



A MITEL
PRODUCT
GUIDE

Mitel OpenScape Contact Center Agile V12

Guide de Gestion du Système

Guide de Gestion du Système

Documentation de service

10/2024

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel"), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively "Unify") or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Sommaire

| | |
|---|-----------|
| 1 A propos de ce guide | 5 |
| 1.1 A qui ce guide est-il destiné ? | 5 |
| 1.2 Conventions de formats | 5 |
| 1.3 Commentaires sur la documentation | 6 |
| 2 Configuration d'un panneau mural | 7 |
| 2.1 Avant de commencer | 7 |
| 2.2 Configuration de la connexion IP pour un panneau mural | 7 |
| 3 Configuration du serveur email d'entreprise | 9 |
| 3.1 Exigences du serveur email d'entreprise | 9 |
| 3.2 Planification du déploiement de Microsoft Office 365 | 10 |
| 3.3 Planification du déploiement de Google G Suite | 11 |
| 3.4 Planification du déploiement de Microsoft Exchange | 11 |
| 3.4.1 Spécification des en-têtes personnalisés (Microsoft Exchange Server 2007, 2010 et 2013 seulement) | 13 |
| 3.5 Planification du déploiement d'IBM Lotus Domino | 14 |
| 3.5.1 Compression de la base de données | 15 |
| 3.6 Configuration d'une connexion sécurisée pour un serveur emails | 16 |
| 3.7 Utilisation de l'authentification sur un serveur email | 16 |
| 3.8 Prise en charge de la fonction Envoyer des rapports par email | 17 |
| 4 Configuration du serveur Web d'entreprise | 19 |
| 4.1 Exigences du système l'utilisation des composants Web | 19 |
| 4.1.1 Exigences du serveur Web d'entreprise | 19 |
| 4.1.2 Exigences du navigateur Web | 20 |
| 4.2 Configuration des composants Web | 20 |
| 4.2.1 Configuration d'un serveur IIS | 20 |
| 4.2.2 Configuration d'un serveur Tomcat | 23 |
| 4.2.3 Configuration d'un Sun Java System Web Server | 25 |
| 4.3 Configuration d'une connexion sécurisée pour un serveur Web | 28 |
| 4.3.1 Activation de la sécurité TLS sur un serveur IIS | 29 |
| 4.3.2 Activation TLS sur un serveur Tomcat ou Sun Java | 29 |
| 4.4 Codes d'erreurs des rappels Web | 30 |
| 5 Configuration de l'intégration de présence | 33 |
| 5.1 Configuration d'un compte utilisateur de l'application OpenScape UC | 33 |
| 5.2 Configuration de l'annuaire externe LDAP | 34 |
| 6 Maintenance du système | 35 |
| 6.1 Arrêt d'un ordinateur serveur pour la maintenance du système | 35 |
| 6.2 Modification des mots de passe pour OpenScape Contact Center et Informix | 36 |
| 6.3 Sauvegarde de la base de données | 37 |
| 6.3.1 Planification d'une sauvegarde de la base de données | 38 |
| 6.3.2 Sauvegarde de la base de données en utilisant l'utilitaire ontape | 40 |
| 6.3.3 Restauration de la base de données en utilisant l'utilitaire ontape | 42 |
| 6.3.4 Restauration d'une sauvegarde de niveau zéro effectuée en utilisant l'utilitaire ontape | 44 |
| 6.3.5 Sauvegarde de la base de données en utilisant l'utilitaire onbar | 44 |
| 6.3.6 Restauration de la base de données en utilisant l'utilitaire onbar | 45 |
| 6.4 Prise en charge de SNMP | 46 |

Sommaire

6.4.1 OpenScape Contact Center SNMP Extension Agent 46

6.4.2 Logiciel OpenScape CAP Fault Management 47

Index49

1 A propos de ce guide

Ce guide décrit comment configurer le matériel de fournisseur tiers, comme les panneaux muraux, les serveurs email et Web d'entreprise, afin de les intégrer au système Unify OpenScape Contact Center Agile V11 R1. Il décrit aussi comment procéder à la maintenance continue du système Unify OpenScape Contact Center Agile V11 R1, y compris la sauvegarde et la restauration de la base de données.

1.1 A qui ce guide est-il destiné ?

Ce guide est destiné aux utilisateurs internes à l'organisation qui sont responsables de la gestion, de la surveillance et du maintien de l'intégrité du système Unify OpenScape Contact Center Agile V11 R1.

1.2 Conventions de formats

Les conventions de formats utilisées dans ce guide sont les suivantes :

Gras

Identifie les composants Unify OpenScape Contact Center Agile V11 R1, les titres des fenêtres et des boîtes de dialogue et les noms d'éléments.

Italique

Cette police identifie les références à une documentation connexe.

`Police monospace`

Caractérise la police du texte que vous entrez ou que l'ordinateur affiche dans un message.

REMARQUE : Les remarques soulignent des informations qui sont utiles sans être essentielles, par exemple, des conseils ou d'autres méthodes pour exécuter une tâche.

IMPORTANT : Les remarques importantes sont destinées à attirer l'attention sur des actions qui pourraient entraver le bon fonctionnement de l'application ou entraîner une perte de données.

A propos de ce guide

Commentaires sur la documentation

1.3 Commentaires sur la documentation

Pour signaler un problème avec ce document, veuillez appeler le centre de support clientèle.

Quand vous appelez, veuillez avoir l'obligeance d'inclure les informations suivantes. Ceci nous aidera à repérer le document qui vous pose problème.

- **Titre** : Guide de Gestion du Système
- **Référence** : A31003-S22B1-S101-01-7720

2 Configuration d'un panneau mural

Ce chapitre décrit comment configurer un panneau mural. Un panneau mural est un panneau de message électronique qui affiche une vue défilante de données statistiques en temps réel et ainsi que des informations générales du système sur le centre de contacts à plusieurs utilisateurs à la fois. Le système OpenScape Contact Center prend en charge les panneaux muraux Spectrum IP, version 4200 R, ainsi que le panneau mural personnalisé qui adhère au protocole EZ Code II.

IMPORTANT : La configuration du panneau mural ne doit être confiée qu'à du personnel qualifié ayant reçu la formation adéquate. Toute tentative de configuration d'un panneau mural par du personnel n'ayant pas reçu la formation pertinente peut être néfaste au bon fonctionnement du système OpenScape Contact Center.

2.1 Avant de commencer

Avant d'installer et de configurer le panneau mural, vous devez :

- Si vous avez un panneau mural série Spectrum, il vous faut un kit de conversion série-IP (NIU aux États-Unis et UDS100 pour le marché international).
- Obtenez une adresse IP fixe pour le panneau mural.
- Vérifiez que vous disposez des versions des microprogrammes compatibles avec le système OpenScape Contact Center.

2.2 Configuration de la connexion IP pour un panneau mural

Cette procédure décrit comment configurer la connexion IP pour un panneau mural. Vous devez au préalable avoir installé l'utilitaire de configuration Lantronix Device Server V2.0 sur l'ordinateur serveur principal OpenScape Contact Center pour le panneau mural.

IMPORTANT : Seule la marche à suivre pour la configuration est indiquée. Pour des instructions et les précautions détaillées, voir la documentation du fournisseur.

Configuration d'un panneau mural

Configuration de la connexion IP pour un panneau mural

Pour configurer la connexion IP pour un panneau mural :

1. Connectez le panneau mural au réseau local.
2. Démarrez l'utilitaire Lantronix Device Server Configuration.
3. Dans le menu **File**, cliquez sur **Search Network**.
4. Voici comment rechercher le réseau pour un panneau existant :
 - a) Cliquez sur **Start Search**.
 - b) Une fois que le ou les panneaux muraux ont été localisés sur le réseau, cliquez sur **Enregistrer**.
 - c) Lorsque le système vous informe que les dispositifs ont été enregistrés, cliquez sur **OK**.
 - d) Cliquez sur **Back**.
5. Sélectionnez l'adresse IP du panneau mural à configurer.
6. Dans le menu **Tools**, cliquez sur **Device Manager**.
7. Cliquez sur **Web Configuration**.
8. Cliquez sur **OK**. Ceci lance Lantronix Web-Manager.
9. Sous **Dedicated Connection**, entrez le numéro de port du panneau mural dans la case **Local Port**, puis cliquez sur **Update Settings**.

REMARQUE : Pour configurer un nouveau panneau n'ayant pas encore d'adresse IP, dans le menu **Outils**, cliquez sur **Assign IP Address**. Recherchez l'adresse matérielle ou Ethernet à l'arrière du panneau mural, puis saisissez-la dans le champ correspondant. Affecter le panneau mural à une adresse IP, puis cliquez sur **Set IP Address**.

3 Configuration du serveur email d'entreprise

Ce chapitre décrit comment configurer le serveur email d'entreprise pour la prise en charge de la fonction des emails OpenScape Contact Center et l'envoi par email des rapports. Les messages email envoyés par les clients sont acheminés par le serveur email d'entreprise au serveur emails OpenScape Contact Center. Tous les messages email sont stockés dans une seule boîte de réception sur le serveur email d'entreprise.

Le serveur emails OpenScape Contact Center et le serveur email d'entreprise communiquent en utilisant le protocole IMAP4. Les applications client OpenScape Contact Center et le serveur email d'entreprise utilisent aussi le protocole IMAP4 pour récupérer et traiter les messages email. Les pièces jointes aux messages sont récupérées en utilisant des fonctions IMAP4 et MIME séparées. Les messages email de réponse sont envoyés aux clients par le serveur emails en utilisant une interface SMTP.

REMARQUE : Dans l'application Manager, le serveur principal d'entreprise est utilisé pour envoyer des rapports aux superviseurs et pour le processus keep-alive

3.1 Exigences du serveur email d'entreprise

Les serveurs email d'entreprise qui ont été testés conjointement au système OpenScape Contact Center sont les suivants :

- Microsoft Office 365
- Microsoft Exchange Server 2007, 2010 et 2013
- IBM Lotus Domino 8.0, 8.5 et 9

Pour plus informations sur ces serveurs, voir la documentation du fabricant.

REMARQUE : Nous recommandons de protéger le contenu du serveur email d'entreprise afin de réduire le risque de suppression par inadvertance de messages email.

Assurez-vous que le serveur email d'entreprise est configuré de la façon suivante :

- **Licences d'accès client** – Vérifiez que vous disposez d'un nombre suffisant de licences d'accès client. Chaque utilisateur pouvant accéder au serveur email OpenScape Contact Center exige une licence d'accès client.

Configuration du serveur email d'entreprise

Planification du déploiement de Microsoft Office 365

- **En-têtes personnalisés** – La fonctionnalité d'email de OpenScape Contact Center utilise des en-têtes personnalisés afin que le serveur email d'entreprise ne filtre pas ou ne supprime pas les en-têtes des messages email.
- **Sessions IMAP** – Une session IMAP est nécessaire pour chaque jour auquel des messages actifs sont associés. Chaque utilisateur a besoin d'une session IMAP lorsqu'il envoie un message e-mail ou lorsqu'il recherche le contenu d'un message e-mail.
- **Connexions simultanées** – Vérifiez que le compte email OpenScape Contact Center a été configuré avec un nombre suffisant de connexions pour supporter le nombre d'utilisateurs qui accéderont simultanément au compte.
- **Filtrage des spams et blocage des adresses emails** – Ceci empêche les messages email non désirés d'être acheminés vers les utilisateurs.
- **Logiciel de vérification des virus** – Les messages email entrants et les pièces jointes du serveur email d'entreprise doivent être analysés.

3.2 Planification du déploiement de Microsoft Office 365

Vous devez planifier soigneusement le déploiement de Microsoft Office 365. Quand vous configurez la période de conservation des messages dans le serveur email OpenScape Contact Center, n'oubliez pas de tenir compte de la disponibilité de la base de données Microsoft Office 365. Pour plus d'informations sur ce sujet et sur d'autres tâches décrites dans cette partie, il faut évaluer le contrat avec Microsoft Office 365.

Vous devez effectuer les configurations suivantes :

- **Comptes d'utilisateurs** – Crée un nouveau compte d'utilisateur que le serveur email OpenScape Contact Center utilisera. Vous devez spécifier un mot de passe pour le nouveau compte d'utilisateur.
- **Stratégie de limitation** – Microsoft Office 365 comporte une stratégie de limitation qui limite le taux de messages SMTP à un maximum de 30 messages/minute. Afin de se conformer à cette limitation, le paramètre OSCC Limite de taux de messages des réglages e-mail doit être réglé sur 30 (ou moins).
- **Sessions IMAP** – Microsoft Office 365 limite le nombre de sessions IMAP actives à 20 sessions par compte. Afin de fonctionner en respectant cette limitation, le paramètre OSCC Sessions IMAP maximum des réglages e-mail doit être réglé sur 20.

3.3 Planification du déploiement de Google G Suite

Vous devez planifier soigneusement le déploiement de Google G Suite. Quand vous configurez la période de conservation des messages dans le serveur email OpenScape Contact Center, n'oubliez pas de tenir compte de la disponibilité de la base de données Google G Suite. Pour plus d'informations sur ce sujet et sur d'autres tâches décrites dans cette partie, il faut évaluer le contrat avec Google G Suite.

Vous devez exécuter les configurations suivantes :

Dans Google G Suite :

- Créez un nouveau compte d'utilisateur GMail que le serveur email OpenScape Contact Center utilisera.
- Dans les paramètres de GMail, dans l'onglet « Transfert et POP/IMAP », assurez-vous qu'« Accès IMAP » est activé.
- Dans les paramètres de sécurité du compte Google :
 - créez un « mot de passe d'application » et utilisez-le dans OpenScape Contact Center.
 - activez l'option « Accès moins sécurisé des applications »

Dans OpenScape Contact Center :

- **Sessions IMAP** - Google G Suite limite le nombre de sessions IMAP actives à 15 sessions par compte. Pour opérer selon cette limitation, le paramètre de l'OSCC **Sessions IMAP maximum dans les Paramètres des emails** doit être établi à 15. 5 de ces sessions sont réservées au serveur email OSCC.

3.4 Planification du déploiement de Microsoft Exchange

Vous devez planifier soigneusement le déploiement de Microsoft Exchange. Quand vous configurez la période de conservation des messages dans le serveur email OpenScape Contact Center, n'oubliez pas de tenir compte de la taille de la base de données Microsoft Exchange. Pour plus d'informations sur cette tâche et d'autres tâches décrites dans cette section, voir la documentation Microsoft Exchange.

IMPORTANT : La configuration de Microsoft Exchange ne doit être effectuée que par un administrateur maîtrisant parfaitement Microsoft Exchange.

Configuration du serveur email d'entreprise

Planification du déploiement de Microsoft Exchange

Vous devez effectuer les configurations suivantes :

- **Comptes d'utilisateurs** – Crée un nouveau compte d'utilisateur que le serveur email OpenScape Contact Center utilisera. Vous devez spécifier un mot de passe pour le nouveau compte d'utilisateur.
- **Alias (facultatif)** – Si ce paramètre est requis, configurez des adresses emails SMTP supplémentaires qui seront utilisées en tant qu'alias pour le nouveau compte d'utilisateur.

Si vous souhaitez présenter plusieurs adresses emails de contact à vos clients, vous devez configurer des alias pour chaque adresse email supplémentaire qui renvoie au nouveau compte de l'utilisateur. La création d'un alias garantit que des messages email envoyés au serveur email d'entreprise sont acheminés à la boîte aux lettres du serveur des emails de OpenScape Contact Center pour la gestion des agents. Pour obtenir de plus amples d'informations, voir l'*Aide de Manager*.

Comme Microsoft Exchange Server 2007 convertit les alias à l'adresse principale du compte utilisateur à la fois pour les messages d'origines interne et externe, vous devez configurer une boîte de réception des messages Exchange pour chaque alias que vous voulez utiliser, et configurer cette boîte de réception pour qu'elle transfère les messages au compte utilisateur. Ceci permet d'être certain qu'un message email envoyé par un client à un alias, par exemple ventes@company.com, est correctement acheminé. Ce paramétrage permet aussi de vous assurer que l'adresse email entrante n'est pas convertie à l'adresse principale du compte sur la réponse.

- **Stratégie de limitation (Microsoft Exchange Server 2013)** – Lorsque vous utilisez Microsoft Exchange Server 2013, les valeurs ImapMaxBurst et ImapRechargeRate dans la stratégie de limitation peuvent dégrader le débit de transmission des e-mails dans le compte email de l'OpenScape Contact Center. Pour parvenir à un débit maximum, nous vous recommandons de créer une stratégie de limitation spécifique pour le compte e-mail d'OpenScape Contact Center et de régler les valeurs ImapMaxBurst et ImapRechargeRate à 8000000 ou plus.
- **Redondance des clichés instantanés (Microsoft Exchange Server 2013)** – Lorsque vous utilisez Microsoft Exchange Server 2013, la fonctionnalité Redondance des clichés instantanés dans les paramètres de configuration du transport peut dégrader le débit de transmission des emails dans le compte email de l'OpenScape Contact Center. Pour parvenir à un débit maximum, nous vous recommandons de régler le drapeau ShadowRedundancyEnabled sur Faux.

3.4.1 Spécification des en-têtes personnalisés (Microsoft Exchange Server 2007, 2010 et 2013 seulement)

Dans Microsoft Exchange Server 2007, 2010 et 2013, les en-têtes personnalisés exigés par la fonctionnalité email OpenScape Contact Center peuvent ne pas être disponibles par le biais de l'interface IMAP de Microsoft Exchange. Si vous voulez utiliser Microsoft Exchange Server 2007, 2010 ou 2013 en tant que serveur email IMAP d'entreprise, vous devez exécuter un utilitaire (osccmseheaders.exe) qui envoie un message email spécial utilisant l'interface SMTP de Microsoft Exchange. Une fois que le message email spécial a été envoyé, les en-têtes personnalisés requis sont disponibles via l'interface IMAP de Microsoft Exchange.

Avant d'utiliser le programme utilitaire, vous devez effectuer les tâches suivantes :

- Configurer Microsoft Exchange Server pour prendre en charge SMTP authentifié. L'utilitaire utilise une session du SMTP authentifié pour les en-têtes personnalisés. Si cela s'avère nécessaire, vous pouvez désactiver le SMTP authentifié après l'exécution de l'utilitaire.
- Si vous utilisez Microsoft Exchange Server 2007 SP2 ou ultérieur, exécutez la commande suivante de l'Exchange Management Shell sur l'ordinateur Microsoft Exchange Server :

```
Set-TransportConfig -HeaderPromotionModeSetting MayCreate
```

Au besoin, vous pouvez revenir à la valeur antérieure de la propriété HeaderPromotionModeSetting après l'exécution de l'utilitaire.

Pour spécifier des en-têtes personnalisés :

1. Sur l'ordinateur principal, allez jusqu'au dossier où le logiciel OpenScape Contact Center est installé, puis double-cliquez sur **osccmseheaders.exe**. Une fenêtre d'invite de commande s'ouvre.
2. Appuyez sur **ENTRÉE** pour continuer.
3. À l'invite pour **l'adresse d'origine** (From), tapez l'adresse email à utiliser en tant qu'adresse d'origine pour envoyer le message email spécial, puis appuyez sur **ENTRÉE**. Ceci doit être l'adresse email associée au compte d'utilisateur servant à l'authentification avec Microsoft Exchange Server, par exemple le compte OSCCEmail.
4. À l'invite pour **l'adresse de destination** (To), tapez l'adresse email où vous voulez envoyer le message email spécial, puis appuyez sur **ENTRÉE**. Il doit s'agir d'une adresse email connue sur le Microsoft Exchange Server.
5. À l'invite **Subject** (Objet), tapez l'objet du message email spécial, puis appuyez sur **ENTRÉE**.

Configuration du serveur email d'entreprise

Planification du déploiement d'IBM Lotus Domino

6. À l'invite **SMTP server host name** (Nom d'hôte du serveur SMTP), tapez le nom d'hôte de l'ordinateur du Microsoft Exchange Server, puis appuyez sur **ENTRÉE**.
7. À l'invite **SMTP server port number** (Numéro de port du serveur SMTP), tapez le numéro de port qui a été configuré pour SMTP sur l'ordinateur Microsoft Exchange Server, puis appuyez sur **ENTRÉE**.
8. À l'invite **SMTP user name** (Nom d'utilisateur SMTP), tapez le nom d'utilisateur pour le compte Microsoft Exchange Server qui sera utilisé pour envoyer le message email spécial et appuyez sur **ENTRÉE**. Le compte doit pouvoir envoyer un message email spécial en utilisant l'adresse d'origine (From) spécifié à l'étape 3.
9. À l'invite **SMTP password** (Mot de passe SMTP), tapez le mot de passe pour le compte Microsoft Exchange Server qui sera utilisé pour envoyer le message email spécial et appuyez sur **ENTRÉE**.

3.5 Planification du déploiement d'IBM Lotus Domino

Pour que le système OpenScape Contact Center utilise Lotus Domino, vous devez configurer une boîte de réception de courrier compatible IMAP où les messages email seront distribués. Assurez-vous que vous configurez **Format preference for incoming mail** pour la boîte aux lettres à **Prefers MIME**. Pour des informations sur la manière de procéder pour cette tâche et d'autres décrites dans cette section, voir la documentation de Lotus Domino.

IMPORTANT : La configuration Lotus Domino doit être effectuée uniquement par un administrateur Lotus Domino compétent.

Si vous souhaitez présenter plusieurs adresses emails de contact à vos clients, vous devez configurer un alias pour chaque adresse email supplémentaire qui pointe vers une boîte de réception de courrier compatible IMAP. La création d'un alias garantit que des messages email envoyés au serveur email d'entreprise sont acheminés à la boîte aux lettres du serveur des emails de OpenScape Contact Center pour la gestion des utilisateurs. Pour obtenir de plus amples d'informations, voir l'*Aide de Manager*.

Reportez-vous à l'aide de l'administrateur Lotus Domino pour obtenir des informations sur :

- Sécurité pour les alias configurés
- Configuration de l'acheminement SMTP

IMPORTANT : Assurez-vous que vous activez **l'indexage de texte complet immédiat** dans la base de données que vous créez. Si vous n'activez pas l'indexage de texte complet immédiat, les recherches IMAP échoueront et les performances du serveur emails du OpenScape Contact Center en souffriront gravement.

3.5.1 Compression de la base de données

Lorsque vous compactez la base de données Lotus Domino, le serveur emails OpenScape Contact Center identifie le serveur email d'entreprise comme désactivé puisque l'accès IMAP à la base de données est interrompu. Selon le type de compactage de la base de données utilisé, la durée d'accessibilité de la base de données Lotus Domino par le serveur emails OpenScape Contact Center varie. Nous recommandons de sélectionner l'option **In-place compacting with space recovery only** (flag -b). C'est la méthode la plus rapide ayant un impact limité sur votre système.

IMPORTANT : Nous recommandons vivement de compacter la base de données du serveur emails de l'entreprise pendant la maintenance des données de OpenScape Contact Center. Si la maintenance est effectuée à un autre moment, le traitement des messages email peut être affecté défavorablement au sein du système OpenScape Contact Center.

3.6 Configuration d'une connexion sécurisée pour un serveur emails

Pour définir une connexion de sécurité (SSL) entre le serveur email d'entreprise et le serveur emails OpenScape Contact Center, vous devez effectuer les tâches suivantes :

- Installez un certificat SSL et activez la sécurité SSL pour les messages email entrants (IMAP4) et/ou sortants (SMTP) sur l'ordinateur serveur de messagerie de l'entreprise. Suivez les instructions du fabricant ou contactez votre prestataire de messagerie électronique pour assistance.

REMARQUE : Les serveurs Lotus Domino permettent des connexions sécurisées SSL sur un port donné si le port n'est pas configuré pour exiger l'emploi de SSL. Ceci n'entraîne aucun problème de fonctionnement. Toutefois, les administrateurs doivent savoir que, bien que OpenScape Contact Center puisse établir une connexion sécurisée avec le serveur Domino, ceci ne constitue pas une preuve que la sécurité SSL est utilisée pour des connexions établies par d'autres clients emails. Si vous avez besoin d'un environnement Domino sécurisé, vous devez vérifier avec attention si la sécurité est active dans la configuration Domino.

- Activez la sécurité SSL pour le serveur correspondant IMAP et/ou le serveur correspondant SMTP dans l'application Manager. Pour des informations détaillées, voir l'*Aide de Manager*.

Nous vous recommandons d'obtenir le certificat d'une autorité de certification reconnue, par exemple VeriSign, bien que les certificats auto-signés soient également pris en charge. Dans chaque cas, le certificat doit toujours être un certificat approuvé.

Remarque : Lorsque vous utilisez un certificat qui est auto-généré ou généré par une autorité de certification non couverte par un keystore Java installé par défaut, et que vous souhaitez installer un nouveau certificat SSL sur les serveurs d'e-mails corporatifs, il se peut que vous devez ajouter la racine+ certificat intermédiaire dans le keystore du pack Java utilisé par le portail Agent. Le certificat peut Être ajouté au keystore à l'aide de la commande de ligne suivante (depuis <Java>\bin directory):

```
keytool -import -alias <server_fqdn> -keystore  
..\lib\security\cacerts -file <certificate file>
```

3.7 Utilisation de l'authentification sur un serveur email

Dans le système OpenScape Contact Center, l'authentification est obligatoire pour le serveur IMAP et le serveur SMTP en option. Les paramètres d'authentification spécifiés sur le serveur email d'entreprise doivent correspondre à ceux spécifié dans le système OpenScape Contact Center.

Pour activer l'authentification dans Microsoft Exchange :

- Sélectionnez **Authentification de base**.
- Si SSL est activé, veuillez à sélectionner Nécessite le cryptage.

Pour activer l'authentification dans IBM Lotus Domino :

- Le système OpenScape Contact Center n'utilise pas de certificat client. Donc pour les options d'authentification SSL, assurez-vous que l'option **Client certificate** est réglée à **No** et que l'option **Name & password** (Nom et mot de passe) est réglée à **Yes** (Oui).

3.8 Prise en charge de la fonction Envoyer des rapports par email

Pour utiliser la fonction Envoyer des rapports par email, le serveur emails OpenScape Contact Center doit pouvoir envoyer des messages email par le serveur email d'entreprise, en utilisant une adresse De différente de l'adresse De que le serveur emails OpenScape Contact Center utilise pour se connecter au serveur email d'entreprise.

Le but est de permettre au serveur emails OpenScape Contact Center d'envoyer des messages email aux noms des autres comptes d'emails SMTP. Par exemple, quand le serveur emails OpenScape Contact Center est connecté au serveur email d'entreprise en tant que "oscc@entreprise.com" et qu'un message email est envoyé pour le compte de "directeur@entreprise.com", on veut que le destinataire du message voit "De : directeur@entreprise.com, et non pas "De : oscc@entreprise.com pour le compte de directeur@entreprise.com".

Quand le serveur email d'entreprise est configuré pour l'authentification SMTP et que le transfert SMTP est limité, cette fonctionnalité peut être réalisée comme suit :

- **Microsoft Exchange Server 2007, 2010 et 2013** – Si vous avez besoin d'envoyer des messages emails à partir d'adresses emails qui sont dans le même domaine, vous pouvez accorder au compte de serveur email OpenScape Contact Center sur le serveur email d'entreprise l'autorisation complète à chacune des boîtes aux lettres de l'utilisateur OpenScape Contact Center via Active Directory. Vous devez aussi créer un nouveau contact dans l'annuaire actif avec l'adresse email SMTP OSCCEmail@company.com, puis donner l'autorisation d'envoi nécessaire (Envoyer en tant que) au compte email de l'ordinateur serveur OpenScape Contact Center pour le nouveau contact. Pour plus de détails, voir la documentation Microsoft Exchange Server.

Configuration du serveur email d'entreprise

Prise en charge de la fonction Envoyer des rapports par email

- **Microsoft Exchange Server 2007, 2010 et 2013 seulement** – Si vous avez besoin d'envoyer des messages emails à partir d'adresses emails qui sont hors du domaine, vous pouvez configurer un connecteur de réception personnalisé. Pour des détails sur la manière de configurer un connecteur de réception, voir la documentation du Microsoft Exchange Server.
- **Lotus Domino 8.0 et 8.5** – La seule condition exigée est de vérifier que la valeur du paramètre SMTPVerifyAuthenticatedSender est définie à 0. Pour des détails sur cette configuration, voir la documentation de Lotus Domino.

4 Configuration du serveur Web d'entreprise

Ce chapitre contient des instructions détaillées sur comment configurer les fichiers du composant Web nécessaires sur l'ordinateur serveur Web d'entreprise pour prendre en charge la OpenScape Contact Center fonctionnalité de rappel Web. Il décrit également comment configurer une connexion de sécurité pour l'ordinateur serveur Web d'entreprise, repérer et personnaliser les fichiers par défaut et corriger les problèmes courants.

IMPORTANT : Avant la mise à niveau sur l'ordinateur serveur Web d'entreprise, copiez tous les fichiers personnalisés des composants à un emplacement protégé afin de pouvoir les réappliquer après la mise à niveau. Tout manquement à cette procédure entraîne la perte des fichiers personnalisés car ils ne sont pas conservés dans la mise à niveau.

REMARQUE : Quand vous créez ou personnalisez des pages Web en vue de leur utilisation avec la fonction Web de OpenScape Contact Center, veuillez à prendre les précautions nécessaires pour réduire les vulnérabilités potentielles de sécurité.

4.1 Exigences du système l'utilisation des composants Web

Pour que les fichiers des composants fonctionnent correctement, assurez-vous que le serveur Web d'entreprise et le navigateur Web utilisés pour accéder à ces fonctions, répondent aux exigences mentionnées dans cette section.

4.1.1 Exigences du serveur Web d'entreprise

Le serveur Web d'entreprise peut utiliser l'un des serveurs Web ci-dessous et des systèmes d'exploitation correspondants :

- Microsoft Internet Information Server (IIS) 8 et 8.5
- Apache Tomcat 6.0 sur serveur Red Hat Enterprise Linux 6
- Apache Tomcat 7.0.63 sur serveur Red Hat Enterprise Linux 6

4.1.2 Exigences du navigateur Web

Les navigateurs Web qui ont été testés conjointement au système OpenScape Contact Center sont les suivants :

- Internet Explorer 6, 7, 8 et 9
- Firefox 10 et 11

Pour plus informations sur ces serveurs, voir la documentation du fabricant.

Assurez-vous que le navigateur Web est configuré de la façon suivante :

- Paramètre de sécurité Internet défini à moyen ou bas
- Javascript activé
- Les affichages instantanés automatiques (popups) sont activés (le blocage des affichages automatiques est désactivé pour permettre aux messages automatiques du site Internet de s'afficher)

4.2 Configuration des composants Web

Cette section décrit comment configurer les composants Web, selon le type de serveur Web installé.

REMARQUE : La configuration du serveur d'interaction Web peut exiger une configuration supplémentaire des composants Web. Par exemple, vous pouvez avoir à configurer une connexion sécurisée pour un serveur Web. Pour plus de détails, voir Section 4.3, "Configuration d'une connexion sécurisée pour un serveur Web", page 28.

4.2.1 Configuration d'un serveur IIS

Cette section décrit comment configurer les composants Web sur un serveur IIS. Pour obtenir des informations sur l'installation et la configuration du serveur IIS, voir la documentation Windows.

REMARQUE : OpenScape Contact Center utilise un mécanisme de surveillance pour surveiller la connexion entre le serveur Web d'entreprise et le serveur d'interaction. Il existe plusieurs configurations sur un serveur IIS comme un recyclage de groupe d'applications, pouvant entraîner le déchargement du composant ISAPI de OpenScape Contact Center. Dans ce cas, l'application

System Monitor indique que la connexion est interrompue. Pour éviter ce problème, changez la configuration comme indiqué dans la documentation Windows.

REMARQUE : Quand le serveur IIS tourne sur un système d'exploitation de 64 bits, le serveur IIS doit être configuré pour exécuter des applications Web 32 bits car ISAPI DLL OpenScape Contact Center est basé sur 32 bits.

4.2.1.1 Configuration des fichiers du composant Web sur un serveur IIS

Vous devez copier les fichiers des composants Web à partir du DVD OpenScape Contact Center sur l'ordinateur serveur Web d'entreprise, puis mettre à jour ces fichiers.

Pour configurer les fichiers des composants Web sur un serveur IIS :

1. Créez un dossier sur l'ordinateur serveur Web de l'entreprise pour stocker les fichiers des composants Web. Par exemple :

c:\HPPC

2. Insérez le DVD OpenScape Contact Center dans le lecteur de DVD-ROM.
3. Sur le DVD, allez au dossier **OpenScape Contact Center Web Components\IIS**.
4. Copiez le fichier **HPPCAgileWeb.zip** sur le serveur Web de l'entreprise et décompressez-le au dossier que vous avez créé à l'étape 1. La structure de fichiers suivante est créée :

c:\HPPC\Default.htm

c:\HPPC\hppcwis.dll

c:\HPPC\HPWC.ini

c:\HPPC\html

c:\HPPC\html\WCCallbackMain.htm

c:\HPPC\html\english (et fichiers correspondants)

c:\HPPC\images (et fichiers correspondants)

IMPORTANT : Ne changez pas la structure des fichiers car elle est exigée pour l'exécution correcte des fichiers.

Configuration du serveur Web d'entreprise

Configuration des composants Web

5. Ouvrez le fichier **HPWC.ini** dans un éditeur de texte et, sous **[HPPCSETTINGS]**, changez le paramètre **Address** en lui donnant le nom d'hôte ou l'adresse IP de l'ordinateur serveur principal OpenScape Contact Center.

IMPORTANT : Assurez-vous que le paramètre du numéro de **port** que vous spécifiez est le même que celui configuré dans l'application Manager et que le port est ouvert dans le pare-feu entre l'ordinateur serveur Web d'entreprise et l'ordinateur serveur principal OpenScape Contact Center. Le numéro de port par défaut est 6021. Si vous changez ce numéro de port, vous devez redémarrer l'ordinateur serveur Web d'entreprise et le serveur d'interaction Web.

6. Enregistrez et fermez le fichier.
7. Dans IIS, créez un nouvel répertoire virtuel pour le site Web par défaut. Pour des détails, voir la documentation Windows. Lors de la création du répertoire virtuel, vous devez :
 - Fournir un alias tel que HPPC.
 - Sélectionner le dossier que vous avez créé à l'étape 1 quand le système vous demande de spécifier le répertoire du contenu du site Web.
 - Activer les autorisations d'accès suivantes :
 - Lire
 - Exécuter les scripts (tels que ASP)
 - Exécuter (par exemple, CGI ou application ISAPI)

IMPORTANT : Assurez-vous que les postes ISAPI ont l'état **autorisé** dans le noeud des postes d'extension du service Web dans IIS Manager pour IIS. Sinon, quand le système essaie d'appeler la fonctionnalité ISAPI du OpenScape Contact Center, l'erreur 404 est renvoyée. Pour activer ou désactiver individuellement les postes SAPI, vérifiez l'aide de la console MMC (Microsoft Management Console) pour obtenir des informations relatives à l'activation et la désactivation du contenu dynamique dans les configurations du serveur.

4.2.1.2 Test de la fonctionnalité de rappel par Web sur un serveur IIS

Cette section décrit comment tester la fonctionnalité de rappel Web sur un serveur IIS.

Pour tester la fonction de rappel par Web sur un serveur IIS :

1. Ouvrez un navigateur Web et entrez l'adresse URL pour accéder à la page de démonstration WCCallbackMain.htm. Le format de l'URL est le suivant :

`http://<nom_hôte>/<nom_hôte>/html/WCCallbackMain.htm`

où

- `<Nom_hôte>` est le nom de l'hôte ou l'adresse IP de l'ordinateur serveur Web d'entreprise.
- `<chemin_virtuel>` est le chemin au répertoire virtuel que vous avez créé.

Par exemple :

`http://127.0.0.1/HPPC/html/WCCallbackMain.htm`

2. Dans la page WCCallbackMain.htm, cliquez sur le bouton **Try Web Callback** (Essayer le rappel par Web). Si une page s'ouvre affichant des champs sur des informations de contact client, vous avez chargé **WebCallback.htm** et vous avez configuré correctement les rappels Web sur le serveur dans une configuration de base par défaut.

REMARQUE : À ce point, si vous cliquez sur le bouton **Submit** sur **WebCallback.htm**, un message d'erreur peut s'afficher. Vous pouvez cliquer sur ce bouton une fois la configuration du serveur terminée.

3. Configurez le serveur d'interaction Web sur l'ordinateur serveur principal OpenScape Contact Center. Pour des informations détaillées, voir l'*Aide de Manager*.

4.2.2 Configuration d'un serveur Tomcat

Cette section décrit comment configurer les paramètres du composants Web sur le serveur Tomcat. Pour obtenir des informations sur l'installation et la configuration du serveur Tomcat lui-même ou la connexion du serveur Tomcat au serveur Apache, voir la documentation du serveur Tomcat.

4.2.2.1 Configuration du fichier .war sur un serveur Tomcat

Cette section décrit comment configurer et déployer le fichier .war sur un serveur Tomcat.

Configuration du fichier .war sur un serveur Tomcat :

1. Insérez le DVD OpenScape Contact Center dans le lecteur de DVD-ROM.
2. Sur le DVD, allez au dossier **OpenScape Contact Center Web Components\Apache Tomcat**.
3. Copiez le fichier **HPPCEnterpriseWeb.war** sur l'ordinateur serveur Web d'entreprise.
4. Renommez le fichier .war avec un nom adapté à votre environnement. Dans les instructions suivantes, le nom du fichier .war a été remplacé par le nom **HPPC.war**. Ceci va déployer l'application Web exemple appelée HPPC. Pour assurer le fonctionnement, le nom du fichier .war doit être en majuscules comme indiqué dans l'exemple de configuration.
5. Assurez-vous que le kit de développement Java (JDK/Java Development Kit) est installé.
6. Pour extraire le fichier config.properties dans un nouveau dossier appelé hpwcapp, ouvrez une fenêtre d'invite de commande, passez au répertoire qui contient le fichier HPPC.war dans la ligne de commande, tapez la commande suivante à l'invite de commande, puis appuyez sur **Entrée** :

```
jar xfv HPPC.war hpwcapp/config.properties
```
7. Ouvrez le fichier **hpwcapp/config.properties** dans un éditeur de texte et effectuez les opérations suivantes :
 - Changez le paramètre **servlet.name** pour refléter le nom du fichier .war spécifié à l'étape 4. Dans l'exemple de configuration, le paramètre est `servlet.name=/HPPC/hppcwebchat`.
 - Remplacez le paramètre **socket.server.name** par le nom de l'hôte ou l'adresse IP de l'ordinateur serveur principal OpenScape Contact Center.

REMARQUE : Assurez-vous que le paramètre **socket.server.port** est le même que celui configuré dans l'application Manager et que le port est ouvert dans le pare-feu entre l'ordinateur serveur Web d'entreprise et l'ordinateur serveur principal OpenScape Contact Center. Le numéro de port par défaut est 6021. Si vous changez ce numéro de port, vous devez redémarrer l'ordinateur serveur Web d'entreprise et le serveur d'interaction Web.

8. Enregistrez et fermez le fichier.

9. Pour mettre à jour le fichier HPPC.war à l'invite de commande dans le même répertoire qu'à l'étape 6, tapez :

```
jar uvf HPPC.war hpwcapp/config.properties
```

10. Déployez le fichier HPPC.war sur le serveur Tomcat. Pour des détails, voir la documentation de l'application Tomcat Web Application Manager.

4.2.2.2 Test de la fonctionnalité de rappel par Web sur un serveur Tomcat

Cette section décrit comment tester la fonction de rappel par Web sur le serveur Tomcat.

Pour tester la fonction de rappel par Web sur un serveur Tomcat :

1. Ouvrez un navigateur Web et entrez l'adresse URL pour accéder à la page de démonstration WCCallbackMain.htm. Le format de l'URL est le suivant :

```
http://<nom_hôte>/HPPC/html/WCCallbackMain.htm
```

où <Nom_hôte> est le nom d'hôte ou l'adresse IP de l'ordinateur serveur Web de l'entreprise.

Par exemple :

```
http://127.0.0.1:8080/HPPC/html/WCCallbackMain.htm
```

2. Dans la page WCCallbackMain.htm, cliquez sur le bouton **Try Web Callback** (Essayer le rappel par Web). Si une page s'ouvre contenant des champs sur des informations de contact client, vous avez chargé **WebCallback.htm**, indiquant que vous avez configuré correctement les rappels par Web sur le serveur Tomcat dans une configuration de base par défaut.

REMARQUE : À ce point, si vous cliquez sur le bouton **Submit** sur **WebCallback.htm**, un message d'erreur peut s'afficher. Vous pouvez cliquer sur ce bouton une fois la configuration du serveur terminée.

3. Configurez le serveur d'interaction Web sur l'ordinateur serveur principal OpenScape Contact Center. Pour des informations détaillées, voir l'*Aide de Manager*.

4.2.3 Configuration d'un Sun Java System Web Server

Cette section décrit comment configurer les composants Web sur un Sun Java System Web Server. Pour obtenir des informations sur l'installation et la configuration du Sun Java System Web Server, voir la documentation Sun.

4.2.3.1 Configuration du fichier .war sur un Sun Java System Web Server

Cette section décrit comment configurer le fichier .war sur un Sun Java System Web Server.

Configuration du fichier .war sur un serveur Web de système Sun Java :

1. Insérez le DVD OpenScape Contact Center dans le lecteur de DVD-ROM.
2. Sur le DVD, allez jusqu'au dossier **OpenScape Contact Center Web Components\Sun Java System Web Server**.
3. Copiez le fichier **HPPCEnterpriseWeb.war** sur l'ordinateur serveur Web d'entreprise.
4. Renommez le fichier .war avec un nom adapté à votre environnement. Dans les instructions suivantes, le nom du fichier .war a été remplacé par le nom **HPPC.war**. Ceci va déployer l'application Web exemple appelée HPPC. Pour assurer le fonctionnement, le nom du fichier .war doit être en majuscules comme indiqué dans l'exemple de configuration.
5. Pour extraire le fichier config.properties dans un nouveau dossier appelé hpwcapp, ouvrez une fenêtre d'invite de commande, passez au répertoire qui contient le fichier HPPC.war dans la ligne de commande, tapez ce qui suit sur la ligne de commande, puis appuyez sur **Entrée** :

```
jar xfv HPPC.war hpwcapp/config.properties
```

6. Ouvrez le fichier **hpwcapp/config.properties** dans un éditeur de texte et effectuez les opérations suivantes :
 - Changez le paramètre **servlet.name** pour refléter le nom du fichier .war spécifié à l'étape 4. Dans l'exemple de configuration, le paramètre est `servlet.name=/HPPC/hppcwebchat`.
 - Remplacez le paramètre **socket.server.name** par le nom de l'hôte ou l'adresse IP de l'ordinateur serveur principal OpenScape Contact Center.

REMARQUE : Assurez-vous que le paramètre **socket.server.port** est le même que celui configuré dans l'application Manager et que le port est ouvert dans le pare-feu entre l'ordinateur serveur Web d'entreprise et l'ordinateur serveur principal OpenScape Contact Center. Le numéro de port par défaut est 6021. Si vous changez ce numéro de port, vous devez redémarrer l'ordinateur serveur Web d'entreprise et le serveur d'interaction Web.

7. Enregistrez et fermez le fichier.
8. Pour mettre à jour le fichier HPPC.war à l'invite de commande dans le même répertoire qu'à l'étape 5, tapez :

```
jar uvf HPPC.war hpwcapp/config.properties
```

9. Allez au site d'administration du Sun Java System Web Server et créez-en une nouvelle instance de serveur. Pour accéder au site d'administration, ouvrez le navigateur Web et tapez l'URL. Le format de l'URL est le suivant :

```
http://<nom d'hôte>/https-admserv/bin/index
```

où <Nom_hôte> est le nom d'hôte ou l'adresse IP de l'ordinateur serveur Web de l'entreprise.

Quand vous créez l'instance du serveur, utiliser **HPPC** pour l'identifiant du serveur. Ceci crée automatiquement un dossier appelé **/https-HPPC**. Pour plus de détails, voir la documentation de Sun.

REMARQUE : Si vous cochez la case **Never attempt to resolve IP addresses into host names (Ne jamais tenter pour résoudre les adresses IP en noms d'hôte)**, vous devez être en accord avec votre configuration. Ceci signifie que l'on peut utiliser les adresses IP ou les noms d'hôte mais pas les deux.

10. Démarrez l'instance du nouveau serveur.
11. Déployez le fichier HPPC.war sur le Sun Java System Web Server. Pour plus de détails, voir la documentation de Sun. Toutefois, assurez-vous que lorsque vous déployez le fichier .war au serveur, que l'URL de l'application est **/HPPC**.

4.2.3.2 Test de la fonction de rappel par Web sur un Sun Java System Web Server

Cette section décrit comment tester la fonction de rappel par Web sur un Sun Java System Web Server.

Pour tester la fonction de rappel par Web sur un Sun Java System Web Server:

1. Démarrez l'instance de serveur que vous avez créée dans Section 4.2.3.1, "Configuration du fichier .war sur un Sun Java System Web Server", page 29.
2. Ouvrez un navigateur Web et entrez l'adresse URL pour accéder à la page de démonstration WCCallbackMain.htm. Le format de l'URL est le suivant :

```
http://<nom_hôte>/HPPC/html/WCCallbackMain.htm
```

où <Nom_hôte> est le nom d'hôte ou l'adresse IP de l'ordinateur serveur Web de l'entreprise.

Par exemple :

```
http://127.0.0.1:8081/HPPC/html/WCCallbackMain.htm
```

Configuration du serveur Web d'entreprise

Configuration d'une connexion sécurisée pour un serveur Web

3. Dans la page WCCallbackMain.htm, cliquez sur le bouton **Try Web Callback** (Essayer le rappel par Web). Si une page s'ouvre contenant des champs sur des informations de contact client, vous avez chargé **WebCallback.htm** indiquant que vous avez configuré correctement les rappels par Web sur le Sun Java System Web Server dans une configuration de base par défaut.

REMARQUE : À ce point, si vous cliquez sur le bouton **Submit** sur **WebCallback.htm**, un message d'erreur peut s'afficher. Vous pouvez cliquer sur ce bouton une fois la configuration du serveur terminée.

4. Configurez le serveur d'interaction Web sur l'ordinateur serveur principal OpenScape Contact Center. Pour des informations détaillées, voir l'*Aide de Manager*.

4.3 Configuration d'une connexion sécurisée pour un serveur Web

Le système peut être configuré pour utiliser l'authentification basée sur certificat TLS pour sécuriser la connexion entre le serveur d'interaction Web et le serveur Web d'entreprise.

Cette section décrit comment activer la sécurité TLS sur le serveur Web d'entreprise selon le type de serveur Web d'entreprise dont vous disposez.

Pour terminer la configuration TLS, vous devez aussi effectuer les tâches suivantes :

1. Sur l'ordinateur serveur principal, installez un certificat TLS. Pour plus de détails, voir le *Guide d'Installation*.
2. Dans l'application Manager, sélectionnez un port activé par TLS pour la connexion Web. Pour des informations détaillées, voir l'*Aide de Manager*.

REMARQUE : Nous vous conseillons de n'activer la sécurité TLS sur le serveur Web d'entreprise que lorsque toutes les autres configurations des serveurs d'interaction Web sont terminées.

4.3.1 Activation de la sécurité TLS sur un serveur IIS

Cette section décrit comment activer la sécurité TLS sur un serveur IIS.

Pour activer la sécurité TLS sur un serveur IIS :

1. Ouvrez le fichier **HPWC.ini** dans un éditeur de texte.
2. Sous **[HPPCSETTINGS]**, assurez-vous que l'**adresse** est définie au nom d'hôte de l'ordinateur serveur principal OpenScape Contact Center qui correspond au nom commun du certificat TLS.
3. Définissez le paramètre **TLSPort** au numéro de port devant être utilisé par les fonctions Web sécurisées, par exemple :

```
SSLPort=443
```

REMARQUE : Assurez-vous que le numéro de port que vous configurez ici correspond au numéro de port TLS configuré dans l'application Manager. Pour des informations détaillées, voir l'*Aide de Manager*.

4. Définissez l'indicateur de rappel à true (vrai) :

```
CallbackUsesSSL=true (vrai)
```

REMARQUE : Quand l'indicateur TLS est défini à true (vrai), la fonction n'est disponible que par TLS sur le port spécifié par le paramètre TLSPort.

5. Dans le menu **File**, cliquez sur **Save**, puis sur **Exit**.

4.3.2 Activation TLS sur un serveur Tomcat ou Sun Java

Cette section décrit comment activer la sécurité TLS sur un serveur Web Tomcat ou un serveur Web de système Java.

Si nécessaire, téléchargez Java Secure Socket Extension (JSSE) avant de commencer. Pour des instructions détaillées, voir la documentation du fabricant.

Pour activer TLS sur un serveur Tomcat ou Sun Java :

1. Installez la mémoire de clé cryptographique selon les instructions du fabricant.
2. Ouvrez le fichier **config.properties** dans un éditeur de texte.

Configuration du serveur Web d'entreprise

Codes d'erreurs des rappels Web

3. Définissez le paramètre **socket.server.name** au nom d'hôte de l'ordinateur serveur principal OpenScape Contact Center qui correspond au nom courant du certificat TLS.

4. Définissez le paramètre **socket.server.port.ssl** au numéro de port devant être utilisé par les fonctions Web sécurisées, par exemple :

```
socket.server.port.ssl=443
```

REMARQUE : Assurez-vous que le numéro de port que vous configurez ici correspond au numéro de port TLS configuré dans l'application Manager. Pour des informations détaillées, voir l'*Aide de Manager*.

5. Définissez l'indicateur de rappel à true (vrai) :

```
socket.webcallback.ssl=true (vrai)
```

REMARQUE : Quand l'indicateur TLS est défini à true (vrai), la fonction n'est disponible que par SSL sur le port spécifié par le paramètre **socket.server.port.ssl**.

6. Dans le menu **File**, cliquez sur **Save**, puis sur **Exit**.

4.4 Codes d'erreurs des rappels Web

Le tableau suivant donne la liste des codes d'erreurs pouvant s'afficher lorsque vous utilisez la fonction des rappels Web. Si le système renvoie les codes d'erreurs figurant dans le tableau, le rappel n'est pas créé.

En plus des codes d'erreurs figurant dans le tableau suivant, vous pouvez également rencontrer des erreurs variées associées au serveur de rappels dans l'application System Monitor.

| Code d'erreur | Description |
|---------------|--|
| 1000 | Une erreur générale s'est produite. |
| 1002 | Le serveur d'interaction Web n'a pas pu se connecter au serveur d'interaction Web. |
| 1003 | La connexion au serveur d'interaction Web a échoué. |
| 1006 | Il est impossible d'accéder à la page Web. |
| 1007 | Une ID de session non valable a été détectée. |
| 1008 | JavaScript n'est pas activé. |
| 1010 | Un paramètre obligatoire est incorrect. |

Tableau 1

Codes d'erreurs des rappels Web

| Code d'erreur | Description |
|---------------|---|
| 1011 | Un paramètre est incorrect. |
| 1012 | Il existe une erreur interne avec le serveur d'interaction Web. |
| 1013 | Erreur d'allocation. |
| 17006 | Un rappel dupliqué a été trouvé dans la base de données. |
| 17021 | Le serveur de rappels ne peut pas traiter une demande en raison d'une erreur interne. |
| 17025 | Une erreur générale s'est produite. |
| 17027 | La file d'attente des rappels n'existe pas. |
| 17028 | Une programmation de rappel n'est pas valable. |
| 17029 | Une programmation de rappel a lieu à l'extérieur de la planification d'acheminement des rappels configurés pour le centre de contacts. |
| 17030 | Le nom du client est trop long. Le maximum est 75 caractères. |
| 17031 | Un numéro de téléphone est l'un des numéros définis comme numéro exclu. |
| 17032 | La description du rappel est trop long. Le maximum est 100 caractères. |
| 17033 | Les données de contact sont trop longues. Le maximum est 1000 caractères. |
| 17035 | La priorité n'est pas valable. La priorité doit être compris entre 1 et 100. |
| 17040 | Une programmation de rappell a expiré. |
| 17047 | La date de début ou de fin d'une programmation de rappel n'est pas valable. Un rappel ne peut être programmé plus de 180 jours en avance. |

Tableau 1 Codes d'erreurs des rappels Web

Configuration du serveur Web d'entreprise

Codes d'erreurs des rappels Web

5 Configuration de l'intégration de présence

Ce chapitre décrit les éléments à configurer pour la prise en charge de l'intégration de la fonction d'intégration de présence. La fonction d'intégration de présence permet aux utilisateurs de l'application Client Desktop d'afficher la présence de différents utilisateurs en utilisant la fonction d'annuaire.

Quand la fonction d'intégration de présence est activée dans l'application Manager et que l'utilisateur de l'application Client Desktop effectue une recherche dans l'annuaire, le système tente d'obtenir la présence de chaque entrée dans les résultats de la recherche, de la façon suivante :

- Le système essaie d'abord d'obtenir l'état de présence de l'utilisateur et l'état de présence au média voix à partir de l'application OpenScape Unified Communications (UC) uniquement quand la fonction d'intégration de l'application OpenScape est activée et configurée.
- Si l'utilisateur n'est pas un utilisateur de l'application OpenScape UC ou si la fonctionnalité d'intégration de l'application OpenScape UC n'est pas activée ou n'est pas disponible, le système essaie d'obtenir l'état de présence de l'utilisateur à partir du système OpenScape Contact Center.

5.1 Configuration d'un compte utilisateur de l'application OpenScape UC

Pour activer le système afin d'intégrer l'application OpenScape UC, vous devez configurer un compte utilisateur dans l'application OpenScape UC que le système OpenScape Contact Center peut utiliser pour accéder à l'application OpenScape UC et avec lequel il peut maintenir la connectivité. Ce compte utilisateur est spécifié quand vous configurez les options d'intégration de présence dans l'application Manager. Pour obtenir des détails sur la configuration d'un nouveau compte utilisateur, voir la documentation de l'application OpenScape UC.

5.2 Configuration de l'annuaire externe LDAP

Pour permettre aux utilisateurs de l'application Client Desktop d'afficher la présence des autres utilisateurs, vous devez configurer l'annuaire externe LDAP pour la prise en charge de l'affichage de la présence.

En particulier, vous devez configurer un ou plusieurs champs suivants :

- **ID de présence** (ID de l'utilisateur de l'application OpenScape UC)
- **Nom d'utilisateur** (le nom d'utilisateur OpenScape Contact Center)

Pour obtenir des détails sur la configuration des champs, voir la documentation de l'application de l'annuaire LDAP.

6 Maintenance du système

Ce guide décrit comment procéder à la maintenance continue du système OpenScape Contact Center, y compris l'arrêt de l'ordinateur serveur principal, le changement des mots de passe et la sauvegarde de la base de données.

L'accès de service distant à un ordinateur serveur principal est fourni par le plug-in du service Smart Services Delivery Platform (SSDP). Le logiciel et la documentation du plug-in du service SSDP sont automatiquement installés sur l'ordinateur serveur au cours de l'installation. Pour configurer le plug-in du service SSDP, suivez les instructions fournies dans la documentation du plug-in du service SSDP, située sur le DVD OpenScape Contact Center dans le dossier Utilities\OpenScape Service Plug-in.

REMARQUE : Lors des procédures générales de maintenance du système, par exemple la mise à jour du réseau, nous recommandons d'éteindre l'ordinateur serveur principal OpenScape Contact Center avant de commencer. Pour des instructions spéciales, voir Section 6.1, "Arrêt d'un ordinateur serveur pour la maintenance du système".

6.1 Arrêt d'un ordinateur serveur pour la maintenance du système

Quand vous arrêtez ou redémarrez un ordinateur serveur OpenScape Contact Center qui exécute Informix, à des fins de maintenance, il arrive qu'Informix n'ait pas le temps d'arrêter le service Informix IDS avant l'arrêt par le système d'exploitation Microsoft Windows. Dans ce cas, la base de données peut être endommagée. Pour éviter ce problème, nous recommandons de toujours arrêter le service Informix IDS avant d'arrêter ou de redémarrer l'ordinateur serveur principal.

REMARQUE : Pour assurer l'intégrité de la base de données, arrêtez toujours le service IDS Informix avant d'arrêter ou de redémarrer un ordinateur serveur.

6.2 Modification des mots de passe pour OpenScape Contact Center et Informix

Si vous avez à changer les mots de passe OpenScape Contact Center ou Informix pour une raison quelconque, vous devez mettre à jour les mots de passe dans les trois emplacements suivants :

- Fenêtre Services
- Fenêtre Computer Management
- Fenêtre Startup Configuration de OpenScape Contact Center (ou application System Monitor)

IMPORTANT : Les mots de passe pour OpenScape Contact Center et Informix ne doivent être modifiés que sous la direction d'un représentant du service d'assistance.

Le mot de passe Informix ne peut pas dépasser 16 caractères et ne peut pas contenir de blanc.

Pour changer les mots de passe OpenScape Contact Center et Informix :

1. Ouvrez la fenêtre **Services**.
2. Pour changer le mot de passe OpenScape Contact Center, procédez suivant l'une de ces méthodes :
 - a) Arrêter les services **OpenScape Contact Center** et **OpenScape Contact Center AutoPA**.
 - b) Pour chaque service, ouvrez le service et entrez le nouveau mot de passe dans l'onglet **Connexion**.
3. Pour changer le mot de passe Informix, procédez suivant l'une de ces méthodes :
 - a) Arrêtez les services suivants : **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_nom_serveur** (*nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center et **Informix Server Discovery Process for SNMP**).
 - b) Ouvrez le service **Informix IDS - ol_nom_serveur** et entrez le nouveau mot de passe dans l'onglet **Connexion**.
 - c) Ouvrez le processus de découverte **Informix Server pour le service SNMP** et indiquez le nouveau mot de passe dans l'onglet **Connexion**.
4. Fermez la fenêtre **Services**.
5. Ouvrez la fenêtre **Computer Management**.

6. Sous **Outils système**, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Utilisateurs**.
7. Pour changer le mot de passe OpenScape Contact Center, effectuez un clic droit sur **hppc**, puis cliquez sur **Définir le mot de passe** et entrez le nouveau mot de passe.
8. Pour changer le mot de passe Informix, effectuez un clic droit sur **informix**, puis cliquez sur **Définir le mot de passe** et entrez le nouveau mot de passe.
9. Fermez la fenêtre **Computer Management**.
10. Ouvrez une fenêtre d'invite de commande.
11. À la ligne de commande, tapez `tcfmmain`, puis appuyez sur la touche **ENTER**. La fenêtre **Démarrer la configuration de OpenScape Contact Center** apparaît.
12. Pour changer le mot de passe, cliquez sur l'onglet **Serveur d'administration** et tapez le nouveau mot de passe dans la case **Mot de passe du serveur de base de données**.

REMARQUE : Quand le système est en exécution, vous pouvez aussi changer le mot de passe Informix en configurant les données de démarrage pour le serveur d'administration en utilisant l'application System Monitor. Pour obtenir de plus amples d'informations, voir *l'aide de l'application System Monitor*.

13. Fermez la fenêtre de **configuration du démarrage de OpenScape Contact Center**.
14. Démarrez les services suivants : **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_nom_serveur** (*nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center) et **Informix Server Discovery Process for SNMP**.
15. Démarrer les services **OpenScape Contact Center** et **OpenScape Contact Center AutoPA**.

6.3 Sauvegarde de la base de données

Il est conseillé de sauvegarder la base de données OpenScape Contact Center régulièrement et chaque fois que vous modifiez la configuration du système pour être certain que les données sont protégées en cas d'une panne ou d'une

Maintenance du système

Sauvegarde de la base de données

corruption. Comme la base de données peut être volumineuse, nous recommandons de la sauvegarder uniquement pendant les périodes de faible activité du centre de contacts.

REMARQUE : En plus de la sauvegarde de la base de données OpenScape Contact Center, nous conseillons de sauvegarder toutes les données sur l'ordinateur serveur en utilisant un utilitaire de sauvegarde. Assurez-vous que la sauvegarde contient les données d'état du système de l'ordinateur serveur, incluant les éléments tels que le fichier de registre et le fichier de démarrage.

Il y a deux types de sauvegardes que vous pouvez effectuer.

- **Sauvegarde complète** - Pour limiter la perte potentielle des données à un jour, nous recommandons vivement d'effectuer une sauvegarde complète de la base de données chaque jour. Vous devez sauvegarder la base de données au minimum une fois par semaine.
- **Sauvegarde incrémental** - Pour réduire le risque de perte des données entre les sauvegardes complètes de la base de données, vous pouvez effectuer une sauvegarde incrémental de la base de données. Par exemple, si vous exécutez une sauvegarde complète au cours de la nuit, vous pouvez exécuter une sauvegarde incrémentale pendant la journée. La sauvegarde incrémentale prend moins de temps car elle n'archive que les changements apportés depuis la dernière sauvegarde complète.

REMARQUE : Certaines des procédures font l'hypothèse que vous maîtrisez parfaitement l'utilisation d'Informix. Pour des instructions détaillées, voir la documentation Informix à l'emplacement suivant :
<http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

6.3.1 Planification d'une sauvegarde de la base de données

Vous pouvez utiliser le Planificateur de tâches dans Windows Server 2012/2012 R2, 2008 R2 pour planifier une tâche qui sauvegardera la base de données OpenScape Contact Center. Cette section contient des directives sur la planification d'une tâche. Pour des instructions détaillées, voir la documentation Microsoft.

IMPORTANT : Les sauvegardes planifiées utilisent les fichiers de commandes FULLBACKUP.BAT et INCREMENTALBACKUP.BAT qui utilisent l'utilitaire Informix ontape pour exécuter la sauvegarde. En conséquence, avant l'exécution de la première sauvegarde planifiée, vous devez modifier les paramètres de l'utilitaire ontape comme décrit à l'étape 2, page 49.

Pour planifier la sauvegarde d'une base de données :

1. En utilisant le Planificateur dans Windows Server 2012/2012 R2, 2008 R2, planifiez une tâche selon les directives suivantes :
 - Sélectionnez l'action **Démarrer un programme**, puis sélectionnez l'un des fichiers de commandes suivants situés dans le dossier où vous avez installé le logiciel OpenScape Contact Center :
 - Pour planifier une sauvegarde complète, sélectionnez **FULLBACKUP.BAT**.
 - Pour planifier une sauvegarde incrémentale, sélectionnez **INCREMENTALBACKUP.BAT**.
 - Spécifiez le compte et le mot de passe d'utilisateur sous le fichier d'exécution de la tâche, conformément au type de système d'exploitation :
 - Pour Windows Server 2012/2012 R2, 2008 R2, spécifiez un compte d'administrateur local.
 - Pour écrire les résultats de la sauvegarde dans un fichier texte, dans les propriétés des tâches, ajoutez l'argument **<return.txt >results.txt**. Assurez-vous que le dossier où le fichier results.txt Fichier est écrit(normalement il s'agit du dossier où vous avez installé le logiciel OpenScape Contact Center) est accessible en lecture à tous les utilisateurs. Dans Windows Server 2012/ 2008 ou Windows Server 2012 R2/ 2008 R2, quand vous ajoutez l'argument, vous devez aussi spécifier le chemin pour le démarrage. Veillez à ne pas utiliser de guillemets quand vous spécifiez le chemin.

6.3.2 Sauvegarde de la base de données en utilisant l'utilitaire ontape

Vous pouvez sauvegarder la OpenScape Contact Center base de données sur un lecteur de bande local ou en réseau en utilisant l'utilitaire ontape Informix.

6.3.2.1 Sauvegarde de la base de données sur un lecteur de bande local

Cette section décrit comment sauvegarder la base de données OpenScape Contact Center sur un lecteur local ou en réseau en utilisant l'utilitaire Informix ontape.

Pour sauvegarder la base de données sur un lecteur sur bande local :

1. Connectez-vous à l'ordinateur serveur sur lequel Informix est installé de la façon suivante :
 - Pour Windows Server 2008 R2, connectez-vous en tant qu'administrateur.
2. Insérez une bande vierge dans le lecteur de bande de l'ordinateur serveur.
3. Ouvrez une fenêtre d'invite de commande Informix en utilisant le raccourci **ol_nom_serveur** où *nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center.
4. Pour démarrer la sauvegarde, procédez comme suit :
 - Pour effectuer une sauvegarde complète de la base de données Informix, sur la ligne de commande, tapez `ontape -s -L 0`, puis appuyez sur **ENTRÉE**.
 - Pour effectuer une sauvegarde incrémentale de la base de données Informix, sur la ligne de commande, tapez `ontape -s -L 1`, puis appuyez sur **ENTRÉE**.

REMARQUE : Le paramètre `-s` indique à l'utilitaire ontape de créer une sauvegarde et le paramètre `-L` spécifie le niveau d'archivage 0 pour une sauvegarde complète ou 1 une sauvegarde incrémentale.

5. S'il n'y a pas suffisamment d'espace sur la bande en place, le système vous demande d'en insérer une autre. Si le programme vous le demande, retirez la bande et étiquetez-la avec la date, l'heure, le niveau et le nombre de bandes dans la séquence. Insérez une autre bande et appuyez sur **ENTRÉE**. Répétez ce processus pour chaque bande nécessaire.

6.3.2.2 Sauvegarde de la base de données sur un lecteur local ou en réseau

Cette section décrit comment sauvegarder la base de données OpenScape Contact Center sur un lecteur local ou en réseau en utilisant l'utilitaire Informix ontape.

Pour sauvegarder la base de données sur un lecteur local ou en réseau :

1. Connectez-vous à l'ordinateur serveur sur lequel Informix est installé de la façon suivante :
 - Pour Windows Server 2008 R2, connectez-vous en tant qu'administrateur.
2. Modifiez les paramètres ontape comme indiqué ci-dessous :
 - Repérez le fichier **ONCONFIG.ol_*nom_serveur*** où *nom_serveur* est le nom de l'ordinateur serveur de OpenScape Contact Center sur lequel Informix est installé et ouvrez le fichier dans un éditeur de texte, par exemple le Bloc-notes. Normalement, ce fichier journal se trouve dans le dossier Fichiers programme\Informix\etc.
 - Dans le paramètre TAPEDEV, spécifiez le chemin et le nom du fichier de sauvegarde sur le lecteur local ou en réseau en format 8.3 (abrégé), (par exemple, C:\Backups\Sauvegarde.001. Avant de démarrer la sauvegarde, vous devez vous assurer que le fichier de sauvegarde existe à l'emplacement spécifié et que l'utilisateur connecté a, au minimum, l'autorisation de modification pour le fichier de sauvegarde. Si le fichier de sauvegarde n'existe pas, vous pouvez créer un fichier vide en utilisant un éditeur de texte, par exemple le Bloc-notes.
 - Dans le paramètre TAPESIZE, spécifiez 0 afin que le fichier de sauvegarde n'atteigne pas une taille maximale.
3. Ouvrez une fenêtre d'invite de commande Informix en utilisant le raccourci **ol_*nom_serveur*** où *nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center.

4. Pour démarrer la sauvegarde, procédez comme suit :

- Pour effectuer une sauvegarde complète de la base de données Informix, sur la ligne de commande, tapez `ontape -s -L 0`, puis appuyez sur **ENTRÉE**.
- Pour effectuer une sauvegarde incrémentale de la base de données Informix, sur la ligne de commande, tapez `ontape -s -L 1`, puis appuyez sur **ENTRÉE**.

REMARQUE : Le paramètre `-s` indique à l'utilitaire `ontape` de créer une sauvegarde et le paramètre `-L` spécifie le niveau d'archivage 0 pour une sauvegarde complète ou 1 une sauvegarde incrémentale.

6.3.3 Restauration de la base de données en utilisant l'utilitaire `ontape`

Cette section décrit comment restaurer les données OpenScape Contact Center sauvegardées au préalable en utilisant l'utilitaire `ontape` Informix.

REMARQUE : Si vous avez effectué une sauvegarde incrémentale, vous avez besoin de la sauvegarde complète la plus récente ainsi que la sauvegarde incrémentale.

REMARQUE : Lorsque vous souhaitez restaurer une sauvegarde L0 avec une installation OSCC nettoyée, vérifiez que les blocs de fichiers répertoriés par l'utilitaire `ontape` apparaissent bien dans le dossier Contact Center Data. Si ce n'est pas le cas, créez ces fichiers sans extension en faisant un clic droit, puis en naviguant jusqu'à **Nouveau -> Document texte**. Ensuite, renommez-les et supprimez l'extension. L'importation ne fonctionnera pas correctement si ces blocs de fichiers ne sont pas présents.

Pour restaurer la base de données en utilisant l'utilitaire `ontape` :

1. Connectez-vous à l'ordinateur serveur sur lequel Informix est installé de la façon suivante :
 - Pour Windows Server 2008 R2, connectez-vous en tant qu'administrateur.
2. Arrêtez les services suivants :

- **OpenScape Contact Center**
 - **Informix IDS - ol_nom_serveur**, où *nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center.
3. Procédez suivant l'une des méthodes suivantes :
 - Si vous restaurez les données à partir d'une bande, insérez la première bande d'archivage de type complet que vous voulez restaurer dans le lecteur de bande de l'ordinateur serveur.
 - Si vous restaurez les données d'un fichier de sauvegarde sur un lecteur local ou en réseau, assurez-vous que le nom et le chemin du fichier de la sauvegarde sont configurés correctement dans le fichier `ONCONFIG.ol_nom_serveur`.
 4. Ouvrez une fenêtre d'invite de commande Informix en utilisant le raccourci **ol_nom_serveur** où *nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center.
 5. À la ligne de commande, tapez `ontape -r`, puis appuyez sur la touche **ENTRÉE**.
 6. Quand le programme vous invite à insérer une bande, appuyez sur **ENTRÉE**.
 7. Quand le programme vous invite à la restauration, (**Continue restore (Y/N)?**), appuyez sur **Y**.
 8. Quand le programme vous invite à sauvegarder les journaux, appuyez sur **N**.
 9. Si vous avez créé une archive incrémentale, quand le programme vous demande s'il s'agit d'une archive de restauration de niveau 1 (**Restore a level 1 archive**), appuyez sur **Y**. Si vous n'avez pas créé une archive incrémentale, appuyez sur **N**.
 10. Quand le programme vous invite à restaurer les bandes des journaux, appuyez sur **N**.
 11. Quand la restauration est terminée, si vous restaurez les données à partir d'un lecteur de bande, retirez la dernière bande du lecteur.
 12. À la ligne de commande, tapez `onmode -m`, puis appuyez sur la touche **ENTRÉE**. Cette commande place Informix dans son mode normal. Son exécution complète peut prendre plusieurs minutes.
 13. À la ligne de commande, tapez `onstat -r`, puis appuyez sur la touche **ENTRÉE**. Cette commande affiche des informations sur l'environnement du serveur Informix. La première ligne indique le mode de l'application Informix et doit être **On-Line**. Pour arrêter la commande Informix `onstat`, appuyez sur **CTRL+C**.
 14. Pour fermer la fenêtre d'invite de la commande, tapez `exit`, puis appuyez sur **Entrée**.

15. Fermez toutes les autres fenêtres ou applications.
16. Redémarrez le service **OpenScape Contact Center**.

6.3.4 Restauration d'une sauvegarde de niveau zéro effectuée en utilisant l'utilitaire ontape

Cette partie décrit comment restaurer les données OpenScape Contact Center sauvegardées au niveau zéro à l'aide d'un processus automatisé.

1. Pour utiliser le script de restauration niveau zéro, copier FullRestore.bat, fullrestore.in et les fichiers replace.vbs dans le serveur. Les fichiers sont compris dans le DVD.
2. Ouverture d'une invite de commande en tant qu'utilisateur Informix
3. Exécuter FullRestore.bat en spécifiant les arguments /tapedev <path> / tapesize<size>, où <path> correspond au chemin vers la sauvegarde Informix niveau zéro, la taille <size> spécifiée est zéro sauf si vous utilisez un dispositif à bande externe.

6.3.5 Sauvegarde de la base de données en utilisant l'utilitaire onbar

Cette section décrit comment sauvegarder la base de données OpenScape Contact Center sur un lecteur local ou en réseau en utilisant l'utilitaire Informix onbar. L'utilitaire Informix onbar peut interfacer directement avec le gestionnaire de stockage Informix ISM (Informix Storage Manager) ou un autre gestionnaire d'application de stockage d'un fournisseur tiers, par exemple Veritas, afin de fournir une solution de sauvegarde de grande souplesse.

REMARQUE : Vous devez configurer l'application Informix Storage Manager (ISM) avant d'exécuter l'utilitaire onbar. Pour des instructions détaillées, voir le guide de l'administrateur Informix (*IBM Informix Storage Manager Administrator's Guide*) ou la documentation de l'utilitaire Storage Manager de tierce partie. La documentation Informix se trouve à l'emplacement suivant : <http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

Pour sauvegarder la base de données sur un disque local :

1. Connectez-vous à l'ordinateur serveur sur lequel Informix est installé de la façon suivante :
 - Pour Windows Server 2008 R2, connectez-vous en tant qu'administrateur.
2. Ouvrez une fenêtre d'invite de commande Informix en utilisant le raccourci **ol_nom_serveur** où *nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center.
3. Pour démarrer la sauvegarde, procédez comme suit :
 - Pour effectuer une sauvegarde complète de la base de données Informix, sur la ligne de commande tapez `onbar -b -L 0`, puis appuyez sur **ENTRÉE**.
 - Pour effectuer un archivage incrémental de la base de données Informix, sur la ligne de commande tapez `onbar -b -L 1`, puis appuyez sur **ENTRÉE**.

REMARQUE : Le paramètre `-b` indique à l'utilitaire `onbar` de créer une sauvegarde et le paramètre `-L` spécifie le niveau d'archivage `0` pour une sauvegarde complète ou `1` une sauvegarde incrémentale.

6.3.6 Restauration de la base de données en utilisant l'utilitaire `onbar`

Cette section décrit comment restaurer les données OpenScape Contact Center sauvegardées au préalable en utilisant l'utilitaire Informix `onbar`.

REMARQUE : Si vous avez effectué une sauvegarde incrémentale, vous avez besoin de la sauvegarde complète la plus récente ainsi que la sauvegarde incrémentale.

Pour restaurer la base de données en utilisant l'utilitaire `onbar` :

1. Connectez-vous à l'ordinateur serveur sur lequel Informix est installé de la façon suivante :
 - Pour Windows Server 2008 R2, connectez-vous en tant qu'administrateur.
2. Ouvrez une fenêtre d'invite de commande Informix en utilisant le raccourci **ol_nom_serveur** où *nom_serveur* est le nom de l'ordinateur serveur OpenScape Contact Center.

3. À la ligne de commande, tapez `onbar -r`, puis appuyez sur la touche **ENTRÉE**.

6.4 Prise en charge de SNMP

Le système prend en charge deux méthodes de génération d'informations pouvant être visualisées par un système de gestion SNMP :

- **OpenScape Contact Center SNMP Extension Agent** – Expose les informations spécifiques OpenScape Contact Center relatives à l'état des objets gérés par OpenScape Contact Center.
- **Logiciel OpenScape CAP Fault Management** – Agit en tant que SNMP Extension Agent pour générer des messages pièges SNMP pour le logiciel OpenScape Contact Center par le biais des journaux d'événements Windows.

Le service SNMP de Windows doit être installé et en exécution sur l'ordinateur serveur principal pour la prise en charge de ces méthodes.

REMARQUE : Vous devez configurer le service SNMP de Windows afin que la liste des noms de communautés ne contiennent pas le mot "public" ou "privé" et que la liste des hôtes ne contiennent que les hôtes exigés pour accéder à ces informations.

6.4.1 OpenScape Contact Center SNMP Extension Agent

OpenScape Contact Center SNMP Extension Agent (osccsnmp.DLL) prend en charge les demandes SNMP pour les ID d'objets. SNMP Extension Agent expose les informations spécifiques OpenScape Contact Center relatives à l'état des objets gérés par OpenScape Contact Center. Les informations peuvent être demandées par tout système de gestion SNMP.

REMARQUE : L'utilisateur du système de gestion SNMP a la responsabilité de s'assurer que des informations peuvent être demandées et récupérées à partir de l'OpenScape Contact Center SNMP Extension Agent.

Les informations OpenScape Contact Center spécifiques qui sont exposées par l'OpenScape Contact Center SNMP Extension Agent sont définies dans le fichier `sen-oscc-mib.mib` qui mappe les objets gérés à leur identification respective. Les informations exposées incluent l'utilisation des postes Call Director, le nombre

d'utilisateurs connectés et numéro actuel et récent des contacts. Pour des détails sur toutes les informations disponibles, voir le fichier `sen-oscc-mib.mib` qui peut être ouvert par un éditeur de texte.

Les informations OpenScape Contact Center spécifiques peuvent être utilisées pour surveiller l'état du système. Par exemple, un technicien dans un centre d'opérations en réseau peut créer une vue qui génère une alarme quand le nombre de postes de processeurs vocaux en service tombent en deçà d'un seuil limite donné en pourcentage du nombre total de postes de processeurs vocaux configurés. Le technicien peut ensuite avertir le client afin que celui-ci ait le temps de résoudre le problème et d'éviter d'être à court de postes.

Les fichiers `osccsnmp.DLL` et `sen-oscc-mib.mib` sont situés dans le dossier d'installation par défaut sur l'ordinateur serveur principal.

REMARQUE : Le fichier `osccsnmp.DLL` est automatiquement enregistré sur l'ordinateur serveur au cours de l'installation du logiciel de serveur OpenScape Contact Center. Si le service SNMP de Windows est désinstallé, l'enregistrement du fichier `osccsnmp.DLL` est alors annulé. Pour enregistrer à nouveau le fichier `.DLL`, utilisez le programme utilitaire `osccregistersnmpextension.exe`, situé dans le dossier d'installation par défaut sur l'ordinateur serveur principal.

6.4.2 Logiciel OpenScape CAP Fault Management

Le logiciel OpenScape CAP Fault Management est un composant en option pouvant être utilisé pour générer des messages pièges SNMP OpenScape Contact Center. Le logiciel OpenScape CAP Fault Management peut être installé automatiquement au cours de l'installation de OpenScape Contact Center ou manuellement à partir du dossier `\OpenScape CAP\Fault Management` situé sur le DVD de OpenScape Contact Center.

REMARQUE : Pour des détails sur comment configurer le logiciel OpenScape CAP Fault Management, voir la documentation de OpenScape CAP Fault Management.

Il existe deux fichiers de configuration pour OpenScape CAP Fault Management :

- **capfm_procenter.ini** – Il s'agit du fichier de configuration par défaut qui est installé au cours de l'installation du logiciel du serveur OpenScape Contact Center. Il déclenche la génération de messages pièges SNMP pour tous les messages OpenScape Contact Center.
- **capfm_procenter_service.ini** – Il s'agit du fichier de configuration de service qui doit être utilisé si vous voulez générer des messages de pièges sous-ensembles de messages qui sont pertinents au centre d'opérations en réseau.

Les deux fichiers de configuration sont situés dans le dossier \Utilities\Install sur le DVD de OpenScape Contact Center.

Index

A

accès de service distant 35
annuaire LDAP, configuration pour l'intégration de la
fonctionnalité de présence 34
Apache Tomcat, version 19
authentification, serveur emails 16

C

changement du mot de passe de OpenScape Contact
Center 36
codes d'erreurs, pour les rappels par Web 30
composants Web
configuration 20
configuration d'une connexion sécurisée 28
configuration sur un serveur IIS 21
configuration sur un serveur Sun Java 25
configuration sur un serveur Tomcat 23
exigences du navigateur Web 20
exigences du système 19
compte utilisateur de l'application OpenScape UC,
configuration pour l'intégration de la fonctionnalité de
présence 33
config.properties
configuration sur un serveur Tomcat 24
configuration sur un Sun Java System Web
Server 26
configuration 9
connexion sécurisée
pour un serveur email d'entreprise 16
pour un serveur Web d'entreprise 28
connexions IP, configuration pour panneaux muraux 7

D

déploiement d'IBM Lotus Domino 14
déploiement de Lotus Domino 14
déploiement de Microsoft Exchange 11
documentation
apport de commentaire 6
conventions de formats 5
public visé 5

E

en-têtes des messages email
insertion personnalisée 13
en-têtes des messages email personnalisés
insertion 13
en-têtes des messages emails

personnalisés requis 10
en-têtes des messages emails personnalisés
à propos 10

F

fichier .war
configuration sur un Sun Java System Web
Server 26
fichier HPWC.ini
activation pour SSL 29
configuration 22
fonction Envoyer des rapports par email, prise en
charge 17
fonction MIME 9

I

Informix
avec l'utilitaire onbar 44
changement du mot de passe 36
configuration des paramètres ontape 39, 41
utilitaire ontape 40
intégration de présence, configuration 33

M

mots de passe, changement 36

N

navigateur Web, exigences 20

O

ordinateur du serveur IIS
création d'un répertoire virtuel 22
ordinateur serveur, arrêt pour maintenance 35

P

panneaux muraux, configuration 7
plug-in de service SSDP 35
postes ISAPI 22
prise en charge de SNMP, méthode 46
protocole IMAP4 9
protocole SMTP 9

R

rappel par Web
codes d'erreurs 30
test sur le serveur Sun Java 27
test sur un serveur IIS 23
test sur un serveur Tomcat 25

répertoire virtuel, ordinateur du serveur IIS 22

S

sauvegardes de bases de données

restauration en utilisant l'utilitaire onbar 45

restauration en utilisant l'utilitaire ontape 42

sauvegardes complètes de la base de données 38

sur un lecteur local (onbar) 44

sur un lecteur local (ontape) 40

sur un lecteur local ou en réseau (ontape) 41

sauvegardes de la base de données

planification 38

sauvegardes incrémentales 38

sauvegardes planifiées 38

sauvegardes, voir sauvegardes de bases de données

serveur email 9

configuration d'une connexion sécurisée 16

utilisation de l'authentification 16

serveur email d'entreprise 9

configuration d'une connexion sécurisée 16

exigences 9

utilisation de l'authentification 16

serveur IIS

configuration d'une connexion sécurisée 29

configuration des composants Web 21

configuration du fichier HPWC.ini 22

test du rappel par Web 23

serveur Tomcat

configuration d'une connexion sécurisée 29

configuration des composants Web 23

configuration et déploiement du fichier .war 24

modification de config.properties 24

test du rappel par Web 25

serveur Web

Apache Tomcat, version 19

configuration 19, 20

configuration d'une connexion sécurisée 28

exigences 19

fichiers personnalisés et mis à jour 19

paramétrage d'une connexion sécurisée 28

prise en charge des systèmes d'exploitation 19

version du Sun Java System 19

serveur Web d'entreprise

configuration 19, 20

exigences 19

fichiers personnalisés et mis à jour 19

prise en charge des systèmes d'exploitation 19

serveur Web d'entreprise

Apache Tomcat, version 19

configuration d'une connexion sécurisée 28

version du Sun Java System 19

serveur Web Sun Java System

configuration d'une connexion sécurisée 29

SSL

activation d'un serveur Sun Java 29

activation d'un serveur Tomcat 29

activation pour un serveur email d'entreprise 16

activation pour un serveur Web d'entreprise 28

activation sur un serveur IIS 29

Sun Java System Web Server

configuration des composants Web 25

configuration et déploiement du fichier .war 26

modification de config.properties 26

test des rappels par Web 27

Sun Java System Web Server, version 19

U

utilitaires

osccmseheaders 13

utilitaires

osccregistersnmpextension 47

W

fichier .war

configuration sur un serveur Tomcat 24

