IBM Host On-Demand version 13.0

Planification, installation et configuration de Host On-Demand

SC43-3097-02

IBM Host On-Demand version 13.0

Planification, installation et configuration de Host On-Demand

SC43-3097-02

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'Annexe E, «Remarques», à la page 167.

Neuvième édition (février 2016)

Réf. US : SC14-7266-02

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 s'applique à la version 12 d'IBM Host On-Demand (numéro de programme 5724-I20) et à toutes les versions et modifications ultérieures sauf avis contraire mentionné dans les nouvelles éditions.

Cette édition s'applique à la version 12 d'IBM Host On-Demand (numéro de programme 5724-I20) et à toutes les versions et modifications ultérieures sauf avis contraire mentionné dans les nouvelles éditions.

Table des matières

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

Le manuel *Planification, installation et configuration de Host On-Demand* vous aide à planifier, installer et configurer le programme Host On-Demand. Ce manuel s'adresse aux administrateurs. Il est divisé en trois parties principales.

Partie 1, «Planification», à la page 1 vous donne des informations relatives à Host On-Demand dont vous devez prendre connaissance avant l'installation et le déploiement. Par exemple, quelle plateforme allez-vous utiliser ? Quel modèle de déploiement allez-vous utiliser ? Comment allez-vous mettre en place la sécurité ?

Partie 2, «Installation, mise à niveau et désinstallation de Host On-Demand», à la page 45 présente les procédures pas à pas en fonction de chaque système d'exploitation.

Partie 3, «Configuration de Host On-Demand», à la page 65 décrit les différents modèles de configuration afin de préciser la manière dont vous allez définir et gérer les informations de configuration de session, les modifier dynamiquement, personnaliser les nouveaux clients et déployer Host On-Demand vers les utilisateurs.

Après avoir effectué l'installation et la configuration de Host On-Demand, utilisez l'aide en ligne pour apprendre à définir des sessions et à effectuer d'autres tâches d'administration.

Planification, installation et configuration de Host On-Demand est également disponible dans le Host On-Demand Knowledge Center.

A propos des autres documents Host On-Demand

Outre le manuel *Planification, installation et configuration de Host On-Demand*, d'autres sources d'informations vous sont proposées pour vous aider à utiliser ce produit. Pour obtenir la documentation décrite ici, accédez à Host On-Demand Knowledge Center. La plupart des documents sont également disponibles dans le produit ou les kits d'outils Host On-Demand.

La fonction MySupport vous permet de personnaliser la vue de votre support et de vous enregistrer afin de recevoir chaque semaine des notifications par courrier électronique qui vous informent des nouveaux groupes de correctifs, téléchargements et informations du support technique relatifs aux produits IBM. Pour s'inscrire aux notifications de support, voir About my notifications.

- *Aide en ligne*. L'aide en ligne est la première source d'informations pour les administrateurs et les utilisateurs après l'installation complète de Host On-Demand. Elle présente la procédure d'exécution détaillée des différentes tâches Host On-Demand. Une table des matières et un index vous permettent de rechercher les écrans d'aide orientée tâches et les écrans d'aide conceptuelle. Lorsque vous utilisez l'interface graphique Host On-Demand, les boutons d'aide permettent d'ouvrir des écrans d'aide pour l'interface graphique.
- *Fichier readme*. Le fichier readme.html contient des informations relatives au produit élaborées trop tard pour être insérées dans la documentation.
- *Web Express Logon Reference*. Ce manuel propose une approche par étapes pour comprendre, mettre en oeuvre et identifier les incidents de la fonction Web

Express Logon. Elle offre une présentation de Web Express Logon, plusieurs exemples détaillés pour vous aider à planifier et déployer Web Express Logon dans votre environnement, ainsi que plusieurs API pour l'écriture de macros et plug-in personnalisés.

- *Macro Programming Guide*. Ce manuel décrit comment créer des macros Host On-Demand pour automatiser les interactions utilisateur avec des applications hôte ou pour transmettre des données entre une application hôte et une application native. Ce manuel fournit des informations détaillées sur tous les aspects liés au développement de macros et comprend une révision des informations relatives au langage de macro précédemment publié dans le manuel "Host Access Beans for Java Reference".
- *Host Printing Reference*. Après avoir configuré vos sessions hôte, utilisez Host Printing Reference pour permettre aux utilisateurs d'enregistrer leurs informations de session hôte dans un fichier ou de les imprimer sur une imprimante locale ou connectée à un réseau LAN.
- *Session Manager API Reference*. Ce manuel fournit des API JavaScript pour la gestion des sessions hôte et des interactions textuelles avec elles.
- *Programmable Host On-Demand*. Ce manuel fournit un ensemble d'API Java permettant aux développeurs d'intégrer différentes parties du code client Host On-Demand, telles que les terminaux, menus et barres d'outils, dans leurs propres applications et applets Java personnalisées.
- *Toolkit Host Access*. Ce manuel explique comment installer et configurer l'outil de développement de Host On-Demand, qui est livré avec Host Access Client Package. L'outil de développement de Host On-Demand est complémentaire du produit de base Host On-Demand puisqu'il offre des Beans Java et d'autres composants qui vont vous aider à optimiser Host On-Demand dans votre environnement.
- *Host Access Beans for Java*. Ce manuel fait partie de l'outil de développement de Host On-Demand. Il est la référence des programmeurs qui souhaitent personnaliser l'environnement Host On-Demand à l'aide des Beans Java et créer des macros pour automatiser la procédure des sessions d'émulation.
- *Host Access Class Library for Java*. Ce manuel fait partie de l'outil de développement de Host On-Demand. Il est la référence des programmeurs qui souhaitent écrire des applets et des applications Java qui accèdent aux informations de l'hôte au niveau du flux de données.
- *Host On-Demand J2EE Connector*. Ce manuel fait partie de l'outil de développement de Host On-Demand. Il sert de référence des programmeurs qui veulent écrire des applets et des servlets qui accèdent à des applications compatibles avec J2EE (Java Enterprise Edition).

Conventions utilisées dans le présent manuel

Les conventions typographiques suivantes sont utilisées dans le manuel *Planification, installation et configuration de Host On-Demand* :

Tableau 1. Conventions utilisées dans le présent manuel

Conventions	Signification
`Non proportionnelle`	Indique le texte que vous devez saisir à une invite de commande et les valeurs que vous devez utiliser de manière littérale, comme les commandes, les options et les attributs de définition des ressources et leurs valeurs. La police non proportionnelle indique également le texte à l'écran et les exemples de code.

Tableau 1. Conventions utilisées dans le présent manuel (suite)

Conventions	Signification
Italique	Signale les valeurs de variable que vous devez fournir (vous devez par exemple entrer le nom d'un fichier pour *filename*). Les caractères en italique sont également utilisés pour les mises en valeur de texte et les titres de manuel.
Retour	Fait référence à la touche libellée Retour ou Entrée, ou représentée par une flèche vers la gauche.
>	Dans les descriptions de menu, affiche une série d'options de menus. Par exemple, “Cliquez sur Fichier > Nouveau” signifie “A partir du menu Fichier, cliquez sur la commande Nouveau.”
	Dans les descriptions d'arborescence, permet d'afficher une série de dossiers ou de développements d'objets. Par exemple, “Développez Servlet HODConfig > Sysplexes > Plex1 > Serveurs J2EE > BBOARS2” signifie : 1. Développez le dossier Servlet HODConfig 2. Développez le dossier Sysplexes 3. Développez le dossier Plex1 4. Développez le dossier Serveurs J2EE 5. Développez le dossier BBOARS2

Cette image attire l'attention du lecteur sur les remarques.

Cette image attire l'attention du lecteur sur les conseils.

Terminologie

Cette section décrit la terminologie employée dans le présent manuel.

applet Un programme écrit en Java qui est référencé dans un fichier HTML. Une applet est lancée par JVM (Java Virtual Machine) qui est exécuté dans un navigateur Web.

application
Programme ou suites de programmes accomplissant une tâche ou une fonction spécifique.

client en cache
Un client en cache Host On-Demand correspond à n'importe quel client Host On-Demand dont les composants ont été placés en mémoire cache, c'est-à-dire stockés localement pour permettre d'y accéder rapidement, sur le disque dur du poste de travail d'un utilisateur.

répertoire de publication par défaut
Le répertoire de diffusion par défaut est le sous-répertoire HOD qui se trouve dans le répertoire d'installation du serveur Host On-Demand ; par exemple, `c:\Program Files\IBM\HostOnDemand\HOD\` sur les plateformes Windows et `/opt/IBM/HostOnDemand/HOD` sur les plateformes AIX, Linux, Solaris, `/QIBM/Programs/IBM/HostOnDemand/HOD` sur i(as/400) et `/usr/lpp/HOD/hostondemand/HOD` sur les plateformes z/OS.

client téléchargé
Les clients téléchargés procèdent eux-mêmes au téléchargement des fichiers d'applet nécessaires, chaque fois que l'utilisateur accède aux fichiers HTML. D'une manière générale, les clients téléchargés sont utilisés dans des environnements en réseau car les connexions réseau haut débit permettent de réduire le délai de téléchargement à partir du serveur Web.

client d'émulation
Un client d'émulation désigne un client Host On-Demand qui lance une session d'émulateur de terminal. Les clients d'émulation fournis avec Host On-Demand sont le client en cache, le client Web Start et le client téléchargé.

répertoire de diffusion utilisateur distinct
Fournit un emplacement séparé accessible en écriture permettant de déployer des fichiers HTML personnalisés, en les isolant des fichiers fournis avec Host On-Demand. Cette possibilité garantit l'accessibilité en lecture seule du répertoire de diffusion de Host On-Demand et facilite l'application des futures mises à niveau.

Remarque : D'autres fichiers modifiés par l'utilisateur (les applets personnalisés ou les programmes HACL, par exemple) doivent encore être exécutés à partir du répertoire de diffusion Host On-Demand.

serveur d'applications Web
Programme d'exécution des applications Web dynamiques. Le serveur d'applications Web inclut la prise en charge des technologies Java Servlet, JSP (JavaServer Pages) et d'autres API (interfaces de programmation d'application) Java d'entreprise. Un serveur d'applications Web fournit les fonctions de communication, de gestion des ressources, de sécurité, de gestion des transactions et de persistance nécessaires aux applications Web. Il comprend aussi généralement une interface d'administration pour la gestion du serveur et des applications déployées.

serveur Web
Serveur connecté à Internet, qui sert des requêtes relatives à des documents HTTP. Un serveur Web contrôle le flux de transactions vers et à partir du navigateur. Il protège la confidentialité des transactions du client et lui garantit que son identité est transmise au serveur en toute sécurité.

Client Web Start
Le client Web Start permet aux utilisateurs d'exécuter des sessions Host On-Demand sans nécessiter de navigateur. Les sessions Host On-Demand sont démarrées via le gestionnaire d'applications de Java Web Start.

Termes relatifs à Java

Notez les termes suivants, ainsi que leur utilisation dans le présent document.

Java Fait référence à JRE (Java Runtime Environment) sur le serveur ou le client HOD.

navigateur compatible Java
Navigateur Web exécutant des applets Java sur la machine virtuelle Java d'un plug-in Java installé, par exemple, Firefox et Internet Explorer avec un plug-in Java. Pour plus d'informations, reportez-vous à «Navigateurs et plug-in Java», à la page 18.

client d'émulation Java, client en cache Java, client téléchargé Java
Version données du client Host On-Demand. La version Java est constituée d'un ensemble complet des composants du client Host On-Demand, compilés via un programme Java.

Partie 1. Planification

Chapitre 1. Présentation d'IBM Host On-Demand

Host On-Demand - Présentation

IBM Host On-Demand propose un accès hôte économique et sécurisé aux utilisateurs par l'intermédiaire ou non d'un navigateur dans des environnements intranet et extranet. Host On-Demand est installé sur un serveur Web, pour une gestion administrative et un déploiement simplifiés. L'applet ou application Host On-Demand est chargée sur le navigateur client afin de lui assurer la connectivité aux applications et données importantes du système hôte.

Host On-Demand prend en charge l'émulation de tous types de terminaux communs, de protocoles de communication, de passerelles de communication et d'imprimantes, à savoir :

- les terminaux TN3270 et TN3270E
- les terminaux TN5250
- les terminaux VT52, VT100, VT220, VT320 et VT420
- Secure Shell (SSH)
- Transport Layer Security (TLS)
- le protocole FTP (File Transfer Protocol)
- la passerelle de transaction CICS (Customer Information and Control System)
- les imprimantes TN3270E et TN5250

Vous pouvez utiliser Host Access Toolkit, outil de développement basé sur des composants Java, afin de créer des applications e-business personnalisées. Cet outil contient un vaste ensemble de bibliothèques Java et d'interfaces de programme d'application (API) : Host Access Class Library (HACL), Host Access Beans for Java et Java Enterprise Edition (J2EE). Host On-Demand contient également Database On-Demand, interface destinée à l'envoi de requêtes SQL (Structured Query Language) aux bases de données DB2 d'IBM hébergées par les systèmes IBM System i7.

Host On-Demand - Fonctionnement

L'illustration et les explications ci-dessous présentent le fonctionnement du système Host On-Demand. Host On-Demand est un système client-serveur. Les clients Host On-Demand sont des applets Java téléchargées du serveur Web vers un navigateur Web sur un ordinateur éloigné.

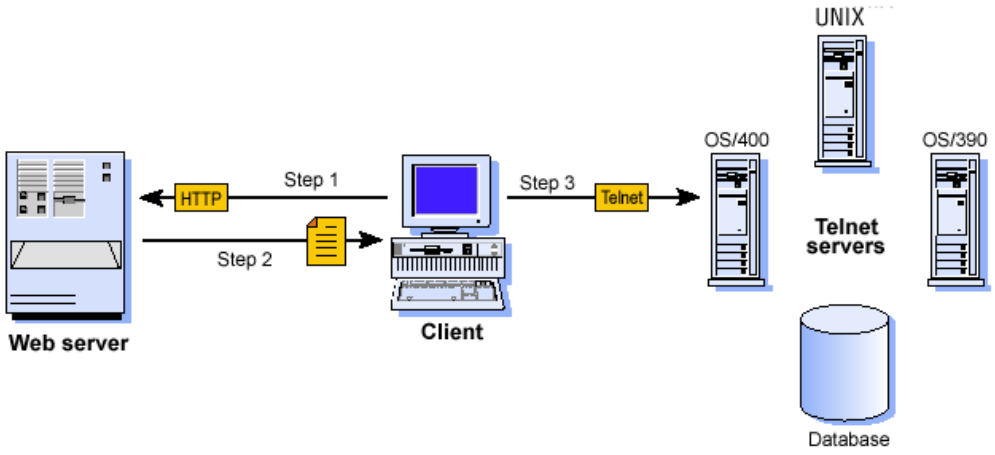

Figure 1. Fonctionnement de Host On-Demand

Etape 1. L'utilisateur ouvre un navigateur et clique sur un lien hypertexte.

Etape 2. L'applet IBM Host On-Demand est téléchargée sur le poste de travail client.

Etape 3. Une fois l'applet téléchargée, IBM Host On-Demand se connecte directement à un serveur Telnet afin d'accéder aux applications hôte.

Les informations de session sont configurées dans le fichier HTML ou sur le serveur de configuration Host On-Demand. Pour plus d'informations sur le serveur de configuration, reportez-vous à Chapitre 2, «Planification du déploiement», à la page 11.

Les applets de client Host On-Demand peuvent être exécutées comme des clients téléchargés, des clients Web Start ou des clients en cache. Les clients téléchargés le sont depuis un serveur Web à chaque fois qu'ils sont utilisés. Le client en cache et les clients Web Start sont téléchargés à partir du serveur Web et stockés sur l'ordinateur client. Après le premier téléchargement, le client en cache est chargé depuis une machine locale. Le client en cache vérifie les nouvelles versions du client sur le serveur Host On-Demand et télécharge automatiquement la mise à jour.

Host On-Demand inclut les composants administratifs suivants :

- L'assistant de déploiement, outil permettant de créer des fichiers HTML de client d'émulation. Il permet aux administrateurs de concevoir rapidement et aisément des fichiers Host On-Demand personnalisés en fonction des besoins de l'entreprise.
- Les clients d'administration, qui peuvent être utilisés par les administrateurs afin de définir des sessions communes, créer des utilisateurs et des groupes et exécuter d'autres tâches administratives sur le serveur Host On-Demand.

En outre, un certain nombre de clients prédéfinis sont également fournis avec Host On-Demand afin de présenter les fonctionnalités du client Host On-Demand aux utilisateurs et aux administrateurs (émulation, Database On-Demand, retrait d'un client en cache et utilitaires d'identification des incidents, par exemple).

Avantages de Host On-Demand

Une connectivité économique

Vous pouvez réduire vos coûts en matière de maintenance et augmenter le retour sur investissement en installant Host On-Demand sur un serveur Web. Ainsi, vous ne gérez plus les postes utilisateur individuels.

Les applets résident sur un serveur et sont téléchargées sur les navigateurs Web à la demande, ce qui élimine les tâches de planification de la maintenance et des mises à niveau. Il suffit de mettre à niveau le logiciel sur le serveur pour que les utilisateurs puissent recevoir la mise à niveau lorsqu'ils accèdent à l'applet client.

Gestion centralisée des données de configuration

Les administrateurs peuvent centraliser la définition et le contrôle de toutes les informations relatives à la configuration de la session mises à la disposition des utilisateurs, à savoir les options de connexion, les fonctions de sécurité, les définitions de macro, les spécifications du clavier et le mappage des couleurs. De plus, les administrateurs ont toute liberté pour décider des zones que l'utilisateur peut ou ne peut pas modifier. Ils peuvent choisir l'emplacement de stockage des mises à jours utilisateur.

Sur les plateformes Windows, l'interface graphique utilisateur Host On-Demand par défaut est basée sur l'interface Nimbus fournie par Java version 1.6 et supérieure. Vous pouvez désactiver l'interface Nimbus des interfaces graphiques utilisateur d'administration en définissant la variable d'environnement **SETHODNIMBUSGUI** sur `false`.

Connexion directe à un serveur Telnet

Avec Host On-Demand, l'applet client contient des fonctionnalités d'émulation. Avec l'émulateur résidant sur le client, il est possible d'éliminer le serveur de niveau intermédiaire, comme IBM Communications Server ou un serveur SNA tiers. Tout point de sécurité et de performance inhérent à cet élément intermédiaire sera également supprimé. Une fois que le client dispose de l'applet, la connexion directe à un serveur Telnet standard est aisée. Ce type de serveur fournit un accès optimal aux données requises. Vous pouvez accéder à plusieurs sessions hôte simultanément. Host On-Demand réduit les restrictions en termes de capacité, en écartant tout recours à un serveur intermédiaire. Pour comprendre son fonctionnement, reportez-vous à figure 1, à la page 4.

Interface utilisateur via un navigateur

L'accès à Host On-Demand par le biais d'un navigateur vous permet de centraliser la gestion et le déploiement en toute simplicité des applications et données vitales d'un système hôte. Host On-Demand utilise la puissance de la technologie Java pour cet accès direct à partir de votre navigateur. Il vous suffit de cliquer sur un lien pour démarrer l'applet Java Host On-Demand. Cette solution de connectivité Web-système hôte offre un accès sécurisé, via un navigateur Web, aux applications et aux données hôte par une émulation de type Java. Vous pouvez ainsi utiliser sur le Web des applications hôte existantes sans avoir à effectuer de tâche de programmation. Host On-Demand étant fondé sur la technologie Java, sa présentation ne varie pas en fonction des divers systèmes d'exploitation.

Sur les plateformes Windows, l'interface graphique utilisateur du client Host On-Demand par défaut est basée sur l'interface Nimbus fournie par Java version

1.6 et supérieure. Vous pouvez désactiver l'interface Nimbus à l'aide du paramètre HTML **setHODNimbusGUI** ou de la variable d'environnement **SETHODNIMBUSGUI**.

Remarque : Les portlets Host On-Demand héritent de la présentation de leur serveur de portail.

Prise en charge de différentes plateformes et environnements de réseau

Un large éventail de plateformes prend en charge les serveurs et clients Host On-Demand qui peuvent être utilisés via tout réseau TCP/IP. Cela assure une plus grande flexibilité quant à la configuration de votre système et permet de déployer Host On-Demand dans votre environnement informatique sans vous équiper de nouveau matériel.

Prise en charge de Java

Host On-Demand est compatible avec les navigateurs qui prennent en charge les normes Java. En outre, certaines nouvelles fonctions de Host On-Demand tirent parti des fonctionnalités exclusivement liées à Java.

Prise en charge du protocole Internet version 6

La prise en charge du protocole IP version 6 nécessite Java 1.4 ou une version supérieure. Cependant, Host On-Demand Version 13 prend en charge Java version 1.6 ou supérieure.

Le protocole IP (Internet Protocol) permet d'acheminer des données de leur source vers leur destination via un environnement Internet. Ce protocole est un intermédiaire entre les couches de protocoles supérieures et le réseau physique.

Le protocole IP version 6 remplace le protocole IP version 4. Le protocole IP version 6 développe le nombre d'adresses IP disponibles et apporte des améliorations en termes d'acheminement et de configuration réseau. Les protocoles IP version 6 et version 4 ont été conçus par le groupe de travail IETF (Internet Engineering Task Force).

En général, l'Internet utilise actuellement le protocole IP version 4. Le protocole IP version 6 est prévu pour remplacer le protocole IP version 4 dans quelques années.

Le serveur Host On-Demand prend également en charge le protocole IP version 6 pour l'agent de réacheminement. Pour plus d'informations, reportez-vous à «Support de l'Agent de réacheminement pour IPv6», à la page 29.

Prise en charge de plusieurs langues nationales

Host On-Demand est disponible en de nombreuses langues, dont celles qui utilisent un jeu de caractères codés sur deux octets (DBCS). En outre, Host On-Demand offre la prise en charge du symbole de l'euro, ainsi que du clavier et de la page de codes de nombreuses langues, telles que l'arabe, l'hébreu et le thaï. Toutes les versions sont disponibles sur le même support, et vous pouvez accéder à plusieurs versions simultanément.

Connexions sécurisées

L'utilisation du protocole TLS (Transport Layer Security) permet à Host On-Demand d'étendre l'accès sécurisé aux données de l'hôte, aux réseaux intranet et extranet, et à Internet. Les travailleurs itinérants peuvent ainsi accéder à un site

Web sécurisé, s'authentifier et établir une communication avec un système hôte sécurisé. Avec la prise en charge du certificat serveur et client, Host On-Demand peut présenter un certificat numérique au serveur Telnet, tel qu'IBM Communications Server for z/OS, pour l'authentification.

Vous pouvez également configurer Host On-Demand et l'utiliser dans des environnements dotés de pare-feu. Les ports de pare-feu doivent être ouverts aux fonctions définies dans vos définitions de session Host On-Demand. Pour plus d'informations, reportez-vous à «Utilisation de Host On-Demand avec un pare-feu» , à la page 30.

Fichiers HTML personnalisés

Host On-Demand inclut un assistant de déploiement qui permet de créer des fichiers HTML personnalisés. Avec ces fichiers, vous pouvez adapter le contenu du client et de la fonction aux besoins de groupes d'utilisateurs spécifiques. Pour plus d'informations sur l'assistant de déploiement, reportez-vous à Chapitre 8, «Configuration des clients d'émulation de Host On-Demand», à la page 67.

Kit d'outils de création de nouvelles applications e-business

Host On-Demand est accompagné de Host Access Toolkit, kit d'outils de développement basé sur des composants Java permettant de créer des applications e-business personnalisées. Ce kit d'outils contient un vaste ensemble de bibliothèques Java et d'interfaces de programme d'application (API), notamment Host Access Class Library (HACL), Host Access Beans for Java et Java Enterprise Edition (J2EE).

HACL offre une interface API non visuelle qui communique avec des machines hôte dorsales exécutant des applications à l'origine conçues pour une interaction humaine. Les applications hôte s'appuient sur une présentation de caractères lisibles, sur des zones formatées, sur une codification par couleur et sur des réponses au clavier. HACL fournit des classes spécialisées pour les fonctionnalités nécessaires à l'imitation des interactions traditionnelles avec une série de présentations de l'écran hôte (écrans verts). HACL ne contient aucune classe d'interface graphique (composant visible). Un programme Java peut par exemple être exécuté sur un grand système en tant qu'application secondaire. Le programme d'application secondaire interagit au premier niveau avec un autre grand système exécutant une application de données CICS, puis avec un navigateur client via des pages HTML générées dynamiquement. L'application secondaire interprète les données d'entrée du client en tant qu'actions du terminal simulées, qui sont envoyées à la machine CICS exécutant l'API HACL. Les écrans de réponse renvoyés par la machine CICS sont capturés via les API HACL, convertis en pages HTML dynamiques, puis renvoyées au client.

Le connecteur J2EE de Host On-Demand fournit un ensemble d'adaptateurs de ressources qui communiquent avec les hôtes 3270, 5250, CICS et VT. Ces adaptateurs de ressources sont déployés sur un serveur d'applications conforme, tel IBM Application Server. Les utilisateurs peuvent écrire des applications Web à l'aide des API fournies dans le connecteur Host On-Demand J2EE via WebSphere Studio Application Developer Integration Edition.

Host On-Demand programmable

La fonction Host On-Demand programmable fournit un ensemble d'API Java permettant aux développeurs d'intégrer différentes parties du code client Host On-Demand, telles que les terminaux, menus et barres d'outils, dans leurs propres

applications et applets Java personnalisées. L'API offre au développeur un contrôle intégral du bureau Host On-Demand (interface utilisateur) sans utilisation des Javabeans Host Access fournis dans le Toolkit. Le code Host On-Demand sous-jacent gère tout le "câblage" entre les différents composants, y compris la sauvegarde des préférences de l'utilisateur (macros, redéfinition des touches du clavier et des couleurs) dans le système de fichiers local, en vue de leur réutilisation ultérieure. Le développeur doit uniquement définir la configuration du bureau Host On-Demand. Pour plus d'informations, reportez-vous à Programmable Host On-Demand Reference.

API du gestionnaire de sessions Host On-Demand

Outre les interfaces de programmation d'applications (API) fournis avec Host Access Toolkit, Host On-Demand contient des API publiques spécialisées destinées à assurer la prise en charge de sessions hôtes imbriquées dans des pages Web utilisant JavaScript. Ces API JavaScript destinées à aider les développeurs d'applications à gérer les sessions hôtes et leurs interactions avec des données texte sont disponibles via le gestionnaire de sessions de Host On-Demand. Pour plus d'informations, reportez-vous à Session Manager API Reference.

Prise en charge de WebSphere Portal

Sur Portal Server, composant de WebSphere Portal, Host On-Demand peut s'exécuter comme un portlet. Le serveur de portail offre des fonctionnalités de sécurité et de gestion de bureau sophistiquées qui permettent aux administrateurs de mieux contrôler les droits d'accès des utilisateurs et aux utilisateurs de mieux gérer l'affichage et l'organisation du bureau du portail.

Les administrateurs peuvent rapidement créer des portlets Host On-Demand personnalisés et aisément utiliser l'assistant de déploiement avant de les télécharger directement dans Portal Server.

Remarque : Portal Server est un produit distinct et nécessite une installation indépendante.

Connexions aux bases de données DB2 sur les serveurs IBM System i

Database On-Demand est fourni avec Host On-Demand afin d'offrir un accès aux informations DB2 stockées sur les serveurs IBM System i5 via un pilote JDBC (Java Database Connectivity). Database On-Demand est une applet Java qui offre la possibilité d'émettre des requêtes SQL (Structured Query Language) sur des bases de données IBM System i5 via un pilote JDBC. Database On-Demand est une applet indépendante de l'applet Host On-Demand et lancée par un fichier HTML distinct. Vous pouvez également utiliser le support de transfert de données à partir d'une session d'émulation pour exécuter des requêtes SQL si vous avez à la fois besoin d'une émulation de terminal et d'un support de requêtes SQL.

Nouveautés

Obtention des dernières informations relatives à Host On-Demand

Pour obtenir les toutes dernières informations concernant Host On-Demand Version 13, reportez-vous à le fichier readme du produit.

Pour obtenir des informations à jour relatives au produit, accédez au site Web Host On-Demand.

Pour consulter les dernières informations techniques relatives à Host On-Demand, accédez au site Host On-Demand Support Portal.

Pour obtenir des informations d'ordre général sur la prise en charge des logiciels, accédez à Software Support Handbook.

Nouvelles fonctions de Host On-Demand Version 13

Les fonctionnalités et améliorations suivantes ont été ajoutées à Host On-Demand version 13 :

- 1. Une nouvelle fonction de recherche de bureau facilite la recherche d'une session sur le bureau HOD. Elle facilite l'utilisation lorsque le nombre de définitions de session est important
- 2. **100% conforme au protocole TLS**
- a. JSSE est défini par défaut pour les connexions sécurisées (y compris pour l'agent de réacheminement et les applications HACL)
- b. Le serveur proxy est pris en charge avec JSSE.
- c. La connexion FTP sécurisée prendra également en charge les connexions TLS.
- d. Le filtrage de certificats client basé sur l'utilisation de clés et de clés étendues pour le client FTP est également pris en charge.
- 3. **Plein écran** - Les utilisateurs peuvent basculer entre la taille d'écran par défaut et le mode plein écran pour faciliter l'utilisation.
- Les polices évoluent pour occuper toute la zone de présentation lors du redimensionnement de l'écran, ce qui permet d'éliminer l'espace vide supplémentaire.
- 5. Nouvelle impression générale avec des icônes de barre d'outils et de barre de menus améliorées, ainsi que des éléments de menu réarrangés pour une meilleure convivialité
- 6. **HACP Extended Edition** - Un nouveau composant HACP EE a été ajouté à HOD 13. HACP EE est un émulateur Web gratuit sans plug-in.
- 7. GSKit n'est plus livré avec Host On-Demand pour la plateforme Windows. Les connexions d'agent de réacheminement utilisent JSSE pour la connexion sécurisée. Sur les plateformes autres que Windows, GSKit est à l'heure actuelle toujours livré.
- 8. **Utilitaire de migration** - Un nouvel utilitaire de migration de ligne de commande est dorénavant disponible pour la migration transparente de la version 11 et/ou 12 à la version 13.

Chapitre 2. Planification du déploiement

Host On-Demand permet d'accéder aux applications hôte depuis un navigateur Web. Le navigateur télécharge l'applet Java Host On-Demand depuis le serveur Web et se connecte à un serveur Telnet pour accéder aux applications hôte. L'applet Host On-Demand doit disposer des données de configuration pour déterminer à quel hôte elle va se connecter et définir d'autres propriétés de la session hôte. Ces informations de configuration peuvent être fournies à l'applet Host On-Demand à partir d'un fichier HTML qui permet de lancer Host On-Demand ou par le serveur de configuration Host On-Demand. Le serveur de configuration est un élément de Host On-Demand qui stocke de façon centralisée les données de configuration des sessions et les préférences utilisateur par ID utilisateur et ID de groupe. Les utilisateurs peuvent ainsi accéder aux données des sessions et aux préférences utilisateur via le serveur de configuration. Ce dernier est géré par le client d'administration. Pour obtenir des informations relatives à la configuration du serveur de configuration Host On-Demand, reportez-vous à l'aide en ligne.

Au fur et à mesure que les navigateurs Web commenceront à supprimer la prise en charge des plug-ins Java, les clients Host On-Demand continueront de travailler avec certaines limitations, telles qu'indiquées dans Prise en charge de navigateur Host On-Demand.

Vous pouvez créer les fichiers HTML personnalisés du client à l'aide de l'assistant de déploiement. Lorsque vous créez ces fichiers HTML, vous pouvez choisir parmi trois modèles de configuration différents pour spécifier comment les informations de configuration de session et les préférences utilisateur doivent être définies et gérées : le modèle basé HTML, le modèle basé sur le serveur de configuration et le modèle combiné.

Ces modèles sont décrits ci-après. Pour obtenir des informations détaillées relatives à chaque modèle et aux avantages et inconvénients de chacun d'eux, reportez-vous à l'aide en ligne.

Présentation du modèle HTML

Si vous choisissez le modèle de type HTML, toutes les données de configuration de la session hôte sont contenues dans le fichier HTML et aucun autre élément n'est nécessaire pour définir les sessions hôte. Il n'est donc pas nécessaire d'utiliser le serveur de configuration pour indiquer les sessions. En d'autres termes, il n'est pas nécessaire d'ouvrir un port dans votre pare-feu. Si vous autorisez les utilisateurs à sauvegarder les modifications apportées aux données de configuration de la session hôte, celles-ci seront stockées dans le système de fichiers local sur lequel s'exécute le navigateur.

Nous vous recommandons de ne pas utiliser le port 8999 car vous n'avez pas à démarrer le serveur HOD en utilisant le modèle HTML. Dans ce cas, la ressource serveur est sauvegardée.

Cette option de définition des données de configuration dans les fichiers HTML est disponible uniquement dans les clients créés à l'aide de l'assistant de déploiement.

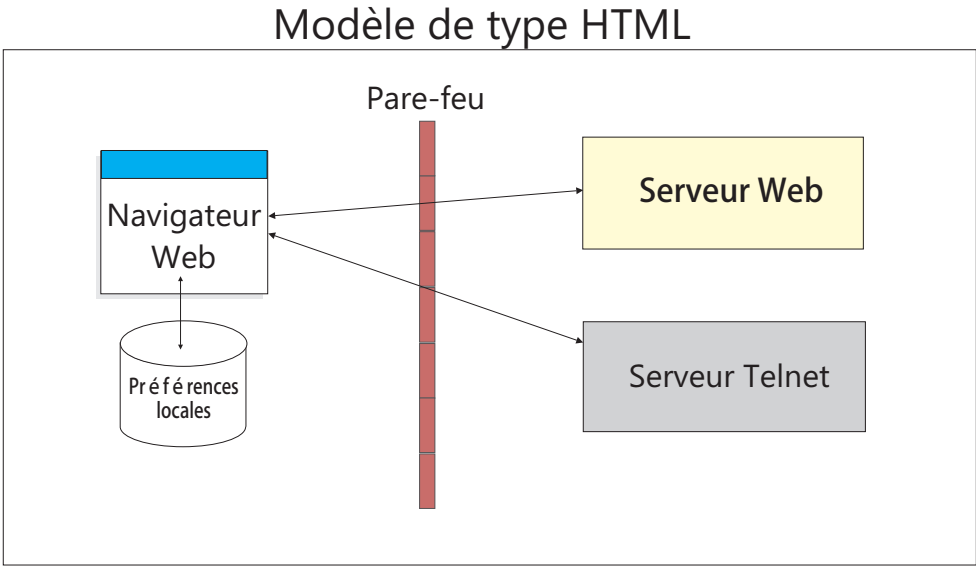

Figure 2. Modèle de type HTML

Présentation du modèle de type serveur de configuration

Dans le modèle de type serveur de configuration, les données de la session hôte sont conservées sur le serveur de configuration grâce au client d'administration et définies à l'aide d'une structure utilisateur et groupe. Par défaut, le serveur de configuration stocke ses données directement sur la machine serveur Host On-Demand, bien qu'il puisse être configuré pour utiliser la machine LDAP à la place. Les utilisateurs accèdent à leurs configurations à l'aide de fichiers HTML personnalisés créés dans l'assistant de déploiement ou de l'un des fichiers HTML fournis dans Host On-Demand. Les ID utilisateur sont définis sur le serveur de configuration et, dans la plupart des cas, l'utilisateur doit se connecter au serveur Host On-Demand pour visualiser ses sessions. Si les administrateurs autorisent les utilisateurs à sauvegarder leurs modifications, les préférences utilisateur sont stockées par ID utilisateur sur le serveur de configuration. Etant donné que la personnalisation est sauvegardée sur le serveur de configuration, ce modèle est probablement le mieux adapté si les utilisateurs doivent accéder à leurs sessions à partir de plusieurs machines.

Par défaut, le navigateur Web communique directement avec le serveur de configuration. Si vous communiquez via un pare-feu, vous devez ouvrir le port du serveur de configuration dans le pare-feu. Vous pouvez également utiliser le servlet de configuration pour éviter d'ouvrir son port sur le pare-feu. Le navigateur Web se connecte au servlet de configuration lors d'une connexion HTTP ou HTTPS ; le servlet de configuration interagit alors avec le serveur de configuration. Pour plus d'informations sur l'utilisation du servlet de configuration, reportez-vous à la section relative à la configuration du servlet de configuration.

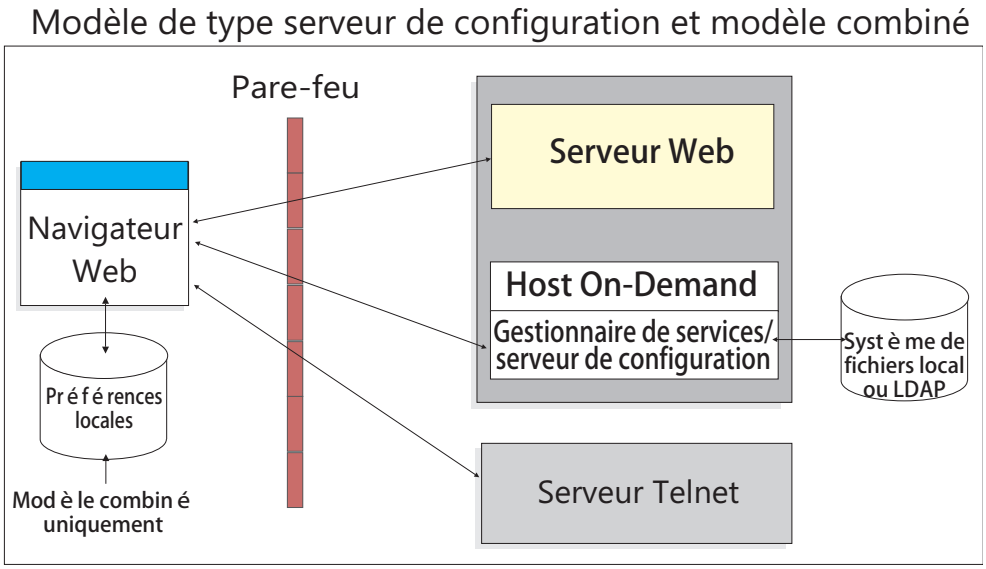

Figure 3. Modèle de type serveur de configuration et modèle combiné

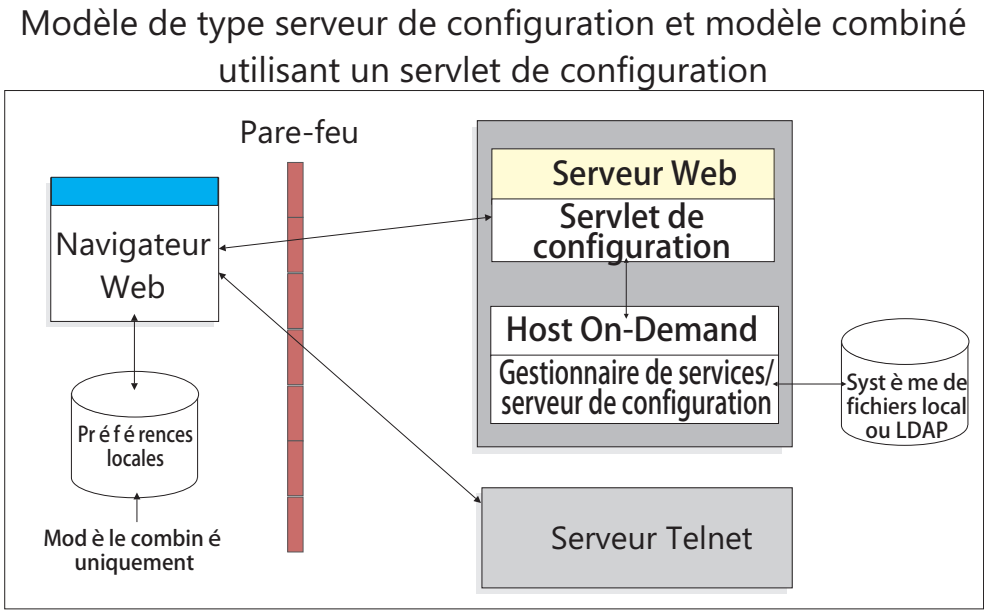

Figure 4. Modèle de type serveur de configuration et modèle combiné utilisant un servlet de configuration

Présentation du modèle combiné

Host On-Demand offre un modèle combiné, grâce auquel les données de la session hôte sont définies dans le serveur de configuration (à l'instar du modèle de type serveur de configuration) et les mises à jour de l'utilisateur sont sauvegardées sur sa machine (à l'instar du modèle de type HTML). En outre, à l'instar du modèle de type HTML, les utilisateurs du modèle combiné n'ont pas besoin de se connecter au serveur Host On-Demand pour afficher leurs sessions.

Remarques relatives au déploiement du client

De plus, pour ce qui est des remarques relatives au déploiement du client, vous devez choisir entre le client en cache, téléchargé ou Web Start (voir Chapitre 10, «Utilisation des clients d'émulation de Host On-Demand», à la page 75) et la version de Java que vous souhaitez utiliser (voir Chapitre 3, «Planification du support Java sur le client», à la page 15).

Chapitre 3. Planification du support Java sur le client

Le présent chapitre fournit des informations détaillées concernant l'exécution du client Host On-Demand dans un navigateur compatible Java.

- La section «Améliorations apportées au client en cache pour Java» décrit les fonctions du client en cache Host On-Demand Java.
- La section «Téléchargement d'un client équipé de Java», à la page 16 décrit les fonctions avancées du client Host On-Demand, disponibles uniquement avec un navigateur compatible Java.
- La section «Mac OS X avec Java», à la page 17 traite des aspects liés à l'utilisation de la plateforme Apple Mac OS X pour le client Host On-Demand Java.
- La section «Navigateurs et plug-in Java», à la page 18 traite des aspects liés à l'utilisation des navigateurs et des plug-in Java.

Améliorations apportées au client en cache pour Java

Avec la version Java du client en cache, vous pouvez désormais :

- Installer le client en cache Java à partir d'une unité de réseau local ou de DVD-ROM. Pour plus d'informations, reportez-vous à «Installation du client en cache à partir d'un réseau local ou d'un DVD», à la page 79.
- Partager le client en cache Java entre plusieurs utilisateurs sous Windows. Pour plus d'informations, reportez-vous à «Prise en charge du client en cache pour Windows», à la page 83.
- Supprimer le client en cache Java en une seule opération, sans avoir à effacer le cache du plug-in Java. Pour plus d'informations, reportez-vous à «Désinstallation du client en cache», à la page 81.
- Effectuer en arrière-plan une mise à niveau le client en cache Java.

Remarque : Les restrictions suivantes s'appliquent :

Un nombre limité de types de client en cache Java ne peuvent pas être mis à niveau en arrière-plan. Reportez-vous à la section «Limites du support» pour plus d'informations.

Ces améliorations sont prises en charge par la quasi totalité des clients en cache Host On-Demand Java. Le client Java Web Start prend également en charge ces améliorations.

Limites du support

Les types de clients en cache Java suivants ne prennent pas en charge les améliorations apportées à cette version du client en cache :

- Fenêtre Traitement de la collection de Impression de la collection d'écrans
- Prise en charge su protocole SSH (Secure Shell) pour les sessions écran VT et les sessions de transfert de fichiers sécurisées SFTP
- IME Auto/Conversion immédiate
- Améliorations apportées à l'impression écran
- Internet Protocol version 6 (IPv6)
- Fonctions d'accessibilité

- Prise en charge des clés en double
- Clavier en incrustation personnalisable
- Prise en charge de la molette
- Dans les langues bidirectionnelles, la prise en charge des CCSID (Code Character Set Identifiers, ID de jeu de caractères codés) pour OS/400 est désormais disponible pour l'affichage des caractères Unicode.

Téléchargement d'un client équipé de Java

Les sections suivantes détaillent les restrictions liées au téléchargement d'un client équipé de Java.

Impossible de télécharger un composant ne figurant pas dans la liste de préchargement

Avec un client Java téléchargé, l'utilisateur ne peut effectuer aucun téléchargement de composant client Host On-Demand qui ne figure pas dans la liste de préchargement initiale. Vous devez donc indiquer, dans la liste de préchargement, tous les composants susceptibles d'être demandés par les utilisateurs.

Cette restriction est due à un conflit entre la méthode utilisée par un client téléchargé lors du transfert de composants non compris dans la liste de préchargement et les restrictions de sécurité imposées par le plug-in Java

Certains composants ne sont pas inclus dans les fichiers HTML

Avec Java, les fichiers HTML du client téléchargé par défaut (HOD_*xx*.html, où *xx* est un suffixe désignant la langue) ne contient pas les composants suivants :

- Transfert de données
- Transfert de fichiers 5250
- Prise en charge de l'impression d'hôte 5250
- Importation/exportation
- SLP
- Sessions en thaï
- Convertisseur de page de codes FTP
- Sessions bidirectionnelles
- Sessions en hindi 5250
- sessions DBCS utilisant les paramètres de caractères définis par l'utilisateur
- ZipPrint dans les sessions DBCS

Ces composants moins fréquemment utilisés que les autres ont été retirés par IBM de la liste de préchargement des fichiers HTML du téléchargement Java par défaut, afin de raccourcir la durée du transfert. Toutefois, avec le client téléchargé Java, aucun composant non mentionné dans la liste de préchargement ne peut être téléchargé par la suite.

Si vous souhaitez faire figurer tout ou partie des composants dans la liste de préchargement, procédez de l'une des manières suivantes :

- Utilisez l'assistant de déploiement pour créer un fichier HTML Java de client téléchargé ou de client en cache contenant les composants dont vous avez besoin.

- Utilisez le fichier HTML par défaut pour le client en cache (HODCached_xx.html, où *xx* est un suffixe à deux lettres désignant la langue) au lieu du fichier HTML par défaut du client téléchargé.
- Utilisez la version de débogage du client téléchargé par défaut (HODDebug_xx.html, xx est un suffixe à deux lettres désignant la langue). Cette version de débogage comprend la totalité des composants. Toutefois, la version de débogage du client téléchargé par défaut est plus volumineuse que la version normale.

Mac OS X avec Java

Les clients de base de données et l'émulateur Host On-Demand Mac OS X prennent en charge Safari, Firefox et la version Mac d'Internet Explorer. Host On-Demand ne prend pas en charge les clients d'administration sur Mac OS X. Host On-Demand version 12.0 prend en charge Java version 1.6 ou supérieure.

La fonction de support de la clé en double requiert Java Plug-in 1.4.2 ou supérieure sur les clients Macintosh. Cependant, Host On-Demand version 12 prend en charge Java version 1.6 ou ultérieure.

Restrictions liées à la plateforme Mac OS X

Mac OS X ne prend pas en charge les améliorations apportées au client en cache Java décrites dans la rubrique «Améliorations apportées au client en cache pour Java», à la page 15. Pour plus d'informations, reportez-vous à «Prise en charge du client en cache sur Mac OS X (clients Java uniquement)», à la page 84.

Temps de démarrage légèrement plus long sur les clients Java

Sur les navigateurs compatibles Java, le démarrage du client Host On-Demand est légèrement plus lent (de 5 à 15 secondes supplémentaires, suivant le type de poste de travail). Ce délai est consécutif au chargement du plug-in Java.

De même, sur les navigateurs compatibles Java, une session hôte lancée dans le bureau du client Host On-Demand peut nécessiter un temps de démarrage légèrement plus long.

Restrictions liées à certains plug-in Java

Si vous utilisez un plug-in Oracle Java et que les caractères Hindi ne sont pas affichés correctement, assurez-vous que vous disposez du niveau le plus récent d'Oracle JRE.

Restrictions liées aux applets fournies par l'utilisateur et à Java

Lorsqu'un utilisateur exécute une applet d'origine externe (c'est-à-dire, une applet développée par une société extérieure ou une tierce partie) dans une session (telle qu'une session écran 3270) lancée à partir d'un client Host On-Demand Java, et que cette applet requiert des droits d'accès Java, vous devez prendre l'une des mesures suivantes pour répondre aux exigences de sécurité de Java :

- L'applet doit être archivée dans un fichier .JAR signé sous Java.
- Les droits d'utilisation doivent avoir été préalablement affectés au poste de travail à l'aide de l'outil Java fourni avec le plug-in Java.

Si vous omettez de répondre aux exigences de sécurité de Java, l'exécution de l'applet échoue implicitement.

Limitations liées aux utilisateurs soumis à des restrictions et à Java

Les utilisateurs dotés de droits d'accès restreints ne sont pas autorisés à installer le plug-in Java. Les utilisateurs dotés des droits d'administration doivent installer le plug-in Java.

Navigateurs et plug-in Java

Cette section traite des aspects liés à l'utilisation des navigateurs et des plug-in Java.

Navigateurs compatibles Java

Un navigateur compatible Java n'intègre aucune instance de machine virtuelle Java. Il permet d'afficher des fichiers HTML, mais nécessite l'installation séparée d'un plug-in Java pour permettre le lancement d'applets telles que le client Host On-Demand. Firefox et Microsoft Internet Explorer avec le plug-in Java installé sont des exemples de navigateurs compatibles Java.

Navigateurs et plug-in pris en charge par les clients Host On-Demand

Les utilisateurs dotés de postes de travail client exécutant Windows peuvent télécharger le plug-in IBM Java sur Fix Central, dans la rubrique du produit Host On-Demand, tant que la société peut bénéficier de HOD.

Etant donné que les fournisseurs de plug-ins Java tels que Oracle et IBM diffusent régulièrement de nouvelles versions de ces plug-ins, dont IBM assure la prise en charge par le biais d'extensions de Host On-Demand, IBM mettra à jour les Rapports de compatibilité du produit logiciel pour la prise en charge de nouvelles versions de JRE.

Microsoft Internet Explorer équipé du plug-in Java

Lorsqu'un plug-in Java est correctement installé et configuré sur un poste de travail client Windows, Microsoft Internet Explorer fonctionnera en tant que navigateur compatible Java, selon le mode utilisé par Host On-Demand pour lancer le client.

Firefox équipé du plug-in Java

Pour exécuter une applet Java sur Firefox, vous devez installer un plug-in Java.

Host On-Demand exige donc que vous configuriez le plug-in Java en tant que module d'exécution Java *par défaut* de Firefox.

Remarque : Les utilisateurs soumis à des restrictions (par exemple, les utilisateurs restreints partageant un client en cache sous Windows ou les utilisateurs restreints exploitant des postes de travail Linux ou Aix) ne peuvent pas installer le plug-in Java

Chapitre 4. Planification de la sécurité

Que vous utilisiez Host On-Demand uniquement au sein du réseau de votre société ou qu'il serve à fournir l'accès à des systèmes hôte par Internet, la sécurité est un facteur important à prendre en compte. Le présent chapitre présente un aperçu de la sécurité de Host On-Demand.

- Transport Layer Security (TLS) . Ces protocoles fournissent un chiffrement, une authentification de type certificat ainsi que des négociations relatives à la sécurité au niveau de la connexion Telnet ou FTP. Voir «TLS pour Host On-Demand», à la page 21 pour plus de détails.
- Agent de réacheminement. Prend en charge les connexions TLS entre les clients et le serveur Host On-Demand. Voir «Agent de réacheminement», à la page 26 pour plus de détails.
- Pare-feu. Vous pouvez configurer Host On-Demand afin qu'il soit protégé par un pare-feu. Voir «Utilisation de Host On-Demand avec un pare-feu», à la page 30 pour plus de détails.
- Sécurité liée à l'ID utilisateur. Inclut Web Express Logon, l'authentification native et la connexion au domaine Windows. Voir «Sécurité liée à l'ID utilisateur», à la page 35 pour plus de détails.
- Environnements FIPS (Information Processing Standards). Si votre environnement nécessite que les composants de sécurité utilisent les composants/modules certifiés FIPS, reportez-vous à «Environnements FIPS», à la page 36.

Transport Layer Security (TLS)

Fonctionnement de la sécurité TLS

TLS est basé sur le protocole SSL. TLS utilise le protocole initial d'établissement de liaison qui permet de procéder à l'authentification client-serveur et au chiffrement. Pour obtenir des informations détaillées sur le protocole TLS, reportez-vous à la rubrique *The TLS Protocol Version 1.0*.

Le protocole TLS utilise une technologie de chiffrement à clé publique et clé symétrique. Le chiffrement à clé publique utilise une paire de clés, l'une publique et l'autre privée. Les données chiffrées à l'aide d'une clé peuvent être déchiffrées uniquement avec l'autre. Par exemple, les données chiffrées avec la clé publique peuvent être déchiffrées uniquement à l'aide de la clé privée associée. La clé publique de chaque serveur est diffusée, tandis que la clé privée reste secrète. Pour transmettre un message sécurisé à un serveur, le client le chiffre en utilisant la clé publique du serveur. Lorsque ce dernier reçoit le message, il le déchiffre à l'aide de sa clé privée.

Le chiffrement avec une clé symétrique utilise la même clé pour coder et décoder les messages. Le client génère de façon aléatoire la clé symétrique devant être utilisée pour le chiffrement de toutes les données de session. Cette clé est alors codée à l'aide de la clé publique du serveur et transmise à ce dernier.

TLS fournit les trois services de base suivants :

Confidentialité des messages
Elle est obtenue par le chiffrement des messages à partir d'une

combinaison de clé publique et de clé symétrique. La totalité du trafic entre un client et un serveur est codée à l'aide d'une clé et d'un algorithme de chiffrement, négocié à l'ouverture de la session.

Intégrité des messages
Elle garantit que le trafic de la session est toujours acheminé de la même façon vers sa destination finale. TLS utilise une paire de clé publique-privée et des fonctions de hachage pour garantir l'intégrité des messages.

Processus d'authentification réciproque
Il s'agit d'une méthode d'identification réciproque obtenue par l'échange de certificats de clé publique. L'identité du client et celle du serveur sont chiffrées dans des certificats de clé publique qui contiennent les composants suivants :

- le nom réservé du destinataire ;
- le nom réservé de l'expéditeur ;
- la clé publique du destinataire ;
- la signature de l'expéditeur ;
- la période de validité ;
- le numéro de série.

Tableau 2. Conseil

Vous pouvez également utiliser le protocole HTTP sécurisé (HTTPS) pour vous assurer que les données de sécurité d'un client sont protégées lors du téléchargement à partir d'un serveur.

Certificats

La sécurité est contrôlée par des certificats numériques qui fonctionnent comme des cartes d'identification électroniques. Le but d'un certificat est de garantir à un programme ou à un utilisateur que la connexion proposée est sécurisée et, lorsqu'une fonction de chiffrement est utilisée, de fournir les clés nécessaires. Ils sont généralement émis par une autorité de certification (AC), institution agréée dont la fonction consiste à émettre des certificats Internet. Un certificat émis par une autorité de certification, également appelé certificat racine, contient la signature de l'AC, sa période de validité et d'autres informations.

Le chiffrement et l'authentification sont mis en oeuvre par l'utilisation d'une paire de clés publique-privée. La clé publique est insérée dans un certificat, appelé certificat site ou serveur. Ce dernier contient plusieurs types d'informations dont le nom de l'autorité de certification qui a émis le certificat, le nom et la clé publique du serveur ou du client, la signature de l'autorité de certification et enfin la date et le numéro de série du certificat. La clé privée est générée lorsque vous créez un certificat autosigné ou que vous faites une demande de certificat auprès d'une AC. Elle est utilisée pour le déchiffrement des messages provenant des clients.

Une session TLS s'établit de la façon suivante :

1. Le client et le serveur échangent des messages destinés à négocier les algorithmes de chiffrement et de hachage (pour l'intégrité des messages) à utiliser pendant la session.
2. Le client demande au serveur un certificat X.509 pour l'identifier. Le serveur peut également requérir un certificat du client. Ces certificats font l'objet des vérifications suivantes : format et validité des dates, présence de la signature d'une autorité de certification agréée (ou certificat autosigné).

3. Le client génère, de façon aléatoire, un ensemble de clés utilisées pour le chiffrement. Ces clés sont ensuite elles-mêmes chiffrées à l'aide de la clé publique du serveur et communiquées en toute sécurité au serveur.

TLS pour Host On-Demand

Il existe trois domaines dans lesquels vous avez la possibilité de configurer la sécurité pour Host On-Demand : la sécurité de niveau session, la sécurité du serveur Web et la sécurité de configuration.

Sécurité au niveau de la session

Host On-Demand version 12.0 fait appel au le protocole TLS pour assurer la sécurité des sessions d'émulation et FTP.

Le protocole TLS assure la confidentialité des communications sur le réseau TCP/IP. Ce protocole est conçu pour prévenir les écoutes, la contrefaçon ou la falsification des messages. Il offre également une structure permettant la conception de nouveaux algorithmes de chiffrement à incorporer aisément. Host On-Demand prend en charge les fonctions de chiffrement des sessions d'émulation, FTP et d'authentification serveur/client en fonction de la norme *TLS Protocol Version 1.0*.

Les éléments suivants sont pris en charge :

- Chiffrement des données RSA type 4 pour les connexions entre les clients Host On-Demand et les serveurs Telnet ou FTP qui prennent en charge le protocole TLS versions 1.0, 1.1 et 1.2.
- Certificats X.509.
- Algorithmes de chiffrement utilisant des clés d'une longueur maximale de 168 bits.
- Algorithmes d'authentification utilisant des clés d'une longueur maximale de 2048 bits.
- Authentification du serveur et des clients.
- Prise en charge du stockage et de l'utilisation de certificats client sur le système client.
- (Facultatif) Message invitant l'utilisateur à fournir un certificat client à la demande du serveur.
- Indicateurs de session sécurisée. Une icône de verrouillage s'affiche sur la barre d'état de la session pour signaler à l'utilisateur que la session est sécurisée. Le niveau de chiffrement, par exemple, 64, 128 ou 256, s'affiche également en regard de l'icône de verrouillage lorsque vous survolez l'icône avec la souris.

Avec Host On-Demand, vous pouvez utiliser un certificat émis par une autorité de certification, mais vous pouvez également créer votre propre certificat autosigné, comme décrit dans la rubrique Using a self-signed certificate de l'aide en ligne.

Un utilitaire graphique de gestion des certificats (pour les plateformes Windows et AIX) offre les fonctions suivantes :

- Création de demandes de certificat,
- Réception et stockage des certificats,
- Création de certificats autosignés.

IKEYCMD est un outil, complémentaire du gestionnaire de certificats, qui peut être utilisé pour gérer les clés, les certificats et les demandes de certificat. Il fonctionne de la même manière que le gestionnaire de certificats et est censé être lancé à partir

de la ligne de commande sans interface graphique. Pour plus d'informations, reportez-vous à Annexe B, «Utilisation de l'interface de ligne de commande IKEYCMD», à la page 147.

Pour prendre en charge les services TLS, Host On-Demand utilise les six bases de données suivantes :

HODServerKeyDb.kdb
La base de données HODServerKeyDb.kdb est créée lors de la première configuration de la sécurisation TLS pour l'Agent de réacheminement Host On-Demand. Elle contient le certificat et la clé privée du serveur, ainsi que la liste des certificats émis par les autorités de certification (ou le signataire). Ces autorités de certification sont considérées comme *connues* et *dignes de confiance* par le serveur Host On-Demand. Dans cette base de données, vous pouvez ajouter des certificats issus d'autres AC (qualifiées d'inconnues) et des certificats que vous créez et que vous signez (qualifiés d'auto-signés). Pour plus d'informations, voir «Agent de réacheminement», à la page 26.

HODServerKeyStore.jks
L'Agent de réacheminement peut être configuré de manière à utiliser JSSE (Java Secure Socket Extenstion) au lieu de GSKit. Configuré avec JSSE, l'Agent de réacheminement lit la clé privée et les certificats dans HODServerKeyStore.jks. Pour plus d'informations, reportez-vous à la rubrique consacrée à l'Agent de réacheminement.

CustomizedCAs.p12
Le fichier CustomizedCAs.p12 est un fichier de classe PKCS#12 qui contient les certificats racine émis par des autorités de certification inconnues et les certificats autosignés qui ne figurent pas dans la liste WellKnownTrusted. Le fichier CustomizedCAs.p12 est utilisé avec SSLite, où CustomizedCAs.jks est utilisé avec le support de JSSE. Si vous utilisez un certificat autosigné ou un certificat émis par une autorité de certification inconnue, vous devez créer ou mettre à jour le fichier CustomizedCAs.p12. Host On-Demand n'installe pas de fichier CustomizedCAs.p12 par défaut. Le fichier CustomizedCAs.p12 a pour fonction de rendre les certificats accessibles au client et est utilisé pendant le processus du protocole d'établissement de liaison TLS entre le client et l'hôte.

Le fichier CustomizedCAs.p12 est la version préférée du fichier CustomizedCAs.class, que vous avez éventuellement créé avec une précédente édition de Host On-Demand. Le fichier CustomizedCAs.class, qui prend en charge les clients de Host On-Demand Version 7 et des versions antérieures, se situe dans le répertoire de diffusion par défaut. Si vous exécutez Windows ou AIX, lorsque vous effectuez une mise à niveau vers la version 12, le programme d'installation de Host On-Demand détecte automatiquement le fichier CustomizedCAs.class, crée le nouveau fichier CustomizedCAs.p12 et le place dans le répertoire de diffusion. Ces deux fichiers demeurent dans le répertoire de diffusion et restent accessibles aux clients d'autres versions. Si vous avez créé un répertoire de diffusion distinct du répertoire par défaut, le programme d'installation de Host On-Demand ne détectera pas le fichier CustomizedCAs.class et vous devrez effectuer la migration manuellement via une ligne de commande.

Si vous créez le fichier CustomizedCAs.p12 pour la première fois à l'aide de l'utilitaire de gestion des certificats Host On-Demand (IKEYMAN), la version antérieure du fichier CustomizedCAs.class est également requise dans le répertoire de diffusion afin que les anciens clients puissent toujours

communiquer avec le nouveau serveur. Si, par ailleurs, vous mettez à jour ultérieurement le fichier CustomizedCAs.p12, vous devez veiller à ce que les modifications apportées soient prises en compte dans le fichier CustomizedCAs.class. Si, dans le cas des plateformes Windows, ces fichiers se trouvent dans le répertoire de diffusion par défaut c:\Program Files\IBM\HostOnDemand\HOD, chaque fois que vous ouvrez IKEYMAN pour modifier le fichier CustomizedCAs.p12, puis refermez IKEYMAN, le fichier CustomizedCAs.class est automatiquement mis à jour, parallèlement au fichier CustomizedCAs.p12. Si ces fichiers sont situés hors du répertoire de diffusion par défaut, vous devez exécuter manuellement l'outil de migration-rétromigration à partir du répertoire de diffusion, via la commande indiquée ci-dessous. La commande est présentée sur trois lignes, mais vous devez la saisir sur une seule ligne.

```
..\hod_jre\jre\bin\java -cp ..\lib\sm.zip;
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT
CustomizedCAs.p12 hod CustomizedCAs.class
```

Sous AIX, pour que le fichier CustomizedCAs.class tienne compte des modifications effectuées dans le fichier CustomizedCAs.p12, vous devez exécuter l'outil de migration-rétromigration manuellement dans le répertoire de diffusion à l'aide de la commande suivante. La commande est présentée sur trois lignes, mais vous devez la saisir sur une seule ligne.

```
../hod_jre/jre/bin/java -cp ../lib/sm.zip
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT
CustomizedCAs.p12 hod CustomizedCAs.class
```

CustomizedCAs.class

CustomizedCAs.class est un fichier de classe Java qui contient les certificats émis par des autorités de certification inconnues et les certificats autosignés qui ne figurent pas dans la liste WellKnownTrusted. Si vous utilisez un certificat autosigné ou un certificat émis par une autorité de certification inconnue, vous devez mettre à jour le fichier CustomizedCAs.class. Toutefois, vous ne pouvez plus, désormais, créer ni mettre à jour le fichier CustomizedCAs.class via l'utilitaire de gestion de certificats sur les plateformes Windows et AIX. Dans la version 9 et les versions suivantes de Host On-Demand, vous ne pouvez créer qu'une nouvelle version de ce fichier CustomizedCAs.p12. Tous les clients continuent néanmoins de prendre en charge l'ancien format. Pour plus d'informations, reportez-vous à la description du fichier CustomizedCAs.p12 ci-dessus.

WellKnownTrustedCAs.class, WellKnownTrustedCAs.p12 et WellKnownTrustedCAs.jks

Les fichiers WellKnownTrustedCAs.class, WellKnownTrustedCAs.p12 et WellKnownTrustedCAs.jks sont fournis par Host On-Demand. Ils contiennent les certificats publics de toutes les AC agréées par Host On-Demand. En aucun cas, vous ne devez modifier ces fichiers.

WellKnownTrustedCAs.class/WellKnownTrustedCAs.p12 et WellKnownTrustedCAs.jks, CustomizedCAs.p12 et/ou CustomizedCAs.class et CustomizedCAs.jks doivent être présents dans le répertoire de diffusion Host On-Demand. Le client Host On-Demand utilise ces fichiers afin de reconnaître le certificat du serveur lors de l'établissement de liaison TLS.

CustomizedCAs.jks

Le fichier CustomizedCAs.jks est différent du fichier CustomizedCAs.p12, mais tous deux remplissent la même fonction. Vous pouvez créer un fichier CustomizedCAs.jks soit en convertissant le fichier CustomizedCAs.p12 existant au format JKS, soit en créant un nouveau fichier dans ce format.

Vous pouvez utiliser l'utilitaire de gestion de certificats installé avec Host On-Demand ou l'outil de ligne de commande keytool.exe, qui est un outil de gestion des certificats et des clés Java disponible dans l'environnement d'exécution Java à cet effet.

Autorisation TLS de base pour les clients Host On-Demand

Lorsque vous sélectionnez le protocole TLS pour le client Host On-Demand, une session TLS de base est établie. Au cours du processus de négociation TLS, le serveur présente son certificat au client. Avec l'autorisation TLS de base, le certificat peut être signé par une autorité à laquelle le client fait confiance. Le client vérifie le fichier WellKnownTrustedCAs.class/WellKnownTrustedCAs.p12 en premier, puis le fichier CustomizedCAs.p12 ou CustomizedCAs.class. Si Host On-Demand est configuré de manière à utiliser JSSE pour l'autorisation TLS, les fichiers WellKnownTrustedCAs.jks et CusomizedCAs.jks sont utilisés. Il rejette la session s'il ne trouve pas le signataire dans ces fichiers. Mais s'il le trouve, la session est établie. Il s'agit de l'authentification du serveur de base. Host On-Demand vous permet de configurer une forme d'authentification du serveur plus évoluée dans cette configuration client. Pour plus d'informations, reportez-vous à la section ci-dessous.

Authentification du serveur

Le chiffrement des données entre le client et le serveur ne garantit pas que le client communique avec le bon serveur. Pour éviter tout risque, vous pouvez activer l'authentification du serveur afin que le client, après s'être assuré que le certificat du serveur est agréé (ou digne de confiance), vérifie que le nom Internet mentionné dans le certificat correspond au nom Internet du serveur. S'ils correspondent, la négociation TLS se poursuit. Sinon, la connexion est immédiatement interrompue. Pour plus d'informations, reportez-vous à server authentication de l'aide en ligne.

Authentification du client

L'authentification du client est similaire à l'authentification du serveur, à ceci près que le serveur Telnet demande un certificat au client pour vérifier qu'il répond bien au profil présenté. Ce processus n'est pas pris en charge sur tous les serveurs (notamment par l'Agent de réacheminement Host On-Demand). Pour configurer l'authentification du client, vous devez :

- obtenir des certificats pour les clients
- envoyer les certificats aux clients
- configurer les clients en vue d'utiliser l'authentification client

Pour plus d'informations, reportez-vous à configuring clients to use client authentication de l'aide en ligne.

Connexion express

Il existe deux types de connexion Express :

- Web Express Logon : permet aux utilisateurs de se connecter aux systèmes et applications hôte sans avoir à fournir d'ID utilisateur ni de mot de passe. Cette fonction, qui opère en complémentarité de votre application de sécurité du réseau, consigne les accréditifs réseau des utilisateurs et les met en correspondance avec ceux de l'hôte, en éliminant le recours à plusieurs ouvertures de session. Suivant l'hôte concerné, le processus d'ouverture automatique de session peut reposer sur une macro ou sur une connexion. Pour plus d'informations, reportez-vous à `Web Express Logon Reference`.
- Connexion express avec certificat : basée sur une macro, elle permet aux utilisateurs de se connecter aux systèmes et applications hôte sans avoir à fournir d'ID utilisateur ni de mot de passe. Son principe est le même

que celui de Web Express Logon, mais vous devez configurer la session pour TLS ainsi que l'authentification du client, et vous assurer que le serveur de communications prend en charge et est configuré pour ce type de connexion. Pour plus d'informations, reportez-vous à Express logon de l'aide en ligne.

Tableau 3. Conseil

En démarrant avec Host On-Demand V9, Web Express Logon offre un type d'automatisation de connexion qui utilise les certificats du client. Ce modèle est nommé Web Express Logon basé sur les certificats et est considérablement différent de Certificate Express Logon. Avec Certificate Express Logon, les certificats client permettent d'authentifier les utilisateurs auprès d'un serveur TN3270 de connexion express qui est configuré pour automatiser le processus de connexion. En revanche, avec Web Express Logon basé sur les certificats, les certificats client permettent d'authentifier les utilisateurs auprès d'un serveur Web ou une application de sécurité réseau, et le processus de connexion est automatisé par un module d'extension et une macro. Pour plus d'informations, reportez-vous à `Web Express Logon Reference`.

Sécurité Telnet basée sur TLS

Cette option permet d'effectuer les négociations relatives à la sécurité entre le client et le serveur Telnet au niveau de la connexion Telnet établie. Vous pouvez configurer la sécurité négociée par Telnet pour les sessions écran et imprimante 3270 Host On-Demand.

Le serveur Telnet doit prendre en charge la sécurité Telnet basée sur TLS (tle que décrit dans le rapport sur Internet rédigé par le groupe de travail IETF *TLS-based Telnet Security*) afin que les clients Host On-Demand puissent utiliser cette fonction. Le serveur Communications Server pour les systèmes z/OS prend en charge via Telnet basée sur TLS.

Pour plus d'informations sur la sécurité négociée par Telnet, reportez-vous à Telnet-negotiated security overview de l'aide en ligne. Pour plus d'informations sur la configuration de la sécurité TLS sur le serveur Telnet, reportez-vous à la documentation qui accompagne ce dernier. Pour obtenir des informations sur la configuration des clients pour la connexion à un serveur Telnet sécurisé, reportez-vous à la rubrique Security de l'aide en ligne.

Sécurité TLS pour FTP

Host On-Demand offre un transfert de fichiers sécurisé de type TLS pour les sessions FTP. La session FTP ne prend pas en charge les négociations TLS implicites/inconditionnelles sur le port 990/989. Par conséquent, le port 990 ne doit pas être utilisé pour les sessions FTP sécurisées. Elle ne prend en charge que les négociations TLS explicites/conditionnelles (commande AUTH) sur n'importe quel autre port.

Les propriétés de sécurité de la session FTP sont indépendantes des propriétés de sécurité de la session d'émulation. Pour une session FTP intégrée, vous devez configurer les informations de sécurité FTP à l'aide du nouvel onglet Sécurité des propriétés de session FTP. Si vous configurez une session d'émulation à sécuriser et que le type de transfert de fichiers défini est FTP, la session FTP n'est pas sécurisée automatiquement. Dans ce cas, le message suivant apparaît lorsque vous cliquez sur le bouton OK : "If a secure file transfer session is desired, configure the security information in File Transfer Defaults." (Si vous souhaitez utiliser une session de transfert, configurez les informations de sécurité des valeurs par défaut du transfert de fichier)

La fonction FTP sécurisée basée TLS est prise en charge par z/OS V1R2 ou version ultérieure.

Exemples d'utilisation de la sécurité de niveau session

Reportez-vous à la liste suivante de cas pratiques dans lesquels la sécurité de niveau session peut être utilisée :

- Vous souhaitez que vos clients puissent commander vos produits sur Internet. Dans ce cas, vous souhaitez chiffrer les informations qu'ils vous fournissent, par exemple leur numéro de carte de crédit, afin qu'elles ne puissent pas être divulguées. De même, vous voulez que les informations que vous fournissez à vos clients soient protégées.
- Vous souhaitez donner à vos fournisseurs et partenaires d'échange un accès à vos ordinateurs hôtes. Vous souhaitez que personne d'autre ne puisse accéder à ces données.
- Vous souhaitez que vos employés puissent accéder aux données stockées sur vos systèmes hôte à partir de sites distants ou lorsqu'ils sont en déplacement.
- Vous souhaitez donner à des médecins l'accès aux enregistrements relatifs à des patients situés en n'importe quel lieu, en vous assurant qu'aucune personne non autorisée ne puisse accéder à ces enregistrements.

Sécurité du serveur Web

Vous pouvez configurer votre serveur Web pour qu'il utilise TLS afin que le flot de données entre le serveur Web et le navigateur soit chiffré. Pour plus d'informations sur la configuration du serveur Web pour TLS, reportez-vous à la documentation relative à ce dernier. Toutefois, une fois que le client est chargé dans un navigateur, il communique directement avec l'hôte. Vous pouvez configurer Host On-Demand pour fournir la sécurité TLS à vos sessions hôte. Pour plus d'informations, reportez-vous à la rubrique Configuring TLS dans l'aide en ligne.

Sécurité de la configuration

Si vous utilisez le modèle HTML, les renseignements de configuration de la session sont chiffrés avec HTTPS. Pour tous les autres modèles, vous devez configurer Host On-Demand afin qu'il utilise le servlet de configuration via HTTPS (après avoir configuré le serveur d'applications Web) pour chiffrer la configuration de la session au lieu de communiquer directement avec le serveur de configuration. Pour de plus amples informations sur l'installation du servlet de configuration, reportez-vous à «Installation du servlet de configuration», à la page 61 du présent manuel. Pour plus d'informations sur la configuration des clients concernant l'utilisation du servlet de configuration, reportez-vous à configuring the configuration servlet de l'aide en ligne.

Agent de réacheminement

L'Agent de réacheminement est un service qui s'exécute sur le serveur Host On-Demand et qui permet à un client Host On-Demand de communiquer avec un serveur Telnet en se connectant à un port de réacheminement sur le serveur Host On-Demand.

Normalement, un client Host On-Demand :

- Se connecte directement au serveur Host On-Demand pour télécharger le code client et accéder aux fichiers HTML publics.
- Il se connecte également directement à un serveur Telnet qui s'exécute sur ou est connecté à un hôte 3270, 5250, VT ou CICS.

En revanche, lorsque l'Agent de réacheminement est utilisé, ce dernier agit en tant qu'intermédiaire entre le client et le serveur Telnet. Au lieu de se connecter directement au serveur Telnet, le client se connecte à un port de réacheminement sur le serveur Host On-Demand. L'Agent de réacheminement envoie alors les données reçues du client au serveur Telnet. Lorsque le serveur Telnet répond, l'Agent de réacheminement envoie les données reçues du serveur Telnet au client. Ce processus se répète pendant toute la durée de la session.

Pourquoi utiliser l'Agent de réacheminement ?

Si votre serveur Telnet ne prend pas en charge le protocole TLS et si vous exécutez le serveur Host On-Demand sur l'un des systèmes d'exploitation sur lequel l'Agent de réacheminement prend en charge les sessions sécurisées (voir «Systèmes d'exploitation pris en charge par l'Agent de réacheminement», à la page 29), vous pouvez configurer l'Agent de réacheminement Host On-Demand pour fournir la prise en charge TLS.

Tableau 4. Conseil

De nombreux serveurs Telnet prennent en charge TLS (par exemple, IBM Communications Servers sur zSeries, IBM System i, AIX ou NT). Si tel est le cas de votre serveur Telnet, il est vivement conseillé de l'utiliser. Si votre serveur Telnet ne prend pas en charge TLS, l'Agent de réacheminement du serveur de communications pour AIX offre une alternative plus évolutive à l'Agent de réacheminement Host On-Demand.

Cet agent fonctionne comme un serveur Proxy Telnet transparent qui procède à une réaffectation des ports pour connecter le serveur Host On-Demand à d'autres serveurs Telnet. Chaque serveur défini peut configurer un ensemble de numéros de ports locaux. Au lieu d'établir une connexion directe avec le serveur Telnet cible, le client l'établit avec le serveur Host On-Demand via son numéro de port. L'Agent de réacheminement mappe le numéro de port local sur le numéro de port hôte du système cible et établit la connexion.

Tableau 5. Recommandation

La solution recommandée pour un Proxy Telnet consiste à utiliser un équilibreur de charge, qui est une fonction de WebSphere Application Server's Edge Components, ou un produit similaire qui offre une fonction de conversion d'adresse comme solution globale de pare-feu, à la place de l'Agent de réacheminement de Host On-Demand.

Fonctionnement de l'Agent de réacheminement

La figure 5, à la page 28 montre comment l'Agent de réacheminement envoie les données client au serveur Telnet et envoie au client les données de réponse du serveur Telnet.

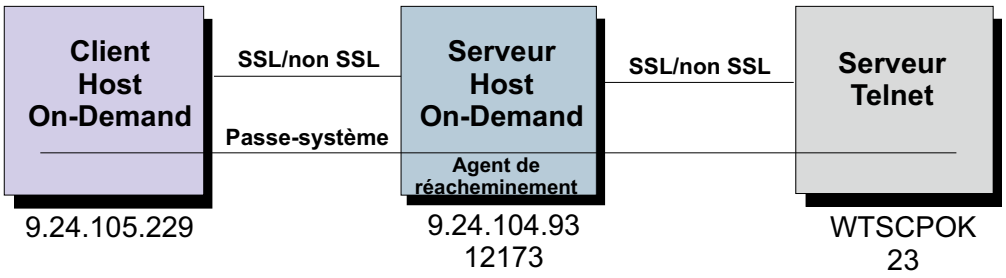

Figure 5. Fonctionnement de l'Agent de réacheminement

L'Agent de réacheminement peut être configuré de l'une des quatre façons suivantes :

- Passe-système
  - L'Agent de réacheminement communique avec le serveur Telnet et le client sans changer le contenu des données.
- Côté client
  - Le client et l'Agent de réacheminement communiquent dans une session sécurisée à l'aide de TLS (le contenu est chiffré/déchiffré).
  - L'Agent de réacheminement et le serveur Telnet communiquent dans une session non sécurisée.
- Côté hôte
  - Le client et l'Agent de réacheminement communiquent dans une session non sécurisée.
  - L'Agent de réacheminement et le serveur Telnet communiquent dans une session sécurisée à l'aide de TLS (le contenu est chiffré/déchiffré).
- Serveur et local
  - Le client et l'Agent de réacheminement communiquent dans une session sécurisée à l'aide de TLS (le contenu est chiffré/déchiffré).
  - L'Agent de réacheminement et le serveur Telnet communiquent dans une session sécurisée à l'aide de TLS (le contenu est chiffré/déchiffré).

Avant d'utiliser les modes côté client, côté serveur ou Serveur et local, vous devez créer HODServerKeyDb.kdb ou HODServerKeyStore.jks (si configuré pour utiliser JSSE) pour l'Agent de réacheminement.

Vous pouvez utiliser le mode Passe-système lorsque le chiffrement par l'Agent de réacheminement s'impose, soit parce que le flot de données ne doit pas être chiffré ou soit parce que le flot de données est déjà chiffré entre le client et le serveur Telnet. Vous devez utiliser le mode Passe-système si le client Host On-Demand se connecte via l'Agent de réacheminement à un hôte qui requiert une authentification de client ou à Express Logon.

Pour plus d'informations, reportez-vous à Adding a host to the Redirector dans l'aide en ligne.

Capacité de chargement de l'Agent de réacheminement

Pour connaître les recommandations relatives à la capacité de charge de l'Agent de réacheminement, consultez le fichier Readme.

Systèmes d'exploitation pris en charge par l'Agent de réacheminement

L'Agent de réacheminement prend en charge :

- Tous les systèmes d'exploitation qui sont pris en charge par le serveur Host On-Demand et qui prennent également en charge Internet Protocol Version 4 (IPv4).
- Certains systèmes d'exploitation qui sont pris en charge par le serveur Host On-Demand et qui prennent également en charge Internet Protocol Version 6 (IPv6).

Tous les modes de réacheminement ne sont pas pris en charge sur chaque système d'exploitation. Les deux prochaines sous-sections décrivent le support de réacheminement de façon plus détaillée. Pour plus d'informations, sur IPv4 et IPv6, reportez-vous à «Prise en charge du protocole Internet version 6», à la page 6.

Systèmes d'exploitation qui prennent en charge IPv4

Pour les systèmes d'exploitation qui prennent en charge IPv4, l'Agent de réacheminement prend en charge ce qui suit :

- Le mode Passe-système sur tous les systèmes d'exploitation pris en charge par le serveur Host On-Demand.
- D'autres modes (côté client, côté hôte, serveur et local) sur certains systèmes d'exploitation pris en charge par le serveur Host On-Demand.

Remarque : z/OS et iSeries ne prennent pas en charge ces modes.
Le tableau 6 et le tableau 7 présentent ces informations :

Tableau 6. Systèmes d'exploitation 32 bits et modes de réacheminement pour lesquels l'Agent de réacheminement prend en charge IPv4 à l'aide de GSKit

Système d'exploitation :	Passe-système :	Côté client :	Côté hôte :	Serveur et local :
Windows	Oui	Oui	Oui	Oui
AIX	Oui	Oui	Oui	Oui
Linux	Oui	Oui	Oui	Oui
Tous les autres systèmes d'exploitation	Oui	Non	Non	Non

Tableau 7. Systèmes d'exploitation 64 bits et modes de réacheminement pour lesquels l'Agent de réacheminement prend en charge IPv4 à l'aide de JSEE

Systèmes d'exploitation	Passe-système :	Côté client :	Côté hôte :	Serveur et local :
Windows	Oui	Oui	Oui	Oui
AIX	Oui	Oui	Oui	Oui
Linux	Oui	Oui	Oui	Oui
Tous les autres systèmes d'exploitation	Oui	Non	Non	Non

Support de l'Agent de réacheminement pour IPv6

Le tableau 8, à la page 30 et le tableau 9, à la page 30 indiquent les systèmes d'exploitation et les modes de réacheminement pour lesquels l'Agent de réacheminement prend en charge Internet Protocol Version 6 (IPv6) :

Tableau 8. Systèmes d'exploitation 32 bits et modes de réacheminement pour lesquels l'Agent de réacheminement prend en charge IPv6 à l'aide de GSKit

Système d'exploitation	Passe-système :	Côté client :	Côté hôte :	Serveur et local :
Windows	Oui	Oui	Oui	Oui
Linux	Oui	Oui	Oui	Oui
AIX	Oui	Oui	Oui	Oui

Tableau 9. Systèmes d'exploitation 64 bits et modes de réacheminement pour lesquels l'Agent de réacheminement prend en charge IPv6 à l'aide de JSEE

Système d'exploitation :	Passe-système :	Côté client :	Côté hôte :	Serveur et local :
Windows	Oui	Oui	Oui	Oui
Linux	Oui	Oui	Oui	Oui
AIX	Oui	Oui	Oui	Oui

Utilisation de Host On-Demand avec un pare-feu

Si vous configurez Host On-Demand pour l'utiliser via un pare-feu, il est souhaitable que l'administrateur du pare-feu n'ouvre que les ports nécessaires au fonctionnement des clients. Les ports Telnet permettent le trafic des sessions chiffrées TLS.

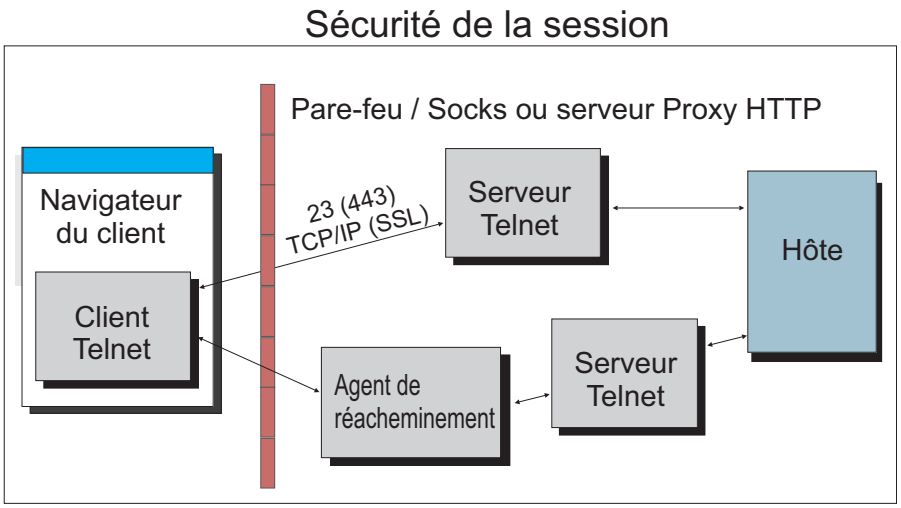

Figure 6. Sécurité de niveau session via un pare-feu ou un serveur Proxy

Si vous utilisez le modèle basé sur le serveur de configuration ou le modèle combiné, le servlet de configuration Host On-Demand permet aux clients Host On-Demand de communiquer avec le serveur de configuration via HTTP ou HTTPS.

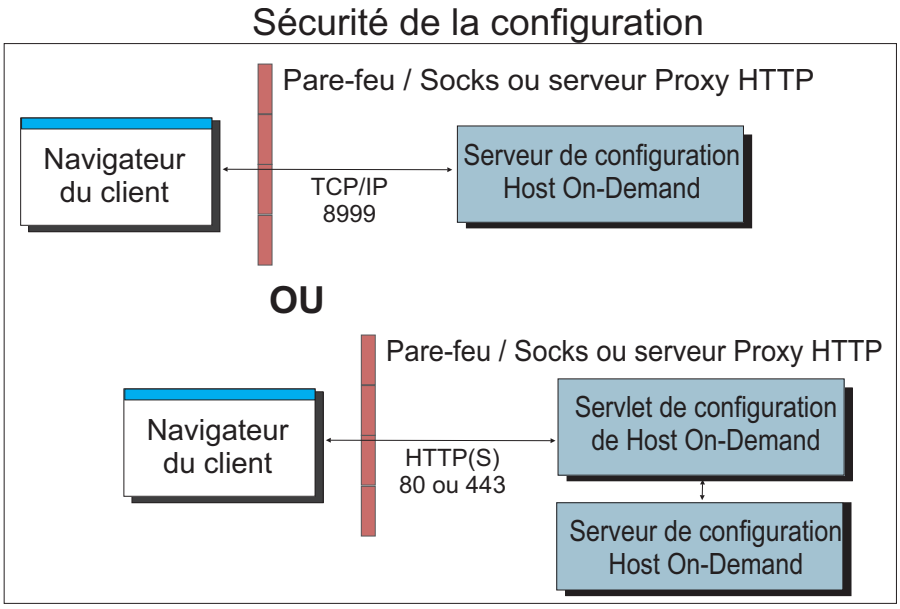

Figure 7. Sécurité de configuration avec ou sans le servlet de configuration par l'intermédiaire du pare-feu ou du serveur Proxy

Pour les clients Host On-Demand qui se connectent à un système hôte par l'intermédiaire de ports ouverts dans le pare-feu, reportez-vous à «Configuration des ports du pare-feu» pour plus d'informations. Pour les clients Host On-Demand qui se connectent à un système hôte par l'intermédiaire d'un serveur Socks ou Proxy HTTP, reportez-vous à «Connexion à un système hôte via un serveur Proxy», à la page 33 pour plus d'informations.

Configuration des ports du pare-feu

Si vous utilisez le modèle basé sur le serveur de configuration ou le modèle combiné, les clients Host On-Demand vont devoir communiquer avec le serveur de configuration. Pour que cette communication s'établisse via un pare-feu, vous devez ouvrir le port du gestionnaire de services de Host On-Demand ou utiliser le servlet de configuration Host On-Demand. Par défaut, le gestionnaire de services est à l'écoute sur le port 8999. Vous pouvez affecter le numéro de port disponible que vous souhaitez à cette valeur par défaut. Pour plus de détails, reportez-vous à Changing the Service Manager port de l'aide en ligne. Le servlet de configuration de Host On-Demand permet aux clients Host On-Demand de communiquer avec le serveur de configuration via HTTP ou HTTPS. Par conséquent, il n'est pas utile d'ouvrir le port du gestionnaire de services dans le pare-feu (voir figure 4, à la page 13). Voir «Installation du servlet de configuration», à la page 61 du présent manuel et à la rubrique Configuring the configuration servlet de l'aide en ligne pour plus de détails sur l'utilisation du servlet de configuration.

Si vous utilisez le modèle de type HTML, aucune condition requise ne limite l'accès des clients Host On-Demand au serveur de configuration, et il n'est pas utile d'ouvrir le port du gestionnaire de services dans le pare-feu. Les clients tenteront toujours de contacter le serveur de configuration pour le comptage des licences, mais s'arrêteront si le port du gestionnaire de services n'est pas ouvert.

Outre ce port du gestionnaire de services, assurez-vous que l'administrateur du pare-feu ouvre tous les ports utilisés par les fonctions nécessaires aux clients. Par exemple, si une session TLS est établie avec l'Agent de réacheminement sur le port

5000, le port 5000 doit être ouvert pour le trafic Telnet. Le tableau suivant répertorie les ports que Host On-Demand peut utiliser.

Tableau 10. Fonctions Host On-Demand et ports qu'elle utilisent

Fonction Host On-Demand	**Ports utilisés**
Emulation écran (3270 et VT) et émulation d'imprimante 3270	23 (Telnet), 80 (HTTP) ou 443 (TLS) et 8999 (serveur de configuration)[3]
Emulation écran et d'impression 5250	23 (Telnet) ou 992 [1] (TLS) ou 80 (HTTP) ou 443 (TLS) et 8999 (serveur de configuration) [3]
Transfert de fichiers 3270	23 (Telnet), 80 (HTTP) ou 443 (TLS) et 8999 (serveur de configuration)[3]
Transfert de fichiers 5250 - fichier de sauvegarde	80 (HTTP), 8999 (config server)[3], 21 (FTP)[4], >1024 (FTP)[4], 446 (drda)[4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], 8475 (as-rmtcmd)[1 4] et 8476 (as-signon)[1 4]
Transfert de fichiers 5250 - base de données	80 (HTTP), 8999 (serveur de configuration)[3], 446 (drda)[4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], 8475 (as-rmtcmd)[1 4] et 8476 (as-signon)[1 4]
Transfert de fichiers 5250 - fichier STREAM	80 (HTTP), 8999 (serveur de configuration)[1 2 4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4] et 8476 (as-signon)[1 4]
FTP	21 (FTP), 80 (HTTP), 8999 (config server)[1 2 4] et >1024 (FTP)[5]
CICS	2006
Database On-Demand	80 (HTTP), 8999 (serveur de configuration)[3], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8471 (as-database)[1 4] et 8476 (as-signon)[1 4]
Clients Host On-Demand	23 (Telnet), 80 (HTTP) et 8999 (serveur de configuration)[3]
Clients d'administration	80 (HTTP) et 8999 (serveur de configuration)[3]
Protocole Secure Shell (SSH)	22

Tableau 11. Remarques

Remarques

:

1 Vous pouvez utiliser la commande `WRKSRVTBLE` pour changer les numéros de port. Les numéros présentés dans ce tableau sont les valeurs par défaut.

2 Le port pour as-central est utilisé uniquement lorsqu'une table de conversion de page de codes doit être créée dynamiquement (EBCDIC de/vers Unicode). Cela dépend de la machine virtuelle Java et de l'environnement local du client.

3 Vous pouvez changer le port du serveur de configuration. Par défaut, il s'agit du port 8999.

4 Ces ports n'ont pas besoin d'être ouverts sur le pare-feu lorsque vous utilisez la prise en charge du serveur proxy d'IBM System i. Vous devez alors ouvrir le port par défaut du serveur proxy, 3470. Vous pouvez changer ce port.

Tableau 11. Remarques (suite)

5 En mode passif (PASV), le client FTP initie des connexions au serveur. De ce fait, il corrige les incidents liés au filtrage, par les pare-feu, des connexions au point d'accès entrant du serveur vers le client. Lorsque vous ouvrez une connexion FTP, le client ouvre localement deux ports non privilégiés aléatoires (N>1024 et N+1). Le premier port permet de contacter le serveur sur le port 21, mais au lieu d'émettre une commande PORT et permettre au serveur de se reconnecter à son point d'accès, le client émet une commande PASV. En conséquence, le serveur ouvre alors un port non privilégié aléatoire (P>1024) et renvoie la commande PORT P au client. Le client initie alors la connexion à partir du port N+1 vers le port P sur le serveur pour transférer les données.

Du point de vue du pare-feu côté serveur, vous devez ouvrir les ports de communication suivants pour prendre en charge la solution FTP en mode passif :

- Le port 21 du serveur FTP de n'importe quel point (le client initie la connexion)
- Le port 21 du serveur FTP aux ports distants >1024 (le serveur répond au port de contrôle du client)
- Les ports du serveur FTP >1024 de n'importe quel point (le client initie la connexion de données au port aléatoire spécifié par le serveur)
- Les ports du serveur FTP >1024 aux ports distants >1024 (le serveur envoie des ACK (et des données) au port de données du client)

Si vous ne souhaitez pas ouvrir le port 8999 sur le pare-feu, vous pouvez toujours autoriser les utilisateurs à accéder à Host On-Demand. Il existe deux possibilités :

- Utilisez l'assistant de déploiement pour créer des fichiers HTML contenant toutes les données de configuration. Ainsi, vous n'avez pas besoin d'accéder au serveur de configuration. Lors de la création des fichiers HTML, sélectionnez **Modèle de type HTML** dans la page Modèle de configuration de l'assistant de déploiement.
- Si vous souhaitez utiliser le serveur de configuration, vous pouvez configurer les clients pour qu'ils utilisent le servlet de configuration. Voir Configuring the configuration servlet dans l'aide en ligne de Host On-Demand. Cette option n'est disponible que si votre serveur d'applications Web prend en charge les servlets.

  Si vous utilisez le serveur de configuration et que ce dernier est séparé de votre navigateur Web par un pare-feu, vous devrez étendre le port du serveur de configuration sur le pare-feu ou exécuter le servlet de configuration Host On-Demand. Le servlet de configuration permet au navigateur de communiquer avec le serveur de configuration sur des protocoles Web standard tels que HTTP ou HTTPS (voir figure 4, à la page 13).

Connexion à un système hôte via un serveur Proxy

Les clients Host On-Demand peuvent utiliser un serveur Proxy pour accéder en toute transparence aux systèmes hôte à partir d'un pare-feu. Deux types de serveurs Proxy sont pris en charge :

- Serveurs Proxy Socks, présentés dans la section «Connexion via un serveur Proxy Socks», à la page 34. Les versions 4 et 5 du protocole Socks sont prises en charge.
- Serveurs Proxy HTTP, présentés dans la section «Connexion via un serveur Proxy HTTP», à la page 34.

Avant de vous connecter à un système hôte par l'intermédiaire d'un serveur Proxy, vous devez rechercher le protocole pris en charge par le serveur Proxy. Choisissez si vous voulez indiquer les paramètres du serveur Proxy par l'intermédiaire du navigateur Web ou identifier de manière explicite un serveur Proxy pour la

session. Si vous optez pour la deuxième solution, vous devez préciser le protocole qu'utilise le serveur Proxy, le nom du serveur, son numéro de port et d'autres renseignement.

D'une manière générale, si un serveur Proxy Socks est disponible, configurez les sessions Host On-Demand de façon à l'utiliser. Configurez les sessions de façon à utiliser un serveur Proxy HTTP s'il s'agit du seul type de serveur Proxy pris en charge sur votre site.

Connexion via un serveur Proxy Socks

De nombreuses entreprises ont recours aux serveurs Proxy Socks afin de protéger les ressources informatiques par un pare-feu. Socks est un protocole adapté aux serveurs Proxy réseau de type TCP/IP. Il permet aux applications situées d'un côté d'un serveur Proxy Socks d'accéder intégralement aux hôtes situés de l'autre côté du serveur Proxy Socks sans s'y connecter directement. En général, les serveurs Proxy sont utilisés avec des pare-feu. Avec le protocole Socks, un client qui demande une connexion au système hôte via un pare-feu se connecte à un serveur Proxy Socks. Ce dernier fait office d'intermédiaire entre le client et le système hôte. Il autorise les demandes de communication, se connecte à l'hôte au nom du client et assure la transmission des données entre les deux systèmes.

Host On-Demand prend en charge les versions 4 et 5 du protocole Socks.

- Le protocole Socks version 4 permet de spécifier le format et les conventions du message afin de permettre aux utilisateurs d'applications de type TCP de communiquer au moyen d'un pare-feu. Il offre un contrôle d'accès reposant sur des informations d'en-tête TCP, dont les adresses IP et les numéros de port source et cible.
- Le protocole Socks version 5 (également connu sous l'acronyme AFT, pour Authenticated Firewall Traversal) est une norme Internet ouverte pour les serveurs Proxy réseau. Il ajoute une authentification, une meilleure prise en charge de la résolution des noms de domaine, la prise en charge des adresses IPv6 et d'autres fonctions à la version 4. Ces fonctions sont très utiles pour les clients extérieurs au pare-feu. Un ID utilisateur de Socks et un mot de passe d'accès au serveur Proxy peuvent éventuellement être envoyés lors de la connexion entre le client Host On-Demand et le serveur Proxy. L'ID utilisateur et le mot de passe ne sont pas chiffrés. Pour plus d'informations sur la version 5, reportez-vous à la rubrique *Socks Protocol Version 5*.

La Machine virtuelle Java (JVM) utilisée dans la plupart des navigateurs Web prend en charge le protocole Socks version 4. Une session peut accéder à un serveur Proxy Socks version 4 ou version 5 en outrepassant les paramètres du serveur Proxy dans le navigateur Web. Vous pouvez également faire en sorte que la session négocie une connexion Socks version 4 si le serveur Proxy ne prend pas en charge la version 5. Pour plus d'informations sur le paramétrage du serveur Proxy Socks, reportez-vous à Proxy Server de l'aide en ligne.

Connexion via un serveur Proxy HTTP

Les serveurs Proxy HTTP traitent des requêtes HTTP via des pare-feu. Ils font office d'intermédiaires entre les réseaux privés locaux et Internet. Le serveur Proxy HTTP est à la fois connecté au réseau local et à Internet. Les utilisateurs locaux configurent leurs navigateurs afin de transmettre les requêtes HTTP via le serveur Proxy HTTP en précisant son adresse IP et son numéro de port TCP. Le serveur Proxy HTTP accepte ces requêtes HTTP et les réachemine vers les serveurs Web en cours spécifiés par les URL entrées dans le navigateur.

Pour les clients Host On-Demand, les serveurs Proxy HTTP font office d'agents de réacheminement pour les connexions à un système hôte. Ils établissent une connexion au système hôte et assurent la transmission des données entre le système hôte et le client. Même si le serveur Proxy HTTP coupe habituellement une connexion après avoir répondu à une requête HTTP, Host On-Demand maintient la connexion pour assurer le trafic de l'hôte en utilisant la méthode HTTP Connect (si elle est activée pour le serveur Proxy).

Si vous souhaitez qu'une session utilise un serveur Proxy HTTP, vous devez sélectionner le Proxy HTTP en tant que type de Proxy et indiquer le nom du serveur Proxy et son numéro de port. Pour plus d'informations sur le paramétrage du serveur Proxy HTTP, reportez-vous à Proxy Server de l'aide en ligne.

Sécurité liée à l'ID utilisateur

Web Express Logon

Si une application de sécurité de réseau est installée et que vous appliquez le modèle basé sur le serveur de configuration, vous pouvez sélectionner la connexion Web Express Logon dans l'assistant de déploiement pour permettre aux utilisateurs d'accéder aux hôtes et aux applications basées sur les hôtes, sans avoir à fournir d'ID utilisateur ni de mot de passe supplémentaires. L'indication de l'URL complète d'accès au serveur du mappeur d'autorisations d'accès indique à Host On-Demand où rechercher le servlet du mappeur d'autorisations d'accès, qui traite les requêtes HTTPS émises par l'utilisateur, effectue une recherche et renvoie les autorisations d'accès de l'utilisateur. Ces autorisations d'accès sont ensuite reprises pour ouvrir une connexion sécurisée et automatique à Host On-Demand.

Authentification native

Si vous utilisez un modèle basé sur le serveur de configuration, vous pouvez configurer vos utilisateurs Host On-Demand en vue de permettre leur authentification native. Cette option permet aux utilisateurs de se connecter à Host On-Demand à l'aide du même mot de passe que celui du système d'exploitation (AIX ou z/OS) sur lequel Host On-Demand est actif. Lorsqu'un utilisateur se connecte à Host On-Demand, son mot de passe est validé par comparaison à celui du système d'exploitation, et non par rapport à un mot de passe Host On-Demand distinct. L'administrateur dispose ainsi d'un point de contrôle unique pour l'administration du mot de passe, et l'utilisateur n'a qu'un seul mot de passe à retenir.

Pour plus d'informations sur l'activation de cette option, reportez-vous à la section Native Authentication de l'aide en ligne.

Connexion au domaine Windows

Si vos utilisateurs sont connectés à un domaine Windows, cette option (proposée avec le modèle de configuration dans l'assistant de déploiement) les connecte automatiquement à Host On-Demand sous leur nom d'utilisateur Windows. La fenêtre de connexion Host On-Demand ne s'ouvre pas et le nom d'utilisateur Windows est adopté en tant qu'ID utilisateur Host On-Demand. Si un ID utilisateur Host On-Demand n'existe pas encore (via la correspondance avec le nom d'utilisateur Windows), vous pouvez également choisir un ID utilisateur créé automatiquement dans le groupe Host On-Demand spécifié.

Pour plus d'informations sur le choix du mode d'accès pour les utilisateurs au serveur de configuration Host On-Demand, reportez-vous à Type de connexion.

Environnements FIPS

Si vous êtes dans un environnement qui impose ou requiert que vos composants de sécurité utilisent des composants/modules certifiés FIPS (Federal Information Processing Standards), tenez compte de ce qui suit. Pour sécuriser les connexions Telnet et FTP, Host On-Demand utilise par défaut les modules FIPS. Si votre environnement requiert une connexion à un hôte IBM System i pour le transfert de fichiers ou de données, assurez-vous que votre système répond aux exigences suivantes :

- Vous utilisez un interpréteur JRE Java certifié FIPS, par exemple, IBM 1.6.0 Service Release 5.
- Vous devez configurer le paramètre HTML UseJSSEforiSeries dans la fenêtre Options avancées de l'assistant de déploiement et le définir sur true.
- Vous devez ajouter le certificat de l'hôte IBM System i au stockage sécurisé du client JSSE (Java Secure Socket Extension) pour le JRE Java. Pour plus d'informations sur la configuration, consultez votre fournisseur JRE Java.

Si vous avez une connexion sécurisée sur un hôte IBM System i et que vous accédez aux fonctions de transfert de fichiers, vous serez invité à saisir le chemin d'accès et le mot de passe du stockage sécurisé de JSSE. Si vous effectuez un transfert de données vers un hôte IBM System i, d'autres zones s'affichent également pour la saisie du chemin d'accès et du mot de passe du stockage sécurisé de JSSE.

Une autre façon d'entrer le chemin d'accès et le mot de passe consiste à utiliser une applet Run qui est fournie avec Host On-Demand. Pour cela, appliquez la procédure suivante :

1. Dans le menu d'une session d'affichage, sélectionnez Actions > Exécution d'une applet.
2. Entrez `com.ibm.eNetwork.HOD.util.jsse.JSSESetup` dans la zone du nom de classe.
3. Cliquez sur OK.

Vous n'avez à configurer le stockage sécurisé JSSE qu'une seule fois. Il s'agit d'un paramètre global qui s'applique à toutes les sessions. Une fois entrées, les valeurs sont conservées jusqu'au prochain redémarrage du navigateur.

Dans les versions antérieures de Host On-Demand, l'authentification du mode FIPS pouvait être activée via un paramètre HTML. Dans cette version de Host On-Demand, une option de menu est fournie pour activer ou désactiver le mode FIPS pour chaque session. Par défaut, le mode FIPS est activé pour toutes les sessions.

Chapitre 5. Planification du support de langue nationale

Host On-Demand est disponible dans de multiples langues. Les fenêtres de session, les panneaux de configuration, les fichiers d'aide et la documentation ont été traduits. En outre, il intègre les fonctions d'écran, de clavier et de traitement pour l'arabe, l'hébreu, le thaï et l'hindi. Pour plus de détails, reportez-vous à l'aide en ligne.

Toutes les versions traduites sont fournies dans le téléchargement. Lorsque vous installez Host On-Demand sous i/OS, OS/400, Windows, AIX, Linux et Solaris à l'aide du programme d'installation graphique, vous pouvez choisir les langues à installer. Sur z/OS, vous pouvez sélectionner la langue par l'intermédiaire du mode console.

Le support de langue nationale varie selon le système d'exploitation utilisé. Ainsi, la police et le clavier correspondant à la langue dans laquelle vous souhaitez installer HOD doivent eux-même être installés sur le système d'exploitation. Par exemple, si vous souhaitez utiliser le Coréen comme langue de session hôte alors que la police coréenne et le support de clavier ne sont pas installés, les caractères ne s'affichent pas correctement.

DBCS ne peut pas être utilisé comme nom de fichier HTML.

Langues prises en charge

Les langues dans lesquelles Host On-Demand a été traduit sont toutes répertoriées ci-dessous, avec les suffixes correspondants. Ces derniers permettent de charger les versions traduites des clients. Par exemple, les pages HTML fournies par IBM ont des extensions de langue permettant d'identifier des installations de langue différente et des fichiers HTML prédéfinis de langue différente, comme HOD_en.html pour l'anglais.

Langue	**Suffixe**
Chinois simplifié	zh
Chinois traditionnel	zh_TW
Tchèque	cs
Danois	da
Néerlandais	nl
Anglais	en
Finnois	fi
Français	fr
Allemand	de
Grec	el
Hongrois	hu
Italien	it
Japonais	ja

Coréen	ko
Norvégien	no
Polonais	pl
Portugais (Brésil)	pt
Portugais	pt_PT
Russe	ru
Slovène	sl
Espagnol	es
Suédois	sv
Turc	tr
Catalan	Ca

Pages de codes hôte prises en charge

Host On-Demand prend en charge plusieurs pages de codes. Vous pouvez choisir des pages de codes différentes selon les sessions.

Pages de codes 3270 et 5250

Les pages de codes indiquées ci-dessous sont prises en charge par les sessions d'émulation 3270 et 5250. Vous pouvez les sélectionner dans la fenêtre Configuration de session.

Pays ou région	Page de codes	Important
Pays arabophones	420	
Autriche	273	
Autriche (euro)	1141	
Bélarus	1025	
Bélarus (euro)	1154	
Belgique	037	
Belgique (euro)	1140	
Belgique (ancien code)	274	
Bosnie-Herzégovine	870	
Bosnie-Herzégovine (euro)	1153	
Brésil	037	
Brésil (euro)	1140	
Brésil (ancien code)	275	
Bulgarie	1025	
Bulgarie (euro)	1154	
Canada	037	
Canada (euro)	1140	
RPC (chinois simplifié étendu)	1388	
Croatie	870	
Croatie (euro)	1153	

République tchèque	870	
République tchèque (euro)	1153	
Danemark	277	
Danemark (euro)	1142	
Estonie	1122	
Estonie (euro)	1157	
Finlande	278	
Finlande (euro)	1143	
France	297	
France (euro)	1147	
Macédoine (ex-République yougoslave)	1025	
Macédoine (ex-République yougoslave) (euro)	1154	
Allemagne	273	
Allemagne (euro)	1141	
Grèce	875	
Israël (nouveau code)	424	
Israël (ancien code)	803	
Inde (hindi)	1137	sessions écran 5250 uniquement
Hongrie	870	
Hongrie (euro)	1153	
Islande	871	
Islande (euro)	1149	
Italie	280	
Italie (euro)	1144	
Japon (katakana)	930	
Japon (katakana étendu)	930	
Japon (katakana Unicode étendu ; JIS2004)	1390	3270 uniquement
Japon (latin étendu)	939	
Japonais 1399 (latin Unicode étendu ; JIS2004)	1399	
Kazakhstan (euro)	1166	
Corée (euro)	1364	3270 uniquement
Corée (étendu)	933	
Amérique latine	284	
Amérique latine (euro)	1145	
Lettonie	1112	
Lettonie (euro)	1156	
Lituanie	1112	
Lituanie (euro)	1156	

Multilingue	500	
Multilingue ISO (euro)	924	
Multilingue (euro)	1148	
Pays-Bas	037	
Pays-Bas (euro)	1140	
Norvège	277	
Norvège (euro)	1142	
Edition ouverte	1047	
Pologne	870	
Pologne (euro)	1153	
Portugal	037	
Portugal (euro)	1140	
Roumanie	870	
Roumanie (euro)	1153	
Russie	1025	
Russie (euro)	1154	
Serbie-Monténégro (cyrillique)	1025	
Serbie-Monténégro (cyrillique, euro)	1154	
Slovaquie	870	
Slovaquie (euro)	1153	
Slovénie	870	
Slovénie (euro)	1153	
Espagne	284	
Espagne (euro)	1145	
Suède	278	
Suède (euro)	1143	
Taïwan (chinois traditionnel étendu)	937	
Taïwan (chinois traditionnel étendu, euro)	1371	
Thaï	838	
Thaïlande (euro)	1160	
Turquie	1026	
Turquie (euro)	1155	
Ukraine	1123	
Ukraine (euro)	1158	
Royaume-Uni	285	
Royaume-Uni (euro)	1146	
Etats-Unis	037	
Etats-Unis (euro)	1140	

Remarques :

- L'impression hôte 3270 avec une table de définition d'imprimantes (PDT) ne prend en charge que les pages de codes Latin-1, DBCS, bidirectionnelles et Thaï. Les autres pages de codes sont prises en charge en mode d'impression PDF ou sur les plateformes Windows sans PDT.
- Pour inclure davantage de caractères (définis dans la norme GB18030 du Gouvernement de la République populaire de Chine), l'Extension 6582 - Unicode A et 1 948 caractères non-Han supplémentaires (mongol, ouïgour, tibétain et yi) ont été ajoutés à la page de codes 1388 en chinois simplifié pour Host On-Demand version 6.

Pages de codes VT

Langue	Page de codes
Arabe	ASMO 708 et ASMO 449
Anglais (Royaume-Uni)	1101
Grec DEC	
Hébreu DEC	
Jeu de caractères de remplacement universel DEC	1100
Technique DEC	
Néerlandais	1102
Finnois	1103
Français	1104
Français (Canada)	1020
Allemand	1011
Hébreu NRCS	
Grec ISO supplémentaire (ISO Latin 7)	813
Hébreu ISO supplémentaire	
ISO Latin 1	819
Italien	1012
Norvégien/Danois	1105
PC Danois/Norvégien	865
International PC	437
Multilingue PC	850
Portugais PC	860
GBK RPC	936
Espagnol PC	220
Espagnol	1023
Suédois	1106
Suisse	1021
Etats-Unis	1100

Pages de codes de la passerelle CICS

Page de codes	Jeu de caractères
000	Détection automatique (par défaut)
437	Latin-1
813	ISO Grec (8859_7)
819	ISO Latin 1 (8859_1)
850	Latin 1
852	Latin 2
855	Cyrillique
856	Hébreu
857	Latin 5
864	Arabe
866	Cyrillique
869	Grec
874	Thaï
912	ISO Latin 2 (8859_2)
915	ISO Cyrillique (8859_5)
920	ISO Latin 5 (8859_9)

Prise en charge des caractères japonais JIS2004 en Unicode

Pour activer la prise en charge des caractères japonais JIS2004, sélectionnez les pages de codes hôte existantes 1390 Japanese (Katakana Unicode Extended) et 1399 Japanese (Latin Unicode Extended). Les fonctions prises en charge sont les suivantes :

- Modification de l'espace de présentation
- Affectation des touches
- Transfert de fichiers
- Impression d'écran
- Session d'impression
- GDI
- Adobe PDF
- Host Access Class Library (HACL)

Les fonctions suivantes ne sont pas incluses en raison de certains formats Unicode actuellement non pris en charge dans Host On-Demand :

- Macro
- Utilisation d'une table de définition d'imprimante (PDT) dans une session d'impression

Mappage des caractères définis par l'utilisateur

Pour les langues utilisant un jeu de caractères codé sur deux octets (DBCS), vous pouvez utiliser le mappage UDC dans votre session (imprimante hôte 3270, 5250, 3270) plutôt que le mappage par défaut. Vous pouvez créer une table de conversion UDC à l'aide de l'éditeur de mappage de caractères définis par

l'utilisateur pour stocker le mappage personnalisé de votre session. Pour plus de détails sur l'utilisation de l'éditeur de mappage UDC pour modifier le mappage des caractères, reportez-vous à Using the user-defined character (UDC) mapping editor de l'aide en ligne.

Support Unicode pour i/OS et OS/400

Voir «Support Unicode pour i/OS et OS/400», à la page 128.

Partie 2. Installation, mise à niveau et désinstallation de Host On-Demand

Chapitre 6. Installation du serveur Host On-Demand et des logiciels associés

Ce chapitre traite de l'installation des trois composants de Host On-Demand suivants :

- Le serveur Host On-Demand, nécessaire à l'utilisation de Host On-Demand. Pour plus d'informations, reportez-vous à «Installation de Host On-Demand à l'aide d'Installation Manager».
- Le servlet de configuration Host On-Demand, nécessaire uniquement si vous prévoyez d'utiliser Host On-Demand avec un pare-feu. Pour plus d'informations, reportez-vous à «Installation du servlet de configuration», à la page 61.
- L'assistant de déploiement, outil particulièrement utile qui s'exécute sous Windows et génère des clients Host On-Demand personnalisés. L'installation de l'assistant de déploiement n'est pas obligatoire, mais elle est vivement recommandée. Pour plus d'informations, reportez-vous à «Assistant de déploiement», à la page 51.

Installation de Host On-Demand à l'aide d'Installation Manager

L'installation de Host On-Demand nécessite IBM Installation Manager. IBM Installation Manager doit d'abord être installé en mode administrateur sur le système où vous envisagez d'installer Host On-Demand. Vous pouvez ensuite utiliser Installation Manager pour installer Host On-Demand.

IBM Installation Manager version 1.8.3 ou ultérieure est requis pour installer Host On-Demand.

Liens importants

Reportez-vous aux instructions de la section Installation ou mise à jour d'Installation Manager pour installer Installation Manager. Pour plus d'informations sur IBM Installation Manager, voir IBM Installation Manager dans IBM Knowledge Center.

Avant l'installation de Host On-Demand

Préparation de l'installation

Vérifiez que la machine sur laquelle l'installation doit avoir lieu satisfait à toutes les conditions préalables.

La configuration logicielle requise pour Host On-Demand est décrite dans la rubrique Software Products Compatibility Reports. Vérifiez chaque point de la liste suivante en vue de la préparation :

- Assurez-vous qu'IBM Installation Manager version 1.8.3 ou ultérieure est installé.
- L'installation nécessite au moins 1,2 Go d'espace disque sur la machine (espace installé et temporaire) pour l'architecture 32 bits et une langue. Pour installer plusieurs langues, cette valeur passe à 4 à 8 Mo pour chaque langue.
- Vous avez besoin d'au minimum 4,5 Go pour le référentiel de produit multiplateforme (téléchargement et extraction).
- Les utilisateurs doivent se connecter avec des privilèges administrateur.

- Une version prise en charge du serveur HTTP (par exemple, IBM HTTP Server ou Apache Server) est installée sur le système.

Mise à niveau de Host On-Demand à partir de versions précédentes

Si vous disposez d'une version précédente de Host On-Demand, telle que Host On-Demand version 11.0, il n'existe pas de chemin de migration direct de Host On-Demand version 11 vers Host On-Demand version 13.0 et versions ultérieures. Pour effectuer la migration, procédez comme suit :

1. Sauvegardez tous les fichiers personnalisés contenus dans les répertoires de la version antérieure de Host On-Demand, spécifiquement dans le répertoire privé, ainsi que toutes les pages client créées avec l'assistant de déploiement. Ces fichiers peuvent être réutilisés dans HOD version 12.0 et versions ultérieures.
2. Désinstallez toutes les installations existantes de Host On-Demand version 11.0.
3. La première installation de Host On-Demand et les installations suivantes nécessitent qu'un chemin vide soit disponible. Par conséquent, vous pouvez soit renommer, soit supprimer les dossiers ou répertoires existants où une version antérieure a déjà été installée.
4. Installez Host On-Demand à l'aide d'IBM Installation Manager. Il est recommandé de ne pas cliquer sur **Annuler** lorsqu'une installation est en cours.
5. Restaurez le répertoire privé dans les dossiers ou répertoires Host On-Demand.
6. Editez tous les clients créés avec l'assistant de déploiement avec l'assistant de déploiement Host On-Demand, puis effectuez le déploiement vers le serveur Host On-Demand.

Pour effectuer la migration de HOD version 12.0 vers HOD version 13.0

1. Démarrez Installation Manager selon les instructions correspondant à la plateforme.
2. Sélectionnez **Fichier > Préférences**.
3. Sélectionnez **Référentiels** à gauche. Cette option montre les référentiels disponibles qui ont été ajoutés à Installation Manager.
4. Sélectionnez **Ajouter un référentiel** si Host On-Demand ne figure pas dans la liste.
5. Cliquez sur **Parcourir** et naviguez jusqu'à l'emplacement du chemin d'accès au module de mise à jour de Host On-Demand extrait, puis sélectionnez le fichier diskTag.inf présent dans le dossier disque1.
6. Cliquez sur **OK** ; l'emplacement du nouveau référentiel devrait être répertorié.
7. Cliquez sur **Tester les connexions** pour vérifier que l'adresse URL du référentiel est accessible.
8. Sur la page d'accueil d'Installation Manager, cliquez sur **Mettre à jour**. Installation Manager recherche les packages disponibles dans les référentiels définis.
9. Sélectionnez IBM Host On-Demand.
10. Cliquez sur le bouton **Suivant**.
11. Lisez les dispositions et cliquez sur le bouton suivant.
12. Cliquez sur le bouton **Mettre à jour**.

Remarque : la migration peut être effectuée via l'utilitaire de migration de HOD, lequel est disponible sur Fix Central et permet de mettre à jour les paramètres de

session, de conditionner tous les fichiers personnalisés et les fichiers HTML, et de les modifier selon les conditions requises par HOD version 13.0.

Pour plus d'informations, voir : Utilitaire de migration

Installation de Host On-Demand

Vous pouvez installer Host On-Demand à l'aide d'Installation Manager sur toutes les plateformes prises en charge. Vous pouvez effectuer l'installation à l'aide de l'interface graphique d'Installation Manager (IM), du mode commande ou du mode console. La plupart des plateformes prennent en charge l'interface graphique d'Installation Manager, à l'exception de z/OS. Pour effectuer une installation sur z/OS, vous pouvez utiliser le mode console ou les travaux BPXBATCH.

Installation à l'aide de l'interface graphique d'Installation Manager

Interface graphique utilisateur d'Installation Manager :

1. Démarrez Installation Manager selon les instructions correspondant à la plateforme.
2. Sélectionnez **Fichier** > **Préférences**.
3. Sélectionnez **Référentiels** à gauche. Cette option montre les référentiels disponibles qui ont été ajoutés à Installation Manager.
4. Sélectionnez **Ajouter un référentiel** si Host On-Demand ne figure pas dans la liste.
5. Cliquez sur **Parcourir** et naviguez jusqu'à l'emplacement du chemin de Host On-Demand extrait. Sélectionnez le fichier diskTag.inf figurant dans le dossier disque 1 pour l'installation initiale.
6. Cliquez sur **OK** ; l'emplacement du nouveau référentiel devrait être répertorié.
7. Cliquez sur **Tester les connexions** pour vérifier que l'adresse URL du référentiel est accessible.
8. Sur la page d'accueil d'Installation Manager, cliquez sur **Installer**. Installation Manager recherche les packages disponibles dans les référentiels définis.
9. Sélectionnez **le package Host On-Demand**. Cliquez sur **Suivant**.
10. Lisez les contrats de licence. Si vous êtes d'accord avec les termes, cliquez sur **J'accepte le contrat de licence** et cliquez sur **Suivant** pour poursuivre.
11. Sélectionnez **Créer un groupe de packages**, puis choisissez **l'architecture**.
12. Si le système d'exploitation est 64 bits, vous devez sélectionner *64 bits* ou *32 bits* pour installer le produit dans le mode de bits correspondant.
13. Cliquez sur **Suivant**.
14. Sélectionnez les langues à installer. La valeur par défaut est *Anglais*. Cliquez sur **Suivant**.
15. Sélectionnez **la fonction Host On-Demand 13.0**. Cliquez sur **Suivant**.
16. Vérifiez et indiquez toutes les informations sous l'onglet Host On-Demand 13.0.
    a. Sur le panneau *Informations de diffusion*, sous Host On-Demand 13.0, définissez le **répertoire de diffusion**, indiquez l'alias de serveur Web ainsi que le *numéro de port du gestionnaire de services*. Cliquez sur **Suivant**.

       Le répertoire de diffusion doit être accessible aux clients. Vous pouvez indiquer le chemin d'accès au répertoire de diffusion. Effectuez les opérations suivantes :

1) Spécifiez un alias pour le répertoire (la valeur par défaut est *hod*).
2) Spécifiez le port du gestionnaire de services destiné à permettre aux clients Host On-Demand de communiquer avec ce gestionnaire. Cette communication est nécessaire pour exploiter les options de déploiement suivantes :
   - Utilisation du serveur de configuration pour assurer la maintenance des informations de configuration de session comme dans les modèles basés sur le serveur de configuration et les modèles de déploiement combinés, tels que décrits dans le Chapitre 2, «Planification du déploiement», à la page 11.
   - IBM recommande la désignation du *port 8999* pour ces besoins. Reportez-vous à la documentation de votre serveur pour savoir si ce port est utilisé. Si tel est le cas, vous pourrez changer de port au cours de l'installation ou plus tard. Pour plus d'informations sur le changement de port du gestionnaire de services, voir Changing the Service Manager's configuration port dans l'aide en ligne.

b. Sur le panneau du serveur Web sous Host On-Demand 13.0, sélectionnez l'option de serveur Web qui correspond à vos besoins :
   - Sélectionnez **Sans serveur Web** lorsque le serveur Web est configuré manuellement par l'utilisateur. Cette option est recommandée pour les serveurs Web tels que IPlanet et Lotus Domino. L'utilisateur est invité à contacter son administrateur de serveur Web ou à se reporter à la documentation du serveur Web pour obtenir des informations détaillées.
   - Sélectionnez l'option 'Sélectionnez dans la liste des serveurs Web détectés', puis sélectionnez le serveur Web dans la liste si plusieurs serveurs sont détectés.
   - Sélectionnez l'option **Sélectionnez manuellement un serveur Web spécifique**, au cas où un serveur IBM HTTP Server ou Apache Web Server serait installé mais non détecté.
     – Sélectionnez le type de serveur Web qui est installé sur votre système.
     – Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier de configuration (httpd.conf) du serveur Web installé dans votre système. Vous pouvez aussi entrer dans la zone le chemin d'accès complet du fichier httpd.conf dans le répertoire d'installation du serveur Web.

c. Sur le panneau du serveur d'applications sous Host On-Demand 13, si le programme d'installation détecte IBM WebSphere Application Server sur votre système, vous pouvez configurer le servlet de configuration. Dans le panneau suivant disponible à partir de l'onglet du serveur d'applications, vous êtes invité à configurer (ou non) le servlet de configuration Host On-Demand dans WebSphere Application Server. Pour plus d'informations, voir Installation du servlet de configuration.

   Décochez la case si vous n'envisagez pas d'utiliser le servlet de configuration.

   Dans le cas contraire, sélectionnez le serveur d'applications dans la liste des serveurs d'applications détectés. Le programme d'installation déploie automatiquement le servlet de configuration sur le serveur d'applications que vous désignez, puis configure vos clients de sorte qu'ils accèdent au gestionnaire de services par le biais du servlet.

   Remarque :

   - Websphere application server est détecté s'il a été installé par le même programme IBM Installation Manager sur le

système. Les versions pouvant être détectées sont Websphere Application Server version 8.0 et Websphere Application Server version 8.5.2.

- La configuration de servlet lors de l'installation n'est pas prise en charge pour un serveur d'applications sur lequel la sécurité administrative est activée.

d. Une fois que les panneaux sont correctement mis à jour, cliquez sur **Suivant**.

17. Lisez le récapitulatif et cliquez sur **Installer**.
18. Une fois l'installation terminée, une page récapitulative est affichée. Vérifiez les messages.
    - Si l'installation a réussi, le programme affiche un message pour confirmer le succès de l'installation. Le programme peut également afficher d'importantes instructions de post-installation. Cliquez sur **Terminer**.
    - Si l'installation a échoué, cliquez sur **Afficher le fichier journal** pour résoudre le problème.
19. Pour vous assurer que l'installation a réussi, vous pouvez effectuer les actions supplémentaires suivantes :
    a. Redémarrez le serveur Web.
    b. Assurez-vous que les pages Host On-Demand sont accessibles sur le navigateur. Si elles ne le sont pas, vérifiez la configuration du serveur Web et assurez-vous que les fichiers du répertoire de diffusion Host On-Demand sont accessibles. Pour plus d'informations sur la configuration du serveur Web, reportez-vous à la documentation relative à ce dernier.

Assistant de déploiement

L'assistant de déploiement est automatiquement installé comme composant de l'installation du serveur Host On-Demand sous Windows. Ce produit est également disponible séparément pour les clients qui ne souhaitent pas installer l'intégralité du serveur Host On-Demand sous Windows.

Pour z/OS et iSeries, le package d'installation de l'assistant de déploiement se trouve sur le serveur HOD, dans le répertoire *<rép_install>/HOD/depwiz* appelé DW.zip. Ce fichier peut être téléchargé sur un poste de travail Windows et installé comme un package distinct.

Mise à niveau de l'assistant de déploiement à partir de versions précédentes

Si vous disposez d'une version précédente de l'assistant de déploiement, telle que Host On-Demand version 11.0, il n'existe pas de chemin de mise à niveau direct de l'assistant de déploiement version 11.0 vers l'assistant de déploiement version 12.0 et versions ultérieures. Pour effectuer la mise à niveau, procédez comme suit :

1. Effectuez une sauvegarde de tous les fichiers personnalisés contenus dans le répertoire de l'assistant de déploiement. Vous pouvez éditer tous les fichiers existants avec l'assistant de déploiement de la version 12.
2. Le nouvel assistant de déploiement nécessite qu'un chemin vide soit disponible. Par conséquent, renommez ou supprimez le dossier d'installation existant de l'assistant de déploiement.
3. Installez l'assistant de déploiement à l'aide d'IBM Installation Manager.
4. Redéployez vos fichiers personnalisés dans le dossier d'installation de l'assistant de déploiement.

Installation de l'assistant de déploiement

Sur les plateformes Windows, l'assistant de déploiement est installé automatiquement à l'installation de Host On Demand.

Pour installer et exécuter l'assistant de déploiement, effectuez les tâches suivantes :

1. Ouvrez Installation Manager.
2. Ajoutez l'emplacement de référentiel Host On-Demand à Installation Manager :
   a. Sur la page d'accueil d'Installation Manager, cliquez sur **Fichier >Préférences**, puis cliquez sur **Référentiels**. La page Référentiels s'ouvre, indiquant tous les référentiels disponibles, leurs emplacements et leur état de connexion.
   b. Dans la page Référentiels, cliquez sur **Ajouter un référentiel**.
   c. Dans la boîte de dialogue Ajouter un référentiel, cliquez sur **Parcourir**.
   d. Accédez à l'emplacement du premier disque de Host On-Demand et sélectionnez le fichier diskTag.inf, puis cliquez sur **OK**. L'emplacement du nouveau référentiel apparaît dans la liste.
   e. Cliquez sur **Tester les connexions** pour vérifier que l'adresse URL du référentiel est accessible.
   f. Sur la page d'accueil, cliquez sur **Installer**. Installation Manager recherche les packages disponibles dans les référentiels définis.
   g. Répétez les étapes ci-dessus pour le deuxième disque. Si vous poursuivez sans configurer le deuxième disque, Installation Manager confirme ce choix à l'utilisateur pendant le processus d'installation.
3. Sélectionnez le package de l'assistant de déploiement Host On-Demand.
4. Assurez-vous que la version 13.0 indiquée en dessous est également sélectionnée. Cliquez sur **Suivant**.
5. Sur le panneau Installer des packages, sélectionnez **Créer un package** et sélectionnez **Assistant de déploiement IBM Host On-Demand** comme nom du groupe de packages.
6. Si l'architecture sélectionnée est 64 bits, remplacez la sélection par 32 bits si nécessaire. Cliquez sur **Suivant**.
7. Sur le panneau Installer des packages, sélectionnez la fonction Assistant de déploiement Host On-Demand 13.0. Les informations sur le disque indiquées dans la zone inférieure du panneau fournissent des informations sur l'espace disque disponible et sur l'espace disque requis. Cliquez sur **Suivant**.
8. Sélectionnez l'onglet relatif au panneau Emplacement du serveur Host On-Demand de l'assistant de déploiement sous l'en-tête Assistant Host On-Demand 13.0 (onglet de gauche). L'emplacement du serveur Host On-Demand indique le lien vers le serveur Host On-Demand. Assurez-vous qu'un lien valide et opérationnel vers le serveur Host On-Demand est entré dans la zone. Cliquez sur **Suivant**.
9. Dans le panneau récapitulatif, vérifiez les packages sélectionnés et les sélections d'installation. Cliquez sur **Installer** pour poursuivre l'installation.

Téléchargement de l'image d'installation de l'assistant de déploiement à partir d'un serveur Host On-Demand

L'image de l'assistant de déploiement est livrée avec toutes les plateformes du serveur Host On-Demand et peut être téléchargée à partir du serveur, puis installée sur toute machine Windows.

Il existe deux manières de télécharger l'assistant de déploiement à partir d'un serveur Host On-Demand : via la page HODMain_xx.html, où xx est le suffixe à deux lettres désignant votre langue, ou via le protocole FTP depuis le serveur. Le téléchargement via HODMain_xx.html se fait à travers le serveur Web. Procédez comme suit :

1. A partir d'une machine Windows, lancez votre navigateur et pointez sur le fichier HODMain_xx.html du serveur Host On-Demand, où *xx* est un suffixe de langue à deux lettres.
2. Cliquez sur l'onglet 3 Administrateurs.
3. Cliquez sur le lien de l'assistant de déploiement pour télécharger l'image d'installation de l'assistant de déploiement sur votre machine Windows.
4. Exécutez Installation Manager pour installer l'assistant de déploiement.
5. Une fois l'installation terminée, vous pouvez démarrer l'assistant de déploiement à partir du menu **Démarrer** > **Programmes**.

Pour télécharger via le protocole FTP, procédez comme suit :

1. A partir de votre machine Windows, établissez le protocole FTP à votre serveur HOD.
2. A l'invite, connectez-vous au serveur.
3. Entrez *bin* pour définir le mode sur binaire.
4. Entrez *cd* pour accéder au répertoire où se trouve le fichier de l'assistant de déploiement. L'emplacement sera *<répertoire_installation>/HOD/depwiz*.
5. Entrez *get DW.zip* pour obtenir le fichier.
6. Extrayez le fichier zip sur la machine Windows.
7. Exécutez Installation Manager pour installer l'assistant de déploiement.
8. Démarrez l'assistant de déploiement à partir du menu **Démarrer** > **Programmes** sur le bureau.

Host Access Toolkit

Host Access Toolkit est installé séparément pour les clients qui souhaitent écrire leur propre application Host On-Demand.

Installation de Host Access Toolkit

Pour installer Host Access Toolkit sur un système Windows, effectuez les étapes de base suivantes :

1. Ouvrez Installation Manager.
2. Ajoutez l'emplacement de référentiel Host On-Demand à Installation Manager.
   a. Sur la page d'accueil d'Installation Manager, cliquez sur **Fichier** >**Préférences**, puis cliquez sur **Référentiels**. La page Référentiels s'ouvre, indiquant tous les référentiels disponibles, leurs emplacements et leur état de connexion.
   b. Dans la page Référentiels, cliquez sur **Ajouter un référentiel**.
   c. Dans la boîte de dialogue Ajouter un référentiel, cliquez sur **Parcourir**. Accédez à l'emplacement du premier disque Host On-Demand, puis sélectionnez le fichier diskTag.inf. Cliquez ensuite sur **OK**. L'emplacement du nouveau référentiel apparaît dans la liste.
   d. Cliquez sur **Tester les connexions** pour vérifier que l'adresse URL du référentiel est accessible.

e. Sur la page d'accueil, cliquez sur **Installer**. Installation Manager recherche les packages disponibles dans ses référentiels définis.

f. Répétez les étapes ci-dessus pour le deuxième disque. Si vous poursuivez sans configurer le deuxième disque, Installation Manager vous confirme ce choix pendant le processus d'installation.

3. Sélectionnez le package Host Access Toolkit.
4. Assurez-vous que la version 13.0 indiquée en dessous est également sélectionnée. Cliquez sur **Suivant**.
5. Sur le panneau Installer des packages, sélectionnez **Créer un package** et sélectionnez **IBM Host Access Toolkit** comme nom du groupe de packages.
6. Si l'architecture sélectionnée est 64 bits, remplacez la sélection par 32 bits (valeur recommandée). Cliquez sur **Suivant**.
7. Sélectionnez les langues à installer. La valeur par défaut est *Anglais*. Cliquez sur **Suivant**.
8. Sur le panneau Installer des packages, sélectionnez la fonction Host Access Toolkit 13.0. Les informations sur le disque indiquées dans la zone inférieure du panneau fournissent des informations sur l'espace disque disponible et sur l'espace disque requis. Cliquez sur **Suivant**.
9. Sélectionnez l'onglet relatif au panneau Host Access Toolkit 13.0 sous l'en-tête Host Access Toolkit 13.0 dans l'onglet de gauche.
10. Dans le panneau récapitulatif, vérifiez les packages sélectionnés et les sélections d'installation. Cliquez sur **Installer** pour poursuivre l'installation.

Installation en mode console

Ce chapitre contient des instructions d'utilisation du mode console d'Installation Manager destinées à l'installation de Host On-Demand sur les plateformes ne prenant pas en charge une interface graphique utilisateur.

Remarque : Si vous effectuez une installation pour IBM iSeries, nous vous invitons à lire la section «Avant l'installation de Host On-Demand sur IBM iSeries», à la page 55.

A propos de l'installation en mode console

Sur les systèmes Linux, UNIX et z/OS qui ne prennent pas en charge une interface graphique utilisateur, les administrateurs peuvent utiliser l'interface console d'Installation Manager pour installer Host On-Demand.

Dans le mode console d'IBM Installation Manager, vous pouvez utiliser les packages d'installation pour effectuer les tâches suivantes :

- Installation
- Mise à niveau
- Modification
- Restauration
- Désinstallation

Pour lancer le mode console d'Installation Manager, utilisez l'utilitaire *imcl* qui est disponible dans le répertoire d'outils d'Installation Manager.

Ces étapes sont typiques d'une installation en mode console. Pendant la session d'installation, les invites en mode console qui s'affichent sont spécifiques au package concerné. Vous pouvez suivre les options qui s'affichent sur l'écran de console pour continuer l'installation.

L'interface en mode console d'Installation Manager suit les conventions ci-dessous :

- [X] indique une option sélectionnée.
- [] indique une option qui n'est pas sélectionnée.
- Les commandes par défaut sont mises entre crochets [ ].
- [N] indique que la commande par défaut est N: Next (Suivant).

Remarque : Plus d'informations sur Installation Manager et sur le mode console sont disponibles dans IBM Knowledge Center, dans la rubrique spécifique à la version d'Installation Manager que vous avez installée.

Vous pouvez installer Installation Manager en suivant les informations de la documentation Installation ou mise à jour d'Installation Manager.

L'installation de Host On-Demand doit s'effectuer en mode Administrateur. Pour plus d'informations sur le téléchargement d'Installation Manager, voir la rubrique sur la configuration requise d'Installation Manager et de Packaging Utility. Le niveau minimal requis pour installer Host On-Demand est la version 1.8.3.

Pour plus d'informations sur l'utilisation d'Installation Manager, voir IBM Installation Manager dans IBM Knowledge Center.

Avant l'installation de Host On-Demand sur IBM iSeries

L'installation de Host On-Demand sur les plateformes IBM iSeries est prise en charge via le mode console d'Installation Manager. Le mode interface graphique utilisateur d'Installation Manager n'est pas disponible sur IBM iSeries.

Des remarques supplémentaires à connaître avant l'installation de Host On-Demand sur IBM iSeries sont indiquées ci-dessous :

- Assurez-vous qu'IBM Installation Manager version 1.8.3 ou ultérieure est installé et qu'il l'a été en mode administrateur. Nous vous recommandons de lire la documentation d'IBM Installation Manager pour obtenir des informations complémentaires. (Pour en savoir plus sur l'installation d'Installation Manager version 1.8.3, voir Installation d'Installation Manager sous IBM i.)
- L'installation doit s'effectuer par un utilisateur disposant de privilèges d'administrateur ou de superutilisateur.
- L'installation distante sous IBM i est indisponible dans Host On-Demand version 13.0 à l'aide d'Installation Manager.

Pour commencer l'installation, vous devez effectuer les tâches suivantes :

1. Copiez les fichiers zip ESD de Host On-Demand sur le serveur IBM i à partir de FTP ou en utilisant une autre méthode classique, puis extrayez le fichier zip.
2. Ouvrez Installation Manager et configurez un référentiel en fournissant le chemin d'accès complet au fichier diskTag.inf qui se trouve sur le disque Host On-Demand.
3. Effectuez les étapes restantes, de la manière prévue dans l'installation en mode console.

Procédure d'installation

Pour installer Host On-Demand en mode console, effectuez les tâches suivantes :

1. Démarrez IBM Installation Manager en mode console. Ouvrez une invite de commande avec les privilèges d'administrateur, puis accédez au dossier *tools* qui se trouve dans le répertoire d'installation d'IBM Installation Manager.
2. Exécutez la commande suivante dans le répertoire tools

   ```
   imcl -c
   ```

   .

   Sur différents systèmes d'exploitation, par exemple :

   - AIX® ou Linux :

     ```
     /opt/IBM/InstallationManager/eclipse/tools/imcl –c
     ```

   - IBM i :

     ```
     /QIBM/ProdData/InstallationManager/eclipse/tools/imcl –c
     ```

   - Windows :

     ```
     \Program Files\IBM\Installation Manager\eclipse\tools\imcl.exe -c
     ```

   - z/OS :

     ```
     /InstallationManager/bin/eclipse/tools/imcl -c
     ```

     Pour plus d'informations sur le démarrage d'Installation Manager en mode console, voir Démarrage du mode console.
3. Dans la fenêtre console, spécifiez le référentiel d'IBM Host On-Demand :
   a. Entrez *P*, puis appuyez sur **Entrée** pour éditer les préférences.
   b. Entrez *1*, puis appuyez sur **Entrée** pour spécifier les référentiels.
   c. Entrez *D*, puis appuyez sur **Entrée** pour ajouter un référentiel.
   d. Entrez le chemin de référentiel pour IBM Host On-Demand 13.0. Par exemple, *<chemin>\HOD\disque1\diskTag.inf*.
   e. Entrez *A*, puis appuyez sur **Entrée** pour sauvegarder les informations de référentiel.
   f. Entrez *R*, puis appuyez sur **Entrée** pour revenir au menu principal.
4. Sélectionnez *1* pour effectuer l'installation à partir du menu principal. Si vous possédez des référentiels qui nécessitent des données d'identification, vous êtes invité à entrer vos ID utilisateur et mot de passe. Vous pouvez également sauvegarder vos données d'identification lorsque cela vous est demandé. Voir Enregistrement des données d'identification en mode console dans la section Installation Manager d'IBM Knowledge Center.
5. Sur le panneau de sélection des packages à installer, entrez le numéro approprié pour sélectionner le package Host On-Demand 13.0.
6. Sur le panneau suivant, entrez le numéro approprié pour sélectionner la version 13.0 à installer, puis appuyez sur la touche **Entrée**.
7. Entrez *N* pour continuer.
8. Entrez le numéro approprié pour afficher le contrat de licence. Pour accepter le contrat de licence, entrez *A*, puis appuyez sur la touche **Entrée**. Entrez N et appuyez sur la touche **Entrée** pour continuer.
9. Sélectionnez le **répertoire de ressources partagées d'Installation Manager**. Pour plus d'informations, reportez-vous à la Présentation des groupes de packages et du répertoire des ressources partagées. Pour changer le répertoire, entrez *M*, puis appuyez sur la touche **Entrée**. Entrez le chemin d'accès correct, puis entrez *N* pour continuer.

10. Le panneau Emplacement vous permet d'indiquer l'emplacement du répertoire d'installation d'IBM Host On-Demand 13.0. Entrez *M* pour changer l'emplacement du répertoire d'installation. Entrez le chemin d'accès correct, puis entrez *N* pour continuer.
11. L'architecture du package s'affiche lorsque vous effectuez une installation sur un système d'exploitation 64 bits. En ce qui concerne les nouveaux groupes de packages, vous pouvez modifier le mode de bits en entrant *T : Passer en architecture bits*. Par exemple, si l'Architecture sélectionnée indique 64 bits et que l'option *T* affichée est Passer en architecture 32 bits, entrez *T* pour passer en architecture 32 bits.
12. Pour accepter les valeurs par défaut ou poursuivre après la saisie d'une valeur différente, entrez *N* pour continuer.
13. Sur le panneau des langues, entrez le numéro indiqué à gauche de la langue pour l'ajouter ou la supprimer de la liste des langues à installer. Vous ne pouvez sélectionner qu'une langue à la fois. Cliquez sur *S* pour sélectionner toutes les langues. L'anglais est sélectionné par défaut et cette langue est obligatoire. Vos choix de langues s'appliquent à tous les packages installés du groupe de packages. Entrez *N* pour continuer.
14. Le panneau suivant est le menu Configurations, dans lequel vous pouvez indiquer les détails de configuration requis par l'installation de Host On-Demand 13 :

    En règle générale, le menu de configuration de Host On-Demand 12 comporte les entrées suivantes :

    - Informations de diffusion
    - Serveur Web

    a. Entrez le numéro approprié à gauche de l'entrée Informations de diffusion pour vérifier les paramètres. Le panneau Informations de diffusion indique les informations suivantes :

       - *Répertoire de diffusion cible* est l'emplacement où les fichiers Host On-Demand auxquels les utilisateurs accèdent à partir du Web sont installés. Une valeur par défaut apparaît dans le panneau. Entrez *1* pour modifier l'emplacement si nécessaire.
       - *Alias de diffusion Host On-Demand* est le paramètre de l'alias de serveur Web pour le répertoire de diffusion Host On-Demand. Entrez *A* pour modifier l'emplacement si nécessaire.
       - *Port du gestionnaire de services* est le numéro de port sur lequel le gestionnaire de services Host On-Demand est en mode écoute. Spécifiez le *port du gestionnaire de services* par le biais duquel les clients Host On-Demand communiqueront avec ce gestionnaire. Cette communication est nécessaire pour exploiter les options de déploiement suivantes :
         – Utilisation du serveur de configuration pour assurer la maintenance des informations de configuration de session (comme dans les modèles basés sur le serveur de configuration et les modèles de déploiement combinés, tels que décrits dans le Chapitre 2, «Planification du déploiement», à la page 11).

       Port 8999 est le port par défaut pour Host On-Demand. Vérifiez auprès de votre administrateur si ce port est occupé. Si tel est le cas, vous pourrez changer de port au cours de l'installation ou plus tard. Pour plus d'informations sur le changement de port du gestionnaire de services, voir Changing the Service Manager's configuration port dans l'aide en ligne.

Entrez le numéro associé à l'une de ces options pour modifier les paramètres respectifs. Reportez-vous aux autres options affichées à l'écran pour vous déplacer.

b. Entrez le numéro approprié à gauche du serveur Web pour vérifier ses paramètres.

1) Le panneau du serveur Web affiche les options suivantes. Vous devez sélectionner l'option de serveur Web qui correspond à vos besoins :

- **Sans serveur Web** : sélectionnez cette option lorsque vous configurez le serveur Web manuellement ou lorsqu'il n'y a pas de serveur Web. Cette option est recommandée pour les serveurs Web tels que IPlanet ou Lotus Domino. Contactez l'administrateur du serveur Web ou reportez-vous à la documentation du serveur Web pour obtenir des détails.

  Remarque : Sélectionnez *Sans serveur Web* pour les installations z/OS car le serveur Web ne pouvant être détecté, il doit être configuré manuellement.

- **Sélectionnez dans la liste des serveurs Web détectés** : sélectionnez cette option pour choisir un serveur Web détecté.
- **Sélectionnez manuellement un serveur Web spécifique** : sélectionnez cette option lorsqu'un serveur IBM HTTP Server 8.5 ou Apache Web Server 2.2 est installé mais non détecté. Vous devez entrer le chemin d'accès complet au fichier httpd.conf dans le répertoire d'installation du serveur Web.

2) Entrez le numéro associé à l'option requise pour modifier les paramètres respectifs. Reportez-vous aux options affichées à l'écran pour vous déplacer. Entrez *N* pour continuer.

c. Si le programme d'installation détecte IBM WebSphere Application Server sur votre système, le panneau suivant, accessible à l'aide de l'onglet Application Server, vous invite à configurer le servlet de configuration Host On-Demand dans WebSphere Application Server. Si les utilisateurs exécutent Host On-Demand via un pare-feu, cela vous dispense d'ouvrir un port supplémentaire pour les communications entre le client et le gestionnaire de services Host On-Demand. Voir «Installation du servlet de configuration», à la page 61 pour plus d'informations.

- Si vous entrez le numéro ou la lettre qui apparaît à gauche de la question, IBM Installation Manager affiche une liste des versions des serveurs d'applications, leurs profils et les serveurs détectés. Les utilisateurs sont alors invités à effectuer une sélection. Le programme d'installation déploie automatiquement le servlet de configuration sur le serveur d'applications que vous désignez, puis configure vos clients de sorte qu'ils accèdent au gestionnaire de services par le biais de ce servlet.
- Si vous poursuivez sans choisir de configurer le servlet, le programme d'installation ne configure pas le servlet de configuration. Les clients peuvent directement accéder au gestionnaire de services sur le *port 8999* (ou sur un autre port que vous avez spécifié).

Remarque :

- Websphere Application Server est détecté s'il a été installé par le même programme IBM Installation Manager sur le système. Les versions pouvant être détectées sont

Websphere Application Server version 8.0 et Websphere Application Server version 8.5.

- La configuration de servlet lors de l'installation n'est pas prise en charge pour un serveur sur lequel la sécurité administrative est activée.

15. Le panneau suivant est le panneau récapitulatif. Passez en revue vos sélections avant de poursuivre l'installation.
16. Pour générer un fichier de réponses d'installation, entrez *G:*.
17. Entrez le nom du fichier de réponses et utilisez l'extension *.xml*, les fichiers de réponses étant des fichiers XML.
18. Lorsque vous entrez le nom du fichier de réponses, indiquez un emplacement de répertoire si vous souhaitez sauvegarder le fichier à un autre emplacement.
19. Entrez *I* pour démarrer l'installation.
20. Lorsque l'installation est terminée, entrez *F:*.
21. Entrez X pour quitter Installation Manager.

Installation de l'assistant de déploiement en mode console

L'assistant de déploiement est automatiquement installé comme composant de l'installation du serveur Host On-Demand sous Windows. Ce produit est également disponible séparément pour les clients qui ne souhaitent pas installer l'intégralité du serveur Host On-Demand sous Windows. Les utilisateurs ont la possibilité de ne sélectionner que l'option Assistant de déploiement pendant l'installation.

Pour plus d'informations, reportez-vous à «Installation en mode console», à la page 54.

Installation de Host Access Toolkit en mode console

Host Access Toolkit est installé automatiquement dans le cadre de l'installation du serveur Host On-Demand sous Windows. Ce produit est également disponible séparément pour les clients qui ne souhaitent pas installer l'intégralité du serveur Host On-Demand sous Windows. Les utilisateurs ont la possibilité de ne sélectionner que l'option Host Access Toolkit pendant l'installation.

Pour plus d'informations, reportez-vous à «Installation en mode console», à la page 54.

Installation en mode silencieux

L'installation de Host On-Demand en mode silencieux vous permet d'utiliser un script d'installation. Vous devez d'abord créer un fichier de réponses avant de lancer Installation Manager à l'aide du fichier de réponses.

Pour plus d'informations sur l'installation de packages en mode silencieux à l'aide d'Installation Manager version 1.8.3, reportez-vous aux rubriques suivantes dans le centre de documentation d'Installation Manager :

- Feuilles de route pour l'installation en mode silencieux
- Arguments de ligne de commande d'Installation Manager pour le mode silencieux

Procédure d'installation

Cette section contient des instructions d'installation de Host On-Demand en mode silencieux.

Pour installer Host On-Demand en mode silencieux, effectuez les tâches suivantes :

1. Pour créer un fichier de réponses, enregistrez un fichier de réponses en utilisant IBM Installation Manager en mode assistant sur une machine où l'interface graphique est disponible, à l'aide de l'option *-record*. Pour obtenir des détails, reportez-vous à Enregistrement d'un fichier de réponses avec Installation Manager. Par exemple, sous Windows, l'enregistrement d'un fichier de réponses se présente comme suit :

   ```
   C:\Program Files (x86)\IBM\Installation Manager\eclipse>IBMIM.exe -record e:\recordResponse.xml
   ```

2. Si nécessaire, ouvrez le fichier XML généré pour afficher et éditer des préférences. Pour obtenir des détails sur le fichier, reportez-vous à Commandes de fichier de réponses d'Installation Manager en mode silencieux.
3. Pour effectuer une installation en mode silencieux à l'aide du fichier de réponses généré, utilisez l'utilitaire de ligne de commande *imcl* fourni par IBM Installation Manager. Des exemples sur différents systèmes d'exploitation sont indiqués ci-dessous :
   - Windows :

     ```
     imcl.exe input fichier_réponses -log fichier_journal
     ```

   - Linux, UNIX, IBM i, IBM z/OS et OS X

   ```
   ./imcl input fichier_réponses -log fichier_journal
   ```

   Pour obtenir des détails, reportez-vous à Installation d'un package en mode silencieux avec un fichier de réponses.

Remarque :

- Il vaux mieux éviter d'utiliser le paramètre *–skipInstall* lors de l'enregistrement d'un fichier de réponses pour l'installation Host On-Demand.
- Si un serveur Web, un serveur d'applications, ou les deux, sont configurés par Host On-Demand pendant l'installation en mode silencieux, vous devez enregistrer le fichier de réponses dans une configuration logicielle de sorte que les préférences utilisateur et les paramètres logiciels soient enregistrés dans le fichier de réponses. Par exemple, si un serveur HTTP version 8.5 doit être configuré, il est recommandé que les paramètres suivants correspondent pour obtenir de meilleurs résultats :
  - La version du serveur HTTP
  - Le chemin de l'emplacement d'installation du serveur HTTP
  - Le chemin de l'emplacement du fichier httpd.conf dans le serveur HTTP

  De la même façon, pour une installation en mode silencieux dans un environnement où réside Websphere Application Server, enregistrez le fichier de réponses sur un système où une installation similaire de Websphere Application Server est disponible.

  Si un fichier de réponses est enregistré dans un environnement où Websphere Application Server n'est pas installé, utilisez-le dans des environnements où Websphere Application Server n'est pas installé.
- Il est recommandé et utile d'avoir des fichiers de réponses distincts qui correspondent aux différents scénarios de déploiement.

- Vous devez enregistrer le fichier de réponses sur la même plateforme de système d'exploitation que celle sur laquelle Host On-demand doit être installé. Par exemple, pour effectuer une installation en mode silencieux sous Linux, enregistrez le fichier de réponses sous Linux. Il est utile d'avoir des fichiers de réponses distincts pour les différents systèmes d'exploitation.
- Les prérequis d'installation en mode console ou interface graphique utilisateur (s'ils sont applicables) sont également pertinents pour l'installation en mode silencieux. La liste devrait comprendre, sans s'y limiter, les prérequis suivants :
  - L'utilisateur connecté doit disposer de privilèges administrateur.
  - Installation Manager doit avoir été installé en mode administrateur.
  - Installation Manager version 1.8.3 ou ultérieure doit avoir été installé pour que l'installation de Host On-Demand soit possible. Si la sécurité administrative est activée sur Websphere Application Server, la configuration du servlet de configuration de Host On-demand n'est pas prise en charge pendant l'installation. Vous devez effectuer cette opération manuellement.

Installation du servlet de configuration

Lorsque vous installez Host On-Demand, vous pouvez choisir d'installer et de configurer le servlet de configuration sous i/OS, OS/400, Windows, AIX, Linux et Solaris for IBM Application Server.

Tous les moteurs de servlet et les serveurs Web se configurent différemment. Pour obtenir des informations sur le servlet de configuration (en fonction du système d'exploitation), reportez-vous à la documentation du moteur de servlet et du serveur Web.

L'installation du servlet de configuration n'est nécessaire que si les deux conditions suivantes sont vérifiées pour le déploiement de Host On-Demand :

- Lorsque vous envisagez de configurer Host On-Demand de sorte que les communications entre le client et le gestionnaire de services soient nécessaires (comme dans les modèles de déploiement basés sur le serveur de configuration et le modèle combiné, si vous activez la fonction de comptage des licences utilisées ou que vous activez l'Agent de réacheminement).
- Lorsqu'un pare-feu protège le ou les serveurs sur lesquels vous souhaitez maintenir les informations de configuration des sessions et que vous ne souhaitez pas ouvrir de port sur le pare-feu, afin d'éviter que des clients externes n'accèdent au gestionnaire de services.

Par défaut, les clients de Host On-Demand utilisent le port 8999 pour accéder aux informations de configuration à partir du gestionnaire de services. Si l'un de vos clients se situe derrière un pare-feu, le port 8999 doit être ouvert par l'administrateur du pare-feu au niveau interne et externe. Toutefois, vous pouvez éviter d'ouvrir ce port en personnalisant vos clients de sorte qu'ils utilisent le servlet de configuration pour accéder aux informations de configuration.

Déploiement du servlet sur WebSphere Application Server

Lors de l'installation de Host On-Demand sous Windows, AIX, Linux et Solaris, l'utilitaire d'installation recherche les instances de WebSphere Application Server.

S'il en détecte une, l'utilitaire d'installation peut automatiquement installer et configurer le servlet de configuration sur WebSphere Application Server versions 5.1, 6.0, 6.1 et 7.0.

Pour les plateformes qui fournissent une programme d'installation telles que System z et d'autres, vous devrez installer manuellement le servlet de configuration. Référez-vous à la documentation de WebSphere Application Server pour connaître la procédure d'installation des applications d'entreprise. Vous pouvez également accéder à l'adresse suivante : `http://www.ibm.com/software/webservers/` et naviguer vers la page de support WebSphere Application Server, où vous trouverez un lien d'accès à la documentation de votre version.

Le fichier du servlet de configuration de Host On-Demand, cfgservlet.ear, est situé dans le répertoire "lib" de l'installation Host On-Demand.

Pour WebSphere Application Server 5 : après avoir sauvegardé les paramètres de déploiement dans la console administrative, vous devez démarrer le servlet de configuration de Host On-Demand dans la fenêtre Applications d'entreprise de WebSphere Application Server. Ouvrez ensuite la fenêtre Environnement et sélectionnez l'option de mise à niveau du plug-in de serveur Web.

Une fois le servlet de configuration installé, vous devez configurer les clients pour qu'ils utilisent ce servlet au lieu d'accéder directement au gestionnaire de service. Vous pouvez utiliser l'assistant de déploiement pour créer des pages HTML personnalisées pour les clients. Cet assistant définit les paramètres de l'applet dans le fichier HTML créé, en fonction des données que vous lui fournissez, de sorte qu'il n'est pas nécessaire que vous connaissiez la syntaxe et les valeurs de paramètres admises. IBM recommande d'utiliser l'assistant de déploiement pour attribuer au paramètre ConfigServerURL du fichier HTML client le nom `HODConfig/HODConfig/hod`.

Pour plus d'informations, reportez-vous à Configuring the configuration servlet dans l'aide en ligne.

Chapitre 7. Désinstallation du serveur Host On-Demand

Vous pouvez désinstaller Host On-Demand Version 13 à l'aide de l'interface graphique d'Installation Manager. Pour ce faire, suivez les étapes ci-dessous :

1. Arrêtez toutes les applications de Host On-Demand associées (par exemple, l'assistant de déploiement et le gestionnaire de services IBM Host On-Demand).
2. Démarrez Installation Manager. Cliquez sur **Désinstaller**.
3. Sélectionnez IBM® Host On-Demand et la version appropriée, puis cliquez sur **Suivant**.
4. Vérifiez les informations récapitulatives, puis cliquez sur **Désinstaller**.
   - Si la désinstallation aboutit, un message de réussite s'affiche.
   - Si la désinstallation échoue, cliquez sur **Afficher le journal** pour identifier et résoudre le problème.
5. Cliquez sur **Terminer**.
6. Cliquez sur **Fichier** > **Quitter** pour fermer Installation Manager.

Désinstallation de Host On-Demand à l'aide du mode console d'Installation Manager

Vous pouvez désinstaller des packages en mode console. Pour effectuer la désinstallation, l'utilisateur doit être l'administrateur ou s'être connecté avec le privilège d'administrateur.

Pour désinstaller HOD à l'aide du mode console d'Installation Manager, effectuez les tâches suivantes :

1. Fermez tous les programmes qui sont associés à l'installation de Host On Demand, par exemple, l'assistant de déploiement et le gestionnaire de services IBM Host On-Demand.
2. Entrez la commande

   ```
   : imcl -c
   ```

   et appuyez sur la touche **Entrée**.
3. Entrez *5* pour continuer la désinstallation.
4. Entrez le numéro qui apparaît à gauche du groupe de packages Host On Demand 13.0. Appuyez sur la touche **Entrée**.
5. Vérifiez les détails du groupe de packages Host On Demand 13.0 à désinstaller. Entrez *N* pour *Suivant* ou appuyez sur la touche **Entrée**. *N* est la sélection par défaut.
6. Sélectionnez le package Host On-Demand en entrant le numéro qui apparaît à gauche du package Host On-Demand 13.0. Appuyez sur la touche **Entrée**. Entrez *N* pour *Suivant*.
7. Confirmez le package à désinstaller. Entrez *U* pour *Désinstaller* et appuyez sur la touche **Entrée**. Ce panneau offre également une option pour créer un fichier de réponses. Entrez *G* et appuyez sur la touche **Entrée** pour continuer la création d'un fichier de réponses. La désinstallation démarre.
8. A l'invite suivante, appuyez sur *F* pour *Terminer*.

Partie 3. Configuration de Host On-Demand

Chapitre 8. Configuration des clients d'émulation de Host On-Demand

Après avoir installé Host On-Demand, vous devez créer des fichiers HTML et configurer des sessions Host On-Demand pour les utilisateurs.

Host On-Demand fournit un échantillon de fichier HTML contenant des sessions d'émulation prêtes-à-l'emploi 3270, 5250, VT et FTP pré-configurées ainsi qu'un client téléchargé et des composants d'auto-détection Java. Ces sessions utilisent le modèle de configuration HTML ; elles sont fournies afin d'activer et d'exécuter Host On-Demand et d'accéder aux systèmes hôte rapidement. Pour utiliser ces sessions d'émulation, appliquez la procédure suivante :

1. Recherchez le fichier hodclients.zip dans le répertoire *votre_répertoire_de_diffusion* \samples\html, où *votre_répertoire_de_diffusion* désigne le nom du répertoire de diffusion Host On-Demand.
2. Vérifiez que le fichier hodclients.zip créé par l'assistant de déploiement se trouve dans le répertoire dans lequel vous souhaitez décompresser les fichiers (dans le répertoire de diffusion de Host On-Demand ou dans un répertoire de diffusion spécifique). Dans le cas contraire, copiez le fichier .zip dans ce répertoire.
3. Utilisez l'outil DWunzip pour décompresser le contenu du fichier hodclients.zip dans le répertoire de diffusion. Pour plus d'informations sur l'utilisation de cet outil, reportez-vous à Utilisation de DWunzip.
4. Utilisez votre navigateur pour pointer sur le fichier hodclients.html qui se trouve sur le serveur Web, par exemple, `http://host/alias/hodclients.html`.
5. Cliquez à l'aide du bouton droit de la souris sur l'icône de session appropriée, puis sélectionnez Propriétés pour ouvrir les propriétés de session. Indiquez l'adresse de destination, le port et les autres propriétés de connexion correspondant à votre système hôte. Cliquez sur OK.
6. Cliquez deux fois sur l'icône de session pour démarrer la session.

Vous pouvez utiliser l'assistant de déploiement pour personnaliser le fichier HTML. Pour plus d'informations, reportez-vous à «Utilisation de l'assistant de déploiement», à la page 69.

Création de fichiers HTML pour Host On-Demand

L'utilisation de l'assistant de déploiement constitue la meilleure façon de créer et de définir des fichiers HTML pour Host On-Demand. Il permet de créer aisément des fichiers HTML personnalisés contenant toutes les fonctions de Host On-Demand adaptées à votre environnement. La liste ci-dessous répertorie certaines des nombreuses fonctions qu'il est possible de configurer à l'aide de l'assistant de déploiement :

- **Modèles de configuration**. Les modèles de configuration définissent l'approche de haut niveau que vous souhaitez suivre en ce qui concerne l'endroit où vous avez défini vos sessions et où se trouvent les préférences utilisateur. Pour plus d'informations relatives aux modèles de configuration, reportez-vous à Chapitre 2, «Planification du déploiement», à la page 11.
- **Préchargements**. Host On-Demand s'exécute comme une applet ou une application et doit télécharger le code sur la machine de l'utilisateur. Par défaut, le client Host On-Demand télécharge tous les composants, mais vous pouvez réduire la taille du téléchargement en supprimant les composants inutiles.

- **Client en cache, client Web Start ou client téléchargé**. Les clients en cache conservent le code fourni lors du premier accès des utilisateurs aux pages HTML, et le stockent sur les machines des utilisateurs. Le client Web Start place en mémoire cache le code client en tant que "client en cache", mais permet également d'exécuter Host On-Demand sans navigateur. Les clients téléchargés procèdent eux-mêmes au téléchargement des fichiers d'applet nécessaires, chaque fois que l'utilisateur accède aux fichiers HTML.
- **Présentation de la page Web (modèles HTML personnalisés)**. Vous pouvez aisément définir un modèle que l'assistant de déploiement va utiliser afin de générer vos fichiers HTML. Cette fonction facilite l'ajout de vos propres arrière-plans, bannières, etc.
- **Options des clients en cache/Web Start**. Lorsque vous lancez le client en cache ou le client Web Start, le code doit être mis à niveau dès la mise à disposition de nouvelles versions du client. Un certain nombre d'options de l'assistant de déploiement permettent de contrôler les mises à niveau.
- **Emplacement de l'installation de Host On-Demand (base de code)**. D'une manière générale, les fichiers de l'assistant de déploiement se trouvent dans le répertoire de diffusion du serveur Host On-Demand. Cependant, il peut parfois s'avérer utile de placer ces fichiers à un emplacement indépendant du serveur Host On-Demand, de sorte que ceux-ci puissent profiter de différents contrôles de sécurité ou faciliter la mise à niveau du serveur Host On-Demand, par exemple.
- **WebSphere Portal**. WebSphere Portal offre une architecture permettant l'insertion d'extensions de contenu connues sous le nom de portlets dans un site Web. Les portlets sont des applications permettant d'organiser le contenu issu de différentes sources et de l'afficher sous forme de fichier HTML unique dans une fenêtre de navigateur. Les fichiers HTML utilisés pour lancer des sessions Host On-Demand peuvent être déployés sous forme de portlets, afin que les utilisateurs puissent accéder à Host On-Demand par l'intermédiaire d'une interface de portail.
- **Connexion au domaine Windows**. Si vos utilisateurs sont connectés à un domaine Windows, cette option les connecte automatiquement à Host On-Demand sous leur nom d'utilisateur Windows. Cette option est disponible uniquement lorsque vous utilisez le modèle de type serveur de configuration de l'assistant de déploiement.
- **API du gestionnaire de sessions**. Le gestionnaire de sessions de Host On-Demand offre des API JavaScript permettant de gérer des sessions hôte et des interactions textuelles avec les sessions hôte. Ces API permettent la prise en charge des sessions hôte imbriquées dans une page Web à l'aide de JavaScript et peuvent être activées à l'aide de l'assistant de déploiement.

Pour utiliser le client Web Start, vous devez faire appel à l'assistant de déploiement. Aucun fichier prédéfini n'est fourni pour ce type de client.

Configuration de sessions Host On-Demand

Outre la définition de fichiers HTML, vous devez définir des sessions pour les utilisateurs. Si vous utilisez le modèle de type HTML, vous configurez vos sessions dans l'assistant de déploiement et créez en même temps les fichiers HTML. Sinon, si vous faites appel au modèle de type serveur de configuration ou au modèle combiné, ou à l'un des clients prédéfinis, vous devez créer des groupes, des utilisateurs et des sessions dans le serveur de configuration à l'aide de l'un des clients d'administration.

Un large éventail d'options est à votre disposition lorsque vous configurez des sessions, que vous utilisiez l'assistant de déploiement ou l'un des clients d'administration :

- **Propriétés de session**. Toutes les propriétés de session peuvent être configurées, y compris les informations de connexion, de sécurité, etc. Chacune des zones peut être verrouillée pour éviter que les utilisateurs ne les mettent à jour.
- **Options d'exécution**. Lorsque vous configurez une session, vous pouvez lancer la session et configurer des options telles que la taille et l'emplacement, les couleurs, la personnalisation de la barre d'outils et les macros. Vous pouvez configurer les options d'exécution dans l'assistant de déploiement et dans le Client d'administration complet.
- **Désactivation des fonctions utilisateur**. Vous pouvez désactiver presque toutes les fonctions dont dispose normalement l'utilisateur avec la session Host On-Demand (la définition de signets, la création ou l'exécution de macros, par exemple).

Utilisation de l'assistant de déploiement

L'assistant de déploiement s'exécute sur les plateformes Windows et d Linux. Pour le démarrer, procédez de l'une des manières suivantes :

- Si vous avez installé automatiquement l'assistant de déploiement en tant que composant du serveur Windows Host On-Demand, sélectionnez **Démarrer** > **Programmes** > **IBM Host On-Demand** > **Administration** > **Assistant de déploiement**.

La fenêtre Assistant de déploiement s'affiche.

L'assistant de déploiement vous guide au cours des étapes de configuration et fournit une aide détaillée pour les options. Lorsque la sélection des options est terminée, l'assistant de déploiement crée les fichiers HTML et d'assistance. Ces fichiers doivent être placés dans le serveur Host On-Demand, dans un répertoire connu de votre serveur Web ; d'une manière générale, ce répertoire se trouve dans le répertoire de diffusion du serveur Host On-Demand.

Distribution des sorties de l'assistant de déploiement au serveur Host On-Demand

Si le serveur Host On-Demand est installé sur une plateforme Windows ou IBM System i, vous pouvez écrire les fichiers de configuration et HTML de l'assistant de déploiement directement dans le répertoire de diffusion du serveur Host On-Demand. Sur l'écran final de l'assistant de déploiement, vous pouvez choisir l'emplacement où vous souhaitez écrire les fichiers générés. Vous pouvez sélectionner l'unité locale ou réseau à laquelle peut accéder la machine équipée de l'assistant de déploiement. Dans ce cas, vous allez diriger la sortie de l'assistant de déploiement vers un répertoire de diffusion du serveur Host On-Demand et indiquer le format de sortie *HTML*. En supposant que vous ayez déjà défini vos sessions, la page HTML est alors accessible par les utilisateurs.

Autrement, si l'assistant de déploiement ne peut pas écrire directement au serveur Host On-Demand, vous devez faire en sorte qu'il génère un fichier Zip pour le format de sortie. Il va alors créer un fichier Zip unique contenant tous les fichiers HTML ainsi que les fichiers d'assistance. Déplacez le fichier Zip vers le serveur Host On-Demand et utilisez DWunzip pour le décompresser dans le répertoire de diffusion souhaité. En supposant que vous ayez déjà défini vos sessions, la page HTML est alors accessible par les utilisateurs.

Chapitre 9. Utilisation des clients dédiés aux nouveaux utilisateurs et à l'administration de Host On-Demand

Host On-Demand offre plusieurs clients prédéfinis pour la gestion de Host On-Demand et la création de comptes utilisateurs. Avant d'accéder à un client d'émulation ou à un client Database On-Demand qui utilise le modèle de déploiement de type serveur de configuration ou mixte, vous devez ajouter des utilisateurs et leur configurer des sessions avec l'un des clients d'administration ou d'administration complets.

Chargement des clients d'administration et des clients nouveaux utilisateurs

Pour charger un client d'administration ou un client nouvel utilisateur, procédez de l'une des manières suivantes :

- Indiquez l'adresse URL complète du fichier HTML dans votre navigateur :

  `http://nom_serveur/alias_hod/nom_client.html`

  où *nom_serveur* est le nom d'hôte ou l'adresse IP du serveur Host On-Demand, *alias_hod* l'alias (ou le chemin d'accès) du répertoire de diffusion, et *nom_client* le nom du fichier HTML du client d'administration ou du client nouvel utilisateur. Par exemple, vous pouvez télécharger la version en cache du client d'administration à partir du serveur Web en indiquant une URL du type :

  `http://hôte.société.com/hod/HODAdminCached.html`

  Pour vous connecter pour la première fois en tant qu'administrateur après l'installation initiale :

  1. Entrez l'ID utilisateur par défaut : admin.
  2. Entrez le mot de passe par défaut : password.
  3. Cliquez sur Connexion.
- Chargez le fichier HODMain_*xx*.html (où *xx* est un suffixe de langue à deux lettres) dans votre navigateur pour afficher les liens vers tous les clients d'administration ou tous les clients nouveaux utilisateurs disponibles, ainsi que vers d'autres clients prédéfinis. HODMain_xx.html se trouve dans le répertoire de diffusion.

Clients d'administration

Les clients d'administration permettent d'effectuer les tâches suivantes pour les données stockées dans votre serveur de configuration :

- gestion des utilisateurs, des groupes et des sessions ;
- configuration et gestion de l'agent de réacheminement et lancement de la fonction de trace sur cette fonction ;
- configuration de Database On-Demand ;
- activation de la fonction de sécurité ;
- affichage des journaux contenant les enregistrements de trace et les messages ;
- désactivation des fonctions pour que les utilisateurs ne puissent pas les utiliser.

Les clients d'administration s'exécutent sur toutes les plateformes client Host On-Demand, sauf MacIntosh. Si vous créez des fichiers HTML dans l'assistant de

déploiement à l'aide du modèle de type serveur de configuration ou du modèle mixte, vous devez configurer des sessions sur le serveur de configuration à l'aide du client d'administration. Reportez-vous à la section Basic Configuration Steps de l'aide en ligne pour obtenir plus de détails sur la configuration du serveur de configuration Host On-Demand.

Host On-Demand offre les clients d'administration prédéfinis et les clients d'administration complets suivants :

Client d'administration (HODAdmin.html)
Charge la version téléchargée du client d'administration.

Client d'administration en cache (HODAdminCached.html)
Charge la version en cache du client d'administration. Ce client présente l'avantage de pouvoir être mis en cache dans le navigateur en même temps que le client en cache.

Pour associer le client d'administration en cache à un signet, vous devez créer manuellement ce dernier. Ce signet doit pointer sur le fichier HODAdminCached.html, de sorte que Host On-Demand puisse comparer la version en cache et la version du serveur. Host On-Demand peut alors déterminer si une version plus récente du client d'administration en cache est disponible sur le serveur et vous en informer.

Client d'administration en cache avec fonction d'identification des incidents (HODAdminCachedDebug.html)[1]
Charge le client d'administration dans un environnement en cache avec la fonction d'identification des incidents (connexion aux session et fonction de trace).

Client d'administration complet (HODAdminFull.html)[2]
Charge la version téléchargée du client d'administration complet. Le client d'administration complet offre la possibilité supplémentaire à l'administrateur de démarrer des sessions pour configurer des propriétés d'exécution. Toutefois, la taille du téléchargement du client d'administration complet est supérieure à celle du client d'administration.

Client d'administration complet en cache (HODAdminCachedFull.html)[2]
Charge la version en cache du client d'administration complet. A l'instar de la version en cache du client d'administration classique, ce client peut être mis en cache dans le navigateur en même temps que le client en cache.

Client d'administration complet avec fonction d'identification des incidents (HODAdminCachedDebugFull.html)[1, 2]
Charge la version en cache du client d'administration complet avec la fonction d'identification des incidents (consignation des informations relatives à la session et fonction de trace).

Remarques :

1. Utilisez la fonction d'identification des incidents uniquement lorsque vous contactez le Support pour résoudre un incident avec votre installation Host On-Demand.
2. Le client d'administration complet est le client d'administration avec la fonction Démarrage de session.
3. Si vous utilisez un navigateur compatible Java, vous devez supprimer le client d'administration en cache par le biais du panneau de configuration Java (Java Control Panel). Pour des instructions, reportez-vous à la rubrique Using the Java plug-in de l'aide en ligne.

Utilitaire d'annuaire

L'utilitaire d'annuaire est une application Java qui permet à l'administrateur de gérer les informations de configuration des utilisateurs, des groupes ou des sessions. Ces informations sont stockées dans le magasin de données Host On-Demand par défaut ou dans un répertoire LDAP. Cet utilitaire est utile uniquement dans un environnement utilisant le modèle de type serveur de configuration. L'utilitaire d'annuaire permet d'ajouter, de supprimer ou de mettre à jour un grand nombre d'utilisateurs, de groupes ou de sessions dans un environnement de traitement par lots et évite d'utiliser le client d'administration. Il lit un fichier ASCII XML contenant les actions suivantes à exécuter pour les utilisateurs, les groupes ou les sessions définies dans le serveur de configuration :

- Ajout, mise à jour et suppression de groupes
- Ajout, mise à jour et suppression d'utilisateurs à partir de groupes
- Ajout, mise à jour ou suppression de sessions à partir d'utilisateurs ou de groupes
- Obtention de la liste des utilisateurs et des groupes dans les fichiers de sortie provenant de recherches uniques
- Obtention de la liste des utilisateurs et des groupes dans des fichiers de sortie pouvant être réutilisées comme des entrées

Les recherches effectuées via les actions avec "list" sont soit basées sur l'utilisateur (renvoi d'informations spécifiques à l'utilisateur), soit basées sur des groupes (informations spécifiques à des groupes). Toutefois, les environnements LDAP prennent en charge uniquement les recherches basées sur les utilisateurs.

Pour obtenir de plus amples informations, reportez-vous à Using the Directory Utility de l'aide en ligne.

Clients nouveaux utilisateurs

Si l'administrateur a sélectionné l'option Permettre aux utilisateurs de créer des comptes dans la fenêtre Utilisateurs/Groupes, les utilisateurs peuvent utiliser les clients nouveaux utilisateurs prédéfinis pour créer des comptes. Pour plus d'informations sur ce client, reportez-vous à la rubrique Enabling users to create accounts de l'aide en ligne.

Les clients nouveaux utilisateurs suivants sont fournis avec Host On-Demand :

Client nouvel utilisateur (NewUser.html)
Charge la version téléchargée du client nouvel utilisateur.

Client nouvel utilisateur en cache (NewUserCached.html)
Charge le client nouvel utilisateur dans un environnement en cache.

Client nouvel utilisateur avec fonction d'identification des incidents (NewUserCachedDebug.html)[1]
Charge le client nouvel utilisateur dans un environnement en cache avec la fonction d'identification des incidents (connexion à la session et à la fonction de trace).

Remarque : Utilisez la fonction d'identification des incidents uniquement lorsque vous contactez le Support pour résoudre un incident avec votre installation Host On-Demand.

Chapitre 10. Utilisation des clients d'émulation de Host On-Demand

Le présent chapitre décrit les difficultés auxquelles vous êtes susceptible d'être confronté lors de la configuration et de l'utilisation des clients d'émulation de terminal Host On-Demand.

- La section «Chargement des clients d'émulation» explique comment accéder aux clients d'émulation Host On-Demand.
- La section «Sélection du client approprié», à la page 76 explique comment déterminer le client répondant le mieux à vos besoins.
- La section «Clients en cache», à la page 77 est consacrée au mode d'utilisation des clients en cache, notamment installation et suppression, déploiement sur Internet, prise en charge sous Windows et Mac OS X ou encore identification des incidents.
- La section «Client Web Start», à la page 85 explique comment utiliser le client Web Start (installation et suppression, configuration du navigateur Web, utilisation de Web Start par les utilisateurs Windows soumis à des restrictions d'accès, mise à niveau).
- La section «Clients téléchargés», à la page 90 explique comment utiliser les clients téléchargés (installation et chargement après le téléchargement d'un client en cache ou d'un client Web Start).
- La section «Clients d'émulation prédéfinis», à la page 90 décrit les clients d'émulation prédéfinis fournis avec Host On-Demand.
- La section «Réduction de la taille de téléchargement du client», à la page 91 présente les stratégies disponibles pour réduire la taille de téléchargement des clients.
- La section «Déploiement d'archives et classes Java fournies par l'utilisateur», à la page 92 explique comment déployer des archives et des fichiers de classe Java sur vos clients.

Chargement des clients d'émulation

Host On-Demand fournit un échantillon de fichier HTML contenant des sessions d'émulation prêtes-à-l'emploi 3270, 5250, VT et FTP pré-configurées ainsi qu'un client téléchargé et des composants d'auto-détection Java. Ces sessions utilisent le modèle de configuration HTML ; elles sont fournies afin d'activer et d'exécuter Host On-Demand et d'accéder aux systèmes hôte rapidement. Pour plus d'informations, reportez-vous à Chapitre 8, «Configuration des clients d'émulation de Host On-Demand», à la page 67.

Pour charger un client d'émulation Host On-Demand, l'utilisateur doit démarrer un navigateur Web et entrer, dans la zone Adresse, l'URL d'un fichier HTML de Host On-Demand. Le fichier HTML de Host On-Demand doit être, selon les cas :

- Un fichier HTML créé via l'assistant de déploiement.
- L'un des fichiers HTML génériques prédéfinis, fournis avec Host On-Demand

IBM recommande d'adopter la première option. Pour plus d'informations sur l'assistant de déploiement, reportez-vous à Deployment Wizard de l'aide en ligne. Pour plus d'informations sur les fichiers HTML génériques prédéfinis, reportez-vous à «Clients d'émulation prédéfinis», à la page 90.

Si votre client d'émulation est déployé à l'aide du modèle de type serveur de configuration ou du modèle combiné, vous devez ajouter des utilisateurs et configurer des sessions avec le client d'administration avant d'utiliser le client d'émulation.

Pour lancer le fichier HTML généré par l'assistant de déploiement, indiquez l'adresse URL complète du fichier HTML dans votre navigateur :

`http://nom_serveur/alias_hod/nom_client.html`

où *nom_serveur* est le nom d'hôte ou l'adresse IP du serveur Host On-Demand, *alias_hod* l'alias (ou le chemin d'accès) du répertoire de diffusion, et *nom_client* le nom du fichier HTML du client. Par exemple, si vous avez créé un fichier HTML dans l'assistant de déploiement appelé 3270sessions.html, vous pouvez le charger en indiquant une URL comme :

`http://hôte.société.com/hod/3270sessions.html`

Pour lancer un fichier HTML prédéfini fourni avec Host On-Demand, pointez votre navigateur sur le fichier HODMain_*xx*.html, où *xx* est un suffixe de langue à deux lettres, pour afficher les liens vers tous les clients prédéfinis disponibles. HODMain_xx.html se trouve dans le répertoire de diffusion.

Lorsque vous accédez à un client, un avertissement relatif à la sécurité s'affiche pour vous informer que Host On-Demand a été créé par **International Business Machines**. Pour pouvoir disposer de privilèges de sécurité pour cette session ou pour toute session ultérieure, les utilisateurs doivent cliquer sur les boutons appropriés afin que Host On-Demand fonctionne correctement.

Remarque : Des logiciels de blocage d'incrustation peuvent empêcher les fenêtres de sécurité Java et d'autres fenêtres de réponse de s'afficher.

Sélection du client approprié

Les types de clients Host On-Demand que vous utilisez dépendent de votre environnement informatique et de vos préférences personnelles.

Les clients en cache et clients Web Start sont stockés en local et peuvent être chargés plus rapidement que les clients téléchargés (à moins qu'une version mise à jour du client soit en cours de téléchargement à partir du serveur Web). Vous pouvez également les utiliser via un réseau et des connexions à accès commuté. Les clients en cache et clients Web Start ont besoin de plus d'espace local que les clients téléchargés, mais sur la plupart des postes, cela n'est pas un problème.

Le client Web Start permet aux utilisateurs d'exécuter des sessions Host On-Demand sans nécessiter de navigateur. Les sessions Host On-Demand sont démarrées via le gestionnaire d'applications de Java Web Start. Si un utilisateur ferme le bureau Host On-Demand alors que des sessions sont en cours d'exécution, il est invité à confirmer la fermeture de toutes les sessions.

D'une manière générale, les clients téléchargés sont utilisés dans des environnements en réseau car les connexions réseau haut débit permettent de réduire le délai de téléchargement à partir du serveur Web. Il n'est pas conseillé de les utiliser via des connexions à accès commuté faible débit car ils doivent être téléchargés à chaque utilisation, ce qui rallonge le délai des connexions à accès

commuté. Le faible encombrement du disque des clients téléchargés est particulièrement adapté aux postes client dont l'espace disque local est insuffisant, comme les postes NetStation.

L'utilisation de clients en cache, Web Start et téléchargés est possible au sein du même environnement Host On-Demand. Pour connaître les instructions de retrait des clients en cache, reportez-vous à la rubrique «Désinstallation du client en cache», à la page 81.

Si vous prévoyez d'utiliser le client Web Start, vous devez générer le fichier HTML à l'aide de l'assistant de déploiement. Que vous décidiez d'utiliser des clients téléchargés ou des clients en cache, IBM recommande de créer vos propres clients à l'aide de l'assistant de déploiement au lieu d'utiliser l'un des clients prédéfinis. Pour plus d'informations, reportez-vous à la section «Réduction de la taille de téléchargement du client», à la page 91.

Clients en cache

Un client en cache Host On-Demand correspond à n'importe quel client Host On-Demand dont les composants ont été placés en mémoire cache, c'est-à-dire stockés localement pour permettre d'y accéder rapidement, sur le disque dur du poste de travail d'un utilisateur. Lorsqu'un utilisateur exécute pour la première fois un client en cache, le code d'initialisation de Host On-Demand télécharge les composants du client Host On-Demand et les enregistre sur le disque dur du poste de travail de l'utilisateur. Cette procédure s'appelle l'installation du client en cache.

Lorsque l'utilisateur exécute ensuite le client en cache, le code d'initialisation de Host On-Demand télécharge une petite applet de démarrage depuis le serveur. Cette applet démarre à son tour le client Host On-Demand à partir des composants en cache placés sur le disque dur.

En lançant le client en cache, l'utilisateur évite d'attendre le téléchargement des composants du client Host On-Demand, puisque ceux-ci sont déjà immédiatement disponibles sur le disque dur du poste de travail. En outre, le client en cache demeure identique même si le système d'exploitation est réinitialisé plusieurs fois et que le navigateur est rechargé. Même si le client en cache était au départ recommandé pour les utilisateurs qui disposent d'un système de connexion lent, tel qu'un accès téléphonique, sur lequel le téléchargement d'une applet de grande taille prendrait beaucoup de temps, de nombreux utilisateurs accordent leur préférence au client en cache, y compris lorsqu'ils disposent de lignes à haut débit.

Comme tous les clients Host On-Demand, le démarrage du client en cache s'effectue (la première fois comme les suivantes) en indiquant l'URL d'un fichier HTML Host On-Demand dans la zone d'adresse d'un navigateur Web pris en charge. IBM vous recommande de créer votre propre fichier HTML à l'aide de l'assistant de déploiement. Vous pouvez cependant utiliser l'un des fichiers HTML génériques prédéfinis du client en cache, fournis avec Host On-Demand.

L'applet qui procède au démarrage du client en cache détermine également si la version de l'un des composants du client Host On-Demand situés sur le serveur Host On-Demand est plus récente que celle des composants téléchargés correspondants. Si tel est le cas, l'applet met à niveau le client en cache en le téléchargeant depuis le serveur le composant le plus récent et en le plaçant en mémoire cache avant le lancement du client.

L'utilisateur peut installer plusieurs types de clients en cache sur un même poste de travail. Par exemple, un client d'émulation en cache, un client Database On-Demand en cache et un client d'administration en cache peuvent être installés sur la même machine. En outre, avec la version Java de Host On-Demand, l'utilisateur peut installer deux versions du même client en cache : l'une avec la fonction de détermination des incidents, l'autre sans.

Installation des clients en cache

Vous pouvez installer un client en cache depuis le serveur Host On-Demand, ou depuis une unité de réseau local ou de DVD-ROM.

Informations installées pour le client en cache

Deux types d'informations sont enregistrées sur le poste de travail de l'utilisateur lors de l'installation d'un client en cache Java :

- Composants Host On-Demand

  Ces composants sont fournis sous forme de fichiers d'archive Java (JAR).
- Informations de contrôle

  Ces informations incluent des données telles que l'URL du serveur Host On-Demand et la version de chaque composant téléchargé.

Client en cache Java : Plusieurs versions du client en cache Java peuvent exister sur le poste de travail de l'utilisateur, car le code d'initialisation du client en cache Java enregistre les composants du client en cache dans un répertoire différent sur le disque dur du poste de travail, pour chaque serveur à partir duquel l'utilisateur a téléchargé un client en cache.

Dans le cas du client en cache Java, tous les composants du client téléchargés à partir d'un même serveur sont stockés dans le même répertoire du disque dur de l'utilisateur. Si par exemple l'utilisateur installe un client d'émulation Java et un client Java Database On-Demand à partir du même serveur, les fichiers de composants correspondant aux deux types de clients sont stockés dans le même répertoire.

Sur certains types de clients en cache Java, les composants du client sont stockés dans le *cache permanent ("sticky cache")* du plug-in Java. Ces composants correspondent aux mêmes types de clients en cache que ceux de la liste indiquée à l'emplacement suivant : «Limites du support», à la page 15.

Installation du client en cache à partir du serveur Host On-Demand

Pour installer le client en cache à partir d'un serveur Host On-Demand, procédez comme suit :

1. Indiquez l'URL complète du fichier HTML dans votre navigateur, comme décrit dans la section «Chargement des clients d'émulation», à la page 75.
2. Si vous souhaitez utiliser un client prédéfini, cliquez sur le lien du client en cache après avoir chargé http://*nom_serveur*/*alias_hod*/HODMain.html, où *nom_serveur* est le nom d'hôte ou l'adresse IP du serveur Host On-Demand et *alias_hod* l'alias (ou le chemin d'accès) du répertoire de diffusion.
3. L'installation du client en cache commence immédiatement. La progression de l'installation s'affiche dans une fenêtre. L'indicateur de progression du haut indique l'état du téléchargement des fichiers individuels, tandis que celle du dessous illustre la progression générale de l'installation.

La fenêtre de progression de l'installation ne s'affiche pas pour certains clients en cache de type Java. Il s'agit des mêmes types de clients en cache Java que ceux de la liste indiquée dans «Limites du support», à la page 15.

4. Une fois l'installation terminée, le code d'installation lance immédiatement le client en cache Java. L'utilisateur n'a pas besoin de relancer le navigateur.

Installation du client en cache à partir d'un réseau local ou d'un DVD

Il est désormais possible à plusieurs ou à tous les utilisateurs de procéder au téléchargement initial du client en cache à partir d'une unité de réseau local ou de DVD-ROM. Pour installer le client en cache, l'utilisateur n'a besoin d'avoir accès qu'une seule fois à l'unité de réseau local ou de DVD-ROM. Après l'installation, l'utilisateur se connecte normalement au serveur Host On-Demand.

Les avantages de cette méthode sont que les composants du client en cache sont installés sur le poste de travail de l'utilisateur plus rapidement que s'ils avaient dû être téléchargés du serveur Web. De plus, l'utilisateur ne place pas de charge supplémentaire sur le serveur Web grâce au téléchargement d'un ensemble complet de composants client en cache.

Cette méthode est prise en charge sur la plupart des plateformes client. Cependant, il existe plusieurs clients en cache Java qui ne supportent pas cette fonctionnalité. Les clients en cache Java qui ne prennent pas en charge cette fonctionnalité sont indiqués dans «Limites du support», à la page 15.

Restrictions : Il n'est pas permis de spécifier un répertoire de publication utilisateur distinct par le biais du fichier HTML (si vous avez défini une base de code dans l'assistant de déploiement, le fichier HTML ne peut pas être utilisé pour installer le client en cache à partir d'une unité de réseau local ou de DVD-ROM). Pour plus d'informations sur la création d'un répertoire de publication séparé, reportez-vous à l'aide en ligne.

Procédure de création d'une image sur DVD ou réseau local par l'administrateur :

1. Utilisez la fenêtre Nom de fichier et Format de sortie de l'assistant de déploiement pour créer des fichiers *.html personnalisés (par exemple, MyHOD.html). Si vous devez distribuer les fichiers de l'assistant de déploiement vers un autre serveur, vous pouvez sélectionner l'option de sortie .zip pour utiliser l'outil DWunzip. Pour plus d'informations, reportez-vous à Using DWunzip de l'aide en ligne.
2. Sur le client en cache Java, vous pouvez éviter à l'utilisateur de saisir le nom d'hôte du serveur Host On-Demand durant l'installation. Pour cela, spécifiez le paramètre HTML complémentaire WebServerHostname dans l'assistant de déploiement. Pour plus d'informations, reportez-vous à HTML parameters de l'aide en ligne.
3. Après avoir chargé les nouveaux fichiers de l'assistant de déploiement sur votre serveur, testez-les pour vous assurer qu'ils fonctionnent comme prévu.
4. Copiez ou chargez par FTP les fichiers suivants à partir du répertoire de diffusion de votre installation de serveur Host On-Demand sur une unité réseau ou un DVD-ROM (assurez-vous que vous placez la même version de Host On-Demand sur l'unité de DVD-ROM ou de réseau local que celle qui est présente sur le serveur Host On-Demand) :
   - MyHOD.html
   - MyHOD.jnlp (s'il existe)

- z_MyHOD.html (s'il existe)
- hoddetect*.html
- hodlogo.gif
- hodbkgnd.gif
- Installer.html
- Installer2.html
- *.jar
- *.properties
- *.js

5. Copiez les fichiers et répertoires suivants, en veillant à préserver la structure des répertoires :
   - msgs\cached_*.properties
   - HODData\MyHOD*.*

Si vous copiez ces fichiers à partir d'une installation z/OS sur une image de DVD, notez que vous devrez supprimer l'extension de fichier .ascii de tous les fichiers HTML, PROPERTIES, JS, JNLP et CSS au préalable. Par exemple, un fichier nommé *.properties.ascii devrait être copié sur le DVD sous la forme suivante : *properties.

Si vous installez le client en cache à partir d'un DVD, celui-ci doit être distribué avec les mêmes instructions que les Contrats de licence et la Réglementation sur l'importation et l'exportation car il contient la technologie de chiffrage.

Procédure à suivre par l'utilisateur : Une fois que l'administrateur a défini l'unité de réseau local ou de DVD-ROM, l'utilisateur doit exécuter la procédure suivante pour installer le client en cache.

1. Préparez la machine client pour l'installation en procédant comme suit :
   - Accédez à l'unité de réseau local ou de DVD-ROM.
   - Recherchez le nom et l'emplacement du fichier HTML, tel que `f:\myPath\MyHOD.html`, que l'administrateur a défini sur l'unité de réseau local ou de DVD-ROM (le nom et le contenu du fichier HTML est identique pour tous les utilisateurs. Ce fichier n'est donc pas réservé à un utilisateur unique).
   - *Pour le client en cache Java uniquement*, recherchez le nom d'hôte du serveur Host On-Demand auquel l'utilisateur se connectera après l'installation du client en cache. Si, par exemple, l'utilisateur se connecte au fichier `http://myHODServer/hod/MyHOD.html`, le nom d'hôte est `myHODServer`.

Sur le client en cache Java, l'administrateur système peut se dispenser de cette étape en ajoutant le paramètre HTML WebServerHostname au fichier HTML. Voir HTML parameters de l'aide en ligne.

2. Exécutez le fichier HTML :

   Entrez le chemin d'accès et le nom du fichier HTML dans la zone de saisie d'adresse du navigateur, par exemple sous la forme :

   `f:/mypath/MyHOD.html`
3. *Pour le client en cache Java uniquement*, indiquez, lorsque vous y êtes invité par le code d'installation, le nom d'hôte du serveur Host On-Demand auquel

l'utilisateur se connectera après l'installation du client en cache. Si, par exemple, l'utilisateur lance le fichier `http://myHODServer/hod/MyHOD.html`, le nom d'hôte est `myHODServer`.

Sur le client en cache Java, l'administrateur système peut se dispenser de cette étape en ajoutant le paramètre HTML WebServerHostname au fichier HTML. Voir HTML parameters de l'aide en ligne.

4. Attendez la fin de l'installation du client en cache Host On-Demand à partir de l'unité de réseau local ou de DVD-ROM.
5. Lorsque vous y êtes invité, redémarrez le navigateur et pointez-le vers le fichier HTML qui identifie le serveur Host On-Demand, tel que :

   ```
   http://myServer/hod/MyHOD.html
   ```

   Le nom du fichier HTML résidant sur le serveur Host On-Demand est le même que celui du fichier HTML présent sur l'unité de réseau local ou de DVD-ROM.

Une fois cette procédure terminée, le client en cache Host On-Demand démarre de la manière habituelle.

Désinstallation du client en cache

Le sections suivantes présentent une méthode de suppression universelle.

Avant de commencer

La suppression du client en cache implique l'effacement des informations enregistrées sur le disque dur de l'utilisateur au moment de l'installation du client en cache Java.

Un utilisateur exécutant la version Java du client en cache dispose d'une version séparée du client en cache pour chaque serveur Host On-Demand sur lequel un client en cache a été téléchargé. Pour plus d'informations, reportez-vous à «Informations installées pour le client en cache», à la page 78.

La suppression du client en cache Java enlève uniquement la version Java du client en cache téléchargée depuis le serveur auquel l'utilisateur accède lorsqu'il effectue la suppression. Par exemple, si l'utilisateur accède au serveur `http://myHODServerA/hod/HODRemove.html` pour supprimer le client en cache Java de son poste de travail, seul le client en cache Java téléchargé depuis le serveur `myHODServerA` est supprimé.

Enfin, dans le cas des clients Java, la suppression du client en cache supprime tous les types de clients en cache (émulation, Database On-Demand et administration) associés à cette installation.

La suppression du client en cache Java sur le poste de travail alors qu'une connexion au serveur `myHODServerA` est en cours entraîne la suppression des clients d'émulation, Database On-Demand et d'administration en cache précédemment téléchargés depuis le serveur `myHODServerA`. Toutefois, seul les composants du client en cache qui ont été téléchargés depuis ce serveur particulier sont supprimés. Les composants de client en cache issus d'autres serveurs, s'ils existent, ne sont pas supprimés, sauf si l'utilisateur se connecte à ce serveur pour y effectuer une suppression.

Suppression des clients en cache Java

La méthode de suppression universelle supprime le client en cache Java. Procédez comme suit :

1. Démarrez votre navigateur.

   Démarrez un navigateur compatible Java pour supprimer un client en cache Java.
2. Connectez-vous au fichier HODMain.html sur le serveur Host On-Demand. Connectez-vous par exemple à l'URL suivante :

   `http://myServer/HOD/HODMain.html`

Si vous supprimez un client en cache Java, vous devez vous connecter au même serveur que celui à partir duquel vous avez installé le client en cache Java. Pour plus d'informations, reportez-vous à «Avant de commencer», à la page 81.

3. Cliquez sur l'entrée suivante sous l'option Utilitaires :

   `Suppression du client en cache`

Il existe une autre manière plus directe d'exécuter la méthode de suppression à usage général. Procédez comme suit :

1. Démarrez votre navigateur.
2. Connectez-vous au fichier HODRemove.html sur le serveur Host On-Demand. Connectez-vous par exemple à l'URL suivante :

   `http://myServer/HOD/HODRemove.html`

   Cette procédure supprime le client en cache.

Si vous supprimez un client en cache Java, vous devez vous connecter au même serveur que celui à partir duquel vous avez installé le client en cache Java. Pour plus d'informations, reportez-vous à «Avant de commencer», à la page 81.

Quelle que soit la méthode de suppression appliquée, vous serez invité à vider le cache du plug-in Java si vous avez supprimé les clients en cache Java suivants :

- Clients d'administration en cache
- Clients en cache sur plateforme Apple Mac OS X
- Clients d'émulation en cache avec API JavaScript Session Manager activée (Mozilla Java uniquement)

Une fenêtre vous demandant de vider le cache du plug-in Java s'affiche. Pour plus d'informations, reportez-vous à la rubrique Using the Java plug-in de l'aide en ligne.

Suppression d'un client en cache partagé par plusieurs utilisateurs

Si plusieurs utilisateurs partagent un même client en cache et que l'un de ces utilisateurs supprime ce dernier, la suppression affecte tous les utilisateurs. Pour plus d'informations sur le partage d'un client en cache unique, reportez-vous à «Prise en charge du client en cache pour Windows», à la page 83.

Problèmes liés à la prise en charge du client en cache lors de l'accès à plusieurs serveurs Host On-Demand

Les sections suivantes décrivent en détails les problèmes pouvant survenir lorsque les utilisateurs d'un client en cache accèdent à des serveurs Host On-Demand multiples.

Client en cache Java

Un client en cache Java installe une copie distincte du code du client pour chaque instance de serveur Host On-Demand visitée par l'utilisateur. L'accès aux serveurs selon différents niveaux de service ne pose donc aucune difficulté particulière. Avec certaines versions du plug-in, les utilisateurs peuvent accroître la taille de leur cache Java s'ils veulent accéder à plusieurs serveurs Host On-Demand.

Les incidents suivants peuvent se produire sur les clients en cache Java.

Problèmes liés à l'application de préférences stockées localement : Si vous utilisez des préférences stockées en local, les fichiers HTML personnalisés que vous créez doivent posséder des noms uniques pour votre société, car les noms de fichier HTML font la différence entre les préférences stockées en local de différents sites. L'utilisation de noms génériques peut entraîner des conflits de préférences pour les utilisateurs.

Pour plus d'informations, visitez le site Web de support Host On-Demand : Si vous rencontrez des difficultés lors de la gestion du déploiement de clients en cache sur Internet, visitez le site http://www.ibm.com/software/webservers/hostondemand/support.html pour plus d'informations.

Prise en charge du client en cache pour Windows

Sur une machine Windows multi-utilisateurs équipée du système d'exploitation Windows 7, Windows 8, Windows 10 ou Windows 2012, les utilisateurs peuvent télécharger leur propre version de client en cache :

- Tout navigateur pris en charge et équipé du plug-in Java

Si l'API JavaScript est activée, il n'est pas possible, pour des raisons techniques, de partager le client en cache entre des navigateurs Java Mozilla.

Vous pouvez, en variante, ajouter la configuration suivante en sélectionnant les paramètres HTML de la fenêtre Options avancées de l'assistant de déploiement :

- ShareCachedClient : permet aux utilisateurs de partager une seule instance du client en cache
- SharedCachedDirectory : vous permet de spécifier l'emplacement du répertoire d'installation du client en cache

Lorsque le client en cache est partagé, mais que vous n'indiquez aucun répertoire, le client en cache est installé dans le répertoire par défaut \Documents and Settings\All Users\IBMHOD. Si vous indiquez un répertoire, par exemple SharedCachedDirectory=c:\ibm, le client en cache Host On-Demand ajoute IBMHOD\HODCC à cette chaîne. Le client en cache est alors installé à ce nouvel emplacement, par exemple c:\ibm\IBMHOD\HODCC. Un administrateur ou un utilisateur avec pouvoir doit créer ce répertoire d'installation manuellement ou procéder à la première installation du client en cache partagé. Dans tous les cas, l'administrateur ou l'utilisateur avec pouvoir doit modifier les paramètres de sécurité de ce répertoire, de sorte que les utilisateurs disposant d'un accès restreint aient un accès en lecture, en modification et en écriture. L'administrateur peut également modifier les paramètres de sécurité puis télécharger le client en cache dans le répertoire, ou télécharger le client en cache partagé dans le répertoire, puis modifier les paramètres de sécurité. Si les paramètres de sécurité ne sont pas mis à jour et qu'un utilisateur disposant d'un accès restreint tente d'installer le client en cache partagé, ce dernier reçoit un message d'erreur lui signalant qu'il est probable qu'un incident soit survenu sur le système de fichiers et qu'il ne pourra pas utiliser ni mettre à jour le client en cache.

Lorsque l'administrateur ou l'utilisateur avec pouvoir a modifié les paramètres de sécurité, un utilisateur disposant d'un accès restreint peut ouvrir une session Windows et peut soit installer le client en cache partagé soit utiliser (ou mettre à jour) une version préalablement installée du client en cache partagé. D'autres utilisateurs disposant d'un accès restreint peuvent ouvrir une session Windows et utiliser le client en cache sans être obligés de le télécharger à nouveau depuis le serveur Host On-Demand. Le cas échéant, ils peuvent également mettre à niveau le client en cache partagé.

Si vous ne souhaitez pas que des utilisateurs disposant d'un accès restreint puissent partager le client en cache, une instance distincte du client en cache est téléchargée dans le répertoire utilisateur pour chacun de ces clients.

Si une version précédente du client en cache a été téléchargée par un administrateur ou un client avec pouvoir, et que vous souhaitez autoriser les utilisateurs disposant d'un accès restreint à y accéder, l'administrateur ou l'utilisateur avec pouvoir doit utiliser le fichier HODRemove.html pour retirer la précédente version du client en cache, puis modifier les paramètres de sécurité du répertoire du client en cache partagé pour accorder un accès en lecture, modification et écriture aux utilisateurs disposant d'un accès restreint, comme cela est décrit ci-dessus.

Pour connaître les informations sur la suppression du client en cache, reportez-vous à «Suppression d'un client en cache partagé par plusieurs utilisateurs», à la page 82.

Prise en charge du client en cache sur Mac OS X (clients Java uniquement)

Les clients en cache présentent les restrictions suivantes sur la plateforme Mac OS X :

- Le transfert des mises à jour de Host On-Demand est géré par serveur.
- Le préchargement de clients en cache à partir d'une unité de réseau local ou de DVD-ROM ne permet de prendre en charge aucune fonction. En effet, lorsque le navigateur est redirigé vers le véritable site Web, le plug-in considère qu'il s'agit d'un serveur Web distinct et que le client est de nouveau mis en cache.
- Host On-Demand s'exécute comme une applet et doit télécharger le code sur la machine de l'utilisateur. Le client Host On-Demand télécharge tous les composants, mais est susceptible de réduire la taille du téléchargement en déplaçant les composants inutiles. Sur Mac OS X, vous ne pouvez installer aucun composant supplémentaire après le téléchargement initial.
- Les fichiers Java Host On-Demand utilisés pour exécuter le client en cache Host On-Demand sur un navigateur Web compatible Java sont stockés dans le cache du JRE (Java Runtime Environment). Pour supprimer le client mis en cache sur Mac OS X, vous devez vider le cache JRE via le panneau de configuration de Java (Java Control Panel). Pour des instructions, reportez-vous à la rubrique Using the Java plug-in de l'aide en ligne.
- Lorsque vous lancez le client en cache, le code doit être mis à niveau dès la mise à disposition de nouvelles versions du client. Un certain nombres d'options de l'assistant de déploiement permettent de savoir à quel moment la mise à niveau a été réalisée. Ces options ne sont pas disponibles sur la plateforme Mac OS X.

Les améliorations apportées au client en cache Java ne concernent pas le client en cache Java pour Mac OS X. Pour plus d'informations, reportez-vous à «Limites du support», à la page 15.

Identification et résolution des incidents liés aux clients en cache

Si vous ne parvenez pas à charger le client en cache, consultez les suggestions suivantes pour identifier les incidents :

Microsoft Internet Explorer 11.0

Après avoir mis à niveau votre navigateur Microsoft Internet Explorer vers la version 11.0, vous pouvez recevoir des exceptions de sécurité sur la console Java. Lorsque vous installez le client en cache, plusieurs fichiers sont stockés dans la structure de répertoires du navigateur. Lorsque vous effectuez une mise à niveau d'Internet Explorer vers la version 11.0, le navigateur n'identifie plus les fichiers CAB qui contiennent le code en cache de Host On-Demand. Etant donné que le navigateur ne trouve pas les fichiers CAB, il tente d'utiliser les fichiers de classes directement depuis le serveur et provoque des exceptions de sécurité. Pour remédier à cet incident, il convient de mettre à niveau le navigateur, supprimer Host On-Demand à l'aide du fichier HODRemove.html, puis réinstaller le produit à l'aide du fichier HODCached.html.

Mozilla et Firefox

Avec Mozilla et Firefox, si rien ne se produit lorsque vous essayez d'installer le client en cache, ou en cas d'échec de la tentative d'installation du client en cache, vérifiez les paramètres du navigateur. Assurez-vous que la configuration de Mozilla et Firefox ne prévoit pas la suppression des fenêtres en incrustation qui apparaissent en haut ou en bas de la fenêtre du navigateur. Ce paramètre empêche en effet l'installation normale du client en cache Host On-Demand.

L'emplacement de ce paramètre dépend de la version de Mozilla :

- Dans Mozilla 1.2, ce paramètre figure sous l'option Edit > Preferences > Advanced > Scripts & Plugins.
- Dans Mozilla 1.3, ce paramètre figure sous l'option Edit > Preferences > Privacy & Security > Popup Windows.

Après l'installation du client en cache, vous pouvez restaurer ce paramètre en vue de supprimer les fenêtres en incrustation. Toutefois, si vous devez réinstaller entièrement le client en cache ou le mettre à jour vers une version plus récente en tâche d'avant-plan, vous devez de nouveau configurer Mozilla ou Firefox de sorte que les fenêtres en incrustation ne soient pas supprimées.

Le paramètre de suppression des fenêtres en incrustation n'empêche pas le téléchargement de composants supplémentaires non compris dans le téléchargement initial (liste de préchargement).

Client Web Start

Le client Web Start permet aux utilisateurs de démarrer Host On-Demand sans nécessiter de navigateur. Dans le cas du client Web Start, vous devez générer un fichier HTML à l'aide de l'assistant de déploiement. Le fichier HTML généré par l'assistant de déploiement pointe vers un fichier de protocole JNLP (Java Network Launch Protocol). Ce fichier JNLP définit une application Java, qui comprend les paramètres transmis à l'application et les archives contenant les fichiers .class utilisés par celle-ci. Le fichier JNLP et les archives associées sont stockés sur un serveur Web.

Lorsqu'un utilisateur pointe vers le fichier JNLP, le navigateur lance l'application Web Start sur le poste client. Il télécharge les archives associées, vérifie que le niveau minimal requis du JRE est présent (si ce paramètre est spécifié), enregistre les archives sur la machine de l'utilisateur, installe les icônes de l'application et enfin, lance cette dernière.

Les sessions Host On-Demand peuvent être démarrées via le gestionnaire d'applications de Java Web Start. Grâce au gestionnaire d'applications de Java Web Start, les sessions Host On-Demand ne reposent plus sur un navigateur. La fermeture du navigateur ne met donc plus fin aux sessions Host On-Demand. Si un utilisateur tente de fermer le bureau Host On-Demand alors que des sessions sont en cours d'exécution, il est invité à confirmer la fermeture de toutes les sessions. Dans pareil cas, les sessions sont refermées en toute sécurité, afin d'éviter tout incident dû à la fermeture brutale du navigateur alors que des sessions sont actives.

Après le lancement initial de l'application, vous pouvez, selon vos préférences, pointer de nouveau le navigateur Web sur le fichier JNLP ou cliquer sur les icônes créées sur le poste client. Après redémarrage de Web Start, le serveur Web est analysé en vue de détecter les mises à jour d'archives qui donnent lieu, le cas échéant, au téléchargement des fichiers correspondants.

Java Web Start est fourni en tant que composant intégré de JRE 1.4.0 ou versions ultérieures de Java Runtime Environment. Si vous utilisez la version JRE 1.3, il convient de procéder à la mise à niveau vers JRE 1.4. Pour plus d'informations sur Java Web Start, visitez le site http://www.javasoft.com. Host On-Demand Version 13 prend en charge Java 1.5 ou une version supérieure.

Le client Web Start de Host On-Demand nécessite l'observation des exigences suivantes :

- JRE 1.4 (ou une version supérieure) est requis pour accéder aux fichiers du serveur Web via le protocole HTTPS.
- JRE 1.4 (ou une version supérieure) est requis pour utiliser un Proxy HTTP avec le client Web Start.
- Les propriétés de session faisant appel aux paramètres de navigateur (serveur Proxy ou TLS) ne sont pas utilisables avec le client Web Start.

Installation du client Web Start

Le client Web Start peut être installé de deux façons. Généralement, les utilisateurs effectuent l'installation à partir d'un serveur Host On-Demand sur le réseau avec ou sans un navigateur Web. Ils peuvent également l'installer à partir d'une unité réseau ou d'un lecteur DVD, ce qui requiert une petite opération de téléchargement sur le réseau. Quel que soit le mode d'installation choisi, une fois que le client est installé sur le système et dans le gestionnaire d'applications Java Web Start, les utilisateurs peuvent le lancer en cliquant sur l'icône approprié dans le gestionnaire d'applications.

Installation du client Web Start à partir du serveur Host On-Demand

Les utilisateurs peuvent installer le client Web Start à partir du serveur Host On-Demand avec ou sans navigateur.

Utilisation d'un navigateur Web : Pour installer le client Web Start à l'aide d'un navigateur Web, les utilisateurs peuvent exécuter la procédure suivante :

1. Indiquez l'URL complète du fichier HTML dans votre navigateur, comme décrit dans la section «Chargement des clients d'émulation», à la page 75.

   L'installation du client Web Start commence immédiatement. La progression de l'installation s'affiche dans une fenêtre. L'indicateur de progression du haut indique l'état du téléchargement des fichiers individuels, tandis que celle du dessous illustre la progression générale de l'installation.
2. Une fois l'installation terminée, le code d'installation lance immédiatement le client Web Start. Vous n'avez pas besoin de redémarrer le navigateur.

Non-utilisation d'un navigateur Web : Pour les utilisateurs Windows, distribuez le fichier JNLP qui a été généré à partir de l'assistant de déploiement (par exemple, myhod.jnlp) pour les utilisateurs finals. Une fois que le fichier est distribué, les utilisateurs peuvent taper `start myhod.jnlp` pour démarrer l'application Web Start et commencer à installer le client Host On-Demand. Etant donné que l'extension de fichier '.jnlp' est enregistrée dans l'application Web Start, cette dernière démarre, lit le fichier et télécharge tous les fichiers archive appropriés à partir du serveur Host On-Demand qui a été spécifié dans le fichier JNLP généré par l'assistant de déploiement. Le client Web Start Host On-Demand redémarre lorsque le téléchargement est terminé.

Si vous n'avez pas distribué le fichier JNLP aux utilisateurs Windows ou si vos clients exécutent des plateformes autres que Windows, les utilisateurs peuvent toujours télécharger le client Web Start sans navigateur Web en démarrant directement le gestionnaire d'applications Java Web Start et en pointant sur le fichier JNLP qui se trouve sur le serveur Web.

Pour les clients Windows, les utilisateurs peuvent exécuter la procédure suivante :

1. Ouvrez le gestionnaire d'applications Java Web Start en cliquant deux fois sur fichier `javaws.exe`, qui se trouve généralement dans le répertoire `C:\Program Files\Java Web Start`.
2. Pointez sur le fichier JNLP sur le serveur Web à l'adresse suivante : `http://HODServer/HODAlias/myhod.jnlp` .

Pour les clients Linux, un utilisateur peut taper `/javaws http://HODServer/HODAlias/myhod.jnlp` pour installer et exécuter la session Host On-Demand. Une icône Host On-Demand s'affiche dans le gestionnaire d'applications de Java Web Start. Les utilisateurs peuvent cliquer deux fois sur cette icône pour lancer Host On-Demand.

Installation du client Web Start à partir d'un réseau local ou d'un DVD-ROM

Afin de réduire le trafic sur le réseau ainsi que le temps de téléchargement, certaines entreprises souhaitent installer pour leurs utilisateurs le client Web Start à partir du réseau local ou du DVD. Etant donné que le client Web Start et le client en cache partagent les mêmes archives en cache, les utilisateurs peuvent installer la majorité du client Web Start en utilisant la même procédure d'installation que le client en cache. Cependant, le client Web Start requiert un composant supplémentaire qui doit être installé directement à partir du serveur Host On-Demand sur le réseau.

L'installation du client Web Start implique deux étapes pour l'administrateur suivies de deux étapes pour l'utilisateur final.

Dans un premier temps, l'administrateur doit exécuter les deux étapes suivantes :

1. En appliquant la «Procédure de création d'une image sur DVD ou réseau local par l'administrateur», à la page 79, utilisez l'assistant de déploiement pour générer un fichier HTML de client en cache.
2. Utilisez cet assistant une seconde fois pour éditer le fichier HTML que vous avez créé lors de l'étape précédente, en remplaçant le type de client, client en cache en client Web Start. (Assurez-vous de ne pas effectuer d'autres modifications afin que les sessions définies et la liste des composants préchargés restent la même.) Cette seconde page HTML est celle que vous devriez diffuser pour que les utilisateurs puissent y accéder.

Dans un deuxième temps, une fois que vous avez diffusé votre fichier HTML, les utilisateurs doivent exécuter les deux étapes suivantes :

1. En appliquant la «Procédure à suivre par l'utilisateur», à la page 80, installez le client en cache que l'administrateur a installé à partir du réseau local ou du DVD.
2. Installez le composant complémentaire du client Web Start en suivant la procédure d'installation du client Web Start à partir du serveur Host On-Demand : «Utilisation d'un navigateur Web», à la page 86. Le code du client Web Start permet de déterminer si les fichiers archive Host On-Demand ont déjà été téléchargés afin d'éviter qu'ils ne soient de nouveau téléchargés. Le composant restant doit se télécharger rapidement et le client Web Start Host On-Demand redémarre.

Configuration du serveur Web pour l'utilisation du client Web Start

L'administrateur doit enregistrer l'extension JNLP en tant que type MIME sur le serveur Web, afin que le navigateur puisse lancer correctement l'application Web Start. Les sections suivantes décrivent par exemple les procédures de configuration d'Apache HTTP Server, IBM HTTP Server et Microsoft IIS.

Configuration d'Apache HTTP Server ou d'IBM HTTP Server

Pour configurer Apache HTTP Server ou IBM HTTP Server en vue d'utiliser le client Web Start, ajoutez la ligne suivante au fichier mime.types :

```
AddType Application/x-java-jnlp-file    .jnlp
```

Microsoft IIS 7.0

Pour configurer Microsoft IIS en vue d'utiliser le client Web Start, procédez comme suit :

1. Cliquez sur Panneau de configuration > Outils d'administration > Services Internet (IIS) et sélectionnez l'option Site Web par défaut.
2. Dans la page Propriétés, cliquez sur l'onglet En-têtes HTTP.
3. Sous l'option MIME, cliquez sur l'onglet Types de fichier et sélectionnez Nouveau type.
4. Dans la zone Extension, tapez `.jnlp`.
5. Dans la zone Type de contenu, tapez `application/x-java-jnlp-file`.
6. Cliquez sur OK.

Mise à niveau du client Web Start

Après l'installation initiale du client Web Start, si les utilisateurs pointent leurs navigateurs sur le fichier HTML généré par l'assistant de déploiement et que les mises à jour sont disponibles sur le serveur Host On-Demand, Host On-Demand invite les utilisateurs à effectuer la mise à jour requise. Si les utilisateurs acceptent d'effectuer la mise à jour, Java Web Start télécharge la mise à jour des fichiers

archive et lance Host On-Demand. Si les utilisateurs refusent d'effectuer la mise à jour, Host On-Demand les réinvitera à le faire la prochaine fois qu'ils lancent le fichier HTML.

Ajout de composants Web Start après l'installation initiale

Si les utilisateurs appellent une fonction qui n'est pas installée sur le client Java Web Start, Host On-Demand les invite à procéder à l'installation des composants additionnels requis par cette fonction. S'ils choisissent d'installer les composants supplémentaires, les utilisateurs doivent redémarrer le client Host On-Demand pour pouvoir les utiliser.

Utilisateurs Web Start et Windows soumis à des restrictions

Les utilisateurs Windows soumis à des restrictions qui exploitent Java Web Start 1.0.1 doivent supprimer l'environnement JRE et Java Web Start, puis réinstaller une version plus récente de JRE équipée de Java Web Start 1.2.

Création de signets pour les sessions utilisant Web Start

Etant donné que l'exécution du client Web Start a lieu en dehors d'un navigateur, la création de signets (fonction dépendante du navigateur) est désactivée. Les administrateurs peuvent créer des clients Web Start apparaissant aux yeux des utilisateurs comme des sessions imbriquées désignées par un signet ; pour cela, ils doivent procéder comme suit :

1. Dans la fenêtre Options avancées de l'assistant de déploiement, ajoutez le paramètre HideHODDesktop positionné sur la valeur "true".
2. Configurez une session unique à démarrage automatique.
3. Configurez la session en vue de désactiver le démarrage dans une fenêtre distincte.

Utilisation du client Web Start avec le protocole HTTPS

Si vous souhaitez exploiter le client Web Start avec le protocole HTTPS, il convient que l'autorité de certification accréditant votre connexion HTTP sécurisée soit une autorité racine connue. Lorsque vous utilisez Host On-Demand en tant qu'applet avec une connexion HTTPS, vous pouvez, si les droits d'accès de niveau superutilisateur ne sont pas reconnus par le navigateur, valider le certificat utilisé pour la connexion HTTPS. Du fait que le client Java Web Start est exécuté en tant qu'application, cette fonctionnalité du navigateur n'est pas disponible. La machine virtuelle Java (JVM) utilisée par le client Java Web Start renferme un certain nombre de droits d'accès de niveau superutilisateur dignes de confiance. Si le certificat provenant de la connexion HTTPS dispose de droits d'accès de niveau superutilisateur affectés à l'une des autorités connues par JVM, l'établissement de la connexion sécurisée a lieu. Si vous souhaitez avoir recours à une autorité de certification autre que celles identifiées par défaut par la machine virtuelle Java (par exemple un certificat d'auto-signature), vous devez importer le certificat dans le magasin de clés de JVM pour chaque client qui accède à ce client Java Web Start. Cette condition est requise pour permettre l'établissement de la connexion HTTP sécurisée.

Suppression du client Web Start

Pour supprimer le client Web Start, suivez les deux procédures indiquées ci-dessous :

1. Dans le gestionnaire d'applications de Java Web Start, sélectionnez l'application souhaitée et cliquez sur Suppression.

2. Lancez la page HODRemove.html dans votre navigateur.

Clients téléchargés

Contrairement au client en cache et au client Web Start, le client téléchargé ne permet aucun contrôle de la méthode ni du moment où les composants du client sont téléchargés sur le disque dur du poste de travail de l'utilisateur. Le client téléchargé délègue au navigateur toutes les décisions relatives à l'utilisation de la mémoire cache.

N'utilisez le client téléchargé que lorsque vous remplissez les *deux* conditions obligatoires suivantes :

- Lorsque vous ne souhaitez pas occuper d'espace disque sur les postes client en installant le client en cache ou le client Web Start.
- Lorsque la durée du téléchargement ne pose aucun problème.

Démarrage du client téléchargé

Démarrez le client téléchargé en le téléchargeant à partir du serveur Host On-Demand vers la fenêtre de votre navigateur, comme décrit dans la section «Chargement des clients d'émulation», à la page 75.

Démarrage du client téléchargé après l'installation du client en cache ou du client Web Start

Java

Avec les clients Java, vous pouvez démarrer le client téléchargé après avoir installé le client en cache ou le client Web Start.

Clients d'émulation prédéfinis

Plusieurs fichiers HTML de client d'émulation prédéfini sont fournis avec Host On-Demand. Ils sont inclus afin de montrer l'éventail des fonctionnalités du client Host On-Demand et servir d'exemple pour la création de fichiers HTML personnalisés dans l'assistant de déploiement. Chacun d'eux utilise le modèle de type serveur de configuration. Pour charger l'un de ces clients, suivez les instructions de la section «Chargement des clients d'émulation», à la page 75.

D'une manière générale, il est conseillé de définir vos propres fichiers HTML personnalisés à l'aide de l'assistant de déploiement au lieu d'utiliser les fichiers HTML du client prédéfini.

Les fichiers HTML suivants du client d'émulation prédéfini sont fournis par Host On-Demand :

Client en cache (HODCached.html)
Fournit toutes les fonctions du client Host On-Demand.

Client en cache avec fonction d'identification des incidents (HODCachedDebug.html)[1]
Démarre le client en cache avec la fonction d'identification des incidents (consignation des informations relatives à la session et fonction de trace).

Client téléchargé (HOD.html)
Fournit toutes les fonctions du client Host On-Demand sauf celle d'identification des incidents.

Avec un navigateur compatible Java, le fichier HOD.html du client téléchargé prédéfini omet certains composants Host On-Demand qui ne sont pas fréquemment utilisés. Pour plus d'informations, ainsi que pour obtenir la liste des composants exclus, avec une description des solutions palliatives possibles, reportez-vous à «Certains composants ne sont pas inclus dans les fichiers HTML», à la page 16. L'accès à HOD.html avec un navigateur Java fonctionne avec des fonctions limitées.

Client téléchargé avec fonction d'identification des incidents (HODDebug.html)[1]
Charge le client téléchargé avec la fonction d'identification des incidents (consignation des informations relatives à la session et fonction de trace).

Remarques :

1. Utilisez la fonction d'identification des incidents uniquement lorsque vous contactez le Support pour résoudre un incident avec votre installation Host On-Demand.

Réduction de la taille de téléchargement du client

D'une manière générale, il est préférable de faire en sorte que la taille de vos clients Host On-Demand (téléchargés, Web Start ou en cache) soit la plus petite possible. Ainsi, vous augmentez la vitesse de leur téléchargement et gardez de l'espace disque sur le poste client.

Le meilleur moyen de réduire la taille de vos clients Host On-Demand consiste à les créer à l'aide de l'assistant de déploiement. Les clients prédéfinis fournis avec Host On-Demand sont en principe plus volumineux que les clients personnalisés créés à l'aide de l'assistant de déploiement car ils contiennent la batterie complète des fonctions client Host On-Demand. Les clients créés dans l'assistant de déploiement ne contiennent que les fonctions que vous avez sélectionnées. En outre, les clients de l'assistant de déploiement sont téléchargés au format compressé. Ainsi, la taille de téléchargement est réduite de manière encore plus significative.

Lorsque vous créez un client à l'aide de l'assistant de déploiement, vous pouvez sélectionner uniquement les fonctions dont les utilisateurs sont supposés avoir besoin dans la fenêtre des options de préchargement de l'assistant de déploiement. Par exemple, si les utilisateurs n'ont besoin que du terminal 3270 et des sessions d'impression 3270, ne sélectionnez que ces types de sessions lors de la création du client dans l'assistant de déploiement. Si vous intégrez une prise en charge des types de sessions inutilisés, vous augmentez la taille du client sans améliorer ses fonctionnalités.

Si vous cliquez sur Sélection automatique dans la fenêtre des options de préchargement, l'assistant de déploiement sélectionne les composants dont vous avez besoin, suivant la configuration de votre session.

Vous pouvez également choisir de ne pas télécharger des composants liés à des fonctions rarement utilisées. A moins que vous ne choisissiez de désactiver cette fonction dans l'assistant de déploiement, les utilisateurs vont être invités à télécharger les composants nécessaires lorsqu'ils y font appel. Si vous avez besoin, par la suite, de types de sessions supplémentaires, vous ne serez pas nécessairement obligé de créer un nouveau type de client. Vous n'aurez qu'à ajouter les nouveaux types de sessions à la liste appropriée de l'écran des options de préchargement.

Sur Mac OS X, vous ne pouvez installer aucun composant supplémentaire après le téléchargement initial. Pour plus d'informations, reportez-vous à «Prise en charge du client en cache sur Mac OS X (clients Java uniquement)», à la page 84.

N'utilisez pas la fonction de débogage ou de d'identification des incidents dans les clients générés ou prédéfinis à l'aide de l'assistant de déploiement. En effet, vous risqueriez d'augmenter la taille du client de manière significative et de ralentir ses performances. Les fonctions de débogage et d'identification des incidents ne sont pas prévues pour un usage général. Utilisez-les uniquement en conjonction avec le support technique de Host On-Demand afin de diagnostiquer et de résoudre les incidents liés au système Host On-Demand.

Déploiement d'archives et classes Java fournies par l'utilisateur

Les archives et classes Java fournies par l'utilisateur sont toutes celles qui ne sont pas livrées avec le client Host On-Demand ni ne font partie de l'environnement JRE (Java Runtime Environment). Il peut s'agir par exemple de fichiers d'archives ou de classes Java que vous avez vous-mêmes mises en oeuvre, ou que vous avez récupérées auprès de tierces parties.

Le déploiement de ces classes ou archives avec le client d'émulation peut être souhaitable dans les situations suivantes :

- Lorsque vous souhaitez que les utilisateurs exécutent des macros destinées à appeler des méthodes Java fournies par eux.
- Lorsque vous souhaitez que les utilisateurs exécutent une applet, fournie par eux, dans la session (qu'il s'agisse d'une applet démarrée automatiquement dans la session ou lancée via les options de menu Actions > Exécution d'applet dans la fenêtre de session).

Pour connaître les restrictions liées à Java lors de l'exécution d'applets fournies par l'utilisateur, reportez-vous à «Restrictions liées aux applets fournies par l'utilisateur et à Java», à la page 17.

Bien qu'il existe plusieurs méthodes possibles pour effectuer le déploiement de ces fichiers, chacune d'elles n'est applicable que dans circonstances bien particulières. Les différentes méthodes disponibles sont les suivantes :

- Définition du paramètre HTML "AdditionalArchives" dans l'assistant de déploiement. Voir «Utilisation du paramètre HTML AdditionalArchives», à la page 93.
- Copie des fichiers dans le répertoire de diffusion du serveur Host On-Demand. Voir «Déploiement à partir du répertoire de diffusion», à la page 93.

La méthode de déploiement sélectionnée dépend des facteurs suivants :

- Le type de fichier déployé (classes et archives Java)
- L'emplacement du déploiement des fichiers (serveur Host On-Demand ou poste de travail client)
- Le type de la plateforme client et du navigateur.

Ces trois méthodes de déploiement d'archives et classes Java fournies par l'utilisateur sont décrites dans les sections suivantes. Reportez-vous en outre à la section «Conseils et astuces pour l'utilisation des fichiers d'archives», à la page 93 pour plus d'informations sur l'utilisation des fichiers d'archive.

Utilisation du paramètre HTML AdditionalArchives

Cette méthode est applicable lorsque vous voulez déployer des archives Java sur un serveur Host On-Demand. Elle fonctionne pour le client d'émulation en cache ou téléchargé, ainsi que pour le client Web Start.

Les archives Java doivent être des fichiers .JAR Java.

L'utilisation du paramètre HTML AdditionalArchives a l'avantage de permettre le téléchargement automatique des archives Java sur le poste de travail de l'utilisateur lorsque ce dernier se connecte au serveur Host On-Demand via le fichier HTML du client en cache ou téléchargé.

L'inconvénient de cette méthode est que les fichiers d'archives ou de classes Java seront à nouveau téléchargés à chaque fois qu'un utilisateur se connecte à ce fichier HTML, que vous utilisiez un client en cache ou un client téléchargé. La raison pour laquelle le téléchargement des archives a lieu a chaque nouvelle connexion de l'utilisateur est due à la nécessité de garantir que le client Host On-Demand dispose des dernières versions de vos fichiers d'archives ou de classes. Cette méthode convient donc le mieux lorsque le nombre et la taille des fichiers d'archives ou de classes Java sont relativement réduits, car le temps de téléchargement est plus court et impose une charge moindre au serveur Web.

Pour utiliser cette méthode, procédez comme suit :

1. Copiez les fichiers d'archives dans le répertoire de diffusion de Host On-Demand. Le répertoire de diffusion par défaut est le sous-répertoire HOD situé sous le répertoire d'installation du serveur Host On-Demand, par exemple `c:\Program Files\IBM\HostOnDemand\HOD\`.
2. Editez le fichier HTML dans l'assistant de déploiement, puis :
   a. Dans la fenêtre Options avancées, cliquez sur Paramètres HTML.
   b. Dans la zone Nom, entrez `AdditionalArchives`.
   c. Dans la zone Valeurs, indiquez le nom des fichiers d'archives Java, séparés par des virgules, sans préciser l'extension (.jar). Par exemple :
      `myCustomA,myCustomB,MyCustomC`

Pour plus d'informations, reportez-vous à AdditionArchives de l'aide en ligne.

Déploiement à partir du répertoire de diffusion

Cette méthode s'applique à la situation suivante :

- Lorsque vous voulez déployer des archives Java sur un serveur Host On-Demand. Les fichiers de classe Java ne doivent faire partie d'aucun module de Host On-Demand.

Pour ce faire, copiez les fichiers d'archives dans le répertoire de diffusion de Host On-Demand. Le répertoire de diffusion par défaut est le sous-répertoire HOD situé sous le répertoire d'installation du serveur Host On-Demand, par exemple `c:\Program Files\IBM\HostOnDemand\HOD\`.

Conseils et astuces pour l'utilisation des fichiers d'archives

Les astuces et conseils suivants donnent des informations utiles lors de l'utilisation des fichiers d'archives :

- Lorsque vous créez l'archive (.jar), veillez à ce que le chemin d'accès à chaque fichier de classe soit correct. Le chemin d'accès à com.mycompany.MyClass, par

exemple, doit être `com\mycompany\`. Il ne doit *en aucun cas* être `C:\MyTestDirectory\com\mycompany\`, ni être vide (étant donné que le fichier de classe fait partie du module).

- Vérifiez que les droits d'accès adéquats aux fichiers d'archive ont été définis. Ainsi, pour les systèmes d'exploitation utilisant des droits d'accès, tels que Linux, AIX, Unix et z/OS, il convient que les droits d'accès aux fichiers d'archives soient définis sur la valeur 755 (rwxr-xr-x).
- Si deux pages de client en cache différentes spécifient des paramètres AdditionalArchives distincts, vous devez fermer, puis redémarrer le navigateur lorsque vous passez d'une page à l'autre. Dans le cas contraire, le client en cache n'est pas rechargé lorsque vous basculez entre les pages, ce qui empêche la vérification du paramètre AdditionalArchives.

Chapitre 11. Utilisation des clients Database On-Demand

Le client Database On-Demand est une applet Java qui permet à un utilisateur de générer des instructions SQL et des instructions de téléchargement en amont, d'envoyer ces instructions à un serveur de base de données éloigné et d'extraire les résultats des requêtes SQL (instructions SQL Select) à partir du serveur de base de données éloigné.

L'utilisateur peut communiquer avec un serveur de base de données fonctionnant sur un serveur IBM System i ou une autre plateforme, aussi longtemps que le pilote de connectivité JDBC (Java Database Connectivity) est installé sur le poste de travail client Database On-Demand. Pour plus d'informations, reportez-vous à «Obtention et installation d'un pilote JDBC», à la page 98 dans ce manuel.

Voici quelques fonctions offertes par Database On-Demand :

- Interfaces texte et graphique pour la construction d'instructions SQL et d'instructions de téléchargement en amont.
- Capacité à sauvegarder et réutiliser les instructions SQL et les instructions de téléchargement en amont.
- Pour les instructions SQL :
  - Capacité d'exécuter une instruction SQL et d'en afficher les résultats.
  - Capacité à sauvegarder les résultats d'une instruction SQL dans un fichier à des formats différents, notamment XML (voir «Formats de fichier d'accès à la base de données», à la page 98 dans ce manuel).
- Pour les instructions de téléchargement en amont :
  - Capacité à utiliser les types de téléchargement en amont suivants : création, remplacement, ajout et mise à jour.
  - Capacité de lire les fichiers de données à des formats variés, notamment XML (voir «Formats de fichier d'accès à la base de données», à la page 98 dans ce manuel).

Le client Database On-Demand est disponible uniquement via l'un des trois fichiers HTML client prédéfinis (voir «Clients prédéfinis Database On-Demand», à la page 97). Vous ne pouvez pas utiliser l'assistant de déploiement pour créer un client Database On-Demand.

En revanche, à la place du client Database On-Demand, vous pouvez maintenant utiliser les fonctions de base de données des clients d'émulation et des macros de Host On-Demand (voir «Fonctions de base de données dans les macros et les clients d'émulation d'écran», à la page 96).

Pour plus d'informations, reportez-vous à Overview of database access dans l'aide en ligne Host On-Demand.

Le client Database On-Demand existe dans la version Java. Par conséquent :

- Un utilisateur final, qui utilise un navigateur Java, exécute automatiquement la version Java du client Database On-Demand.

Ce client Database On-Demand peut bénéficier des capacités avancées du plug-in Java.

Fonctions de base de données dans les macros et les clients d'émulation d'écran

En alternative au client Database On-Demand, presque toutes les fonctions qui sont disponibles dans le client Database On-Demand sont maintenant disponibles dans le client d'émulation d'écran, y compris les types de sessions suivantes :

- Session écran 3270
- Session écran 5250
- Session écran du terminal virtuel

De même, vous pouvez utiliser les instructions SQL et les instructions de téléchargement en amont dans les macros des sessions client d'émulation d'écran (voir SQLQuery action et File Upload action dans *Macro Programming Guide*).

Par exemple, lorsque vous êtes connecté à un hôte éloigné dans la session d'écran 3270, vous pouvez lancer une macro qui lit automatiquement les données de la fenêtre de session d'écran 3270 et écrit les données dans une table d'une base de données qui se trouve sur un autre hôte éloigné. De même, vous pouvez lancer une macro qui lit automatiquement les données d'une table d'un hôte éloigné et écrit les données dans la fenêtre de session d'écran 3270.

Pour plus d'informations, reportez-vous à Overview of database access dans l'aide en ligne Host On-Demand.

Démarrage d'un client Database On-Demand

Pour démarrer un client Database On-Demand sur le poste de travail client, utilisez l'une des deux méthodes suivantes :

- Connectez votre navigateur à un fichier HTML Database On-Demand en tapant l'adresse URL du fichier HTML dans le champ d'adresse de votre navigateur (ou en cliquant sur un lien qui renvoie le navigateur à cette adresse URL). Le format de l'adresse est le suivant :

  `http://nom_serveur/alias_hod/nom_client.html`

  nom_serveur est le nom de l'hôte ou de l'adresse IP du serveur Host On-Demand, *alias_hod* est l'alias du répertoire de diffusion et *nom_client* est le nom du fichier HTML. Par exemple, supposons que l'adresse www.myHODServer.com est votre serveur Host On-Demand et que hod est l'alias du répertoire de diffusion, alors l'adresse URL de la version de téléchargement du client Database On-Demand sera :

  `http://www.myHODServer.com/hod/HODDatabase.html`
- Connectez votre navigateur sur le fichier HTML client IBM Host On-Demand, puis cliquez sur le lien du client Database On-Demand que vous souhaitez exécuter. L'URL du fichier HTML client :

  `http://nom_serveur/alias_hod/HODMain_xx.html`

  nom_serveur et *alias_hod* ont les mêmes significations qu'au-dessus. Dans le nom du fichier HODMain_*xx*, the *xx* est une mnémonique à deux lettres qui désigne la langue que vous souhaitez utiliser. Par exemple, pour l'anglais, le fichier se nomme HODMain_en.html et l'adresse URL complète (en supposant qu'il s'agit du même serveur et alias qu'au-dessus) :

  `http://www.myHODServer.com/hod/HODMain_en.html`

Clients prédéfinis Database On-Demand

Le client Database On-Demand client est disponible via l'un des trois fichiers HTML client. Vous ne pouvez pas utiliser l'assistant de déploiement pour créer un fichier HTML client Database On-Demand. Les clients prédéfinis sont décrits ci-dessous.

Client Database On-Demand (HODDatabase.html)

Il s'agit du client téléchargé. "Téléchargé" signifie que l'intégralité du code client est téléchargé vers le poste de travail client chaque fois que l'utilisateur final démarre le client Database On-Demand.

Client en cache Database On-Demand (HODDatabaseCached.html)

Il s'agit du client en cache. "En cache" signifie que la majeure partie du code client est téléchargée la première fois que l'utilisateur démarre le client Database On-Demand, pour ensuite le stocker sur le poste de travail client. Après le premier téléchargement, le client en cache démarre beaucoup plus vite le client téléchargé du fait que car la majeure partie du code client est déjà disponible sur le poste de travail client. Le client Database On-Demand en cache comporte de nombreux composants en commun avec le client Host On-Demand en cache.

Pour le client en cache, si votre utilisateur final requiert plusieurs pages de code, vous devez ajouter le nom du fichier archive (fichier .jar) pour chaque page de code supplémentaire à la liste préchargée dans le fichier HTML prédéfini. Pour obtenir la liste des langues des pages de codes et des noms de fichiers .jar correspondants, reportez-vous à «Utilisation de plusieurs pages de codes avec Database On-Demand», à la page 98.

Client en cache Database On-Demand avec fonction d'identification des incidents (HODDatabaseCachedDebug.html)

Il s'agit du client en cache avec un code d'identification des incidents supplémentaire pour les événements de session de consignation et de traçage.

Utilisez le client d'identification des incidents uniquement lorsque vous contactez le Support IBM pour résoudre un incident avec votre installation Host On-Demand.

Configuration de Database On-Demand pour les utilisateurs

Pour configurer Database On-Demand pour les utilisateurs, appliquez la procédure suivante :

1. Utilisez l'utilitaire d'administration pour définir les groupes et les utilisateurs (voir Managing users and groups dans l'aide en ligne Host On-Demand).
2. Spécifiez les fonctions de base de données que vous souhaitez que les groupes et les utilisateurs puissent exécuter, puis spécifiez les valeurs par défaut pour certains des paramètres de base de données dans les nouvelles instructions SQL et les instructions de téléchargement en amont (voir Database On-Demand Group/User Options dans l'aide en ligne Host On-Demand).

Si vous voulez créer des instructions SQL et des instructions de téléchargement en amont prédéfinies pour les utilisateurs et les groupes, procédez comme suit :

1. Exécutez le client Database On-Demand comme utilisateur final, puis créez des instructions SQL et des instructions de téléchargement en amont (voir Getting started with Database On-Demand dans l'aide en ligne Host On-Demand).
2. Lancez l'utilitaire d'administration et copiez les instructions SQL et les instructions de téléchargement en amont pour les autres utilisateurs ou groupes (voir Database On-Demand Group/User Statements dans l'aide en ligne Host On-Demand).

Obtention et installation d'un pilote JDBC

Pour connecter un serveur de base de données exécuté sur un hôte éloigné, l'utilisateur final doit avoir un pilote de connectivité JDBC installé sur le poste de travail client.

Le client Host On-Demand et le client Database On-Demand incluent toujours un pilote provenant de IBM AS/400 Toolbox for Java. Ce pilote permet au client d'accéder à une base de données DB2/400 sur un système hôte IBM System i ou AS/400 correctement configuré. Vous n'avez pas besoin d'enregistrer ni de déployer ce pilote.

Si vous avez besoin d'un autre pilote JDBC :

1. Pour cela, contactez votre fournisseur ou l'administrateur de la base de données éloignée.
2. Enregistrez le pilote JDBC avec Host On-Demand ou Database On-Demand. Voir Registering a JDBC driver dans l'aide en ligne Host On-Demand.
3. Déployez le pilote JDBC sur les postes de travail de vos utilisateurs finals. Voir Deploying a JDBC driver dans l'aide en ligne Host On-Demand.

Formats de fichier d'accès à la base de données

L'utilisateur final sélectionne le type de fichier pour l'instruction SQL ou l'instruction de téléchargement en amont dans l'onglet Sortie de la fenêtre de l'Assistant SQL ou dans l'onglet Fichier de la fenêtre de téléchargement en amont.

Pour plus d'informations sur les formats de fichier, reportez-vous à File formats for database access dans l'aide en ligne Host On-Demand.

Utilisation de plusieurs pages de codes avec Database On-Demand

Si vous souhaitez utiliser plusieurs pages de codes avec Database On-Demand, vous devez ajouter des fichiers jar ou cab en plus de votre fichier HTML. Seules les pages de codes qui correspondent à la langue du fichier HTML sont automatiquement chargées. Par exemple, pour accéder à un hôte néerlandais lorsque vous utilisez un ordinateur français, vous devez apporter les modifications ci-après.

Editez le fichier CommonJars.js. Si vous utilisez un client téléchargé, recherchez la ligne commençant par «dbaDownloadJars =» et ajoutez les noms de fichiers appropriés du tableau ci-dessous. Utilisez les noms des fichiers jar, même si vos clients utilisent Internet Explorer (les noms vont être ultérieurement convertis en noms de fichiers cab). Si vous utilisez un client téléchargé, recherchez la ligne commençant par «dbaCachedComps =» et ajoutez le nom de composant approprié du tableau ci-dessous.

Pages de codes Database On-Demand prises en charge

Le tableau suivant répertorie les langues prises en charge pour les pages de codes du client Database On-Demand, les noms des fichiers .jar correspondants et les noms des composants en cache :

Langue de la page de codes	Nom du fichier .JAR	Nom du composant
Arabe	hacpar.jar	HACPAR
Tchèque, hongrois, polonais, slovène	hacpce.jar	HACPCE
Danois, finnois, néerlandais, norvégien, suédois	hacp1b.jar	HACP1B
Allemand, espagnol, français, italien, portugais, portugais du Brésil	hacp1a.jar	HACP1A
Grec	hacpgr.jar	HACPGR
Hébreu	hacphe.jar	HACPHE
Japonais	hacpja.jar	HACPJA
Coréen	hacpko.jar	HACPKO
Russe	hacpru.jar	HACPRU
Chinois simplifié	hacpzh.jar	HACPZH
Thaï	hacpth.jar	HACPTH
Turc	hacptr.jar	HACPTR
Chinois traditionnel	hacptw.jar	HACPTW

Chapitre 12. Création et déploiement des bibliothèques de macros du serveur

Les bibliothèques de macros du serveur sont disponibles pour les utilisateurs de pages de modèle HTML et de modèles de configuration. Pour une page HTML, les utilisateurs peuvent faire appel à l'assistant de déploiement pour personnaliser la bibliothèque de macros du serveur ; pour un modèle de configuration, ils peuvent utiliser la console d'administration de Host On-Demand. Une configuration basée sur l'interface graphique utilisateur permet à l'administrateur de configurer chaque session. Pour que l'administrateur configure toutes les sessions définies, utilisez le paramètre HTML **SetServerMacroLibraryPath**.

La valeur du paramètre **SetServerMacroLibraryPath** est un *chemin de partage* ou un *chemin relatif*. Les valeurs permettent de créer et gérer un référentiel central de macros accessibles aux utilisateurs à partir de leurs sessions Host On-Demand. Ces macros ne sont téléchargées sur le poste de l'utilisateur que lorsqu'elles sont nécessaires. Lorsque vous modifiez une macro de serveur, les utilisateurs récupèrent automatiquement vos mises à jour lorsqu'ils accèdent de nouveau à la macro.

Les bibliothèques de macros du serveur présentent un certain nombre d'avantages :

- Elles offrent un moyen pratique de stocker, modifier et administrer des macros, à partir d'un emplacement unique et facile d'accès.
- Elles permettent d'effectuer le partage aisé de macros parmi de multiples utilisateurs, sur un nombre illimité de sessions.
- Elles éliminent la nécessité de recourir à l'importation de macros au sein des sessions Host On-Demand, ce qui permet de réduire la taille des sessions. Le téléchargement des macros sur l'ordinateur de l'utilisateur a lieu uniquement à la condition et au moment où l'utilisateur y accède.
- Vous pouvez éditer des macros et remplacer les fichiers contenus dans la bibliothèque de macros du serveur à tout moment, sans régénérer les sessions Host On-Demand ni modifier les fichiers HTML. Toute modification apportée se trouve automatiquement disponible dès qu'une demande portant sur la macro concernée est émise par un utilisateur.

Les bibliothèques de macros de serveur peuvent résider sur un serveur Web ou sur une unité réseau partagée. Quel que soit le type de bibliothèque, vous pouvez sélectionner les macros qui seront accessibles aux sessions Host On-Demand particulières. Si vous utilisez une bibliothèque de macros résidant sur Internet, vous devez créer un fichier texte identifiant quelles macros particulières doivent être mises à la disposition de la session que vous configurez. Si vous utilisez une bibliothèque de macros basée sur une unité réseau partagée, *tous* les fichiers contenus dans le répertoire spécifié seront disponibles pour la session. Les utilisateurs ne seront pas autorisés à écrire dans une bibliothèque de macros basée sur le Web, mais ils peuvent mettre à jour une bibliothèque de macros basée sur une unité partagée s'ils disposent d'un accès en écriture.

Déploiement d'une bibliothèque de macros du serveur sur un serveur Web

1. Placez les macros dans un répertoire accessible aux utilisateurs par le biais d'un serveur Web. Il ne doit pas nécessairement s'agir du répertoire de diffusion de Host On-Demand.
2. Pour chaque session nécessitant la définition d'une série de macros distincte, créez un fichier texte dressant la liste des noms de fichiers de macros. Ce fichier texte doit être formaté de sorte que les noms des fichiers de macros apparaissent sur une seule ligne, par exemple :

   ```
   macro1.mac
   macro2.mac
   macro3.mac
   ```

   Assurez-vous de bien respecter les consignes suivantes :
   - Le nom de la macro doit être le premier élément indiqué sur la ligne, car toute information spécifiée après le premier élément est ignorée.
   - Si le premier élément indiqué sur la ligne commence par les caractères //, la ligne est considérée comme un commentaire et est ignorée.
   - Chaque macro citée dans le fichier texte doit être pourvue d'une extension .mac.
3. Placez ce fichier texte dans le même répertoire que les macros auxquelles il fait référence.
4. Dans l'assistant de déploiement, cliquez sur le menu Configuration de la fenêtre Sessions hôte et sélectionnez l'option Bibliothèque de macros du serveur. Cochez la case "Utilisation d'une bibliothèque de macros du serveur pour cette session" et sélectionnez l'option Bibliothèque de macros du serveur Web.
5. Indiquez l'URL qualifiée complète de la liste de macros que vous avez créée à l'étape 2, par exemple http://nom_serveur/hod/liste_macros.txt. Cliquez sur OK.

Lorsque les utilisateurs ouvrent une session, ils peuvent faire appel aux fenêtres Exécution de macro ou Macros disponibles pour visualiser les macros spécifiées dans la liste créée pour leur session. Ces macros deviennent disponibles lorsque les utilisateurs sélectionnent la bibliothèque de serveur pour stocker leurs macros. L'emplacement de la bibliothèque du serveur est accessible uniquement si vous avez configuré la session en vue d'utiliser une bibliothèque de macros de serveur.

Remarque : La bibliothèque de macros du serveur peut également être configurée dans le client d'administration.

Déploiement d'une bibliothèque de macros du serveur sur une unité partagée

1. Placez les macros dans un répertoire partagé de votre réseau.
2. Dans la fenêtre Sessions hôte de l'assistant de déploiement, sélectionnez la session que vous souhaitez configurer, cliquez sur le menu Configuration et sélectionnez l'option Bibliothèque de macros du serveur. Cochez la case "Utilisation d'une bibliothèque de macros du serveur pour cette session" et sélectionnez l'option Bibliothèque de macros pour unité partagée.
3. Spécifiez le chemin d'accès au répertoire. Voici des exemples de chemins d'accès corrects :

- Chemins d'accès absolus. Les indicatifs d'unités de réseau mappées peuvent également être utilisés dans le chemin d'accès absolu. Il est à noter qu'une bibliothèque de macros du serveur ne doit jamais pointer vers une unité locale.
- Les noms ou adresses IP d'ordinateurs distants sont autorisés, du moment que l'ordinateur de l'utilisateur est déjà connecté à distance et authentifié sur la machine partageant le répertoire concerné. Voici deux exemples de chemins d'accès à des bibliothèques de macros hébergées sur une unité partagée :
  - `\\your_host\macro_library`, où *your_host* désigne le nom de l'hôte et *macro_library* désigne le répertoire des macros.
  - `\\123.45.67.89\macro_library`, où *123.45.67.89* désigne l'adresse IP de l'hôte et *macro_library* désigne le répertoire des macros.

  Si vous procédez à la configuration d'une bibliothèque de macros pour plusieurs sessions et que chaque session utilise son propre ensemble de macros, vous devez créer un répertoire distinct pour chaque session.

4. Cliquez sur OK.

Lorsque les utilisateurs ouvrent une session, ils peuvent faire appel aux fenêtres Exécution de macro ou Macros disponibles pour visualiser la liste des macros contenues dans ce répertoire. Ces macros deviennent disponibles lorsque les utilisateurs sélectionnent la bibliothèque de serveur pour stocker leurs macros. L'emplacement de la bibliothèque du serveur est accessible uniquement si vous avez configuré la session en vue d'utiliser une bibliothèque de macros de serveur.

Chapitre 13. Modification dynamique des propriétés de session

Les sessions Host On-Demand sont définies par l'administrateur et extraites par le client Host On-Demand lorsqu'un utilisateur accède à une page HTML de Host On-Demand. Les propriétés de session affichées par un utilisateur sont des valeurs fixes, composées de la configuration initiale de l'administrateur et des mises à jour utilisateur. Cependant, avec certaines pages HTML ou certaines propriétés de session, il peut parfois s'avérer utile de définir une valeur de manière dynamique au moment où un utilisateur accède aux pages HTML. Ce type de contrôle permet de définir des propriétés de session en fonction de certaines informations, comme l'adresse IP du client ou l'heure.

Pour définir les propriétés de session de manière dynamique lors de l'accès aux pages HTML, l'administrateur doit écrire un programme s'exécutant sur le serveur Web et modifiant de manière effective la page HTML juste avant son envoi au client. Même si les propriétés de session initiales ne sont pas définies dans la page HTML, Host On-Demand offre la possibilité de substituer la plupart des propriétés de session de cette page. Ainsi, les nouvelles propriétés sont toujours utilisées par le client et prennent toujours le pas sur les propriétés de session initiales définies par l'administrateur et sur toutes les mises à jour des propriétés effectuées par l'utilisateur. La valeur HTML de substitution n'est jamais enregistrée. Ainsi, le client a la possibilité d'utiliser de nouveau les paramètres précédents chaque fois que l'administrateur retire les substitutions. De même, la propriété de substitution est verrouillée de sorte qu'un utilisateur n'ait pas la possibilité de la modifier.

L'administrateur peut écrire un programme permettant de définir de manière dynamique une ou plusieurs propriétés de plusieurs façons à l'aide des substitutions de pages HTML, comme les Java Server Pages (JSP), les servlets, Perl, REXX ou Active Server Pages (ASP). Ce chapitre est illustré d'exemples centrés sur les problèmes administrateur. Ces exemples sont censés représenter la syntaxe et la technique de substitution de propriétés particulières. Ces mécanismes s'appliquent à toutes les approches de programmation choisies par l'administrateur.

Configuration du fichier HTML initial

Le fichier HTML initial doit être créé à l'aide de l'assistant de déploiement, qui permettra de configurer les fonctions que vous jugez importantes, comme la taille du code téléchargé et les fonctions disponibles à vos utilisateurs. Les sections ci-après décrivent les paramètres HTML que vous allez devoir inclure. Toutefois, n'oubliez pas que le format exact nécessaire de ces paramètres varie en fonction du format de la page HTML. Notez que dans Host On-Demand version 7 ou supérieure, certaines des pages HTML sont générées à l'aide de JavaScript, et que les paramètres HTML sont spécifiés dans un tableau JavaScript ou à l'aide des instructions JavaScript document.write. De même, le format de la page HTML varie en fonction du client (client en cache ou téléchargé) sélectionné.

Définition de la base de code

Pour définir la base de code lors de la création d'un fichier HTML à l'aide de l'assistant de déploiement, procédez comme suit :

1. Dans la fenêtre Options supplémentaires, Cliquez sur Options avancées et accédez à l'autre branche de la vue en arborescence.
2. Entrez le chemin d'accès relatif /hod/ dans la zone Code de base.
3. Sauvegardez le fichier HTML dans le répertoire de diffusion par défaut de Host On-Demand : *répertoire_installation*\HOD.

Le fichier HTML se trouve à présent dans le même répertoire que les fichiers d'archive de Host On-Demand.

La base de code fait référence au répertoire de diffusion de l'installation de Host On-Demand, et non au répertoire dans lequel les fichiers de l'assistant de déploiement sont publiés. Bien que vous puissiez entrer une URL qualifiée complète dans la zone Base de code, il est fortement conseillé d'indiquer le chemin d'accès relatif /hod/ comme répertoire de diffusion par défaut lors de la modification dynamique des propriétés de session. Si vous indiquez une URL qualifiée complète, tous les utilisateurs spécifiant le nom d'hôte autrement que pour la base de code ne pourront pas accéder à ces fichiers, même si les entrées DNS permettent la résolution de la même adresse IP.

Ajout du paramètre ConfigBase

Ajoutez un paramètre au fichier HTML nommé ConfigBase. Identique à l'opération de définition de la base de code /hod/ dans «Définition de la base de code», à la page 105, le paramètre ConfigBase est indispensable car vous pouvez être amené à déployer votre fichier JSP à un emplacement qui est différent du répertoire de diffusion par défaut et l'applet Host On-Demand doit identifier le mode de recherche des fichiers de configuration dans le répertoire hostondemand/HOD/HODData. Ces fichiers sont créés au même moment où vous enregistrez le fichier HTML de l'assistant de déploiement dans le répertoire de diffusion. Contrairement à la base de code, le paramètre ConfigBase requiert une URL complète. ConfigBase est un terme spécifique à Host On-Demand.

Pour plus d'informations, reportez-vous à Developing JavaServer Pages files with WebSphere extensions.

Substitution des paramètres HTML

Vous devez suivre plusieurs étapes pour définir les propriétés de session de manière dynamique (les exemples présentés ci-après vont vous permettre de mieux comprendre comment certains de ces paramètres doivent être spécifiés) :

1. **Activation des substitutions HTML**. Par défaut, le client va ignorer les substitutions HTML. Pour activer les substitutions, vous devez inclure un paramètre HTML appelé EnableHTMLOverrides et lui affecter la valeur 'true'.
2. **Liste des sessions à substituer**. Etant donné qu'il peut exister plusieurs sessions associées à des pages HTML, vous devez répertorier celles que vous souhaitez substituer. Vous allez devoir inclure un paramètre HTML appelé TargetedSessionList, qui aura pour valeur les noms exacts des sessions qui peuvent être substituées. Cette valeur doit être une liste de noms de sessions séparées par des virgules ("Session1Name, Session2Name", par exemple).
3. **Spécification de la substitution elle-même**. Pour chaque propriété de session à substituer, vous devez inclure un paramètre HTML appelé nom de propriété, dont la valeur est la substitution souhaitée. La valeur que vous indiquez va alors s'appliquer à toutes les sessions répertoriées dans le paramètre TargetedSessionList. Si vous souhaitez remplacer uniquement un sous-ensemble

des sessions dans le paramètre TargetedSessionList, vous pouvez indiquer une valeur au format "Session1Name=value1, Session2Name=value2", par exemple.

Propriétés de session spécifiques pouvant être substituées

Le tableau suivant présente les propriétés de session qui peuvent être substituées et donne les valeurs admises de chaque paramètre :

Tableau 12. Propriétés de session pouvant être substituées

Nom du paramètre	Description	Valeurs admises
Host	Nom d'hôte ou adresse IP du serveur cible. S'affiche en tant qu'"Adresse de destination" dans les panneaux de propriétés. S'applique à tous les types de sessions.	Nom d'hôte ou adresse IP.
HostBackup1	Nom d'hôte ou adresse IP du serveur de sauvegarde Backup1. S'affiche en tant qu'"Adresse de destination" dans les panneaux de propriétés de Backup1. S'applique à tous les types de sessions.	Nom d'hôte ou adresse IP.
HostBackup2	Nom d'hôte ou adresse IP du serveur de sauvegarde Backup2. S'affiche en tant qu'"Adresse de destination" dans les panneaux de propriétés de Backup2. S'applique à tous les types de sessions.	Nom d'hôte ou adresse IP.
Port	Numéro de port sur lequel le serveur cible est en mode écoute. S'affiche en tant que "Port de destination" dans les panneaux de propriétés. S'applique à tous les types de sessions.	Tout numéro de port TCP/IP admis.
PortBackup1	Numéro de port sur lequel le serveur Backup1 est en mode écoute. S'affiche en tant que "Port de destination" dans les panneaux de propriétés de Backup1. S'applique à tous les types de sessions.	Tout numéro de port TCP/IP admis.
PortBackup2	Numéro de port sur lequel le serveur Backup2 est en mode écoute. S'affiche en tant que "Port de destination" dans les panneaux de propriétés de Backup2. S'applique à tous les types de sessions.	Tout numéro de port TCP/IP admis.

Tableau 12. Propriétés de session pouvant être substituées (suite)

Nom du paramètre	Description	Valeurs admises
CodePage	Page de codes du serveur auquel se connecte la session. S'affiche en tant que "Page de codes hôte" dans les panneaux de propriétés. S'applique à tous les types de sessions hormis FTP.	Partie numérique (037, par exemple) de la page de codes hôte prise en charge dans l'écran de propriétés de la session.
SessionID	Nom abrégé que vous souhaitez affecter à cette session (s'affiche dans la ZIO). Il doit être unique à cette configuration. S'affiche en tant qu'"ID de session" dans les panneaux de propriétés. S'applique à tous les types de sessions.	Un caractère : de A à Z.
LUName	Nom de l'unité logique (LU) ou du groupe de LU, défini au serveur cible, auquel vous souhaitez connecter cette session. S'affiche en tant que "Nom de LU ou de groupe" dans les panneaux de propriétés. S'applique aux types de sessions écran 3270 et imprimante 3270.	Nom d'une LU ou d'un groupe de LU.
LUNameBackup1	Nom de l'unité logique (LU) ou du groupe de LU, défini au serveur Backup1, auquel vous souhaitez connecter cette session. S'affiche en tant que "Nom de LU ou de groupe" dans les panneaux de propriétés de Backup1. S'applique aux types de sessions écran 3270 et imprimante 3270.	Nom d'une LU ou d'un groupe de LU.
LUNameBackup2	Nom de l'unité logique (LU) ou du groupe de LU, défini au serveur Backup2, auquel vous souhaitez connecter cette session. S'affiche en tant que "Nom de LU ou de groupe" dans les panneaux de propriétés de Backup2. S'applique aux types de sessions écran 3270 et imprimante 3270.	Nom d'une LU ou d'un groupe de LU.

Tableau 12. Propriétés de session pouvant être substituées (suite)

Nom du paramètre	Description	Valeurs admises
WorkstationID	Nom de ce poste de travail. S'affiche en tant qu'"ID du poste de travail" dans les panneaux de propriétés. S'applique aux types de sessions écran 5250 et imprimante 5250.	Nom unique de ce poste de travail.
ScreenSize	Permet de définir le nombre de lignes et de colonnes de l'écran. S'affiche en tant que "Taille de l'écran" dans les panneaux de propriétés. S'applique aux types de sessions écran 3270 et 5250, ainsi qu'aux types de sessions VT.	• valeur = lignes x colonnes • 2 = 24 x 80 (3270, 5250, VT) • 3 = 32 x 80 (3270) • 4 = 43 x 80 (3270) • 5 = 27 x 132 (3270, 5250) • 6 = 24 x 132 (VT) • 7 = 36 x 80 (VT) • 8 = 36 x 132 (VT) • 9 = 48 x 80 (VT) • 10 = 48 x 132 (VT) • 11 = 72 x 80 (VT) • 12 = 72 x 132 (VT) • 13 = 144 x 80 (VT) • 14 = 144 x 132 (VT) • 15 = 25 x 80 (VT) • 16 = 25 x 132 (VT)
SLPScope	Protocole SLP (Service Location Protocol). S'affiche en tant que "Portée" dans "Options SLP" dans les panneaux de propriétés. S'applique aux types de sessions écran 3270, imprimante 3270, écran 5250 et imprimante 5250.	Prenez contact avec votre administrateur afin d'obtenir les valeurs admises pour cette zone.
SLPAS400Name	Permet de connecter une session à un serveur IBM System i spécifique. S'affiche en tant que "Nom iSeries (SLP)" dans les panneaux de propriétés. S'applique aux types de sessions écran 5250 et imprimante 5250.	Nom qualifié complet de CP SNA (USIBMNM.RAS400B, par exemple).
FTPUser	Indique l'ID utilisateur que la session utilise lors de la connexion au serveur FTP. S'affiche en tant qu'"ID utilisateur" dans les panneaux de propriétés. S'applique aux types de sessions FTP.	Un ID utilisateur admis.

Tableau 12. Propriétés de session pouvant être substituées (suite)

Nom du paramètre	Description	Valeurs admises
FTPPassword	Permet de préciser le mot de passe utilisé par la session lors de la connexion au serveur FTP. S'affiche en tant que "Mot de passe" dans les panneaux de propriétés. S'applique aux types de sessions FTP.	Un mot de passe admis.
UseFTPAnonymousLogon	Permet à la session de se connecter à un serveur FTP à l'aide d'un ID utilisateur anonyme. s'affiche en tant que "Connexion anonyme" dans les panneaux de propriétés. S'applique aux types de sessions FTP.	Oui ou Non.
FTPEmailAddress	Permet de préciser l'adresse électronique à utiliser lors de la connexion au serveur FTP en utilisant la Connexion anonyme. S'affiche en tant qu'"Adresse électronique" dans les panneaux de propriétés. S'applique aux types de sessions FTP.	Une adresse électronique admise.
PromptForDestinationAddress	Invite l'utilisateur à préciser ou non l'adresse de destination à utiliser lors de la connexion au serveur FTP. S'affiche en tant qu'"Adresse de destination" dans les panneaux de propriétés. S'applique aux types de sessions FTP.	yes ou no
CICSInitialTransEnabled	Active une transaction initiale lancée lors de l'établissement d'une session passerelle CICS.	true / false

Tableau 12. Propriétés de session pouvant être substituées (suite)

Nom du paramètre	Description	Valeurs admises
CICSInitialTrans	Spécifie le nom de la transaction initiale lancée lors de la connexion à un hôte CICS. Ne s'applique qu'aux sessions passerelle CICS. Le paramètre CICSInitialTransEnabled doit être défini sur la valeur "true" pour permettre le démarrage de la transaction spécifiée.	Les identificateurs de transaction admis sont des chaînes comprenant entre 1 et 128 caractères. La chaîne identifie la transaction initiale et tous les paramètres complémentaires exécutés durant la connexion au serveur. Les quatre premiers caractères, ou les caractères inclus avant le premier espace dans la chaîne, sont pris en compte pour la transaction. Les données restantes sont transmises à la transaction lors de l'appel de cette dernière.
Netname	Nom de la ressource de terminal à installer ou réserver. Si cette zone est vide, le type de terminal sélectionné est imprévisible. Ne s'applique qu'aux sessions CICS.	Un nom de ressource de terminal admis.

Toutes les erreurs survenues lors du traitement des paramètres HTML s'affichent sur la console Java.

Exemple 1 : substitution du nom de LU en fonction de l'adresse IP du client

Les administrateurs peuvent éviter de préciser les noms de LU directement dans les définitions de sessions. Cet exemple présente un moyen simple d'utilisation de l'adresse IP du client pour consulter un nom de LU répertorié dans le fichier texte et l'utiliser comme valeur de substitution dans une session.

Cet exemple est écrit avec JSP. L'assistant de déploiement a été utilisé pour créer un fichier HTML contenant deux sessions appelées écran 3270 et écran 5250. Notez que dans Host On-Demand version 7 ou supérieure, certaines des pages HTML sont générées à l'aide de JavaScript, et que les paramètres HTML sont spécifiés dans un tableau JavaScript ou à l'aide des instructions JavaScript document.write. De même, le format de la page HTML varie en fonction du client (client en cache ou téléchargé) sélectionné.

Cet exemple exploite une page Java en cache pour commencer ; les modifications requises pour le code HTML étant signalées en gras. Lorsque l'assistant de déploiement est utilisé pour générer une page Java2 en cache, il crée les fichiers suivants :

- Example1.html
- z_Example1.html
- Example_J2.html

Un client Macintosh utilise une page Example_J2.html.

Un fichier (c:\luname.table) est lu. Il contient des paires adresse IP/nom de LU. L'adresse IP du client est utilisée pour consulter le nom de LU correct, qui est remplacé dans la session "écran 3270". Reportez-vous aux commentaires de l'exemple pour obtenir plus de détails. Les lignes ajoutées à la sortie de l'assistant de déploiement apparaissent en **gras**.

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<%
// Read the luname.table file into a properties variable.
// Les lignes du fichier luname.table se présentent au format suivant :
// ipaddress=luname
Properties lunames = new Properties();
lunames.load(new FileInputStream("c:\\luname.table"));
%>
<HTML>
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<!-- TITLE Begin -->
<TITLE>Example1 page title</TITLE>
<!-- TITLE End -->
<!-- SUMMARY Begin -->
<!--
Configuration Model
 What configuration model would you like to use?
 -HTML-based model
Host Sessions
 -3270 Display
 -5250 Display
Additional Options
 -Cached = Cached client
 -Java Type = java2
Disable Functions
Preload Options
 -5250 Sessions = True
 -Change Session Properties = True
 -3270 Sessions = True
Cached Client/Web Start Options
 Basic Options
 -Debug = False
 -Height (in pixels) = 250
 -Width  (in pixels) = 550
 Upgrade Options
 -Percent of users who can upgrade by default = 100
 -Prompt user (user decides foreground or background)
Advanced Options
 HTML parameters
 -None
 Code base
 - /hod/
 HTML templates
 -Default
 Problem determination
 -Debug = False
 User updates
 -Persist user updates? = True
 Appearance
 -Standard Host On-Demand Client
 Applet size
 -Autosize to browser
 Session Manager API
 -Enable Session Manager JavaScript API = False
 Server connection
 Language
 -Locale = Use the system Locale
 Maximum sessions
 - 26
-->
<!-- SUMMARY End -->
</HEAD>

<BODY BACKGROUND="/hod/hodbkgnd.gif">
<CENTER>
<IMG src="/hod/hodlogo.gif" ALT="hodlogo.gif">
<P>
```

```
<SCRIPT LANGUAGE="JavaScript">
function writeAppletParameters()
{
   return "";
}
</SCRIPT>


<SCRIPT LANGUAGE="JavaScript" SRC="/hod/HODVersion.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonJars.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonParms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonJ2Parms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript">
var db = parent.location;
var hod_Locale = '';
var hod_AppName ='';
var hod_AppHgt = '340';
var hod_AppWid = '550';
var hod_CodeBase = '/hod/';
var hod_Comps = 'HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HA3270;HODCFG;HA5250';
var hod_Archs = 'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hafntib.jar,hafntap.jar,
                 ha3270n.jar,hodcfgn.jar,ha5250n.jar';

var hod_URL = new String(window.location);
var hod_DebugOn = false;

// put cached client installation applet parameters here
var hHod_AppletParams = new Array;
hHod_AppletParams[0] = '<PARAM NAME="DebugCachedClient" VALUE="false">';
hHod_AppletParams[1] = '<PARAM NAME="ShowDocument"      VALUE="_parent">';
hHod_AppletParams[2] = '<PARAM NAME="CachedClient"      VALUE="true">';
hHod_AppletParams[3] = '<PARAM NAME="ParameterFile"     VALUE="HODData\\Example1\\params.txt">';
hHod_AppletParams[4] = '<PARAM NAME="JavaScriptAPI"     VALUE="false">';
hHod_AppletParams[5] = '<PARAM NAME="BookmarkPage"      VALUE="Example1.html">';

// The next 2 lines are required in order to override session properties.
// La première ligne sert à activer le traitement pour cette fonction et
// n'a pas besoin d'être modifiée.  La deuxième ligne sert à identifier la
// session que vous souhaitez modifier.  Dans l'exemple qui suit, 2 sessions
// sont identifiées, à savoir : "3270 Display" et "5250 Display".

hHod_AppletParams[6]='<PARAM NAME="EnableHTMLOverrides" VALUE="true">';
hHod_AppletParams[7]='<PARAM NAME="TargetedSessionList" VALUE="3270 Display,5250 Display">';

// La ligne suivante modifie le paramètre de session LUName pour la session
// "3270 Display".  Dans cet exemple, le paramètre LUName est défini sur
// la valeur d'adresse IP du client contenue dans le fichier c:\luname.table.
// Avant d'insérer vos modifications, vous pouvez utiliser une valeur
// constante afin de vous assurer que la syntaxe est correcte.
hHod_AppletParams[8]='<PARAM NAME="Luname" VALUE="3270
                      Display=<%=lunames.get(request.getRemoteAddr())%>">';

//hHod_AppletParams[x] = '<PARAM NAME="DebugCode"             VALUE="65535">';


var pg = buildJ2Page(db);
pg += writeAppletParameters();
pg += '</APPLET>';
if(hod_DebugOn) alert('J2 page complete, result = \n' + pg);
document.write(pg);
</SCRIPT>

</CENTER>
</BODY>
</HTML>
```

Exemple 2 : permettre à l'utilisateur de préciser l'hôte auquel se connecter à l'aide d'un formulaire HTML

Les administrateurs peuvent également utiliser des formulaires HTML pour indiquer les valeurs de substitution au lieu de les calculer. L'exemple suivant présente un formulaire simple pour l'entrée d'un nom d'hôte. Le formulaire permet de soumettre un programme JSP qui utilise le nom d'hôte indiqué dans le formulaire afin de substituer le nom d'hôte dans la session 3270.

Cet exemple est écrit avec JSP. L'assistant de déploiement a été utilisé pour créer un fichier HTML contenant deux sessions appelées "écran 3270" et "écran 5250". Notez que dans Host On-Demand version 7 ou supérieure, certaines des pages HTML sont générées à l'aide de JavaScript, et que les paramètres HTML sont spécifiés dans un tableau JavaScript ou à l'aide des instructions JavaScript document.write. De même, le format de la page HTML varie en fonction du client (client en cache ou téléchargé) sélectionné.

Lorsque vous utilisez ces formulaires, les données doivent être conservées lors des requêtes au programme. En effet, les fichiers HTML Host On-Demand se rechargent pour la détection Java et pour le support de mise en signet lors de l'utilisation des pages du modèle de type serveur de configuration. Lorsque vous sélectionnez Java 1 et désélectionnez le support de mise en signet si vous utilisez le modèle de type serveur de configuration, la page ne doit pas être rechargée pour conserver les données du formulaire. Cet exemple permet d'utiliser une session JSP afin de stocker les données du formulaire pendant le rechargement.

Voici un fichier HTML simple permettant d'entrer un nom d'hôte. Le formulaire est soumis au programme JSP (example2.jsp) :

```
<form method="POST"  action="hod/example2.jsp">
Hostname <input name="form.hostname"><br>
<input type="submit">
</form>
```

Voici une sortie modifiée de l'assistant de déploiement. Reportez-vous aux commentaires de l'exemple pour obtenir plus de détails. Les lignes ajoutées à la sortie de l'assistant de déploiement apparaissent en **gras**.

```
<HTML>
<%
// Get a session or create if necessary and store the hostname
// entered in the form in the session.
HttpSession session = request.getSession(true);
String hostname = request.getParameter("form.hostname");
if (hostname!=null) {
session.putValue("session.hostname", hostname);
}
%>
<!-- HOD WIZARD HTML -->
<!-- Deployment Wizard Build : 8.0.0-B20030605 -->
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<TITLE>Page de titre - Exemple 2</TITLE>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonJars.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/HODJavaDetect.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonParms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript">

//---- Start JavaScript variable declarations ----//
var hod_Locale = '';
var hod_jsapi=false;
var hod_AppName ='';
var hod_AppHgt = '80%';
var hod_AppWid = '80%';
var hod_CodeBase = '/hod/';
var hod_FinalFile = 'z_example2.html';
var hod_JavaType = 'java2';
var hod_Obplet = '';
var hod_jars = 'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hodsignn.jar,ha3270n.jar,
                hodcfgn.jar,ha5250n.jar';

var hod_URL = new String(window.location);
var hod_DebugOn = false;
var hod_SearchArg = window.location.search.substring(1);

var hod_AppletParams = new Array;
hod_AppletParams[0] = '<PARAM NAME="ParameterFile" VALUE="HODData\\example2\\params.txt">';
hod_AppletParams[1] = '<PARAM NAME="ShowDocument"  VALUE="_parent">';
hod_AppletParams[2] = '<PARAM NAME="JavaScriptAPI" VALUE="' + hod_jsapi + '">';
```

```
hod_AppletParams[3] = '<PARAM NAME="PreloadComponentList" VALUE="HABASE;HODBASE;HODIMG;
                                                                HACP;HAFNTIB;HAFNTAP;
                                                                HA3270;HODCFG;HA5250">';

// The next 2 lines are required in order to override session properties.
// The first line turns on the processing for this function and does not
// need to be modified. The second line identifies the sessions that you
// want to change. In this example, there are 2 sessions identified
// named: "3270 Display" and "5250 Display".
// Be careful to increment the array index correctly.

hod_AppletParams[4] = <PARAM NAME="EnableHTMLOverrides" VALUE="true">;
hod_AppletParams[5] = <PARAM NAME="TargetedSessionList" VALUE="3270 Display,5250 Display">;

// The following line changes the Host or Destination Address session parameter
// for the session named "3270 Display". In this example, the Host is being set
// to the value saved in the JSP session from the HTML form.
// When you are initially testing your changes, you may want to use a constant
// value to verify that the syntax is correct before you insert your
// calculations.
// Here we override the host for the 3270 session to the value saved in the
// jsp session from the html form.

hod_AppletParams[6] = <PARAM NAME="Host" VALUE="3270
                       Display=<%=session.getValue("session.hostname")%>">;

//hod_AppletParams[x] = '<PARAM NAME="DebugCode"     VALUE="65535">';

//---- End JavaScript variable declarations ----//

function getHODMsg(msgNum) {
  return HODFrame.hodMsgs[msgNum];
}

function getHODFrame() {
  return HODFrame;
}

var lang = detectLanguage(hod_Locale);
document.writeln('<FRAMESET cols="*,10" border=0 FRAMEBORDER="0">');
document.writeln('<FRAME    src="/hod/hoddetect_' + lang + '.html" name="HODFrame">');
document.writeln('</FRAMESET>');

</SCRIPT>
</HEAD>
</HTML>
```

Chapitre 14. Configuration de Host On-Demand sur zSeries

Ce chapitre explique comment définir des répertoires de diffusion et privé en lecture/écriture distincts pour la configuration de Host On-Demand sur un système zSeries.

Le but de ce scénario de configuration est de fournir des instructions pour les tâches de configuration zSeries communes.

Définition des répertoires de diffusion et privé en lecture/écriture distincts

Définition d'un système de gestion hiérarchique des fichiers pour le répertoire privé Host On-Demand

Lorsque Host On-Demand est installé, les fichiers qui se trouvent dans le répertoire */usr/lpp/HOD/hostondemand/private* sont mis à jour dans un environnement d'exécution, en plus des mises à jour de régénération de conception. Etant donné que ce répertoire est désormais mis à jour lors de l'exécution du logiciel Host On-Demand, il est recommandé de monter un système de gestion hiérarchique des fichiers (HFS) distinct. Pour ce faire, vous pouvez :

- Monter le système HFS à l'emplacement du répertoire privé en cours (*/usr/lpp/HOD/hostondemand/private*, par exemple).
- Créer un lien symbolique vers le répertoire privé, en procédant comme suit :
  1. Exécuter la commande TSO MKDIR afin de créer un point de montage différent (*/etc/HOD/private*, par exemple).
  2. Renommer, ou sauvegarder, puis supprimer votre répertoire privé d'origine.
  3. Créer un lien symbolique à partir de l'emplacement prévu (*/usr/lpp/HOD/hostondemand/private*) vers l'emplacement réel (*/etc/HOD/private*). Utilisez la commande chaînée suivante :

     ```
     ln -s /etc/HOD/private /usr/lpp/HOD/hostondemand/private
     ```

Si vous utilisez LDAP et une authentification native, copiez manuellement HODrapd et le répertoire */keys* dans le répertoire */private* spécifique au système.

Une fois le répertoire */private* spécifique au système monté, il recouvre mais ne supprime pas le répertoire */private* maître. Lorsque les mises à jour correctives sont appliquées, utilisez le répertoire */private* maître. Si ces fichiers ont été modifiés, copiez-les dans le répertoire */private* spécifique au système.

Définition d'un répertoire de diffusion utilisateur distinct

Les fichiers générés à partir de l'assistant de déploiement peuvent être placés dans un répertoire personnalisé qui est indépendant du répertoire de diffusion Host On-Demand. Cette possibilité facilite l'application des futures mises à niveau. Ainsi, le répertoire de diffusion Host On-Demand reste en lecture seule et fournit un emplacement inscriptible pour déployer les fichiers de l'assistant de déploiement.

Pour plus d'informations sur le déploiement des fichiers de l'assistant de déploiement dans un répertoire distinct et sur les autres fichiers modifiés par

l'utilisateur qui peuvent être placés hors du répertoire de diffusion, reportez-vous aux instructions de migration de l'assistant de déploiement.

Vous pouvez créer et monter un système de fichiers distinct pour le répertoire de diffusion défini par l'utilisateur. Le fichier zip de l'assistant de déploiement généré doit être transféré vers ce répertoire et dézippé à l'aide de l'utilitaire DWUnzip. Le serveur Web doit inclure une instruction d'alias spécifique au répertoire de diffusion défini par l'utilisateur.

Vous pouvez accéder à la page via l'URL qui indique l'alias de l'emplacement de diffusion défini par l'utilisateur. Par exemple, si le répertoire de diffusion est /usr/lpp/HOD/publish et que l'alias est userpublish, l'URL permettant d'accéder à la page du client serait *http://<nom_serveur>/userpublish/<nom_page>.html*.

Remarques relatives à la migration sous z/OS

Lorsque vous effectuez une mise à niveau d'un niveau antérieur de Host On-Demand vers Host On-Demand version 13.0, vous devez prendre en compte les personnalisations précédentes. Une fois que Host On-Demand version 13.0 est installé, vous pouvez copier votre répertoire privé précédent dans le nouveau répertoire privé pour l'ensemble des groupes, utilisateurs et sessions précédemment définis. Utilisez ensuite la commande *pax* ou *tar* pour copier votre répertoire privé existant dans le système de fichiers Host On-Demand version 13.0. Voir «Sauvegarde du répertoire privé».

Comme pour les clients précédents créés avec l'assistant de déploiement, vous devez installer l'assistant de déploiement sur un ordinateur Windows. Ensuite, éditez et redéployez le client sur le serveur Host On-Demand version 12.0. Voir «Installation de l'assistant de déploiement à partir du serveur z/OS».

Sauvegarde du répertoire privé

Vous pouvez sauvegarder votre répertoire privé à l'aide des commandes *pax* ou *tar*. Supposons que le répertoire privé en cours pour Host On-Demand version 11 est */usr/lpp/HOD/hostondemand/private* :

1. A partir du système de fichiers de Host On-Demand version 11, accédez au répertoire privé : *cd /usr/lpp/HOD/hostondemand/private*.
2. Archivez ce répertoire privé dans un répertoire temporaire /tmp. L'option *-z* compresse le fichier ; l'option *-v* fournit une liste des fichiers et sous-répertoires archivés (facultatif) : *pax -wzvf /tmp/private.pax.Z **.
3. Copiez le fichier private.tar.Z dans le répertoire */tmp* du système pour Host On-Demand version 12, s'il s'agit d'un système différent.
4. A partir du système hiérarchique de fichiers de Host On-Demand version 12.0, accédez au répertoire privé d'où le fichier sera extrait : *cd /usr/lpp/HOD/hostondemand/private*.
5. Exécutez la commande *pax* pour extraire le fichier private.pax.Z. L'option *-z* spécifie un fichier compressé ; l'option *-v* fournit une liste des fichiers et sous-répertoires extraits (facultatif) : *pax -rzvf /tmp/private.pax.Z*.

Installation de l'assistant de déploiement à partir du serveur z/OS

L'assistant de déploiement réside généralement sur une machine Windows au cours de l'installation du produit. Sous z/OS, un téléchargement est fourni pour que vous puissiez installer l'assistant de déploiement sous Windows et ainsi

générer des pages de client pour le serveur Host On-Demand sous z/OS. Pour installer l'assistant de déploiement à partir du serveur z/OS, procédez comme suit :

1. Utilisez FTP dans le binaire pour replacer ce fichier d'un poste de travail Windows : */usr/lpp/HOD/hostondemand/HOD/depwiz/DW.zip*.
2. Extrayez le fichier zip dans un dossier.
3. Pour démarrer l'installation, accédez à *<dossier>\AssistantDéploiement\disque1* dans l'Explorateur.
4. Cliquez deux fois sur imLauncherWindows.bat pour lancer l'interface utilisateur d'Installation Manager.
5. Suivez les instructions pour terminer l'installation.

Une fois l'assistant de développement installé, vous pouvez le lancer. Accédez à **Démarrer** > **Tous les programmes** > **Assistant de déploiement IBM Host On-Demand**.

Chapitre 15. Configuration de Host On-Demand sur un système IBM System i

Après avoir installé Host On-Demand sur la plateforme IBM System i, configurez le logiciel comme suit :

- Pour configurer le gestionnaire de services, suivez les instructions de la section «Configuration, démarrage et arrêt du gestionnaire de services Host On-Demand sur un système IBM System i».
- Pour utiliser l'assistant de déploiement avec un système IBM System i, suivez les instructions de la section «Utilisation de l'assistant de déploiement avec IBM System i», à la page 124.
- Pour configurer la sécurité, suivez les instructions de la section «Configuration des serveurs IBM System i pour la connexion sécurisée», à la page 124.
- Pour connaître les exigences liées à la prise en charge des caractères Unicode utilisant les identificateurs de jeux de caractères codés, reportez-vous à «Support Unicode pour i/OS et OS/400», à la page 128.

Configuration, démarrage et arrêt du gestionnaire de services Host On-Demand sur un système IBM System i

Les commandes suivantes peuvent être utilisées à partir de la ligne de commande IBM iv7r1 ou OS/400.

Configuration

Vous pouvez utiliser le fichier script NCServiceManager-OS400.sh pour configurer le gestionnaire de services. NCServiceManager-OS400.sh se trouve dans le répertoire suivant sous IBM System i :

```
répertoire_installation_HOD>/lib/samples/NCServiceManager/.
```

Pour configurer les paramètres du gestionnaire de services, effectuez les tâches suivantes :

1. Accédez au répertoire */<répertoire_installation_HOD>/lib/samples/NCServiceManager/*. Ici, *<répertoire_installation_HOD>* représente l'emplacement ou le chemin d'installation de Host On Demand. Par exemple, */QIBM/ProdData/HostOnDemand/*.
2. Ouvrez le fichier NCServiceManager-OS400.sh.
3. Vérifiez que les variables d'exécution sont correctes et qu'elles correspondent à votre environnement. Si ce n'est pas le cas, modifiez leurs valeurs par défaut. Les variables d'environnement sont les suivantes :
   - • Emplacement de l'environnement d'exécution Java : **JAVA_ENGINE**

     Mettez à jour la valeur de JAVA_ENGINE en lui affectant le chemin d'accès complet ou l'emplacement de la machine virtuelle Java installée sur le système. Il doit s'agir de Java version 6 ou ultérieure. JAVA_ENGINE doit pointer sur *<installation_java>/bin/java* dans le répertoire d'installation Java.
   - • Emplacement du répertoire de diffusion Host On-Demand sur le serveur : **MY_HOD_DIRECTORY**

     Vérifiez, et mettez à jour s'il y a lieu, la valeur de MY_HOD_DIRECTORY en lui affectant le chemin d'accès complet du répertoire d'installation HostOnDemand. Cet emplacement doit être le répertoire d'installation de

Host On-Demand, qui contient les dossiers /bin, /lib et d'autres dossiers de Host On-Demand. En général, cette valeur est mise à jour une seule fois au moment de l'installation. Par exemple, */QIBM/ProdData/HostOnDemand*.

- • Chemins cible spécifiés dans le fichier de commandes : **MY_PUBLISHED_DIRECTORY**

  Vérifiez, et mettez à jour s'il y a lieu, la valeur de MY_PUBLISHED_DIRECTORY en lui affectant le chemin d'accès complet du répertoire de diffusion Host On-Demand. En général, il s'agit du répertoire *<installation_HOD>/HOD*, où *<installation_HOD>* correspond au répertoire d'installation Host On-Demand.

4. Vérifiez que NCServiceManager-OS400.sh dispose des droits d'exécution nécessaires et des droits d'écriture sur les répertoires de l'installation Host On Demand sur le serveur.

Démarrage

Pour démarrer le gestionnaire de services Host On-Demand, exécutez NCServiceManager-OS400.sh pour qu'il démarre et continue de s'exécuter en arrière-plan.

Pour démarrer le gestionnaire de services sur un serveur IBM iSeries, vous pouvez, entre autres méthodes, soumettre un travail en invoquant l'utilitaire IBM PASE for System i pour exécuter le script. Contactez votre administrateur IBM iSeries afin de connaître les meilleures pratiques pour soumettre un travail adapté aux exigences et à la configuration de votre iSeries.

Exemple de commande de soumission d'un travail :

```
sbmjob cmd(call pgm(qp2shell) parm('/QOpenSys/usr/bin/-sh' '/QIBM/ProdData/HostOnDemand/lib/samples/I
```

Arrêt

Pour arrêter le gestionnaire de services, terminez le travail sur le système iSeries. Pour obtenir des informations sur la méthode appropriée pour arrêter le service, contactez votre administrateur iSeries.

L'une de ces méthodes est la suivante :

1. Entrez **WRKACTJOB** pour ouvrir une liste des travaux actifs.
2. Dans le menu **Work with Active Jobs**, le travail du gestionnaire de services Host On-Demand apparaît dans la liste sous le nom de fonction *JVM-NCServiceM*. Faites défiler le menu jusqu'à cette entrée de travail et sélectionnez l'option **Work with Active Jobs**, (en général l'option 5).
3. Sélectionnez l'option **End job**. Pour cela, entrez *41* pour arrêter le travail, puis appuyez sur le bouton **Entrée**. Le travail du gestionnaire de services se termine et le gestionnaire de services s'arrête.

Vérification du statut du serveur Host On-Demand

Pour déterminer si le gestionnaire de services est en cours d'exécution, il faut vérifier si le programme Java NCServiceManager, lancé au moyen du script NCServiceManager-OS400.sh, est en cours d'exécution ou non. La méthode permettant de vérifier le statut du serveur peut varier selon la méthode utilisée pour démarrer le gestionnaire de services.

Dans l'exemple ci-dessus, le gestionnaire de services est démarré en soumettant un travail qui exécute le script NCServiceManager-OS400.sh. Dans ce cas, deux méthodes s'offrent à vous pour vérifier le statut :

1. Utiliser la commande WRKACTJOB pour vérifier le statut :
   a. Entrez la commande :
      ```
      WRKACTJOB
      ```
      pour afficher une liste des travaux actifs.
   b. Dans le menu Work with Active Jobs, le travail du gestionnaire de services Host On-Demand apparaît dans la liste sous le nom de fonction **JVM-NCServiceM**. Utilisez le bouton **Page suivante** ou **Page précédente** pour faire défiler le menu jusqu'à l'entrée du travail, puis entrez le numéro d'option correspondant au travail **Work with Active Jobs** (en général l'option 5).
   c. Utilisez les options du menu pour vérifier le statut du travail.
2. Interroger le statut du processus dans la ligne de commande.

Dans l'exemple de «Démarrage», à la page 122, le script NCServiceManager-OS400.sh est exécuté en appelant IBM PASE for System i (qp2shell) dans la commande SBMJOB. Dans ce cas, les étapes suivantes peuvent également vous permettre de vérifier le statut :

1. Sous IBM System i, connectez-vous à une ligne de commande d'écran vert.
2. Entrez l'environnement de l'interpréteur de commandes PASE. Sur la ligne de commande d'écran vert, entrez la commande suivante :
   ```
   call qp2term
   ```
   .
3. Sur l'interpréteur de commandes PASE, entrez la commande suivante :
   ```
   ps –ef | grep NCServ
   ```
   .

   Remarque : *NCServiceManager* est le nom du programme Java qui exécute le gestionnaire de services.

Si la commande détecte que le gestionnaire de services est en cours d'exécution, le résultat ressemble à ce qui suit :

```
 $
> ps -ef | grep NCServ
  kushald 3146    1   0 15:23:30      -  0:00 /QIBM/ProdData/OS400/Java400/jFr
  omPASE java -classpath .:sm.zip:ibmjndi.jar:jndi.jar:jsdk.jar:ods.jar:jt400.j
  ar -Djava.net.preferIPv4Stack=true -DFIPS=on com.ibm.eNetwork.HODUtil.service
  s.admin.NCServiceManager /QIBM/ProdData/HostOnDemand
  $
```

Remarque : L'interpréteur de commandes PASE est sensible à la casse. Il est donc important de respecter la casse préconisée dans la commande (étape c).

Gestion des certificats

Les fonctions de gestion de certificats peuvent être exécutées à l'aide de l'utilitaire P12Keyring fourni par Host On-Demand. Ces fonctions sont un moyen de créer et de déployer facilement une base de données de fichiers de clés SSL. Utilisez cette option pour manipuler des certificats SSL dans l'un des fichiers de clés Host

On-Demand. Voir Chapitre 4, «Planification de la sécurité», à la page 19 pour obtenir des informations générales relatives aux sessions SSL.

Des informations sur l'utilitaire P12Keyring et sur son utilisation sont disponibles dans l'Annexe C. Utilitaire P12Keyring.

Pour afficher quelques exemples de commandes, utilisez le lien How to create, add or convert certificates to CustomizedCAs.p12 file on z/OS for Host On-Demand.

Démarrage du programme de groupage d'informations

Si vous souhaitez obtenir une assistance auprès du service de support IBM, utilisez le fichier script du programme de groupage d'informations déjà disponible pour rassembler les informations relatives à la configuration Host On-Demand.

Pour obtenir des informations d'utilisation, reportez-vous à la section Running the Information Bundler dans le document Host On-Demand version 10.

Création d'une table de définition d'imprimante Host On-Demand

Créez une table de définition d'imprimante personnalisée pour les sessions d'imprimante Host On-Demand (3270). Pour utiliser cette fonction, reportez-vous à la section Compiling a printer definition table pour un serveur iSeries.

Une définition d'imprimante personnalisée peut s'avérer nécessaire si vous disposez d'un format de papier spécial ou si l'imprimante n'est pas prise en charge. Les options suivantes sont indisponibles sur Host On-Demand version 13.0 :

Utilisation de l'assistant de déploiement avec IBM System i

Pour utiliser l'assistant de déploiement afin de déployer des écrans vers un serveur Host On-Demand basé sur IBM System i, procédez de la manière suivante :

1. A partir d'un poste de travail Windows, mappez une unité réseau au répertoire `/qibm` sur le système IBM System i, qui est le serveur Host On-Demand. Pour plus d'informations, reportez-vous au site Web IBM System i.
2. Téléchargez l'image d'installation de l'assistant de déploiement depuis un serveur Host On-Demand version 12 déjà installé. Accédez à HODMain.html (par exemple, *http://hodserver.name.com/hod/HODMain.html*, puis cliquez sur **Image d'installation de l'assistant de déploiement pour Windows**.
3. Pour installer l'assistant de déploiement, reportez-vous aux instructions d'installation. Vous pouvez l'exécuter sans avoir à installer complètement le serveur Host On-Demand.
4. Choisissez les fonctions et sélections personnalisées.
5. Sauvegardez le fichier HTML personnalisé dans l'unité réseau mappée (par exemple, *y:\ProdData\hostondemand\hod\myweb*).
6. A l'aide d'un navigateur, testez le fichier (par exemple, *http://iSeries.name.com/hod/myweb.html*).

Configuration des serveurs IBM System i pour la connexion sécurisée

Si vous utilisez des certificats autosignés ou émis par une autorité de certification (AC) non répertoriée dans la liste des AC connues, utilisez l'utilitaire P12Keyring pour configurer le fichier de clés CustomizedCAs. Pour plus de détails, reportez-vous à la section Annexe C. Utilitaire P12Keyring.

Pour configurer un fichier de clés CustomizedCAs, effectuez les étapes suivantes :

1. Assurez-vous que Java est installé dans le système.
2. Ouvrez une ligne de commande UNIX/AIX. Par exemple, un interpréteur de commandes QSHELL ou IBM i PASE.
3. Accédez au dossier de diffusion Host on-Demand dans le répertoire d'installation Host On-Demand. Il s'agit généralement de */QIBM/ProdData/HostOnDemand/HOD/*.
4. Entrez la commande

   ```
   java -classpath .:votre_répertoire_d'installation/lib/sm.zip com.ibm.hod5sslight.tools.P12Keyr
   ```

   . Cette opération peut prendre plusieurs minutes. Si un mot de passe vous est demandé, entrez *hod* et appuyez sur **Entrée**.
5. Sélectionnez le numéro de certificat correspondant à l'Autorité de certification (AC) que vous souhaitez ajouter au fichier de clés. Veillez à bien ajouter le certificat de l'AC et non le certificat du site. Si le port ne répond pas, voir la section Configuration des serveurs IBM i 7.1 pour la connexion sécurisée.
6. Reprenez les étapes 3 à 5 pour chaque serveur cible.

Pour afficher le contenu du fichier de clés CustomizedCAs, procédez comme suit :

1. Assurez-vous que Java est installé dans le système.
2. Ouvrez un interpréteur de commandes basé sur Linux, par exemple un interpréteur de commandes QSHELL ou IBM i PASE.
3. Accédez au dossier de diffusion Host on-Demand dans le répertoire d'installation Host On-Demand. Il s'agit généralement de */QIBM/ProdData/HostOnDemand/HOD/*.
4. Entrez la commande

   ```
   java -classpath.:votre_répertoire_d'installation/lib/sm.zip com.ibm.hod5sslight.tools.P12Keyri
   ```

   .

Installation et configuration de Host On-Demand avec TLS sous i/OS et OS/400

La liste suivante fournit une présentation générale des étapes requises pour l'installation et la configuration de Host On-Demand avec TLS :

1. Vérifiez si les configurations logicielle et système requises sont respectées.
2. Installez tous les produits logiciels IBM System i nécessaires. Pour plus de détails, reportez-vous à la documentation relative à IBM System i.
3. Installez tous les PTF requis. Les derniers PTF sont disponibles sur le portail de support d'IBM eServer System i.
4. Installez et configurez IBM HTTP Server ou IBM Application Server. Pour plus de détails, reportez-vous à la documentation relative au produit.
5. Créez une autorité de certification (CA) à partir du Gestionnaire de certificats numériques sur le serveur d'administration IBM ou procurez-vous une autorité de certification publique. Pour plus de détails, reportez-vous à la documentation relative à IBM System i.
6. Configurez TLS sur IBM HTTP Server ou IBM Application Server. Pour plus de détails, reportez-vous à la documentation relative au produit.
7. Configurez Host On Demand avec TLS. Pour plus de détails, reportez-vous à la Configuration de TLS (Transport Layer Security) dans l'aide en ligne.

Configuration d'un serveur Telnet pour les connexions sécurisées

Dans l'IBM Knowledge Center, accédez aux rubriques relatives aux systèmes IBM System i et recherchez *TLS* pour connaître les étapes nécessaires à l'activation de TLS. Vous devrez répéter ces étapes chaque fois que vous souhaiterez utiliser un système IBM System i7 dont vous voulez sécuriser les connexions.

Configuration du fichier de clés CustomizedCAs de Host On-Demand

Si vous utilisez des certificats autosignés ou émis par une autorité de certification (AC) non répertoriée dans la liste des AC connues, utilisez l'utilitaire P12Keyring pour configurer le fichier de clés CustomizedCAs. Pour plus de détails, reportez-vous à la section Annexe C. Utilitaire P12Keyring.

Pour configurer un fichier de clés CustomizedCAs, procédez comme suit :

1. Assurez-vous que Java est installé dans le système.
2. Ouvrez un interpréteur de commandes basé sur Linux, par exemple un interpréteur de commandes QSHELL ou IBM i PASE.
3. Accédez au dossier de diffusion Host on-Demand dans le répertoire d'installation Host On-Demand. Il s'agit généralement de */QIBM/ProdData/HostOnDemand/HOD/*.
4. Entrez la commande

   ```
   java -classpath .:votre_répertoire_d'installation/lib/sm.zip com.ibm.hod5sslight.tools.P12Keyring
   ```

   Cette opération peut prendre plusieurs minutes. Si un mot de passe vous est demandé, entrez hod et appuyez sur **Entrée**.
5. Sélectionnez le numéro de certificat correspondant à l'Autorité de certification (AC) que vous souhaitez ajouter au fichier de clés. Veillez à bien ajouter le certificat de l'AC et non le certificat du site. Si le port ne répond pas, voir la section Configuration des serveurs IBM System i pour la connexion sécurisée.
6. Reprenez les étapes 3 à 5 pour chaque serveur cible.

Pour afficher le contenu du fichier de clés CustomizedCAs, procédez comme suit :

1. Assurez-vous que Java est installé dans le système.
2. Ouvrez un interpréteur de commandes basé sur Linux, par exemple un interpréteur de commandes QSHELL ou IBM i PASE.
3. Accédez au dossier de diffusion Host on-Demand dans le répertoire d'installation Host On-Demand. Il s'agit généralement de */QIBM/ProdData/HostOnDemand/HOD/*.
4. Entrez la commande

   ```
   java -classpath.:votre_répertoire_d'installation/lib/sm.zip com.ibm.hod5sslight.tools.P12Keyring
   ```

   .

Si vous disposez de plusieurs machines IBM System i et que vous souhaitez créer un certificat unique pour toutes, optez pour la certification croisée. Pour plus d'informations sur la certification croisée, reportez-vous aux rubriques Managing Security, Cryptographic Services APIs et Application System/400 Cryptographic Support/400 Version 3.

Authentification du client

Pour optimiser la sécurité, optez pour TLS avec authentification du client afin de contrôler de façon plus stricte les utilisateurs pouvant accéder à Telnet sur votre système via Internet. Par exemple, vous pouvez configurer le serveur Telnet pour qu'il n'autorise l'authentification que si le certificat client a été émis par votre IBM System i (via le gestionnaire de certificats numériques).

Les certificats client présentent une période de validité limitée (par exemple, 90 jours). Lorsque le certificat expire, l'utilisateur doit procéder au téléchargement du certificat client pour continuer. Ce processus nécessite un ID utilisateur et un mot de passe IBM System i valides.

Certains logiciels client Telnet ne peuvent pas effectuer d'authentification des clients. Lorsqu'elles sont activées, les connexions Telnet compatibles avec TLS établies avec IBM System i nécessitent un certificat utilisateur.

Pour plus d'informations, reportez-vous au site Web IBM System i.

Configuration du proxy OS/400 Host On-Demand pour les connexions sécurisées

Le proxy OS/400 peut être configuré pour chiffrer le transfert de fichiers et les connexions Database On-Demand. Pour cela, vous devez installer les logiciels suivants sur chaque système IBM System i cible :

- IBM Cryptographic Access Provider
- IBM Client Encryption
- Serveurs hôtes
- Gestionnaire de certificats numériques

Définition des droits d'accès utilisateur TLS

Vous devez contrôler les droits des utilisateurs sur les fichiers. Pour répondre aux responsabilités juridiques TLS, vous devez modifier les droits d'accès du répertoire contenant les fichiers TLS afin d'en contrôler l'accès utilisateur. Pour modifier ces droits d'accès, procédez comme suit :

1. Entrez la commande `wrklnk '/QIBM/ProdData/HTTP/Public/jt400/*'`
2. Sélectionnez l'option 9 dans le répertoire .
   a. Assurez-vous que *PUBLIC dispose du droit de niveau *EXCLUDE.
   b. Accordez aux utilisateurs qui doivent accéder aux fichiers TLS le droit de niveau *RX sur le répertoire. Vous pouvez accorder des droits à des utilisateurs individuels ou à des groupes d'utilisateurs. L'accès aux fichiers TLS ne peut pas être refusé aux utilisateurs disposant du droit spécial de niveau *ALLOBJ.

Fonction de serveur Web sécurisé

Le serveur Host On-Demand utilise le serveur Web pour télécharger des objets de programme sur le navigateur. Ces informations peuvent être chiffrées, mais les performances peuvent s'en trouver très réduites.

Le port par défaut pour la fonction de serveur Web sécurisé est 443. Si ce port n'est pas activé, le port 80 est utilisé. Pour activer la fonction de serveur Web sécurisé, procédez comme suit :

1. A partir d'un navigateur Web, entrez : `http://<nom.serveur>:2001` (où <nom.serveur> est le nom d'hôte TCP/IP de votre IBM System i). Si vous ne

pouvez pas vous connecter, démarrez le serveur HTTP à l'aide des commandes i/OS et OS/400 suivantes :

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

2. Entrez le profil et le mot de passe d'utilisateur i/OS ou OS/400 (lorsque vous y êtes invité). Vous devez disposer des droits de niveau *ALLOBJ et *SECADM pour effectuer les opérations de configuration restantes.
3. Cliquez sur IBM HTTP Server pour AS/400.
4. Cliquez sur Configuration et administration.
5. Cliquez sur Configurations.
6. Sélectionnez la configuration CONFIG dans la liste.
7. Cliquez sur Configuration de la sécurité.
8. Pour les options Autoriser les connexions HTTP et Autoriser les connexions TLS :
   - Numéro de port (443)
   - Sélectionnez l'authentification client TLS Aucun(e).
   - Sélectionnez Validation.
9. Cliquez sur le bouton Tâches AS/400 situé dans la partie inférieure gauche de l'écran.
10. Cliquez sur Gestionnaire de certificats numériques.
11. Cliquez sur Certificats du système.
12. Cliquez sur Utiliser les applications sécurisées.
13. Cliquez sur QIBM_HTTP_SERVER_CONFIG, puis sur Utiliser les certificats du système.
14. Cliquez sur Affecter un nouveau certificat.
15. Terminez l'instance du serveur HTTP d'administration à l'aide des commandes i/OS et OS/400 suivantes :

    ```
    ENDTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)
    ```
16. L'instance HTTP s'arrête au bout de 10 secondes.
17. Démarrez l'instance du serveur HTTP d'administration à l'aide des commandes i/OS et OS/400 suivantes :

    ```
    STRTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)
    ```
18. A partir d'un navigateur Web, entrez `https://`*`nom.serveur`*`/hod/hodmain.html` (où *nom.serveur* est le nom d'hôte TCP/IP de votre IBM System i).

Pour plus d'informations sur un grand nombre de rubriques d'IBM System i, voir Fichiers PDF et manuels IBM i.

Support Unicode pour i/OS et OS/400

Informations générales

Dans une session écran 5250, Host On-Demand prend en charge l'affichage des données Unicode contenues dans des zones identifiées par des CCSID (Coded Character Set Identifiers). Pour plus d'informations, voir Prise en charge d'Unicode pour i/OS et OS/400 par des CCSID.

Informations de programmation de l'hôte

Pour obtenir des informations sur la programmation de l'hôte, reportez-vous au site Web d'IBM System i.

Chapitre 16. Déploiement de Host On-Demand avec WebSphere Portal

L'accès à Host On-Demand peut se faire par le biais d'un fichier HTML. Les utilisateurs ont également la possibilité de recourir à l'un des composants de WebSphere Portal, Portal Server. Portal Server offre une structure permettant l'ajout d'extensions de contenu connues sous le nom de *portlets* à un site Web. Les portlets sont des applications exécutables dans Portal Server. Ils permettent d'organiser le contenu issu de sources différentes (sites Web, courriers électroniques ou applications métier) et de l'afficher dans un fichier HTML unique au sein d'une fenêtre de navigateur. Les fichiers WAR générés par l'assistant de déploiement qui permet de lancer les sessions Host On-Demand, peuvent être déployés comme des portlets afin de permettre aux utilisateurs d'accéder à Host On-Demand via l'interface du portail. Si vous envisagez d'utiliser Host On-Demand et le serveur de portail conjointement avec un pare-feu, reportez-vous à «Utilisation de Host On-Demand avec un pare-feu», à la page 30. De même, si vous envisagez d'utiliser les fonctions de sécurité de WebSphere Portal, comme l'ID de portail de l'utilisateur ou le coffre d'accréditations du serveur de portail, reportez-vous à *Web Express Logon Reference*.

Host On-Demand et Portal Server doivent être installés pour pouvoir exécuter un portlet Host On-Demand.

Fonctionnement de Host On-Demand avec Portal Server

La figure 8 illustre le fonctionnement de Host On-Demand avec Portal Server.

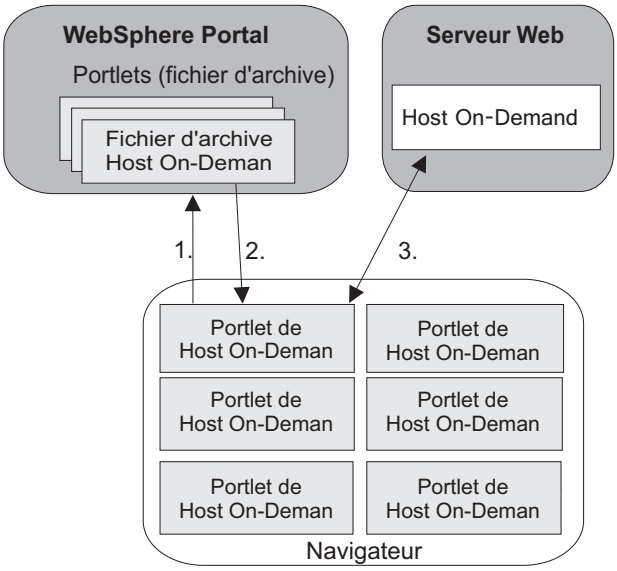

Figure 8. Fonctionnement de Host On-Demand avec Portal Server

1. Un utilisateur se connecte au portail par l'intermédiaire d'un navigateur et obtient l'autorisation d'accès grâce à un ID utilisateur et un mot de passe.
2. L'ensemble des portlets personnalisés de l'utilisateur est téléchargé sur son poste et affiché dans le navigateur.

3. Si l'utilisateur a configuré un portlet Host On-Demand, Host On-Demand démarre. Cela permet à l'utilisateur de disposer de la totalité des fonctionnalités proposées par Host On-Demand dans la fenêtre du portlet, y compris la possibilité de démarrer des sessions tout en effectuant d'autres tâches Host On-Demand.

Utilisation des clients Host On-Demand avec Portal Server

Pour utiliser Host On-Demand avec Portal Server, un portlet Host On-Demand est nécessaire. Vous avez la possibilité de créer rapidement et facilement des portlets personnalisés à l'aide de l'assistant de déploiement. Reportez-vous à l'aide en ligne de l'assistant de déploiement pour obtenir plus de détails sur la création de portlets. Vous pouvez également télécharger des échantillons de portlets Host On-Demand à partir du site Host On-Demand Service Key sur la page de régénération de fabrication Host On-Demand sous Tools and Utilities.

Une fois le portlet personnalisé créé ou le modèle obtenu, vous pouvez l'importer directement dans Portal Server comme tout autre portlet. Pour plus d'informations, reportez-vous à WebSphere Portal for Multiplatforms.

Limitations liées à l'accès à Host On-Demand via un portlet

L'environnement de portail prend en charge la fonctionnalité Host On-Demand complète avec les restrictions suivantes :

- Même si Host On-Demand prend en charge les navigateurs client Mac OS, ceux-ci ne sont pas recommandés pour les environnements de portail. Pour plus d'informations les navigateurs pris en charge, reportez-vous à WebSphere Portal for Multiplatform.
- Si vous exécutez plusieurs portlets sur une même page WebSphere Portal, appliquez les recommandations suivantes :
  - Utilisez le modèle de configuration HTML.
  - Utilises Java lorsque vous configurez les portlets en clients en cache.
  - Configurez vos portlets pour qu'ils soient téléchargés ou des clients en cache et non une association des deux.
- Lorsque vous utilisez un navigateur compatible Java pour les sessions qui sont configurées pour s'exécuter dans un navigateur différent et que la valeur du paramètre AssociateEmbeddedMenuBar est False, le menu des sessions hôte 3270 et 5250 s'affiche en incrustation. Pour les sessions d'impression hôte et FTP, le menu en incrustation ne s'affiche pas par défaut. Pour qu'il s'affiche, vous devez configurer les sessions pour qu'elles se lancent dans une fenêtre distincte.
- Pour incorporer la barre de menus à la session Host On-Demand qui est configurée pour *ne pas* s'exécuter dans une fenêtre distincte, vous devez disposer d'un navigateur Java et définir la valeur par défaut True pour le paramètre AssociateEmbeddedMenuBar. Dans les circonstances suivantes, la barre de menus des sessions hôte 3270, 5250, VT et CICS s'affiche sous la forme d'un menu en incrustation (et non incorporée à la session) :
  - Le navigateur client est activé avec Java et le paramètre AssociateEmbeddedMenuBar est défini sur false.

  Si la session Host On-Demand est configurée pour démarrer dans une fenêtre distincte, la barre de menus est toujours associée à la fenêtre de la session et ne peut s'afficher sous la forme d'un menu en incrustation.

- Si le portlet utilise la mise en cache pour Host On-Demand (configurée dans l'assistant de déploiement), chaque poste utilisé pour accéder au portlet met en cache le client Host On-Demand.
- La mise en signets Host On-Demand ne fonctionne pas en environnement de portail.
- Si vous ne configurez aucune taille d'applet dans l'assistant de déploiement, la valeur par défaut Moyenne est automatiquement définie.
- Lorsque le portlet Host On-Demand est exécuté, des messages d'avertissement peuvent s'afficher dans la console Java, par exemple : `java.io.FileNotFoundException`. Les messages sont générés par un nom de fichier archive invalide que le portlet Host On-Demand utilise pour activer plusieurs portlets Host On-Demand à exécuter sur une même page de portail. Ces messages n'ont aucune incidence sur les performances du portlet, par conséquent n'en tenez pas compte.

Considérations particulières relatives à l'utilisation d'un portlet Host On-Demand

Lorsque vous utilisez Host On-Demand avec Portal Server, vous devez tenir compte des questions suivantes :

- **Sessions Host On-Demand lorsque l'utilisateur se déconnecte de Portal Server.** Host On-Demand s'exécute comme une applet sur le poste de l'utilisateur et par conséquents ne sait pas à quel moment l'utilisateur se déconnecte de Portal Server. Si la session s'exécute dans une fenêtre distincte (option par défaut), la session Host On-Demand se poursuit tant que l'utilisateur ne ferme pas la session ou le navigateur. Si la session Host On-Demand s'exécute dans une fenêtre Portal Server imbriquée et que l'utilisateur se déconnecte de Portal Server, la session semble se terminer, bien que la connexion reste active tant que la fenêtre du navigateur n'est pas fermée. Nous conseillons vivement aux utilisateurs de fermer la fenêtre du navigateur au moment où ils se déconnectent de Portal Server. De plus, vous devez configurer un délai d'inactivité de session pour vos sessions.
- **Délai d'inactivité de session**. Par défaut, Host On-Demand ne déclenche pas automatiquement de délai d'inactivité des connexions de session. Toutefois, lors de l'exécution d'un portlet, il peut être bénéfique de définir un délai d'inactivité des sessions afin de réduire la consommation de ressources. Ce délai d'inactivité peut être défini pour la plupart des émulateurs, dont l'écran et les sessions d'impression 3270, l'écran et les sessions d'impression 5250 et VT. Vous pouvez activer et définir le paramètre de délai d'inactivité en minutes pour chaque session dans la `fenêtre Connexion` des propriétés de session.
- **Installation de WebSphere Portal et Host On-Demand sur des serveurs différents**. Si vous installez WebSphere Portal et Host On-Demand sur des serveurs différents, certains navigateurs risquent de vous signaler une atteinte à la sécurité lors de l'accès au portlet Host On-Demand. Cet incident est dû au fait que certaines fonctionnalités de Host On-Demand s'appuient considérablement sur l'interaction entre Java (à partir du serveur Host On-Demand) et JavaScript (à partir de WebSphere Portal), et certains navigateurs n'autorisent pas cette interaction car Java et JavaScript proviennent de serveurs différents. Une solution consiste à utiliser la mise en Proxy pour faire croire au navigateur que WebSphere Portal et Host On-Demand se trouvent sur le même serveur. Voici un exemple de la procédure à suivre pour définir une mise en Proxy sur IBM HTTP Server ou sur le serveur Apache :

1. Configurez "l'URL du serveur HOD" du portlet Host On-Demand (hodCodeBase) pour qu'elle pointe sur l'hôte hébergeant WebSphere Portal, en précisant /hod/ (http://portal.company.com/hod, par exemple).
2. Supprimez le signe # devant la phrase commençant par LoadModule proxy_module dans le fichier httpd.config pour que celle-ci n'apparaisse plus en commentaire.
3. Ajoutez une règle ProxyPass au fichier httpd.conf pour convertir la demande d'URL adressée au serveur HOD en une requête adressée au véritable serveur Host On-Demand (ProxyPass /hod/ http://hod.société.com/hod/, par exemple).
4. Redémarrez le serveur Web.

•

Désormais, le navigateur du client va demander les fichiers Host On-Demand à partir du même hôte que le portail, mais ces requêtes vont être redirigées en interne par le serveur Web vers l'emplacement en cours de votre installation Host On-Demand.

- **Mise en cache ou non ?** Les paramètres par défaut de l'assistant de déploiement prévoient la mise en cache de Host On-Demand sur chaque poste du client. Vous êtes nombreux à apprécier cette option de Host On-Demand car elle permet d'installer de manière effective tous les codes nécessaires sur le poste du client sans vous obliger à passer par le réseau à chaque fois que vous accédez à un fichier HTML ou à un portlet. Cependant, tous les utilisateurs de Portal Server ne sont peut-être pas familiarisés avec la mise en cache, et peut-être choisirez-vous de ne pas utiliser cette option.
- **Choix du modèle de l'assistant de déploiement**. Le modèle que vous choisissez pour votre portlet (Serveur de configuration, HTML ou Mixte) indique l'emplacement de configuration de vos sessions et détermine le mode de sauvegarde des modifications effectuées par l'utilisateur. Bien que Host On-Demand traite les portlets de la même façon que les fichiers HTML, tenez compte des caractéristiques suivantes lorsque vous décidez de la manière dont vous allez configurer votre portlet :
  - Modèle HTML : Ce modèle est le modèle de configuration recommandé pour les portlets Host On-Demand. Il n'a aucune dépendance sur le serveur de configuration Host On-Demand. Si les utilisateurs sont autorisés à effectuer des mises à jour, ces dernières sont stockées partie intégrante de la configuration du portail WebSphere, elles ne sont pas enregistrées sur la machine locale de l'utilisateur. Ce qui permet aux utilisateurs de passer d'une machine à l'autre et de toujours avoir accès aux mises à jour.

    

    Les préférences utilisateur sont stockées dans WebSphere Portal uniquement si vous avez accordé aux utilisateurs les droits d'accès appropriés au portlet et à la page Web qui permet d'accéder au portlet. Les utilisateurs WebSphere Portal doivent disposer du droit d'accès Privileged User, Editor, Manager ou Administrator. Pour plus d'informations sur l'octroi des droits d'accès aux utilisateurs, reportez-vous à la documentation WebSphere Portal.

  - Modèle basé sur le serveur de configuration : Ce modèle requiert que les utilisateurs accèdent au serveur de configuration Host On-Demand. Il permet aux utilisateurs de passer d'une machine à une autre et de toujours avoir accès aux modifications de session qu'ils ont effectuées ; cependant, cela implique que les utilisateurs doivent s'authentifier via le serveur de configuration Host On-Demand et WebSphere Portal.
  - Modèle mixte : Ce modèle requiert que les utilisateurs aient accès au serveur de configuration Host On-Demand afin d'obtenir les configurations de session

initiales. Du fait que les modifications sont stockées en tant que partie intégrante de la configuration de WebSphere Portal et qu'elles ne sont pas enregistrées localement, ce modèle permet aux utilisateurs de passer d'une machine à une autre et de toujours avoir accès aux modifications de session qu'ils ont effectuées ; cependant, cela implique que les utilisateurs doivent s'authentifier via le serveur de configuration Host On-Demand et WebSphere Portal.

Les préférences utilisateur sont stockées dans WebSphere Portal uniquement si vous avez accordé aux utilisateurs les droits d'accès appropriés au portlet et à la page Web qui permet d'accéder au portlet. Les utilisateurs WebSphere Portal Version 5 doivent disposer du droit d'accès Privileged User, Editor, Manager ou Administrator. Pour plus d'informations sur l'octroi des droits d'accès aux utilisateurs, reportez-vous à la documentation WebSphere Portal.

- **Configuration d'autres paramètres**. Lorsque vous utilisez les portlets Host On-Demand, vous pouvez souhaiter configurer les paramètres supplémentaires suivants pour obtenir la présentation souhaitée sur la page de portail :
  - Démarrage automatique : Affectez Oui à cette option, dans la fenêtre Préférences > Options de démarrage des propriétés de session pour autoriser le portlet Host On-Demand à démarrer automatiquement.
  - Démarrage dans une fenêtre distincte : Affectez Non à cette option dans la fenêtre Préférences > Options de démarrage des propriétés de session pour autoriser le portlet Host On-Demand à apparaître sous forme de portlet imbriqué
  - Masquage du bureau HOD au démarrage : Sélectionnez cette option dans la fenêtre Options avancées > Présentation pour masquer le bureau Host On-Demand.
- **Spécification de noms de portlets uniques dans Portal Server**. Utilisez la zone Titre de la page de la page Nom de fichier et Format de sortie de l'assistant de déploiement pour indiquer des noms de portlets uniques dans Portal Server.

Extension des portlets Host On-Demand

Dans certaines circonstances, vous devez modifier la présentation ou les fonctionnalités des portlets Host On-Demand. Voici quelques conseils et instructions qui vont vous aider à étendre vos portlets :

- Les modèles de fichier de portlet se trouvent dans le sous-répertoire du portail placé sous le répertoire de diffusion de Host On-Demand (ou dans le répertoire d'installation de l'assistant de déploiement, s'il est installé séparément). Si vous modifiez ces modèles, vous risquez d'affecter tous les portlets générés par la suite. N'oubliez donc pas de sauvegarder ces fichiers si vous prévoyez de les modifier. Les modèles de fichier incluent les modèles de JSP utilisés pour afficher l'applet de Host On-Demand et les modèles de descripteurs XML utilisés pour déployer les portlets vers WebSphere Portal.
- Chaque portlet est une archive qui peut être aisément extraite, puis de nouveau archivée à l'aide d'un utilitaire zip ou jar livré avec un JRE. Extrayez le portlet vers un répertoire temporaire, en préservant les noms de répertoire. Vous pouvez alors modifier les fichiers appropriés, puis les archiver de nouveau à partir du répertoire temporaire de niveau supérieur.
- Les descripteurs XML se trouvent dans le répertoire de niveau supérieur de votre portlet. Les fichiers JSP se trouvent dans le répertoire /WEB-INF/hod/html pour WebSphere Portal 6.

- Vous devez ajouter un fichier d'aide personnalisé à votre portlet. Pour ce faire, vous devez indiquer dans le fichier portlet.xml que vous prenez en charge le mode de marquage *help*. Ajoutez un fichier intitulé WpsHODHelp.jsp (respectez les majuscules et les minuscules) contenant les informations d'aide et le programme de formatage HTML au répertoire JSP de votre portlet.
- Vous devez développer un portlet personnalisé qui modifie de manière dynamique les propriétés de session. Le nom de l'utilisateur du portlet ou l'adresse IP du client demandant la page peuvent être des données utiles auxquelles vous souhaiterez probablement accéder. Consultez les API du portlet pour savoir comment accéder à ces données. Vous pouvez utiliser la syntaxe de substitution HTML décrite dans le Chapitre 13, «Modification dynamique des propriétés de session», à la page 105 pour insérer les données dérivées de ces informations dans l'ensemble des paramètres de l'applet.
- Pour obtenir des informations détaillées sur le développement du portlet et les API, consultez la documentation WebSphere Portal installée avec le produit.

Chapitre 17. Prise en charge du plug-in Eclipse

Ce chapitre explique comment configurer Host On-Demand pour le plug-in IBM Eclipse.

Remarque : Host On-Demand ne prend actuellement en charge le plug-in Eclipse que sur les plateformes Windows. Vérifiez le fichier readme concernant des prises en charge supplémentaires, ce fichier étant mis à jour lors de l'ajout de plateformes.

Le plug-in Eclipse est la référence en termes d'informatique réseau de la génération future. Construit sur la plateforme client enrichi Eclipse, ce produit fournit des fonctions supplémentaires permettant de gérer et de déployer facilement des applications pour les utilisateurs finals.

Avec le plug-in Eclipse, toutes les applications sont regroupées en tant que “fonctions” d'Eclipse, qui consistent en “plug-in” et “fragments”. Les fonctions d'Eclipse s'installent en général à partir d'un “site de mise à jour” qui est un répertoire sur une machine accessible par le web.

Host On-Demand comprend une applet Java, "Utilitaire Site de mise à jour", permettant de construire le plug-in Host On-Demand pour le plug-in Eclipse. Cette applet convertit les fichier JAR de Host On-Demand en plug-in et fragments Eclipse puis les place dans un répertoire, existant ou nouveau, de site de mise à jour.

Les procédures d'installation de fonctions à partir d'un site de mise à jour varient en fonction des plateformes de plug-in Eclipse, telles que Workplace Managed Client (WMC) ou WebSphere Everyplace Deployment (WED). Si vous utilisez WMC, la procédure de configuration comprend des étapes supplémentaires sur son serveur homologue, Workplace Collaboration Service (WCS). L'applet Utilitaire Site de mise à jour génère un fichier XML, ce qui facilite la procédure de configuration sur WCS.

Création de plug-in de Host On-Demand

Pour créer et déployer des plug-in de Host On-Demand à exécuter dans le plug-in Eclipse, procédez comme suit :

1. Vérifiez que vous disposez d'une page HTML Assistant de déploiement qui définisse les sessions pour votre plug-in. Vous pouvez utiliser n'importe quel modèle de page html ou en créer une nouvelle.

   Remarque : Seuls les modèles de page HTML sont pris en charge pour le plug-in Eclipse.

   Une fois votre page terminée, placez les fichiers de sortie de l'assistant de déploiement dézippés dans le répertoire de diffusion de Host On-Demand.
2. Créez un répertoire, par exemple *c:\update*, qui servira de site de mise à jour d'Eclipse pour vos plug-in, si vous n'en avez pas déjà défini. Puis,
3. Définissez un alias pour ce répertoire dans la configuration du serveur Web, puis redémarrez le serveur Web.
4. Vous pouvez créer maintenant le plugin de Host On-Demand. Sur la machine du site de mise à jour d'Eclipse, ouvrez un navigateur, qui exécute le JRE Java

(1.6 ou une version ultérieure) et pointez-le sur l'URL de Host On-Demand : *http://<nom_hôte>/<alias>/WCTConfig.html* .

Remarque : Sous Linux, vous devez définir la variable d'environnement LD_LIBRARY_PATH si vous utilisez le plug-in Java 1.4.2 Service Release 2 ou les versions ultérieures.

Par exemple, si vous souhaitez utiliser le plug-in Java transmis par le serveur Host On-Demand pour Linux, utilisez la commande d'exportation pour définir la variable d'environnement LD_LIBRARY_PATH comme suit :

```
exportez LD_LIBRARY_PATH=/opt/ibm/HostOnDemand/hod_jre/jre/bin:
  $LD_LIBRARY_PATH
```

5. Cette URL va exécuter une applet Utilitaire Site de mise à jour spéciale pour vous aider à construire le plug-in.
6. Remplissez le panneau Basic Information de l'applet comme suit :
   - **Mettre à jour le répertoire de destination du site de mise à jour (obligatoire)** Précisez le répertoire de site de mise à jour d'Eclipse créé à l'étape 2, c:\updates par exemple.
   - **Base du code HOD (obligatoire)** Cette zone doit normalement être déjà remplie si vous avez pointé vers WCTConfig.html comme demandé à l'étape 3. Cette zone doit comprendre l'emplacement du répertoire de diffusion de Host On-Demand sous la forme *http://<nom_hôte>/<alias>*. Le nom de serveur de Host On-Demand doit être un nom complet. Ce nom ne peut être un nom d'URL relatif ou un nom tel que le “système hôte local” ou “127.0.0.1”.
   - **Fichier de sortie de l'assistant de déploiement (obligatoire)** Précisez le nom de la page HTML de l'assistant de déploiement créée à l'étape 1.
   - **Version de fonction (obligatoire)** Précisez la chaîne de la version utilisée dans la fonction générée, au format major.minor.service, tel que *1.0.0*.
   - **Chemin d'accès au fichier JAR utilisateur (facultatif)** Précisez le chemin d'accès au fichier JAR contenant le code client pour les solutions nécessitant ce type de code pour interagir avec les sessions de Host On-Demand. Vous pouvez définir plusieurs fichiers en les séparant par des virgules (,).

     Remarque : Si vous avez besoin d'utiliser la fonction **Exécuter une applet**, vous devez regrouper vos applets en package dans un fichier JAR et préciser ici le chemin d'accès au fichier.
7. Vous pouvez réduire la taille du plug-in Eclipse à créer en décochant les fonctions inutiles ou les pages de code hôte sur les panneaux **Codes d'exécution** and the **Pages de codes** du panneau **Utilitaire Site de mise à jour**.
8. Une fois toutes les zones remplies, sélectionnez **Générer et déployer le plug-in**. L'applet crée le plug-in de Host On-Demand et le place dans le site de mise à jour que vous avez défini.
9. Les fichiers suivants sont créés ou modifiés dans le répertoire de destination du site de mise à jour :
   - **Fichier Plan du site (site.xml) :** ce fichier répertorie les fonctions installées à partir de ce site de mise à jour.
   - **Fichier script XMLAccess :** ce fichier est une entrée de l'utilitaire WebSphere Portal XMLAccess pour l'installation de Host On-Demand sur WCS. Les noms de fichier sont au format suivant : (nom du fichier de sortie de l'assistant de déploiement)_DeployScript.xml. Dans XMLAccess, reportez-vous à Raccourcis clavier IBM pour la famille WebSphere Portal.

- **Sous-répertoire des fonctions :** ce sous-répertoire comprend les archives de Host On-Demand.
- **Sous-répertoire des plug-in :** ce sous-répertoire comprend les éléments suivants :

Le plug-in de Host On-Demand	Il s'agit du plug-in lui-même. Le nom de fichier est au format : *com.ibm.eNetwork.HOD.wct_(version plug-in).jar*
Le fragment de code de Host On-Demand	Code d'exécution de Host On-Demand. Le nom de fichier est au format : *com.ibm.eNetwork.HOD.wct.(nom fonction)_(version plug-in).jar*
Le fragment de configuration	Fragment stockant les informations de configuration. Le nom de fichier est au format : *com.ibm.eNetwork.HOD.wct.configs.(nom fichier de sortie assistant de déploiement)_(version fonction).jar*

- **Sous-répertoire d'images :** ce sous-répertoire comprend un fichier image utilisé sur WMC/WCS.

Pour plus d'informations sur l'installation du plug-in sur le client, reportez-vous à les documents fournis avec les plateformes de plug-in Eclipse.

Définition dynamique des propriétés de session

Vous ne pouvez pas remplacer le langage HTML sur la plateforme de plug-in Eclipse afin de définir de façon dynamique les propriétés de session parce qu'aucun fichier HTML n'est utilisé pour l'exécution du plug-in de Host On-Demand. Si vous avez besoin d'une fonctionnalité similaire, procédez comme suit :

1. Implémentez une classe Java qui met en oeuvre l'interface *com.ibm.eNetwork.HOD.wct.IHODConfigFactory*, stockée dans le fichier wct.jar. Ce fichier est installé dans le répertoire de diffusion de Host On-Demand. L'interface comporte deux méthodes publiques :

   ```
   La chaîne publique setHodHtmlFileName()
   Les propriétés publiques getHodHtmlParameters()
   ```

   L'exemple ci-dessous illustre ce type de classes Java :

```
package com.ibm.eNetwork.HOD.wct.samples;

import java.util.Properties;

import com.ibm.eNetwork.HOD.wct.IHODConfigFactory;

public class ConfigOverride implements IHODConfigFactory {
    /* (non-Javadoc)
     * @see com.ibm.eNetwork.HOD.wct.IHODConfigFactory#getHodHtmlFileName()
     */
    public String getHodHtmlFileName() {
        return "hodwmc";
    }

    /* (non-Javadoc)
     * @see com.ibm.eNetwork.HOD.wct.IHODConfigFactory#getHodHtmlParameters()
     */
    public Properties getHodHtmlParameters() {
        Properties p = new Properties();
        p.put("EnableHTMLOverrides", "true");
        p.put("TargetedSessionList", "3270 Display");
        p.put("host", "3270 Display=hostname");
        return p;
    }
```

Figure 9. Exemple de classes Java

2. Regroupez la classe java dans un fichier JAR.
3. Editez le fichier HTML de Utilitaire Site de mise à jour (WCTConfig.html) dans le répertoire de diffusion de Host On-Demand et définissez le paramètre showUserClass sur true :

   ```
   var showUserClass="true";
   ```

4. Exécutez l'applet **Utilitaire Site de mise à jour** puis définissez les autres paramètres comme suit : Chemin d'accès au fichier JAR utilisateur : chemin du fichier JAR créé à l'étape 2. Fabrique de classe de configuration utilisateur : nom de la classe java implémentée à l'étape 1, à la page 137.
5. Générez un plug-in de Host On-Demand puis déployez-le sur votre plateforme de plug-in Eclipse.

Utilisation d'un répertoire de diffusion utilisateur distinct

Lorsque vous utilisez un autre répertoire de diffusion que celui de Host On-Demand, vous devez définir ce répertoire sur l'applet Utilitaire Site de mise à jour en suivant la procédure ci-dessous :

1. Editez le fichier HTML de Utilitaire Site de mise à jour (WCTConfig.html) dans le répertoire de diffusion de Host On-Demand et définissez le paramètre showAlternatePublishDirectory sur true :

   ```
   var showAlternatePublishDirectory ="true";
   ```

2. Exécutez l'applet Utilitaire Site de mise à jour puis définissez votre répertoire de diffusion utilisateur dans la zone de saisie Répertoire de diffusion de remplacement.

Identificateurs de vue utilisés dans le plug-in de Host On-Demand

La liste ci-dessous énumère les identificateurs de vue utilisés par le plug-in de Host On-Demand. Vous êtes censé les connaître pour la configuration manuelle de la mise en page sur WCS.

Identificateur	Description
com.ibm.eNetwork.HOD.wct.SessionsView	Sessions configurées
com.ibm.eNetwork.HOD.wct.SessionLabelsView	Sessions actives
com.ibm.eNetwork.HOD.wct.TerminalView	Terminal (Affichage, Imprimante, FTP etc.)

Restrictions liées à l'utilisation de Host On-Demand dans un environnement de plug-in Eclipse

Les restrictions (non mentionnées ci-dessus) liées à l'utilisation de Host On-Demand dans un environnement de plug-in Eclipse sont les suivantes :

1. Il peut arriver qu'une boîte de dialogue modale de Host On-Demand passe derrière la fenêtre de l'interpréteur de commandes du plug-in Eclipse. Cela se produit lorsqu'une boîte de dialogue de Host On-Demand est ouverte et que l'utilisateur bascule sur une autre application extérieure au plug-in Eclipse. Celui-ci doit alors appuyer sur les touches ALT-TAB pour rechercher la boîte de dialogue HOD dont il faut accuser réception.
2. Le paramètre “Confirm On Exit” ne fonctionne pas. Le paramètre “Confirmer à la sortie” est ignoré dans un environnement de plug-in Eclipse. N'étant pas prise en charge, cette option a été supprimée des propriétés de session.
3. Si une session est lancée, mais l'adresse de destination n'a pas été configurée, l'applet de Host On-Demand peut lancer la boîte de dialogue des propriétés de session. Dans l'environnement de plug-in Eclipse, l'utilisateur reçoit un message signalant qu'une adresse de destination doit être saisie et que la boîte de dialogue des propriétés ne s'ouvre pas.
4. Il est impossible d'ajouter de manière dynamique des éléments de l'interface graphique, tels que gestionnaire de macro, clavier et barre d'outils, à une session en cours d'exécution. Ces outils doivent en fait être activés à l'aide des propriétés existantes dans la section Préférences des propriétés de session.
5. L'option “Démarrer dans une fenêtre séparée” n'a aucun sens ici puisque la session figure toujours dans un panneau d'éditeur. Cette option a donc été supprimée des propriétés de session.
6. Seul un client avec des fonctions de débogage est disponible. Il est impossible de réduire les composants de logiciel préinstallé avec les options de préinstallation de l'assistant de déploiement pour diminuer les encombrements (à l'exception des pages de code hôtes et du transfert de fichier 5250).
7. Contrairement au client en cache de Host On-Demand, le client ne met pas à jour le nouveau niveau de code automatiquement. L'administrateur doit reconfigurer le site de mise à jour pour que la plateforme de plug-in Eclipse puisse installer les nouveaux plug-in/fragments.
8. La fonction Exécution de l'applet fonctionne uniquement si l'applet a été regroupée dans un fichier JAR et installée sur les machines client.
9. La fonction de trace IPMON est uniquement prise en charge en mode “normal”. Le mode “automatique” n'est pas pris en charge. Concernant les modes d'exécution de la fonction IPMON, reportez-vous à “Overview of IPMON tracing” de l'aide en ligne.

10. Lorsque plusieurs fonctions de Host On-Demand sont installées, le plug-in affiche la liste de ces fonctions dans la vue de sessions configurée pour que l'utilisateur puisse sélectionner celle qui l'intéresse. Après avoir sélectionné une fonction, l'utilisateur doit redémarrer WED pour en sélectionner une autre.
11. Si vous enfoncez puis relâchez la touche Alt, vous émettez une exception sur la console Java. Ce problème a été identifié sur l'interpréteur JRE 1.4.2 d'IBM. Il a été résolu sur la version IBM 1.4.2 Service Release 4.1 et les versions suivantes.

Chapitre 18. Configuration du serveur Host On-Demand pour LDAP

Le serveur Host On-Demand permet de gérer des données de configuration pour les modèles de type serveur de configuration ou combiné. Lorsque le mode d'opération par défaut du serveur Host On-Demand est utilisé, ces données sont sauvegardées dans un répertoire de stockage privé non partagé. Certaines sociétés doivent gérer des données de configuration réparties sur plusieurs serveurs Host On-Demand. Si elles utilisent le répertoire de stockage privé non partagé, les administrateurs doivent gérer les données de chaque serveur Host On-Demand séparément. Un répertoire de serveur LDAP (Lightweight Directory Access Protocol) offre la possibilité de partager les données de configuration des utilisateurs et des groupes par l'intermédiaire de différentes instances du serveur de configuration Host On-Demand.

L'utilisation d'un serveur d'annuaire LDAP pour la gestion et le partage des définitions entre plusieurs serveurs Host On-Demand est une fonction en option qu'il convient de planifier et de mettre en place avec précaution. La migration à partir du répertoire de stockage privé, en particulier, a des conséquences sur les données de configuration. Le protocole LDAP permet au client de gérer les données de configuration Host On-Demand en organisant les utilisateurs en groupes, dans une structure arborescente. Si les utilisateurs existants sont membres de plusieurs groupes, certaines données sont perdues. Notez que les données de configuration du répertoire de stockage privé ne sont pas modifiées lorsqu'une migration vers LDAP se produit. Pour plus d'informations, reportez-vous à la section Implications of migrating to LDAP de l'aide en ligne Host On-Demand.

Définition du support LDAP

1. Choisissez le serveur LDAP et, si nécessaire, installez-le.
2. Si vous utilisez une version de LDAP qui ne prend pas en charge le schéma pour Host On-Demand, installez les fichiers d'extension de schéma On-Demand comme cela est décrit dans la section «Installation des extensions de schéma», à la page 142 (les fichiers d'extension du schéma ne sont pas nécessaires pour LDAP IBM version 3.x ou supérieure).
3. Demandez à votre administrateur LDAP quel suffixe va utiliser Host On-Demand pour le stockage des données de configuration. Notez le nom distinctif (DN - Distinguished Name) de ce suffixe. Vous en aurez besoin pour l'installation.
4. Demandez à votre administrateur LDAP un DN administrateur et un mot de passe pour Host On-Demand. Vous en aurez besoin pour vous identifier auprès du serveur LDAP. Ce DN administrateur doit disposer de droits de création, de modification et de suppression sur le suffixe mentionné à l'étape précédente. Notez le DN et le mot de passe. Vous en aurez besoin au cours de l'installation.
5. Activez le protocole LDAP dans la page Service d'annuaire de l'utilitaire d'administration. De même, vous pouvez migrer les données de configuration du répertoire de stockage privé vers le serveur d'annuaire LDAP. Pour plus d'informations, reportez-vous à Chapitre 18, «Configuration du serveur Host On-Demand pour LDAP».

Les utilisateurs et groupes déjà définis dans LDAP à d'autres fins ne sont pas utilisés par Host On-Demand. Les utilisateurs et groupes de Host On-Demand doivent être définis séparément en migrant les données de configuration à partir du répertoire de stockage privé ou en définissant les utilisateurs et groupes dans Host On-Demand après avoir activé LDAP.

Si vous exploitez le serveur IBM LDAP sur les plateformes Windows et AIX et que vous créez un grand nombre d'utilisateurs, assurez-vous que la valeur du paramètre APP_CTL_HEAP_SZ est correctement configurée dans DB2. Bien que la valeur affectée à cette variable dépende de chaque installation, le positionnement du paramètre APP_CTL_HEAP_SZ sur la valeur 512 constitue un bon choix de départ.

Pour définir la taille de segment DB2 dans un environnement Windows ou AIX, exécutez les commandes suivantes :

1. set DB2INSTANCE=ldapdb2
2. db2 connect to ldapdb2
3. db2 update db cfg for ldapdb2 using APP_CTL_HEAP_SZ 512
4. db2 force application all
5. db2 terminate
6. db2stop
7. db2start

Assurez-vous également que la valeur de STMTHEAP est suffisamment élevée. La taille de ces paramètres dépend exclusivement de la configuration individuelle de chaque client, ainsi que du nombre d'utilisateurs de Host On-Demand dont la migration vers LDAP a été effectuée.

Installation des extensions de schéma

Les extensions Host On-Demand du schéma d'annuaire LDAP se trouvent dans plusieurs fichiers situés dans le sous-répertoire LDAP du répertoire de diffusion (par exemple, `votre_répertoire_installation\HOD\ldap`, où *votre_répertoire_installation* désigne le répertoire que vous avez spécifié pour l'installation de Host On-Demand). Ils sont stockés au format slapd standard. Ils doivent être installés pour que Host On-Demand puisse stocker des données de configuration sur un serveur LDAP. Pour les installer, prenez contact avec l'administrateur LDAP.

Reportez-vous au répertoire de programme pour obtenir des instructions d'installation des extensions de schéma pour zSeries.

Si l'administrateur LDAP a déjà installé ces extensions de schéma pour un autre produit IBM, vous n'avez pas à suivre ces étapes. Si vous utilisez IBM Directory Server version 3.1.1 ou supérieure, le schéma est pré-installé et vous pouvez également ignorer ces étapes.

Pour installer les extensions de schéma Host On-Demand sur un serveur d'annuaire LDAP Netscape, procédez comme suit :

1. Copiez les fichiers slapd suivants du répertoire /ldap <répertoire de diffusion Host On-Demand> dans le répertoire config LDAP Netscape sur le serveur LDAP :

   ```
   Netscape.IBM.at
   Netscape.IBM.oc
   ```

2. Arrêtez le serveur LDAP.
3. Editez le fichier / slapd.conf du <répertoire Netscape LDAP config>/ et ajoutez les instructions suivantes :

   ```
   userat "<Netscape LDAP config directory>/Netscape.IBM.at"
   useroc "<Netscape LDAP config directory>/Netscape.IBM.oc"
   ```

4. Redémarrez le serveur LDAP.

Pour installer les extensions de schéma Host On-Demand sur un serveur d'annuaire LDAP IBM, procédez comme suit :

1. Copiez les fichiers slapd suivants du répertoire /ldap répertoire de diffusion Host On-Demand dans le répertoire <répertoire d'installation>/etc qui se trouve sur le serveur LDAP :

   ```
   V2.1.IBM.at
   V2.1.IBM.oc
   ```

2. Arrêtez le serveur LDAP.
3. Editez le fichier <répertoire d'installation>/etc/slapd.at.conf et ajoutez l'instruction suivante à la fin du fichier :

   ```
   include /etc/V2.1.IBM.at
   ```

4. Editez le fichier <répertoire d'installation>/etc/slapd.oc.conf et ajoutez l'instruction suivante à la fin du fichier :

   ```
   include /etc/V2.1.IBM.oc
   ```

5. Redémarrez le serveur LDAP.

Configuration du serveur Host On-Demand pour utiliser LDAP en tant que répertoire de stockage

1. Ouvrez la fenêtre d'administration et connectez-vous à Host On-Demand.
2. Cliquez sur Services > Service d'annuaire
3. Cochez la case Utiliser le service d'annuaire (LDAP) et entrez les informations sur le serveur LDAP.

   Adresse de destination
   Entrez l'adresse IP de l'annuaire LDAP. Vous pouvez indiquer un nom d'hôte ou utiliser le format en notation décimale à point. La valeur par défaut est le nom hôte du serveur Host On-Demand.

   Port de destination
   Entrez le port TCP/IP sur lequel le serveur LDAP acceptera une connexion à partir d'un client LDAP. Le port par défaut est 389.

   Nom distinctif administrateur
   Entrez le nom distinctif (DN) de l'administrateur d'annuaire qui autorise la mise à jour des données par Host On-Demand. Vous devez utiliser le format de chaîne LDAP pour les noms distinctifs (par exemple, cn=Chris Smith,o=IBM,c=US).

   Mot de passe administrateur
   Entrez le mot de passe de l'administrateur de l'annuaire.

   Suffixe de nom distinctif
   Entrez le nom distinctif (DN) de l'entrée la plus élevée de l'arborescence d'annuaire (DIT) pour laquelle sont sauvegardées les données. Host On-Demand stocke toutes les données de configuration sous ce suffixe dans l'arborescence DIT. Vous devez utiliser le format de chaîne LDAP pour les noms distinctifs (par exemple, cn=HOD,o=IBM,c=US).

Migration de la configuration vers le service d'annuaire
Cochez cette case pour faire migrer les utilisateurs et les groupes du répertoire de stockage privé vers l'annuaire LDAP. La migration vers LDAP a des conséquences significatives sur les données de configuration des groupes et des utilisateurs. Pour plus d'informations, reportez-vous à LDAP Migration Implications de l'aide en ligne. Vous pouvez cocher cette case avant ou après être passé à l'utilisation du serveur d'annuaire.

La configuration de l'Agent de réacheminement ne fait pas l'objet d'une migration vers le serveur d'annuaire.

Si un incident se produit lors de la connexion au LDAP et lors de la migration, essayez de vous connecter au LDAP. Une fois que la connexion est établie, tentez d'effectuer la migration.

4. Cliquez sur Validation.

   Lorsque vous devez vous authentifier pour la première fois auprès de l'annuaire LDAP, indiquez l'ID utilisateur "admin" et le mot de passe "password". Vous pouvez changer ce mot de passe lors de votre deuxième connexion. Même si vous avez modifié le mot de passe du répertoire de stockage privé, cet ID et ce mot de passe seront toujours valables pour ce répertoire uniquement. Pour le répertoire LDAP, un ID et un mot de passe distincts sont requis. Pour éviter toute confusion, vous pouvez affecter le mot de passe du répertoire de stockage privé au répertoire LDAP.

Les modifications apportées à ce panneau prennent effet de façon immédiate. Une fois que vous êtes passé à l'utilisation du serveur LDAP, les modifications ultérieures des données des utilisateurs seront apportées uniquement sur le serveur LDAP. Ces modifications incluent les modifications d'ordre administratif apportées aux groupes, aux utilisateurs ou aux sessions, mais également les changements de mot de passe, de macros, d'affectation des touches du clavier, etc., effectués par l'administrateur ou par un utilisateur.

Annexe A. Utilisation des clients installés en local

Le client installé en local s'installe sur un disque local. L'applet client est chargée directement dans le navigateur par défaut du système. Il n'y a donc aucune opération de téléchargement à partir d'un serveur. Ce client sert généralement aux utilisateurs qui se connectent à distance via des lignes téléphoniques lentes et pour lesquels le temps de téléchargement et la connectivité posent un problème. Vous pouvez également utiliser ce client pour tester les fonctionnalités de l'accès au système hôte sans installer le produit Host On-Demand dans sa totalité.

Systèmes d'exploitation prenant en charge les clients installés en local

Host On-Demand peut être installé en tant que client sur les systèmes d'exploitation suivants :

- Windows 7
- Windows 8
- Windows 10
- Windows Server 2012

Le client installé en local requiert environ 320 Mo d'espace disque.

Installation du client local

Pour installer le client local Host On-Demand sous Windows, vous devez être membre du groupe Administrateurs.

1. Insérez le DVD, puis exécutez le fichier `hodinstallwin.exe -lc` dans le répertoire `\HODINST` qui se trouve sur le DVD.
2. Cliquez sur Installation.
3. Suivez les instructions qui s'affichent dans les autres fenêtres.
4. Si vous ne l'avez pas déjà fait, lisez le fichier readme qui s'affiche dans la dernière fenêtre.

A l'issue de l'installation, le gestionnaire de services Host On-Demand est configuré et démarre automatiquement. Sous Windows 7, Windows 8 et Windows 10, le gestionnaire de services est installé en tant que service.

Démarrage du client local

Pour démarrer Host On-Demand en tant que client, cliquez sur **Démarrer** > **Programmes**> **IBM Host On-Demand**> **Host On-Demand**.

Suppression du client local

Pour procéder au retrait du client installé en local, appelez la fonction Ajout/Suppression de programmes dans le Panneau de configuration.

Annexe B. Utilisation de l'interface de ligne de commande IKEYCMD

IKEYCMD est un outil de ligne de commande, complémentaire du gestionnaire de certificats Host On-Demand, qui peut être utilisé pour gérer les clés, les certificats et les demandes de certificat. Il fonctionne de la même manière que le gestionnaire de certificats et est censé être lancé à partir de la ligne de commande sans interface graphique. Il peut être appelé à partir de scripts d'interpréteur de commandes natifs et de programmes utilisés lorsque des applications préfèrent ajouter des interfaces personnalisées aux certificats et aux tâches de gestion des clés. Il crée des fichiers de bases de données de clés pour tous les types que l'utilitaire de gestion de certificats prend actuellement en charge. Il crée des demandes de certificat, importe des certificats signés par une autorité de certification et gère les certificats autosignés. Il est basé sur Java et est disponible sur les plateformes Windows, AIX, Linux Intel et Linux zSeries.

Vous pouvez utiliser IKEYCMD pour les tâches de configuration liées à la création et à la gestion des clés publiques ou privées. Vous ne pouvez pas utiliser IKEYCMD pour les options de configuration permettant de mettre à jour le fichier de configuration du serveur httpd.conf. Pour ces options de mise à jour du fichier de configuration du serveur, vous devez utiliser le serveur d'administration IBM.

Configuration de l'environnement pour l'interface de ligne de commande IKEYCMD

Pour définir les variables d'environnement permettant d'utiliser l'interface de ligne de commande IKEYCMD, procédez comme suit :

Pour les plateformes Windows :

- A l'aide de l'interface utilisateur ou en modifiant le fichier autoexec.bat dans une fenêtre de commande, définissez ou modifiez la variable PATH pour inclure l'emplacement des fichiers exécutables Java :

  ```
  set PATH=c:\Program Files\IBM\HostOnDemand\hod_jre\jre\bin;%PATH%;
  ```

- A l'aide de l'interface utilisateur ou en modifiant le fichier autoexec.bat dans une fenêtre de commande, définissez ou modifiez la variable d'environnement CLASSPATH comme suit :

  ```
  set CLASSPATH=c:\Program Files\IBM\GSK7\classes\cfwk.zip;C:\
  Program Files\IBM\GSK7\classes\gsk7cls.jar;%CLASSPATH%;
  ```

Pour les plateformes AIX :

Assurez-vous en premier lieu que les fichiers xlC (qui constituent la bibliothèque d'exécution du compilateur standard AIX C++) répondent l'une des exigences suivantes :

- Sur AIX 5.2 : l'ensemble de fichiers xlC.aix50.rte doit être au niveau 6.0.0.3 ou supérieur

Utilisez la commande suivante pour confirme votre version :

```
lslpp -ha "xlC.aix*.rte"
```

(si votre ensemble de fichiers xlC est périmé et que vous démarrez le gestionnaire de services Host On-Demand alors que le gestionnaire de certificats est actif, des erreurs se produisent).

Spécifiez ensuite les informations suivantes :

- Définissez la variable PATH dans laquelle réside le fichier exécutable Java ou JRE :

  ```
  EXPORT PATH=/opt/IBM/HostOnDemand/hod_jre/jre/bin:$PATH
  ```

- Définissez la variable d'environnement CLASSPATH suivante :

  ```
  EXPORT CLASSPATH=/usr/local/ibm/gsk7/classes/cfwk.zip:/
  usr/local/ibm/gsk7/classes/gsk7cls.jar:$CLASSPATH
  ```

Une fois cette procédure terminée, IKEYCMD peut être exécuté à partir de tout répertoire. La syntaxe suivante permet d'exécuter une commande IKEYCMD :

```
java com.ibm.gsk.ikeyman.ikeycmd <command>
```

Syntaxe de la ligne de commande IKEYCMD

La syntaxe de l'interface de ligne de commande Java est la suivante :

```
java [-Dikeycmd.properties=<properties_file>]
com.ibm.gsk.ikeyman.ikeycmd <object> <action> [options]
```

où

- Le fichier -Dikeycmd.properties permet de préciser le nom du fichier de propriétés en option à utiliser pour cet appel Java. Le fichier de propriétés par défaut ikminit_hod.properties est fourni en tant que modèle de fichier contenant les paramètres par défaut de Host On-Demand.
- L'objet est l'un des suivants :
  - -keydb : actions réalisées sur la base de données de clés (fichier de base de données de clés CMS ou classe TLSight)
  - -version : affichage des informations relatives à la version de IKEYCMD
- Voici les différentes actions possibles :
  - -cert : actions réalisées sur un certificat
  - -certreq : actions réalisées sur une demande de certificat
  - -help : affichage de l'aide pour les appels IKEYCMD

L'action représente l'action spécifique à réaliser sur l'objet. Les options sont celles (obligatoires et facultatives) indiquées pour la paire objet-action.

Les mots clés objet et action sont à position fixe et doivent être indiqués dans l'ordre sélectionné. Toutefois, les options ne sont pas à position fixe et peuvent être indiquées dans n'importe quel ordre, à condition qu'elles soient précisées sous forme de paire option-opérande.

Liste IKEYCMD des tâches pour Host On-Demand

Les sections suivantes de la présente annexe répertorient les tâches de l'interface de ligne de commande IKEYCMD requises pour Host On-Demand :

- «Création d'une base de données de clés», à la page 149
- «Liste des Autorités de certification (AC)», à la page 150
- «Affichage de la clé par défaut dans une base de données de clés», à la page 156

Création d'une base de données de clés

Une base de données de clés est un fichier que le serveur utilise pour stocker une ou plusieurs paires de clés et de certificats. Elle est obligatoire pour activer les connexions sécurisées entre le serveur Host On-Demand et les clients. Avant de configurer une communication TLS, vous devez créer le fichier de base de données de clés HODServerKeyDb.kdb dans *votre_répertoire_installation*\bin pour Windows et *votre_répertoire_installation*/bin pour AIX. Ce fichier n'est pas livré avec Host On-Demand. Vous devez donc le créer après la première installation.

Par exemple, pour créer une base de données de clés sur des plateformes Windows à l'aide de l'interface de ligne de commande IKEYCMD, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -type cms -expire <days> -stash
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Notez les descriptions suivantes :

- <password> : le mot de passe est obligatoire pour chaque opération de la base de données de clés. Même si une base de données de type sslight requiert un mot de passe spécifié, le mot de passe peut être une chaîne nulle (sous forme "").
- -type : le fichier HODServerKeyDb.kdb utilisé par le serveur Host On-Demand est de type CMS.
- -expire : le nombre de jours avant expiration du mot de passe.
  - Si vous n'avez pas défini ce paramètre, alors le mot de passe n'expire pas.
  - **AVERTISSEMENT** : Si vous définissez ce paramètre et si vous utilisez la base de données de clés avec l'Agent de réacheminement, assurez-vous que l'agent ne réussit pas à s'exécuter après l'expiration du mot de passe. Si l'Agent de réacheminement échoue, *aucun* message d'erreur ne spécifie que le mot de passe de la base de données de clés a expiré.
- -stash : stocke le mot de passe de la base de données de clés. Le stockage du mot de passe sur le système est **obligatoire** pour IBM HTTP Server et le serveur Host On-Demand.

  Lorsque l'option -stash est spécifiée lors de la création de la base de données de clés, le mot de passe est stocké dans un fichier HODServerKeyDb.sth.

  Une fois le fichier HODServerKeyDb.kdb créé, il contient toutes les informations relatives à la sécurité dont a besoin le serveur Host On-Demand. Des informations supplémentaires et des modifications sont insérées dans le fichier de base de données de clés HODServerKeyDb.kdb existant.

A chaque création ou modification du fichier HODServerKeyDb.kdb, vous devez arrêter, puis redémarrer le gestionnaire de services Host On-Demand.

Définition du mot de passe de la base de données

Lorsque vous créez une base de données de clés, vous devez indiquer un mot de passe de base de donnée de clés. Ce mot de passe permet de protéger la clé privée. Cette dernière est la seule clé pouvant signer des documents ou déchiffrer des messages chiffrés à l'aide de la clé publique. Prenez l'habitude de modifier fréquemment le mot de passe de la base de données de clés.

Indiquez le mot de passe à l'aide des instruction suivantes :

- Utilisez le jeu de caractères U.S. English pour préciser le mot de passe.
- Le mot de passe doit être composé de six caractères au minimum et contenir au moins deux chiffres non consécutifs. Veillez à ce qu'il ne comporte pas d'informations connues vous concernant (vos initiales ou date de naissance, ou celles d'un membre de votre famille, par exemple).
- Stockez le mot de passe.

N'oubliez pas les dates d'expiration du mot de passe. S'il expire, un message est écrit dans le journal des erreurs. Le serveur démarre, mais la connexion réseau sécurisée n'est pas assurée.

Modification du mot de passe de la base de données

Pour changer le mot de passe d'accès à la base de données, procédez comme suit :

Pour les plateformes Windows, tapez par exemple la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -changepw
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -new_pw <new_password> -expire <days> -stash
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Notez les descriptions suivantes :

- -new_pw : nouveau mot de passe d'accès à la base de données de clés ; il doit être différent de l'ancien mot de passe et ne peut pas être une chaîne nulle.
- -expire : nombre de jours avant l'expiration du mot de passe.
- -stash : stocke le mot de passe de la base de données de clés. Le stockage du mot de passe est obligatoire pour IBM HTTP Server et le serveur Host On-Demand.

Liste des Autorités de certification (AC)

Pour afficher la liste des AC dignes de confiance dans la base de données de clés HODServerKeyDb.kdb, procédez comme suit :

Pour les plateformes Windows, tapez par exemple la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -list CA
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -type cms
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Par défaut, HODServerKeyDb.kdb est livré avec les certificats des autorités de certification dignes de confiance suivantes :

- IBM World Registry
- Integrion CA Root (d'IBM World Registry)
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 4 Public Primary CA
- VeriSign Test CA
- RSA Secure Server CA (de VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

Création d'une paire de clés et d'une demande de certificat

Pour créer une paire de clés publique-privée et une demande de certificat, procédez comme suit :

1. Pour les plateformes Windows, tapez par exemple la commande suivante :

   ```
   java com.ibm.gsk.ikeyman.ikeycmd -certreq -create
   -db votre_répertoire_installation\bin\HODServerKeyDb.kdb
   -pw <password> -size <1024 | 512> -dn <distinguished_name>
   -file <filename> -label <label>
   ```

   où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

   Notez les descriptions suivantes :

   - -size : taille de la clé (512 ou 1024)
   - -label : étiquette associée au certificat ou à la demande de certificat
   - -dn : nom distinctif X.500. Il s'agit d'une entrée sous forme de chaîne de caractères délimitée présentée au format suivant : (seuls CN, O et C sont obligatoires ; CN=nom_commun, O=organisation, OU=unité_organisation, L=emplacement, ST=état ou province, C=pays).

     ```
     "CN=weblinux.raleigh.ibm.com,O=ibm,OU=IBM HTTP Server,L=RTP,ST=NC,C=US"
     ```

   - -file : nom du fichier dans lequel la demande de certificat va être stockée. Par défaut, Host On-Demand utilise le nom certreq.arm, qui doit être stocké dans le répertoire *répertoire_installation*\bin (où *répertoire_installation* concerne Host On-Demand), dans lequel se trouve le fichier HODServerKeyDb.kdb.

2. Assurez-vous que la création du certificat a abouti.

   a. Affichez le contenu du fichier de demande de certificat que vous avez créé.

   b. Vérifiez que la base de données de clés a enregistré la demande de certificat :

   ```
   java com.ibm.gsk.ikeyman.ikeycmd -certreq -list
   -db <filename> -pw <password>
   ```

   L'étiquette que vous avez créée doit s'afficher.

3. Envoyez le fichier créé à l'autorité de certification.

Stockage du certificat de serveur

Réception d'un certificat signé par une autorité de certification

Cette procédure permet de recevoir un certificat par courrier électronique de la part d'une autorité de certification (AC), désignée comme AC digne de confiance sur votre serveur. Par défaut, les certificats d'AC sont stockés dans la base de données de clés HODServerKeyDb.kdb et désignés comme certificats d'AC digne de confiance :

- IBM World Registry
- Integrion CA Root (d'IBM World Registry)
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 4 Public Primary CA
- VeriSign Test CA
- RSA Secure Server CA (de VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

L'autorité de certification peut encore envoyer plusieurs certificats. Outre le certificat lié à votre serveur, l'autorité de certification peut également envoyer des certificats de signature ou des certificats d'AC intermédiaires complémentaires. Par exemple, Verisign inclut un certificat d'AC intermédiaire lors de l'envoi du certificat Global Server ID. Avant de recevoir le certificat de serveur, recevez des certificats d'AC intermédiaires complémentaires. Suivez les instructions présentées dans la section «Stockage d'un certificat émis par une autorité de certification», à la page 153 pour recevoir des certificats d'AC intermédiaires.

Si l'autorité de certification qui émet le certificat n'est pas une AC digne de confiance de la base de données de clés, vous devez tout d'abord stocker le certificat de l'AC et désigner l'autorité de certification comme digne de confiance. Vous pouvez dès lors recevoir le certificat signé par l'autorité de certification dans votre base de données. Vous ne pouvez pas recevoir ce même certificat s'il est émis par une autorité de certification qui n'est pas digne de confiance. Pour obtenir plus d'instructions, reportez-vous à «Stockage d'un certificat émis par une autorité de certification», à la page 153

Par exemple, pour recevoir un certificat signé par l'autorité de certification dans une base de données de clés sur les plateformes Windows, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -receive -file <filename>
-db
votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password>
-format <ascii | binary> -default_cert <yes | no>
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Notez les descriptions suivantes :

- -format : l'autorité de certification peut fournir un certificat au format ASCII ou binaire
- -label : étiquette associée au certificat de l'AC.
- -trust : permet d'indiquer si l'autorité de certification est digne de confiance. Utilisez les options d'activation lors de la réception d'un certificat de l'AC.
- -file : fichier contenant le certificat de l'AC.

Stockage d'un certificat émis par une autorité de certification

Pour stocker un certificat émis par une autorité de certification qui n'est pas digne de confiance pour les plateformes Windows par exemple, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -label <label> -format <ascii | binary>
-trust <enable |disable> -file <file>
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Notez les descriptions suivantes :

- -label : étiquette associée au certificat ou à la demande de certificat
- -format : les autorités de certification doivent fournir un fichier ASCII binaire.
- -trust : indique si cette AC est digne de confiance. La réponse doit être Oui.

Vous devez arrêter, puis redémarrer le gestionnaire de services Host On-Demand après cette opération.

Création d'un certificat autosigné

D'une manière générale, l'obtention d'un certificat de la part d'une autorité de certification connue prend deux à trois semaines. En attendant l'émission d'un certificat, utilisez IKEYCMD pour créer un certificat de serveur autosigné afin d'activer des sessions TLS entre les clients et le serveur. Suivez cette procédure si vous agissez en tant qu'autorité de certification propre pour un réseau Web privé.

Pour créer un certificat autosigné pour les plateformes Windows par exemple, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -create
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -size <1024 | 512> -dn <distinguished name>
-label <label> -default_cert <yes or no>
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Notez les descriptions suivantes :

- -size : taille de la clé (512 ou 1024)
- -label : entrez un commentaire descriptif permettant d'identifier la clé et le certificat dans la base de données.
- -dn : entrez un nom distinctif X.500. Il s'agit d'une entrée sous forme de chaîne de caractères délimitée présentée au format suivant : (seuls CN, O et C sont

obligatoires ; CN=nom_commun, O=organisation, OU=unité_organisation, L=emplacement, ST=état, province, C=pays).

```
"CN=weblinux.raleigh.ibm.com,O=ibm,OU=IBM HTTP Server,L=RTP,ST=NC,C=US"
```

- -default_cert : entrez Oui si vous souhaitez que ce certificat soit le certificat par défaut de la base de données de clés. Sinon, entrez Non.

Mise à disposition de certificats de serveur auprès des clients

Tous les certificats de HODServerKeyDb.kdb sont accessibles au serveur Host On-Demand. Toutefois, dans certaines configurations, l'un de ces certificats doit être également à la disposition des clients qui accèdent au serveur. Si votre serveur utilise un certificat émis par une autorité de certification inconnue, la racine du certificat doit être disponible pour le client. Si votre serveur utilise un certificat autosigné, une copie de ce certificat doit être mis à la disposition des clients.

Pour les clients en cache et téléchargés de Host On-Demand, il suffit d'extraire le certificat vers un fichier temporaire et de créer ou mettre à jour un fichier intitulé CustomizedCAs.p12, qui doit être présent dans le répertoire de diffusion de Host On-Demand.

Pour créer le fichier CustomizedCAs.p12 pour les clients téléchargés ou en cache, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman -keydb -create -db
CustomizedCAs.p12 -pw hod -type pkcs12
```

Le mot de passe par défaut est hod.

Ajout de la racine d'une autorité de certification inconnue au fichier CustomizedCAs.p12

Tout d'abord, extrayez le certificat racine de l'autorité de certification ou un certificat autosigné du fichier de base de données de clés HODServerKeyDb.kdb. Pour les plateformes Windows, tapez par exemple la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -extract
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -label <label> -target cert.arm -format ascii
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Notez les descriptions suivantes :

- -label : étiquette associée au certificat.
- -pw : mot de passe permettant d'ouvrir le fichier de base de données de clés HODServerKeyDb.kdb.
- -target : fichier ou base de données de destination. Dans ce cas, il s'agit du nom du fichier au format ASCII Armored Base64 (nom de fichier par défaut de cert.arm).
- -format : ASCII ou Binaire.

Maintenant, ajoutez ce certificat racine de l'autorité de certification au fichier CustomizedCAs.p12. Pour ajouter un certificat racine de l'AC ou un certificat autosigné à la liste des signataires de CustomizedCAs.p12, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
```

```
-db CustomizedCAs.p12 -pw hod -label <label>
-file cert.arm -format ascii -trust <enable | disable>
```

Dans le cas des clients plus anciens, ajoutez ce certificat racine de l'autorité de certification au fichier CustomizedCAs.class, entrez l'une des commandes suivantes :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db CustomizedCAs.class -label <label>
-file cert.arm -format ascii -trust <enable | disable>
```

Notez les descriptions suivantes :

- -label : étiquette associée au certificat ajouté.
- -file : nom du fichier vers lequel le certificat a été extrait. Dans ce cas, il s'agit du nom du fichier au format ASCII Armored Base64 (nom de fichier par défaut de cert.arm).
- -format : ASCII ou Binaire.
- -trust : permet de définir en tant que clé d'authentification. Son activation permet de définir le certificat racine de l'AC ou le certificat autosigné en tant que clé d'authentification. Sa désactivation produit l'effet inverse.

Une fois cette tâche accomplie, arrêtez, puis redémarrez le gestionnaire de services Host On-Demand.

Pour les anciens clients, vous devez convertir le fichier CustomizedCAs.p12 en CustomizedCAs.class pour le téléchargement ou pour les clients en cache, vous devez taper la commande suivante. La commande est présentée sur trois lignes, mais vous devez la saisir sur une seule ligne.

```
..\hod_jre\jre\bin\java -cp ..\lib\sm.zip;
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT
CustomizedCAs.p12 hod CustomizedCAs.class
```

Exportation de clés

Pour exporter des clés vers une autre base de données de clés ou vers un fichier PKCS12, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -export -db <filename>
-pw <password> -label <label> -type <cms | jks | jceks | pks12>
-target <filename> -target_pw <password>
-target_type <cms | jks | jceks | pkcs12> -encryption <strong | weak>
```

Notez les descriptions suivantes :

- -label : étiquette associée au certificat.
- -target : fichier ou base de données de destination.
- -target_pw : mot de passe de la base de données de clés cible.
- -target_type : type de base de données spécifié par l'opérande -target.
- -encryption : degré de chiffrement. La valeur par défaut est Elevé.

Importation de clés

Pour importer des clés à partir d'une autre base de données de clés, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -import -db <filename>
-pw <password> -label <label> -type <cms | jks | jceks | pks12> -target
<filename> -target_pw <password> -target_type <cms | jks | jceks | pks12>
```

Pour importer des clés à partir d'un fichier PKCS12, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -import -file <filename>
-pw <password> -type pkcs12 -target <filename>
-target_pw <password> -target_type <cms | jks | jceks | pks12>
```

Notez les descriptions suivantes :

- -label : étiquette associée au certificat.
- -target : base de données de destination.
- -target_pw : mot de passe de la base de données de clés si -target indique une base de données de clés.
- -target_type : type de base de données spécifié par l'opérande -target.

Affichage de la clé par défaut dans une base de données de clés

Pour afficher l'entrée de clé par défaut sous Windows par exemple, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -getdefault
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password>
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Stockage de la base de données chiffrée dans un fichier de dissimulation

Pour assurer une connexion réseau sécurisée, stockez le mot de passe de la base de données dans un fichier de dissimulation. Sous Windows par exemple, pour stocker le mot de passe lors de la création d'une base de données, entrez la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create
-db votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password> -type cms -expire <days> -stash
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Sous Windows par exemple, vous pouvez stocker le mot de passe après la création de la base de données en entrant la commande suivante :

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -stashpw
-db
votre_répertoire_installation\bin\HODServerKeyDb.kdb
-pw <password>
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Présentation du paramètre de lancement IKEYCMD

Le tableau ci-dessous décrit chaque action qu'il est possible d'exécuter sur un objet spécifié.

Objet	Action	Description
-keydb	-changepw	Modification du mot de passe d'une base de données de clés
	-convert	Conversion du format d'une base de données de clés
	-create	Création d'une base de données de clés
	-delete	Suppression d'une base de données de clés
	-stashpw	Stockage du mot de passe d'une base de données de clés dans un fichier
-cert	-add	Ajout d'un certificat de l'autorité de certification d'un fichier vers une base de données de clés
	-create	Création d'un certificat autosigné
	-delete	Suppression d'un certificat de l'AC
	details	Liste des informations détaillées d'un certificat spécifique
	-export	Exportation d'un certificat personnel et de sa clé privée associée d'une base de données de clés vers un fichier PKCS#12 ou une autre base de données de clés
	-extract	Extraction d'un certificat d'une base de données de clés
	-getdefault	Obtention du certificat personnel par défaut
	-import	Importation d'un certificat à partir d'une base de données de clés ou d'un fichier PKCS#12
	-list	Liste de tous les certificats
	-modify	Modification d'un certificat (REMARQUE : actuellement, la zone Certificate Trust est la seule qui puisse être modifiée)
	-receive	Réception d'un certificat d'un fichier vers une base de données de clés

	-setdefault	Définition du certificat personnel par défaut
	-sign	Signature d'un certificat stocké dans un fichier avec un certificat stocké dans une base de données de clés et stockage du certificat signé résultant dans un fichier
-certreg	-create	Création d'une demande de certificat
	-delete	Suppression d'une demande de certificat d'une base de données de demandes de certificat
	-details	Liste des informations détaillées d'une demande de certificat spécifique
	extract	Extraction d'une demande de certificat à partir d'une base de données de demandes de certificat vers un fichier
	-list	Liste de toutes les demandes de certificat de la base de données de demandes de certificat
	-recreate	Recréation d'un demande de certificat
-help		Affichage de l'aide pour la commande IKEYCMD
-version		Affichage des informations relatives à la version de IKEYCMD

Présentation des options de ligne de commande IKEYCMD

Le tableau ci-dessous répertorie chaque option pouvant alimenter la ligne de commande. Les options sont répertoriées sous forme de groupe complet ; toutefois, leur utilisation dépend de l'objet et de l'action spécifiés sur la ligne de commande.

Option	**Description**
-db	Chemin d'accès qualifié complet d'une base de données de clés
-default_cert	Permet de définir un certificat à utiliser par défaut pour l'authentification du client (oui ou non). La valeur par défaut est non.
-dn	Nom distinctif X.500. Entrée sous forme de chaîne de caractères délimitée présentée au format suivant (seuls CN, O et C sont obligatoires) : "CN=Jane Doe,O=IBM,OU=Java Development,L=Endicott, ST=NY,ZIP=13760,C=pays"

-encryption	Degré de chiffrage utilisé dans une commande d'exportation de certificat (élevé ou bas). La valeur par défaut est élevé.
-expire	Délai d'expiration d'un certificat ou d'un mot de passe d'accès à une base de données (en jours). Les valeurs par défaut sont respectivement de 365 jours et de 60 jours.
-file	Nom de fichier d'un certificat ou d'une demande de certificat (selon l'objet indiqué)
-format	Format d'un certificat (ascii pour Base64_encoded ASCII ou binaire pour Binary DER data). La valeur par défaut est ascii.
-label	Etiquette associée à un certificat ou à une demande de certificat
-new_format	Nouveau format de la base de données de clés
-new_pw	Nouveau mot de passe d'accès à la base de données
-old_format	Ancien format de la base de données de clés
-pw	Mot de passe de la base de données de clés ou du fichier PKCS#12. Voir «Création d'une base de données de clés», à la page 149.
-size	Taille de la clé (512 ou 1024). La valeur par défaut est 1024.
-stash	Indicateur pour stocker le mot de passe de la base de données de clés dans un fichier. S'il est précisé, le mot de passe est stocké dans un fichier.
-target	Fichier ou base de données de destination
-target_pw	Mot de passe de la base de données de clés si -target indique une base de données de clés. Voir «Création d'une base de données de clés», à la page 149.
-target_type	Type de la base de données spécifiée par l'opérande -target (voir -type).
-trust	Etat de confiance d'un certificat émis par une autorité de certification (activer ou désactiver). La valeur par défaut est activer.
-type	Type de la base de données. Les valeurs autorisées sont cms (désigne une base de données de clés CMS), jce (désigne l'extension JCE - Java Cryptography Extension - de Sun), jceks (désigne le fichier de clés JCE de Sun) ou pkcs12 (désigne un fichier PKCS#12).
-x509version	Version du certificat X.509 à créer (1, 2 ou 3). La valeur par défaut est 3.

Appel d'une ligne de commande

Voici une liste de chaque appel de ligne de commande, dont les paramètres facultatifs sont en italique.

Pour plus de clarté, l'appel Java en cours (java com.ibm.gsk.ikeyman.ikeycmd) est omis de chacun des appels de ligne de commande.

```
-keydb -changepw -db <filename> -pw <password>
-new_pw <new_password> -stash -expire <days>

-keydb -convert -db <filename> -pw <password>
-old_format <cms | webdb> -new_format <cms>

-keydb -create -db <filename> -pw <password> -type <cms | jks | jceks | pks12>
-expire <days> -stash

-keydb -delete -db <filename> -pw <password>

-keydb -stashpw -db <filename> -pw <password>

-cert -add -db <filename> -pw <password> -label <label>
-file <filename> -format <ascii | binary> -trust <enable | disable>

-cert -create -db <filename> -pw <password> -label <label>
-dn <distinguished_name> -size <1024 | 512> -x509version <3 | 1 | 2>
-default_cert <no | yes>

-cert -delete -db <filename> -pw <password> -label <label>

-cert -details -db <filename> -pw <password> -label <label>

-cert -export -db <filename> -pw <password> -label <label>
-type <cms | jks | jceks | pks12> -target <filename> -target_pw <password>
-target_type <cms | jks | jceks | pkcs12> -encryption <strong | weak>

-cert -extract -db <filename> -pw <password> -label <label>
-target <filename> -format <ascii | binary>

-cert -getdefault -db <filename> -pw <password>

-cert -import -db <filename> -pw <password> -label <label>
-type <cms | jks | jceks | pks12> -target <filename> -target_pw <password>
-target_type <cms | jks | jceks | pks12>

-cert -import -file <filename> -type <pkcs12> -target <filename>
-target_pw <password> -target_type <cms | jks | jceks | pks12>

-cert -list <all | personal | CA | site> -db <filename>
-pw <password> -type <cms | jks | jceks | pks12>

-cert -modify -db <filename> -pw <password> -label <label>
-trust <enable | disable>

-cert -receive -file <filename> -db <filename> -pw <password>
-format <ascii | binary> -default _cert <no | yes>

-cert -setdefault -db <filename> -pw <password> -label <label>

-cert -sign -file <filename> -db <filename> -pw <password>
-label <label> -target <filename> -format <ascii | binary>
-expire <days>

-certreq -create -db <filename> -pw <password> -label <label>
-dn <distinguished_name> -size <1024 | 512> -file <filename>

-certreq -delete -db <filename> -pw <password> -label <label>

-certreq -details -db <filename> -pw <password> -label <label>

-certreq -extract -db <filename> -pw <password> -label <label>
-target <filename>

-certreq -list -db <filename> -pw <password>

-certreq -recreate -db <filename> -pw <password> -label <label>
-target <filename>

-help

-version
```

Fichier de propriétés de l'utilisateur

Afin d'éviter de saisir les appels de l'interpréteur de lignes de commande Java, les propriétés de l'utilisateur peuvent être indiquées dans un fichier de propriétés. Ce dernier peut être spécifié sur l'appel de ligne de commande Java via l'option Java -Dikeycmd.properties. Sous Windows, un modèle de fichier de propriétés (ikminit_hod.properties) est fourni dans *votre_répertoire_installation*\bin, où *votre_répertoire_installation* représente le répertoire d'installation de Host On-Demand. Sous AIX, ce fichier est fourni dans *votre_répertoire_installation*/bin. Ces répertoires d'installation contiennent les paramètres par défaut de Host On-Demand.

Annexe C. Utilitaire de gestion des fichiers de clés P12

Un utilitaire graphique de gestion des certificats (pour les plateformes Windows et AIX) permet de créer des demandes de certificat, de recevoir et d'enregistrer des certificats, et de créer des certificats autosignés. L'utilitaire de gestion de fichiers de clés P12 est principalement destiné aux plateformes ne permettant pas d'exploiter l'utilitaire de gestion de certificats pour créer une base de données de fichiers de clés contenant des certificats racine émis par des autorités de certification auto-signées et inconnues. Toutefois, il peut être utilisé sur n'importe quelle plateforme Host On-Demand. Cet utilitaire fournit aux administrateurs système le moyen de créer et déployer facilement une base de données de fichiers de clés TLS.

L'utilitaire P12 Keyring est écrit en langage Java. Il permet d'obtenir un certificat de serveur à partir d'un serveur Telnet ou FTP (ou d'un Agent de réacheminement) configuré pour prendre en charge TLS. Une connexion TLS est configurée spécifiquement pour un serveur et un port TLS. Si aucun port n'est spécifié, le port sécurisé Telnet ou FTP le plus connu est utilisé. Le certificat de serveur est extrait et ajouté au fichier P12 spécifié.

L'accès à la base de données de fichiers de clés est protégé par un mot de passe. Une invite de spécification du mot de passe est lancée avant toute exécution de commande. Si le fichier de clés spécifié est inexistant, il est créé et le mot de passe est enregistré dans ce fichier.

Le support TLS de Host On-Demand requiert le mot de passe `hod`. Si vous ajoutez un certificat privé à la base de données de fichiers de clés, une autre invite de spécification de mot de passe est lancée pour le second fichier P12.

Utilisation

```
P12Keyring p12FileName connect ipaddr[:port] [ftp]
P12Keyring p12FileName add p12FileName2
P12Keyring p12FileName list
```

Options

connect - établit une connexion TLS avec l'adresse IP et le port spécifiés. Le numéro de port et le mot clé "ftp" sont facultatifs. Si aucun numéro de port n'est spécifié, le port Telnet sécurisé par défaut 443, ou le port FTP sécurisé par défaut 990 est utilisé.

Si le mot clé **ftp** est spécifié, la connexion est établie avec un serveur FTP sécurisé configuré avec des fonctions de sécurité. Deux types d'options de sécurité sont disponibles pour les serveurs FTP :

- Sécurité implicite sur le port 990
- Sécurité explicite sur n'importe quel autre port

Si le mot clé "ftp" est spécifié, mais pas le numéro de port, ou si ce dernier est 990, des négociations de sécurité implicites sont effectuées. Si le mot clé ftp est défini et que le numéro de port ne correspond pas à 990, les négociations de sécurité explicites sont établies en émettant au préalable la commande `AUTH TLS`.

add - ajoute un certificat client privé à la base de données de fichiers de clés spécifiée.

list - affiche la liste des certificats enregistrés dans la base de données de fichiers de clés spécifiée.

Exemples

Windows :

```
C:\votre_répertoire_installation\lib\P12Keyring
c:\votre_répertoire_installation\HOD\CustomizedCAs
connect myServer.raleigh.ibm.com:702

C:\votre_répertoire_installation\lib\P12Keyring
c:\votre_répertoire_installation\HOD\CustomizedCAs
connect myFTPServer.raleigh.ibm.com:5031 ftp
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Unix :

```
cd votre_répertoire_installation/HOD
Java –classpath
.;votre_répertoire_installation/lib/sm.zip \
com.ibm.hod5sslight.tools.P12Keyring CustomizedCAs connect
myServer.raleigh.ibm.com:702
```

où *votre_répertoire_installation* est le répertoire d'installation de Host On-Demand.

Annexe D. Options de ligne de commande des programmes de lancement natifs

Lorsque vous entrez les options de ligne de commande suivantes dans le programme de lancement natif de votre plateforme, elles sont transmises au programme d'installation de Host On-Demand en tant que paramètres de l'installation. Les options qui suppriment l'assistant graphique sont marquées en conséquence.

Tableau 13. Options de ligne de commande

Option	Objectif	Exemple de syntaxe
`-console` (supprime l'assistant graphique)	Installe Host On-Demand en mode console.	`install.exe`
`-log #!`*filename* où # renvoie l'écran sur une sortie standard et !*filename* nomme le fichier journal. Si vous spécifiez l'option '!' sans indique de nom de fichier, le nom du fichier journal par défaut est utilisé.	Génère un fichier journal d'installation portant le nom spécifié.	`hodinstallwin.exe -log #!\mydirectory\logfile`
`-options` *filename*	Installe Host On-Demand avec les options de ligne de commande qui définissent les propriétés spécifiées pour l'installation.	`hodinstallwin.exe -silent -options c:\mydirectory\ responseFile`
`-options-record` *filename*	Génère un fichier texte d'options, qui enregistre vos réponses à l'assistant d'installation de Host On-Demand, en les établissant en tant que valeurs par défaut des variables d'installation.	`hodinstallwin.exe -options-record responses.txt`
`-options-template` *filename*	Génère un fichier texte d'options contenant les valeurs d'installation par défaut.	`hodinstallwin.exe -options-template template.txt`
`-silent` (supprime l'assistant graphique)	Installe Host On-Demand en mode silencieux, en acceptant toutes les valeurs d'installation par défaut.	`hodinstallwin.exe -silent`

Les options de lignes de commandes supplémentaires suivantes s'appliquent uniquement au *processus* d'appel et d'exécution du programme d'installation. Entrez-les sur la ligne de commande à l'aide du programme de lancement natif de la plateforme.

Tableau 14. Options de ligne de commande spécifiques aux lancements

Option	Objectif	Exemple de syntaxe
`-is:log`*filename*	Génère un fichier journal des recherches JVM effectuées avec le programme de lancement natif.	`hodinstallwin.exe -is:log myLogFile.txt`
`-is:silent`	Empêche l'affichage de l'interface utilisateur du programme de lancement lorsque des recherches JVM ou d'autres initialisations sont en cours (option fréquemment utilisée parallèlement à l'option de ligne de commande `silent`).	`hodinstallwin.exe -is:silent`
`-is:tempdir`*répertoire*	Définit le répertoire temporaire utilisé par le programme d'installation de Host On-Demand.	`hodinstallwin.exe -is:tempdir "c:\temp"`

Annexe E. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus d'informations, 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 puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. 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
Armonk, NY 10504-1785
U.S.A.
```

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues 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 paragraphe suivant ne s'applique ni au Royaume Uni, ni dans aucun pays (ou région) dans lequel il serait contraire aux lois locales : LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. 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. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels 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 :

```
Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.
```

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

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

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance. Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les informations concernant des 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 ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Annexe F. Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays : **IBM**

Java, ainsi que l'ensemble des logos et des marques Java, sont des marques de Oracle Corporation aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows et le logo Windows sont des marques de Microsoft Corporation.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Imprimé en France

SC43-3097-02