HP Universal CMDB Configuration Manager

pour les systèmes d'exploitation Windows et Linux

Version du logiciel : 9.20

Manuel de déploiement

Date de publication du document : Juin 2011
Date de publication du logiciel : Juin 2011

Mentions légales

Garantie

Les seules garanties applicables aux produits et services HP sont celles figurant dans les déclarations de garantie expresse accompagnant les dits produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. HP ne peut en aucun cas être tenu pour responsable des erreurs ou omissions techniques ou rédactionnelles du présent document.

Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

Légende de restriction des droits

Logiciel confidentiel. Licence HP valide requise pour la détention, l'utilisation ou la copie. En accord avec les articles FAR 12.211 et 12.212, les logiciels informatiques, la documentation des logiciels et les informations techniques commerciales sont concédés au gouvernement américain sous licence commerciale standard du fournisseur.

Mentions relatives aux droits de reproduction

Mises à jour de la documentation

La page de titre de ce document contient les informations d'identification suivantes :

- La date de publication du document est actualisée à chaque modification.
- La date de la version correspond à la date de disponibilité de cette version du logiciel.

Pour rechercher des mises à jour ou vérifier que vous disposez de l'édition la plus récente d'un document, visitez le site :

http://h20230.www2.hp.com/selfsolve/manuals

Pour accéder à ce site, vous devrez disposer d'un identificateur HP Passport. Le cas échéant, accédez à la page suivante pour demander un identificateur HP Passport :

http://h20229.www2.hp.com/passport-registration.html

Vous pouvez également cliquer sur le lien **New users - please register** (Nouveaux utilisateurs - Inscrivez-vous) de la page de connexion à HP.

Vous pouvez recevoir des mises à jour ou de nouvelles éditions de ce document si vous vous abonnez au service d'assistance approprié. Pour plus de détails, contactez votre représentant commercial HP.

Support technique

Visitez le site d'assistance technique de HP Software à l'adresse :

http://www.hp.com/go/hpsoftwaresupport

Ce site Web indique les coordonnées des services et contient des informations sur les produits, les services et le support technique proposés par HP Software.

L'assistance technique en ligne offre aux utilisateurs des fonctions interactives pour résoudre des problèmes. De manière efficace et rapide, il vous donne un accès direct aux outils de support technique nécessaires à la gestion de vos opérations. En tant que client du support technique, vous pouvez réaliser les opérations suivantes sur ce site Web :

- rechercher des documents de connaissances présentant un réel intérêt ;
- soumettre et suivre des demandes de support et des demandes d'améliorations ;
- télécharger des correctifs logiciels ;
- gérer des contrats d'assistance ;
- rechercher des contacts HP spécialisés dans l'assistance ;
- consulter les informations sur les services disponibles ;
- participer à des discussions avec d'autres clients qui utilisent les logiciels ;
- rechercher des cours de formation sur les logiciels et vous y inscrire.

Pour accéder à la plupart des offres de support, vous devez vous inscrire en tant qu'utilisateur disposant d'un compte HP Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance. Le cas échéant, accédez à la page suivante pour demander un identificateur HP Passport :

http://h20229.www2.hp.com/passport-registration.html

Les informations relatives aux niveaux d'accès sont détaillées à l'adresse suivante :

http://h20230.www2.hp.com/new_access_levels.jsp

Table des Matières

PARTIE I: INSTALLATION ET CONFIGURATION

Partie I

Installation et configuration

1

Présentation

Contenu de ce chapitre :

Composants

HP Universal CMDB Configuration Manager est une version contenant plusieurs composants :

- **HP Universal CMDB Foundation**

  HP Universal CMDB Foundation (UCMDB Foundation) est une base de données de gestion de la configuration (CMDB) destinée aux entreprises informatiques pour documenter, enregistrer et gérer les définitions de services métier et les relations d'infrastructure associées.

  UCMDB Foundation implémente un modèle de données, la gestion des flux de données et des fonctionnalités de modélisation des données. Il fournit également l'analyse de l'impact, le suivi des modifications et des fonctions de création de rapports pour transformer les données CMDB en données compréhensibles pouvant être traitées afin de mieux répondre aux questions critiques et résoudre les problèmes métier.

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager (Configuration Manager) offre une nouvelle topologie basée sur des politiques et la gestion de la configuration d'inventaire. Créé spécifiquement pour les gestionnaires de configuration et les propriétaires de configuration, il permet à ces utilisateurs d'effectuer une analyse approfondie en plus des données des CI et du contenu de la topologie disponibles dans UCMDB. Configuration Manager leur offre les outils nécessaires pour configurer facilement les politiques de configuration de topologie et d'inventaire, et déterminer automatiquement leur niveau de compatibilité avec les normes organisationnelles.

Configuration Manager est déployé en tant que serveur supplémentaire basé sur Tomcat. Il communique avec le serveur UCMDB à l'aide de UCMDB SDK complet.

➤ **HP Discovery and Dependency Mapping Advanced Edition**

Le logiciel HP Discovery and Dependency Mapping Advanced Edition (DDMA), dont le contenu riche est mis à jour constamment, est la méthode préférée d'UCMDB pour l'acquisition et la gestion des données d'infrastructure informatiques.

➤ **HP Operations Orchestration**

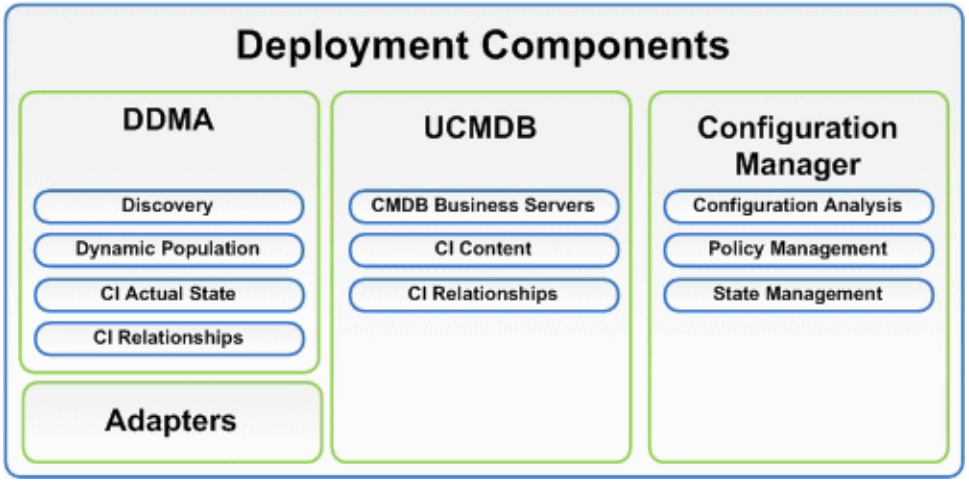
HP Operations Orchestration **(**OO) est un outil de création et de déploiement de flux. Les fonctions intuitives glisser-déposer d'OO Studio permettent aux utilisateurs de concevoir, créer, partager et personnaliser des flux en ayant peu ou pas de compétences en matière de programmation. OO Studio prend en charge la collaboration entre plusieurs auteurs à l'aide de fonctionnalités de contrôle de version. L'outil de débogage puissant intégré, qui permet de tester les flux dans plusieurs environnements, accélère le développement de contenu et permet de valider les flux en vue d'une exécution stable et fiable.

OO Studio permet également aux utilisateurs de déployer des flux. Il permet aux utilisateurs de comparer et de promouvoir les flux dans plusieurs environnements (développement, test, intermédiaire et production). Les processus standard peuvent être documentés et une documentation structurée peut être créée pour répondre aux besoins de compatibilité à l'aide de Studio.

➤ **Intégration de Configuration Manager dans OO**

Configuration Manager permet d'exécuter des flux OO à partir de l'infrastructure de Configuration Manager. Il existe deux méthodes principales pour exécuter des flux OO :

- **Intégration de processus** – permet d'ouvrir un RFC dans une demande de bureau de service externe qui aligne un CI spécifique sur une politique de configuration particulière.
- **Correction de politique** – permet de déclencher un flux OO qui corrige le problème de configuration. Par exemple, vous pouvez allouer de la mémoire supplémentaire à un ordinateur hôte virtuel.



Identifier votre environnement

Ce guide décrit la procédure de déploiement de HP Universal CMDB Configuration Manager à partir de différents points de départ possibles :

Pour Configuration Manager

➤ Si Configuration Manager version 9.10 est installé

Pour plus d'informations sur la mise à niveau de Configuration Manager en fonction de la version actuelle, voir "Mise à niveau de Configuration Manager", page 39.

➤ Si la version de Configuration Manager n'est pas installée

Pour plus d'informations, voir :

- "Installation de HP Universal CMDB Configuration Manager sur une plate-forme Windows", page 17
- "Installation de HP Universal CMDB Configuration Manager sur une plate forme Linux", page 43

Pour UCMDB

➤ Si une version d'UCMDB antérieure à la version 9.03 est installée

Procédez comme suit :

- Effectuez la mise niveau UCMDB version 9.03. Pour plus d'informations, voir *HP Universal CMDB Manuel de déploiement* (format PDF). Vous pouvez télécharger le manuel à partir du site www.hp.com/go/hpsoftwaresupport.
- Installez Cumulative Update Pack 2. Vous pouvez l'obtenir sur le support d'installation de Configuration Manager ou le télécharger à partir de www.hp.com/go/hpsoftwaresupport.

Pour plus d'informations sur la configuration de la disponibilité de l'entreprise, voir "Configurer la base de données ou le schéma d'utilisateur", page 18.

➤ Si UCMDB version 9.03 est installé

Installez Cumulative Update Pack 2. Vous pouvez l'obtenir sur le support d'installation de Configuration Manager ou le télécharger à partir de www.hp.com/go/hpsoftwaresupport.

Pour plus d'informations sur la configuration de la disponibilité de l'entreprise, voir "Configurer la base de données ou le schéma d'utilisateur", page 18.

➤ Si aucune version d'UCMDB n'est installée

Essayez l'une des solutions suivantes :

➤ Utilisez le Gestionnaire de déploiement (systèmes Windows uniquement) pour installer UCMDB lors de l'installation de Configuration Manager. Pour plus d'informations, voir "Installation de HP Universal CMDB Configuration Manager sur une plate-forme Windows", page 17.

➤ Installez Configuration Manager sur un système Linux en suivant les instructions de "Installation de HP Universal CMDB Configuration Manager sur une plate forme Linux", page 43.

Informations générales

Ce guide prend également en compte les déploiements UCMDB spéciaux de votre environnement (par exemple, déploiement haute disponibilité) et fournit les ajustements nécessaires de la procédure de déploiement pour ces déploiements.

Remarque : L'installation d'UCMDB et de Configuration Manager sur le même serveur est prise en charge. Pour les besoins de mise à l'échelle dans un environnement de production, HP Software recommande d'installer ces composants sur des serveurs distincts.

L'utilisation de Configuration Manager requiert la configuration d'UCMDB en mode schéma consolidé et la création d'un nouvel état UCMDB (Autorisé). Ces configurations sont exécutées automatiquement par la procédure de déploiement dans les deux installations (si une installation d'UCMDB existe déjà ou s'il a été installé par le Gestionnaire de déploiement).

Important : Si vous référencez une installation UCMDB existante et que son schéma n'est pas déjà consolidé, l'étape de consolidation peut prendre du temps (20 à 60 minutes) pour les bases de données volumineuses (celles qui contiennent plus de 5 millions de CI).

Sachez que si vous déployez uniquement Configuration Manager (utilisation d'une installation existante ou mise à niveau d'UCMDB), le serveur UCMDB doit fonctionner pour terminer l'installation de Configuration Manager.

Matrice de prise en charge

Configuration système requise pour le serveur

Processeur	4 cœurs au minimum
Mémoire (RAM)	4 Go au minimum
Plateforme	x64
Système d'exploitation	Windows (64 bits) ➤ Windows 2003 Enterprise SP2 et R2 SP2 ➤ Windows 2008 Enterprise SP2 et R2 Linux ➤ Red Hat Enterprise Linux x86 (64 bits)

Base de données	➤ Microsoft SQL Server 2005 SP2 ; 2005 Mode de compatibilité 80 ; (Enterprise Editions pour tous) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
Serveur Web	➤ Microsoft IIS 7 ➤ Apache 2
HP Universal CMDB	➤ HP Universal CMDB version 9.03 avec CUP 2 (installation CMDB standard) Pour une liste complète de la configuration système requise, voir le *HP Universal CMDB Manuel de déploiement* (format PDF). **Remarque :** ➤ Lorsque le serveur HP Universal CMDB est déployé avec Configuration Manager, Enterprise Edition d'Oracle et l'option Oracle Partitioning sont requis. ➤ Si vous avez déjà déployé le serveur HP Universal CMDB avec Standard Edition d'Oracle, et que vous prévoyez d'ajouter Configuration Manager à votre installation, vous devez d'abord convertir votre base de données Standard Edition en base Enterprise Edition après avoir activé l'option de partitionnement.
LDAP (facultatif)	➤ Active Directory ➤ SunONE 6.x
Taille minimale de schéma de base de données recommandée (facultatif)	2 Go

Configuration système requise pour le client

Système d'exploitation	➤ Windows XP x86 (32 bits) ➤ Windows Vista x86 (32 et 64 bits) ➤ Windows 7 x86 (32 et 64 bits)
Navigateur	➤ Microsoft Internet Explorer 7.0, 8.0 ➤ Mozilla Firefox 3.x, 4
Plugin de navigateur Flash Player	Flash Player 9 ou ultérieure **Remarque :** Téléchargez Flash Player depuis le site : http://www.adobe.com/products/flashplayer/.
Résolution d'écran	➤ 1 024 x 768 minimum ➤ 1 280 x 1 024 recommandée
Qualité couleur	16 bits minimum

HP Operations Orchestration (facultatif)

HP Operations Orchestration	➤ 7.51, 9.0

2

Installation de HP Universal CMDB Configuration Manager sur une plate-forme Windows

Important : Veuillez lire les notes de mise à jour pour connaître les instructions d'installation actualisées.

Contenu de ce chapitre :

Configuration de la pré-installation

Cette section inclut les rubriques suivantes :

Configurer la base de données ou le schéma d'utilisateur

Remarque : Cette tâche est exécutée automatiquement dans le cadre du processus d'installation de Configuration Manager. Cependant, vous pouvez l'exécuter manuellement si vous le souhaitez.

Pour utiliser Configuration Manager, vous devez fournir un schéma de base de données. Configuration Manager et UCMDB utilisent différents schémas. Configuration Manager prend en charge Microsoft SQL Server et Oracle Database Server. Cette tâche décrit comment créer un schéma pour Configuration Manager. Si vous installez UCMDB, vous devez configurer une base de données séparée ou un schéma d'utilisateur correspondant. Pour plus d'informations, voir *HP Universal CMDB Manuel de déploiement* (format PDF).

Remarque : Pour connaître la configuration système Microsoft SQL Server et Oracle Server requise, voir "Configuration système requise pour le serveur", page 14.

Pour configurer votre base de données :

1 Allouez une base de données Microsoft SQL Server ou un schéma d'utilisateur Oracle Server.

➤ Pour **Microsoft SQL Server** : Activez la fonctionnalité d'isolement de capture d'instantané.

Exécutez la commande suivante une fois la base de données créée :

```
alter database <nom_basededonnées_ccm> set read_committed_snapshot on
```

Pour plus d'informations sur la fonctionnalité d'isolement de capture d'instantané SQL Server, visitez le site http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

➤ Pour **Oracle** : Attribuez à l'utilisateur Oracle uniquement les rôles **Connect** et **Resource**.
(L'octroi du privilège **Select any table** provoque l'échec de la procédure de remplissage du schéma.)

2 Vérifiez les informations suivantes, nécessaires lors de ce processus de configuration :

✔	**Informations requises**
	Nom d'hôte et port de la base de données
	Nom d'utilisateur et mot de passe de la base de données
	Pour MS SQL : Nom de la base de données
	Pour Oracle : SID

Installer Configuration Manager dans un environnement haute disponibilité UCMDB

Pour utiliser Configuration Manager dans un environnement haute disponibilité UCMDB, procédez comme suit :

1 Arrêtez le serveur de sauvegarde (passif). Attendez deux minutes après l'arrêt.

2 Installez Configuration Manager version 9.20.

a Utilisez les détails de l'hôte d'équilibrage de la charge.

b Installez Configuration Manager sur un troisième serveur, pas un serveur UCMDB.

3 Vérifiez que UCMDB et Configuration Manager fonctionnent correctement.

4 Démarrez le serveur de sauvegarde (passif) pour assurer la haute disponibilité.

Remarque : Le mode Haute disponibilité n'est pas pris en charge pour HP Universal CMDB Configuration Manager version 9.20.

Installer Configuration Manager

Le Gestionnaire de déploiement peut installer UCMDB, Configuration Manager et DDMA dans différentes configurations (choisies et configurées dans la page Sélection de produit de l'assistant d'installation) :

- Installation d'une nouvelle instance d'UCMDB
- Installation d'une nouvelle instance de Configuration Manager et connexion à une instance nouvelle ou existante d'UCMDB
- Intégration d'une nouvelle instance de Configuration Manager à une instance existante d'OO
- Installation de plusieurs instances de DDMA

Remarque :

- Le Gestionnaire de déploiement vous permet d'installer des produits, des composants et des intégrations sur un ordinateur cible. Le Gestionnaire de déploiement ne prend pas en charge la désinstallation des produits, la modification de produits et l'installation des correctifs sur un produit installé. Ces opérations doivent être exécutées manuellement.
- Une fois que vous avez appuyé sur le bouton **Suivant** dans la page Sélection de produit, vous ne pouvez pas revenir à cette page et sélectionner à nouveau la configuration de déploiement. Si des modifications doivent être apportées à la configuration de déploiement, redémarrez le Gestionnaire de déploiement.

Pour installer Configuration Manager :

1. Pour démarrer l'installation, insérez le support d'installation de Configuration Manager dans l'ordinateur et recherchez le fichier **setup.exe**.
2. Double-cliquez sur le fichier **setup.exe** pour exécuter le Gestionnaire de déploiement.

3 Désactivez le pare-feu Windows sur l'ordinateur cible pendant l'installation. Pour plus d'informations sur le pare-feu, allez à l'étape 6 de cette procédure.

4 Acceptez les termes du Contrat de Licence Utilisateur Final et cliquez sur **Suivant** pour ouvrir la page Sélection de produit.

Remarque : Les termes de ce contrat s'appliquent à l'ensemble des produits sélectionnés dans la page Sélection du produit du Gestionnaire de déploiement.

---

5 Sélectionnez les produits appropriés au déploiement dans la page Sélection de produit. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Emplacement du serveur.

La page Sélection de produit permet de sélectionner les produits à installer et de spécifier les options de configuration exécutées pendant le déploiement.

a Sélectionnez une option d'installation HP Universal CMDB Foundation.

Il existe deux options d'installation d'UCMDB Foundation :

- **Connect to an Existing Server** – Une fois sélectionnée, cette option connecte et configure Configuration Manager ou Discovery and Dependency Mapping selon une instance existante d'un serveur UCMDB Foundation.

  Remarque : La version UCMDB d'un serveur existant doit avoir la version 9.03 avec CUP 2 ou supérieur.

- **Install New Server** – une fois sélectionnée, cette option installe, configure et connecte une nouvelle instance d'un serveur UCMDB Foundation et configure et connecte Configuration Manager ou DDMA à la nouvelle instance du serveur UCMDB Foundation.

b Cochez la case **Configuration Manager** pour installer et configurer une nouvelle instance de Configuration Manager.

Si nécessaire, sélectionnez **Connect to an Existing HP Operation Orchestration instance**. Cette option configure une intégration entre Configuration Manager et Operations Orchestration en renseignant Configuration Manager avec les détails de connexion du serveur OO.

c **HP Discovery and Dependency Mapping Advanced Edition.** Une fois sélectionnée, cette option installe et configure de nouvelles instances de DDMA.

L'option **Number of DDMA instance** permet d'installer plusieurs instances DDMA. Le nombre spécifié dans le champ de saisie indique le nombre d'instances DDMA connectées à une instance de serveur UCMDB.

Remarque : Le Gestionnaire de déploiement prend en charge plusieurs déploiements d'instances DDMA dans le même DMZ. Il prend en charge jusqu'à 10 instances d'analyse de détection dans chaque déploiement. Si des analyses de détection supplémentaires sont requises, installez-les en plusieurs phases de déploiement par groupes de dix.

---

6 Spécifiez l'emplacement des serveurs distants et les informations d'identification des ordinateurs de déploiement cible pour les produits sélectionnés pour le déploiement dans la page Emplacement du serveur. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Connexions.

Options de déploiement

Sélectionnez une option de déploiement pour l'emplacement cible. Il existe deux options :

- **Deploy on the local machine** – utilisez cette option lors du déploiement d'un produit sur le même ordinateur que le Gestionnaire de déploiement. Dans ce cas, les champs contenant les détails et les informations d'identification des hôtes distants sont désactivés.
- **Deploy on the following machine** – une fois sélectionnée, vous devez fournir l'adresse de l'hôte distant et les détails du système d'exploitation. Des privilèges d'administrateur doivent être associés aux informations d'identification de l'utilisateur sur l'hôte distant.

Remarque : Lorsque vous spécifiez le nom d'hôte pour le déploiement du produit, veillez à utiliser uniquement des lettres (a-z), des chiffres (0-9) et le tiret ('-').

Les informations suivantes s'appliquent lors de la spécification des détails de l'ordinateur distant :

- **WMI and SMB Protocols** – permettent de se connecter à l'ordinateur distant. Les conditions préalables suivantes doivent exister pour que le Gestionnaire de déploiement se connecte avec succès à l'ordinateur distant.
  - **WMI Service** – le service WMI doit fonctionner sur l'ordinateur hôte.
  - **Server Service** – pour activer le protocole SMB, le service Serveur doit fonctionner sur l'ordinateur distant.

➤ **Pare-feu Windows** – l'ordinateur distant doit autoriser les connexions admin distantes. Exécutez la commande appropriée sur la console d'invite de commande de l'ordinateur distant :

Système d'exploitation	Commande
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

Tester la connexion

Cliquez sur **Tester la connexion** pour vérifier que les informations d'identification et les détails de la connexion sont corrects et analyser les ressources système locales et distantes.

Si le test de la connexion échoue, le Gestionnaire de déploiement affiche un message d'erreur contenant les détails de l'échec. Appuyez sur le bouton **Suivant** pour forcer automatiquement la vérification du test de la connexion.

Les ressources de l'ordinateur sont validées aux emplacements suivants :

➤ **Plate-forme du système d'exploitation** – vérifier que le système d'exploitation est certifié pour le déploiement du produit.

➤ **Espace disque** – vérifier que l'espace disque est suffisant.

➤ **Mémoire** – vérifier que la mémoire physique est suffisante.

➤ **Ports** – vérifier que les ports nécessaires sont disponibles.

Les validations de ressources effectuées par l'option de test de la connexion varient selon les matrices de produits prises en charge.

Remarque : Si le test renvoie une erreur **Inconnu**, vérifiez que les services suivants fonctionnent sur l'ordinateur hôte de déploiement :

- Serveur
- Infrastructure de gestion Windows

Vérifiez que le contrôle de compte d'utilisateur (UAC) est désactivé avant de cliquer sur **Suivant**. Pour plus d'informations sur le contrôle de compte d'utilisateur, visitez le site Web http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

7 Configurez des connexions entre les produits sélectionnés sur la page Connexions. Les options de connexion de cette page reflètent les composants sélectionnés pour le déploiement dans la page Sélection de produit. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Configuration de l'installation.

- Intégration d'UCMDB dans Configuration Manager

  Cette section apparaît lorsque vous choisissez d'installer Configuration Manager à l'aide de l'option **Connect to an Existing Server** et permet de configurer l'intégration de Configuration Manager dans UCMDB.

  Remarque : Pour établir une connexion à une instance existante d'UCMDB, cette installation doit comporter UCMDB version 9.03 avec CUP 2 ou ultérieur.

Indiquez les détails UCMDB suivants :

Champ	Définition
UCMDB Host Name/IP	Adresse de l'emplacement de déploiement d'UCMDB. ➤ Si UCMDB est configuré en mode haute disponibilité, suivez les instructions de la section "Installer Configuration Manager dans un environnement haute disponibilité UCMDB", page 19. ➤ Si UCMDB est installé sur l'ordinateur local et Configuration Manager est installé sur un ordinateur distant, le nom de l'instance UCMDB locale doit être le nom de domaine complet (FQDN) et non localhost. ➤ Si UCMDB et Configuration Manager comportent des noms de domaine DNS différents et que l'intégration LW-SSO est requise, vous devez spécifier le nom de domaine complet (FQDN) dans le champ de saisie de l'hôte UCMDB.
Protocole	HTTP ou HTTPS.
Port UCMDB HTTP(S)	Les valeurs du port HTTP ou HTTPS sont **8080** pour HTTP et **8443** pour HTTPS.
Client Certificate File	Ce champ apparaît lorsque le protocole HTTPS est sélectionné. Vous devez placer manuellement le fichier de certificat client UCMDB sur l'hôte cible de Configuration Manager et spécifier le chemin de fichier complet y compris le nom du fichier dans le champ de saisie adjacent. Si UCMDB utilise HTTPS, l'utilisation d'un échange de clés est requis. Cet échange n'est pas validé pendant le test de la connexion.

Champ	Définition
Nom du client	Le nom du client UCMDB par défaut est **Client par défaut**. La valeur du nom du client est utilisée pendant la configuration de l'intégration d'UCMDB et de Configuration Manager. Cette valeur n'est pas validée par le test de la connexion. Si vous indiquez une valeur incorrecte, le déploiement échouera.
Port JMX	La valeur par défaut est ***29601***.
UCMDB System User (JMX)	L'utilisateur système UCMDB (JMX) est utilisé pour activer les fonctions JMX telles que la création d'un utilisateur d'intégration Configuration Manager et déployer le package Configuration Manager. La valeur par défaut prête à l'emploi est **sysadmin**.
UCMDB System Password	Mot de passe de l'utilisateur système UCMDB. La valeur par défaut est **sysadmin**.

Remarque : Configuration Manager est configuré à l'aide d'un référentiel utilisateur interne. Si vous souhaitez utiliser un LDAP externe comme référentiel utilisateur, vous devez configurer Configuration Manager pour qu'il l'utilise. Pour plus d'informations, voir "Paramètres système" dans le *Manuel de l'utilisateur HP Universal CMDB Configuration Manager.*

➤ Intégration de Configuration Manager dans OO

Cette section apparaît lorsque vous sélectionnez l'option **Connect to an Existing HP Operation Orchestration instance**. Elle permet de configurer l'intégration de Configuration Manager dans OO.

Indiquez les détails OO suivants :

Champ	Définition
OO Version	Versions OO valides : 7.5 et 9.0.
OO Host Name/IP	Hôte ou adresse IP de l'ordinateur serveur OO.
OO Port Number	Le numéro port par défaut est **8443**.
Nom d'utilisateur OO	Le nom d'utilisateur OO par défaut est **admin**. L'utilisateur doit être configuré comme externe dans OO.
OO Password	Le mot de passe OO par défaut est **admin**.

➤ Configuration DDMA

Les champs suivants apparaissent lorsque vous sélectionnez l'option **Discovery and Dependency Mapping Advanced Edition instance**. Elle permet de configurer une connexion DDMA à UCMDB.

Indiquez les détails DDMA suivants :

Champ	Définition
Data Flow Probe Identifier	La valeur par défaut est le nom hôte de l'ordinateur DDMA. Ce champ est renseigné automatiquement. Vous pouvez modifier cette valeur.
Use Default Domain	Cette option est sélectionnée par défaut. Elle affecte la valeur du nom de domaine. Si vous désélectionnez cette case à cocher, vous pouvez remplacer le nom par défaut par une autre valeur.
Nom de domaine	La valeur par défaut est **DefaultDomain**. Pour activer ce champ, désélectionnez la case **Utiliser le domaine par défaut**.
Initial Heap Size in MB	La taille initiale de mémoire affectée au JVM de DDMA. La valeur par défaut est 256 Mo.
Maximum Heap Size in MB	Taille maximale de mémoire affectée au JVM. La valeur par défaut est 512 Mo.

8 Définissez les détails du répertoire cible de déploiement pour les déploiements du produit que vous avez sélectionnés dans la page Configuration de l'installation. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Configuration de la base de données.

Un chemin de répertoire par défaut est indiqué pour chaque produit sélectionné. Si vous effectuez le déploiement sur un ordinateur local, une option Parcourir est disponible pour sélectionner un autre chemin de répertoire. Si vous effectuez l'installation sur un ordinateur distant, cette option est désactivée.

Remarque : Le nom du répertoire d'installation ne doit pas contenir d'espaces. Vous ne pouvez utiliser que des lettres (a-z), des chiffres (0-9) et le tiret ('-').

---

9 Configurez la connexion à la base de données et le schéma de base de données de chaque produit dans la page Configuration de la base de données. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Configuration du port.

Vous pouvez configurer les bases de données suivantes (schémas) :

- schéma UCMDB-CM
- schéma UCMDB
- schéma Historique UCMDB

Champ	Définition
Database Host Name/IP	Adresse de l'emplacement du serveur de la base de données.
Port	MSSQL et Oracle utilisent des ports par défaut différents. Le port par défaut de la base de données Oracle est 1521 et celui de la base de données MSSQL est 1433.
SID (Oracle)	Nom de l'instance de base de données Oracle.

Champ	Définition
Nom d'utilisateur Admin (Oracle)	Entrez le nom d'utilisateur de l'administrateur Oracle en fonction du serveur Oracle.
Mot de passe Admin (Oracle)	Entrez le mot de passe de l'administrateur Oracle en fonction du serveur Oracle.
Tester la connexion	Tester la connexion à l'hôte de la base de données cible, à l'aide des informations d'identification fournies.
Schema Name (Oracle)	Entrez le nom du schéma.
Schema Password (Oracle)	Entrez le mot de passe du schéma. Ce champ apparaît lorsque vous créez un nouveau schéma.
Default Tablespace (Oracle)	Entrez le nom de l'espace disque logique par défaut.
Temporary Tablespace (Oracle)	Entrez le nom de l'espace disque logique temporaire.
Database Name (MSSQL)	Entrez le nom du schéma de base de données à utiliser/créer sur le serveur MSSQL.
Database Username (MSSQL)	Entrez le nom d'utilisateur de l'administrateur MSSQL en fonction du serveur MSSQL.
Database Password (MSSQL)	Entrez le mot de passe de l'administrateur MSSQL en fonction du serveur Oracle.

Remarque :

- Si l'espace disque logique UCMDB est plein, le déploiement des produits aboutira mais les produits et les composants ne fonctionneront pas correctement.
- La création d'un nouveau schéma UCMDB et la connexion à un schéma historique UCMDB existant ne sont pas prises en charge.
- Pour des raisons de sécurité, l'utilisation de l'authentification NTLM lors de la configuration de schémas UCMDB à l'aide d'une base de données MSSQL, lorsqu'UCMDB est installé à distance, n'est pas prise en charge. Si l'authentification NTLM est requise, déployez UCMDB localement.

Mode Schéma

Configuration Manager requiert la configuration d'UCMDB en mode schéma consolidé et la création d'un nouvel état UCMDB.

Si vous référencez une installation UCMDB existante et que son schéma n'est pas déjà consolidé, l'étape de consolidation automatique peut prendre du temps (20 à 60 minutes) pour les bases de données volumineuses (celles qui contiennent plus de 5 millions de CI).

Remarque : Les connexions Oracle Real Application Cluster (RAC) et SQL Server NTLM ne sont pas prises en charge dans le cadre de cette installation. Si ces connexions sont requises, installez d'abord Configuration Manager avec une simple connexion à la base de données et lorsque l'installation est terminée, modifiez la connexion dans la configuration appropriée. Pour ce faire, modifiez le fichier **database.properties** en fonction des spécifications de la base de données. Pour plus d'informations, voir "Configuration avancée de base de données (pour Configuration Manager)", page 32.

Mode Configuration de la base de données

Configuration Manager et UCMDB doivent utiliser différents schémas.

Configuration Manager permet à l'utilisateur de configurer chaque base de données sur un serveur de base de données Oracle ou MSSQL.

Types de configuration

Vous pouvez vous connecter à un schéma existant ou créer un nouveau schéma. La connexion à un schéma existant remplace son contenu.

Configuration de la base de données

Cette étape est exécutée automatiquement par le Gestionnaire de déploiement. Pour exécuter cette étape manuellement, voir "Configurer la base de données ou le schéma d'utilisateur", page 18.

Configuration avancée de base de données (pour Configuration Manager)

Une connexion à la base de données doit être configurée et associée à une connexion URL standard. Si plusieurs fonctions avancées sont requises, telles que Oracle Real Application Cluster, configurez une connexion standard et modifiez manuellement le fichier **database.properties** pour configurer ces fonctions.

Configuration Manager utilise des pilotes natifs pour les bases de données Oracle et Microsoft SQL Server. Toutes les fonctions natives de pilote sont prises en charge, à condition qu'elles puissent être configurées à l'aide de l'URL de base de données. L'URL se trouve dans le fichier **database.properties**.

Lorsque l'exécution de l'assistant du Gestionnaire de déploiement est terminée, d'autres configurations de base de données et de schéma peuvent être exécutées.

Champs de configuration de base de données

Deux types de base de données disponibles – Oracle et MSSQL. Les champs de saisie changent selon le type de base de données sélectionné.

10 Spécifiez les ports de connexion Configuration Manager sur la page Configuration du port. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Configuration utilisateur.

Configuration Manager fournit les paramètres de port par défaut prêts à l'emploi qui apparaissent dans les champs de saisie de la page de l'assistant Configuration du port.

Si un numéro de port est en conflit avec une installation existante, consultez un responsable informatique avant de modifier le numéro de port.

Champ	Définition
Application HTTP Port	8180
Port HTTP JMX	39900
Port Tomcat	8005
Port AJP	8009 (protocole Apache Java)
Port HTTPS de l'application	8143
Port distant JMX	39600

Cliquez sur le bouton **Revert to Default Values** pour restaurer les valeurs par défaut des ports fournies par le Gestionnaire de déploiement.

11 Créez les utilisateurs suivants dans la page Configuration des utilisateurs :

- Instance utilisateur de connexion initiale UCMDB-CM disposant d'autorisations d'administrateur.
- Utilisateur d'intégration dans UCMDB - Un utilisateur d'intégration est créé à la demande dans UCMDB par Configuration Manager pour prendre en charge l'intégration entre ces deux produits.

Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Configuration de la sécurité.

12 Activez Global LW-SSO sur une nouvelle instance d'UCMDB et Configuration Manager dans la page Configuration de la sécurité. LW-SSO est configuré uniquement dans les nouvelles instances de Configuration Manager ou UCMBD, selon la sélection effectuée dans la page Sélection de produit. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Récapitulatif.

LW-SSO est une infrastructure modulaire utilisée pour valider différents types d'authentification et de jetons de sécurité (tels que LW-SSO et SAML2). LW-SSO est utilisé pour faire le pont et tirer parti des informations authentifiées dans différents environnements dans les contextes de sécurité d'application d'une application ou d'une infrastructure de sécurité.

La configuration LW-SSO diffère selon les composants des produits sélectionnés.

Lors de la connexion de Configuration Manager à une instance UCMDB ou OO existante, LW-SSO est configuré dans Configuration Manager uniquement. Vous devez extraire la chaîne LW-SSO d'UCMDB ou OO et entrer cette chaîne dans le champ de saisie Chaîne LW-SSO. Lors de la connexion à UCMDB et OO, vérifiez que les chaînes LW-SSO définies dans les instances UCMDB et OO correspondent.

Lors de la connexion d'une nouvelle instance de Configuration Manager à une instance existante d'UCMDB, utilisez le nom de domaine complet (FQDN) comme nom d'hôte UCMDB.

Pour extraire la chaîne LW-SSO d'UCMDB :

a Ouvrez UCMDB et sélectionnez **Administration** > **Gestionnaire des paramètres d'infrastructure**.

b Dans la colonne **Nom**, sélectionnez et double-cliquez sur le champ Chaîne d'initialisation de LW-SSO.

c Copiez la chaîne du champ de saisie Valeur actuelle.

d Insérez la valeur dans le champ de saisie de la chaîne LW-SSO de la page Configuration de la sécurité.

Lors de la connexion de Configuration Manager à une nouvelle instance UCMDB, LW-SSO est configuré automatiquement dans UCMDB et Configuration Manager.

13 Vérifiez les paramètres d'installation et de configuration de la page Récapitulatif. Lorsque vous avez terminé, cliquez sur **Suivant** pour passer à la page Validation.

Cette page centralise tous les détails de la configuration et l'entrée utilisateur. Vous pouvez vérifier le contenu du récapitulatif, si nécessaire, en cliquant sur le bouton Retour des pages jusqu'à ce que vous atteigniez la page souhaitée, et définir les paramètres de déploiement. Revenez à la page Récapitulatif en cliquant sur **Suivant** comme indiqué.

14 Le Gestionnaire de déploiement exécute une série d'actions qui vérifie que les ressources système des ordinateurs distants sont suffisantes, que l'entrée utilisateur est correcte et qui valide les paramètres de configuration de la base de données. Ces validations indiquent si les paramètres des définitions utilisateur sont conformes aux limitations environnementales connues. La procédure de validation commence automatiquement, ou si vous avez réaffiché une page précédente du Gestionnaire de déploiement et modifié la configuration, cliquez sur **Exécuter la validation** pour lancer la procédure de validation. Lorsque vous avez terminé, cliquez sur **Déployer** pour passer à la page Déploiement.

15 Cette page reflète l'état de progression de la procédure de déploiement. Celle-ci inclut des installations de produits, les procédures de démarrage et leurs intégrations et connexions à d'autres produits.

La procédure de déploiement est terminée lorsque tous les produits ont été démarrés avec succès.

Cliquez sur **Détails** pour afficher les détails de la progression du déploiement, notamment les étapes effectuées par le Gestionnaire de déploiement pour le déploiement de chaque produit sélectionné.

Cliquez sur **Annuler** pour annuler le déploiement, en autorisant la fin de l'action de déploiement en cours avant l'arrêt du déploiement.

Cliquez sur **Abandonner** (accessible uniquement après avoir cliqué sur **Annuler**) pour forcer la fin de l'action en cours et le déploiement. L'abandon du déploiement peut être à l'origine de l'état Indéterminé des produits.

Validations

Le tableau ci-dessous contient une liste des validations réalisées par le Gestionnaire de déploiement.

Validation	Message d'erreur	Description
Vérifier les informations d'identification	Credentials verification failed	Les informations d'identification utilisateur fournies sont incorrectes.
		La connexion ne peut pas être établie.
Vérifier la compatibilité du système d'exploitation	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	Le système d'exploitation cible actuel ne correspond pas à la liste des systèmes d'exploitation certifiés pour le produit.
Vérifier la mémoire	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	La mémoire est insuffisante sur l'ordinateur cible pour tous les produits affectés
	<Memory> MB of memory are verified to be available on <Target Machine>	La validation a réussi.
Vérifier l'espace disque	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	L'espace disque est insuffisant sur l'ordinateur cible pour tous les produits affectés.
	<Memory> MB of disk space are verified to be available on drive <Target>	La validation a réussi.

Validation	Message d'erreur	Description
Vérifier que toutes les propriétés obligatoires ont été fournies	Missing the target storage device for the product: <Target>	Le répertoire d'installation du produit n'est pas défini.
Vérifier qu'un ordinateur de déploiement est défini	No deployment machine is defined for <Product Name>	Le produit n'est pas configuré pour être déployé sur un ordinateur.
Vérifier les informations d'identification	Credentials verification failed	Informations d'identification incorrectes.
Vérifier que l'UAC est désactivé	The UAC is enabled	Le contrôle de compte d'utilisateur (UAC) sur l'ordinateur cible.
Vérifier les ports libres	The required port number <Port> is already in use on <Target>	Le port requis de l'ordinateur cible est déjà utilisé.
Vérifier que le périphérique de stockage cible existe	The target storage device <Device> does not exist on <Target>	Le périphérique de stockage cible sélectionné n'existe pas sur l'ordinateur cible.
Valider l'existence du schéma	Schema <Name> does not exist/ already exist	Le schéma de l'ordinateur cible existe/n'existe pas.
Valider l'existence de l'autorisation du schéma	Validate <Permissions> schema tables user permissions existence	L'utilisateur DB ne dispose pas de suffisamment d'autorisations
Valider l'existence des tables de schéma	Schema Tables <Tables> on the database: <Tables> existent déjà	Les tables de schéma de la base de données existent déjà.
Valider l'existence des autorisations utilisateur Tables de schéma	The database user does not have the correct permissions	L'utilisateur de la base de données ne dispose pas des autorisations appropriées.

Validation	Message d'erreur	Description
Vérifier la connexion UCMDB	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	Échec de la connexion de test à UCMDB avec les paramètres de connexion indiqués.
	Existing UCMDB version must be 9.03 with CUP 2 or later.	La version UCMDB doit être 9.03 avec CUP 2 ou supérieur.
Vérifier la connexion DB	The host name/IP address validation failed	L'adresse IP/le nom d'hôte spécifiés de la base de données sont inaccessibles
	The username or password validation failed	Les informations d'identification utilisateur spécifiées sont incorrectes.
	The port validation failed	Le port de base de données spécifié est inaccessible.
	The SID validation failed	Le SID de la base de données n'existe pas dans la base de données.
Vérification de l'installation	The product is already installed	Le produit est déjà installé sur l'hôte cible

Mise à niveau de Configuration Manager

La procédure de mise à jour commence par effectuer automatiquement les vérifications et les validations suivantes :

- la connexion au serveur UCMDB fonctionne correctement.
- le correctif CUP 2 a été installé pour UCMDB.
- le port JMX est correct.

Si l'un de ces éléments n'a pas été installé ou configuré correctement, vous obtiendrez un message d'erreur pour vous en informer. Vous pouvez corriger le problème et effectuer ensuite la mise à niveau.

- Si la mise à niveau échoue parce que vous ne pouvez pas vous connecter à UCMDB, vérifiez que le serveur UCMDB est configuré et qu'il fonctionne.
- Si la mise à niveau échoue en raison de la non installation du correctif, installez CUP 2 en suivant les instructions du site Web : http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- Si la mise à niveau échoue en raison d'un port UCMDB JMX incorrect, sélectionnez le port JMX correct. Pour ce faire, modifiez la propriété ucmdb.jmx.port du fichier **upgrade.properties**, situé dans le **<répertoire d'installation de Configuration Manager >\utilities\Upgrade**.

Pour effectuer la mise à niveau, procédez comme suit :

Remarque : Vérifiez que le serveur UCMDB fonctionne lorsque vous lancez la procédure de mise à niveau.

---

1. Sauvegardez vos schémas Configuration Manager et UCMDB.
2. Localisez le fichier **setup-win64.msi** situé dans le sous-dossier Windows du support d'installation de Configuration Manager.
3. Double-cliquez sur le fichier pour exécuter l'assistant d'installation de Configuration Manager.

4. Cliquez sur **Suivant** pour ouvrir la page Contrat de Licence Utilisateur Final.
5. Acceptez les termes de la licence et cliquez sur **Suivant** pour ouvrir la page Informations client.
6. Entrez vos informations et cliquez sur **Suivant** pour ouvrir la page Type d'installation.
7. Sélectionnez le dossier d'installation de Configuration Manager. Assurez-vous de sélectionner un emplacement différent de celui utilisé pour la version antérieure.

   Par défaut, Configuration Manager est installé dans le répertoire suivant : **c:\hp\cnc920**. Cliquez sur **Suivant** pour accepter l'emplacement par défaut ou cliquez sur **Parcourir** pour sélectionner un autre emplacement et cliquez sur **Suivant**.

   Remarque : Le nom du répertoire d'installation ne doit pas contenir d'espaces.

   ---

8. Cliquez sur **Suivant** pour confirmer et lancer l'installation.

   Lorsque l'assistant d'installation est terminé, l'assistant de Post-Installation de Configuration Manager démarre automatiquement.
9. Cliquez sur **Suivant** jusqu'à ce que vous soyez invité à effectuer une nouvelle installation de Configuration Manager ou une mise à niveau.
10. Sélectionnez **Mettre à niveau** et cliquez sur **Suivant**.
11. Lorsque l'installation est terminée, vérifiez le fichier **post_installation.log** (situé dans le **<répertoire d'installation de Configuration Manager /tmp/log**) pour vous assurer qu'elle s'est terminée sans erreurs.

    En cas d'erreur pendant la procédure de mise à niveau, un message s'affiche pour vous permettre de fermer l'assistant. Dans ce cas, contactez l'assistance HP.
12. Démarrez le service Configuration Manager.

Remarque : Après la mise à niveau, vous devez réexécuter la configuration SSL. Pour plus d'informations, voir "Sécurisation renforcée", page 89.

3

Installation de HP Universal CMDB Configuration Manager sur une plate forme Linux

Important : Veuillez lire les notes de mise à jour pour connaître les instructions d'installation actualisées.

Contenu de ce chapitre :

Configuration de la pré-installation

Cette section inclut les rubriques suivantes :

Conditions préalables

➤ Au moins 400 Mo d'espace disque libre

➤ Écran X d'affichage recommandé

Obtenir le fichier setup.bin

Le fichier d'installation de Linux (**setup.bin**) se trouve sur le support d'installation ou l'image ISO que vous pouvez télécharger à partir du site Web HP. Pour accéder à ce fichier, procédez comme suit :

➤ Montez un DVD sur votre ordinateur Linux :

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ Montez une image ISO comme un périphérique de traitement par blocs de bouclage :

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

➤ Copiez le fichier **setup.bin** dans un emplacement temporaire de votre ordinateur Linux.

Installer Configuration Manager

Cette tâche décrit l'installation de Configuration Manager sur votre serveur, et la configuration de la connexion à la base de données et l'intégration d'UCMDB.

Si vous disposez d'un écran X d'affichage, l'assistant de post-installation apparaît sur l'interface utilisateur ; sinon, les informations de l'assistant sont affichées en mode console.

Remarque : Les étapes de ce manuel sont décrites pour le mode console ; cependant des étapes équivalentes apparaissent si vous utilisez l'assistant de l'interface utilisateur.

Pour installer Configuration Manager :

1 Pour installer Configuration Manager à l'emplacement en cours, lancez la commande suivante :

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 Un Contrat de Licence Utilisateur Final s'affiche. Vous devez l'accepter. Faites défiler le contrat en cliquant sur la barre d'espace de manière répétitive jusqu'à ce que vous atteigniez la fin du contrat. Pour accepter et continuer l'installation, saisissez **Oui** et appuyez sur **Entrée**.

HP Universal CMDB Configuration Manager est installé dans l'emplacement en cours dans le sous-dossier **cnc**.

Page de bienvenue

```
<============================>
Welcome
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

Appuyez sur **Enter** pour passer à la page suivante.

Sélection du fournisseur de la base de données

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Appuyez sur **Entrée** pour sélectionner Oracle ou saisissez **2** et appuyez sur **Entrée** pour sélectionner Microsoft.

Nom d'hôte de la base de données

```
-------------
Set Hostname:
-------------
        Hostname: = "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Saisissez le nom d'hôte de votre base de données et appuyez sur **Entrée**. La valeur par défaut du nom d'hôte fourni est **localhost**.

Port de la base de données

```
---------
Set Port:
---------
        Port: = "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Le port par défaut d'Oracle est 1521 et le port par défaut de Microsoft est 1433. Si vous souhaitez utiliser un autre numéro de port, saisissez-le ici et appuyez sur **Entrée**.

Nom SID/DB

```
-----------
Set SID/DB:
-----------
        SID/DB: = "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pour Oracle, ce champ définit le SID de la base de données ; pour Microsoft, ce champ définit le nom de la base de données. Saisissez une valeur valide et appuyez sur **Entrée**.

Nom et mot de passe utilisateur/schéma

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Saisissez le nom d'utilisateur de la base de données et appuyez sur **Entrée**.

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Saisissez le mot de passe du schéma et appuyez sur **Entrée**.

Connexion à la base de données de test

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour tester la connexion à la base de données.

Étant donné que cet assistant tente de créer des tables dans le schéma de la base de données, il est vivement recommandé de tester la connexion à la base de données. Si vous ne souhaitez pas tester la connexion, saisissez **Non** et appuyez sur **Entrée**.

Lorsque le test de la connexion à la base de données a réussi, le message suivant s'affiche :

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour continuer. Si une erreur se produit lors du test de la connexion, un message d'erreur s'affiche. Vous serez invité à réexécuter le test. Corrigez le problème de connexion, testez à nouveau et continuez l'installation.

Nom d'hôte du serveur d'applications

```
<============================>
Application Server Configuration
<============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

La valeur par défaut du nom d'hôte est le nom d'hôte réel de l'ordinateur. Si vous effectuez l'installation derrière un équilibrage de charge ou un proxy inverse, saisissez le nom externe ici.

Personnaliser les ports du serveur d'applications

```
------------------
Select Customize ports
------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Si vous souhaitez utiliser les ports par défaut pour Configuration Manager, appuyez sur **Entrée**. Si vous souhaitez utiliser les ports personnalisés, saisissez **Oui** et appuyez sur **Entrée**. Les numéros de port par défaut sont :

Nom du port	Numéro de port
HTTP	8180
HTTPS	8443
Gestion Tomcat	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

Si vous choisissez de personnaliser les ports, pour chaque port répertorié ci-dessous il vous sera demandé de saisir une valeur. Saisissez la nouvelle valeur et appuyez sur **Entrée** pour chacun d'entre eux :

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Utilisateur administratif initial

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Un utilisateur administratif initial est créé pour être l'administrateur ou le super-utilisateur du système lors de la connexion initiale. Saisissez le nom d'utilisateur admin que vous souhaitez utiliser et appuyez sur **Entrée**.

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Saisissez le mot de passe de l'utilisateur admin et appuyez sur **Entrée**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pour confirmer, saisissez à nouveau le mot de passe de l'utilisateur admin et appuyez sur **Entrée**.

Utilisateur de l'intégration

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Sélectionnez le nom d'utilisateur d'intégration UCMDB. Cet utilisateur est créé dans UCMDB lors de la procédure de post-installation. HP recommande d'utiliser un nom d'utilisateur qui n'inspire aucun doute sur l'intégration (par exemple cm_integration). Saisissez le nom d'utilisateur sélectionné et appuyez sur **Entrée**.

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Saisissez le mot de passe de l'utilisateur de l'intégration et appuyez sur **Entrée**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pour confirmer, saisissez à nouveau le mot de passe de l'utilisateur de l'intégration et appuyez sur **Entrée**.

Nom d'hôte du serveur HP Universal CMDB

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname:
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Saisissez le nom d'hôte du serveur UCMDB et appuyez sur **Entrée**. Il sera probablement différent du localhost par défaut car il n'est pas recommandé d'installer UCMDB et Configuration Manager sur le même ordinateur dans un environnement de production.

Port du serveur HP Universal CMDB

```
Port:
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour accepter le numéro de port par défaut 8080 pour le serveur UCMDB ou saisissez un numéro de port et appuyez sur **Entrée**.

Protocole du serveur HP Universal CMDB

```
Protocol:
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour utiliser HTTP ou saisissez 2 et appuyez sur **Entrée** pour utiliser HTTPS.

Remarque : Si vous sélectionnez HTTPS, vous devez échanger les clés avec UCMDB. Pour plus d'informations, voir "Sécurisation renforcée", page 89. Cette procédure configure HTTPS à l'aide d'un certificat auto-signé non configuré.

Client du serveur HP Universal CMDB

```
Customer:
----
Set
----
         = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour accepter le nom du client par défaut pour le serveur UCMDB ou saisissez un nom de client et appuyez sur **Entrée**.

Informations d'identification Sysadmin du serveur HP Universal CMDB

```
Administrative username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Entrez le nom d'utilisateur sysadmin du serveur UCMDB . Il s'agit d'un utilisateur pouvant exécuter les méthodes JMX sur le serveur UCMDB. Cet utilisateur existe déjà. Il n'est pas créé pendant l'installation. Obtenez les informations d'identification pour l'utilisateur sysadmin auprès de l'administrateur du serveur UCMDB.

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Saisissez le mot de passe de l'utilisateur sysadmin du serveur UCMDB et appuyez sur **Entrée**.

Tester la connexion au serveur HP Universal CMDB

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour tester la connexion au serveur UCMDB. Étant donné que cet assistant tente de déployer les packages et configurer le serveur UCMDB , il est vivement recommandé de tester la connexion au serveur. Si vous ne souhaitez pas tester la connexion, saisissez **Non** et appuyez sur **Entrée**.

Lorsque le test de la connexion au serveur a réussi, le message suivant s'affiche :

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Appuyez sur **Entrée** pour continuer. Si une erreur se produit lors du test de la connexion, un message d'erreur s'affiche. Vous serez invité à réexécuter le test. Corrigez le problème de connexion, testez à nouveau et continuez l'installation.

Résumé

L'assistant affiche un résumé de toutes les sélections que vous avez effectuées avant de les exécuter réellement.

```
<============================>
Post Installation Actions Summary
<============================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username: admin
HP Universal CMDB Platform integration username: cm_integration

Base de données
--------
Vendor: Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password? Yes
Create schema objects? Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service? No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username: sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

Appuyez sur **Entrée** pour continuer la phase de configuration. Une barre de progression s'affiche lorsque la configuration est lancée. L'assistant exécute les tâches suivantes :

1. Créer les tables et les objets de base de données.
2. Compléter la base de données avec les valeurs par défaut et initiales.
3. Créer l'utilisateur administratif initial.
4. Créer l'utilisateur de l'intégration sur le serveur UCMDB.
5. Consolider le serveur UCMDB.
6. Créer l'état Autorisé sur le serveur UCMDB.
7. Déployer les packages de Configuration Manager sur le serveur UCMDB.

Lorsque la configuration est terminée, le message suivant s'affiche :

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

Appuyez sur **Entrée** pour quitter l'assistant.

Option d'installation en mode silencieux

Vous pouvez installer Configuration Manager en mode silencieux. Les fichiers sont extraits du package d'installation, mais aucune configuration de post-installation n'est effectuée. Pour effectuer l'installation en mode silencieux, exécutez la commande suivante :

```
$ /path/to/installation/kit/setup.bin -silent
```

Exécuter le serveur d'applications Configuration Manager

Pour exécuter Configuration Manager, lancez les commandes suivantes :

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

Vous pouvez créer un script dans le répertoire **/etc/init.d** pour lancer automatiquement Configuration Manager au démarrage de l'ordinateur.

4

Connexion à Configuration Manager

Contenu de ce chapitre :

Accès à Configuration Manager

Vous accédez à Configuration Manager à l'aide d'un navigateur Web pris en charge, à partir de n'importe quel ordinateur par le biais d'une connexion réseau (intranet ou Internet) sur le serveur Configuration Manager. Le niveau d'accès octroyé à l'utilisateur dépend de ses autorisations. Pour plus d'informations sur l'octroi d'autorisations utilisateur, consultez la section "Gestion des utilisateurs" du Manuel de l'utilisateur *HP Universal CMDB Configuration Manager*.

Pour plus d'informations sur la configuration du navigateur Web, et la configuration minimale requise pour afficher Configuration Manager, voir "Matrice de prise en charge", page 14.

Pour plus d'informations sur l'accès en toute sécurité à Configuration Manager, voir "Sécurisation renforcée", page 89.

Pour obtenir des informations sur la résolution des problèmes d'accès à Configuration Manager, voir "Résolution des problèmes", page 123.

Se connecter à Configuration Manager

1. Dans le navigateur Web, entrez l'URL du serveur Configuration Manager, par exemple, http://<nom du serveur ou adresse IP>.<nom de domaine>:<port>/cnc, où **<nom du serveur ou adresse IP>.<nom de domaine>** représente le nom de domaine complet (FQDN) du serveur Configuration Manager et **<port>** le port sélectionné au cours de l'installation.
2. Entrez le nom d'utilisateur et le mot de passe que vous avez définis dans l'Assistant Post-installation de Configuration Manager.
3. Cliquez sur **Connexion**. Une fois la connexion établie, le nom d'utilisateur s'affiche en haut à droite de l'écran.
4. (Recommandé) Connectez-vous au serveur LDAP organisationnel et attribuez des rôles administratifs aux utilisateurs LDAP pour que les administrateurs Configuration Manager puissent accéder au système. Pour plus d'informations sur l'attribution de rôles aux utilisateurs du système Configuration Manager, voir "Gestion des utilisateurs" dans le *Manuel de l'utilisateur HP Universal CMDB Configuration Manager*.

Se déconnecter

Lorsque vous avez terminé votre session, il est recommandé de vous déconnecter du site Web afin d'éviter toute entrée non autorisée.

Pour cela, cliquez sur **Déconnexion** en haut de la page.

Remarque : Le temps d'expiration par défaut d'une session est de 30 minutes.

Accès à la console JMX de Configuration Manager

Pour résoudre les problèmes ou modifier certaines configurations, il peut être nécessaire d'accéder à la console JMX.

Pour accéder à la console JMX :

1. Ouvrez la console JMX à l'adresse http://<nom de serveur ou adresse IP>:<port>/cnc/jmx-console. Il s'agit du port configuré au cours de l'installation de Configuration Manager.
2. Entrez les informations d'identification de l'utilisateur par défaut. Elles sont identiques à celles utilisées pour la connexion à Configuration Manager.

5

Autres cas d'utilisation

Contenu de ce chapitre :

Transférer une installation Configuration Manager entre des ordinateurs

Cette procédure doit être utilisée pour transférer une installation de Configuration Manager d'un ordinateur vers un autre tout en conservant intact le schéma de base de données et en se connectant au même serveur UCMDB.

1 Dans le **<répertoire d'installation de Configuration Manager >\cnc\bin**, exécutez la commande suivante : edit-server-0.bat.

2 Enregistrez tous les paramètres que vous identifiez, y compris les ports (par exemple, le port JMX).

3 Arrêtez le serveur Configuration Manager sur l'ordinateur source. (Si l'ordinateur source est installé sur un système Windows, faites-le en arrêtant le service Configuration Manager).

4 Installez Configuration Manager sur l'ordinateur cible :

- ➤ Sous Windows : exécutez le fichier **setup-win64.msi** (situé dans le dossier **windows** du support d'installation).
- ➤ Sous Linux : suivez les instructions de la section "Installer Configuration Manager", page 44.

5 Annulez l'Assistant de post-installation lorsqu'il démarre.

6 Copiez tous les fichiers du répertoire d'installation précédent sur l'ordinateur source à l'emplacement de la nouvelle installation sur l'ordinateur cible.

7 Sur l'ordinateur cible, remplacez le nom d'hôte par le nom de l'ordinateur cible dans **client-config.properties** et **resources.properties** (situés dans le dossier **conf**).

Remarque : Si l'ordinateur cible se trouve dans un autre domaine de l'ordinateur source, modifiez l'ancienne référence du domaine dans le fichier **lwssofmconf.xml**.

---

8 Sur l'ordinateur cible, exécutez le fichier **bin/create-windows-service.bat** pour créer le service Windows. Définissez l'indicateur **-h** pour afficher les options disponibles et utiliser les paramètres enregistrés du service de l'ordinateur source (que vous avez enregistré à l'étape 2) comme indiqué. Pour le paramètre du nom de domaine, utilisez server-0. La commande se présente comme suit lorsque les valeurs par défaut sont utilisées :

c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 Démarrez le serveur Configuration Manager sur l'ordinateur cible.

Modifier les numéros de ports après l'installation

1. Arrêtez le serveur Configuration Manager.
2. Sauvegardez le contenu du **<répertoire d'installation de Configuration Manager >\servers\server-0**.
3. Supprimez le **<répertoire d'installation de Configuration Manager >\servers\server-0**.
4. Exécutez le script **create-node.bat** à l'aide de l'indicateur **-h** pour afficher les options disponibles. Transférez tous les numéros de port requis à l'utilitaire.
5. Sur l'ordinateur cible, remplacez le port par le nouveau numéro de port HTTP dans **client-config.properties** et **resources.properties** (situés dans le dossier **\conf**).
6. Exécutez le script **edit-server-0.bat**, situé dans le **<répertoire d'installation de Configuration Manager >\bin**.
7. (Pour les systèmes Windows) Dans la fenêtre Propriétés HP Universal CMDB Configuration Manager affichée, cliquez sur l'onglet Java et remplacez les paramètres **jmx.http.port** et **com.sun.management.jmxremote.port** par vos nouveaux numéros de port.
8. Démarrez le service Configuration Manager sur l'ordinateur cible.

Copier des paramètres système entre des systèmes

1 Sur l'ordinateur source, ouvrez Configuration Manager. Sélectionnez **Système** > **Paramètres** et cliquez sur le bouton **Exporter le jeu de configurations vers un fichier ZIP**.

   Avant d'exporter, vous pouvez exclure des portions spécifiques de la configuration en désélectionnant la case à cocher en regard des éléments de configuration concernés.

2 Copiez la configuration exportée sur l'ordinateur cible.

3 Sur l'ordinateur cible, ouvrez Configuration Manager. Sélectionnez **Système** > **Paramètres** et cliquez sur le bouton **Importer un jeu de configurations**.

Sauvegarde et restauration

Vous pouvez sauvegarder une installation de Configuration Manager pour effectuer une récupération à l'issue de n'importe quel type d'échec qui nécessiterait une nouvelle installation complète.

Sauvegarder

Sauvegardez les informations suivantes :

- les sous-dossiers **conf** et **security** du répertoire d'installation de Configuration Manager. Peut être réalisé pendant le fonctionnement du système, sans l'interrompre.
- le schéma de la base de données.

Restaurer (sur un système Windows)

Cette procédure doit être exécutée sur un nouveau système sur lequel Configuration Manager n'est pas installé.

1 Installez Configuration Manager sur l'ordinateur cible en exécutant le fichier **setup-win64.msi** (situé dans le dossier **windows** du support d'installation) en mode silencieux comme suit :

```
msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive
```

2 Restaurez les répertoires **conf** et **security**. Utilisez la méthode de correspondance pour restaurer ce que vous avez sauvegardé. Remplacez les répertoires créés par l'installation effectuée à l'étape 1.

3 Restaurez le schéma de la base de données. Si vous restaurez sur un autre serveur de base de données, vous devez modifier la propriété **url** dans le fichier **database.properties** (situé dans le répertoire **conf**) pour qu'elle corresponde au nouveau nom du serveur de base de données.

4 Utilisez l'utilitaire **create-windows-service** (avec l'indicateur **-h** pour afficher les options disponibles) pour créer un service Windows.

5 Démarrez le serveur Configuration Manager.

Restaurer (sur un système Linux)

1 Installez Configuration Manager sur l'ordinateur cible en exécutant le fichier **setup.bin** (situé sur le support d'installation). Pour plus d'informations, voir "Installer Configuration Manager", page 44. Vous devez annuler l'installation effectuée à la première étape de l'assistant de post-installation. Tous les fichiers seront déployés, mais votre système ne sera pas configuré.

2 Restaurez les répertoires **conf** et **security**. Utilisez la méthode de correspondance pour restaurer ce que vous avez sauvegardé. Remplacez les répertoires créés par l'installation effectuée à l'étape 1.

3 Restaurez le schéma de la base de données. Si vous restaurez sur un autre serveur de base de données, vous devez modifier la propriété **url** dans le fichier **database.properties** (situé dans le répertoire **conf**) pour qu'elle corresponde au nouveau nom du serveur de base de données.

4 Démarrez le serveur Configuration Manager.

6

Configuration avancée

Contenu de ce chapitre :

Options avancées de connexion à la base de données

Si vous souhaitez utiliser plus de propriétés avancées de connexion à la base de données pour prendre en charge le déploiement de votre base de données, vous pouvez le faire après l'exécution de l'assistant Post-installation. Configuration Manager prend en charge toutes les options de connexion à la base de données reconnues par le pilote JDBC du fournisseur. Elles peuvent être configurées à l'aide de l'URL de connexion à la base de données. Pour configurer d'autres connexions avancées, modifiez la propriété **jdbc.url** dans le **<répertoire d'installation de Configuration Manager >\conf\database.properties**.

Remarque : Lors de la configuration avancée sur un système Linux, procédez comme suit :

- Dans les instructions, remplacez le sens des barres obliques par (/).
- Remplacez **.bat** par **.sh** dans les exécutions du script.

Voici des exemples d'options plus avancées Microsoft SQL Server :

- **Authentification Windows (NTLM).** Pour appliquer une authentification Windows, ajoutez la propriété du domaine à l'URL de connexion de votre JTDS dans le fichier database.properties. Spécifiez le domaine Windows à authentifier.

  Par exemple :

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode
  =false;domain=myDomain
  ```

- **SSL.** Pour plus d'informations sur la sécurisation de la connexion MS SQL Server à l'aide de SSL, visitez le site http://jtds.sourceforge.net/faq.html.

Voici des exemples d'options plus avancées pour Oracle Database Server :

- **URL Oracle.** Spécifiez l'URL de connexion du pilote natif Oracle. Spécifiez un nom de serveur Oracle et un SID valides. Si vous utilisez **Oracle RAC**, vous pouvez également spécifier les détails de la configuration Oracle RAC.

  Remarque : Pour plus d'informations sur la configuration du format de l'URL JDBC Oracle native, visitez le site http://www.orafaq.com/wiki/JDBC#Thin_driver. Pour plus d'informations sur la configuration de l'URL pour Oracle RAC, visitez le site http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Pour plus d'informations sur la sécurisation de la connexion Oracle à l'aide de SSL, visitez les sites suivants :
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Configuration de la base de données - Prise en charge de MLU (Multi-Lingual Unit)

Cette section décrit les paramètres de base de données requis pour la localisation du support.

Paramètres Oracle Server

Les paramètres Oracle Server sont répertoriés dans le tableau ci-dessous :

Option	Pris en charge	Recommandé	Remarques
Jeu de caractères	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Paramètres Microsoft SQL Server

Les paramètres Microsoft SQL Server sont répertoriés dans le tableau ci-dessous :

Option	Pris en charge	Recommandé	Remarques
Collation (Classement)	Non-respect de la casse. HP Universal CMDB ne prend pas en charge l'ordre de tri binaire ni le respect de la casse. Seul l'ordre de non-respect de la casse avec une combinaison d'accent, kana ou paramètres de largeur est pris en charge.	Utilisez la boîte de dialogue Collation Settings (Paramètres de classement) pour sélectionner le classement. Ne cochez pas la case Binary (Binaire). La sensibilité à l'accent, kana et largeur doit être sélectionnée en fonction des besoins de la langue des données appropriée. La langue sélectionnée doit être identique à celle des paramètres régionaux du système d'exploitation Windows.	Limité aux définitions de paramètres régionaux Collation et English par défaut
Collation Database Property (Propriété de la base de données de classement)	Valeur par défaut Server (Serveur)		

Remarque :

Pour toutes les langues : **<Langue>_CI_AS** est l'option minimum requise. Par exemple, en japonais, si vous souhaitez sélectionner la sensibilité Kana et les options de sensibilité à la largeur, l'option recommandée est la suivante : **Japanese_CI_AS_KS_WS** ou **Japanese_90_CI_AS_KS_WS**. Cette recommandation indique que les caractères japonais sont sensibles à l'accent, à Kana et à la largeur.

- **Sensibilité à l'accent (_AS).** Distinction entre les caractères accentués et non accentués. Par exemple, **a** est différent de **á**. Si cette option n'est pas sélectionnée, Microsoft SQL Server considère les versions des lettres accentuées et non accentuées comme identiques pour le tri.
- **Sensibilité Kana (_KS).** Distinction entre les deux types de caractères Kana japonais : Hiragana et Katakana. Si cette option n'est pas sélectionnée, Microsoft SQL Server considère les caractères Hiragana et Katakana comme identiques pour le tri.
- **Sensibilité à la largeur (_WS).** Distinction entre un caractère codé sur un octet et le même caractère représenté sous la forme d'un caractère codé sur deux octets. Si cette option n'est pas sélectionnée, Microsoft SQL Server considère les caractères codés sur un octet et sur deux octets comme identiques pour le tri.

SSO (Single Sign-On)

La connexion unique entre Configuration Manager et UCMDB est réalisée à l'aide de la technologie LWSSO de HP. Pour plus d'informations, voir "LW-SSO (Lightweight Single Sign-On Authentication) – Références générales", page 119.

Cette section inclut les rubriques suivantes :

Activer LW-SSO entre Configuration Manager et UCMDB

Certains utilisateurs de Configuration Manager sont également autorisés à se connecter à UCMDB. Pour plus de facilité, Configuration Manager fournit un lien direct à l'interface utilisateur UCMDB (sélectionnez **Administration** > **UCMDB Foundation**). Pour utiliser la connexion unique (qui exclut le besoin de se connecter à UCMDB après la connexion à Configuration Manager), vous devez activer LW-SSO pour Configuration Manager et UCMDB et vérifier qu'ils utilisent la même initString. Cette tâche doit être exécutée manuellement sauf si elle a déjà été réalisée dans le cadre de l'installation du Gestionnaire de déploiement.

Pour activer LW-SSO :

1. Dans le répertoire d'installation de Configuration Manager, modifiez le fichier **\conf\lwssofmconf.xml**.
2. Localisez la section suivante :

   enableLWSSO enableLWSSOFramework="true"

   et vérifiez que la valeur est **true**.
3. Localisez la section suivante :

   lwssoValidation id="ID000001">
   <domaine> </domain>

   et entrez le domaine du serveur Configuration Manager après **<domaine>**.

4 Localisez la section suivante :

<initString="Cette chaîne doit être remplacée"></crypto>

et remplacez "Cette chaîne doit être remplacée" par une chaîne partagée utilisée par toutes les applications approuvées s'intégrant dans LW-SSO.

5 Localisez la section suivante :

<!--multiDomain>
<trustedHosts>
<DNSDomain>Cette valeur doit être remplacée par votre domaine d'application</DNSDomain>
<DNSDomain>Cette valeur doit être remplacée par un domaine d'une autre application</DNSDomain>
</trustedHosts>
</multiDomain-->

Remarque : Le second DNSDomain doit être inclus uniquement si Configuration Manager et une autre application se trouvent dans différents domaines.

Supprimez le caractère de commentaire situé au début et entrez tous les domaines de serveur (si nécessaire) dans les éléments DNSDomain (à la place de Cette valeur doit être remplacée par votre domaine d'application ou Cette valeur doit être remplacée par le domaine de l'autre application. La liste doit contenir le domaine de serveur entré à l'étape 3 à la page 74.

6 Enregistrez le fichier modifié et redémarrez le serveur.

7 Lancez un navigateur Web et entrez l'adresse suivante : http://<adresse du serveur UCMDB>.<nom_domaine>:8080/jmx-console.

Entrez les informations d'identification pour l'authentification de la console JMX, qui sont par défaut :

- Nom de connexion = **sysadmin**
- Mot de passe = **sysadmin**

8. Sous **UCMDB-UI**, sélectionnez **Configuration LW-SSO** pour ouvrir la page Vue JMX MBEAN.
9. Sélectionnez la méthode **setEnabledForUI**, définissez la valeur sur **true** et cliquez sur **Appeler**.
10. Sélectionnez la méthode **setDomain**. Entrez le nom de domaine du serveur UCMDB et cliquez sur **Appeler**.
11. Sélectionnez la méthode **setInitString**. Entrez la même initString que vous avez entrée pour Configuration Manager à l'étape 4 à la page 75 et cliquez sur **Appeler**.
12. Si Configuration Manager et UCMDB se trouvent dans des domaines distincts, sélectionnez la méthode **addTrustedDomains** et entrez les noms de domaine des serveurs UCMDB et Configuration Manager. Cliquez sur **Appeler**.
13. Pour afficher la configuration LW-SSO telle qu'elle a été sauvegardée dans le mécanisme des paramètres, sélectionnez la méthode **retrieveConfigurationFromSettings** et cliquez sur **Appeler**.
14. Pour afficher la configuration actuelle LW-SSO chargée, sélectionnez la méthode **retrieveConfiguration** et cliquez sur **Appeler**.

Configurer LW-SSO dans Operations Orchestration

Si LW-SSO est activé dans Configuration Manager et Operations Orchestration (OO), les utilisateurs connectés à Configuration Manager sont autorisés à se connecter à Operations Orchestration par le biais du niveau Web sans indiquer un nom d'utilisateur et un mot de passe (administrateurs système).

Remarque :

- Dans la procédure suivante, <OO_HOME> représente le répertoire de base d'Operations Orchestration.
- LW-SSO exige que les comptes utilisés pour la connexion à Operations Orchestration et Configuration Manager aient le même nom de compte (mais ils peuvent comporter des mots de passe différents).
- LW-SSO exige que le compte d'Operations Orchestration ne soit pas interne.

Pour configurer LW-SSO dans Operations Orchestration :

1. Arrêtez le service RSCentral.
2. Dans <**OO_HOME**>**Central****WEB-INF****applicationContext.xml**, activez l'importation entre LWSSO_SECTION_BEGIN et LWSSO_SECTION_END comme indiqué ci-dessous :

```
<!--  LWSSO_SECTION_BEGIN-->
      <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3. Dans <**OO_HOME**>**Central****WEB-INF****web.xml**, activez tous les filtres et les mappages entre LWSSO_SECTION_BEGIN et LWSSO_SECTION_END comme indiqué ci-dessous :

```
<!--  LWSSO_SECTION_BEGIN-->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
```

```
            </filter-class>
            <init-param>
                <param-name>targetBean</param-name>
                <param-value>dharma.LWSSOFilter</param-value>
            </init-param>
        .....
        </filter>
    <!--  LWSSO_SECTION_END -->

    <!--  LWSSO_SECTION_BEGIN-->
        <filter-mapping>
            <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
        </filter-mapping>
    <!--  LWSSO_SECTION_END -->

    <!--  LWSSO_SECTION_BEGIN-->
        <filter-mapping>
            <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
        </filter-mapping>
        <filter-mapping>
            <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
        pattern>/*</url-pattern>
            </filter-mapping>
    <!--  LWSSO_SECTION_END -->
```

4 Dans <**OO_HOME**>**Central****conf****lwssofmconf.xml**, modifiez les deux paramètres suivants :

- domain : nom de domaine du serveur OO.
- initString : doit être identique à la valeur initString dans la configuration OO LW-SSO (longueur minimum : 12 caractères). Par exemple, smintegrationlwsso.

Par exemple :

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 Redémarrez le service RSCentral pour que la configuration soit prise en compte.

Exécuter l'authentification du Gestionnaire des identités

Cette tâche décrit comment configurer HP Universal CMDB Configuration Manager pour accepter l'authentification du Gestionnaire des identités.

Si vous utilisez le Gestionnaire des identités et si vous prévoyez d'ajouter HP Universal CMDB Configuration Manager, vous devez exécuter cette tâche.

Cette tâche inclut les étapes suivantes :

➤ "Conditions préalables", page 80

➤ "Configurer HP Universal CMDB Configuration Manager pour accepter le Gestionnaire des identités", page 80

Conditions préalables

Le serveur Tomcat Configuration Manager doit être connecté à votre serveur Web (IIS ou Apache) protégé par votre Gestionnaire des identités à l'aide d'un connecteur Tomcat Java (AJP13).

Pour les instructions d'utilisation d'un connecteur Tomcat Java (AJP13), voir la documentation Tomcat Java (AJP13).

Configurer HP Universal CMDB Configuration Manager pour accepter le Gestionnaire des identités

Pour configurer Tomcat Java (AJP13) à l'aide d'IIS6 :

1. Configurez le Gestionnaire des identités pour envoyer un en-tête / rappel de personnalisation contenant le nom de l'utilisateur, et demander le nom de l'en-tête.
2. Ouvrez le **<répertoire d'installation de Configuration Manager >\conf \lwssofmconf.xml** et localisez la section commençant par **in-ui-identity-management**.

   Par exemple :

   ```
   <in-ui-identity-management enabled="false">
     <identity-management>
    <userNameHeaderName>sm-user</userNameHeaderName>
     </identity-management>
   </in-ui-identity-management>
   ```

   a. Activez la fonctionnalité en supprimant le caractère de commentaire.

   b. Remplacez **enabled**="**false**" par **enabled**="**true**".

   c. Remplacez **sm-user** par le nom d'en-tête que vous avez demandé à l'étape 1.
3. Ouvrez le **<répertoire d'installation de Configuration Manager >\conf\client-config.properties** et modifiez les propriétés suivantes :

   a. Modifiez **bsf.server.url** selon l'URL du Gestionnaire des identités et modifiez le port selon le port du Gestionnaire des identités :

   bsf.server.url=http://< URL du Gestionnaire des identités>:< Port du Gestionnaire des identités>/bsf

b Modifiez **bsf.server.services.url** selon le protocole HTTP et modifiez le port selon le port original Configuration Manager :

bsf.server.services.url=http://<URL Configuration Manager> :
<Port Configuration Manager >/bsf

Exemple d'utilisation du connecteur Java pour configurer le Gestionnaire des identités pour Configuration Manager à l'aide d'IIS6 sur un système d'exploitation Windows 2003

Cette tâche de l'exemple décrit comment installer et configurer le connecteur Java permettant de configurer le Gestionnaire des identités pour l'utiliser avec Configuration Manager à l'aide d'IIS6 fonctionnant sur un système d'exploitation Windows 2003.

Pour installer le connecteur Java et le configurer pour IIS6 sous Windows 2003 :

1 Téléchargez la dernière version du connecteur Java (par exemple, **djk-1.2.21**) à partir du site Web Apache.

a Cliquez sur http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/.

b Sélectionnez la dernière version.

c Téléchargez le fichier **isapi_redirect.dll** à partir du répertoire **amd64**.

2 Enregistrez le fichier dans le **<répertoire d'installation de Configuration Manager>\tomcat\bin\win32**.

3 Créez un nouveau fichier texte appelé **isapi_redirect.properties** dans le même répertoire contenant isapi_redirect.dll.

Le contenu de ce fichier est le suivant :

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=<répertoire d'installation de Configuration Manager >\servers
\server-0\logs\isapi.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Full path to the workers.properties file
worker_file==<répertoire d'installation de Configuration Manager >\tomcat
\conf\workers.properties.minimal
# Full path to the uriworkermap.properties file
worker_mount_file==<répertoire d'installation de Configuration Manager >\tomcat
\conf\uriworkermap.properties
```

4 Créez un nouveau fichier texte appelé **workers.properties.minimal** dans le **<répertoire d'installation de Configuration Manager >\tomcat\conf**.

Le contenu de ce fichier est le suivant :

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
        worker.list=ajp13w
        worker.ajp13w.type=ajp13
        worker.ajp13w.host=localhost
        worker.ajp13w.port=8009
#END
```

5 Créez un nouveau fichier texte appelé **uriworkermap.properties** dans le **<répertoire d'installation de Configuration Manager >\tomcat\conf**.

Le contenu de ce fichier est le suivant :

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Important : Notez que Configuration Manager doit comporter deux règles. La nouvelle syntaxe leur permet de constituer une seule règle, telle que :

/cnc|/*=ajp13w

---

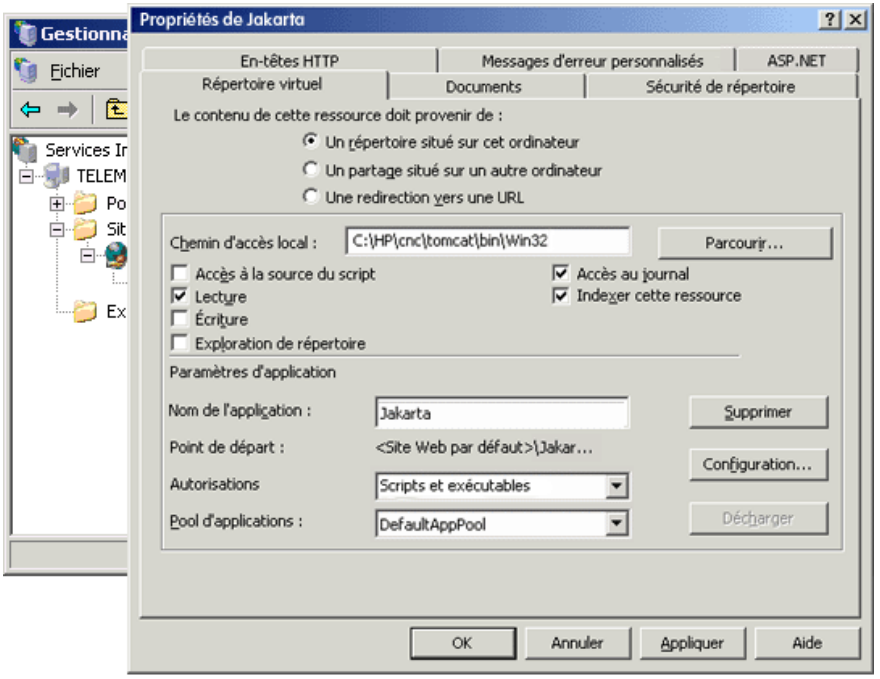
6 Créez le répertoire virtuel dans l'objet Site Web correspondant de la configuration IIS.

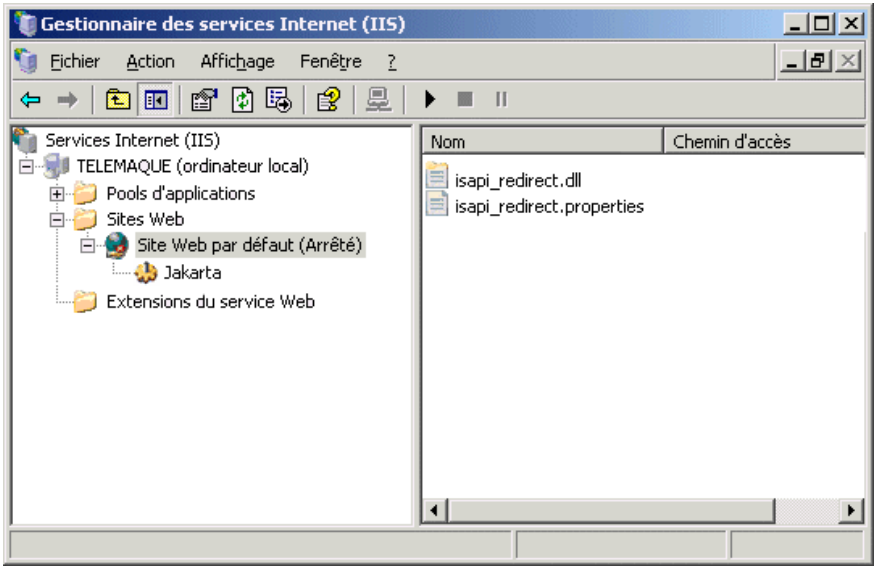
a Dans le menu Démarrer de Windows, sélectionnez **Paramètres** > **Panneau de configuration** > **Outils d'administration** >**Gestionnaire Internet Information Services (IIS)**.

b Dans le volet de droite, cliquez avec le bouton droit sur le **<nom de l'ordinateur local>\Sites Web\<Le nom de votre site Web>** et sélectionnez **Nouveau\Répertoire virtuel**.

c Attribuez au répertoire le nom d'alias **Jakarta**, et définissez le chemin local jusqu'au répertoire contenant isapi_redirect.dll.

La fenêtre du Gestionnaire ressemble à la suivante :





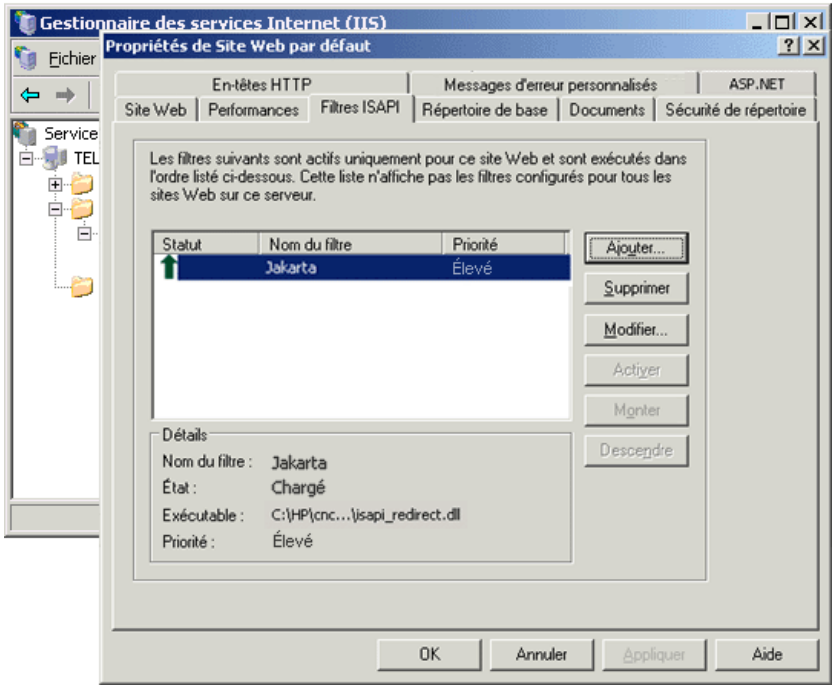
7 Ajoutez **isapi_redirect.dll** comme filtre ISAPI.

a Cliquez avec le bouton droit sur le **<nom de votre site Web>** et sélectionnez **Propriétés**.

b Sélectionnez l'onglet **Filtres ISAPI**, et cliquez sur le bouton **Ajouter…**.

c Sélectionnez le nom du filtre **Jakarta**, et parcourez jusqu'à **isapi_redirect.dll**. Le filtre est ajouté, mais il n'est pas activé.

La fenêtre de configuration ressemble à la suivante :



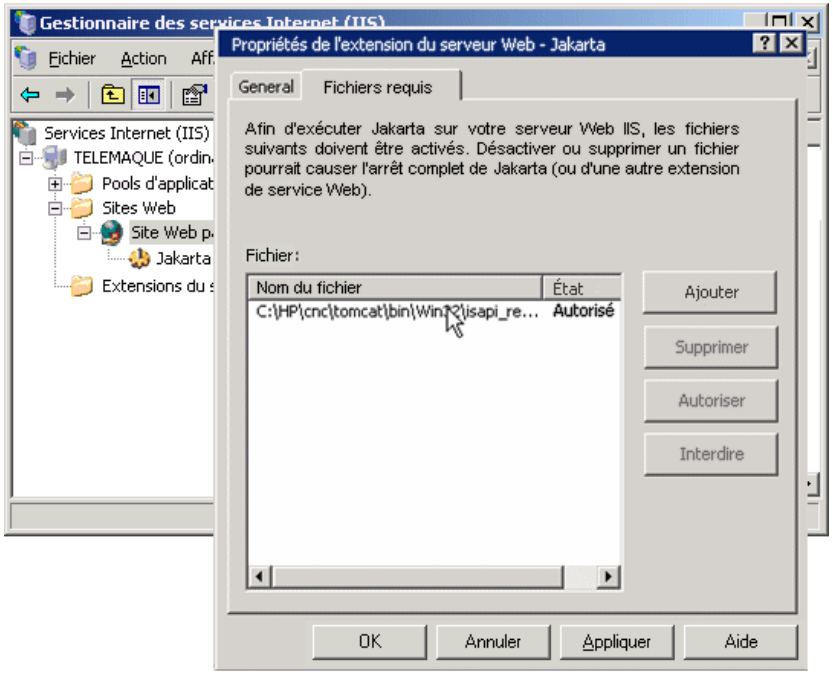
d Cliquez sur le bouton **Appliquer**.

8 Définissez et autorisez la nouvelle extension du service Web.

a Cliquez avec le bouton droit sur l'entrée **<nom de l'ordinateur local >\\Extensions du service Web** et sélectionnez l'option de menu **Ajouter une nouvelle extension du service Web…**.

b Attribuez le nom **Jakarta** à la nouvelle extension du service Web, et parcourez jusqu'au fichier **isapi_redirect.dll**.

Remarque : Avant de cliquer sur le bouton **OK**, cochez la case **Définir l'état de l'extension à Autorisée**.



9 Redémarrez le serveur Web IIS, et accédez à l'application par le biais du service Web.

Prise en charge IPv6

Configuration Manager prend en charge les URL IPv6 pour les URL client uniquement.

Pour travailler avec Configuration Manager en utilisant une adresse IPv6 :

1. Vérifiez que votre système d'exploitation prend en charge IPv6 et IPv4. Pour plus d'informations, consultez la documentation du système d'exploitation.
2. Ouvrez le fichier **client-config.properties**, situé dans le <**répertoire d'installation de Configuration Manager** >/**conf** et modifiez les valeurs suivantes :
   - Modifiez la valeur du paramètre **bsf.server.url** et vérifiez qu'il utilise le nom d'hôte. Par exemple :

     bsf.server.url=http://monordinateur:8080/bsf
   - Modifiez la valeur du paramètre **bsf.server.services.url** et vérifiez que l'URL Configuration Manager est l'adresse du nom d'hôte. Par exemple :

     bsf.server.services.url=http://<Nom d'hôte Configuration Manager> : <Port Configuration Manager>/bsf
3. Ouvrez le fichier Tomcat **servers\server-0\conf\server.xml** et modifiez les valeurs suivantes :
   - Ajoutez l'adresse IPv6 au crochet SHUTDOWN en ajoutant **address**="**[::]**" à l'indicateur suivant :

     <Server port="8005" shutdown="SHUTDOWN" **address**="**[::]**" >
   - Dupliquez le connecteur HTTP. Pour le second connecteur, ajoutez l'adresse IPv6 [::]. Par exemple :

```
<Connector port="8180" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
           connectionTimeout="20000"
           redirectPort="8443" />
```

➤ Dupliquez le connecteur AJP. Pour le second connecteur, ajoutez l'adresse IPv6 [::]. Par exemple :

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 Ajoutez la variable d'environnement au serveur : useIPv6="true":

Ouvrez le fichier **edit_server-0.bat**, situé dans le **<répertoire d'installation de Configuration Manager >/bin**. Dans l'onglet Java, ajoutez la propriété suivante aux options Java : -DuseIPv6.

5 Redémarrez le serveur.

LDAP

LDAP peut être configuré dans Configuration Manager. Pour plus d'informations, voir "Paramètres système" dans le manuel de l'utilisateur *HP Universal CMDB Configuration Manager*.

Sécurisation renforcée

Contenu de ce chapitre :

Remarque : Après la mise à niveau, vous devez réexécuter la configuration SSL. Pour plus d'informations, voir "Mise à niveau de Configuration Manager", page 39.

Sécurisation renforcée de Configuration Manager

Cette section présente le concept d'une application de sécurisation Configuration Manager et décrit la planification et l'architecture requises pour implémenter la sécurité. Il est vivement recommandé de lire cette section avant de suivre la discussion sur la sécurisation renforcée dans les sections suivantes.

Configuration Manager a été conçu pour faire partie d'une architecture sécurisée, et peut par conséquent répondre au défi du traitement des menaces de sécurité auxquelles il peut être exposé.

Les directives relatives à la sécurisation renforcée traitent la configuration requise pour implémenter une application Configuration Manager plus sécurisée (renforcée).

Les informations relatives à la sécurisation renforcée fournies sont destinées principalement aux administrateurs Configuration Manager. Ceux-ci doivent se familiariser avec les paramètres et recommandations de sécurisation renforcée avant de commencer les procédures de sécurisation renforcée.

Voici les recommandations pour préparer la sécurisation renforcée de votre système :

- Évaluez le risque de sécurité/l'état de sécurité de l'ensemble de votre réseau, et basez-vous sur les conclusions pour effectuer le meilleur choix pour intégrer Configuration Manager dans votre réseau.
- Développez une bonne compréhension de l'infrastructure technique de Configuration Manager et des fonctionnalités de sécurité de Configuration Manager.
- Étudiez toutes les directives relatives à la sécurisation renforcée.
- Vérifiez que Configuration Manager est entièrement opérationnel avant de commencer les procédures de sécurisation renforcée.
- Suivez les procédures de sécurisation renforcée pas à pas, en suivant la chronologie de chaque section.

Important :

- Les procédures de sécurisation renforcée sont basées sur le fait que vous n'implémentez que les instructions fournies dans ces sections, et que vous n'exécutez pas d'autres étapes de sécurisation renforcée décrites ailleurs.
- Lorsque les procédures de sécurisation renforcées s'appliquent à une architecture distribuée spécifique, cela n'implique pas qu'il s'agit de la meilleure architecture qui réponde aux besoins de votre entreprise.
- Les procédures indiquées dans les sections suivantes doivent être exécutées sur des ordinateurs dédiés à Configuration Manager. L'utilisation de ces ordinateurs pour d'autres opérations en plus de Configuration Manager peut engendrer des résultats inattendus.
- Les informations de sécurisation renforcée fournies dans cette section ne doivent pas servir de guide pour évaluer les risques de sécurité de vos systèmes informatisés.

Chiffrer le mot de passe de base de données

Le mot de passe de base de données est enregistré dans le **<répertoire d'installation de Configuration Manager >\conf\database.properties**. Si vous souhaitez chiffrer le mot de passe, notre algorithme de chiffrement par défaut est compatible avec les normes FIPS 140-2.

Le chiffrement est réalisé à l'aide d'une clé, qui permet de chiffrer le mot de passe. La clé est ensuite chiffrée à l'aide d'une autre clé, appelée clé principale. Les deux clés sont chiffrées à l'aide du même algorithme. Pour plus d'informations sur les paramètres utilisés dans la procédure de chiffrement, voir "Paramètres de chiffrement", page 92.

Attention : Si vous modifiez l'algorithme de chiffrement, tous les mots de passe préalablement chiffrés ne sont plus utilisables.

Pour modifier le chiffrement de votre mot de passe de base de données :

1 Ouvrez le **<répertoire d'installation de Configuration Manager >\conf \encryption.properties** et modifiez les champs suivants :

- **engineName.** Entrez le nom de l'algorithme de chiffrement.
- **keySize.** Entrez la taille de la clé principale de l'algorithme sélectionné.

2 Exécutez le script **generate-keys.bat**, qui crée le répertoire suivant : **cnc920\security\encrypt_repository** et génère la clé de chiffrement.

3 Exécutez l'utilitaire **bin\encrypt-password** pour chiffrer le mot de passe. Définissez l'indicateur **-h** pour afficher les options disponibles.

4 Copiez le résultat de l'utilitaire de chiffrement de mot de passe et insérez le chiffrement obtenu dans le fichier **conf\database.properties**.

Paramètres de chiffrement

Le tableau ci-dessous contient les paramètres inclus dans le fichier **encryption.properties** utilisé pour le chiffrement de mot de passe de base de données. Pour plus d'informations sur le chiffrement du mot de passe de base de données, voir "Chiffrer le mot de passe de base de données", page 91.

Paramètre	Description
cryptoSource	Indiquer l'infrastructure d'implémentation de l'algorithme de chiffrement. Les options sont les suivantes : ➤ **lw.** Uses Bouncy Castle lightweight implementation (Option par défaut) ➤ **jce.** Java Cryptography Enhancement (infrastructure de chiffrement Java standard)
storageType	Indiquer le type de stockage de clé. Actuellement, seul le **fichier binaire** est pris en charge.
binaryFileStorageName	Indiquer l'emplacement du fichier dans lequel la clé principale est stockée.
cipherType	Type de chiffrement. Actuellement, seul **symmetricBlockCipher** est pris en charge.

Paramètre	Description
engineName	Nom de l'algorithme de chiffrement. Les options suivantes sont disponibles : ➤ **AES.** American Encryption Standard. Ce chiffrement est compatible FIPS 140-2. (Option par défaut) ➤ **Blowfish** ➤ **DES** ➤ **3DES.** (Compatible FIPS 140-2) ➤ **Null**. Aucun chiffrement
keySize	Taille de la clé principale. Elle est déterminée par l'algorithme : ➤ **AES.** 128, 192 ou 256 (Option par défaut 256) ➤ **Blowfish** 0-400 ➤ **DES** 56 ➤ **3DES.** 156
encodingMode	Codage ASCII des résultats du chiffrement binaire. Les options suivantes sont disponibles : ➤ **Base64** (Option par défaut) ➤ **Base64Url** ➤ **Hex**
algorithmModeName	Mode de l'algorithme. Actuellement, seul **CBC** est pris en charge.
algorithmPaddingName	Algorithme de remplissage utilisé. Les options suivantes sont disponibles : ➤ **PKCS7Padding** (Option par défaut) ➤ **PKCS5Padding**
jceProviderName	Nom de l'algorithme de chiffrement JCE. **Remarque :** Ne s'applique que si crytpSource est **jce**. Pour **lw**, engineName est utilisé.

Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé

Ces sections expliquent comment configurer Configuration Manager pour prendre en charge l'authentification et le chiffrement à l'aide du canal SSL (Secure Sockets Layer).

Configuration Manager utilise Tomcat 7.0 comme serveur d'applications.

Remarque : Tous les emplacements de répertoire et de fichier dépendent de votre plateforme, du système d'exploitation et de vos préférences d'installation.

---

1 Conditions préalables

Avant de lancer la procédure suivante, supprimez l'ancien fichier **tomcat.keystore** situé dans le **<répertoire d'installation de Configuration Manager >\java\lib\security\tomcat.keystore**.

2 Générer un Keystore de serveur

Créez un keystore (type JKS) à l'aide d'un certificat auto-signé et d'une clé privée correspondante :

➤ À partir du répertoire bin de l'installation Java du répertoire d'installation de Configuration Manager, exécutez la commande suivante :

```
keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
security\tomcat.keystore
```

La boîte de dialogue Console s'affiche.

➤ Entrez le mot de passe keystore. S'il a été modifié, changez-le manuellement dans le fichier.

➤ Répondez à la question, **Quels sont vos nom et prénom ?** Entrez le nom du serveur Web Configuration Manager. Entrez les autres paramètres inhérents à votre entreprise.

➤ Entrez le mot de passe de la clé. Il DOIT être identique au mot de passe keystore.

Un keystore JKS est créé sous le nom **tomcat.keystore** avec un certificat de serveur appelé **hpcert**.

3 Placer le certificat dans le magasin de données de confiance du client

Ajoutez le certificat aux magasins approuvés du client dans Internet Explorer sur votre ordinateur (**Outils** > **Options Internet** > **Contenu** > **Certificats**). Sinon, vous serez invité à le faire lors de la première utilisation de Configuration Manager.

Pour plus d'informations sur l'utilisation de certificats client, voir "Certificats client", page 101.

Limitation : **tomcat.keystore** ne peut contenir qu'un seul certificat de serveur.

---

4 Vérifier les paramètres de configuration du client

Ouvrez le fichier **client-config.properties**, situé dans le répertoire **conf** du répertoire d'installation de Configuration Manager. Définissez le protocole de **bsf.server.url** sur **https** et le port sur **8443**.

5 Modifier le fichier server.xml

Ouvrez le fichier **server.xml**, situé dans le **<répertoire d'installation de Configuration Manager>\servers\server-0\conf**. Localisez la section commençant par

```
Connector port="8443"
```

qui apparaît sous forme de commentaires. Activez le script en supprimant le caractère de commentaire et ajoutez les attributs suivants au connecteur HTTPS :

keystoreFile="<emplacement du fichier tomcat.keystore>" (voir l'étape 2 à la page 94)
keystorePass="<password>"

Excluez la ligne suivante par un commentaire :

<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />

6 Redémarrer le serveur

7 Vérifier la sécurité du serveur

Pour vérifier que le serveur Configuration Manager est sécurisé, entrez l'URL suivante dans le navigateur Web : **https://<Nom du serveur ou adresse IP Configuration Manager>:8443/cnc**.

Conseil : Si vous n'arrivez pas à vous connecter, utilisez un autre navigateur ou passez à une version plus récente du navigateur.

Activer SSL sur l'ordinateur serveur à l'aide d'un certificat d'une autorité de certification

Pour utiliser un certificat émis pour une autorité de certification, keystore doit être au format Java. L'exemple suivant explique comment formater le keystore pour un ordinateur Windows.

1 Conditions préalables

Avant de lancer la procédure suivante, supprimez l'ancien fichier **tomcat.keystore** situé dans le **<répertoire d'installation de Configuration Manager >\java\lib\security\tomcat.keystore**.

2 Générer un Keystore de serveur

a Générez un certificat signé par une autorité de certification et installez-le sous Windows.

b Exportez le certificat dans un fichier ***.pfx** (y compris les clés privées) à l'aide de Microsoft Management Console (**mmc.exe**).

➤ Entrez une chaîne comme mot de passe pour le fichier **pfx**. (Ce mot de passe vous est demandé lors de la conversion du type de keystore en un keystore JAVA.)
Le fichier **.pfx** contient un certificat public et une clé privée et il est protégé par un mot de passe.

c Copiez le fichier **.pfx** que vous avez créé dans le dossier suivant : **<Répertoire d'installation de Configuration Manager>\java\lib\security**.

d Ouvrez l'invite de commande et remplacez le répertoire par le **<répertoire d'installation de Configuration Manager>\bin\jre\bin**.

➤ Remplacez le type de keystore **PKCS12** par un keystore **JAVA** en exécutant la commande suivante :

```
keytool -importkeystore -srckeystore <répertoire d'installation de Configuration Manager >\conf\security\<nom de fichier pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

Le mot de passe du keystore source (**.pfx**) vous est demandé. Il s'agit du mot de passe que vous avez fourni lors de la création du fichier pfx à l'étape b.

3 Vérifier les paramètres de configuration du client

Ouvrez le fichier suivant : **<répertoire d'installation de Configuration Manager >\cnc\conf\client-config.properties** et vérifiez que la propriété **bsf.server.url** est définie sur **https** et que le port est **8443**.

4 Modifier le fichier server.xml

Ouvrez le fichier **server.xml**, situé dans le **<répertoire d'installation de Configuration Manager>\servers\server-0\conf**. Localisez la section commençant par

Connector port="8443"

qui apparaît sous forme de commentaires. Activez le script en supprimant le caractère de commentaire et ajoutez les deux lignes suivantes :

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

Excluez la ligne suivante par un commentaire :

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

5 Redémarrer le serveur

6 Vérifier la sécurité du serveur

Pour vérifier que le serveur Configuration Manager est sécurisé, entrez l'URL suivante dans le navigateur Web : **https://<Nom du serveur ou adresse IP Configuration Manager>:8443/cnc**.

Limitation : **tomcat.keystore** ne peut contenir qu'un seul certificat de serveur.

Remarque : Tous les emplacements de répertoire et de fichier dépendent de votre plateforme, du système d'exploitation et de vos préférences d'installation.

Par exemple : java/{os name}/lib.

Activer SSL à l'aide d'un certificat client

Si le certificat utilisé par le serveur Web de Configuration Manager est émis par une autorité de certification bien connue, il est fort probable que votre serveur Web valide le certificat sans action supplémentaire.

Si l'autorité de certification n'est pas approuvée par le magasin d'approbations du serveur, importez le certificat CA dans ce magasin.

L'exemple suivant démontre comment importer le certificat auto-signé **hpcert** dans le magasin d'approbations du serveur (cacerts).

Pour importer un certificat dans le magasin d'approbations du serveur :

1. Sur l'ordinateur client, localisez et renommez le certificat **hpcert** en **hpcert.cer**.
2. Copiez **hpcert.cer** sur l'ordinateur serveur dans le **<répertoire d'installation de Configuration Manager >\java\bin**.
3. Sur l'ordinateur serveur, importez le certificat d'Autorité de certification dans le magasin d'approbations (cacerts) à l'aide de l'utilitaire keytool avec la commande suivante :

   ```
   <répertoire d'installation de Configuration Manager >\java\bin\keytool.exe -import-alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Modifiez le fichier **server.xml** (situé dans le **<répertoire d'installation de Configuration Manager>\servers\server-0\conf**) comme suit :
   a. Appliquez les modifications décrites à l'étape 5 à la page 95.
   b. Après avoir apporté ces modifications, ajoutez les attributs suivants au connecteur HTTPS :

      ```
      truststoreFile="../../java/lib/security/cacerts"
      truststorePass="changeit" />
      ```

   c. Définissez clientAuth="true".
5. Vérifiez la sécurité du serveur comme indiqué à l'étape 7 à la page 96.

Activer SSL pour l'authentification uniquement

Cette tâche décrit comment configurer Configuration Manager pour prendre en charge l'authentification uniquement. Il s'agit du niveau minimum de sécurité requis pour utiliser Configuration Manager.

1 Suivez l'une des procédures d'activation de SSL sur l'ordinateur serveur comme indiqué dans "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé", page 94 jusqu'à l'étape 6 à la page 96 ou "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat d'une autorité de certification", page 96 jusqu'à l'étape 5 à la page 98.

2 Entrez l'URL suivante dans le navigateur Web : http://<Nom du serveur ou adresse IP Configuration Manager>:8080/cnc.

Activer l'authentification de certificat client

Cette tâche décrit comment configurer Configuration Manager pour accepter l'authentification de certificat côté client.

1 Suivez la procédure pour activer SSL sur l'ordinateur serveur comme indiqué dans "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé", page 94.

2 Ouvrez le fichier suivant : **<répertoire d'installation de Configuration Manager >\conf\lwssofmconf.xml.** Localisez la section commençant par in-client certificate. Par exemple :

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
```

Activez la fonctionnalité de certificat client en supprimant le caractère de commentaire.

3 Extrayez le nom d'utilisateur du certificat en procédant comme suit :

a Le paramètre **userIdentifierRetrieveField** indique le champ de certificat qui contient le nom d'utilisateur. Les options sont les suivantes :

- **SubjectDN**
- **SubjectAlternativeName**

b Le paramètre **userIdentifierRetrieveMode** indique si le nom d'utilisateur correspond au contenu du champ approprié ou seulement une partie de ce champ. Les options sont les suivantes :

- **EntireField**
- **FieldPart**

c Si la valeur de **userIdentifierRetrieveMode** est **FieldPart**, le paramètre **userIdentifierRetrieveFieldPart** indique la partie du champ approprié correspondant au nom d'utilisateur. La valeur est une lettre de code basée sur la légende définie dans le certificat.

4 Ouvrez le fichier suivant : **<répertoire d'installation de Configuration Manager >\conf\client-config.properties** et modifiez les propriétés suivantes :

- Modifiez **bsf.server.url** pour utiliser le protocole HTTPS et remplacez le port HTTPS par le port décrit dans "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé", page 94.
- Modifiez **bsf.server.services.url** pour utiliser le protocole HTTP et remplacez le port par le port HTTP original.

Certificats client

Contenu de ce chapitre :

Informations sur les certificats client

Cette section décrit les informations sur les certificats client et l'extraction d'un identificateur utilisateur d'un certificat client.

- **Identificateur d'utilisateur**

  L'identificateur d'utilisateur correspond à la portion unique du certificat client utilisée pour déterminer l'identité de l'utilisateur.

➤ **Informations sur les certificats client**

Les informations de base relatives aux certificats client sont les suivantes :

Champ Certificat	Description
Version	Version du certificat crypté. Exemple : 1 (0x1)
Numéro de série	Entier positif affecté par l'autorité de certification à chaque certificat. Exemple : 0 (0x0)
Algorithme de signature	L'identificateur de l'algorithme utilisé par l'autorité de certification pour signer le certificat. Exemple : md5WithRSAEncryption
Émetteur	Entité ayant signé et émis le certificat. Exemple : CN=Émetteur, C=US, ST=NY, L=New York, O=Organisation du travail, O=exemple.com
Validité	Intervalle pendant lequel l'autorité de certification garantit la conservation des informations sur l'état du certificat : ➤ **Pas avant**. Spécifier la date de début de la période de validité du certificat. Exemple : Nov 25 04:34:49 2009 GMT ➤ **Pas après**. Spécifier la date de fin de la période de validité du certificat. Exemple : Nov 25 04:34:49 2010 GMT
Objet	Entité associée à la clé publique enregistrée dans le champ de clé publique de l'objet.
Subject Public Key Info	Utilisée pour contenir la clé publique et identifier l'algorithme avec lequel la clé est utilisée (par exemple, RSA, DSA ou Diffie-Hellman).

Pour plus d'informations, voir Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile :

http://tools.ietf.org/html/rfc5280

➤ **Champ Objet**

Ce champ (également appelé Subject Distinguish Name ou SubjectDN) identifie l'identité associée à la clé publique.

Ce champ contient les attributs suivants (il peut également contenir d'autres attributs) :

Attribut Objet	Description de l'attribut Objet	Exemple
CN	Nom commun	CN=Bob BobFamily
emailAddress	Adresse e-mail	*emailAddress=bob@exemple.com*
C	Nom du pays	C=US
ST	État ou nom de province	ST=NY
L	Nom de localité	L=New York
O	Nom de l'organisation	O=Organisation du travail
OU	Nom de l'unité organisationnelle	OU=Responsables

Pour extraire l'identificateur de l'utilisateur de l'objet, vous pouvez utiliser le champ SubjectDN ou l'attribut SubjectDN.

➤ **Extension des informations sur les certificats client**

Les extensions définies pour les certificats X.509 v3 fournissent des méthodes d'association d'attributs supplémentaires aux utilisateurs ou aux clés publiques pour la gestion des relations entre les autorités de certification. Le Champ Nom de remplacement de l'objet peut contenir l'identificateur d'utilisateur.

➤ **Champ Nom de remplacement de l'objet**

L'extension du nom de remplacement de l'objet permet aux identités d'être liées à l'objet du certificat. Ces identités peuvent être ajoutées à l'identité ou la remplacer dans le champ Objet du certificat.

Le champ Nom de remplacement de l'objet peut contenir les entités suivantes :

Identité	Exemple
otherName	Autre nom : Nom principal= *bobOtherAltName@exemple.com*
rfc822Name	Nom RFC822 =*bobRFC822AltName@exemple.com*
dNSName	Nom DNS=exemple1.com
x400Address	
directoryName	Adresse du répertoire : E=*bobDirAltName@exemple.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/
iPAddress	Adresse IP=192.168.7.1
registeredID	ID enregistrée=1.2.3.4

Pour extraire l'identificateur d'utilisateur du nom de remplacement de l'objet, vous pouvez utiliser l'une des entités.

Configuration

Configuration Manager utilise LW-SSO pour tirer parti de l'identificateur d'utilisateur d'un certificat client. Le gestionnaire de certificats client utilise les attributs suivants pour configurer LW-SSO pour qu'il tire parti de l'identificateur d'utilisateur :

Pour tirer parti des informations d'un certificat client, Configuration Manager doit être configuré pour extraire l'identificateur d'utilisateur.

Les éléments suivants doivent être choisis :

- Le champ à utiliser : SubjectDN ou Subject Alternative Name ?
- Le champ entier ou une partie du champ à utiliser ?
- Si une partie du champ de saisie est utilisée, attribuez-lui une valeur : indiquez l'attribut de l'objet pour SubjectDN ou l'identité pour le nom de remplacement de l'objet.

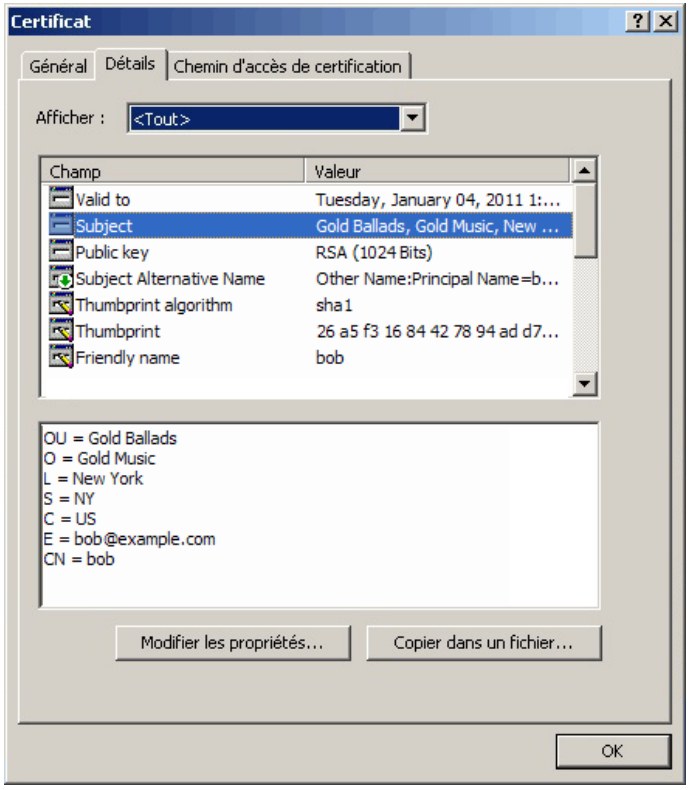
Les attributs suivants sont utilisés par le gestionnaire de certificats client pour configurer LW-SSO :

Nom de l'attribut	Description
enabled	Spécifier si le gestionnaire est activé ou désactivé. **Important** : Il est vivement recommandé de définir explicitement la valeur sur false et d'activer le gestionnaire uniquement lorsque la validation du certificat client est requise.
userIdentifierRetrieveField	Le paramètre indique le champ de certificat qui contient l'identificateur d'utilisateur. Options : **SubjectDN** ou **SubjectAlternativeName**.
userIdentifierRetrieveMode	Le paramètre userIdentifierRetrieveMode indique si l'identificateur d'utilisateur correspond au contenu du champ approprié ou seulement une partie de ce champ. Options : **EntireField** ou **FieldPart**.

Nom de l'attribut	Description
userIdentifierRetrieveFieldPart	Si la valeur de **userIdentifierRetrieveMode** est **FieldPart**, ce paramètre indique la partie du champ approprié correspondant au nom d'utilisateur. La valeur est une lettre de code basée sur la légende définie dans le certificat. **Remarque** : Cet attribut ne peut pas être vide lorsque **userIdentifierRetrieveMode** est défini sur **FieldPart**. Il ne peut pas être vide lorsque **userIdentifierRetrievField** est défini sur **SubjectAlternativeName**.

Exemples

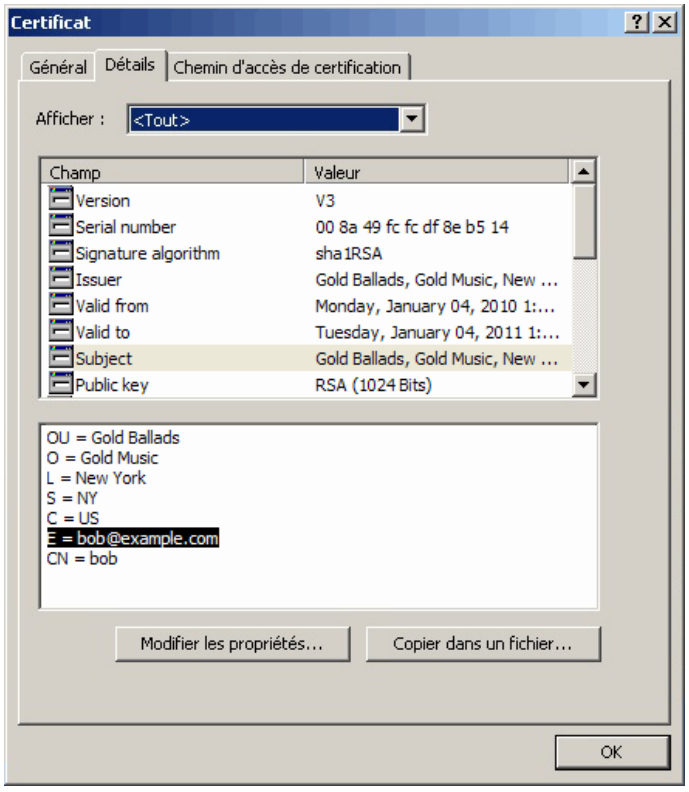
➤ L'objet permet de contenir l'identificateur d'utilisateur



L'exemple suivant indique comment configurer le gestionnaire pour extraire l'identificateur d'utilisateur de SubjectDN :

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

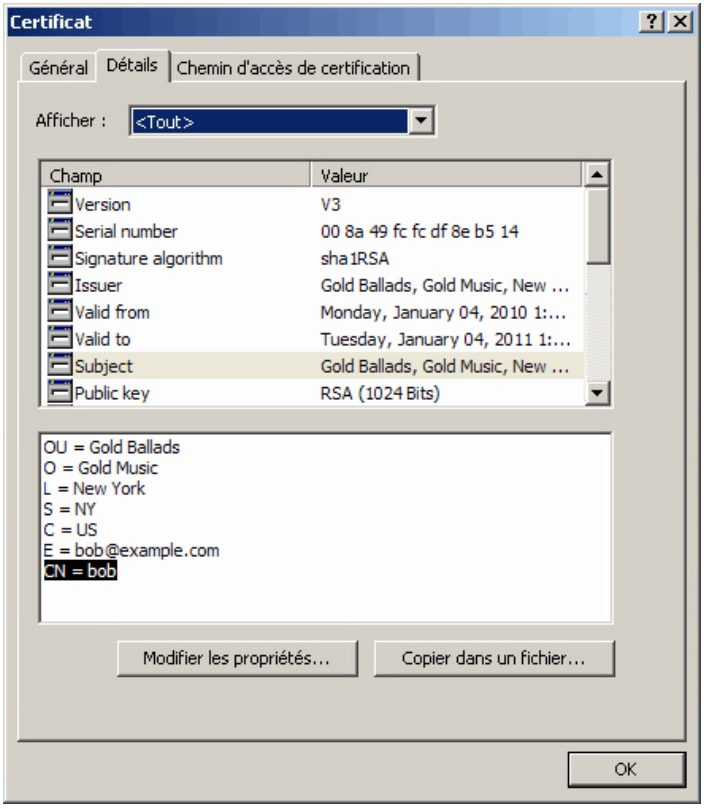
➤ **Le champ E-mail de l'objet permet de contenir l'identificateur d'utilisateur**



Utilisez les noms des champs affichés dans la légende du certificat client. L'exemple suivant indique comment configurer le gestionnaire pour extraire l'identificateur d'utilisateur du champ E-mail de l'objet :

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="E" />
```

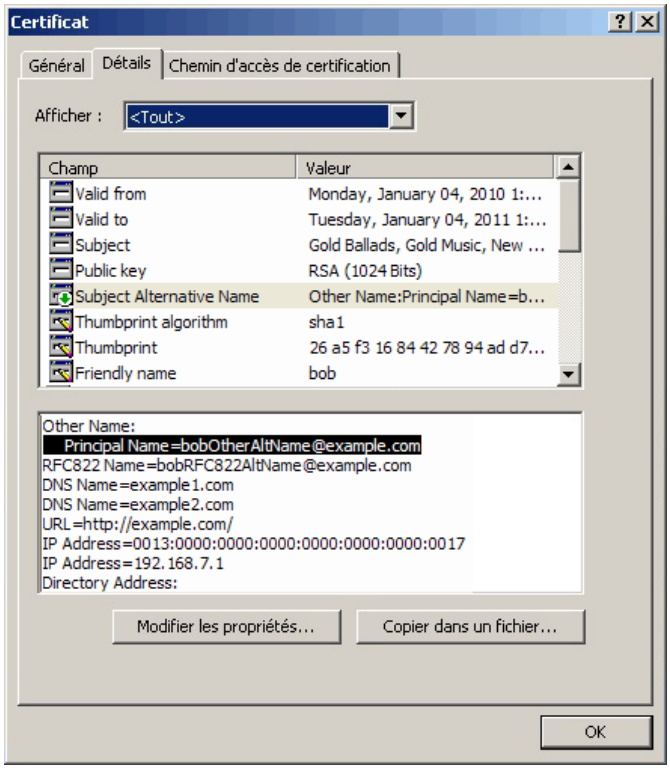
➤ **Le champ Nom de commande de l'objet permet de contenir l'identificateur d'utilisateur**



Utilisez les noms des champs affichés dans la légende du certificat client. L'exemple suivant indique comment configurer le gestionnaire pour extraire l'identificateur d'utilisateur du champ Nom personnalisé de l'objet :

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="CN" />
```

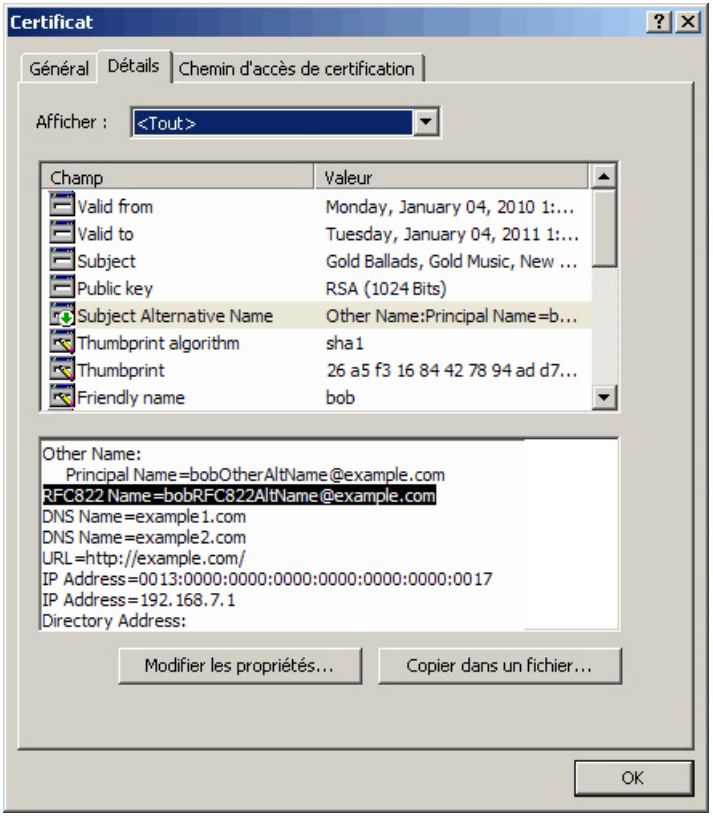
➤ **L'identité otherName du nom de remplacement de l'objet permet de contenir l'identificateur d'utilisateur**



Utilisez le nom de l'identité affiché dans la légende du certificat client. L'exemple suivant indique comment configurer le gestionnaire pour extraire l'identificateur d'utilisateur de l'identité otherName du Nom de remplacement de l'objet :

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Nom
principal" />
```

➤ **L'identité rfc822Name du nom de remplacement de l'objet permet de contenir l'identificateur d'utilisateur**



Utilisez le nom de l'identité affiché dans la légende du certificat client. L'exemple suivant indique comment configurer le gestionnaire pour extraire l'identificateur d'utilisateur de l'identité rfc822Name du Nom de remplacement de l'objet :

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Nom
principal" />
```

Configurer Configuration Manager pour fonctionner avec UCMDB à l'aide de SSL

Vous pouvez configurer Configuration Manager pour fonctionner avec UCMDB en utilisant SSL (Secure Sockets Layer). Le connecteur SSL du port 8443 est activé par défaut dans UCMDB.

Pour exporter le certificat du serveur et l'importer dans le magasin approuvé du client

1. Allez dans le **<répertoire d'installation d'UCMDB>\bin\jre\bin** et exécutez la commande suivante :

   keytool -export -alias hpcert -keystore <répertoire du serveur UCMDB> \conf\security\server.keystore -storepass hppass -file <fichiercertificat>

2. Importez le certificat dans le magasin d'approbations Configuration Manager (le magasin d'approbations par défaut) :

   <ACCUEIL_JAVA_CM>\bin\keytool -import -trustcacerts -alias hpcert -keystore <ACCUEIL_JAVA_CM>\lib\security\cacerts -storepass changeit -file <fichiercertificat>

3. Définissez les propriétés de connexion UCMDB dans Configuration Manager :

   Sélectionnez **Système** > **Paramètres** > **Integrations** > **UCMDB Foundation** > **UCMDB Foundation**. Définissez la stratégie de connexion sur **HTTPS**, le port du serveur UCMDB sur le port HTTPS UCMDB et modifiez l'URL d'accès UCMDB sur https://<Nomhôte>:8443.

4. Enregistrez le jeu de configurations et activez-le. Redémarrez Configuration Manager.

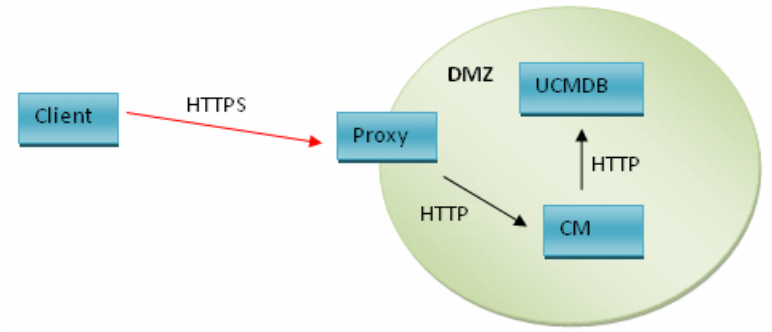
Pour configurer Configuration Manager pour fonctionner avec d'autres produits (tels que les processus d'équilibrage) en utilisant SSL (Secure Sockets Layer), importez le certificat de sécurité du produit dans le magasin d'approbations Configuration Manager (magasin d'approbations par défaut) en exécutant la commande suivante :

<ACCUEIL_JAVA_CM>\bin\keytool -import -trustcacerts -alias <alias> -keystore <ACCUEIL_JAVA_CM>\lib\security\cacerts -storepass changeit -file <fichiercertificat>

Proxy inverse

Si Configuration Manager et UCMDB sont situés dans un DMZ, il est recommandé de configurer le système pour fonctionner avec un serveur proxy inverse. Les étapes de configuration sont identiques à celles de la configuration d'UCMDB pour fonctionner avec un proxy inverse. Pour activer l'accès à Configuration Manager, vous devez mapper les chemins **/cnc** et **/bsf** sur les URL du serveur distant sur lequel Configuration Manager est installé.

L'image suivante illustre la procédure de configuration d'un proxy inverse pour Configuration Manager :



Par exemple, si le proxy inverse est un serveur Apache, ajoutez les lignes suivantes au fichier **Apache2.2\conf\extra\httpd-ssl.conf** et redémarrez le serveur Apache :

```
ProxyPass /cnc http://<NOMHOTE_CM>:<PORT_HTTP_CM>/cnc
ProxyPassReverse /cnc http:// <NOMHOTE_CM>:<PORT_HTTP_CM>/cnc
ProxyPass /bsf http://< NOMHOTE_CM >:<PORT_HTTP_CM>/bsf
ProxyPassReverse /bsf http:// <NOMHOTE_CM>:<PORT_HTTP_CM>/bsf
```

Différents types de proxy inverse peuvent requérir différentes étapes de configuration. Pour plus d'informations, consultez la documentation du serveur proxy.

Pour configurer un proxy inverse pour Configuration Manager :

Mettez à jour le fichier **client-config.properties** dans le **<répertoire d'installation de Configuration Manager >\conf** comme suit :

```
bsf.server.url=https://<nom-serveur-proxy>:443/bsf
```

Le port HTTPS par défaut du proxy Apache est 443.

Partie II

Annexes

A

Limitations de capacité

Les limitations de capacité de Configuration Manager sont répertoriées dans le tableau ci-dessous.

Nombre maximum de vues	100
Nombre maximum de politiques	300
Nombre maximum de CI composites par vue	5000
Nombre maximum d'utilisateurs concurrents	50
Nombre maximum de CI composites dans le module Analyse de la configuration	1000

B

LW-SSO (Lightweight Single Sign-On Authentication) – Références générales

Contenu de ce chapitre :

Authentification LW-SSO - Présentation

LW-SSO est une méthode de contrôle d'accès qui permet à un utilisateur d'établir une seule connexion aux ressources de plusieurs systèmes logiciels sans avoir à se reconnecter par la suite. Les applications figurant dans le groupe configuré de systèmes logiciels tiennent compte de cette authentification. Il n'est donc pas nécessaire de procéder à une autre authentification lorsque vous passez d'une application à une autre.

Les informations de cette section s'applique à LW-SSO versions 2.2 et 2.3.

Pour obtenir des informations sur la résolution des problèmes liés à LW-SSO, voir "LW-SSO - Résolution des problèmes et limitations", page 137.

Cette section contient les rubriques suivantes :

Délai d'expiration du jeton LW-SSO

La valeur du délai d'expiration du jeton LW-SSO détermine la validité de la session de l'application. Par conséquent, la valeur de son délai d'expiration doit être au moins identique à celle de la session de l'application.

Configuration recommandée pour le délai d'expiration du jeton LW-SSO

Chaque application qui utilise LW-SSO doit configurer le délai d'expiration du jeton. La valeur recommandée est 60 minutes. Pour une application ne requérant pas un haut niveau de sécurité, il est possible de configurer une valeur de 300 minutes.

Heure GMT

Toutes les applications impliquées dans une intégration LW-SSO doivent utiliser la même heure GMT avec une différence maximum de 15 minutes.

Fonctionnalité multi-domaines

La fonctionnalité multi-domaines requiert que toutes les applications qui participent à l'intégration LW-SSO configurent les paramètres trustedHosts (ou les paramètres **protectedDomains**), s'ils sont requis pour s'intégrer dans des applications de différents domaines DNS. De plus, ils doivent également ajouter le domaine approprié dans l'élément **lwsso** de la configuration.

Obtenir un SecurityToken pour la fonctionnalité URL

Pour recevoir des informations envoyées sous la forme d'un **SecurityToken pour URL** en provenance d'autres applications, l'application hôte doit configurer le domaine approprié dans l'élément **lwsso** de la configuration.

Avertissements de sécurité LW-SSO

Cette section présente les avertissements de sécurité relatifs à la configuration LW-SSO :

➤ **Paramètre confidentiel InitString dans LW-SSO.** LW-SSO utilise une méthode de chiffrement symétrique (Symmetric Encryption) pour valider et créer un jeton LW-SSO. Le paramètre **initString** de la configuration sert à l'initialisation de la clé secrète. Une application crée un jeton et chaque application partageant le même paramètre initString valide le jeton.

Attention :

➤ Il n'est pas possible d'utiliser LW-SSO sans définir le paramètre **initString**.

➤ Le paramètre **initString** contient des informations confidentielles et doit être traité comme tel en termes de publication, de transport et de persistance.

➤ Le paramètre **initString** doit être partagé uniquement entre des applications mutuellement intégrées à l'aide de LW-SSO.

➤ Le paramètre **initString** doit contenir au minimum 12 caractères.

➤ **Activer LW-SSO uniquement en cas de besoin.** LW-SSO doit être désactivé sauf spécification contraire.

➤ **Niveau de sécurité d'authentification.** L'application qui utilise l'infrastructure d'authentification la plus faible et émet un jeton LW-SSO devant être approuvé par d'autres applications intégrées détermine le niveau de sécurité d'authentification de toutes les applications.

Seules les applications qui utilisent des infrastructures d'authentification fortes et sécurisées émettent un jeton LW-SSO.

- **Implications du chiffrement symétrique.** LW-SSO utilise le chiffrement symétrique pour émettre et valider des jetons LW-SSO. Par conséquent, toute application qui utilise LW-SSO peut émettre un jeton devant être approuvé par toutes les autres applications qui partagent le même paramètre **initString**. Ce risque potentiel est pertinent lorsqu'une application qui partage un paramètre initString, réside ou est accessible depuis un emplacement non approuvé.

- **Mappage des utilisateurs (Synchronisation).** L'infrastructure LW-SSO n'assure pas le mappage des utilisateurs entre les applications intégrées. Par conséquent, l'application intégrée doit contrôler le mappage des utilisateurs. Nous vous recommandons de partager le même registre utilisateur (comme LDAP/AD) entre toutes les applications intégrées.

  L'échec du mappage des utilisateurs peut provoquer des violations de sécurité et un comportement négatif des applications. Par exemple, le même nom d'utilisateur peut être attribué à différents utilisateurs réels dans les différentes applications.

  De plus, lorsqu'un utilisateur se connecte à une application (AppA) et accède ensuite à une seconde application (AppB) qui utilise l'authentification de conteneur ou d'application, l'échec du mappage de l'utilisateur peut forcer l'utilisateur à se connecter manuellement à AppB et à entrer un nom d'utilisateur. Si l'utilisateur entre un autre nom que celui utilisé pour la connexion à AppA, le comportement suivant peut se produire : si l'utilisateur accède ensuite à une troisième application (AppC) à partir d'AppA ou d'AppB, il va y accéder en utilisant les noms d'utilisateur spécifiés pour la connexion à AppA ou AppB respectivement.

- **Gestionnaire des identités**. Utilisé pour l'authentification, toutes les ressources non protégées du Gestionnaire des identités doivent être configurées à l'aide du paramètre **nonsecureURLs** du fichier de configuration LW-SSO.

C

Résolution des problèmes

Contenu de ce chapitre :

Résolution des problèmes et limitations

Limitations

Vous n'obtiendrez pas le nouveau type de CI créé dans UCMDB tant que vous n'aurez pas fermé et rétabli la connexion à Configuration Manager.

Résolution des problèmes

Problème. L'attribut **name** du type CI Nœud n'est pas qualifié comme modification contrôlée et n'est pas copié à l'état Autorisé pendant l'autorisation du CI. Cela se produit si Configuration Manager version 9.20 est installé sans Content Pack 9 pour UCMDB.

Solution. Essayez l'une des solutions suivantes :

- Définissez manuellement l'attribut **name** pour qu'il soit qualifié comme modification contrôlée dans le Gestionnaire des types de CI UCMDB.
- Installez Content Pack 9.

Problème. Lorsque vous démarrez le service Configuration Manager, vous recevez le message d'erreur suivant :

> Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

Solution. Procédez comme suit :

1. Allez dans le <**répertoire d'installation de Configuration Manager**>**cnc****bin** et exécutez la commande suivante :

   edit-server-0.bat

2. Sélectionnez l'onglet Démarrer. Dans la liste déroulante Mode (en bas), sélectionnez **jvm** au lieu de **exe**.
3. Sélectionnez l'onglet Arrêt. Dans le champ Classe, remplacez le nom **Boostrap** par **Bootstrap**.
4. Cliquez sur **OK**.
5. Exécutez votre service.

Gestionnaire de déploiement - Résolution des problèmes et limitations

Pour dépanner le Gestionnaire de déploiement, ouvrez le journal de session de la session précédente, situé dans le répertoire suivant :

%temp%\HP\ucmdb-dm\Workspace\Sessions

Directives générales de redéploiement

Pendant l'installation, notez les avertissements et les erreurs affichés sur la page Validation du Gestionnaire de déploiement en cliquant sur le bouton de détails situé en regard de chaque composant déployé.

Lorsqu'un problème a été détecté pendant le déploiement et qu'une solution a été trouvée, procédez comme suit :

1. Désinstallez les produits déployés et redémarrez l'ordinateur.
2. Redémarrez le Gestionnaire de déploiement et entrez à nouveau toutes les configurations.

Problèmes liés à l'échec du déploiement

Problème. Erreur d'autorisation pendant le déploiement.

Le journal de session indique qu'un problème est survenu au niveau des autorisations utilisateur de la base de données lors de la création d'un nouveau schéma.

Solution. Pour créer une base de données, vous devez disposer des autorisations appropriées. Vérifiez que les informations d'authentification utilisateur appliquées dans le déploiement sont suffisantes pour la création de l'espace disque logique et du schéma.

Problème. Échec de la configuration du schéma/de la base de données dans UCMDB.

Le journal de session indique que le Gestionnaire de déploiement n'a pas réussi à créer un schéma ou une base de données.

Solution :

Remarque : Notez que vous ne pouvez pas créer un nouveau schéma UCMDB et vous connecter à un schéma historique UCMDB existant (quel que soit le type de serveur de base de données).

Vérifiez que le schéma UCMDB et le schéma historique UCMDB n'utilisent pas le type de connexion suivant :

- Schéma UCMDB - Créer un nouveau schéma
- Schéma historique UCMDB - Se connecter à un schéma existant

Problème. Échec de la configuration du schéma/de la base de données dans UCMDB.

Le journal de session indique que le schéma n'a pas pu être créé.

Solution. Ouvrez session.log et localisez le message d'erreur :
Erreur SQL d'exécution de l'instruction CREATE USER <nom du schéma>

Lors de la désignation du schéma Oracle dans la page Configuration de la base de données du Gestionnaire de déploiement, veillez à utiliser uniquement des lettres (a-z), des chiffres (0-9) et le tiret ('-').

Problème. Impossible de créer le schéma étant donné que l'espace est insuffisant.

Solution. Augmentez l'espace libre dans le schéma ou la base de données. Utilisez les interfaces de gestion standard fournies par Oracle et Microsoft.

Problème. Échec de la configuration de la base de données. Erreur :
NT AUTHORITY\ANONYMOUS LOGON – Could not connect to database.

Lors de la sélection d'un serveur MSSQL à l'aide de l'authentification NTLM pour la configuration de la base de données UCMDB, la configuration de la base de données a échoué, provoquant l'échec du déploiement.

Solution. Déployez UCMDB sur un ordinateur localhost (l'unique emplacement où l'authentification NTLM est prise en charge).

Problème. Échec de la configuration de la base de données Configuration Manager lors de la création d'une base de données.

Les erreurs suivantes peuvent s'afficher dans le panneau des détails du Gestionnaire de déploiement :

> Failed to create Oracle schema due to error: ORA-01031 : insufficient privileges

ou

> Failed to create a schema to the database: machineName.
> Reason: ORA-01919: role 'RESOURCE' does not exist

Solution. Vérifiez que l'utilisateur de la base de données dispose des privilèges de rôle suivants :

- Connecter
- Ressource

Problème. Échec du déploiement en raison d'une insuffisance de l'espace disque sur l'ordinateur hôte cible.

Solution. Connectez-vous à l'ordinateur hôte cible et assurez-vous que l'espace disque est suffisant pour assurer la réussite du déploiement :

- UCMDB requiert 1 Go d'espace disque
- Configuration Manager requiert 1 Go d'espace disque
- DDMA requiert 1 Go d'espace disque

Remarque : Outre les besoins inhérents au produit, un espace supplémentaire de 1 Go est requis pour la gestion des fichiers temporaires.

Problème. Échec du ping de l'utilitaire UCMDB.

Cet utilitaire est exécuté à partir de l'ordinateur Configuration Manager et vérifie que la connexion à l'instance UCMDB existante est disponible. Ouvrez session.log et localisez le message d'erreur :
Échec de la connexion test en raison d'une erreur : java.net.ConnectException: Connection refused: connect.

Solution :

- Vérifiez que le port 8080 de l'UCMDB cible n'est pas bloqué par le pare-feu Windows.
- Vérifiez que le serveur UCMDB est accessible à partir de l'ordinateur Configuration Manager, et que le déploiement UCMDB a été exécuté avec succès et qu'il fonctionne.

Connexion à l'ordinateur hôte non disponible

Problème. RPC non disponible ou erreur inconnue.

L'activation du bouton Tester la connexion génère une erreur RPC non disponible.

Solution. Corrigez le nom d'hôte s'il est incorrect, et assurez-vous que le service WMI et les services Server fonctionnent et que le pare-feu Windows ne bloque pas l'accès à l'interface WMI.

Désactivez le pare-feu Windows ou ajoutez une exception de pare-feu permettant d'accéder à l'administration à distance.

Pour ce faire, ouvrez le panneau de configuration du **Pare-feu** et sélectionnez **Règles de trafic entrant.** Activez tous les fichiers et imprimantes, les règles WMI et le port 8080.

Échec du test de la connexion

Problème. Accès refusé.

L'accès est refusé en raison d'un nom d'utilisateur et/ou d'un mot de passe incorrect, de paramètres DNS incorrects, ou le nom d'utilisateur appliqué au déploiement ne dispose pas des informations d'identification administratives sur l'ordinateur hôte cible.

Solution. Vérifiez que les informations d'identification utilisateur spécifiées sont correctes et que l'utilisateur dispose d'informations d'identification administratives sur l'ordinateur hôte cible.

Échec de l'accès à l'application

Problème. Déploiement réussi – échec de l'accès à l'application (UCMDB ou Configuration Manager).

Solution. Vérifiez que les services UCMDB et Configuration Manager suivants existent et fonctionnent.

- Service **UCMDB_Server**
- Service **HPUCMDBCMoasisSNAPSHOTserver0**

Vérifiez les journaux de déploiement situés dans le répertoire des sessions pour connaître les erreurs.

LW-SSO est désactivé

Problème. Déploiement réussi - la fonctionnalité LW-SSO est désactivée.

Solution. Vérifiez que la chaîne init et le domaine LW-SSO sont identiques sur UCMDB et Configuration Manager (et OO, si applicable).

Vérifiez les paramètres de configuration LW-SSO dans les produits à l'aide des méthodes suivantes :

- Configuration Manager – Ouvrez le fichier **lwssofmconf.xml** et vérifiez les définitions de domaine et de chaîne init. Le fichier est situé dans le **<répertoire d'installation de Configuration Manager >\conf** .
- UCMDB – Ouvrez UCMDB et sélectionnez **Gestionnaires** > **Administration** > **Gestionnaire de paramètres d'infrastructure**.

Si Configuration Manager et UCMDB résident sur des ordinateurs hôtes ayant différents domaines DNS, vérifiez que les paramètres **Domaines approuvés** incluent les domaines DNS et qu'ils sont activés dans les deux produits.

Pour recevoir des informations supplémentaires sur le déploiement, le Gestionnaire de déploiement peut être activé en mode débogage. Ce mode fournit des informations complémentaires sur le déploiement.

Pour activer le mode de débogage :

1. Après l'exécution du Gestionnaire de déploiement, ouvrez une fenêtre de navigateur et saisissez %temp% sur la barre d'adresse.
2. Naviguez jusqu'au dossier **hp\ucmdb-dm**.
3. Ouvrez le fichier **ini** dans un éditeur de texte et ajoutez la propriété suivante sur la dernière ligne du fichier :

   –Ddebug.mode=true

4. Utilisez **%temp%\HP\ucmdb-dm\ucmdb-dm.exe** pour exécuter le Gestionnaire de déploiement.

Accès à Configuration Manager - Résolution des problèmes et limitations

Limitations

➤ Chaque fois que l'heure est modifiée sur le serveur tomcat Configuration Manager, il doit être redémarré pour mettre à jour l'heure du serveur.

Résolution des problèmes

Problème. Après avoir modifié le jeu de configurations dans **Système** > **Paramètres** , le serveur ne démarre pas.

Solution. Rétablissez le jeu de configurations précédent. Procédez comme suit :

1. Exécutez la commande suivante pour rechercher l'ID du dernier jeu de configurations activé :

   <répertoire d'installation de Configuration Manager >\bin\export-cs.bat <propriétés de la base de données> --history

où <**propriétés de la base de données**> peut être spécifié en pointant sur l'emplacement du <**répertoire d'installation de Configuration Manager** >**\conf\database.properties** ou en spécifiant la propriété de chaque base de données. Par exemple :

```
cd <répertoire d'installation de Configuration Manager >\bin export-cs.bat -p ..\conf\database.properties --history
```

2 Exécutez la commande suivante pour exporter le dernier jeu de configurations :

```
<répertoire d'installation de Configuration Manager >\bin\export-cs.bat <propriétés de la base de données> <ID jeu de configurations> <nom de fichier de vidage>
```

où <**ID jeu de configurations**> est l'ID du jeu de configurations de l'étape précédente et <**fichier de vidage**> le nom d'un fichier temporaire utilisé pour enregistrer le jeu de configurations. Par exemple, pour exporter un jeu de configurations à l'aide de l'ID **491520** dans le fichier **mydump.zip**, entrez la commande suivante :

```
cd <répertoire d'installation de Configuration Manager >\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip
```

3 Arrêtez le service Configuration Manager.

4 Exécutez la commande suivante pour importer et activer le jeu de configurations précédent :

```
<répertoire d'installation de Configuration Manager >\bin\import-cs.bat <propriétés de la base de données> -i <nom du fichier de vidage> --activate
```

Problème. La connexion UCMDB comporte une erreur.

Solution. La cause peut être l'une des suivantes :

- Le serveur UCMDB est arrêté. Redémarrez Configuration Manager une fois qu'UCMDB est entièrement activé (vérifiez que l'état du serveur UCMDB est **Activé**).
- Le serveur UCMDB est activé, mais les informations d'identification de la connexion à Configuration Manager ou l'URL sont erronées. Démarrez Configuration Manager. Sélectionnez **Système** > **Paramètres** > **Intégrations** > **UCMDB Foundation** > **UCMDB Foundation**, modifiez les paramètres et enregistrez le nouveau jeu de configurations. Activez le jeu de configurations et redémarrez le serveur.

Problème. Les paramètres de connexion LDAP sont erronés.

Solution. Rétablissez le jeu de configurations précédent. Définissez les paramètres de connexion LDAP appropriés et activez le nouveau jeu de configurations.

Problème. Les modifications appliquées au modèle de classe UCMDB ne sont pas détectées dans Configuration Manager.

Solution. Redémarrez le serveur Configuration Manager.

Problème. Le journal Configuration Manager contient une erreur **UCMDB Délai d'exécution expiré**.

Solution. Cela se produit lorsque la base de données UCMDB est surchargée. Pour remédier à ce problème, augmentez le délai de connexion comme suit :

1. Créez un fichier jdbc.properties dans le dossier **UCMDBServer\conf**.
2. Entrez le texte suivant : QueryTimeout=<nombre de secondes>.
3. Redémarrez le serveur UCMDB.

Problème. Configuration Manager n'autorise pas l'ajout d'une vue à gérer.

Solution. Lorsqu'une vue est ajoutée pour être gérée, un nouveau TQL est créé dans UCMDB. Si la limite maximale des TQL actifs est atteinte, la vue ne peut pas être ajoutée. Augmentez la limite des TQL actifs dans UCMDB en modifiant les paramètres suivants dans le Gestionnaire des paramètres d'infrastructure :

- Nombre max de TQL actifs dans le serveur
- Nombre max de TQL actifs client

Problème. Le certificat du serveur HTTPS n'est pas valide.

Solution. La cause peut être l'une des suivantes :

- La date de validation du certificat est obsolète. Vous devez obtenir un nouveau certificat.
- L'autorité de certification du certificat n'est pas une autorité approuvée. Ajoutez l'autorité de certification à votre liste Autorité de certification racine approuvée.

Problème. Lors de la connexion à partir de la page de connexion Configuration Manager, vous obtenez une erreur de connexion ou une page de refus d'accès.

Solution. La cause peut être l'une des suivantes :

- Le nom d'utilisateur n'est peut-être pas défini dans le fournisseur d'authentification (LDAP externe/partagé). Ajoutez l'utilisateur dans le système du fournisseur d'authentification.
- L'utilisateur est défini, mais ne dispose pas d'autorisation de connexion à Configuration Manager. Octroyez l'autorisation de connexion utilisateur. La meilleure pratique est d'attribuer une autorisation de connexion au groupe racine de tous les utilisateurs de Configuration Manager.
- Ces solutions ne s'appliquent qu'en cas d'échec de la connexion provenant d'une connexion système IDM.

Problème. Le serveur Configuration Manager ne démarre pas en raison d'informations d'identification de base de données erronées.

Solution. Si vous modifiez les informations d'identification de base de données et que le serveur ne démarre pas, ces informations sont peut-être erronées. (**Remarque** : L'Assistant Post-Installation ne teste pas automatiquement les informations d'identification entrées. Vous devez cliquer sur le bouton **Test** de l'Assistant.) Vous devez chiffrer à nouveau le mot de passe de la base de données et entrer de nouvelles informations d'identification dans le fichier de configuration. Procédez comme suit :

1. Sur la ligne de commande, exécutez la commande suivante pour chiffrer le mot de passe de base de données mis à jour :

   <répertoire d'installation de Configuration Manager >\bin\encrypt-password.bat –p <mot de passe>

   qui renvoie le mot de passe chiffré.

2. Copiez le mot de passe chiffré (notamment le préfixe {ENCRYPTED}), dans le paramètre **db.password** du **<dossier d'installation de Configuration Manager>\conf\database.properties**.

Problème. Si le DNS n'est pas correctement configuré, vous pouvez peut-être vous connecter à l'aide de l'adresse IP du serveur. Lors de la saisie de l'adresse IP, une seconde erreur DNS se produit.

Solution. Remplacez à nouveau le nom de l'ordinateur par l'adresse IP. Par exemple :

Si vous vous connectez à l'aide de l'adresse IP suivante :
http://16.55.245.240:8180/cnc/

et que vous obtenez une adresse contenant le nom de l'ordinateur indiquant une erreur DNS, telle que :
http://mon.exemple.com:8180/bsf/secure/authenicationPointURL.jsp...

remplacez-la par :
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

et relancez l'application dans le navigateur.

Problème. Le serveur tomcat Configuration Manager ne démarre pas.

Solution. Essayez l'une des solutions suivantes :

- Exécutez l'Assistant Post-Installation et remplacez les ports du serveur Configuration Manager.
- Abandonnez l'autre procédure qui occupe les ports Configuration Manager.
- Modifiez manuellement les ports des fichiers de configuration Configuration Manager en éditant le fichier suivant : **<dossier d'installation de Configuration Manager >\servers\server-0\conf\server.xml** et en mettant à jour les ports appropriés :
  - HTTP (8080) : ligne 69
  - HTTPS (8443) : lignes 71, 90

Problème. Vous recevez un message "mémoire insuffisante".

Solution. Pour modifier les paramètres de démarrage du serveur, procédez comme suit :

1. Exécutez le fichier de commandes suivant :

   <répertoire d'installation de Configuration Manager>/bin/edit-server-0.bat

2. Modifiez les paramètres suivants :

   -Dapplication.ms=<taille initiale du pool de mémoire>
   -Dapplication.ms=<taille maximale du pool de mémoire>

Problème. Il s'est déroulé un long délai pour que l'Assistant Post-installation réagisse après avoir cliqué **Terminer**.

Solution. Pour un système UCMDB non préconfiguré pour le mode consolidé, la consolidation du schéma peut être longue (dépend du volume de données). Attendez 15 minutes. Si aucune progression n'est détectée, abandonnez l'Assistant Post-Installation et relancez la procédure.

Problème. Les modifications apportées aux CI d'UCMDB ne sont pas reflétées dans Configuration Manager.

Solution. Configuration Manager exécute une procédure d'analyse asynchrone hors connexion. La procédure n'a peut-être pas encore traité les dernières modifications apportées à UCMDB. Pour résoudre ce problème, essayez l'une des solutions suivantes :

- Attendez quelques minutes. L'intervalle par défaut entre les exécutions de la procédure d'analyse est de 10 minutes. Il peut être configuré dans **Système** > **Paramètres**.
- Exécutez un appel JMX pour effectuer le calcul de l'analyse hors connexion sur la vue appropriée.
- Sélectionnez **Administration** > **Politiques** > **Politiques de configuration**. Cliquez sur le bouton **Recalculer l'analyse de la politique**. La procédure d'analyse hors connexion est appelée pour toutes les vues (peut prendre un certain temps). Vous pouvez également apporter une modification artificielle à une politique et la sauvegarder.

Problème. Lorsque vous cliquez sur **Administration** > **UCMDB Foundation**, la page de connexion UCMDB s'affiche.

Solution. Pour accéder à UCMDB sans vous reconnecter, vous devez activer la connexion unique. Pour plus d'informations, voir "SSO (Single Sign-On)", page 74. Par ailleurs, vérifiez que l'utilisateur Configuration Manager connecté est défini dans le système de gestion des utilisateurs UCMDB.

Problème. Lors de la configuration d'une connexion UCMDB dans l'Assistant Post-Installation vers une adresse IPv6, l'option de menu **Administration** > **UCMDB Foundation** ne fonctionne pas.

Solution. Procédez comme suit :

1. Sélectionnez **Système** > **Paramètres** > **Intégrations** > **UCMDB Foundation** > **UCMDB Foundation**.
2. Ajoutez des crochets à l'adresse IP dans l'URL d'accès UCMDB. L'URL doit avoir le format suivant : http://[x:x:x:x:x:x:x:x]:8080/.
3. Enregistrez le jeu de configurations et activez-le.
4. Redémarrez Configuration Manager.

LW-SSO - Résolution des problèmes et limitations

Problèmes connus

Cette section décrit les problèmes connus en matière d'authentification LW-SSO.

- **Contexte de la sécurité.** Le contexte de la sécurité LW-SSO ne prend en charge qu'une valeur d'attribut par nom d'attribut.

  Par conséquent, lorsque le jeton SAML2 envoie plusieurs valeurs pour le même nom d'attribut, une seule valeur est acceptée par l'infrastructure LW-SSO.

  De même, si le jeton IdM est configuré pour envoyer plusieurs valeurs pour le même nom d'attribut, une seule valeur est acceptée par l'infrastructure LW-SSO.

- **Fonctionnalité de déconnexion multi-domaines dans Internet Explorer 7**. La fonctionnalité de déconnexion multi-domaines peut échouer dans les conditions suivantes :

  - Le navigateur utilisé est Internet Explorer 7 et l'application appelle plus de trois verbes de redirection HTTP 302 consécutifs dans la procédure de déconnexion.

  Dans ce cas, Internet Explorer 7 risque de ne pas interpréter correctement la réponse de redirection HTTP 302 et afficher une page d'erreur **Internet Explorer ne peut pas afficher la page Web**.

  Pour contourner le problème, il est recommandé, si possible, de réduire le nombre de commandes de redirection de l'application dans la séquence de déconnexion.

Limitations

Notez les limitations suivantes lors de l'authentification LW-SSO :

- **Accès client à l'application**.

  Si un domaine est défini dans la configuration LW-SSO :

  - Les clients de l'application doivent accéder à l'application à l'aide d'un nom de domaine complet (FQDN) dans l'URL de connexion, par exemple, http://monserveur.**domaineentreprise**.com/AppWeb.
  - LW-SSO ne peut pas prendre en charge les URL contenant une adresse IP, par exemple, http://192.168.12.13/WebApp.
  - LW-SSO ne peut pas prendre en charge les URL ne contenant pas de domaine, http://monserveur/AppWeb.

  Si un domaine n'est pas défini dans la configuration LW-SSO : Le client peut accéder à l'application sans FQDN dans l'URL de connexion. Dans ce cas, un cookie de session LW-SSO est créé spécifiquement pour un seul ordinateur sans informations de domaine. Par conséquent, le cookie n'est pas délégué par le navigateur à un autre navigateur, et ne transmet pas aux autres ordinateurs situés dans le même domaine DNS. Cela signifie que LW-SSO ne fonctionne pas dans le même domaine.

- **Intégration de l'infrastructure LW-SSO.** Les applications peuvent influencer et utiliser les fonctionnalités LW-SSO uniquement si elles sont pré-intégrées dans l'infrastructure LW-SSO.

- **Prise en charge multi-domaines**.

  - La fonctionnalité multi-domaines repose sur un point d'accès HTTP. Par conséquent, LW-SSO prend en charge les liens d'une application vers une autre et non pas la saisie d'une URL dans une fenêtre de navigateur, sauf si les applications partagent le même domaine.
  - Le premier lien croisé de domaine qui utilise **HTTP POST** n'est pas pris en charge.

La fonctionnalité multi-domaines ne prend pas en charge la première demande **HTTP POST** d'une seconde application (seule la demande **HTTP GET** est prise en charge). Par exemple, si votre application comporte un lien HTTP vers une seconde application, une demande **HTTP GET** est prise en charge, mais une demande **HTTP FORM** ne l'est pas. Toutes les demandes émises après la première peuvent être **HTTP POST** ou **HTTP GET**.

- Taille du jeton LW-SSO :

  Le volume des informations que LW-SSO peut transférer d'une application d'un domaine vers une autre application d'un autre domaine est limité à 15 Groupes/Rôles/Attributs (notez que chaque élément peut contenir en moyenne 15 caractères).

- Liaison d'une page protégée (HTTPS) à une page non protégée (HTTP) dans une configuration multi-domaines :

  La fonctionnalité multi-domaines ne fonctionne pas pour la liaison d'une page protégée (HTTPS) à une page non protégée (HTTP). Il s'agit d'une limitation du navigateur où l'en-tête du point d'accès n'est pas envoyé lors de la liaison à partir d'une ressource protégée à une ressource non protégée. Pour un exemple, voir : http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- **Jeton SAML2**

  - La fonctionnalité de déconnexion n'est pas prise en charge lorsque le jeton SAML2 est utilisé.

    Par conséquent, si le jeton SAML2 est utilisé pour accéder à une seconde application, un utilisateur qui se déconnecte de la première application ne l'est pas de la seconde.

  - Le délai d'expiration du jeton SAML2 n'est pas reflété dans la gestion de session de l'application.

    Par conséquent, si le jeton SAML2 est utilisé pour accéder à une seconde application, la gestion de chaque session de l'application est traitée de manière indépendante.

- **Domaine JAAS.** Le domaine JAAS de Tomcat n'est pas pris en charge.

- **Utilisation d'espaces dans les répertoires Tomcat.** L'utilisation d'espaces dans les répertoires Tomcat n'est pas prise en charge.

Il n'est pas possible d'utiliser LW-SSO lorsqu'un chemin d'installation Tomcat (dossiers) inclut des espaces (par exemple, Program Files) et que le fichier de configuration LW-SSO est situé dans le dossier Tomcat **common\classes**.

➤ **Configuration du processus d'équilibrage de la charge.** Un processus d'équilibrage de la charge déployé avec LW-SSO doit être configuré pour utiliser des sessions permanentes.

Résolution des problèmes

Problème : Un cookie LW-SSO n'est pas créé après la connexion.

➤ **Cause possible :** Un domaine non vide n'est pas correctement défini dans l'élément LW-SSO de la configuration.

➤ **Cause possible** : Vérifiez que le domaine défini dans l'élément LW-SSO de la configuration est égal au domaine de l'application.

➤ **Cause possible :** Un domaine non vide transmis sous la forme d'un paramètre à la fonction enableSSO est incorrect.

➤ **Cause possible** : Assurez-vous que le domaine transmis en tant que paramètre à la fonction enableSSO est égal au domaine de l'application.

➤ **Cause possible :** Vous n'avez pas accédé à l'application à l'aide du nom de domaine complet (FQDN) dans l'URL de connexion lorsqu'un domaine est défini dans la configuration LW-SSO (par exemple : http://192.168.12.13/WebApp).

➤ **Cause possible** : Assurez-vous de pouvoir accéder à l'application à l'aide du nom de domaine complet (FQDN) dans l'URL de connexion (par exemple : http://monserveur.domainentreprise.com/WebApp).

Problème : LW-SSO n'a pas réussi à créer un cookie pour la fonctionnalité AutoCookieCreation.

➤ **Cause possible :** Un domaine n'est pas correctement défini dans l'élément LW-SSO de la configuration.

➤ **Cause possible** : Vérifiez que le domaine défini dans l'élément LW-SSO de la configuration est égal au domaine de l'application.

Problème : Le jeton LW-SSO n'a pas été validé.

- **Cause possible :** Les deux applications comportent des paramètres initString différents dans l'élément crypto de la configuration (ou d'autres paramètres crypto).
- **Cause possible** : Utilisez le même initString dans les deux applications (en plus de tous les autres paramètres crypto de l'élément de création LW-SSO).
- **Cause possible :** La différence d'heure GMT entre les deux applications est supérieure à 15 minutes.
- **Cause possible** : Assurez-vous que toutes les applications impliquées dans une intégration LW-SSO sont définies sur la même heure GMT avec une différence maximum de 15 minutes.
- **Cause possible :** Un domaine est vide dans l'élément LW-SSO de la configuration et vous accédez à une seconde application d'un autre ordinateur avec le même domaine DNS.
- **Cause possible** : Vérifiez que le domaine défini dans l'élément LW-SSO de la configuration est égal au domaine de l'application.
- **Cause possible :** Un domaine n'est pas défini dans l'élément LW-SSO de la configuration et vous accédez à une seconde application d'un autre ordinateur avec le même domaine DNS.
- **Cause possible** : Ajoutez un domaine à l'élément LW-SSO et assurez-vous que le domaine est défini comme étant égal au domaine de l'application.

Problème : LW-SSO n'a pas réussi à valider le jeton LW-SSO dans un environnement multi-domaines

- **Cause possible :** Dans la configuration de l'une des applications, un domaine n'est pas correctement défini dans l'élément LW-SSO.
- **Cause possible** : Le domaine défini dans l'élément LW-SSO de la configuration de l'application doit être identique à celui de l'application selon les domaines réels utilisés.
- **Cause possible :** Dans la configuration de l'une des applications, un domaine n'est pas correctement défini dans les paramètres trustedHosts (ou les paramètres protectedDomains).

- **Cause possible** : Vérifiez que les domaines des paramètres trustedHosts (ou des paramètres protectedDomains) des configurations de toutes les applications sont correctement définis.
- **Cause possible :** Le cookie de session LW-SSO est bloqué ou refusé lors de l'utilisation d'Internet Explorer 6.x, 7.x ou 8.x.
- **Cause possible** : Ajoutez tous les serveurs LW-SSO à la zone "Intranet"/"Approuvé" dans les zones de sécurité Internet Explorer de votre ordinateur (Outils > Options Internet > Sécurité > Intranet local > Sites > Avancé). Tous les cookies seront ainsi acceptés.
- **Cause possible :** Des applications comportent des paramètres initString différents dans l'élément crypto de la configuration (ou d'autres paramètres crypto).
- **Cause possible** : Utilisez le même initString dans toutes les applications (en plus de tous les autres paramètres crypto de l'élément de création LW-SSO).
- **Cause possible :** Des applications comportent une différence d'heure GMT supérieure à 15 minutes.
- **Cause possible** : Assurez-vous que toutes les applications impliquées dans une intégration LW-SSO sont définies sur la même heure GMT avec une différence maximum de 15 minutes.
- **Cause possible :** Un lien multi-domaines relie la ressource protégée (HTTPS) à la ressource non protégée (HTTP).
- **Cause possible** : Lors de la liaison ou du passage d'un domaine à un autre, assurez-vous que la première demande de lien/passage passe d'une ressource protégée (HTTPS) à une autre ressource protégée (HTTPS).

Prise en charge IPv6 - Résolution des problèmes et limitations

Limitations

- L'URL ne peut pas contenir une adresse IP.
- Le système d'exploitation doit prendre en charge IPv6 et IPv4. Vous ne pourrez pas vous connecter au serveur Configuration Manager si l'adresse IPv4 n'est pas fermée ou n'est pas prise en charge.
- Chaque fois que l'heure est modifiée sur le serveur tomcat Configuration Manager, celui-ci doit être redémarré pour que son heure soit mise à jour.

Résolution des problèmes

Problème. Après la configuration d'une connexion UCMDB en fonction d'une adresse IPv6 lors de l'installation, l'option de menu **Administration** > **UCMDB Foundation** ne fonctionne pas.

Solution. Procédez comme suit :

1. Sélectionnez **Système** > **Paramètres** > **Intégrations** > **UCMDB Foundation** > **UCMDB Foundation**.
2. Ajoutez des crochets à l'adresse IP dans le champ de l'URL d'accès UCMDB. L'URL doit avoir le format suivant : http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/.
3. Enregistrez le jeu de configurations et activez-le.
4. Redémarrez Configuration Manager.

Authentification - Résolution des problèmes et limitations

Cette section décrit les problèmes connus liés à l'authentification.

Problème : Pendant l'authentification dans une application après la redirection vers un point d'authentification, vous recevez l'erreur 500.

- **Cause possible :** Les composants WAR et BSF WAR de Configuration Manager comportent des paramètres initString différents dans l'élément crypto de la configuration (ou d'autres paramètres crypto).
- **Cause possible :** Utilisez le même initString dans les deux applications (en plus de tous les autres paramètres crypto de l'élément de création LW-SSO).

Problème : Pendant l'authentification dans une application après la redirection vers un point d'authentification, vous ne pouvez pas afficher le formulaire de connexion.

Solution : Le cookie de la session d'authentification de Configuration Manager est bloqué ou refusé lors de l'utilisation des navigateurs Internet Explorer version 6.0, 7.0 ou 8.0. Ajoutez le serveur Configuration Manager dans la zone **Intranet/Approuvé** des zones de sécurité Internet Explorer de votre ordinateur (**Outils** > **Options Internet** > **Sécurité** > **Intranet local** > **Sites** > **Avancé**). Tous les cookies seront ainsi acceptés.

Problème : Après l'authentification, vous recevez l'erreur 403.

- **Cause possible :** Un domaine n'est pas correctement défini dans l'élément LW-SSO de la configuration de l'application.
- **Cause possible :** Vérifiez que le domaine défini dans l'élément LW-SSO de la configuration de l'application est égal au domaine de l'application.
- **Cause possible :** Vous n'avez pas accédé à l'application à l'aide du nom de domaine complet (FQDN) dans l'URL de connexion lorsqu'un domaine est défini dans la configuration LW-SSO (par exemple : http://192.168.12.13/WebApp).
- **Cause possible :** Assurez-vous de pouvoir accéder à l'application à l'aide du nom de domaine complet (FQDN) dans l'URL de connexion (par exemple : http://monserveur.domainentreprise.com/WebApp).

Problème : Après l'authentification, la page **Obtenir les détails de l'utilisateur Acegi** s'affiche.

Solution : Le cookie de la session d'authentification de Configuration Manager est bloqué ou refusé lors de l'utilisation des navigateurs Internet Explorer version 6.0, 7.0 ou 8.0. Ajoutez le serveur Configuration Manager dans la zone **Intranet/Approuvé** des zones de sécurité Internet Explorer de votre ordinateur (**Outils** > **Options Internet** > **Sécurité** > **Intranet local** > **Sites** > **Avancé**). Tous les cookies seront ainsi acceptés.