des services système z/OS UNIX.
STC	Les demandes de travaux incluent tous les travaux initiés par les commandes START et MOUNT. STC inclut aussi des espaces adresse de composants système.



Le tableau 6 répertorie des qualificateurs supplémentaires que vous pouvez utiliser pour attribuer une charge de travail à une classe de service spécifique. Pour plus d'informations sur les qualificateurs répertoriés, voir MVS Planning: Workload Management (SA22-7602).

Tableau 6. Qualificateurs de travaux WLM

		ASCH	JES	OMVS	STC
AI	Comptabilité des informations	x	x	x	x
LU	Nom de l'unité logique (*)				
PF	Effectuer (*)		x		x
PRI	Priorité		x		
SE	Nom de l'environnement de planification		x		
SSC	Nom de collection du sous-système		x		
SI	Instance du sous-système (*)		x		
SPM	Paramètre du sous-système				x
PX	Nom Sysplex	x	x	x	x
SY	Nom du système (*)	x		x	x
TC	Classe Transaction/travail (*)	x	x		
TN	Nom Transaction/travail (*)	x	x	x	x
UI	ID utilisateur (*)	x	x	x	x

**Remarque :** S'agissant des qualificateurs marqués avec (\*), vous pouvez indiquer des groupes de classification en ajoutant un G à l'abréviation du type. Par exemple, un groupe de nom de transaction doit être TNG.

## Définition des objectifs

Comme nous l'avons documenté dans «Classification des charges de travail», à la page 29, Developer for z Systems crée différents types de charges de travail sur votre système. Ces différentes tâches communiquent entre elles, ce qui implique que le temps écoulé réel devienne important pour éviter des problèmes de délai d'attente lors des connexions entre les tâches. En conséquence, une tâche Developer for z Systems doit être placée dans des classes de services de hautes performances avec une priorité élevée.

Une révision, et probablement une mise à jour, de vos objectifs WLM en cours est donc recommandée, notamment s'il agit de charges de travail OMVS critique en temps ou nouvelles des magasins MVS traditionnels.

### Remarque :

- Les informations d'objectif qui figurent dans cette section sont délibérément maintenues à un niveau descriptif, car les objectifs de performances réels sont très spécifiques du site.
- Pour mieux comprendre l'impact d'une tâche spécifique sur votre système, nous employons des termes comme utilisation de ressources minimale, modérée et substantielle. Tous ces termes sont relatifs à l'utilisation de la totalité des ressources de Developer for z Systems proprement dit, et non du système dans son intégralité.

La tableau 7 présente les espaces adresse pouvant être utilisés par z/OS Explorer et Developer for z Systems. z/OS UNIX remplace "x" dans la colonne "Nom de la tâche" par un nombre aléatoire comportant un seul chiffre.

*Tableau 7. Charges de travail WLM*

Description	Nom de la tâche	Charge de travail
Gestionnaire de débogage	DBGMGR	STC
(z/OS Explorer) Moniteur de travaux JES	JMON	STC
(z/OS Explorer) Démon RSE	RSED	STC
(z/OS Explorer) Pool d'unités d'exécution RSE	RSEDx	OMVS
(ISPF) Passerelle ISPF interactive (service de commande TSO)	<id utilisateur>	JES
(ISPF) Passerelle ISPF existante (service de commandes TSO et SCLMDT)	<id utilisateur>x	OMVS
(z/OS Explorer) Service de commandes TSO (APPC)	FEKFRSRV	ASCH
CARMA (lot)	CRA<port>	JES
CARMA (crastart)	<id utilisateur>x	OMVS
CARMA (passerelle client ISPF)	<id utilisateur> et <id utilisateur>x	OMVS
Génération MVS (travail par lots)	*	JES
Génération z/OS UNIX (commandes shell)	<id utilisateur>x	OMVS
Interpréteur de commandes de z/OS UNIX	<id utilisateur>	OMVS

## Remarques relatives à la sélection des objectifs

Les remarques générales suivantes relatives à WLM peuvent vous aider à bien définir les définitions d'objectifs correctes pour Developer for z Systems :

- Vous devez baser des objectifs sur ce qui peut être réellement obtenu, et non sur vos souhaits concernant ce qui pourrait arriver. Si vous définissez des supérieurs à ce qui est nécessaire, WLM déplace des ressources d'un travail de moindre importance vers un travail d'importance plus élevée qui pourrait ne pas avoir véritablement besoin des ressources.
- Limite le volume de travail attribué aux classes de service SYSTEM et SYSSTC, car ces classes bénéficient d'une priorité de distribution supérieure à n'importe quelle classe gérée WLM. Utilisez ces classes pour un travail qui est d'importance élevée, bien qu'utilisant peu d'unité centrale.
- Un travail qui n'entre pas dans les règles de classification finit par aboutir dans la classe SYSOTHER, qui a un objectif discrétionnaire. Un objectif discrétionnaire recommande à WLM d'agir au mieux lorsque le système a des ressources disponibles.

Lors de l'utilisation des objectifs de temps de réponse :

- Il doit exister un taux d'arrivée stable de tâches (au moins 10 tâches en 20 minutes) pour permettre à WLM de gérer correctement un objectif de temps de réponse.

- Utilisez des objectifs de temps de réponse moyen uniquement pour bien contrôler des charges de travail, car une transaction longue et unique a un impact énorme sur le temps de réponse moyen et peut contraindre WLM à réagir de façon excessive.

Lors de l'utilisation des objectifs de vitesse :

- D'une manière générale, vous ne pouvez pas obtenir d'objectif de vitesse supérieur à 90 % et ce pour différentes raisons. Par exemple, tous les espaces adresse SYSTEM et SYSSTC bénéficient d'une priorité de distribution supérieure à tout objectif de type vitesse.
- WLM utilise un nombre minimum de modèles (utilisation et délai) sur lesquels se fondent ses décisions en termes d'objectifs de vitesse. Ainsi, moins il y aura de travaux exécutés dans une classe de service, plus cela prendra de temps pour collecter le nombre requis de modèles et ajuster la règle de répartition.
- Réévaluez les objectifs de vitesse lors du changement de votre matériel. Notamment, vers une diminution, des processeurs plus rapides imposent des changements dans les objectifs de vitesse.

## STC

Toutes les tâches démarrées Developer for z Systems assurent le service des demandes clients en temps réel.

*Tableau 8. Charges de travail et STC WLM*

Description	Nom de la tâche	Charge de travail
Gestionnaire de débogage	DBGMGR	STC

- Gestionnaire de débogage

Le gestionnaire de débogage fournit des services pour connecter les programmes à déboguer aux clients qui les déboguent. Vous devez indiquer un objectif de vitesse et de hautes performances sur une période, car la tâche ne signale pas les transactions individuelles à WLM. L'usage des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de type minimal.

## OMVS

Toutes les charges de travail utilisent l'ID utilisateur du client comme base pour le nom de l'espace adresse. (z/OS UNIX remplace "x" dans la colonne "Nom de la tâche" par un nombre aléatoire comportant un seul chiffre.)

Les charges de travail finiront toutes par aboutir dans la même classe de service en raison d'une convention commune d'attribution de nom d'espace adresse. Vous devez indiquer un objectif à périodes multiples pour cette classe de service. Les premières périodes doivent être des objectifs de temps de réponse percentiles à hautes performances, tandis que la dernière période doit avoir un objectif de vitesse à performances modérées. Certaines charges de travail, comme une passerelle client ISPF, signaleront des transactions individuelles et d'autres non.

*Tableau 9. Charges de travail - OMVS WLM*

Description	Nom de la tâche	Charge de travail
Passerelle ISPF existante (service Commandes TSO et SCLMDT)	<id utilisateur>x	OMVS
CARMA (crastart)	<id utilisateur>x	OMVS

Tableau 9. Charges de travail - OMVS WLM (suite)

Description	Nom de la tâche	Charge de travail
CARMA (passerelle client ISPF)	<id utilisateur> et <id utilisateur>x	OMVS
Génération z/OS UNIX (commandes shell)	<id utilisateur>x	OMVS
Interpréteur de commandes de z/OS UNIX	<id utilisateur>	OMVS

- Passerelle ISPF existante

La passerelle ISPF existante est un service ISPF appelé par Developer for z Systems pour exécuter des commandes TSO et ISPF qui ne sont pas interactives. Il peut s'agir de commandes explicites émises par le client ainsi que de commandes implicites émises par le composant SCLMDT de Developer for z Systems. L'usage des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de type minimal.

- CARMA

CARMA est un serveur Developer for z Systems facultatif qui permet d'interagir avec des gestionnaires de configuration logicielle (SCM) basés sur l'hôte, comme CA Endevor® SCM. Developer for z Systems autorise différentes méthodes de démarrage pour un serveur CARMA, dont certaines deviennent une charge de travail OMVS. L'usage des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de type minimal.

- Génération z/OS UNIX

Lorsqu'un client initie une génération pour un projet z/OS UNIX, z/OS UNIX REXEC (ou SSH) démarre une tâche qui exécute plusieurs commandes shell z/OS UNIX pour effectuer la génération. L'utilisation des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de modéré à substantiel, selon la taille du projet.

- Interpréteur de commandes de z/OS UNIX

Cette charge de travail traite les commande shell z/OS UNIX shell émises par le client. L'usage des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de type minimal.

## JES

Developer for z Systems utilise les processus de traitement par lots gérés par JES de différentes manières. L'usage le plus classique concerne les générations MVS dans lesquelles un travail est soumis et contrôlé pour déterminer quand il prend fin. Toutefois, Developer for z Systems pourrait aussi démarrer un serveur CARMA dans un traitement par lots et communiquer avec celui-ci via TCP/IP.

Tableau 10. Charge de travail - JES WLM

Description	Nom de la tâche	Charge de travail
CARMA (lot)	CRA<port>	JES
Génération MVS (travail par lots)	*	JES

- CARMA

CARMA est un serveur Developer for z Systems qui permet d'interagir avec les gestionnaires de configuration logicielle (SCM), tels que CA Endevor® SCM. Developer for z Systems autorise différentes méthodes de démarrage pour un serveur CARMA, dont certaines deviennent une charge de travail JES. Vous

devez indiquer un objectif de vitesse et de hautes performances sur une période, car la tâche ne signale pas les transactions individuelles à WLM. L'usage des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de type minimal.

- Génération MVS

Lorsqu'un client initie une génération pour un projet MVS, Developer for z Systems démarre une tâche de traitement par lots pour exécuter la génération. L'utilisation des ressources dépend fortement des actions des utilisateurs et donc fluctuera, mais on s'attend à être de modéré à substantiel, selon la taille du projet. Différentes stratégies d'objectifs à performances modérées peuvent être recommandées, selon des circonstances locales.

- Vous pourriez indiquer un objectif à périodes multiples avec une période à objectif de temps de réponse percentile et une période à objectif de vitesse secondaire. Dans ce cas, vos développeurs doivent utiliser pour la plupart la même procédure de génération et des fichiers d'entrée de tailles similaires pour créer des travaux ayant des temps de réponse uniformes. Il doit aussi exister un taux d'arrivée stable de travaux (au moins 10 travaux en 20 minutes) pour permettre à WLM de gérer correctement un objectif de temps de réponse.
- Un objectif de vitesse est plus approprié à la plupart des travaux en traitement par lots, car ces objectifs peuvent gérer des temps d'exécution et des taux d'arrivée extrêmement variables.



---

## Chapitre 5. Remarques relatives à la fonction d'envoi au client

La fonction d'envoi au client, ou contrôle client résidant sur l'hôte, prend en charge la gestion centralisée des éléments suivants :

- Fichiers de configuration client
- Version de produit client
- Définitions de projet

Les rubriques suivantes sont traitées dans le présent chapitre :

- «Introduction»
- «Projets résidant sur l'hôte», à la page 38

Developer for z Systems se construit par-dessus IBM Explorer for z/OS. Pour plus d'informations sur z/OS Explorer, voir la section concernant les remarques relatives à la fonction d'envoi au client par commande push (push-to-client) dans le manuel *IBM Explorer for z/OS - Guide de référence de la configuration hôte* (SC27-8438).

---

### Introduction

Les clients Developer for z Systems peuvent extraire les fichiers de configuration client et les informations de mise à jour de produit depuis l'hôte lorsqu'ils se connectent, ce qui permet de garantir que tous les clients sont paramétrés de la même façon et qu'ils sont à jour.

L'administrateur client peut créer plusieurs jeux de configuration client et plusieurs scénarios de mise à jour client afin de répondre aux besoins des différents groupes de développeurs. Ainsi, les utilisateurs peuvent recevoir une configuration personnalisée, basée sur des critères tels que l'appartenance d'un groupe LDAP ou les droits d'accès à un profil de sécurité.

Les projets z/OS peuvent être définis de façon individuelle via la perspective Projets z/OS sur le client, ou de façon centralisée sur l'hôte, puis propagés individuellement sur le client pour chaque utilisateur. Ces projets résidant sur l'hôte ressemblent et fonctionnent exactement comme des projets définis sur le client, sauf que leur structure, leurs membres et leurs propriétés ne peuvent pas être modifiés par le client et qu'ils sont accessibles uniquement lorsque vous êtes connecté à l'hôte.

Un responsable de projet de développement définit un projet et affecte chaque développeur à ce projet.

Voir l'Developer for z Systems IBM Knowledge Center([http://www-01.ibm.com/support/knowledgecenter/SSQ2R2/rdz\\_welcome.html](http://www-01.ibm.com/support/knowledgecenter/SSQ2R2/rdz_welcome.html)) pour des détails sur la façon dont le responsable de projet de développement effectue les tâches qui lui ont été affectées.

Lorsque vous activez le support de contrôle de version ou de configuration pour plusieurs groupes de développeurs, une équipe supplémentaire est chargée de la

gestion de la fonction d'envoi au client. L'équipe dédiée à cette tâche varie en fonction de l'option qui a été choisie pour identifier les groupes auxquels un développeur appartient. :

- Un administrateur LDAP gère les définitions de groupe qui placent chaque développeur dans aucun groupe LDAP, dans un groupe LDAP ou dans plusieurs groupes LDAP FEL.PTC.\*.
- Un administrateur de sécurité gère les listes d'accès aux profils de sécurité FEL.PTC.\*. Un développeur peut disposer de droits d'accès sur aucun profil, sur un profil ou sur tous les profils.

---

## Projets résidant sur l'hôte

Les projets z/OS peuvent être définis de façon individuelle via la perspective Projets z/OS sur le client, ou de façon centralisée sur l'hôte, puis propagés individuellement sur le client pour chaque utilisateur. Ces projets résidant sur l'hôte ressemblent et fonctionnent exactement comme des projets définis sur le client, sauf que leur structure, leurs membres et leurs propriétés ne peuvent pas être modifiés par le client et qu'ils sont accessibles uniquement lorsque vous êtes connecté à l'hôte.

Le répertoire de base pour les projets résidant sur l'hôte est défini (par l'administrateur client) dans `/var/rdz/pushtoclient/keymapping.xml`. Il s'agit du répertoire par défaut `/var/rdz/pushtoclient/projects`.

Pour configurer des projets résidant sur l'hôte, le responsable de projet ou le développeur doit définir les types de fichier de configuration suivants. Tous les fichiers sont des fichiers XML codés en UTF-8.

- Les fichiers d'instance de projet sont spécifiques à un ID utilisateur unique et pointent vers des fichiers de définition de projet réutilisables. Chaque utilisateur qui fonctionne avec des projets résidant sur l'hôte a besoin d'un sous-répertoire, `/var/zexpl/pushtoclient/projects/<userid>/`, qui contient un fichier d'instance de projet (`*.hbpin`) pour chaque projet à télécharger.
- Les fichiers de définition de projet définissent la structure et le contenu du projet et sont réutilisables par plusieurs utilisateurs. Les fichiers de définition de projet (`*.hbppd`) répertorient les sous-projets contenus par le projet et sont situés dans le répertoire de définition de projet racine ou dans l'un de ses sous-répertoires.
- Les fichiers de définition de sous-projet définissent la structure et le contenu du sous-projet et sont réutilisables par plusieurs utilisateurs. Les fichiers de définition de sous-projet (`*.hbpsd`) définissent l'ensemble de ressources nécessaires pour générer un module de chargement et sont situés dans le répertoire de définition de projet racine ou dans l'un de ses sous-répertoires.
- Les fichiers de propriétés de sous-projet sont des fichiers de propriétés avec prise en charge de substitution de variable réutilisables par plusieurs sous-projets. Les fichiers de propriétés de sous-projet (`*.hbppr`) prennent en charge la substitution de variable afin de permettre le partage de fichiers de propriétés entre plusieurs utilisateurs et sont situés dans le répertoire de définition de projet racine ou dans l'un de ses sous-répertoires.

Les projets résidant sur l'hôte peuvent également être sélectionnés pour faire partie de la configuration de plusieurs groupes. Cela signifie que les projets résidant sur l'hôte peuvent également être définis dans `/var/rdz/pushtoclient/grouping/<devgroup>/projects/`.



Lorsqu'un espace de travail est lié à un groupe spécifique et qu'il existe des définitions de projet pour un utilisateur dans ce groupe et dans le groupe par défaut, l'utilisateur reçoit les définitions de projet depuis ces deux groupes.



---

## Chapitre 6. Remarques relatives à CICSTS

Ce chapitre regroupe des références aux composants Developer for z Systems pouvant fonctionner dans des régions CICSTS.

---

### Prise en charge de langues bidirectionnelles

Pour plus d'informations sur la prise en charge de langues bidirectionnelles, voir la section sur la prise en charge de langues bidirectionnelles CICS dans le chapitre "Autres tâches de personnalisation" du manuel *Rational Developer for z Systems - Guide de configuration hôte* (SC27-8577).

---

### Messages IRZ de diagnostic pour Enterprise Service Tools

Pour plus d'informations sur les messages IRZ de diagnostic pour Enterprise Service Tools, voir la section correspondante dans le chapitre "Autres tâches de personnalisation" du manuel *Rational Developer for z Systems - Guide de configuration hôte* (SC27-8577).

---

### Débogage de transactions CICS

Pour plus d'informations sur le débogage des transactions CICS, voir la section "Mises à jour CICS du débogueur intégré" dans le chapitre "(Facultatif) Débogueur intégré" du manuel *IBM Rational Developer for z Systems - Guide de configuration de l'hôte* (SC11-6285).



---

## Chapitre 7. Configuration de AT-TLS

Cette section vous aide à résoudre certains problèmes susceptibles de se produire lors de la configuration d'AT-TLS (Application Transparent Transport Layer Security) ou pendant la vérification ou la modification d'une configuration existante.

Le protocole TLS (Transport Layer Security) défini dans RFC 2246 offre une confidentialité pour les communications sur Internet. Comme son prédécesseur SSL (Secure Socket Layer), ce protocole permet aux applications client et serveur de communiquer de façon à empêcher les écoutes clandestines, les contrefaçons et la falsification des messages. Le protocole AT-TLS (Application Transparent Transport Layer Security) consolide l'implémentation de TLS pour les applications z/OS dans un emplacement, ce qui permet à toutes les applications de prendre en charge le chiffrement TLS sans avoir connaissance du protocole TLS. Pour plus d'informations sur AT-TLS, voir le document *Communications Server IP Configuration Guide* (SC31-8775).

Le débogueur intégré de Developer for z Systems s'appuie sur AT-TLS pour les communications chiffrées avec le client car les données de la session de débogage ne passent pas par le même canal que les autres communications client/hôte de Developer for z Systems.

Les actions nécessaires pour configurer AT-TLS varient d'un site à l'autre, selon les véritables besoins et ce qui est déjà disponible au niveau du site.

Les informations contenues dans cette section expliquent comment configurer l'agent de règles TCP/IP qui gère AT-TLS et définir une règle pour l'utilisation par le débogueur intégré Developer for z Systems sur un système z/OS 1.13, avec une prise en charge de TLS v1.2.

1. «Configuration de syslogd», à la page 44
2. «Configuration AT-TLS dans PROFILE.TCPIP», à la page 44
3. «Tâche démarrée par l'agent de règles», à la page 44
4. «Configuration de l'agent de règles», à la page 45
5. «Règle AT-TLS», à la page 45
6. «Mises à jour de sécurité AT-TLS», à la page 48
7. «Activation de la règle AT-TLS», à la page 50

Une convention d'attribution de nom uniforme est utilisée dans cette section :

- Port du gestionnaire de débogage pour communication externe : 5335
- ID utilisateur du gestionnaire de débogage : stcdm
- ID utilisateur de l'agent de règles : pagent
- Certificat : dbgmgr
- Stockage des clés et des certificats : dbgmgr.racf

Certaines des tâches décrites dans les sections suivantes nécessitent des actions de votre part dans z/OS UNIX. Vous pouvez les effectuer en lançant la commande TSO **OMVS**. Utilisez la commande **oedit** pour éditer les fichiers sous z/OS UNIX. Utilisez la commande **exit** pour retourner à TSO.

---

## Configuration de syslogd

La documentation TCP/IP conseille d'écrire les messages de l'agent de règles dans le journal système (syslog) z/OS UNIX au lieu d'utiliser le fichier journal par défaut. AT-TLS écrit toujours les messages dans le journal système (syslog) z/OS UNIX.

Pour ce faire, le démon syslog z/OS UNIX, `syslogd`, doit être configuré et actif. Vous devez également disposer d'un mécanisme permettant de contrôler la taille des fichiers journaux créés par `syslogd`.

Les mises à jour suivantes du fichier de configuration permettent de configurer et démarrer `syslogd`, à l'aide d'un mécanisme simple de gestion des fichiers journaux (effacement des journaux existants lorsque z/OS UNIX démarre et création de nouveaux journaux au démarrage de `syslogd`).

- `/etc/services`  
`syslog 514/udp`
- `/etc/syslog.conf`  

```
# /etc/syslog.conf - control output of syslogd
# 1. all files with will be printed to /tmp/syslog.auth.log
auth.* /tmp/syslog.auth.log
# 2. all error messages printed to /tmp/syslog.error.log
*.err /tmp/syslog.error.log
# 3. all debug and above messages printed to /tmp/syslog.debug.log
*.debug /tmp/syslog.debug.log
# The files named must exist before the syslog daemon is started,
# unless -c startup option is used
```
- `/etc/rc`  

```
# Start the SYSLOGD daemon for logging
# (clean up old logs)
sed -n '/^#/!s/.* \(.*\)/\1/p' /etc/syslog.conf | xargs -i rm {}
# (create new logs and add userid of message sender)
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -cuf /etc/syslog.conf &
sleep 5
```

---

## Configuration AT-TLS dans PROFILE.TCPIP

La prise en charge AT-TLS est activée par le paramètre TTLS sur l'instruction TCPCONFIG dans le fichier PROFILE.TCPIP. AT-TLS est géré par l'agent de règles qui doit être actif pour pouvoir appliquer la règle AT-TLS. Étant donné que l'agent de règles doit attendre que TCP/IP soit actif, l'instruction AUTOSTART dans PROFILE.TCPIP est un endroit approprié pour déclencher le démarrage de ce serveur.

Ces exigences aboutissent aux modifications suivantes apportées à PROFILE.TCPIP, souvent appelé TCPIP.TCPPARMS(TCPPROF).

```
TCPCONFIG TTLS ; Required for AT-TLS
AUTOLOG
PAGENT ; POLICY AGENT, required for AT-TLS
ENDAUTOLOG
```

---

## Tâche démarrée par l'agent de règles

Comme indiqué précédemment, AT-TLS est géré par l'agent de règles, qui peut être démarré comme une tâche démarrée. Utilisez le JCL précédent pour créer SYS1.PROCLIB(PAGENT), à l'aide du fichier de configuration par défaut et de l'emplacement de journal recommandé (SYSLOGD). Les définitions nécessaires

dans le logiciel de sécurité sont abordées ultérieurement.

```
//PAGENT PROC PRM='-L SYSLOGD' * '' or '-L SYSLOGD'
//*
//* TCP/IP POLICY AGENT
//* (PARM) (envar)
//* default cfg file: /etc/pagent.conf (-C) (PAGENT_CONFIG_FILE)
//* default log file: /tmp/pagent.log (-L) (PAGENT_LOG_FILE)
//* default log size: 300,3 (3x 300KB files) (PAGENT_LOG_FILE_CONTROL)
//*
//PAGENT EXEC PGM=PAGENT,REGION=0M,TIME=NOLIMIT,
// PARM='ENVAR("TZ=EST5DST")/&PRM'
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//*
```

---

## Configuration de l'agent de règles

L'agent de règles applique les règles relatives à TCP/IP créées par l'administrateur TCP/IP. Il gère les règles pour AT-TLS, appelé TTLS, mais également pour des services tels que IPSec. L'agent de règles utilise un fichier de configuration pour savoir quelles règles appliquer et où elles se trouvent. Le fichier de configuration par défaut est /etc/pagent.conf, mais un autre endroit peut être indiqué dans la tâche JCL démarrée par l'agent de règles.

```
#
# TCP/IP Policy Agent configuration information.
#
TTLSConfig /etc/pagent.ttls.conf
# Specifies the path of a TTLS policy file holding stack specific
# statements.
#
#TcpImage TCP/IP /etc/pagent.conf
# If no TcpImage statement is specified, all policies will be installed
# to the default TCP/IP stack.
#
#LogLevel 31
# The sum of the following values that represent log levels:
# LOGL_SYSERR 1
# LOGL_OBJERR 2
# LOGL_PROTERR 4
# LOGL_WARNING 8
# LOGL_EVENT 16
# LOGL_ACTION 32
# LOGL_INFO 64
# LOGL_ACNTING 128
# LOGL_TRACE 256
# Log Level 31 is the default log loglevel.
#
#Codepage IBM-1047
# Specify the EBCDIC code page to be used for reading all configuration
# files and policy definition files. IBM-1047 is the default code page.
```

Cet exemple de fichier de configuration indique l'endroit où l'agent de règles peut trouver la règle TTLS. Il utilise les valeurs par défaut de l'agent de règles pour d'autres instructions.

---

## Règle AT-TLS

Une règle TTLS décrit les règles AT-TLS souhaitées. Comme défini dans le fichier de configuration de l'agent de règles, la règle TTLS se trouve dans /etc/pagent.ttls.conf. Les définitions nécessaires dans le logiciel de sécurité sont abordées ultérieurement.

Cet exemple illustre une règle double, assez simple, qui désactive SSL v3 et active la prise en charge de TLS v1, TLS v1.1 et TLS v1.2 pour les deux chemins de communication pris en charge par le débogueur intégré, le gestionnaire de débogage et la sonde-client Developer for z Systems. Comme défini dans le fichier de configuration de l'agent de règles, la règle TTLS se trouve dans /etc/pagent.ttls.conf.

```
##
## TCP/IP Policy Agent AT-TLS configuration information.
##
##-----
TTLSRule                                RDz_Debug_Manager
{
    LocalPortRange                        5335
    Direction                            Inbound
    TTLSGroupActionRef                    grp_Production
    TTLSEnvironmentActionRef              act_RDz_Debug_Manager
}
##-----
TTLSEnvironmentAction                    act_RDz_Debug_Manager
{
    HandshakeRole Server
    TTLSKeyRingParms
    {
        Keyring dbgmgr.racf      # Keyring must be owned by the Debug Manager
    }
    TTLSEnvironmentAdvancedParms
    {
        ## TLSV1.2 only for z/OS 2.1 and higher
        # TLSV1.2 On              # TLSv1 & TLSv1.1 are on by default
        SSLV3 Off                 # disable SSLv3 }
    }
}
##-----
TTLSRule                                RDz_Debug_Probe-Client
{
    RemotePortRange                        8001
    Direction                            Outbound
    TTLSGroupActionRef                    grp_Production
    TTLSEnvironmentActionRef              act_RDz_Debug_Probe-Client
}
##-----
TTLSEnvironmentAction                    act_RDz_Debug_Probe-Client
{
    HandshakeRole                        Client
    TTLSKeyRingParms
    {
        Keyring *AUTH*/*            # virtual key ring holding CA certificates
    }
    TTLSEnvironmentAdvancedParms
    {
        ## TLSV1.2 only for z/OS 2.1 and higher
        # TLSV1.2 On              # TLSv1 & TLSv1.1 are on by default
    }
}
##-----
TTLSGroupAction                          grp_Production
{
    TTLSEnabled                          On
    ## TLSv1.2zOS1.13 only for z/OS 1.13
    TTLSGroupAdvancedParmsRef            TLSv1.2zOS1.13
    Trace                                3      # Log Errors to syslogd & IP joblog
    #Trace                                254    # Log everything to syslogd
}
##-----
```



```

TTLSTGroupAdvancedParms      TLSv1.2z0S1.13
{
  Envfile /etc/pagent.ttls.TLS1.2z0S1.13.env
}

```

Une règle TTLS permet à tout un ensemble de filtres d'indiquer le moment où une règle s'applique.

Le gestionnaire de débogage est un serveur qui écoute sur le port 5335 les connexions entrantes en provenance du moteur de débogage. Ces informations sont capturées dans la règle RDz\_Debug\_Manager.

Etant donné que la communication chiffrée nécessite l'utilisation d'un certificat serveur, indiquez que le gestionnaire de règles doit utiliser les certificats figurant dans le fichier de clés dbgmgr.racf qui appartient à l'ID utilisateur de la tâche démarrée par le gestionnaire de débogage. Par défaut, la prise en charge de TLS v1.2 est désactivée, donc cette règle l'active explicitement. Le protocole SSLv3.0 est désactivé explicitement en raison de vulnérabilités connues.

Lorsque la sonde de débogage est démarrée avec l'option Language Environment (LE) TEST(,,TCP/IP&&ipaddress%8001:\*), il lui est demandé de ne pas utiliser le gestionnaire de débogage, mais de contacter directement le client Developer for z Systems sur le port 8001. Du point de vue de TCP/IP, cela implique que la sonde de débogage client soit un client qui contacte un serveur (l'interface graphique de débogage) dans le client Developer for z Systems. Ces informations sont capturées dans la règle RDz\_Debug\_Probe-Client.

L'hôte étant un client TCP/IP, le gestionnaire de règles devra disposer d'un moyen lui permettant de valider le certificat serveur présenté par l'interface graphique de débogage. Au lieu d'utiliser un fichier de clés nommé de manière uniforme pour tous les utilisateurs qui peuvent requérir une session de débogage chiffrée, nous utilisons le fichier de clés virtuel CERTAUTH de RACF (\*AUTH\*/\*). Ce fichier de clés virtuel contient les certificats publics des autorités de certification et peut être utilisé si l'interface graphique de débogage présente un certificat serveur signé par l'une des autorités de certification sécurisées.

Notez que pour des règles plus complexes, il est conseillé d'utiliser l'assistant de configuration IBM pour z/OS Communications Server. Il s'agit d'un outil de type interface graphique qui fournit une interface guidée permettant de configurer les fonctions réseau basées sur des règles TCP/IP et qui est disponible comme une tâche dans IBM z/OS Management Facility (z/OSMF), et comme une application de poste de travail autonome.

## Remarques relatives à TLS v1.2

La prise en charge de TLS v1.2 est devenue disponible dans z/OS 2.1, et elle est désactivée par défaut. Cette règle montre la commande (TLSV1.2 On) qui permet de l'activer explicitement, mais elle est mise en commentaire car le système cible utilise z/OS 1.13.

En appliquant les deux APAR suivants, la prise en charge de TLS v1.2 est ajoutée à z/OS 1.13 :

- System SSL - APAR OA39422
- Communications Server (AT-TLS) - APAR PM62905

z/OS 1.13 System SSL, qui est utilisé par AT-TLS pour implémenter la communication chiffrée TLS, nécessite certains paramètres supplémentaires pour la

prise en charge de TLS v1.2. Ils sont fournis par la règle AT-TLS à l'aide d'un fichier avec des variables d'environnement System SSL, /etc/pagent.ttls.TLS1.2zOS1.13.env.

```
#
# Add TLSv1.2 support to AT-TLS
# requires z/OS 1.13 with OA39422 and PM62905
#
GSK_RENEGOTIATION=ALL
GSK_PROTOCOL_TLSV1_2=ON
```

---

## Mises à jour de sécurité AT-TLS

Plusieurs mises à jour de sécurité sont requises pour permettre le bon fonctionnement de AT-TLS. Cette section comporte des exemples de commande RACF permettant d'effectuer la configuration requise.

Comme indiqué dans «Tâche démarrée par l'agent de règles», à la page 44, vous utilisez une tâche démarrée pour exécuter l'agent de règles. Pour cela, il faut que soient définis l'ID utilisateur d'une tâche démarrée ainsi qu'un profil dans la classe STARTED.

```
# define started task user ID
# BPX.DAEMON permit is required for non-zero UID
ADDUSER PAGENT DFLTGRP(SYS1) OMVS(UID(0) SHARED HOME('/')) +
  NAME('TCP/IP POLICY AGENT') NOPASSWORD

# define started task
RDEFINE STARTED PAGENT.* STDATA(USER(PAGENT) GROUP(SYS1)) +
  DATA('TCP/IP POLICY AGENT')

# refresh to make the changes visible
SETROPTS RACLIST(STARTED) REFRESH
```

Définissez un profil appelé MVS.SERVGR.PAGENT dans la classe OPERCMDS et accordez à l'ID utilisateur PAGENT CONTROL l'accès à ce profil. Le profil limite le nombre d'utilisateurs autorisés à démarrer l'agent de règles. Si le profil n'est pas défini et que son accès est fermé par un profil générique, PAGENT ne pourra pas démarrer l'agent de règles, ce qui empêchera l'initialisation de la pile TCP/IP.

```
# restrict startup of policy agent
RDEFINE OPERCMDS MVS.SERVGR.PAGENT UACC(NONE) +
  DATA('restrict startup of policy agent')
PERMIT MVS.SERVGR.PAGENT CLASS(OPERCMDS) ACCESS(CONTROL) ID(PAGENT)

# refresh to make the changes visible
SETROPTS RACLIST(OPERCMDS) REFRESH
```

Comme indiqué dans «Configuration AT-TLS dans PROFILE.TCPIP», à la page 44, l'agent de règles est démarré après l'initialisation de TCP/IP. Cela signifie qu'il existe une (petite) fenêtre dans laquelle les applications peuvent utiliser la pile TCP/IP sans que la règle TTLS soit appliquée. Définissez le profil EZB.INITSTACK.\*\* dans la classe SERVAUTH pour empêcher l'accès à la pile pendant cette fenêtre de temps, sauf pour les applications ayant accès en lecture au profil. Vous devez autoriser un nombre limité d'applications d'administration à accéder au profil pour assurer l'initialisation complète de la pile, comme indiqué dans la section "TCP/IP stack initialization access control" du document *Communications Server IP Configuration Guide (SC31-8775)*.

**Remarque :** L'agent de règles émet le message ESD1586I lorsque toutes les règles sont actives.

```
# block stack access between stack and AT-TLS availability
# SETROPTS GENERIC(SERVAUTH)
# SETROPTS CLASSACT(SERVAUTH) RACLIST(FACILITY)
  RDEFINE SERVAUTH EZB.INITSTACK.** UACC(NONE)
# Policy Agent
  PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(PAGENT)
# OMPROUTE daemon
  PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(OMPROUTE)
# SNMP agent and subagents
  PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(OSNMPPD)
  PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(IOBSNMP)
# NAME daemon
  PERMIT EZB.INITSTACK.** CLASS(SERVAUTH) ACCESS(READ) ID(NAMED)

# refresh to make the changes visible
SETROPTS RACLIST(SERVAUTH) REFRESH
```

(Facultatif) La commande z/OS UNIX **pasearch** affiche des définitions de règles actives. Définissez le profil EZB.PAGENT.\*\* dans la classe SERVAUTH pour limiter l'accès à la commande **pasearch**.

```
# restrict access to pasearch command
# RDEFINE SERVAUTH EZB.PAGENT.** UACC(NONE) +
#   DATA('restrict access to pasearch command')
# PERMIT EZB.PAGENT.** CLASS(SERVAUTH) ACCESS(READ) ID(tcpadmin)

# refresh to make the changes visible
# SETROPTS RACLIST(SERVAUTH) REFRESH
```

Comme indiqué à la section «Règle AT-TLS», à la page 45, le gestionnaire de débogage a besoin d'un certificat pour permettre à AT-TLS de configurer la communication chiffrée pour son compte. Ces exemples de commande créent un nouveau certificat intitulé dbgmgr qui est stocké dans un fichier de clés RACF appelé dbgmgr.racf. Le certificat et le fichier de clés appartiennent tous les deux à STCDBM, l'ID utilisateur de la tâche démarrée par le gestionnaire de débogage.

```
# permit Debug Manager to access certificates
#RDEFINE FACILITY IRR.DIGTCERT.LIST      UACC(NONE)
#RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
  PERMIT IRR.DIGTCERT.LIST      CLASS(FACILITY) ACCESS(READ) ID(stcdbm)
  PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ACCESS(READ) ID(stcdbm)

# refresh to make the changes visible
SETROPTS RACLIST(FACILITY) REFRESH

# create self-signed certificate
RACDCERT ID(stcdbm) GENCERT SUBJECTSDN(CN('RDz Debug Manager') +
  OU('RTP labs') O('IBM') L('Raleigh') SP('NC') C('US')) +
  NOTAFTER(DATE(2015-12-31)) KEYUSAGE(HANDSHAKE) WITHLABEL('dbgmgr')

# (optional) additional steps required to use a signed certificate
# 1. create a signing request for the self-signed certificate
  RACDCERT ID(stcdbm) GENREQ (LABEL('dbgmgr')) DSN(dsn)
# 2. send the signing request to your CA of choice
# 3. check if the CA credentials (also a certificate) are already known
  RACDCERT CERTAUTH LIST
# 4. mark the CA certificate as trusted
  RACDCERT CERTAUTH ALTER(LABEL('CA cert')) TRUST
#   or add the CA certificate to the database
  RACDCERT CERTAUTH ADD(dsn) WITHLABEL('CA cert') TRUST
# 5. add the signed certificate to the database;
#   this will replace the self-signed one
  RACDCERT ID(stcdbm) ADD(dsn) WITHLABEL('dbgmgr') TRUST
# Do NOT delete the self-signed certificate before replacing it.
# If you do, you lose the private key that goes with the certificate,
# which makes the certificate useless.
```

```

# create key ring
RACDCERT ID(stcdbg) ADDRING(dbgmgr.racf)

# add certificate to key ring
RACDCERT ID(stcdbg) CONNECT(LABEL('dbgmgr') +
RING(dbgmgr.racf) USAGE(PERSONAL) DEFAULT)

# additional step required to use a signed certificate
# 6. add CA certificate to key ring
RACDCERT ID(stcdbg) CONNECT(CERTAUTH LABEL('CA cert') +
RING(dbgmgr.racf))

# refresh to make the changes visible
SETROPTS RACLIST(DIGTCERT) REFRESH

```

La règle AT-TLS décrit également l'utilisation du fichier de clés virtuel CERTAUTH pour la validation du certificat serveur présenté par l'interface graphique de débogage dans le scénario Sonde-Client. Cela implique que le certificat de l'autorité de certification utilisé par l'interface graphique de débogage est sécurisé par votre hôte z/OS.

```

# check if the CA credentials (also a certificate) are already known
RACDCERT CERTAUTH LIST
# mark the CA certificate as trusted
RACDCERT CERTAUTH ALTER(LABEL('CA cert')) TRUST
# or add the CA certificate to the database
RACDCERT CERTAUTH ADD(dsn) WITHLABEL('CA cert') TRUST

# refresh to make the changes visible
SETROPTS RACLIST(DIGTCERT) REFRESH

```

Use the following commands to verify your setup:

```

# verify started task setup
LISTGRP SYS1 OMVS
LISTUSER PAGENT OMVS
RLIST STARTED PAGENT.* ALL STDATA

# verify Policy Agent startup permission
RLIST OPERCMDS MVS.SERVCMGR.PAGENT ALL

# verify initstack protection
RLIST SERVAUTH EZB.INITSTACK.** ALL

# verify pasearch protection
RLIST SERVAUTH EZB.PAGENT.** ALL

# verify certificate setup
RACDCERT CERTAUTH LIST(LABEL('CA cert'))
RACDCERT ID(stcdbg) LIST(LABEL('dbgmgr'))
RACDCERT ID(stcdbg) LISTRING(dbgmgr.racf)

```

---

## Activation de la règle AT-TLS

La configuration de AT-TLS est maintenant terminée et la règle sera activée lors du prochain démarrage du système (IPL). Pour commencer à utiliser la règle sans IPL, procédez comme suit :

1. Activez le support AT-TLS dans la pile TCP/IP.

Créez un fichier obey TCP/IP, par exemple, TCPIP.TCPPARMS(OBEY), avec le contenu suivant :

```
TCPCONFIG TTLS
```

Activez-le à l'aide de la commande de l'opérateur suivante :

V TCPIP,,OBEY,TCPIP.TCPPARMS(OBEY)

Vérifiez le résultat en consultant le message de console suivant :

EZZ4249I stackname INSTALLED TTLS POLICY HAS NO RULES

2. Démarrez l'agent de règles.

Exécutez la commande de l'opérateur suivante :

S PAGENT

Vérifiez le résultat en consultant le message de console suivant :

EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR stackname

3. Redémarrez le gestionnaire de débogage pour interrompre toutes les sessions actives non chiffrées.

Exécutez les commandes de l'opérateur suivantes :

P DBGMR

S DBBMGR



# Bibliographie

## Publications référencées

Les publications suivantes sont référencées dans ce document :

Tableau 11. Publications référencées

Titre de la publication	Référence de la commande	Référence	Site Web de référence
Répertoire du programme d'IBM Rational Developer for z Systems	GI11-7314	Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
Répertoire du programme pour l'utilitaire hôte IBM Rational Developer for z Systems	GI11-7463	Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
IBM Rational Developer for z Systems - Guide de configuration de l'hôte	SC43-2904	Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
IBM Rational Developer for z Systems - Guide de référence de configuration de l'hôte	SC43-2902	Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
IBM Rational Developer for z Systems Common Access Repository Manager Developer's Guide	SC23-7660	Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
SCLM Developer Toolkit Administrator's Guide	SC11-6464	Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
IBM Explorer for z/OS Host Configuration Guide	SC27-8437	z/OS Explorer	
IBM Explorer for z/OS Host Configuration Reference	SC27-8438	z/OS Explorer	
Communications Server IP CICS Sockets Guide	SC31-8807	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
Communications Server IP Configuration Guide	SC31-8775	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
Communications Server IP Configuration Reference	SC31-8776	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
MVS Initialization and Tuning Guide	SA22-7591	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
MVS Initialization and Tuning Reference	SA22-7592	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
MVS JCL Reference	SA22-7597	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
MVS Planning Workload Management	SA22-7602	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>

Tableau 11. Publications référencées (suite)

Titre de la publication	Référence de la commande	Référence	Site Web de référence
MVS System Commands	SA22-7627	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
Security Server RACF Command Language Reference	SA22-7687	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
Security Server RACF Security Administrator's Guide	SA22-7683	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
UNIX System Services Command Reference	SA22-7802	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
UNIX System Services Planning	GA22-7800	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
UNIX System Services User's Guide	SA22-7801	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>
Using REXX and z/OS UNIX System Services	SA22-7806	z/OS 1.13	<a href="http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/">http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/</a>

Les sites Web suivants sont référencés dans le présent document :

Tableau 12. Sites Web référencés

Description	Site Web de référence
IBM Knowledge Center - Developer for z Systems	<a href="http://www-01.ibm.com/support/knowledgecenter/SSQ2R2/rdz_welcome.html">http://www-01.ibm.com/support/knowledgecenter/SSQ2R2/rdz_welcome.html</a>
Bibliothèque Developer for z Systems	<a href="http://www-01.ibm.com/support/docview.wss?uid=swg27038517">http://www-01.ibm.com/support/docview.wss?uid=swg27038517</a>
Page d'accueil Developer for z Systems	<a href="http://www-03.ibm.com/software/products/en/developperforsystemz/">http://www-03.ibm.com/software/products/en/developperforsystemz/</a>
Developer for z Systems Recommended service	<a href="http://www-01.ibm.com/support/docview.wss?rs=2294&amp;context=SS2QJ2&amp;uid=swg27006335">http://www-01.ibm.com/support/docview.wss?rs=2294&amp;context=SS2QJ2&amp;uid=swg27006335</a>
Developer for z Systems - Demande d'amélioration	<a href="https://www.ibm.com/developerworks/support/rational/rfe/">https://www.ibm.com/developerworks/support/rational/rfe/</a>
Télécharger Apache Ant	<a href="http://ant.apache.org/">http://ant.apache.org/</a>

## Publications d'information

Les publications suivantes peuvent s'avérer utiles pour vous aider à comprendre les incidents de configuration pour les composants de système hôte requis :

Tableau 13. Publications d'information

Titre de la publication	Référence de la commande	Référence	Site Web de référence
ABCs of z/OS System Programming Volume 9 (z/OS UNIX)	SG24-6989	Redbook	<a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a>
Guide du programmeur système pour : Workload Manager	SG24-6472	Redbook	<a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a>



Tableau 13. Publications d'information (suite)

Titre de la publication	Référence de la commande	Référence	Site Web de référence
TCPIP Implementation Volume 1: Base Functions, Connectivity, and Routing	SG24-7532	Redbook	<a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a>
TCPIP Implementation Volume 3: High Availability, Scalability, and Performance	SG24-7534	Redbook	<a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a>
TCP/IP Implementation Volume 4: Security and Policy-Based Networking	SG24-7535	Redbook	<a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a>
Tivoli Directory Server for z/OS	SG24-7849	Redbook	<a href="http://www.redbooks.ibm.com/">http://www.redbooks.ibm.com/</a>



---

## Glossaire

### action de verrouillage

Verrouille un membre.

### attribut bidirectionnel

Type de texte, orientation du texte, Permutation numérique et Permutation symétrique.

### base de données

Collection d'éléments de données liés entre eux ou indépendants, stockés ensemble, destinée à être utilisée dans une ou plusieurs applications.

### bibliothèque de chargement

Bibliothèque contenant des modules de chargement.

### bidirectionnel (bidi)

Caractérise des scripts, tels que l'arabe et l'hébreu, qui s'exécutent généralement de droite à gauche, à l'exception des nombres, qui s'exécutent de gauche à droite. La définition de ce terme est extraite du glossaire Localization Industry Standards Association (LISA).

### compiler

1. Dans les langages Integrated Language Environment (ILE), traduire des instructions source en modules qui peuvent ensuite être associés en programmes ou programmes de service.
2. Traduire tout ou partie d'un programme exprimé en langage haut niveau en un programme exprimé en langage intermédiaire, un langage d'assemblage ou un langage machine.

### conteneur

1. Dans CoOperative Development Environment/400, objet système qui contient et organise des fichiers source. Par exemple, un conteneur peut être une bibliothèque i5/OS ou un fichier partitionné pour MVS.
2. Dans l'architecture Java EE, entité qui fournit la gestion du cycle de vie, la

sécurité, le déploiement et des services d'exécution pour les composants.

(Sun) Chaque type de conteneur (EJB, Web, JSP, servlet, applet et client d'application) fournit également des services spécifiques des composants.

3. Dans Backup Recovery and Media Services, objet physique utilisé pour stocker ou déplacer des supports, tels qu'une case, un chemin ou une armoire.
4. Dans un serveur Virtual Tape Server (VTS), réceptacle dans lequel un ou plusieurs volumes logiques exportés (LVOL) peuvent être stockés. Un volume empilé qui contient un ou plusieurs LVOL et qui réside en dehors d'une bibliothèque VTS est considéré comme le conteneur de ces volumes.
5. Lieu de stockage physique des données. Par exemple, un fichier, un répertoire ou un périphérique.
6. Colonne ou rang utilisé pour la disposition d'un portlet ou d'un autre conteneur sur une page.
7. Élément de l'interface utilisateur qui contient des objets. Dans le gestionnaire de dossier, objet qui contient les autres dossiers ou documents.

### débogage

Détecter, diagnostiquer et éliminer les erreurs des programmes.

### demande de génération

Demande du client pour effectuer une transaction de génération.

### désinstallation en mode silencieux

Processus de désinstallation qui n'envoie pas les messages vers la console mais stocke les messages et erreurs dans des fichiers journaux après que la commande d'installation a été appelée.

**fichier** Unité principale de stockage et d'extraction des données, qui est

constituée d'une collection de données disposée selon une des structures imposées et décrites par les données de contrôle auxquelles le système a accès.

#### **fichier de réponses**

1. Fichier qui contient un ensemble de réponses prédéfinies aux questions envoyées par un programme afin d'éviter d'entrer ces valeurs une par une.
2. Fichier ASCII qui peut être personnalisé au moyen des données de configuration pour automatiser une installation. Les données de configuration sont généralement entrées lors d'une installation interactive alors qu'un fichier de réponses permet d'effectuer l'installation sans aucune intervention.

#### **ID action**

Identificateur numérique d'une action entre 0 et 999

#### **installation en mode silencieux**

Installation qui n'envoie pas les messages vers la console mais stocke les messages et les erreurs dans des fichiers journaux. Une installation en mode silencieux peut également utiliser des fichiers de réponses pour entrer les données.

#### **instance de référentiels**

Projet ou composant existant dans un SCM.

#### **interpréteur**

Programme qui traduit et exécute successivement toutes les instructions en langage de programmation haut niveau.

#### **interpréteur de commandes**

Interface logicielle entre les utilisateurs et le système d'exploitation qui interprète les commandes et les interactions utilisateur et les communique au système d'exploitation. Un ordinateur possède des interpréteurs de commandes sur plusieurs niveaux, qui correspondent aux différents niveaux d'interaction avec l'utilisateur.

#### **isomorphe**

A chaque élément composé (c'est-à-dire, contenant d'autres éléments) du document d'instance XML lancé à partir de la racine correspond un seul et unique élément de

groupe COBOL dont la profondeur d'imbrication est identique à la profondeur d'imbrication de son équivalent XML. Chaque élément non composé (à savoir, ne contenant pas d'autres éléments) dans le document d'instance XML, en partant du haut, comporte une seule donnée élémentaire COBOL correspondante dont la profondeur d'imbrication est identique à la profondeur d'imbrication de son équivalent XML et dont l'adresse mémoire lors de l'exécution peut être identifiée de manière unique.

#### **liste des tâches**

Liste des procédures qui peuvent être exécutées par un seul flux de contrôle.

#### **mémoire tampon des erreurs**

Partie de mémoire servant à contenir provisoirement les données de sortie des erreurs.

#### **nom d'interpréteur de commandes**

Nom de l'interface de l'interpréteur de commandes.

#### **passerelle**

1. Composant intermédiaire qui relie Internet aux environnements intranet lors des appels de service Web.
2. Logiciel qui fournit des services entre les points d'arrêt final et le reste de l'environnement Tivoli.
3. Composant de Voice over Internet Protocol constituant un pont entre VoIP et les environnements commutés par circuit.
4. Périphérique ou programme utilisé pour la connexion de réseaux ou systèmes à d'autres architectures réseau. Ces systèmes peuvent présenter des caractéristiques différentes, telles que des protocoles de communication différents, une architecture réseau ou des stratégies de sécurité différentes, la passerelle réalisant alors leur traduction et leur connexion.

### **perspective**

Groupe de vues présentant les divers aspects des ressources d'un plan de travail. L'utilisateur du plan de travail peut basculer entre les perspectives en fonction de la tâche en cours et personnaliser l'affichage des vues et des éditeurs depuis la perspective.

### **perspective Systèmes distants**

Offre une interface permettant de gérer des systèmes distants par l'intermédiaire de conventions similaires à ISPF.

**RAM** Repository Access Manager

### **référentiel**

1. Zone de stockage des données.  
Chaque référentiel comporte un nom et un type d'élément métier associé. Par défaut, son nom sera le même que celui de l'élément métier. Par exemple, un référentiel de factures sera appelé Factures. Il existe deux types de référentiels d'information : local (spécifiques du processus) et global (réutilisable).
2. Fichier VSAM dans lequel sont stockés les états des processus du BTS.  
Lorsqu'un processus ne s'exécute pas sous de contrôle du BTS, son état (et les états des tâches qui le composent) sont protégés en écriture dans un fichier de référentiel. Les états de tous les processus d'un type de processus donné (et les instances de leurs tâches) sont stockés dans le même fichier de référentiel. Les enregistrements des types multiprocessus peuvent être écrits dans ce même référentiel.
3. Zone de stockage permanente du code source et des autres ressources d'application. Dans un environnement de programmation en équipe, un référentiel partagé permet à plusieurs utilisateurs d'accéder en même temps aux ressources de l'application.
4. Collection d'informations sur les gestionnaires de file d'attente qui sont membres d'un cluster. Ces informations comprennent les noms des gestionnaires de files d'attente, leurs emplacements, leurs canaux, les files d'attente qu'ils hébergent, etc.

### **script de shell**

Fichier contenant des commandes qui peuvent être interprétées par l'interpréteur de commandes. Pour que le shell exécute les commandes du script, l'utilisateur doit saisir le nom du fichier de script à l'invite de commande du shell.

### **section de liaison**

Section de la division des données d'une unité activée (programme ou méthode appelé(e)) qui décrit les éléments de données disponibles à partir d'une unité d'activation (programme ou méthode). L'unité activée et l'unité d'activation peuvent toutes deux se référer à ces éléments de données.

### **serveur d'applications**

1. Programme qui traite toutes les opérations d'une application qui s'exécutent entre des ordinateurs dotés d'un navigateur et les applications dorsales ou bases de données de l'entreprise. Une classe spécifique de serveurs d'applications Java prend en charge la norme Java EE. Le code Java EE peut être facilement porté entre ces différents serveurs. Ils peuvent supporter des JSP et des servlets destinés au contenu Web dynamique et des EJB pour les transactions et l'accès aux bases de données.
2. Cible d'une demande émise à partir d'une application distante. Dans l'environnement DB2, la fonction du serveur d'applications est fournie par la fonction de données réparties et permet d'accéder aux données DB2 à partir d'applications distantes.
3. Programme serveur dans un réseau réparti qui fournit l'environnement d'exécution d'un programme d'application.
4. Cible d'une demande émise par un demandeur d'application. Le système de gestion de base de données du site du serveur de l'application fournit les données demandées.
5. Logiciel qui traite les communications avec le client lorsque celui-ci demande un actif et les requêtes du Content Manager.

**session de débogage**

Tâches de débogage exécutées entre l'heure à laquelle le développeur lance le débogage, et l'heure à laquelle il sort de l'application.

**Sidedeck**

Bibliothèque qui publie les fonctions d'un programme DLL. Les noms des entrées et des modules sont stockés dans la bibliothèque après la compilation du code source.

**système de fichiers distant**

Système de fichiers résidant sur un serveur ou un système d'exploitation séparé.

**système distant**

Tout autre système du réseau avec lequel votre système peut communiquer.

**transaction de génération**

Travail démarré sur MVS pour effectuer des générations après qu'une demande de génération a été reçue du client.

**URL** Uniform Resource Locator

**utilitaire ISPF (Interactive System Productivity Facility)**

Logiciel sous licence IBM servant d'éditeur plein écran et de gestionnaire de boîte de dialogue. Utilisé dans l'écriture de programmes d'application, il permet de générer des panneaux d'écran standard et des boîtes de dialogue interactives entre le programmeur et l'utilisateur final. ISPF est constitué de quatre composants principaux : DM, PDF, SCLM et C/S. Le composant DM (Dialog Manager) est le gestionnaire qui fournit des services pour les boîtes de dialogue et les utilisateurs finaux. Le composant PDF (Program Development Facility) offre des services d'aide au développeur de boîtes de dialogue ou d'applications. Le composant SCLM (Software Configuration Library Manager) offre aux développeurs d'applications des services destinés à leurs bibliothèques de développement d'applications. Le composant C/S (Client/Server), qui permet d'exécuter ISPF sur un poste de travail programmable, d'afficher les panneaux au moyen de la fonction d'affichage sur le

système d'exploitation de votre poste de travail et d'intégrer des outils et données de poste de travail au moyen des outils et des données de l'hôte.

**vue Console de sortie**

Affiche les données de sortie d'un processus et vous permet d'entrer à partir du clavier les données d'un processus.

**vue de sortie**

Affiche les messages, les paramètres et résultats associés aux objets sur lesquels vous travaillez.

**vue Définition de données**

Affiche une image locale des bases de données, ainsi que des objets qu'elles contiennent. Elle fournit également les fonctions nécessaires pour manipuler ces objets et les exporter vers une base de données distante.

**vue du navigateur**

Fournit une vue hiérarchique des ressources du plan de travail.

**non isomorphe**

Mappage simple d'éléments COBOL et d'éléments XML faisant partie de documents XML et de groupes COBOL de forme non identique (non isomorphe). Un mappage non isomorphe peut également être créé entre des éléments non isomorphes de structures isomorphes.

**vue Référentiels**

Affiche les emplacements des référentiels CVS qui ont été ajoutés à votre plan de travail.

**vue Serveurs**

Présente une liste de tous les serveurs et des configurations qui leur sont associées.

---

## Remarques

La présente documentation a été rédigée pour des produits et services proposés aux Etats-Unis. Ce matériel peut être disponible auprès d'IBM dans d'autres langues. Vous pouvez toutefois devoir détenir une copie du produit ou une version du produit dans cette langue pour pouvoir y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans certains pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit IBM. Toutefois, il appartient à l'utilisateur d'évaluer et de vérifier le fonctionnement de produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans la présente documentation. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

Pour le Canada, veuillez adresser votre courrier à :

*IBM Director of Commercial Relations  
IBM Canada Ltd.  
3600 Steeles Avenue East  
Markham, Ontario  
L3R 9Z7  
Canada*

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès du IBM Intellectual Property Department de votre pays ou par écrit à l'adresse suivante :

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION

D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Elle est mise à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et/ou programmes décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans cette documentation et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'IBM Customer Agreement, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performances et les exemples de clients ne sont présentés qu'à des fins d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation spécifiques.

Les informations concernant les produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle n'accepte aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document contient des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins



illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

#### LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programme sont fournis en l'état, sans garantie d'aucune sortie. IBM ne sera en aucun cas responsable des dommages résultant de votre utilisation des exemples de programmes.

---

## Documentation sur l'interface de programmation

---

### Marques

IBM, le logo IBM et [ibm.com](http://ibm.com) sont des marques d'International Business Machines dans de nombreux pays. Les autres noms de produits et de services sont des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

---

## Conditions d'utilisation de la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

### Conditions d'utilisation

Ces dispositions s'ajoutent aux conditions d'utilisation relatives au site Web IBM.

### Usage personnel

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

### Usage commercial

Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

## Droits

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES "EN L'ETAT" ET SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

---

## Licence de copyright

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programme sont fournis "EN L'ETAT", sans garantie d'aucune sorte. IBM ne peut en aucun cas être tenu pour responsable des dommages liés à l'utilisation de ces exemples de programme.

---

## Marques

IBM, le logo IBM et [ibm.com](http://www.ibm.com) sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produit et service sont des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à <http://www.ibm.com/legal/copytrade.shtml>.

Adobe et PostScript sont des marques d'Adobe Systems Incorporated.

Cell Broadband Engine - Sony Computer Entertainment Inc.

Rational est une marque d'International Business Machines Corporation et de Rational Software Corporation aux Etats-Unis et/ou dans certains autres pays.

Intel, Intel Centrino, Intel SpeedStep, Intel Xeon, Celeron, Itanium et Pentium sont des marques d'Intel Corporation aux Etats-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de Central Computer and Telecommunications Agency.

ITIL est une marque de Minister for the Cabinet Office.

Linear Tape-Open, LTO et Ultrium sont des marques de HP, IBM Corp. et Quantum.

Linux est une marque de Linus Torvalds.

Microsoft, Windows et le logo Windows sont des marques ou des marques déposées de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java et toutes les marques et logos incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.



---

# Index

## A

accès au débogueur intégré 22  
activation de la règle AT-TLS 50  
agent de règles, tâche démarrée 44  
AQEZPCM 11  
authentification du gestionnaire de débogage 11  
autorisation APF  
    FELSFELAUTH 23

## B

bibliothèques contrôlées par programme  
    MVS pour RSE, Définition 17  
bibliothèques contrôlées pour RSE,  
    Définition par programme MVS 17  
bibliothèques pour RSE, définition par  
    programme MVS 17

## C

CARMA et ports TCP/IP 27  
CICSTS, sécurité 13  
classification des charges de travail,  
    WLM 29  
communication, externe 25  
communication, Interne 26  
communication chiffrée  
    débogueur intégré 12  
communication interne 26  
communications externes 25  
configuration AT-TLS,  
    PROFILE.TCPIP 44  
configuration de AT-TLS 43  
configuration de l'agent de règles 45  
configuration de syslogd 44

## D

débogage, sécurité 13  
débogage, transactions CICS 41  
débogage de transactions CICS 41  
débogueur intégré 6  
    communication chiffrée 12  
débogueur intégré, accès 22  
définition de droit d'accès aux fichiers  
    z/OS UNIX pour RSE 19  
définition de fichiers contrôlés par  
    programme z/OS UNIX pour RSE 20  
définition de la prise en charge de  
    passticket pour RSE 18  
Définition des bibliothèques contrôlées  
    par un programme MVS pour RSE 17  
définition des objectifs, WLM 31  
définition du serveur RSE en tant que  
    serveur z/OS UNIX sécurisé 16  
définitions, sécurité 14  
définitions de sécurité 14

définitions de sécurité, Liste de  
    contrôle 14  
démon Lock (LOCKD) 4  
démon RSE 25  
démon RSE (RSED) 4  
description de Developer for z  
    Systems 3  
Developer for z Systems, description 3  
Developer for z Systems, présentation du  
    composant  
    représentation graphique 3  
droit d'accès aux fichiers z/OS UNIX,  
    définir pour RSE 19

## E

Enterprise Service Tools 41  
envoi au client, remarques sur la  
    fonction 37

## F

FEJJCNFG 26  
FELRACF, définitions de sécurité 14  
fichiers contrôlés par programme UNIX  
    pour RSE, définition 20  
fichiers contrôlés par programme z/OS  
    UNIX pour RSE, définition 20

## G

gestionnaire de débogage,  
    authentification 11  
gestionnaire de déploiement d'application  
    (ADM) 4

## I

intégré, débogueur 6  
introduction, remarques relatives à la  
    fonction d'envoi au client 37

## J

JMON 21

## M

messages IRZ 41  
messages IRZ de diagnostic 41  
Méthodes, Authentification 11  
méthodes d'authentification 11  
mises à jour de sécurité AT-TLS 48  
moniteur de travaux JES (JMON) 4

## O

objectifs, définition dans WLM 31

## P

paramètres de sécurité, vérification 23  
paramètres et classes, Activation de la  
    sécurité 15  
paramètres et classes de sécurité,  
    Activation 15  
port TCP/IP, réservation 27  
ports, CARMA et TCP/IP 27  
ports, TCP/IP 25  
ports TCP/IP 25  
ports TCP/IP, représentation  
    graphique 25  
présentation du composant, Developer  
    for z Systems  
    représentation graphique 3  
prise en charge de langues,  
    bidirectionnelles 41  
prise en charge de langues  
    bidirectionnelles 41  
PROFILE.TCPIP, configuration  
    AT-TLS 44  
profils, Définition de fichier 22  
profils de fichier, Définition 22  
projets, résidant sur l'hôte 38  
projets résidant sur l'hôte 38  
propriétaires de tâches 4  
protection d'application pour RSE,  
    définition 19  
publications, référencées 53  
publications référencées 53

## R

règle AT-TLS 45  
règles de classification, WLM 30  
remarques, sécurité 11  
remarques à propos de WLM xiv, 29  
remarques relatives à CICSTS 41  
remarques relatives à la sécurité 11  
remarques relatives à TLS v1.2 47  
réservation, port TCP/IP 27  
réservation de port TCP/IP 27  
RSE, définition d'un serveur z/OS UNIX  
    sécurisé 16  
RSE, Définition de droit d'accès aux  
    fichiers z/OS UNIX 19  
RSE, définition de fichiers contrôlés par  
    programme z/OS UNIX pour 20  
RSE, définition de la protection  
    d'application pour 19  
RSE, définition des bibliothèques  
    contrôlées par programme MVS 17  
RSE, définition du support passticket  
    pour 18

## S

SCLM, sécurité 13  
SCLM Developer Toolkit 17  
SCLM Developer Toolkit (SCLMDT) 4

- sécurité, CICSTS 13
- sécurité, connexion 12
- sécurité, définition des commandes
  - JES 20
- sécurité, SCLM 13
- sécurité des commandes, définition
  - JES 20
- sécurité des commandes JES,
  - définition 20
- sécurité des connexions 12
- sécurité du débogage 13
- segment, Définition OMVS 16
- segment OMVS, Définition 16
- serveur RSE 25
- serveur UNIX, définition de RSE en tant
  - que 16
- serveur z/OS UNIX, définition de RSE en
  - tant que 16
- serveur z/OS UNIX sécurisé, définition
  - de RSE en tant que 16
- service Commandes TSO 4
- structure de répertoire, z/OS UNIX
  - représentation graphique 9
- structure de répertoire z/OS UNIX
  - représentation graphique 9
- support passticket pour RSE,
  - Définition 18
- support pour RSE, définition du
  - passticket 18

## T

- tâche démarrée par l'agent de règles 44
- tâches démarrées, définir pour Developer
  - for z Systems
    - tâches démarrées JMON 16
    - tâches démarrées RSED 16
- tâches démarrées Developer for z
  - Systems, définir 16
- types de sous-système
  - ASCH 30
  - CICS 30
  - JES 30
  - OMVS 30
  - STC 30

## V

- Vérification des paramètres de
  - sécurité 23

## W

- WLM, règles de classification 30
- workload manager 29





SC43-2902-00

