Bull

AIX 5L Web–based System Manager
Guide d’administration

AIX

REFERENCE
86 F2 34EF 02

Bull

AIX 5L Web–based System Manager
Guide d’administration

AIX

Logiciel

Octobre 2002

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 F2 34EF 02

Imprimé en France

Vos suggestions sur la forme et le fond de ce manuel seront les bienvenues. Une feuille destinée à recevoir vos remarques se trouve à la fin de ce document.

Pour commander d’autres exemplaires de ce manuel ou d’autres publications techniques Bull, veuillez utiliser le bon de commande également fourni en fin de manuel.

Marques déposées

Toutes les marques déposées sont la propriété de leurs titulaires respectifs.

AIX® est une marque déposée d’IBM Corp. et est utilisée sous licence.

UNIX est une marque déposée, licenciée exclusivement par Open Group.

A propos de ce manuel

Ce manuel indique comment utiliser Web-based System Manager en vue d'administrer des systèmes.

A qui s'adresse ce manuel ?

Ce manuel est destiné aux administrateurs réseau qui souhaitent utiliser Web–based System Manager pour gérer leurs systèmes.

Conventions typographiques

Les conventions typographiques ci–après sont utilisées dans ce guide.

Mise en évidence	Description
Gras	Permet d'identifier les commandes, les sous–programmes, les mots clés, les fichiers, les arborescences, les répertoires, ainsi que d'autres éléments dont le nom est prédéfini par le système. Permet également d'identifier les objets graphiques, tels que les boutons, les libellés et les icônes sélectionnés par l'utilisateur.
Italique	Permet d'identifier les paramètres dont les noms ou les valeurs doivent être indiqués par l'utilisateur.
`Espacement fixe`	Permet d'identifier les exemples de données spécifiques, les exemples de textes similaires aux textes affichés, les exemples de parties de code similaires au code que vous serez susceptible de rédiger en tant que programmeur, les messages système ou les informations que vous devez saisir.

Distinction majuscules/minuscules dans AIX

La distinction majuscules/minuscules s'applique à toutes les données entrées dans le système d'exploitation AIX. Vous pouvez, par exemple, utiliser la commande **ls** pour afficher la liste des fichiers. Si vous entrez `LS`, le système affiche un message d'erreur indiquant que la commande entrée est introuvable. De la même manière, **FICHEA**, **FiChea** et **fichea** sont trois noms de fichiers distincts, même s'ils se trouvent dans le même répertoire. Pour éviter toute action indésirable, vérifiez systématiquement que vous utilisez la casse appropriée.

ISO 9000

Des systèmes de qualité homologuée **ISO 9000** ont été utilisés lors du développement et de la fabrication de ce produit.

Bibliographie

Vous trouverez des informations relatives à Web–based System Manager dans les ouvrages suivants :

- *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*
- *AIX 5L Version 5.2 System Management Guide: Operating System and Devices*

Table des matières

Chapitre 1. Présentation de Web-based System Manager

Web-based System Manager est une application de gestion de système qui permet d'administrer des ordinateurs. Elle est installée par défaut sur des systèmes graphiques et sa conception a été complètement repensée pour AIX 5.2.

Web-based System Manager comporte une console de gestion de système permettant d'administrer plusieurs hôtes. Une architecture constituée de modules complémentaires facilite l'extension de la suite. Web-based System Manager permet en outre le contrôle dynamique des événements système et leur notification à l'administrateur.

Concepts de base de Web-based System Manager

Web-based System Manager est une application client–serveur qui fournit une interface utilisateur puissante destinée à la gestion des systèmes UNIX. L'interface graphique de Web-based System Manager permet à l'utilisateur d'accéder à de multiples machines éloignées et d'en assurer la gestion. Elle se compose d'une *fenêtre de console* divisée en deux panneaux principaux. Le panneau de gauche affiche les machines que l'utilisateur peut gérer depuis la fenêtre de console. Ce panneau est appelé *zone de navigation*. Le panneau de droite (appelé *zone de contenu*) affiche des informations sur l'élément sélectionné dans la zone de navigation. La machine sur laquelle vous souhaitez effectuer des opérations de gestion doit être sélectionnée dans la zone de navigation. Lorsqu'il accède à l'opération souhaitée dans la zone de navigation, la zone de contenu est mise à jour afin d'afficher les options disponibles.

La procédure suivante présente un exemple d'utilisation de Web-based System Manager en vue de modifier les propriétés d'un utilisateur :

1. Démarrez Web-based System Manager dans une fenêtre AIX graphique en entrant la commande suivante :

   ```
   /usr/websm/bin/websm
   ```

2. Dans la zone de contenu, cliquez deux fois sur l'icône **Utilisateurs**.

   La zone de contenu affiche les catégories suivantes :

   – Rôles administratifs
   – Tous les groupes
   – Tous les utilisateurs
   – Généralités et tâches

3. Cliquez deux fois sur l'icône **Tous les utilisateurs**. La zone de contenu affiche la liste des utilisateurs et indique pour chacun d'eux s'il s'agit d'un utilisateur de base ou d'un administrateur.
4. Cliquez deux fois sur l'icône située en regard du nom de l'utilisateur dont vous souhaitez modifier les propriétés. La boîte de dialogue qui s'affiche permet de modifier les propriétés de l'utilisateur sélectionné.
5. Pour sauvegarder les modifications, cliquez sur **OK**. Pour les annuler, cliquez sur **Annulation**.

La partie client de Web-based System Manager fonctionne sur la *machine gérante*. Dans l'exemple ci–dessus, il n'est pas précisé si l'utilisateur faisant l'objet de la modification se trouvait sur la machine exécutant Web-based System Manager (le client) ou sur une machine gérée (un serveur). Pour modifier un utilisateur sur une machine gérée, sélectionnez une machine dans la zone de navigation. Si cette machine n'a encore fait l'objet d'aucune connexion, une boîte de dialogue s'affiche, qui vous demande d'entrer votre nom d'hôte, votre nom d'utilisateur et votre mot de passe. Cette boîte de dialogue vous permet de vous connecter à la machine gérée. Une fois connecté, vous pouvez effectuer des opérations à partir de la console Web-based System Manager sur une autre machine gérée et revenir à la machine (en la sélectionnant dans la zone de navigation) sans vous connecter à nouveau.

Chaque utilisateur a intérêt à conserver une machine Web-based System Manager *personnelle*. Celle–ci doit être utilisée comme machine gérante, même si l'utilisateur démarre Web-based System Manager depuis une machine autre que la machine *personnelle*. En effet, la présentation initiale de la fenêtre de console est déterminée par un fichier situé sur la machine gérante. Ainsi, vous pourrez démarrer Web-based System Manager à partir du bureau d'un autre utilisateur, définir une machine *personnelle* comme machine gérante, et créer une fenêtre de console à partir des préférences que vous avez sauvegardées. Pour en savoir plus sur la sauvegarde de préférences, reportez–vous à Fichiers de préférences, page 3-13.

La partie la plus importante des préférences sauvegardées par l'utilisateur est sans doute l'environnement de gestion de la machine. L'environnement de gestion est un mécanisme puissant qui permet de définir des ensembles de machines placées sous votre responsabilité et d'y accéder. Lorsqu'une machine de l'environnement de gestion est sélectionnée par l'utilisateur, un *serveur Web–based System Manager* est lancé sur cette machine. Ce serveur fournit au client (et indirectement à la fenêtre de console) des *objets gérés à distance*. La partie cliente de l'application présente ces objets via des fenêtres et d'autres éléments d'interface utilisateur graphique (GUI). En gérant ces éléments GUI, la partie client de l'application peut afficher des informations concernant les objets de la *machine gérée* éloignée et vous autoriser à mettre ces informations à jour.

Une fois qu'une machine de l'environnement de gestion est *active* (si vous l'avez sélectionnée dans cet environnement et que vous y êtes connecté), vous pouvez basculer d'une machine à une autre à l'aide de la souris.

Vous pouvez ainsi gérer un grand nombre de machines à l'aide d'une unique et puissante interface.

Modes d’exploitation

Vous pouvez configurer plusieurs modes d’exploitation pour Web-based System Manager. Les environnements d’exploitation dans lesquels Web-based System Manager peut être démarré sont *application autonome*, *client–serveur*, *applet* et *client éloigné*. Ces modes d’exploitation sont décrits dans les sections ci–dessous.

Mode application autonome

Aucune configuration n'est nécessaire pour exécuter Web-based System Manager en mode application autonome. Entrez la commande suivante sur la ligne de commande :

```
/usr/websm/bin/wsm
```

Pour démarrer la console Web-based System Manager depuis l'environnement CDE (environnement CDE), procédez comme suit :

1. Cliquez sur l'icône **Gestionnaire d'applications** du panneau CDE.
2. Cliquez sur l'icône **System_Admin**.
3. Cliquez sur l'icône **Console de gestion**.

Par défaut, vous pouvez exécuter des tâches de gestion de système sur la machine sur laquelle vous avez lancé la console.

Mode client–serveur

Vous pouvez gérer votre machine locale à partir de la console Web-based System Manager. Vous pouvez également gérer des machines configurées pour la gestion éloignée (voir Configuration de Web–based System Manager en mode client–serveur, page 2-4). Vous spécifiez les machines que vous voulez gérer en les ajoutant à l'environnement de gestion (voir Configuration de l'environnement de gestion, page 4-1).

Il est également possible de sélectionner en tant que *machine gérante* un hôte différent de votre machine personnelle. Utilisez pour cela la commande suivante :

```
/usr/websm/bin/wsm –host [   hôte machine gérante  ]
```

L'hôte que vous spécifiez comme [*hôte machine gérante*] s'affiche dans la zone de navigation en première position dans la liste des hôtes pouvant être gérés. Par ailleurs, cet hôte est utilisé pour charger le fichier des préférences utilisateur de Web–based System Manager (**$HOME/WebSM.pref**). L'argument **–host** affiche la console de la machine que vous utilisez, mais charge le fichier de préférences de l'hôte éloigné que vous spécifiez (voir Fichiers de préférences, page 3-13).

Remarque : Le serveur Web-based System Manager doit être installé et configuré sur tous les hôtes cible gérés par Web-based System Manager. Pour plus d'informations, reportez–vous à la section Configuration de Web–based System Manager en mode client–serveur, page 2-4.

Mode applet

Le mode applet est similaire à l'utilisation de Web-based System Manager en mode client–serveur avec l'argument **–host**. En mode client–serveur, vous utilisez la commande suivante :

```
/usr/websm/bin/wsm –host [   machine gérante  ]
```

alors qu'en mode applet, vous indiquez l'URL suivante dans votre navigateur :

```
http://   machine gérante  /wsm.html
```

Dans les deux cas, *machine gérante* est la machine sur laquelle se trouve l'application Web-based System Manager. La *machine gérée* est la première machine répertoriée dans l'environnement de gestion.

Mode applet ou mode client–serveur

Les modes applet et client–serveur sont très différents. En mode applet, vous ne pouvez gérer qu'un ensemble de machines disposant de la même version de Web-based System Manager. En effet, une restriction s'applique généralement aux applets, pour des motifs de sécurité, et ne leur permet de charger des classes Java qu'à partir du serveur HTTP exécutant l'applet. Alors que les classes Java nécessaires pour exploiter la console Web-based System Manager proviennent de la *machine gérante*, un autre jeu de classes Java est utilisé pour exécuter les tâches sur les machines gérées. Ces classes doivent être chargées depuis la machine gérée (différente de la machine gérante) afin d'être utilisables avec le système d'exploitation géré. En mode applet, cela est impossible.

Mode client éloigné

Le mode client éloigné permet à l'utilisateur de démarrer la console Web-based System Manager sur un système fonctionnant sous Windows ou Linux et de gérer des ordinateurs AIX éloignés. Ce mode est similaire à l'utilisation de Web-based System Manager en mode client–serveur avec l'argument *–host*. Vous pouvez démarrer le mode client éloigné de plusieurs façons :

Sous Windows, procédez comme suit :

- Cliquez deux fois sur l'icône **Client distant Web–based System Manager**, qui se trouve sur le bureau Windows, afin d'ouvrir l'application.
- Cliquez sur le bouton Démarrer dans la barre des tâches, puis sélectionnez **Programmes —> Web–based System Manager —> Client distant Web–based System Manager**.
- A partir d'une invite MS–DOS, exécutez la commande **wsm.bat** dans le répertoire bin du client éloigné.
- Dans l'Explorateur Windows, cliquez deux fois sur l'icône **wsm.bat** dans le dossier bin du client éloigné.

Sous Linux, si vous utilisez le bureau Gnome, procédez comme suit :

- Cliquez sur le bouton du menu Gnome dans la barre des tâches, puis sélectionnez **Programmes —> Client distant Web–based System Manager**.
- A partir d'une invite xterm, exécutez la commande **wsm** dans le répertoire bin du client éloigné.

Sous Linux, si vous utilisez le bureau KDE, procédez comme suit :

- Cliquez sur le bouton du menu KDE dans la barre des tâches, puis sélectionnez **Programmes —> Client distant Web–based System Manager**.
- A partir d'une invite xterm, exécutez la commande **wsm** dans le répertoire bin du client éloigné.

Comme avec le mode client–serveur, les systèmes répertoriés dans la zone d'environnement de gestion sont des machines gérées. Cependant, le système Windows ou Linux qui exécute le client éloigné correspond à la machine gérante et ne s'affiche pas dans la zone d'environnement de gestion.

Les incidents liés à la sécurité concernant les classes de chargement sont les mêmes qu'en mode client–serveur. Par contre, le mode applet comporte quelques restrictions ; vous ne pouvez gérer qu'un ensemble de machines disposant de la même version de Web-based System Manager. Pour en savoir plus, reportez–vous au chapitre Sécurité Web-based System Manager, page 5-1.

Pour de plus amples informations, reportez–vous aux sections Mode client–serveur, page 1-6 et Mode applet, page 1-7.

Applications personnalisées

Vous pouvez utiliser l'application Outils personnalisés pour ajouter des commandes et applications disponibles sur votre système AIX sur l'environnement de Web-based System Manager, qui peuvent ensuite être exécutés directement à partir de la fenêtre de console.

Si vous souhaitez obtenir plus d'intégration que ce qu'offre l'application Outils personnalisés, vous pouvez augmenter les capacités de Web-based System Manager en écrivant des applications personnalisées. Ceci implique de connaître le langage de programmation Java. Si cette possibilité vous intéresse, veuillez prendre contact avec votre revendeur.

Chapitre 2. Installation de Web-based System Manager

Les procédures suivantes sont requises pour l'installation de Web–based System Manager :

Configuration minimale recommandée

Pour utiliser Web-based System Manager, vous devez être équipé d'un ordinateur client présentant la configuration minimum suivante :

- Système d'exploitation de base AIX 5.2 (Java 1.3.1 inclus)
- Écran graphique connecté
- 300 Mo d'espace disque disponible
- 256 Mo de mémoire disponible au minimum (512 Mo sont recommandés)
- Processeur cadencé à 300 MHz

Les versions antérieures d'AIX ne peuvent pas prendre en charge les versions ultérieures d'AIX, et réciproquement. Par exemple, si un client exécute AIX 4.3.3, un serveur utilisant AIX 5.1 ne pourra le prendre en charge. L'inverse est également vrai. Les clients et les serveurs doivent donc utiliser le même niveau d'AIX pour pouvoir se prendre en charge mutuellement.

Si vous exécutez Web-based System Manager sur un PC en mode applet, il doit intégrer un processeur cadencé au minimum à 800 MHz.

Si vous exécutez Web-based System Manager sur un système Windows ou Linux en mode client éloigné, reportez–vous à Spécifications système recommandées pour le client éloigné, page 2-7 pour savoir quelles sont les autres spécifications.

Bien qu'il ne soit absolument pas nécessaire de disposer d'un ordinateur équipé de la mémoire et du processeur requis, il faut savoir que les performances peuvent être réduites sur des machines de moindre puissance. La configuration minimum requise présentée ci–dessus s'applique principalement à un ordinateur client. Si ce dernier n'est pas doté de la configuration minimum recommandée, ses performances peuvent être réduites.

Étant donné que les machines serveur n'affichent pas de graphiques à l'utilisateur, il n'est pas obligatoire qu'elles répondent aux critères de configuration minimum recommandés. Pour en savoir plus, reportez–vous à Modes d'exploitation, page 1-4.

En mode applet et client–serveur, la machine client n'est pas nécessairement celle sur laquelle s'affiche la console Web-based System Manager.

L'utilisation de Web-based System Manager avec des émulateurs X (tels que ceux utilisés sur un PC) n'est pas recommandée car les performances obtenues avec ces émulateurs ne sont pas satisfaisantes.

Installation de Web-based System Manager

Web–based System Manager doit être installé sur le client et sur toutes les machines gérées. Si AIX 5.2 est déjà installé sur votre machine, il est possible que Web-based System Manager soit également déjà installé.

Pour vous en assurer, entrez la commande suivante :

```
lslpp –h sysmgt.websm.framework
```

Si Web-based System Manager n'est pas installé, un message similaire à celui–ci s'affiche :

```
lslpp: L'ensemble de fichiers sysmgt.websm.framework n'est pas installé.
```

Si Web-based System Manager est installé, un tableau similaire à celui–ci s'affiche :

```
Ensemble de fichiers
            Niveau Opération   Etat            Date        Heure
-------------------------------------------------------------------------------
Chemin : /usr/lib/objrepos
  sysmgt.websm.framework
                5.2.0.0     VALIDATION       TERMINEE     03/09/01
17:30:14

Chemin : /etc/objrepos
  sysmgt.websm.framework
                5.2.0.0     VALIDATION       TERMINEE     03/09/01
17:35:31
```

Si l'ensemble de fichiers **sysmgt.websm.framework** n'est pas installé, vous devez utiliser les outils d'installation du système d'exploitation. Pour accéder à ces outils d'installation, tapez les commandes suivantes (en vérifiant que le CD version 5.2 de AIX est bien chargé dans votre unité de CD–ROM) :

```
/usr/lib/instl/sm_inst installp_cmd -a \
-d /dev/cd0 -f sysmgt.websm.framework  -c -N -g -X
```

Cette commande installe l'ensemble d'images requis pour l'exécution de Web–based System Manager.

Configuration de Web–based System Manager en mode client–serveur

En mode client–serveur (voir Modes d'exploitation, page 1-4) le client Web-based System Manager fait appel à des services serveur à partir d'une machine gérée par l'intermédiaire du port 9090. Le mode client–serveur doit être activé sur les serveurs qui seront gérés en tant que machine éloignées. Pour activer une machine en tant que serveur Web-based System Manager ou la désactiver, vous pouvez utiliser la commande **wsmserver** (voir Outils de la ligne de commande, page 3-15) de la façon suivante :

```
/usr/websm/bin/wsmserver –enable
```

Pour désactiver une machine afin qu'il ne soit plus possible de la gérer à partir d'un client Web-based System Manager, entrez la commande suivante :

```
/usr/websm/bin/wsmserver –disable
```

Affectation des valeurs de ports

Deux types de ports peuvent être utilisés avec le serveur Web-based System Manager : les ports inetd et les ports socket de serveur. Dans certains cas, vous devez modifier les numéros de ces ports.

Ports inetd

Le port inetd est susceptible d'être utilisé par plusieurs programmes de votre système. Si un autre programme de votre système utilise le numéro de port inetd 9090, modifiez le numéro de port attribué à la connexion du serveur Web-based System Manager en procédant de l'une des manières suivantes :

- Définissez un numéro de port différent dans le fichier **/etc/services**. Si vous optez pour cette méthode, utilisez la commande **wsm** avec l'argument **–port** (voir Outils de la ligne de commande, page 3-15).
- Entrez la commande suivante :

  wsmserver –enable –listenport *numéro de port*

où *numéro de port* est le nouveau port de connexion du serveur Web-based System Manager.

Lorsque vous définissez un numéro de port inetd autre que 9090, vous devez indiquer à la machine client le numéro que vous avez choisi, afin qu'elle puisse se connecter au serveur. Pour ce faire, ajoutez l'hôte au domaine (realm) du client en utilisant le format suivant :

hôte : *port*

où *hôte* est le nom de la machine serveur ou hôte, et *port* correspond au numéro de port.

Ports socket de serveur

Les numéros de ports socket de serveur sont sélectionnés de façon dynamique par le système lors de l'exécution, dans la plage de valeurs indiquée. Pour définir cette plage, entrez la commande suivante :

wsmserver –enable –portstart *début de plage* –portend *fin de plage*

où *début de plage* est le plus petit numéro de port disponible et *fin de plage* est le plus grand numéro de port disponible. Le serveur Web-based System Manager crée alors des ports socket en utilisant les numéros contenus dans cette plage. Si vous voulez que plusieurs serveurs Web-based System Manager puissent s'exécuter simultanément, veillez à indiquer une plage de numéros de ports permettant à chaque serveur de disposer de son propre port.

Ensembles de fichiers optionnels disponibles avec Web-based System Manager

Les ensembles de fichiers facultatifs suivants peuvent être installés pour optimiser Web–based System Manager :

sysmgt.msg. *Langue*.websm.apps
: Autorise l'utilisation d'une langue locale si la variable d'environnement **LANG** est définie ou si l'argument **–lang** est utilisé avec la commande **wsm**.

sysmgt.websm.security
: Permet la prise en charge des communications SSL (Secure Socket Layer) entre le client et le serveur. Il permet le chiffrement sur 40 bits et est disponible dans l'Expansion Pack.

sysmgt.websm.security–us
: Permet la prise en charge des communications SSL (Secure Socket Layer) entre le client et le serveur. Il permet le chiffrement sur 128 bits et est disponible dans l'Expansion Pack. En raison de la réglementation américaine concernant les exportations et importations, cet ensemble de fichiers peut ne pas être disponible dans certains pays.

Les ensembles de fichiers présentés dans la liste ci–dessus ne sont pas installés par défaut avec le système d'exploitation de base. Cependant, ils peuvent être installés à l'aide de la procédure d'installation des images–mémoire de Web-based System Manager (voir plus haut). Entrez la commande suivante à partir du support contenant l'ensemble de fichiers :

```
/usr/lib/instl/sm_inst installp_cmd –a –d /dev/cd0 \
–f   ens_fichiers_à_installer   –c –N –g –X
```

Spécifications d'installation pour la prise en charge du mode Applet

Outre le mode d'application standard de Web-based System Manager, vous devez disposer de l'ensemble de fichiers **sysmgt.websm.webaccess** pour pouvoir utiliser le mode applet. Cet ensemble de fichiers est automatiquement installé avec le système d'exploitation de base.

La machine à utiliser comme **machine gérante** doit être définie comme serveur HTTP. Cette définition peut être effectuée en installant et en configurant le serveur HTTP de votre choix. Le serveur HTTP est disponible sur l'Expansion Pack AIX 5.2. Utilisez la commande **/usr/websm/bin/configassist** pour configurer automatiquement le serveur HTTP.

La configuration permettant d'utiliser Web-based System Manager en mode applet avec Netscape Communicator ou Internet Explorer est la suivante :

- Système d'exploitation : Windows NT 4.0, 2000 ou XP.
- La version 4.7 ou 4.7x de Netscape Communicator est requise. (Netscape Communicator 6.0 ou ultérieur n'est pas pris en charge.)
- Le module complémentaire Java 1.3 doit être installé.

Remarque : Le mode applet n'est pas supporté sur PowerPC. Reportez–vous à Modes d'exploitation, page 1-4 pour plus de détails sur la gestion des systèmes PowerPC.

Pour configurer un serveur pour le mode applet, procédez comme suit :

1. Installez un serveur HTTP sur la machine sur laquelle réside Web-based System Manager. Le serveur Web recommandé est le serveur HTTP. Reportez–vous à la documentation de chaque produit pour l'installation et la configuration du serveur HTTP.
2. Lorsque le serveur HTTP est en cours d'exécution, vous pouvez configurer Web-based System Manager de sorte qu'il s'exécute à partir de ce serveur. Pour cela, entrez la commande suivante :

   ```
   /usr/websm/bin/configassist
   ```

3. Dans l'assistant de configuration, suivez les instructions jusqu'à ce que vous atteigniez l'écran principal.
4. Sélectionnez **Configuration d'un serveur Web pour exécution de** Web-based System Manager **dans un navigateur**.
5. Cliquez sur **Suivant**.
6. Suivez les instructions affichées sur les écrans successifs pour terminer les configurations.

Configuration du client (navigateur)

La configuration requise pour le client est la suivante :

- Netscape Communicator 4.7 ou 4.7x (Netscape Communicator 6.0 ou ultérieur n'est pas pris en charge), ou Internet Explorer 5.0 ou ultérieur.
- Module complémentaire Java 1.3.

Si vous utilisez le navigateur Internet Explorer, il vous sera proposé de télécharger automatiquement le module complémentaire. Si vous cliquez sur **oui**, le module complémentaire est téléchargé et son script d'installation est exécuté. Si vous cliquez sur **non**, Web-based System Manager se ferme.

Si le navigateur que vous utilisez est Netscape Communicator, il se peut qu'il n'arrive pas à localiser le module complémentaire Java correct. Dans ce cas, vous pouvez le télécharger et l'installer manuellement.

Installation du client distant Web-based System Manager

Les rubriques suivantes fournissent des informations concernant l'installation de la sécurité du client éloigné Web-based System Manager :

Spécifications système recommandées pour le client éloigné

Si vous comptez utiliser un PC pour exécuter Web-based System Manager en mode client éloigné, l'ordinateur considéré doit être configuré comme suit :

- Système d'exploitation : Windows (les versions prises en charge sont NT, 2000 et XP) ou Linux (les versions prises en charge sont Red Hat 7.2 et Red Hat 7.3).
- 75 Mo d'espace disque sur l'unité par défaut pour une utilisation temporaire pendant la procédure d'installation.
- 75 Mo d'espace disque sur l'unité sur laquelle vous voulez installer le client distant Web-based System Manager.
- Processeur cadencé à 800 MHz.
- 256 Mo de mémoire disponible au minimum (512 Mo sont recommandés).

Spécifications d'installation pour le support du mode client éloigné

Pour installer le client distant Web-based System Manager sur un réseau, l'ensemble de fichiers **sysmgt.websm.webaccess** doit être installé sur au moins un système AIX. Cet ensemble de fichiers est automatiquement installé avec le système d'exploitation de base.

La machine utilisée pour installer le client distant Web-based System Manager doit être définie comme serveur HTTP. Cette définition peut être effectuée en installant et en configurant le serveur HTTP de votre choix. Le serveur HTTP est disponible sur l'Expansion Pack AIX 5.2. Utilisez la commande **/usr/websm/bin/configassist** pour configurer automatiquement le serveur HTTP.

Configuration d'un serveur AIX pour l'installation du client éloigné

La procédure suivante vous permet de configurer un serveur AIX pour l'installation du client distant Web-based System Manager :

1. Installez un serveur HTTP sur le serveur sur lequel réside Web-based System Manager. Le serveur Web recommandé est le serveur HTTP. Reportez–vous à la documentation de chaque produit pour l'installation et la configuration du serveur HTTP.
2. Une fois que le serveur HTTP est activé, entrez la commande suivante pour configurer Web–based System Manager :
   `/usr/websm/bin/configassist`

3. Dans l'assistant de configuration, suivez les instructions jusqu'à ce que vous atteigniez l'écran principal.
4. Sélectionnez **Configuration d'un serveur Web pour exécution de** Web-based System Manager **dans un navigateur**.
5. Cliquez sur **Suivant**.
6. Suivez les instructions affichées sur les écrans successifs pour terminer les configurations.

Installation du client distant Web-based System Manager sur le système Windows

1. Désinstallez les versions précédentes du client distant Web-based System Manager. Pour plus d'informations, reportez–vous à Désinstallation du client distant Web-based System Manager d'un système Windows, page 2-8.
2. Entrez l'adresse suivante dans le navigateur Web de votre machine :

   ```
   http://   nom_hôte  /remote_client.html
   ```

   où *nom_hôte* est le nom du serveur AIX configuré pour l'installation du client distant Web-based System Manager.
3. Cliquez sur le lien **Windows** qui s'affiche sur la page Web. Le fichier **setup.exe** est téléchargé sur votre machine.
4. Le téléchargement terminé, exécutez le fichier **setup.exe** pour démarrer la procédure d'installation.
5. Lorsque le panneau d'**installation du client éloigné** s'affiche, cliquez sur **Suivant** pour continuer.
6. Pour installer en utilisant l'emplacement par défaut, cliquez sur **Suivant** ou entrez l'emplacement choisi, puis cliquez sur **Suivant**.
7. Un écran de confirmation s'affiche pour indiquer l'emplacement de l'installation, le module installé et la taille approximative du dossier d'installation. Cliquez sur **Suivant** pour démarrer l'installation. Si une ou plusieurs des informations affichées sont incorrectes, cliquez sur **Précédent** pour revenir en arrière afin de pouvoir apporter les corrections requises.
8. Un écran d'état affiche des messages d'erreur si des erreurs se sont produites lors de l'installation, ou un message indiquant que l'installation a réussi. Cliquez sur **Fin** pour fermer le panneau.

Désinstallation du client distant Web-based System Manager d'un système Windows

1. A partir de la barre des tâches, sélectionnez **Démarrer —> Paramètres —> Panneau de configuration**.
2. Dans le **panneau de configuration**, cliquez deux fois sur l'icône **Ajout/Suppression de programmes**.
3. Sélectionnez **Client distant Web–based System Manager** dans la liste de programmes de la fenêtre d'**installation/désinstallation**, puis cliquez sur le bouton **Modifier/Supprimer** pour démarrer l'assistant de désinstallation.

Remarque : Il est possible que les versions antérieures du client distant s'intitulent **Client PC** Web-based System Manager.

4. Cliquez sur **Suivant** dans le panneau initial.
5. Cliquez sur **Suivant** dans le panneau de confirmation pour désinstaller le client distant.

6. Un écran d'état affiche des messages d'erreur si des erreurs se sont produites lors de l'installation, ou un message indiquant que l'installation a réussi. Cliquez sur **Fin** pour fermer le panneau.

Installation du client distant Web-based System Manager sur un système Linux

1. Désinstallez la version précédente du client distant Web-based System Manager sur votre machine. Pour plus d'informations, reportez–vous à Désinstallation du client distant Web-based System Manager d'un système Linux, page 2-9.
2. Entrez l'adresse suivante dans le navigateur Web de votre machine :

   ```
   http://   nom_hôte  /remote_client.html
   ```

   où *nom_hôte* est le nom du serveur AIX configuré pour l'installation du client distant Web-based System Manager.
3. Cliquez sur le lien **Linux** qui s'affiche sur la page Web. Le fichier **wsmlinuxclient.exe** est téléchargé sur votre machine.
4. Exécutez ce fichier pour démarrer la procédure d'installation. Si la procédure de démarre pas, modifiez les droits d'accès au fichier afin de disposer des droits d'exécution. Pour ce faire, entrez la commande suivante sur la ligne de commande :

   ```
   chmod 755 wsmlinuxclient.exe
   ```
5. Lorsque le panneau d'**installation du client éloigné** s'affiche, cliquez sur **Suivant** pour continuer.
6. Pour installer en utilisant l'emplacement par défaut, cliquez sur **Suivant** ou entrez l'emplacement choisi, puis cliquez sur **Suivant**.
7. Un écran de confirmation s'affiche pour indiquer l'emplacement de l'installation, le module installé et la taille approximative du dossier d'installation. Cliquez sur **Suivant** pour démarrer l'installation. Si une ou plusieurs des informations affichées sont incorrectes, cliquez sur **Précédent** pour revenir en arrière afin de pouvoir apporter les corrections requises.
8. Un écran d'état affiche des messages d'erreur si des erreurs se sont produites lors de l'installation, ou un message indiquant que l'installation a réussi. Cliquez sur **Fin** pour fermer le panneau.

Remarque : Si les modifications ne prennent pas effet immédiatement, fermez votre session en cours et ouvrez–en une autre, ou régénérez votre fichier**. /etc/profile**.

Désinstallation du client distant Web-based System Manager d'un système Linux

Pour désinstaller le client éloigné sur un système Linux, entrez la commande suivante :

```
rép_install  /_uninst/uninstall
```

où *rép_install* est le nom du répertoire dans lequel le client distant est installé.

Installation de la sécurité du client distant Web-based System Manager

Les rubriques suivantes fournissent des informations concernant l'installation de la sécurité du client distant Web-based System Manager :

- Spécifications système recommandées pour la sécurité du client éloigné, page 2-10
- Spécifications d'installation pour le support de la sécurité du client éloigné, page 2-10

- Configuration d'un serveur AIX pour l'installation de la sécurité du client éloigné, page 2-10
- Installation de la sécurité du client distant Web-based System Manager sur le système Windows, page 2-11
- Désinstallation de la sécurité du client distant Web-based System Manager d'un système Windows, page 2-11
- Installation de la sécurité du client distant Web-based System Manager sur un système Linux, page 2-12
- Désinstallation de la sécurité du client distant Web-based System Manager d'un système Linux, page 2-12

Spécifications système minimum recommandées pour la sécurité du client éloigné

Si vous comptez utiliser un PC pour exécuter Web-based System Manager en mode client éloigné sécurisé, l'ordinateur considéré doit être configuré comme suit :

- Système d'exploitation : Windows (les versions prises en charge sont NT, 2000 et XP) ou Linux (les versions prises en charge sont Red Hat 7.2 et Red Hat 7.3).
- 75 Mo d'espace disque sur l'unité par défaut pour une utilisation temporaire pendant la procédure d'installation.
- 75 Mo d'espace disque sur l'unité sur laquelle vous voulez installer la sécurité du client distant Web-based System Manager.
- Un processeur cadencé au minimum à 800 MHz.
- 256 Mo de mémoire disponible au minimum (512 Mo sont recommandés).

Spécifications d'installation pour le support de la sécurité du client éloigné

Pour installer la sécurité du client distant Web-based System Manager sur un réseau, l'ensemble de fichiers **sysmgt.websm.security** doit être installé sur au moins un système AIX. Pour un chiffrement plus efficace, installez aussi l'ensemble de fichiers **sysmgt.websm.security–us**. Ces ensembles de fichiers sont disponibles sur l'Expansion Pack AIX 5.2.

La machine utilisée pour installer le client distant Web-based System Manager doit être définie comme serveur HTTP. Cette définition peut être effectuée en installant et en configurant le serveur HTTP de votre choix. Le serveur HTTP est disponible sur l'Expansion Pack AIX 5.2. Utilisez la commande **/usr/websm/bin/configassist** pour configurer automatiquement le serveur HTTP. De plus, l'ensemble de fichiers **sysmgt.websm.security** doit être installé sur le serveur, l'installation de l'ensemble de fichiers **sysmgt.websm.security–us** étant facultative.

Configuration d'un serveur AIX pour l'installation de la sécurité du client éloigné

Remarque : Si vous avez déjà configuré un serveur AIX pour l'installation du client distant Web-based System Manager, vous pouvez ignorer cette section.

La procédure suivante vous permet de configurer un serveur AIX pour l'installation du client distant Web-based System Manager :

1. Installez un serveur HTTP sur le serveur sur lequel réside Web-based System Manager. Le serveur Web recommandé est le serveur HTTP. Reportez–vous à la documentation de chaque produit pour l'installation et la configuration du serveur HTTP.
2. Une fois que le serveur HTTP est activé, entrez la commande suivante pour configurer Web–based System Manager :

```
/usr/websm/bin/configassist
```

3. Dans l'assistant de configuration, suivez les instructions jusqu'à ce que vous atteigniez l'écran principal.
4. Sélectionnez **Configuration d'un serveur Web pour exécution de** Web-based System Manager **dans un navigateur**.
5. Cliquez sur **Suivant**.
6. Suivez les instructions affichées sur les écrans successifs pour terminer les configurations.

Installation de la sécurité du client distant Web-based System Manager sur le système Windows

1. Désinstallez les versions précédentes de la sécurité du client distant Web-based System Manager. Pour plus d'informations, reportez–vous à Désinstallation de la sécurité du client distant Web-based System Manager d'un système Windows, page 2-11.
2. Entrez l'adresse suivante dans le navigateur Web de votre machine :

   http:// *nom_hôte* /remote_client_security.html

   où *nom_hôte* est le nom du serveur AIX configuré pour l'installation de la sécurité du client distant Web-based System Manager.
3. Cliquez sur le lien **Windows** qui s'affiche sur la page Web. Le fichier **setupsec.exe** est téléchargé sur votre machine.
4. Exécutez ce fichier pour démarrer la procédure d'installation.
5. Lorsque le panneau d'**installation de la sécurité du client éloigné** s'affiche, cliquez sur **Suivant** pour continuer.
6. Pour installer en utilisant l'emplacement par défaut, cliquez sur **Suivant** ou entrez l'emplacement choisi, puis cliquez sur **Suivant**.

Remarque : Dans cette étape, vérifiez que vous avez sélectionné le même emplacement que celui que vous avez choisi à l'étape 6 de la section Installation du client distant Web-based System Manager sur le système Windows, page 2-8.

7. Un écran de confirmation s'affiche pour indiquer l'emplacement de l'installation, le module installé et la taille approximative du dossier d'installation. Cliquez sur **Suivant** pour démarrer l'installation. Si une ou plusieurs des informations affichées sont incorrectes, cliquez sur **Précédent** pour revenir en arrière afin de pouvoir apporter les corrections requises.
8. Un écran d'état affiche des messages d'erreur si des erreurs se sont produites lors de l'installation, ou un message indiquant que l'installation a réussi. Cliquez sur **Fin** pour fermer le panneau.

Désinstallation de la sécurité du client distant Web-based System Manager d'un système Windows

1. A partir de la barre des tâches, sélectionnez **Démarrer —> Paramètres —> Panneau de configuration**.
2. Dans le **panneau de configuration**, cliquez deux fois sur l'icône **Ajout/Suppression de programmes**.
3. Sélectionnez **Sécurité du client distant Web–based System Manager** dans la liste de programmes de la fenêtre d'**installation/désinstallation**, puis cliquez sur le bouton **Modifier/Supprimer** pour démarrer l'assistant de désinstallation.

Remarque : Il est possible que les versions antérieures de la sécurité du client distant s'intitulent **Sécurité du Client PC** Web-based System Manager.

4. Cliquez sur **Suivant** dans le panneau initial.

5. Cliquez sur **Suivant** dans le panneau de confirmation pour désinstaller la sécurité du client distant.
6. Un écran d'état affiche des messages d'erreur si des erreurs se sont produites lors de l'installation, ou un message indiquant que l'installation a réussi. Cliquez sur **Fin** pour fermer le panneau.

Installation de la sécurité du client distant Web-based System Manager sur un système Linux

1. Désinstallez la version précédente de la sécurité du client distant Web-based System Manager sur votre machine. Pour plus d'informations, reportez–vous à Désinstallation de la sécurité du client distant Web-based System Manager d'un système Linux, page 2-12.
2. Entrez l'adresse suivante dans le navigateur Web de votre machine :

   ```
   http://   nom_hôte  /remote_client_security.html
   ```

   où *nom_hôte* est le nom du serveur AIX configuré pour l'installation de la sécurité du client distant Web-based System Manager.
3. Cliquez sur le lien **Linux** qui s'affiche sur la page Web. Le fichier **setupsecl.exe** est téléchargé sur votre machine.
4. Le téléchargement terminé, exécutez le fichier **setupsecl.exe** pour démarrer la procédure d'installation. Si la procédure ne démarre pas, modifiez les droits d'accès au fichier afin de disposer des droits d'exécution. Pour ce faire, entrez la commande suivante sur la ligne de commande :

   ```
   chmod 755 setupsecl.exe
   ```
5. Lorsque le panneau d'**installation de la sécurité du client éloigné** s'affiche, cliquez sur **Suivant** pour continuer.
6. Pour installer en utilisant l'emplacement par défaut, cliquez sur **Suivant** ou entrez l'emplacement choisi, puis cliquez sur **Suivant**.

Remarque : Dans cette étape, vérifiez que vous avez sélectionné le même emplacement que celui que vous avez choisi à l'étape 6 de la section Installation du client distant Web-based System Manager sur le système Linux, page 2-9.

7. Un écran de confirmation s'affiche pour indiquer l'emplacement de l'installation, le module installé et la taille approximative du dossier d'installation. Cliquez sur **Suivant** pour démarrer l'installation. Si une ou plusieurs des informations affichées sont incorrectes, cliquez sur **Précédent** pour revenir en arrière afin de pouvoir apporter les corrections requises.
8. Un écran d'état affiche des messages d'erreur si des erreurs se sont produites lors de l'installation, ou un message indiquant que l'installation a réussi. Cliquez sur **Fin** pour fermer le panneau.

Remarque : Si les modifications ne prennent pas effet immédiatement, fermez votre session en cours et ouvrez–en une autre, ou régénérez votre fichier**. /etc/profile**.

Désinstallation de la sécurité du client distant Web-based System Manager d'un système Linux

Pour désinstaller la sécurité du client éloigné sur un système Linux, entrez la commande suivante :

```
rép_install  /_uninstssl/uninstallssl
```

où *rép_install* est le nom du répertoire dans lequel le client distant est installé.

Spécifications d'installation pour le support Secure Socket Layer

Pour que Web-based System Manager fonctionne en mode sécurisé (à l'aide de sockets SSL qui chiffrent les données transmises sur le réseau), l'ensemble de fichiers **sysmgt.websm.security** doit être installé sur le serveur et la sécurité doit être configurée sur le client et le serveur.

Pour le chiffrement sur 128 bits des données envoyées sur le réseau, l'ensemble de fichiers **sysmgt.websm.security–us** doit être installé en complément de l'ensemble **sysmgt.websm.security**. Cette configuration est décrite dans le chapitre Sécurité Web-based System Manager, page 5-1.

Intégration de Web-based System Manager dans la console de contrôle Tivoli Netview

Si vous utilisez Tivoli NetView pour AIX, vous pouvez intégrer Web–based System Manager dans la console. Cette intégration permet aux systèmes de serveurs AIX qui apparaissent sur la console NetView d'être gérés à l'aide de Web–based System Manager.

Pour ajouter Web-based System Manager à Tivoli NetView, entrez la commande suivante :

```
/usr/websm/bin/install_nv6k
```

Remarque : Avant de lancer cette commande, vous devez vous assurer que Tivoli NetView est installé et qu'il fonctionne correctement.

Pour supprimer Web-based System Manager de Tivoli NetView, entrez la commande suivante :

```
/usr/websm/bin/remove_nv6k
```

Chapitre 3. Utilisation de Web–based System Manager

Vous pouvez accéder à la console Web-based System Manager à partir de n'importe quel système connecté localement à la console et disposant d'une interface graphique. Utilisez l'une des méthodes décrites dans la section Modes d'exploitation, page 1-4 pour démarrer Web-based System Manager :

La console comporte les cinq éléments suivants :

- Zone de navigation; page 3-2
- Zone de contenu, page 3-3
- Menus et barre d'outils, page 3-6
- Zone Astuces, page 3-9
- Barre d'état, page 3-11

Zone de navigation

La *zone de navigation* affiche une hiérarchie d'icônes représentant des groupes d'ordinateurs, des ordinateurs individuels, des ressources gérées et des tâches. Chaque icône de la zone de navigation identifie un *module complémentaire*. L'*environnement de gestion* se trouve à la racine de la structure hiérarchique. Le module complémentaire Environnement de gestion contient au moins un module complémentaire correspondant à un ordinateur hôte géré par la console. Chaque module complémentaire d'ordinateur contient plusieurs modules complémentaires d'application comportant des objets gérés, des tâches et des actions pour un ensemble lié d'entités ou de ressources système.

Lorsque vous cliquez sur l'icône d'un module complémentaire dans la zone de navigation, il s'ouvre et affiche son contenu dans la zone de contenu. Les icônes de la zone de navigation peuvent être précédées d'un signe '+' (symbole d'extension) ou d'un signe '–' (symbole de réduction). Le symbole d'extension indique que le module complémentaire correspondant contient d'autres modules complémentaires qui ne sont pas affichés. Le symbole de réduction indique que le module complémentaire a déjà été étendu pour afficher les modules complémentaires qu'il contient. Cliquer sur le symbole permet d'afficher ou de masquer les modules complémentaires contenus dans le module considéré mais n'affecte pas la zone de contenu. Lorsque vous cliquez une fois sur une icône de la zone de navigation, les modules complémentaires de niveau inférieur s'affichent dans la zone de contenu, mais la branche de la zone de navigation représentée par le symbole d'extension n'est pas développée. En revanche, lorsque vous cliquez deux fois sur une icône de la zone de navigation, l'arborescence de la branche de navigation se développe et la zone de contenu est mise à jour de manière à afficher les modules complémentaires de niveau inférieur.

Vous pouvez ajuster la largeur de la zone de navigation par rapport à la zone de contenu en cliquant sur la barre de fractionnement et en la faisant glisser vers la droite ou vers la gauche. Pour optimiser l'espace disponible pour la zone de contenu dans la console, vous pouvez masquer totalement la zone de navigation en faisant glisser la barre de fractionnement à l'extrême gauche de la fenêtre. Vous pouvez également cliquer sur le cadre de la zone de navigation pour la fermer, ou pour la rouvrir, selon qu'elle est affichée ou non.

Zone de contenu

La zone de contenu affiche les éléments contenus dans un module complémentaire. La zone de contenu affiche les trois principaux types de modules complémentaires suivants :

- Conteneurs, page 3-3
- Généralités, page 3-5
- Lanceurs, page 3-5

Conteneurs

Les conteneurs ou *modules complémentaires Conteneur* renferment d'autres modules complémentaires, des icônes représentant les ressources système (*objets gérés*) ou des objets gérés associés à des modules complémentaires. Les conteneurs constituent le principal type de module complémentaire de l'interface utilisateur de Web-based System Manager. Ils s'apparentent à des dossiers contenant des sous–dossiers ou des objets renfermant des informations.

Les conteneurs permettent entre autres de visualiser les caractéristiques, de créer ou de supprimer des ressources système. Ils présentent des objets de ressources dans une ou plusieurs *vues*. Web-based System Manager prend en charge les vues suivantes :

- Icônes normales
- Icônes réduites
- Détails
- Arborescence
- Arborescence détaillée

Filtrage et tri des vues

Les types d'affichage Icônes normales, Icônes réduites et Détails permettent de définir les objets à afficher en *filtrant* la vue. Cette fonction est utile pour les conteneurs denses pour lesquels vous souhaitez uniquement afficher des objets ou des types d'objets spécifiques. Ainsi, si vous gérez des utilisateurs, vous pouvez uniquement faire apparaître les administrateurs.

- Pour filtrer les objets, procédez comme suit :
  1. Sélectionnez le menu Vue.
  2. Sélectionnez **Filtrage des icônes**. L'onglet **Filtre** vous permet de définir une liste d'objets à exclure de l'affichage.
- Pour indiquer un objet à masquer, procédez comme suit :
  1. Vérifiez que la valeur de l'option **Eléments correspondants** est **masqués**.
  2. Tapez son nom dans la zone située à droite du bouton **Ajout**.
  3. Cliquez sur le bouton **Ajout**.

     Répétez cette opération pour chaque objet que vous souhaitez masquer.

     Vous pouvez également cliquer sur le bouton **Parcourir** pour afficher la liste des objets pouvant être masqués. Sélectionnez alors les objets que vous souhaitez masquer et cliquez sur **OK**. Ceux–ci sont répertoriés dans la liste **Objets masqués**.
  4. Pour supprimer des objets répertoriés dans la zone de contenu, cliquez sur **OK** ou sur **Application**.

  Pour afficher uniquement les éléments correspondant aux critères de filtrage, vous pouvez définir l'option **Eléments correspondants** sur la valeur *affichés*.

- L'onglet **Avancé** permet de définir de une à trois règles de masquage des objets basées sur les attributs de ces objets. Par exemple, pour masquer tous les administrateurs dans le module complémentaire Tous les utilisateurs, procédez comme suit :

  1. Ouvrez la boîte de dialogue de filtrage et sélectionnez l'onglet **Avancé**. Vérifiez que la case **Masquage des objets** est cochée.
  2. Vérifiez que la valeur de l'option **Eléments correspondants** est **masqués**.

     Si vous définissez plusieurs règles de masquage, gardez à l'esprit que :

     - la valeur **Correspond à toutes les règles** filtre les éléments qui correspondent à toutes les règles définies ;
     - la valeur **Correspond à une règle quelconque** filtre les éléments qui correspondent à l'une des règles définies au moins.
  3. Sélectionnez la caractéristique **Type** et la relation **=**.
  4. Tapez la valeur correspondante **Administrateur**, puis cliquez sur **OK** ou sur **Application**.

     Tous les administrateurs sont supprimés de l'affichage. Pour créer des règles supplémentaires, cliquez sur le bouton **Ajout d'une règle**. Une nouvelle ligne de définition de règles s'affiche. Les règles multiples sont combinées par l'opérateur AND.

     Pour supprimer des règles, cliquez sur le bouton **Suppression** situé à droite de la règle à supprimer. Pour supprimer la dernière règle, supprimez la valeur de la règle.

  Pour afficher uniquement les éléments correspondant aux critères de filtrage, vous pouvez définir l'option **Eléments correspondants** sur la valeur *affichés*.

- Dans l'un des deux onglets de la boîte de dialogue de filtrage, vous pouvez désactiver le filtrage en cochant la case **Désactiver tous les filtres**. Vos critères de filtrage restent définis et vous pouvez les réactiver en désélectionnant cette case.

Lorsque la case **Masquage** est cochée sur les onglets **Filtre** et **Avancé**, vous pouvez les utiliser en association.

Les modes d'affichage Icônes normales, Icônes réduites et Détails permettent également de modifier l'ordre d'affichage des objets en effectuant un tri. Ce tri peut s'effectuer selon un grand nombre d'attributs (ou *caractéristiques*).

Deux modes de tri sont disponibles :

- **Vue Détails**

  Pour trier les objets, cliquez sur l'en–tête de colonne correspondant à l'attribut de tri souhaité. L'ordre de tri alterne entre croissant et décroissant à chaque clic sur l'en–tête.

  La vue Détails permet également de modifier l'ordre des colonnes ainsi que leur largeur. Pour changer la position d'une colonne, déplacez son en–tête jusqu'à l'emplacement voulu (l'en–tête de colonne de gauche, qui correspond généralement au nom des objets, est verrouillé). Pour modifier la largeur d'une colonne, déplacez vers la droite ou vers la gauche la ligne verticale qui sépare son en–tête de celui de la colonne suivante ou précédente.

- **Vue Arborescence**

  Les vues Arborescence et Détails sont identiques aux vues Icônes et Détails, à cette différence près que les informations y sont présentées sous forme d'arborescence. Les lignes qui comportent un symbole plus (+) peuvent être développées d'un clic pour afficher les lignes filles supplémentaires. Les lignes qui comportent un symbole moins (–) peuvent être réduites d'un clic pour masquer les lignes filles supplémentaires. Le tri et le filtrage ne sont pas disponibles dans les vues Arborescence.

- **Vue Icônes**

  Vous pouvez trier les objets en sélectionnant le menu **Vue**, puis l'option **Réorganiser les icônes**. La liste des caractéristiques disponibles pour le tri de la vue apparaît alors.

Dans Web–based System Manager, les icônes sont souvent utilisées pour indiquer l'état d'un objet géré. Le tableau suivant décrit les conventions utilisées pour indiquer les principaux états ou conditions :

Condition ou état	Aspect	Exemple	Signification
Objet normal, actif	Icône pleine	  	Compte utilisateur actif Volume logique (connecté) Processus actif
Objet inactif, non configuré ou incomplet	Contour de l'objet uniquement	  	Compte utilisateur expiré Volume logique (déconnecté) Processus inactif
Objet manquant	Contour de l'objet en pointillés		Processus supprimé (zombie)
Traitement – Objet en cours de mise à jour	Indicateur temporel		Mise à jour
Problème au niveau de l'objet	Alarme		Avertissement
Problème grave au niveau de l'objet – Une intervention immédiate est requise	Danger		Problème grave

Généralités

Les modules complémentaires Généralités sont des interfaces de type page Web qui s'affichent dans la zone de contenu et qui :

- décrivent les fonctions fournies par un ou plusieurs modules complémentaires constituant une application ;
- fournissent un accès direct à des tâches de routine ou d'*initiation* ;
- constituent un récapitulatif de l'état des principales ressources gérées par l'application.

Dans la mesure où les généralités n'affichent pas d'objets, elles simplifient l'accès aux tâches courantes. Elles sont également utilisées avec les fonctions de gestion ne concernant qu'une seule tâche et ne nécessitant pas d'icône pour représenter les ressources système (sauvegarde et restauration, par exemple).

Lanceurs

Les lanceurs (ou modules complémentaires Lancement) sont similaires aux modules complémentaires Généralités. Il s'agit de panneaux de type page Web destinés à décrire et à fournir des points d'origine aux applications fonctionnant dans un environnement propre, indépendamment de la console Web-based System Manager.

Menus et barre d'outils

La barre de menus de la console permet d'effectuer toutes les opérations concernant l'exploitation de la console et le traitement des objets gérés. Les menus sont organisés comme suit :

Menu Console

Le menu Console contient des options qui permettent d'exploiter la console. Il permet d'ajouter et de supprimer des ordinateurs dans l'environnement de gestion, de spécifier comment se connecter automatiquement à une machine hôte avec un mot de passe enregistré, de visualiser le journal des sessions de la console, de quitter la console et d'enregistrer les préférences afférentes à celle–ci, dont le thème et la taille de police (reportez–vous à Fichiers de préférences, page 3-13).

Menu *Objet*

Le titre du menu *Objet* change selon le type de ressource gérée par le module complémentaire actif. Par exemple, si le module complémentaire de gestion d'unités matérielles est sélectionné, le titre du menu Objet devient *Unités*. Le menu Objet propose des options générales et des opérations associées à un module complémentaire qui ne requièrent pas la sélection d'objets spécifiques sur lesquels agir. Généralement, les actions visant la création de nouveaux objets de ressource sont situées dans le menu Objet. La fonction de **recherche** se trouve également dans le menu Objet. Le contenu de ce menu est actualisé quand un nouveau module complémentaire est sélectionné.

Menu Sélectionné(s)

Le menu Sélectionné(s) contient les actions de module complémentaire pour lesquelles l'utilisateur doit sélectionner les objets gérés cibles de l'action, par exemple : *Ouverture*, *Caractéristiques*, *Copie*, *Suppression* ou *Démarrage*. Le contenu de ce menu est actualisé lorsqu'un nouveau module complémentaire est sélectionné. Il est désactivé lorsque les modules complémentaires Généralités et Lancement sont chargés.

Menu Vue

Le menu Vue contient les options de navigation, telles que *Précédent*, *Suivant* et *Niveau supérieur*. Dans le menu, figure également le sous–menu *Affichage* qui contient des options de personnalisation de la console. Ainsi, vous pouvez choisir d'afficher ou de masquer la barre d'outils et la barre d'état. Lorsque des modules complémentaires Conteneur sont chargés, le menu Vue propose des options qui gèrent le mode de présentation des objets. Par exemple, si le module complémentaire propose des options de vues, telles que *Icônes normales*, *Icônes réduites*, *Détails* et *Arborescence*, ces options sont affichées. Si le module complémentaire ne gère qu'une seule vue, aucun choix n'est disponible. Lorsqu'un module complémentaire affiche une icône ou la vue *Détails*, le menu Vue comporte des options de tri et de filtrage du conteneur.

Menu Fenêtre

Le menu Fenêtre contient des actions permettant de gérer les sous–fenêtres de l'espace de travail de la console. *Nouvelle fenêtre* permet de créer une sous–fenêtre de console dans l'espace de travail. Les autres options permettent de contrôler la disposition des sous–fenêtres de la console. Par exemple, vous pouvez faire en sorte que les fenêtres recouvrent totalement l'espace de travail en mosaïque, ou qu'elles se superposent (disposition en cascade).

Menu Aide

Le menu Aide répertorie les options d'aide à l'utilisateur. Lorsque l'ordinateur exploité en tant que serveur de gestion de système est correctement configuré avec un serveur HTTP pour faire office de *serveur de documentation*, vous disposez d'une aide en ligne complète accessible depuis un navigateur Web. Plusieurs options sont proposées, qui permettent d'afficher le sommaire de l'aide, d'effectuer une recherche sur une rubrique particulière et d'afficher l'aide relative aux touches de raccourci.

Menus en incrustation

Les menus en incrustation (également appelés *menus contextuels*) permettent d'accéder rapidement à diverses options de menu. Pour utiliser les menus en incrustation au moyen d'une souris, cliquez avec le bouton droit sur un objet. Le menu en incrustation affiche les actions disponibles dans les menus Sélectionné(s) et Objet applicables à l'objet ou aux objets considérés.

Barre d'outils

La barre d'outils répertorie les actions courantes qui sont disponibles lorsque le module complémentaire en cours est chargé. Elle inclut les commandes de navigation, les options de recherche et de visualisation (si disponibles). La barre d'outils affiche également une info–bulle lorsque le pointeur de la souris reste positionné sur une icône de la barre pendant quelques secondes.

Aide

Web-based System Manager propose un grand nombre de procédures d'obtention d'assistance et d'informations complémentaires.

Infobulles

Fournit une assistance sur les icônes de la barre d'outils. Placez le curseur sur une icône de la barre d'outils et attendez quelques secondes. Un petit encart de texte apparaît, présentant la signification de l'icône.

Astuces

Fournit de l'aide sur les tâches courantes effectuées avec le module complémentaire actif. Les astuces sont affichées entre les barres de menus et d'outils. Elles apparaissent sous la forme d'instructions simples ou de liens hypertextes vers l'aide Java. À l'aide du sous–menu Affichage du menu Vue, l'utilisateur peut choisir de masquer ou d'afficher les astuces.

Aide contextuelle

Fournit une assistance sur l'utilisation des boîtes de dialogue. Pour accéder à l'aide contextuelle, cliquez sur le bouton **Aide** dans l'angle inférieur droit de la boîte de dialogue. Une petite fenêtre d'aide contextuelle apparaît. Lorsque vous cliquez sur les différentes commandes de la boîte de dialogue, l'assistance correspondant à l'utilisation de ces commandes apparaît dans la fenêtre d'aide contextuelle. Lorsque l'aide contextuelle est activée, vous ne pouvez accéder aux commandes de la boîte de dialogue que pour visualiser l'aide les concernant. Pour pouvoir utiliser les commandes, vous devez tout d'abord fermer la fenêtre d'aide contextuelle en cliquant sur le bouton **Fermeture** de cette fenêtre ou en cliquant sur le bouton **Aide** de la boîte de dialogue pour laquelle vous avez cherché de l'aide.

Aide Java

Fournit des informations exhaustives concernant les tâches de l'aide Java. Pour pouvoir utiliser le système d'aide Java, vous devez avoir configuré un serveur de documents. Une fois que le serveur d'aide a été identifié auprès de l'hôte géré, vous pouvez accéder à l'aide Java en effectuant une sélection dans le menu Aide de la barre de menus ou en cliquant sur un lien dans la zone Astuces.

Zone Astuces

La zone Astuces propose des réponses rapides à des questions fréquemment posées. Une *astuce* peut être une simple instruction d'une ligne, comme « Pour ajouter un hôte à gérer, sélectionnez Console, puis Ajout ». Il est cependant plus fréquent de trouver des astuces sous forme de liens hypertextes. Si l'aide HTML (par navigateur) est correctement configurée, le fait de cliquer sur une astuce hypertexte ouvre votre navigateur Web par défaut et charge la rubrique correspondant au lien. Vous pouvez choisir d'afficher ou de masquer la barre d'astuces en activant ou désactivant l'option Zone Astuces du sous–menu Affichage du menu *Vue*.

Boîte de dialogue d'exécution

La boîte de dialogue d'exécution s'affiche lorsque des opérations longues sont exécutées sur un ordinateur géré. En fonction de l'application, il peut s'agir d'une simple boîte de dialogue contenant une animation indiquant la progression de l'opération. En mode simple, vous pouvez agrandir la boîte de dialogue d'exécution pour afficher les détails de l'opération en cours d'exécution. Pour afficher les détails, cliquez sur le bouton **Détails** dans la partie inférieure de la boîte. Vous pouvez afficher deux types de détails :

Commandes
: Script shell en cours d'exécution.

Messages
: Informations affichées sur la sortie standard (stdout).

Réciproquement, lorsque les détails sont affichés, vous pouvez réduire la taille de la boîte en cliquant sur le même bouton pour les masquer.

En fonction de l'application, la boîte de dialogue d'exécution peut disparaître automatiquement lorsque l'opération est terminée. Si l'opération échoue, la boîte de dialogue reste ouverte et s'agrandit pour afficher les détails des messages pour vous aider à diagnostiquer l'incident rencontré. Pour les tâches pour lesquelles il est important que vous examiniez les résultats d'une opération qui s'est correctement terminée, la boîte de dialogue reste ouverte.

Barre d’état

La *barre d’état* est située tout en bas de la fenêtre de console. Elle comporte les cinq zones d’affichage d’informations d’état suivantes :

- L’icône représentant un **cadenas** indique, lorsque ce cadenas est fermé, que la console s’exécute en mode **sécurisé**. Dans ce cas, les communications entre la plateforme cliente qui exécute la console et l’ordinateur géré sont chiffrées par le protocole SSL. Lorsque les communications ne s’effectuent pas en mode sécurisé, l’icône représente un **cadenas** ouvert.
- État de chargement du module complémentaire. Lorsqu’un module complémentaire est chargé, le message `Prêt` s’affiche. Lorsque le module complémentaire est en cours de chargement, une barre de progression s’affiche.
- Nombre d’objets visibles dans la zone de contenu. Il est possible que des objets présents sur l’hôte géré soient masqués par le filtre de la vue.
- Nombre d’objets sélectionnés dans la zone de contenu.
- Contexte de sécurité (noms d’utilisateur et d’hôte) de l’administrateur pour le module complémentaire actif.

Vous pouvez afficher ou masquer la barre d’état en sélectionnant ou désélectionnant l’option **Barre d’état** dans le sous–menu Affichage du menu Vue.

Espace de travail de la console

La console Web-based System Manager possède une interface MDI (Multiple Document Interface) permettant d'afficher plusieurs perspectives dans l'environnement de gestion. Cette interface peut être configurée pour afficher plusieurs sous–fenêtres, appelées *documents*, à l'intérieur du cadre de la fenêtre, appelé *espace de travail*. Par défaut, à l'ouverture de la console, une fenêtre de document unique apparaît, avec sa taille maximum. Pour créer plusieurs vues de l'environnement de gestion, réduisez la fenêtre de document en utilisant les commandes de droite de la barre d'outils.

L'icône du milieu permet de réduire la taille de la fenêtre de document. L'icône de gauche réduit la taille de la fenêtre située dans la console extérieure. Vous pouvez créer une seconde fenêtre de document en sélectionnant l'option **Nouvelle fenêtre** du menu Fenêtre.

Il est possible de se déplacer dans différents endroits de la fenêtre de document. Vous pouvez ainsi comparer les paramètres de configuration des différentes ressources sur des hôtes distincts.

Le menu Fenêtre de chaque fenêtre interne propose des options de menu afin de gérer plusieurs fenêtres de l'espace de travail. Le tableau ci–dessous décrit ces options.

Option de menu	Fonction
Nouvelle fenêtre	Crée une nouvelle instance de la fenêtre interne de l'espace de travail.
Cascade	Superpose les fenêtres internes.
Juxtaposition horizontale	Dispose les fenêtres internes de gauche à droit afin d'occuper complètement l'espace de travail.
Juxtaposition verticale	Dispose les fenêtres internes de haut en bas afin d'occuper complètement l'espace de travail.
Réduction autres fenêtres	Réduit la taille de toutes les fenêtres internes à l'exception de la fenêtre active (fenêtre dans laquelle cette option de menu a été sélectionnée).
Restauration globale	Restaure les fenêtres réduites à leur taille et position initiale.
1. /Environnement de gestion/	Liste des fenêtres internes actives. Si vous sélectionnez une fenêtre dans cette liste, elle s'ouvre (si elle était réduite), passe au premier–plan et devient active.

Fichiers de préférences

Un fichier de **préférences** est utilisé pour contrôler les fonctions suivantes de Web–based System Manager :

- Formatage d'une fenêtre fille dans la fenêtre de la console pour que seuls les composants spécifiés par l'utilisateur s'affichent.
- Définition des préférences relatives aux vues, filtres et tris spécifiées par l'utilisateur.
- Définition d'une procédure de gestion de différents domaines de machines.

Lorsque Web-based System Manager est démarré, le fichier de préférences sélectionné affiche la session avec les préférences sauvegardées lors du dernier enregistrement. Ces préférences comprennent, entre autres, le format de la fenêtre de console et les machines gérées. Par défaut, le fichier de préférences est enregistré sous :

```
$HOME/WebSM.pref
```

où $HOME représente le répertoire principal de l'utilisateur sur la machine qui effectue la gestion.

Pour sauvegarder l'état de la console, utilisez l'option de menu **Console –> Sauvegarde**.

Vous pouvez également enregistrer l'état de la console dans d'autres fichiers de préférences. Pour cela, utilisez l'option de menu **Console –> Sauvegarde sous...** pour afficher une boîte de dialogue dans laquelle vous pouvez entrer un autre chemin d'accès.

Pour utiliser un fichier de préférences autre que celui par défaut, reportez–vous à Modes d'exploitation, page 1-4.

Les fenêtres filles d'une fenêtre de console Web-based System Manager possèdent de nombreux composants qui peuvent être affichés ou masqués selon vos préférences. Les préférences de format de ces fenêtres filles sont enregistrées dans un fichier de préférences et utilisées lorsqu'une session est lancée avec le fichier de préférences spécifié. Vous pouvez afficher ou masquer les composants de la fenêtre fille à l'aide de l'option du menu en cascade **Vue –> Affichage**. Le tableau suivant présente les composants que vous pouvez afficher ou masquer et indique s'ils sont enregistrés dans le fichier de préférences :

Composant	L'état est–il enregistré dans le fichier de préférences ?
Zone de navigation	Non
Barre d'outils	Oui
Barre d'astuces	Oui
Barre de description	Oui
Barre d'état	Oui

Lors d'une session Web-based System Manager, vous pouvez ouvrir plusieurs fenêtres filles. Les préférences de format des fenêtres filles enregistrées à la fin d'une session (à condition que l'utilisateur précise que les préférences doivent être sauvegardées lors de la fermeture) sont celles de la fenêtre fille en cours à la fin de la session. Lorsque ce fichier de préférences est utilisé pour lancer une autre session, la fenêtre fille de la fenêtre de console (une seule fenêtre fille est créée lorsqu'une session est lancée) utilise les préférences de format enregistrées.

Pour chaque application chargée, vous pouvez définir les objets à afficher et le type d'affichage à l'aide des options de vue, de tri et de filtrage. Les options sélectionnées pour chaque application sont stockées dans le fichier de préférences. Ces options sont alors utilisées lorsqu'une session est lancée avec le fichier de préférences à leur emplacement d'enregistrement. Vous pouvez définir ces options de plusieurs façons :

- Choisissez une vue d'application en sélectionnant l'option de menu **Vue –> Option de vue**.
- Choisissez un ordre de tri des objets en sélectionnant l'option du menu en cascade **Vue –> Réorganiser les icônes**.
- Choisissez de filtrer les objets affichés en sélectionnant l'option de menu **Vue –> Filtrage des icônes**.

Les ordinateurs hôtes gérés lors d'une session Web-based System Manager sont sauvegardés dans le fichier de préférences. Vous pouvez ainsi gérer plusieurs domaines de machines en lançant des sessions avec différents fichiers de préférences. Vous pouvez donc disposer d'un fichier de préférences correspondant à un groupe constitué de serveurs HTTP et d'un autre fichier de préférences correspondant à un groupe constitué de serveurs de transactions.

Pour enregistrer un groupe de machines dans un fichier de préférences, vous devez les ajouter à l'environnement de gestion de Web-based System Manager lors d'une session. Pour ajouter des machines à l'environnement de gestion pendant une session, sélectionnez l'option de menu **Console –> Ajout –> Hôtes...**. Cette option affiche une boîte de dialogue dans laquelle vous pouvez entrer des ordinateurs hôtes individuels ou une liste de machines hôtes contenue dans un fichier.

Gestion des erreurs de chargement ou de sauvegarde des fichiers de préférences

Les situations suivantes peuvent provoquer des erreurs :

- Vous n'avez pas accès en lecture au fichier ou le fichier contient des données incorrectes. Si l'utilisateur ne spécifie pas de fichier de préférences, le fichier par défaut **$HOME/WebSM.pref** est utilisé. Un message d'avertissement s'affiche et les paramètres par défaut sont utilisés. Il est possible de sélectionner un autre fichier en utilisant l'option de menu **Console –> Sauvegarde sous...** ou l'option **Sauvegarde de l'état de la console pour la session suivante** dans la boîte de dialogue de confirmation de sortie, lorsque vous quittez une session Web-based System Manager.
- Vous indiquez un fichier de personnalisation, mais vous n'avez pas accès en lecture à ce fichier ou ce fichier contient des données incorrectes. Les procédures qui s'appliquent sont les mêmes que précédemment. Vous n'avez pas accès en écriture au fichier enregistré. Un message d'avertissement s'affiche et vous pouvez sélectionner un autre fichier à l'aide de l'option de menu **Console –> Sauvegarde sous...** ou quitter sans enregistrer le fichier de préférences.
- Si le processus de chargement des préférences échoue, les paramètres par défaut sont utilisés. Dans le cas de la sortie d'une session Web-based System Manager, l'option **Sauvegarde de l'état...** sera désélectionnée pour éviter que les données soient écrasées par erreur. Vous pouvez sélectionner **Sauvegarde de l'état...** pour remplacer le fichier sélectionné.

Outils de la ligne de commande

Le tableau suivant présente les instructions de ligne de commande couramment utilisées pour gérer Web–based System Manager :

Commande	Utilisation
/usr/websm/bin/configassist	Permet de démarrer l'assistant de configuration qui apparaît automatiquement après l'installation du système d'exploitation pour vous aider à effectuer vos tâches de configuration. Cet assistant peut également être démarré à tout moment pour procéder à une configuration supplémentaire. Utilisez l'assistant de configuration pour configurer un système sur lequel un serveur HTTP est installé pour exécuter Web-based System Manager dans un navigateur. Pour plus d'informations, reportez–vous à la section Mode applet, page 1-7. **Arguments :** Aucun.

/usr/websm/bin/wsm	Démarrage d'une session client Web-based System Manager. **Arguments :** • **–host *hôte gérant*** Contraint Web-based System Manager à se connecter d'abord à l'hôte spécifié. Bien que vous puissiez facilement gérer d'autres hôtes lorsque vous exécutez Web–based System Manager, cette option vous permet de démarrer Web-based System Manager avec les préférences que vous avez définies sur la machine hôte indiquée. • **–lang *Langue*** Indique la langue utilisée pour les messages. Si l'ensemble de fichiers **sysmgt.msg.*Langue*.websm.apps** n'est pas installé, les messages s'affichent en anglais. • **–port *numéro de port*** Force Web-based System Manager à se connecter à tout autre hôte à l'aide du port spécifié. Ce numéro de port doit correspondre à celui des machines gérées pour le service **wsmserver** spécifié dans le fichier **/etc/services**. • **–profile *chemin du fichier de préférences*** Spécifie un fichier de préférences *différent*. Le fichier de préférences par défaut, appelé **WebSM.pref**, se trouve dans le répertoire personnel de l'utilisateur. Cette option vous permet d'utiliser un autre fichier de préférences. Elle peut s'avérer utile si l'utilisateur gère différents ensembles de machines pour différent clients. **Remarque :** Le fichier de préférences est lu soit sur la machine locale (personnelle), soit sur la machine spécifiée dans l'argument **–host**.

	• **–user *nom d'utilisateur*** Contraint Web-based System Manager à s'exécuter sous le nom d'utilisateur indiqué. L'utilisateur est invité à entrer son mot de passe. • **DdefaultTurners= *valeur*** Lorsque la ***valeur*** est true, les tourneurs de Java Look and Feel sont utilisés à la place des tourneurs de Windows pour des nœuds d'arborescence parents dans la zone de navigation et dans la zone de contenu. Aucune ligne brisée n'est tracée entre les objets de l'arborescence. • **–DdrawTreeLine= *valeur*** Lorsque la *valeur* est **true** et que **–DdefaultTurners=true**, des lignes brisées sont tracées entre des objets d'arborescence dans la zone de navigation et dans la zone de contenu. • **–Ddatadir= *chemin*** Indique un autre répertoire à examiner pour rechercher les fichiers de configuration se trouvant normalement dans **/var/websm/config/user_settings**. • **–DfontSize= *valeur*** Indique le corps des caractères en points (de 12 à 18). La taille par défaut est 12. • **–DthemeType= *valeur*** Indique un thème. Vous avez le choix entre Classic, option par défaut correspondant à la valeur 0, et Titanium, option associée à la valeur 1. Le thème Classic se caractérise par un fond blanc dans les zones de navigation et de contenu (panneau de droite), des barres de défilement violettes et une mise en évidence en violet des objets sélectionnés. Le thème Titanium se caractérise par un fond gris foncé dans les zones de navigation et de contenu (panneau de droite), des barres de défilement gris clair et une mise en évidence en jaune des objets sélectionnés.

/usr/websm/bin/wsmaccess	Conteneur de la commande **wsm** pour activer les fonctions d'accessibilité. **Arguments :** Identiques à **/usr/websm/bin/wsm**.
/usr/websm/bin/wsmserver	Active ou désactive une machine utilisée comme serveur Web-based System Manager, à savoir une machine pouvant être gérée via un client Web-based System Manager. **Arguments :** • **–enable** Met à jour les services TCP/IP de telle sorte que le démon **inetd** traite les requêtes client Web–based System Manager sur le port 9090. Par défaut, Web-based System Manager est configuré à l'installation pour refuser les requêtes client. • **–disable** Supprime le port 9090 des ports traités par le démon **inetd**. Ainsi, la machine ne répond plus aux nouvelles requêtes client Web-based System Manager. Elle ne met pas fin aux processus serveur Web-based System Manager existants. • **–listenport** *numéro de port* Permet de changer le port auquel Web-based System Manager se connecte. • **–portstart** *début de plage* Définit le plus petit numéro de port de la plage de ports socket de serveur dans laquelle le système effectue dynamiquement un choix. • **–portend** *fin de plage* Définit le plus grand numéro de port de la plage de ports socket de serveur dans laquelle le système effectue dynamiquement un choix. • **–ssloptional** Permet à l'utilisateur de gérer le serveur via une connexion SSL ou une connexion standard. • **–sslalways** Ne permet au client de gérer le serveur que si une connexion SSL peut être établie entre le client et le serveur.

Fichiers modifiables par l'utilisateur

Il est possible que l'utilisateur ou l'administrateur doive modifier certains fichiers de Web-based System Manager. En règle générale, l'état d'une session est sauvegardé pour chaque utilisateur dans le fichier de préférences (reportez–vous à Fichiers de préférences, page 3-13). Les seuls fichiers susceptibles d'être modifiés pour affecter le fonctionnement général de Web–based System Manager sont les suivants :

- **/var/websm/config/user_settings/websm.cfg**

  Ce fichier contient des paramètres qui contrôlent le fonctionnement général de l'appli–cation Web–based System Manager. Son contenu est décrit dans le tableau suivant :

Nom de variable	Description	Valeurs possibles
forcessl	Si cette variable est définie sur **true**, elle indique que la machine sur laquelle le fichier **websm.cfg** est stocké ne peut être gérée que si le client concerné peut établir une connexion SSL avec la machine gérante. Reportez–vous à Sécurité Web-based System Manager, page 5-1. **Remarque :** Sur les systèmes antérieurs à AIX 5.1, Web-based System Manager interprétait l'indicateur *forcessl* différemment. En effet, lorsque *forcessl* avait pour valeur « true » *et* que la fonction SSL était configurée sur le serveur, l'application considérait qu'une communication SSL était nécessaire. Sous AIX 5.1, le serveur ne peut pas être géré par un client éloigné si *forcessl* a pour valeur « true » et si la fonction SSL n'est pas configurée.	**true** ou **false**
remote_timeout	Temps (en millisecondes) pendant lequel un client attend une connexion à une machine gérée. Si la connexion ne peut pas être établie dans ce laps de temps, le client abandonne l'opération. Si le client n'abandonne pas l'opération, il peut attendre indéfiniment si une tentative de gestion d'une machine inexistante a été effectuée.	**Valeurs entières** La valeur appropriée peut dépendre des performances du réseau. La valeur par défaut est définie à 30 000 (30 secondes). Si les performances du réseau sont réduites (il est fréquent que des tentatives d'accès à des machines éloignées existantes et disponibles n'aboutissent pas), cette valeur doit être augmentée.

  La seule option que Web-based System Manager utilise actuellement est *forcessl*. Cet indicateur est utilisé lorsqu'un client se connecte à une machine gérée. Si la valeur de *forcessl* est **true**, le serveur pourra se connecter au client uniquement par l'intermédiaire de connexions sécurisées (sockets SSL). Sinon, le serveur tentera de se connecter via des connexions sécurisées si la fonction SSL est configurée sur le client et sur le serveur. En cas d'incident lors d'une connexion via des sockets SSL, le serveur autorisera le client à se connecter au moyen de sockets non sécurisés (reportez–vous à Sécurité Web-based System Manager, page 5-1).

Utilisation de Web-based System Manager à partir du clavier

Web-based System Manager peut s'utiliser avec ou sans dispositif de pointage (tel qu'une souris, par exemple). Si vous choisissez de ne pas utiliser de dispositif de pointage, vous pouvez vous déplacer entre les commandes et les menus à l'aide du clavier.

Mnémoniques et raccourcis

Vous pouvez accéder aux différentes fonctions des menus à l'aide des méthodes d'utilisation du clavier suivantes :

- **Mnémoniques :** il s'agit de lettres soulignées dans les options des menus et des boîtes de dialogue. Pour accéder à une option de menu ou une commande visible, appuyez sur la touche Alt, puis sur le mnémonique. Lorsque vous utilisez des mnémoniques, il n'est pas nécessaire d'utiliser la barre d'espace ou la touche Entrée pour sélectionner un élément.
- **Raccourcis :** également appelés *accélérateurs*, ce sont des combinaisons de touches du clavier qui activent directement les options fréquemment utilisées. Ils permettent également d'accéder aux fonctions par une combinaison de touches composée de la touche Ctrl et d'un caractère. Contrairement aux mnémoniques, les raccourcis de menu ne requièrent pas que les options de menus soient visibles pour que vous puissiez y accéder directement.

Déplacement dans la console à l'aide du clavier

Les touches suivantes permettent de vous déplacer dans la console de Web-based System Manager :

Touches	Actions
Flèches	Permettent de se déplacer entre : • les objets de la zone de navigation. Les flèches vers la gauche et vers la droite permettent d'agrandir et de réduire les nœuds ; les flèches vers le haut et vers le bas permettent de se déplacer verticalement entre les éléments. • les objets de la zone de contenu. • les icônes de la barre d'outils. • les différents éléments des menus.
Ctrl + flèche	Place le curseur sur un autre objet de la zone de contenu (panneau de droite) sans le sélectionner. Si vous combinez l'utilisation de la touche Ctrl, des flèches et de la barre d'espace, vous pouvez sélectionner plusieurs objets non contigus.
Échap	Ferme un menu ouvert sans activer de sélection.
F1	Ouvre la table des matières de l'aide orientée navigateur.
F8	Déplace la barre de fractionnement entre la zone de navigation et la zone de contenu de la console à l'aide des touches ORIGINE, FIN et les flèches.
F10	Active et désactive (touche à bascule) la barre de menus.
Touche Maj + flèche	Agrandit une sélection contiguë.
Barre d'espace, Entrée	Sélectionne l'objet actif.
Tabulation, Maj + Tabulation	Déplace le curseur entre les différentes zones de la console.

Déplacement dans les boîtes de dialogue à l'aide du clavier

Les touches suivantes permettent de naviguer dans les boîtes de dialogue de Web-based System Manager :

Touches	Actions
Alt+F6	Active ou désactive une boîte de dialogue.
Flèches	• Ouvrent les listes déroulantes. • Permettent de se déplacer entre les différentes options des listes. • Permettent de se déplacer entre les onglets dans les boîtes de dialogue à onglets lorsqu'un onglet est actif.
Ctrl + Tabulation, Ctrl + Maj + Tabulation	Permet de passer d'une commande à une autre.
Entrée	Appuie sur le bouton de commande activé.
Échap	Annule l'ouverture de la boîte de dialogue.
F1	Ouvre la fenêtre d'aide contextuelle.
Barre d'espace	• Sélectionne l'option activée. • Active le bouton de commande sur lequel le curseur est positionné.

Accès à l'aide depuis le clavier

Les touches suivantes permettent de vous déplacer dans l'aide de Web-based System Manager :

Remarque : Le système d'aide doit être spécialement configuré pour que ces fonctions de clavier puissent s'exécuter.

Touches	Actions
F1	• Ouvre l'aide orientée navigateur dans la zone de contenu. • Dans les boîtes de dialogue, ouvre la fenêtre d'aide contextuelle.
F9	Affiche l'aide sur les touches.
Alt + F6	En mode aide contextuelle, permet de passer de la fenêtre d'aide contextuelle à la boîte de dialogue parent.

Journal de session

Le journal de session est une fonction de la console qui permet d'effectuer le suivi des modifications effectuées sur les hôtes gérés au cours d'une session Web-based System Manager. Dès qu'un administrateur utilise Web-based System Manager pour apporter une modification à un hôte, une entrée est créée dans le journal. Des entrées peuvent également être générées par des applications pour la consignation des résultats intermédiaires, d'avertissements ou de conditions d'erreur.

Chaque entrée indique la date, l'heure et l'auteur de la modification, l'hôte sur lequel elle a été effectuée et un bref message. Pour consulter la totalité du texte d'un message, cliquez deux fois sur le message. Cliquez sur les colonnes affichées dans la fenêtre du journal pour modifier l'ordre de tri des entrées. Vous pouvez, par exemple, trier les entrées par date et par heure (ordre par défaut), par nom d'hôte, par nom d'utilisateur et par message.

La fenêtre du journal inclut une fonction de *recherche* qui permet de rechercher les entrées comportant une chaîne de texte donnée. L'administrateur peut également gérer le journal en effaçant son contenu à l'aide du bouton **Effacement** ou en sauvegardant son contenu à l'aide des boutons **Sauvegarde** ou **Sauvegarde sous**.

Pour afficher le journal de session, sélectionnez **Console –> Journal de session**.

Chapitre 4. Configuration de l'environnement de gestion

L'environnement de gestion est un ensemble de machines que vous pouvez gérer ou utiliser pour effectuer des tâches d'administration de systèmes à partir de l'application Web-based System Manager. Vous pouvez ajouter des membres à cet ensemble ou en supprimer. La zone de navigation et la zone de contenu de la fenêtre de l'application Web-based System Manager comprennent une interface pour accéder à ces machines. L'application Web-based System Manager vous permet d'ajouter ou de supprimer une machine de deux manières. La première repose sur l'utilisation du menu Console. La seconde fait appel au module complémentaire Environnement de gestion Web-based System Manager. Ces deux approches guident l'utilisateur dans les procédures d'ajout ou de suppression d'une machine de l'environnement de gestion.

De plus, Web-based System Manager offre à l'utilisateur des moyens de sauvegarder un ensemble de machines sur une session particulière. Lorsque Web-based System Manager est initialement lancé, la seule machine présente dans la zone de navigation et dans la zone de contenu est la machine gérante. Après l'ajout d'une machine, celle–ci peut être conservée en vue d'une utilisation ultérieure si vous choisissez d'enregistrer les préférences à l'aide du menu Console ou lorsque vous quittez Web-based System Manager.

Ajout d'une machine à Web-based System Manager

Web-based System Manager identifie les machines de l'environnement de gestion à l'aide du nom exact qui leur a été attribué par l'utilisateur lors de leur ajout à l'environnement. Ceci signifie qu'une machine ajoutée à la fois avec son nom de système hôte complet et son abréviation sera répertoriée deux fois dans l'environnement de gestion, comme s'il s'agissait de deux ordinateurs distincts.

Par exemple, si votre nom de domaine est *macomp.com*, vous pourrez créer une machine dans l'environnement de gestion appelée *nom_machine* ainsi que *nom_machine.macomp.com*. Pour Web–based System Manager, il s'agit de deux machines distinctes. Un message d'avertissement vous informe qu'une autre machine porte le même nom d'hôte et que vous êtes sur le point d'ajouter à la fois *nom_machine* et *nom_machine.macomp.com*. Si vous ne voulez pas avoir les deux noms de machines dans l'environnement de gestion, vous pouvez prendre des mesures préventives.

Vous pouvez utiliser l'une des méthodes suivantes pour ajouter une machine à Web–based System Manager :

Menu Console :

1. Sélectionnez **Console** dans le menu d'applications Web-based System Manager.
2. Sélectionnez **Ajout**.
3. Sélectionnez **Hôtes**.

Module complémentaire Environnement de gestion de **Web–based System Manager** :

1. Sélectionnez **Environnement de gestion** dans la zone de navigation.
2. Sélectionnez **Environnement de gestion** dans le menu d'applications Web-based System Manager.
3. Sélectionnez **Nouveau**.
4. Sélectionnez **Hôtes**.

Une fois la boîte de dialogue d'ajout ouverte, vous pouvez ajouter la machine de l'une des manières suivantes :

- en ajoutant un ordinateur individuel, avec la possibilité de vérifier son existence sur le réseau ;
- en ajoutant une liste d'ordinateurs à partir d'un fichier.

Exemples

Pour ajouter une seule machine appelée chocolat.bull.com :

1. Sélectionnez **Ajout de cet hôte :**
2. Dans la zone de saisie, tapez `chocolat.bull.com .`
3. Cliquez sur **Ajout**.

Le nom d'ordinateur attribué s'affiche dans la zone de navigation et dans le panneau de navigation. Sous la barre de progression, un message indique : `Ajout réussi... chocolat.bull.com`.

Pour ajouter une seule machine et vérifier sa présence sur le **réseau** :

1. Sélectionnez **Ajout de cet hôte :**
2. Dans la zone de saisie, tapez `coco.bull.com`.
3. Sélectionnez **Vérification de la présence de l'hôte sur le réseau**.
4. Cliquez sur **Ajout**.

Le nom d'ordinateur attribué s'affiche dans la zone de navigation et dans le panneau de navigation. Si l'ordinateur hôte n'existe pas sur le réseau, un message d'erreur Web-based System Manager s'affiche, indiquant que l'hôte ne peut être contacté.

Pour ajouter une liste d'ordinateurs à partir d'un fichier :

1. Sélectionnez **Ajout des hôtes du fichier :**
2. Tapez le chemin d'accès complet du fichier dans la zone de saisie, ou cliquez sur **Parcourir** et sélectionnez le **fichier**.
3. Cliquez sur **oui** dans la boîte de dialogue de confirmation pour ajouter la liste de machines.

Un message s'affiche sous la barre de progression indiquant la machine dont l'ajout est en cours. A la fin de l'opération, le message `Opération exécutée avec succès` s'affiche. Les noms des machines ajoutées s'affichent dans la zone de navigation et dans le panneau de navigation.

Suppression d’une machine

L’application Web-based System Manager a deux approches pour retirer ou supprimer des machines de la zone de navigation :

Menu Console :

1. Sélectionnez **Console** dans le menu d’applications Web-based System Manager.
2. Sélectionnez **Retrait**.
3. Sélectionnez **Hôtes**.
4. Sélectionnez les machines à supprimer.
5. Cliquez sur **Retrait**.
6. Sélectionnez **oui** dans la boîte de dialogue de confirmation pour retirer les machines sélectionnées.

Module complémentaire Environnement de gestion :

1. Sélectionnez **Environnement de gestion** dans la zone de navigation.
2. Sélectionnez les machines à supprimer de la zone de navigation.
3. Sélectionnez **Sélectionné(s)** dans le menu d’applications Web–based System Manager.
4. Sélectionnez **oui** dans la boîte de dialogue de confirmation pour retirer les machines sélectionnées.

Chapitre 5. Sécurité Web-based System Manager

La sécurité Web-based System Manager sécurise le fonctionnement de Web-based System Manager en mode client–serveur. Lorsque Web-based System Manager fonctionne en mode sécurisé, les machines gérées sont des serveurs et les utilisateurs qui effectuent la gestion sont les clients. Les communications entre les serveurs et les clients s'effectuent via le protocole SSL, qui gère l'authentification des serveurs ainsi que le chiffrement et l'intégrité des données. Vous gérez la machine dans Web-based System Manager en utilisant un compte sur cette machine et vous vous authentifiez auprès du serveur Web-based System Manager en envoyant l'ID utilisateur et le mot de passe via le protocole sécurisé SSL.

Chaque serveur Web-based System Manager possède sa clé privée et un certificat de sa clé publique signé par une autorité de certification (CA) à laquelle les clients Web-based System Manager font confiance. La clé privée et le certificat du serveur sont stockés dans son fichier de clés privées. Le client Web-based System Manager possède un fichier de clés publiques contenant les certificats des autorités de certification habilitées.

En mode applet (fonctionnement à partir du navigateur), le client doit être assuré que l'applet (fichiers **.class**) reçu par le navigateur provient du bon serveur. En outre, dans ce mode, le fichier de clés publiques est situé sur le serveur et transféré au client avec le reste des fichiers **.class** de l'applet, parce que le navigateur n'autorise pas les applets à lire les fichiers locaux. Pour garantir l'authentification de l'émetteur et l'intégrité de ces fichiers, le client doit utiliser les fonctions SSL de son navigateur et contacter uniquement le serveur au moyen du protocole **HTTPS** (HTTPS://...). Il est possible d'utiliser les fonctionnalités SSL du serveur HTTP sur chaque machine gérée ou d'utiliser le démon **SMGate** installé avec la sécurité Web-based System Manager. **SMGate** sert de passerelle SSL entre le navigateur client et le serveur Web.

Cette section aborde les procédures et processus de sécurité suivants :

Installation de la sécurité Web-based System Manager

L'ensemble de fichiers de la sécurité Web-based System Manager, **sysmgt.websm.security**, lorsqu'il existe, se trouve dans l'Expansion Pack AIX 5.2.

Un ensemble de fichiers supplémentaire, **sysmgt.websm.security–us**, qui possède des capacités de chiffrement plus élevées, est disponible dans l'Expansion Pack AIX 5.2 fourni dans certains pays. Cet ensemble de fichiers exige que vous disposiez du fichier **sysmgt.websm.security**.

Sur les clients Windows ou Linux, la sécurité du client distant Web-based System Manager doit aussi être installée. Pour en savoir plus, reportez–vous à Installation de la sécurité du client distant Web-based System Manager, page 2-9.

Configuration de la sécurité Web-based System Manager

La sécurité Web-based System Manager offre une interface graphique et une interface de type ligne de commande pour configurer l'administration sécurisée.

Pour accéder à l'interface graphique, sélectionnez **Environnement de gestion —> *nom d'hôte* —> Sécurité Web–based System Manager —> Généralités et états**. Ces tâches sont uniquement accessibles en mode local. Dans les différents scénarios exposés ci–après, elles sont désignées par Présentation de l'autorité de certification et Présentation de la sécurité du serveur. L'interface graphique est utilisée dans ces scénarios. La commande correspondante est indiquée à chaque étape.

Scénarios de sécurité

Les différentes possibilités de configuration, ou scénarios, sont décrites dans les sections suivantes :

Fichiers de clés « prêts »

Les fichiers de clés prêts à l'emploi constituent la méthode la plus rapide pour accéder à l'état opérationnel sécurisé. Dans ce scénario, utilisez le même poste de travail pour définir une autorité de certification (CA) interne et générer des fichiers de clés prêts à l'emploi pour tous vos serveurs et clients Web-based System Manager. Cette opération génère un fichier de clés publiques que vous devez copier sur tous les serveurs et clients et un fichier unique de clés privées pour chaque serveur.

Les étapes suivantes décrivent l'utilisation des fichiers de clés prêts à l'emploi :

1. **Définir une autorité** de **certification interne** Web-based System Manager.

   Utilisez un système sécurisé pour l'autorité de certification, car sa clé privée constitue l'information la plus sensible de la configuration des paramètres de sécurité Web-based System Manager.

   Remarque : N'utilisez pas un poste de travail sans disque ou sans données comme autorité de certification, car la clé privée serait transmise sur le réseau.

   Après avoir déterminé l'autorité de certification, connectez–vous localement en tant qu'utilisateur root et démarrez Web–based System Manager. Vous ne pouvez pas accéder aux applications de configuration des paramètres de sécurité de Web-based System Manager si vous ne vous êtes pas connecté en tant qu'utilisateur root ou si vous exécutez Web-based System Manager dans une application éloignée ou en mode applet.

   Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Autorité de certification**.

   Dans la liste des tâches de l'**Autorité de certification**, sélectionnez **Configuration de ce système comme autorité de certification** Web-based System Manager. Lorsque l'assistant s'affiche, indiquez les informations suivantes :

   – **Nom distinctif de l'autorité de certification**
     Indiquez un nom descriptif permettant d'identifier l'autorité de certification et son instance. Par exemple : le nom d'hôte de la machine et un numéro de séquence. Les noms peuvent contenir des blancs. Si vous redéfinissez l'autorité de certification, utilisez un autre numéro de séquence afin de pouvoir déterminer l'instance de l'autorité responsable de la signature du certificat. Le nom ne doit pas être exactement le même que le nom TCP/IP complet, car cela ne fonctionnera pas avec le démon **SMGate**.

   – **Nom de société**
     Indiquez un nom descriptif qui identifie votre société ou votre organisation.

   – **Code pays ou région ISO**
     Indiquez votre code région ou code pays ISO (2 caractères) ou sélectionnez–le dans la liste.

   – **Date d'expiration**
     À l'expiration du certificat, reconfigurez les paramètres de sécurité Web-based System Manager en redéfinissant l'autorité de certification et en générant de nouveaux fichiers de clés privées pour tous vos serveurs. Vous pouvez modifier cette date ou conserver la valeur par défaut.

   – **Répertoire du fichier de clés publiques**
     Le fichier de clés publiques contenant les certificats de l'autorité de certification est enregistré dans ce répertoire. Copiez ce fichier dans le répertoire Web-based System Manager **codebase** sur tous les serveurs et clients Web-based System Manager.

– **Mot de passe**
Ce mot de passe permet de chiffrer le fichier de clés privées de l'autorité de certification. Vous devez l'entrer chaque fois que vous effectuez une tâche sur cette autorité de certification.

Vous pouvez également définir une CA interne à partir de la ligne de commande avec la commande **/usr/websm/bin/smdefca**.

2. **Créer des fichiers de clés privées pour les serveurs** Web-based System Manager**.**

   Indiquez les noms TCP/IP complets de tous vos serveurs Web-based System Manager.

   Dans la liste des tâches de l'**Autorité de certification**, sélectionnez **Création des fichiers de clés privées des serveurs**. Dans la boîte de dialogue de mot de passe de l'autorité de certification, entrez le mot de passe spécifié lors de la création de l'autorité de certification. Entrez les informations suivantes :

   – **Liste de serveurs**
   Ajoutez à la liste le nom de vos serveurs Web-based System Manager. Vous pouvez les saisir dans la boîte de dialogue (un à la fois) ou indiquer le nom d'un fichier contenant la liste de vos serveurs (un par ligne). Pour obtenir le nom des serveurs à partir du fichier, saisissez le nom du fichier dans la zone **Fichier contenant une liste des serveurs** et cliquez sur **Affichage du fichier**. La boîte de dialogue **Parcourir le fichier contenant une liste des serveurs** vous permet de sélectionner certains (ou tous les) serveurs de la liste.

   – **Nom de société**
   Indiquez un nom descriptif qui identifie votre société ou votre organisation.

   – **Code pays ou région ISO**
   Indiquez votre code région ou code pays ISO (2 caractères) ou sélectionnez–le dans la liste.

   – **Emplacement des fichiers de clés privées**
   Saisissez le répertoire dans lequel vous désirez que les fichiers de clés privées du serveur soient contenus. Vous devez ensuite les transférer sur les serveurs et les installer.

   – **Longueur des clés serveur (en bits)**
   Sélectionnez une **longueur** de clé.

   Remarque : Cette zone s'affiche uniquement si l'ensemble de fichiers **sysmgt.websm.security–us** est installé.

   – **Date d'expiration**
   À l'expiration du certificat, vous devez générer des nouveaux fichiers de clés privées pour vos serveurs. Vous pouvez modifier cette date ou conserver la valeur par défaut.

   – **Chiffrement des fichiers de clés privées serveur**
   Cette boîte de dialogue crée un fichier de clés privées pour chaque serveur spécifié. Chacun de ces fichiers contient la clé privée d'un serveur. Par conséquent, il doit toujours être protégé. Pour cela, vous pouvez chiffrer ces fichiers. Si vous sélectionnez cette option, vous êtes invité à entrer un mot de passe. Ce mot de passe est nécessaire lorsque vous installez les clés privées sur les serveurs.

   Lorsque vous cliquez sur **OK**, un fichier de clés privées est créé pour chaque serveur que vous avez spécifié.

   Vous pouvez également générer des fichiers de clés publiques à partir de la ligne de commande avec la commande **/usr/websm/bin/smgenprivkr**.

3. **Copier le fichier de clés publiques (SM.pubkr) sur tous les serveurs et clients**.

   Une copie du fichier de clés publiques de l'autorité de certification contenu dans le répertoire indiqué à l'étape 1 doit être placée sur vos serveurs et clients Web-based System Manager, dans le répertoire que vous avez choisi lors de l'installation et qui doit être conforme aux indications suivantes :

– sur un client AIX, utilisez le répertoire **/usr/websm/codebase** ;

– sur un client Windows, utilisez le répertoire **Program Files\websm\codebase** ;

– sur un client Linux, utilisez le répertoire **/opt/websm/codebase**.

Remarque : Ce fichier doit être copié au format binaire.

Remarque : Le contenu de ce fichier n'est pas confidentiel. Cependant, si vous le placez sur une machine client, il devient possible de connaître l'autorité de certification à laquelle le client se fie. L'accès à ce fichier sur le client doit donc être limité. En mode applet, le client peut faire confiance au serveur pour transmettre ce fichier en même temps que l'applet, à condition d'utiliser le protocole **HTTPS**.

4. **Copier les fichiers de clés privées sur tous les serveurs**

   Chaque fichier de clés privées doit être installé sur le serveur.

   Vous pouvez transférer les fichiers vers les cibles appropriées en toute sécurité. Vous pouvez utiliser un répertoire partagé et une disquette TAR, de la manière suivante :

   – **Répertoire partagé :** Placez tous les fichiers de clés sur un répertoire partagé (NFS ou DFS, par exemple) accessible à chaque serveur.

   Remarque : Pour utiliser cette méthode, vous devez avoir choisi de chiffrer les fichiers de clés privées du serveur dans la boîte de dialogue **Création des fichiers de clés privées des serveurs**, car les fichiers transférés ne sont pas chiffrés. Nous vous recommandons également de n'accorder qu'à l'administrateur les droits d'accès au répertoire partagé.

   – **Disquette TAR :** Générez une disquette TAR contenant tous les fichiers de clés privées du serveur. L'archive TAR ne doit faire mention que des noms de fichiers, sans les chemins d'accès. Pour cela, placez les répertoires dans le répertoire contenant les fichiers de clés privées du serveur et exécutez la commande **tar –cvf /dev/fd0 *.privkr**.

   Installez les fichiers de clés privées sur chaque serveur.

   a. Connectez–vous sur chaque serveur en tant qu'utilisateur root, lancez Web-based System Manager et sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Sécurité serveur**.

   b. Dans la liste des tâches, sélectionnez **Installation du fichier de clés privées du serveur**.

   c. Sélectionnez l'emplacement des fichiers de clés privées du serveur. Si vous utilisez une disquette, sélectionnez `Disquette tar`.

   d. Insérez la disquette.

   e. Cliquez sur **OK**.

   Si les fichiers de clés privées ont été chiffrés, vous devez indiquer le mot de passe. La clé privée du serveur est installée dans le fichier **/var/websm/security/SM.privkr**.

   Répétez cette procédure pour chaque serveur.

   Vous pouvez également distribuer des fichiers de clés privées à tous les serveurs à partir de la ligne de commande avec la commande **/usr/websm/bin/sminstkey**.

Gestion de sites multiples

Utilisez ce scénario si vous possédez plusieurs sites et si vous ne souhaitez pas répartir les fichiers de clés privées entre ces sites. Supposons que vous possédez un site A et un site B et que vous définissez une autorité de certification interne Web-based System Manager sur une machine du site A. Reportez–vous à l'étape 1 de la section Fichiers de clés « prêts », page 5-4 pour savoir comment configurer une autorité de certification.

Remarque : Pour tous les clients et pour les serveurs du site A, vous pouvez suivre les instructions dans Fichiers de clés « Prêts », page 5-4.

Pour les serveurs du site B, procédez comme suit :

1. **Créer des clés privées et des demandes de certificats pour vos serveurs** Web-based System Manager**.**

   Indiquez les noms complets TCP/IP de tous les serveurs Web-based System Manager du site B. Vous pouvez les saisir consécutivement dans la boîte de dialogue ou indiquer un fichier contenant la liste de vos serveurs (un par ligne).

   Connectez–vous sur un serveur du site B en tant qu'utilisateur root et lancez Web–based System Manager. Vous ne pouvez pas accéder aux applications de configuration des paramètres de sécurité de Web-based System Manager si vous ne vous êtes pas connecté en tant qu'utilisateur root ou si vous exécutez Web-based System Manager dans une application éloignée ou en mode applet.

   Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Sécurité serveur**.

   Dans la liste des tâches de la **Sécurité serveur**, sélectionnez **Création de clés privées et de demandes de certificats pour les serveurs**. Entrez les informations suivantes :

   – **Liste de serveurs**
   Ajoutez à cette liste les noms des serveurs Web-based System Manager du site B. Vous pouvez les entrer un par un dans la boîte de dialogue ou taper le nom d'un fichier contenant la liste de vos serveurs (un par ligne). Pour obtenir le nom des serveurs à partir du fichier, saisissez le nom du fichier dans la zone **Fichier contenant une liste des serveurs** et cliquez sur **Affichage du fichier**. La boîte de dialogue **Parcourir le fichier contenant une liste des serveurs** vous permet de sélectionner certains (ou tous les) serveurs de la liste.

   – **Nom de société**
   Indiquez un nom descriptif qui identifie votre société ou votre organisation.

   – **Code pays ou région ISO**
   Indiquez votre code région ou code pays ISO (2 caractères) ou sélectionnez–le dans la liste.

   – **Emplacement des fichiers de clés privées**
   Entrez le nom du répertoire d'écriture des fichiers de clés privées du serveur et des demandes de certificats. Dans l'étape 2, transférez les fichiers de demandes de certificats à l'autorité de certification du site A pour signature. Dans l'étape 3, transférez les certificats signés de l'autorité de certification du site A vers ce répertoire.

   – **Longueur des clés serveur (en bits)**
   Sélectionnez une **longueur de clé** (cette zone s'affiche uniquement si l'ensemble de fichiers **sysmgt.websm.security–us** est installé sur votre système).

– **Chiffrement des fichiers de clés privées serveur**
Cette boîte de dialogue crée un fichier de clés privées pour chaque serveur spécifié. Chacun de ces fichiers contient la clé privée d'un serveur. Par conséquent, il doit toujours être protégé. Pour cela, vous pouvez chiffrer ces fichiers. Si vous sélectionnez cette option, vous êtes invité à entrer un mot de passe. Ce mot de passe est nécessaire lorsque vous importez les certificats signés et que vous installez les clés privées sur les serveurs.

Lorsque vous cliquez sur **OK**, un fichier de clés privées et une demande de certificat sont créés pour chaque serveur spécifié.

Vous pouvez également générer des clés privées et des demandes de certificats à partir de la ligne de commande avec la commande **/usr/websm/bin/smgenkeycr**.

2. **Obtenir la signature de la CA dans le site A**.

   Transférez les fichiers de demandes de certificats à l'autorité de certification pour le site A. Ces demandes ne contiennent pas des données confidentielles. Cependant, leur intégrité et authenticité doivent être garanties pendant le transfert.

   Transférez une copie des fichiers de demandes de certificats du serveur du site B vers un répertoire de la machine de l'autorité de certification du site A.

   Connectez–vous localement à la machine de l'autorité de certification du site A en tant qu'utilisateur root, puis lancez Web–based System Manager. Vous ne pouvez pas accéder aux applications de configuration des paramètres de sécurité de Web-based System Manager si vous ne vous êtes pas connecté en tant qu'utilisateur root ou si vous exécutez Web-based System Manager dans une application éloignée ou en mode applet.

   Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Autorité de certification**.

   Dans la liste des tâches de l'**Autorité de certification**, sélectionnez **Signature des demandes de certificats**. Entrez les informations suivantes :

   – **Répertoire des demandes de certificats**
   Indiquez le nom du répertoire contenant les demandes de certificats. Puis, cliquez sur **Mise à jour de la liste**. La liste de demandes de certificats s'affiche.

   – **Sélectionnez les demandes de certificats à signer**
   Pour sélectionner des demandes de certificats individuellement, cliquez sur leur nom dans la liste. Pour sélectionner toutes les demandes de certificats répertoriées, cliquez sur **Sélection globale**.

   – **Date d'expiration du certificat**
   À l'expiration du certificat, vous devez répéter cette procédure pour générer des nouveaux fichiers de clés privées pour vos serveurs. Vous pouvez modifier cette date ou conserver la date indiquée par défaut.

   Lorsque vous cliquez sur **OK**, un fichier de certificat est créé pour chaque serveur que vous avez sélectionné. Les certificats sont enregistrés dans le répertoire contenant les demandes de certificats.

   Vous pouvez également obtenir les certificats signés par la CA en exécutant la commande suivante à partir de la ligne de commande : **/usr/websm/bin/smsigncert**.

3. **Importer les certificats signés dans les fichiers de clés privées des serveurs**.

   Lors de cette étape, transférez les certificats de l'autorité de certification du site A au serveur du site B. Copiez–les dans le répertoire contenant les demandes de certificats et les fichiers de clés privées du serveur créés à l'étape 1.

   Puis, sur le serveur du site B, sélectionnez **Importation de certificats signés** dans la liste des tâches de **Sécurité serveur**.

Entrez les informations suivantes :

– **Répertoire de certificats et de clés privées**
Tapez le nom du répertoire contenant les certificats signés et les fichiers de clés privées du serveur. Cliquez sur **Mise à jour de la liste**. La liste des serveurs pour lesquels un certificat a été signé ainsi qu'un fichier de clés privées s'affichent.

– **Sélectionnez un ou plusieurs serveurs dans la liste**
Pour sélectionner des serveurs individuellement, cliquez sur leur nom dans la liste. Pour sélectionner tous les serveurs répertoriés, cliquez sur **Sélection globale**.

Lorsque vous cliquez sur **OK**, vous êtes invité à entrer le mot de passe si les fichiers de clés privées du serveur ont été chiffrés à l'étape 1. Pour chaque serveur sélectionné, le certificat est ensuite importé dans le fichier de clés privées et ce dernier est créé.

Vous pouvez importer des certificats signés à partir de la ligne de commande avec la commande **/usr/websm/bin/smimpservercert**.

4. **Copier les fichiers de clés privées sur tous les serveurs**.

   Chaque fichier de clés privées doit être installé sur le serveur.

   Vous pouvez transférer les fichiers vers les cibles appropriées en toute sécurité. Vous pouvez utiliser un répertoire partagé et une disquette TAR, de la manière suivante :

   – **Répertoire partagé :** Placez tous les fichiers de clés sur un répertoire partagé (NFS ou DFS, par exemple) accessible à chaque serveur.

   Remarque : Pour utiliser cette méthode, vous devez avoir choisi de chiffrer les fichiers de clés privées du serveur dans la boîte de dialogue **Création de clés privées et de demandes de certificat pour ce serveur ou d'autres**, car les fichiers ne sont pas chiffrés par défaut. Nous vous recommandons également de n'accorder qu'à l'administrateur les droits d'accès au répertoire partagé.

   – **Disquette TAR :** Générez une disquette TAR contenant tous les fichiers de clés privées du serveur. L'archive TAR ne doit faire mention que des noms de fichiers, sans les chemins d'accès. Pour cela, accédez au répertoire contenant les fichiers de clés privées du serveur et exécutez la commande **tar –cvf /dev/fd0 *.privkr**.

   Installez les fichiers de clés privées sur chaque serveur.

   a. Connectez–vous sur chaque serveur en tant qu'utilisateur root et lancez Web–based System Manager.

   b. Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Sécurité serveur**.

   c. Sélectionnez **Installation du fichier de clés privées du serveur**.

   d. Sélectionnez l'emplacement des fichiers de clés privées du serveur. Si vous utilisez une disquette TAR, insérez–la dans le lecteur.

   e. Cliquez sur **OK**.

   Si les fichiers de clés privées ont été chiffrés, vous devez indiquer le mot de passe. La clé privée du serveur est installée dans le fichier **/var/websm/security/SM.privkr**. Répétez cette procédure pour chaque serveur.

   Vous pouvez également distribuer les fichiers de clés privées à partir de la ligne de commande avec la commande **/usr/websm/bin/sminstkey**.

5. **Copier le fichier de clés publiques de l'autorité de certification sur tous les serveurs et clients du site B**.

Une copie du fichier de clés publiques de l'autorité de certification contenu dans le répertoire indiqué à l'étape 1 doit être placée sur vos serveurs et clients Web-based System Manager, dans le répertoire que vous avez choisi lors de l'installation et qui doit être conforme aux indications suivantes :

- sur un client AIX, utilisez le répertoire **/usr/websm/codebase** ;
- sur un client Windows, utilisez le répertoire **Program Files\websm\codebase** ;
- sur un client Linux, utilisez le répertoire **/opt/websm/codebase**.

Remarque : Ce fichier doit être copié au format binaire.

Remarque : Le contenu de ce fichier n'est pas confidentiel. Cependant, si vous le placez sur une machine client, il devient possible de connaître l'autorité de certification à laquelle le client se fie. L'accès à ce fichier sur le client doit donc être limité. En mode applet, le client peut faire confiance au serveur pour transmettre ce fichier en même temps que l'applet, à condition d'utiliser le protocole **HTTPS**.

Eviter le transfert des clés privées

Ce scénario permet de créer une clé privée sur le serveur correspondant en prévenant tout transfert éventuel (via le réseau ou une disquette) vers d'autres systèmes. Les serveurs peuvent êtres configurés séparément en répétant la procédure.

Avant d'appliquer ce scénario, vous devez configurer votre CA en suivant les étapes de la section Fichiers de clés « prêts », page 5-4.

Le scénario comprend les tâches suivantes :

1. **Créer une clé privée et une demande de certificat pour votre serveur** Web-based System Manager**.**

   Connectez–vous sur le serveur en tant qu'utilisateur root et lancez Web–based System Manager. Vous ne pouvez pas accéder aux applications de configuration des paramètres de sécurité de Web-based System Manager si vous ne vous êtes pas connecté en tant qu'utilisateur root ou si vous exécutez Web-based System Manager dans une application éloignée ou en mode applet.

   Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Sécurité serveur**.

   Dans la liste des tâches de **Sécurité serveur**, sélectionnez **Création de clés privées et de demandes de certificats pour ce serveur ou d'autres**. Entrez les informations suivantes :

   – **Liste de serveurs**
   Ajoutez à la liste le nom du serveur Web-based System Manager. Le nom du serveur apparaît par défaut dans la première zone de texte. Cliquez sur **Ajout à la liste**.

   – **Nom de société**
   Saisissez un nom descriptif qui identifie votre société ou organisation.

   – **Code pays ou région ISO**
   Indiquez votre code région ou code pays ISO (2 caractères) ou sélectionnez–le dans la liste.

   – **Emplacement des fichiers de clés privées**
   Entrez le nom du répertoire d'écriture du fichier de clés privées et de la demande de certificat. Dans l'étape 2, transférez le fichier de demande de certificat à l'autorité de certification (CA) pour signature. Dans l'étape 3, transférez le certificat signé de l'autorité de certification vers ce répertoire.

   – **Longueur des clés serveur (en bits)**
   Sélectionnez une **longueur de clé** (cette zone s'affiche uniquement si l'ensemble de fichiers **sysmgt.websm.security–us** est installé sur votre système).

   – **Chiffrez les fichiers de clés privées serveur**
   Cette boîte de dialogue crée un fichier de clés privées pour le serveur spécifié. Le fichier contient la clé privée d'un serveur. Par conséquent, il doit toujours être protégé (par chiffrement, par exemple). Si vous sélectionnez cette option, vous êtes invité à entrer un mot de passe. Ce mot de passe est nécessaire lorsque vous importez le certificat signé et que vous installez la clé privée sur le serveur.

   Lorsque vous cliquez sur **OK**, un fichier de clés privées et une demande de certificat sont créés pour ce serveur.

   Vous pouvez effectuer cette tâche depuis la ligne de commande en tapant la commande **/usr/websm/bin/smgenkeycr**.

2. **Obtenir la signature de la CA.**

Transférez le fichier de demande de certificat à l'autorité de certification. Le certificat ne contient pas de données confidentielles. Cependant, leur intégrité et authenticité doivent être garanties pendant le transfert.

Transférez une copie du fichier de demande de certificat du serveur vers un répertoire de la machine de l'autorité de certification. Pour gagner du temps, vous pouvez transférer les demandes de certificats à partir de tous les serveurs et les faire signer par l'autorité de certification.

Connectez–vous sur la machine de la CA en tant qu'utilisateur root et lancez Web–based System Manager. Vous ne pouvez pas accéder aux applications de configuration des paramètres de sécurité de Web-based System Manager si vous ne vous êtes pas connecté en tant qu'utilisateur root ou si vous exécutez Web-based System Manager dans une application éloignée ou en mode applet.

Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Autorité de certification**.

Dans la liste des tâches de l'**Autorité de certification**, sélectionnez **Signature des demandes de certificats**. Entrez les informations suivantes :

– **Répertoire des demandes de certificats**
  Saisissez le nom du répertoire contenant les demandes de certificats. Puis, cliquez sur **Mise à jour de la liste**. La demande de certificat s'affiche.

– **Sélectionnez les demandes de certificats à signer**
  Cliquez sur les demandes de certificats répertoriées.

– **Date d'expiration du certificat**
  À la date d'expiration du certificat, vous devez créer un nouveau fichier de clés privées sur votre serveur. Vous pouvez modifier cette date ou conserver la date indiquée par défaut.

Lorsque vous cliquez sur **OK**, un fichier de certificat est créé pour chaque serveur que vous avez sélectionné. Le certificat est enregistré dans le répertoire contenant les demandes de certificats.

Vous pouvez exécuter cette tâche à partir de la ligne de commande avec la commande **/usr/websm/bin/smsigncert**.

3. **Importer les certificats signés dans les fichiers de clés privées**

   Transférez le certificat de l'autorité de certification vers le serveur et copiez–le dans le répertoire contenant la demande de certificat et le fichier de clés privées serveur créés à l'étape 1.

   Puis, sur le serveur, sélectionnez **Importation de certificats signés** dans la liste des tâches de **Sécurité serveur**.

   Entrez les informations suivantes :

   – **Répertoire de certificats et de clés privées**
     Saisissez le nom du répertoire contenant le certificat signé et le fichier de clés privées serveur. Puis, cliquez sur **Mise à jour de la liste**. Le nom du serveur s'affiche dans la liste.

   – **Sélectionnez un ou plusieurs serveurs dans la liste**
     Cliquez sur le nom de votre serveur dans la liste.

   Lorsque vous cliquez sur **OK**, vous êtes invité à entrer le mot de passe si le fichier de clés privées serveur a été chiffré dans l'étape 1. Le certificat du serveur est ensuite importé dans le fichier de clés privées et ce dernier est créé.

   Vous pouvez exécuter cette tâche à partir de la ligne de commande avec la commande **/usr/websm/bin/smimpservercert**.

4. **Installer la clé privée sur le serveur.**

   Dans la liste des tâches de la **Sécurité serveur**, sélectionnez **Installation du fichier de clés privées du serveur**. Sélectionnez le bouton **Répertoire** et entrez le répertoire contenant le fichier de clés privées du serveur. Le système vous invite à entrer un mot de passe si le fichier de clés a été chiffré. La clé privée du serveur est installée dans le fichier **/var/websm/security/SM.privkr**.

   Vous pouvez effectuer cette tâche depuis la ligne de commande en tapant la commande **/usr/websm/bin/sminstkey**.

5. **Copier le fichier de clés publiques (SM.pubkr) sur tous les serveurs et clients.**

   Une copie du fichier de clés publiques de l'autorité de certification contenu dans le répertoire indiqué à l'étape 1 doit être placée sur vos serveurs et clients Web-based System Manager, dans le répertoire que vous avez choisi lors de l'installation et qui doit être conforme aux indications suivantes :

   – sur un client AIX, utilisez le répertoire **/usr/websm/codebase** ;

   – sur un client Windows, utilisez le répertoire **Program Files\websm\codebase** ;

   – sur un client Linux, utilisez le répertoire **/opt/websm/codebase**.

   Remarque : Ce fichier doit être copié au format binaire.

   Remarque : Le contenu de ce fichier n'est pas confidentiel. Cependant, si vous le placez sur une machine client, il devient possible de connaître l'autorité de certification à laquelle le client se fie. L'accès à ce fichier sur le client doit donc être limité. En mode applet, le client peut faire confiance au serveur pour transmettre ce fichier en même temps que l'applet, à condition d'utiliser le protocole **HTTPS**.

Utilisation d'une autre autorité de certification

Ce scénario est recommandé lorsque vous ne voulez pas utiliser une autorité de certification interne Web-based System Manager, mais une autre autorité de certification interne qui fonctionne peut–être déjà sur votre système. Dans ce scénario, vos demandes de certificats sont signées par cette autre autorité de certification.

1. **Créer des clés privées et des demandes de certificats pour vos serveurs** Web-based System Manager**.**

   Entrez les noms TCP/IP de tous vos serveurs Web-based System Manager dans la boîte de dialogue (un à la fois) ou indiquez le nom d'un fichier contenant la liste de vos serveurs (un serveur par ligne dans ce fichier).

   Connectez–vous sur un serveur en tant qu'utilisateur root et lancez Web–based System Manager. Vous ne pouvez pas accéder aux applications de configuration des paramètres de sécurité de Web-based System Manager si vous ne vous êtes pas connecté en tant qu'utilisateur root ou si vous exécutez Web-based System Manager dans une application éloignée ou en mode applet.

   Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Sécurité serveur**.

   Dans la liste des tâches de **Sécurité serveur**, sélectionnez **Création de clés privées et de demandes de certificats pour ce serveur ou d'autres**. Entrez les informations suivantes :

   – **Liste de serveurs**
     Ajoutez à la liste le nom de vos serveurs Web-based System Manager. Vous pouvez les entrer un par un dans la boîte de dialogue ou indiquer le nom d'un fichier contenant la liste de vos serveurs (un serveur par ligne dans ce fichier). Pour obtenir le nom des serveurs à partir du fichier, entrez le nom du fichier dans la zone **Fichier contenant une liste des serveurs** et cliquez sur **Affichage du fichier**. La boîte de dialogue **Parcourir le fichier contenant la liste des serveurs** vous permet de sélectionner certains (ou tous les) serveurs de la liste.

   – **Nom de société**
     Saisissez un nom descriptif qui identifie votre société ou organisation.

   – **Code pays ou région ISO**
     Indiquez votre code région ou code pays ISO (2 caractères) ou sélectionnez–le dans la liste.

   – **Emplacement des fichiers de clés privées**
     Entrez le nom du répertoire d'écriture des fichiers de clés privées et des demandes de certificats. Dans l'étape 2, transférez les fichiers de demandes de certificats à l'autorité de certification pour signature. Dans l'étape 3, transférez les certificats signés de l'autorité de certification vers ce répertoire.

   – **Longueur des clés serveur (en bits)**
     Sélectionnez une **longueur de clé** (cette zone s'affiche uniquement si l'ensemble de fichiers **sysmgt.websm.security–us** est installé sur votre système).

   – **Chiffrement des fichiers de clés privées serveur**
     Cette boîte de dialogue crée un fichier de clés privées pour chaque serveur spécifié. Chacun de ces fichiers contient la clé privée d'un serveur. Par conséquent, il doit toujours être protégé. Pour cela, vous pouvez chiffrer ces fichiers. Si vous sélectionnez cette option, vous êtes invité à entrer un mot de passe. Ce mot de passe est nécessaire lorsque vous importez les certificats signés et que vous installez les clés privées sur les serveurs.

   Lorsque vous cliquez sur **OK**, un fichier de clés privées et une demande de certificat sont créés pour chaque serveur spécifié.

Vous pouvez exécuter cette tâche à partir de la ligne de commande avec la commande **/usr/websm/bin/smgenkeycr**.

2. **Obtenir la signature de la CA.**

   Transférez les fichiers de demandes de certificats à l'autorité de certification. Ces demandes ne contiennent pas de données confidentielles. Cependant, leur intégrité et authenticité doivent être garanties pendant le transfert.

   Transférez une copie des fichiers de demandes de certificats du serveur vers un répertoire de la machine de l'autorité de certification.

   Suivez les instructions de votre autorité pour générer les certificats signés suite aux demandes de certificats.

3. **Importer les certificats signés dans les fichiers de clés privées du serveur**.

   Transférez les certificats de l'autorité de certification vers le serveur. Copiez–les dans le répertoire contenant les demandes de certificats et les fichiers de clés privées du serveur que vous avez créés lors de l'étape 1. Cette étape exige que le fichier du certificat d'un serveur *S* soit nommée **S.cert**.

   Puis, sur le serveur, dans **Sécurité serveur**, sélectionnez **Importation de certificats signés**.

   Entrez les informations suivantes :

   – **Répertoire de certificats et de clés privées**
     Saisissez le nom du répertoire contenant les certificats signés et les fichier de clés privées du serveur. Puis, cliquez sur **Mise à jour de la liste**. La liste des serveurs pour lesquels il existe un certificat signé ainsi qu'un fichier de clés privées s'affiche.

   – **Sélectionnez un ou plusieurs serveurs dans la liste**
     Pour sélectionner des serveurs individuels, cliquez dessus dans la zone de liste. Pour sélectionner tous les serveurs répertoriés, cliquez sur **Sélection globale**.

   Lorsque vous cliquez sur **OK**, vous êtes invité à entrer le mot de passe si les fichiers de clés privées serveur ont été chiffrés dans l'étape 1. Puis, pour chaque serveur sélectionné, le certificat est importé dans le fichier de clés privées et ce dernier est créé.

   Vous pouvez exécuter la tâche décrite ci–dessus à partir de la ligne de commande avec la commande **/usr/websm/bin/smimpservercert**.

4. **Copier les fichiers de clés privées sur tous les serveurs**

   Chaque fichier de clés privées doit être installé sur le serveur.

   Vous pouvez transférer les fichiers vers les cibles appropriées en toute sécurité. Vous pouvez utiliser un répertoire partagé et une disquette TAR, de la manière suivante :

   – **Répertoire partagé :** Placez tous les fichiers de clés sur un répertoire partagé (NFS ou DFS, par exemple) accessible à chaque serveur.

     Remarque : Pour utiliser cette méthode, vous devez avoir choisi de chiffrer les fichiers de clés privées du serveur dans la boîte de dialogue **Création de clés privées et de demandes de certificats pour ce serveur ou d'autres**, car les fichiers ne sont pas chiffrés par défaut. Nous vous recommandons également de n'accorder qu'à l'administrateur les droits d'accès au répertoire partagé.

   – **Disquette TAR :** Générez une disquette TAR contenant tous les fichiers de clés privées du serveur. L'archive TAR ne doit faire mention que des noms de fichiers, sans les chemins d'accès. Pour cela, placez les répertoires dans le répertoire contenant les fichiers de clés privées du serveur et exécutez la commande **tar –cvf /dev/fd0 *.privkr**.

   Installez les fichiers de clés privées sur chaque serveur.

a. Connectez–vous sur chaque serveur en tant qu'utilisateur root et lancez Web–based System Manager.

b. Sélectionnez **Environnement de gestion —> *nom_hôte* —> Sécurité Web–based System Manager —> Sécurité serveur**.

c. Sélectionnez **Installation du fichier de clés privées**.

d. Sélectionnez l'emplacement des fichiers de clés privées du serveur. Si vous utilisez une disquette TAR, insérez–la dans le lecteur.

e. Cliquez sur **OK**.

Si les fichiers de clés privées ont été chiffrés, vous devez indiquer le mot de passe. La clé privée du serveur est installée dans le fichier **/var/websm/security/SM.privkr**. Répétez cette procédure pour chaque serveur.

Vous pouvez exécuter cette tâche à partir de la ligne de commande avec la commande **/usr/websm/bin/sminstkey**.

5. **Importer le certificat de l'autorité de certification dans le fichiers de clés publiques**.

   Réceptionnez le certificat auto–signé de votre autorité de certification. Copiez–le dans un répertoire du serveur sur lequel vous travaillez.

   Puis, sur le serveur, sélectionnez **Importation du certificat de la CA** dans la liste des tâches de la **Sécurité serveur**.

   Entrez les informations suivantes :

   – **Répertoire contenant le fichier de clés publiques**
     Entrez le répertoire contenant le fichier de clés publiques de l'autorité de certification. Ce fichier doit être transféré sur tous les serveurs et clients.

   – **Nom complet du fichier du certificat CA**
     Entrez le nom du répertoire contenant le certificat auto–signé de votre CA.

   Lorsque vous cliquez sur **OK**, le fichier de clés publiques **SM.pubkr** sera écrit dans le répertoire que vous avez spécifié.

   Vous pouvez exécuter la tâche décrite ci–dessus à partir de la ligne de commande avec la commande **/usr/websm/bin/smimpcacert**.

6. **Copier le fichier de clés publiques sur tous les clients et serveurs**.

   Une copie du fichier de clés publiques de l'autorité de certification contenu dans le répertoire indiqué à l'étape 1 doit être placée sur vos serveurs et clients Web-based System Manager, dans le répertoire que vous avez choisi lors de l'installation et qui doit être conforme aux indications suivantes :

   – sur un client AIX, utilisez le répertoire **/usr/websm/codebase** ;

   – sur un client Windows, utilisez le répertoire **Program Files\websm\codebase** ;

   – sur un client Linux, utilisez le répertoire **/opt/websm/codebase**.

   Remarque : Ce fichier doit être copié au format binaire.

   Remarque : Le contenu de ce fichier n'est pas confidentiel. Cependant, si vous le placez sur une machine client, il devient possible de connaître l'autorité de certification à laquelle le client se fie. L'accès à ce fichier sur le client doit donc être limité. En mode applet, le client peut faire confiance au serveur pour transmettre ce fichier en même temps que l'applet, à condition d'utiliser le protocole **HTTPS**.

Configuration du démon SMGate

Le démon **SMGate** installé avec les fonctions de sécurité Web-based System Manager vous permet de fonctionner en mode applet sécurisé sans avoir à configurer les paramètres de sécurité sur chaque système géré. **SMGate** sert de passerelle SSL entre le navigateur client et le serveur Web local.

Pour utiliser le démon **SMGate**, installez le certificat émis par l'autorité de certification sur chaque navigateur client, comme suit :

1. Si vous utilisez l'autorité de certification interne Web-based System Manager, vous pouvez obtenir le certificat auprès de cette autorité en procédant comme suit :
   a. Connectez–vous sur la machine de l'autorité de certification en tant qu'utilisateur root.
   b. Lancez Web–based System Manager.
   c. Ouvrez l'environnement de gestion et sélectionnez votre hôte local.
   d. Dans la liste des tâches, sélectionnez **Exporter le certificat de l'autorité de certification**.
   e. Dans la boîte de dialogue d'**exportation du certificat de l'autorité de certification**, entrez le nom complet du chemin d'accès de destination du certificat.
   f. Cliquez sur **OK**.

   Vous pouvez également entrer l'instruction suivante sur la ligne de commande :

   ```
   /usr/websm/bin/smexpcacert
   ```

   Remarque : Si vous n'utilisez pas l'autorité de certification interne Web-based System Manager, utilisez alors les procédures de votre autorité de certification pour obtenir une copie de son certificat.
2. Copiez le certificat dans un répertoire du serveur HTTP, de sorte que vous puissiez y accéder depuis le navigateur client. Le type MIME transmis par le serveur HTTP doit être **application/x–x509–ca–cert**.
3. Dans chacun de vos navigateurs clients, pointez le navigateur vers le fichier du certificat CA, puis suivez la procédure du navigateur afin de l'accepter comme un certificat signataire.

Vos navigateurs sont à présent paramétrés pour vous permettre de vous connecter à vos serveurs par l'intermédiaire de **SMGate**. Pour en savoir plus sur l'activation de **SMGate**, reportez–vous à Activation du démon SMGate, page 5-20. Pour en savoir plus sur le fonctionnement de SMGate, reportez–vous à Mode applet, page 5-21.

Affichage des propriétés de configuration

À l'issue de la configuration des paramètres de sécurité, vous pouvez visualiser les propriétés de l'autorité de certification, des différents serveurs et clés publiques du client.

Pour afficher les propriétés de l'autorité de certification, procédez comme suit :

1. Ouvrez l'environnement de gestion et sélectionnez votre hôte local.
2. Sélectionnez **Sécurité Web–based System Manager**.
3. Sélectionnez **Autorité de certification**.
4. Dans la liste des tâches, sélectionnez **Caractéristiques**.
5. Entrez le mot de passe.

Remarque : Les informations fournies concernant l'autorité de certification ne sont pas modifiables.

Pour plus d'informations concernant les fonctions de l'autorité de certification (création de clés ou signature de certificats, par exemple), reportez–vous à son fichier journal **/var/websm/security/SMCa.log**.

Vous pouvez exécuter cette tâche à partir de la ligne de commande avec la commande **/usr/websm/bin/smcaprop**.

Pour afficher les propriétés du serveur, procédez comme suit :

1. Ouvrez l'environnement de gestion et sélectionnez votre hôte local.
2. Sélectionnez **Sécurité Web–based System Manager**.
3. Sélectionnez **Sécurité serveur**.
4. Dans la liste des tâches, sélectionnez **Affichage des caractéristiques du serveur**.
5. Entrez le mot de passe.

Remarque : Les informations fournies concernant le serveur ne sont pas modifiables.

Vous pouvez exécuter cette tâche à partir de la ligne de commande avec la commande **/usr/websm/bin/smserverprop**.

Contenu de la clé publique

Pour visualiser le certificat de l'autorité de certification inclus dans la clé publique correspondante, entrez **/usr/websm/bin/smlistcerts**.

Activation de la sécurité Web-based System Manager

Sur chaque système géré, vous pouvez activer l'option de sécurité que vous souhaitez appliquer.

Pour activer la sécurité de telle sorte que le système géré accepte des connexions sécurisées ou non sécurisées, exécutez la commande **wsmserver –ssloptional**. Dans ce mode, vous pouvez sélectionner une option dans la boîte de dialogue de connexion de Web-based System Manager afin de spécifier le type de connexion (sécurisée ou non).

Pour permettre à un système géré de n'accepter que les connexions sécurisées, exécutez la commande **/usr/websm/bin/wsmserver –sslalways**.

Activation du démon SMGate

Le démon SMGate ne peut être activé qu'après installation de la clé privée du serveur.

Pour activer SMGate, entrez la commande suivante :

```
/usr/websm/bin/wsmserver -enablehttps
```

Cette commande lance SMGate et ajoute une entrée au fichier **/etc/inittab** de façon à ce qu'il soit automatiquement activé lors du redémarrage du système. Le numéro de port par défaut pour SMGate est `9092`. Consultez le fichier **/etc/services** pour vous assurer que ce port n'est pas utilisé par un autre service. Vous pouvez configurer SMGate de manière à ce qu'il utilise un port différent en entrant :

```
/usr/websm/bin/wsmserver -enablehttps   port
```

où *port* est le numéro du port à utiliser.

Si vous modifiez la configuration de sécurité du serveur, vous devez désactiver SMGate. Pour désactiver SMGate, entrez la commande suivante :

```
/usr/websm/bin/wsmserver -disablehttps
```

Pour configurer votre navigateur afin qu'il fonctionne avec SMGate, reportez–vous à Configuration du démon SMGate, page 5-17.

Exécution de la sécurité Web-based System Manager

Web-based System Manager fonctionne en mode application lorsque vous utilisez une machine en tant que client pour gérer une autre machine.

Mode client–serveur

Pour activer le mode client–serveur sur le poste client, entrez la commande suivante :

```
wsm –host   nom_hôte
```

où *nom_hôte* est le nom de la machine distante que vous voulez gérer.

Si la machine à gérer est configurée pour autoriser uniquement les connexions sécurisées (reportez–vous à Activation de la sécurité Web-based System Manager, page 5-19), l'ensemble de fichiers **sysmgt.websm.security** doit être installé sur le client, avec une copie du fichier de clés publiques de l'autorité de certification dans le répertoire **/usr/websm/codebase**. Lorsque ce mode est activé, la boîte de dialogue de connexion de Web-based System Manager indique qu'une connexion sécurisée est requise.

Si le poste à gérer est configuré pour permettre des connexions sécurisées ou non sécurisées (reportez–vous à Activation de la sécurité Web-based System Manager, page 5-19) et que le client possède une copie du fichier de clés publiques de l'autorité de certification dans le répertoire **/usr/websm/codebase**, la boîte de dialogue de connexion de Web-based System Manager vous permet de spécifier une connexion sécurisée ou non sécurisée.

Lorsqu'elle est activée en mode client–serveur, la connexion sécurisée est indiquée par le message `Connexion sécurisée`, qui apparaît sur la ligne d'état en bas de la fenêtre.

Mode client éloigné

Pour démarrer en mode client éloigné, reportez–vous à Mode client éloigné, page 1-7 et suivez les étapes correspondant au type de votre machine.

Si la machine à gérer est configurée pour autoriser uniquement les connexions sécurisées (reportez–vous à Activation de la sécurité Web-based System Manager, page 5-19), la sécurité du client éloigné doit être installée sur le client, avec une copie du fichier de clés publiques de l'autorité de certification dans le répertoire **websm/codebase**. Lorsque ce mode est activé, la boîte de dialogue de connexion de Web-based System Manager indique qu'une connexion sécurisée est requise.

Si le poste à gérer est configuré pour permettre des connexions sécurisées ou non sécurisées (reportez–vous à Activation de la sécurité Web-based System Manager, page 5-19), la boîte de dialogue de connexion de Web-based System Manager vous permet de spécifier une connexion sécurisée ou non sécurisée. Pour que vous puissiez utiliser une connexion sécurisée à partir d'un poste client, la sécurité du client éloigné doit y être installée et une copie du fichier de clés publiques de l'autorité de certification doit se trouver dans le répertoire **websm/codebase** du client.

Lorsqu'elle est activée en mode client–serveur, la connexion sécurisée est indiquée par le message `Connexion sécurisée`, qui apparaît sur la ligne d'état en bas de la fenêtre.

Mode applet

Web-based System Manager fonctionne en mode applet lorsque vous utilisez un navigateur pour vous connecter la machine à gérer. Le mode applet impose une mesure de sécurité supplémentaire pour le transfert sécurisé du fichier de clés publiques de l'autorité de certification et des fichiers **.class** de l'applet. Pour une sécurité totale en mode applet, le client doit utiliser les fonctions SSL de son navigateur et contacter le serveur uniquement par l'intermédiaire du protocole **HTTPS**. Cela requiert que le serveur HTTP soit configuré pour la sécurité ou que SMGate soit configuré à travers une des options suivantes :

- Une possibilité est d'utiliser la fonction SSL du serveur Web sur la machine gérée. Pour pouvoir procéder de cette façon, les options de sécurité du serveur Web doivent être spécialement configurées. Suivez les instructions fournies avec votre serveur Web. Vous pouvez ensuite accéder à Web-based System Manager sur la machine gérée avec l'adresse Web suivante : **https:// *nom_hôte* /wsm.html**, où *nom_hôte* est le nom de la machine distante que vous voulez gérer. Lorsque vous utilisez cette option, l'applet et le fichier de clés publiques **SM.pubkr** sont transférés de façon sécurisée du serveur Web de la machine gérée vers le client.
- Une autre option consiste à utiliser le démon **SMGate**. **SMGate** est exécuté sur les machines gérées et sert de passerelle SSL entre le navigateur client et le serveur Web local. **SMGate** répond à la requête HTTPS du navigateur client et crée une connexion SSL avec lui en utilisant la clé privée et le certificat du serveur Web-based System Manager. Au sein de la machine gérée, **SMGate** créé une connexion non sécurisée sur le serveur Web local.

  Lorsque vous utilisez cette option, l'applet et le fichier de clés publiques **SM.pubkr** sont transférés de façon sécurisée depuis le démon **SMGate** de la machine gérée vers le navigateur client. Les communications entre la machine gérée et le client transitent par SSL. Lorsque vous utilisez **SMGate**, vous pouvez accéder à Web-based System Manager sur la machine gérée via l'adresse Web suivante : https:// *nom_hôte*:9092/wsm.html, où *nom_hôte* est le nom de la machine distante que vous voulez gérer.

  Remarque : `9092` est le numéro de port par défaut pour **SMGate**. Si vous avez activé **SMGate** avec un autre numéro de port, précisez ce numéro.

Lorsque vous fonctionnez en mode applet, assurez–vous que les indicateurs de sécurité suivants sont présents :

- l'indicateur **HTTPS** du navigateur ;
- le message `Connexion sécurisée`, qui s'affiche sur la ligne d'état en bas de la fenêtre Web-based System Manager.

Si l'un de ces indicateurs est absent, la connexion n'est pas totalement sécurisée.

Chapitre 6. Accessibilité de Web-based System Manager

Web-based System Manager offre plusieurs fonctions d'accessibilité, qui sont décrites en détail dans la section qui suit.

Accessibilité au clavier

L'accessibilité au clavier vous permet d'utiliser Web-based System Manager sans recourir à une souris. Vous disposez des fonctions d'accessibilité au clavier suivantes :

- Mnémoniques de menus : Tous les choix de menus peuvent être sélectionnés à partir du clavier en tapant la lettre indiquée dans le titre du menu. Pour ouvrir un menu, tapez la lettre soulignée tout en maintenant enfoncée la touche **Alt**. Cela ne concerne que l'ouverture du menu. Une fois le menu ouvert, relâchez la touche **Alt**.

  Ainsi, pour sélectionner l'option Caractéristiques du menu Sélectionné(s), appuyez simultanément sur la touche `s` et sur la touche **Alt** pour ouvrir le menu, puis relâchez la touche **Alt** et appuyez sur `r` pour sélectionner l'option voulue. Pour pouvoir utiliser les mnémoniques de la barre de menus de Web-based System Manager, vous devez placer le curseur de la souris dans la fenêtre de la console.

- Accélérateur de menu ou raccourcis clavier : Les combinaisons de clés sont disponibles pour les actions communes. Par exemple, Ctrl + Q permet de quitter le programme, F9 permet d'obtenir de l'aide sur l'affectation des touches.

- Caractéristiques d'accessibilité des boîtes de dialogue : Les mnémoniques et les accélérateurs sont disponibles pour les boutons de boîtes de dialogue. Par exemple, la touche Entrée active le bouton OK et la touche Echap active le bouton Annulation.

La touche F9 (aide sur l'affectation des touches) fournit une description de l'ensemble des raccourcis clavier et des accélérateurs. Il existe d'autres raccourcis associés à des touches spéciales, qui permettent notamment de passer d'une zone de la console à une autre ou de développer une arborescence.

Annexe A. Identification des incidents

Les rubriques d'identification et de résolution des incidents présentées dans cette annexe sont les suivantes :

Identification des incidents sur une machine distante

Incident	Résolution

Impossible de gérer un système hôte éloigné comme une machine gérée de type Web–based System Manager.	• Vérifiez si l'hôte que vous essayez de gérer comporte un **sysmgt.websm.framework** dont le niveau de version est postérieur à AIX 5.1.0.15. Les machines avec des niveaux de **sysmgt.websm.framework** postérieurs à AIX 5.1.0.15 ne peuvent être gérées que par des systèmes du même niveau. Par conséquent, pour gérer une machine sur laquelle une version antérieure est installée, procédez de l'une des manières suivantes :
	– utilisez un système avec un **sysmgt.websm.framework** du même niveau ;
	– mettez le système à jour avec AIX 5.1.0.15 ou une version ultérieure ;
	– gérez le système localement.
	• Assurez–vous que l'hôte que vous tentez de gérer est à l'écoute sur le port inetd 9090. Si tel est le cas, il y aura une ligne dans le fichier **/etc/services** similaire à :
	`wsmserver 9090/tcp`
	De plus, il y aura une ligne dans le fichier **/etc/inetd.conf** similaire à la suivante :
	`wsmserver stream tcp nowait root \`
	`/usr/websm/bin/wsmserver wsmserver –start`
	Dans le cas contraire, utilisez la commande suivante :
	`/usr/websm/bin/wsmserver –enable`
	Il est possible d'effectuer un test à l'aide de la commande suivante :
	`tn hostname 9090`
	Si l'hôte éloigné est correctement configuré, il enverra en retour un message similaire à :
	`Tentative...`
	`Connecté à saga.bull.com.`
	`Le caractère d'échappement est '|T'.`
	`Langue reçue du client :`
	`Setlocale: en_US`
	`WServer.HANDSHAKING 41292 WServer.HANDSHAKING en_US`
	où *en_US* est remplacé par l'ensemble de fichiers de langue installé sur votre machine.
	S'il ne répond pas par le résultat précédent, un processus de serveur en veille qui consomme des ressources système est en cours de fonctionnement sur la machine. Connectez–vous au serveur distant et utilisez la commande **kill** sur le processus inactif de WServer.

Le module complémentaire installé sur un hôte éloigné ne s'affiche pas lors de la gestion à partir d'un client.	• Le module complémentaire sur l'hôte distant peut être à un niveau qui ne peut pas être géré par le niveau **sysmgt.websm.framework** installé sur le système client. Dans ce cas, un message d'erreur est affiché lorsque la connexion est faite à l'hôte distant, qui répertorie le module complémentaire et sa version, ainsi que la version de **sysmgt.websm.framework** requise pour gérer ce module. Pour le gérer, vous devrez trouver un système où la version de **sysmgt.websm.framework** est au niveau correct pour le module ou gérer ce module localement sur cet hôte. • Le fichier **App*.db** sur l'hôte distant n'est pas formaté correctement. Un message d'erreur est affiché pour le module complémentaire, avertissant que le fichier **App*.db** n'a pas le format correct pour ce module et que ce dernier n'a pas pu être chargé. Si ce message s'affiche, contactez votre revendeur pour connaître l'action corrective à entreprendre.

Identification des incidents de Web-based System Manager en mode applet

Incident	**Résolution**
Lors de l'utilisation de Netscape Communicator sur un PC, le navigateur vous invite à télécharger le module complémentaire Java. Netscape Communicator ouvre la page mais ne trouve pas le module Java.	1. Vérifiez que vous utilisez Netscape Communicator 4.7 ou 4.7x. Netscape Communicator 6.0 et les versions ultérieures ne sont pas pris en charge. 2. Netscape Communicator ne trouve pas toujours le module correct. Téléchargez–le et installez–le manuellement.
Le navigateur se bloque après un clic sur le bouton Actualiser ou Recharger, Web–based System Manager s'affiche.	Parfois, les navigateurs ne rechargent pas correctement les applets. Vous disposez de deux options : • Régénérez ou supprimez le cache du navigateur. • Redémarrez le navigateur. Celui–ci doit alors recharger les applets.
La tentative de connexion à http://*votremachine*/wsm.html n'affiche que la page d'accueil de votre serveur Web.	Les fichiers html n'ont pas été copiés dans le répertoire **pub** du serveur Web. Pour remédier à cet incident, procédez comme suit : 1. Exécutez **configassist**. 2. Configurez un serveur Web pour exécuter Web–based System Manager. 3. Vérifiez que les fichiers de Web-based System Manager se trouvent dans le répertoire **pub** du serveur Web.

Identification des incidents de Web-based System Manager en mode client éloigné

Incident	Résolution
L'application ne démarre pas.	Les variables de l'environnement système sont créées ou modifiées lors de l'installation. Assurez–vous qu'elles sont définies, en procédant comme suit : • Sous Windows, accédez à l'onglet **Environnement** du **panneau de commande** et vérifiez que la valeur de la variable **WSMDIR** ne contient que la valeur du répertoire d'installation, par exemple, **C:\ProgramFiles\websm**, qui est le répertoire d'installation par défaut. Ce répertoire doit également être contenu dans la variable **PATH**. • Sous Linux, modifiez le fichier **/etc/profile** de telle sorte que la variable **WSMDIR** soit définie et exportée. Vous pouvez alors exécuter la commande **env** pour vérifier que la variable **WSMDIR** est bien présente. Si elle ne l'est pas, fermez votre session et ouvrez–en une autre ou régénérez votre fichier**. /etc/profile** dans cette fenêtre. Ce répertoire doit également être contenu dans la variable **PATH**.
L'installation échoue.	L'une des causes suivantes peut entraîner cet échec : • L'espace disponible sur l'unité par défaut est inférieur à 75 Mo. • L'espace disponible sur l'unité de destination est inférieur à 75 Mo. • Le serveur AIX n'est pas configuré correctement pour l'installation du client éloigné. Pour en savoir plus, reportez–vous à Installation du client distant Web-based System Manager, page 2-7.

Identification des incidents liés à la sécurité

Incident	Résolution
Les fonctions de sécurité sont inopérantes.	Assurez–vous que vous êtes connecté comme utilisateur root et que vous exploitez Web-based System Manager sur la machine locale.
Lorsque vous essayez d'utiliser l'autorité de certification (CA) pour générer des fichiers de clés ou obtenir la signature des certificats, un message s'affiche, indiquant que cette autorité est en cours d'utilisation.	Si vous êtes certain qu'aucun autre administrateur n'utilise l'autorité de certification actuellement, retirez le fichier de verrouillage de l'autorité de certification **/var/websm/security/SMCa.lock**.
Dans la configuration SMGate, le navigateur ne reconnaît pas comme tel le fichier du certificat CA.	Vérifiez que le type mime envoyé par le serveur Web pour le fichier du certificat est **application/x–x509–ca–cert**.

Echec de l'activation distante sécurisée de Web-based System Manager.	• Assurez–vous que Web-based System Manager travaille en mode non sécurisé. Il sera peut–être nécessaire de modifier la configuration du serveur s'il ne prend pas en charge les connexions non sécurisées.
	• Correspondance et expiration du certificat :
	– Connectez–vous au serveur en tant qu'utilisateur root et utilisez la boîte de dialogue des caractéristiques du serveur de l'icône **Serveur** (ou la commande **smserverprop**) pour vérifier la date d'expiration du certificat du serveur. Enregistrez le nom de l'autorité de certification.
	– Si l'incident s'est produit en mode application, entrez :
	`/usr/websm/bin/smlistcerts /usr/websm/codebase`
	sur le client, puis vérifiez que le client comporte un certificat de l'autorité de certification qui a signé le certificat du serveur (ci–dessus) et que ce certificat n'a pas expiré. Si l'incident s'est produit en mode applet, entrez :
	`/usr/websm/bin/smlistcerts /usr/websm/codebase`
	`sur le serveur, car le fichier de clés publiques réside sur le serveur et est transféré au client.`
	– En mode client éloigné, assurez–vous que le répertoire **codebase** de Web–based System Manager sur la machine client contient le fichier de clés publiques de l'autorité de certification (**SM.pubkr**). Assurez–vous également qu'il y a été placé au format binaire.

Index

N

P

R

S

W

Z

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull AIX 5L Web–based System Manager : Guide d'administration

Nº Référence / Reference Nº : 86 F2 34EF 02

Daté / Dated : Octobre 2002

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Technical Publications Ordering Form

Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL CEDOC
ATTN / Mr. L. CHERUBIN
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Phone / Téléphone : +33 (0) 2 41 73 63 96
FAX / Télécopie +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web sites at: / Ou visitez nos sites web à:

http://www.logistics.bull.net/cedoc
http://www-frec.bull.com   http://www.bull.com

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	

[_ _] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente

NOM / NAME : ______________________ Date : __________

SOCIETE / COMPANY : ______________________

ADRESSE / ADDRESS : ______________________

____

PHONE / TELEPHONE : ______________ FAX : ______________

E–MAIL : ______________________

For Bull Subsidiaries / Pour les Filiales Bull :
Identification: ______________________

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :
Customer Code / Code Client : ______________________

For Bull Internal Customers / Pour les Clients Internes Bull :
Budgetary Section / Section Budgétaire : ______________________

For Others / Pour les Autres :
Please ask your Bull representative. / Merci de demander à votre contact Bull.

PLACE BAR CODE IN LOWER LEFT CORNER

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 F2 34EF 02

Bull

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

AIX 5L
Web–based
System
Manager
Guide
d’administration
86 F2 34EF 02

AIX 5L
Web–based
System
Manager
Guide
d’administration
86 F2 34EF 02

AIX 5L
Web–based
System
Manager
Guide
d’administration
86 F2 34EF 02