



A MITEL
PRODUCT
GUIDE

Unify OpenScape Contact Center Agile V11 R1

Systemverwaltungshandbuch

Systemverwaltungshandbuch

Service-Dokumentation

10/2020

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

Inhalt

1 Informationen zu diesem Handbuch	5
1.1 An wen richtet sich dieses Handbuch?	5
1.2 Formatierungskonventionen	5
1.3 Feedback zur Dokumentation	6
2 Konfigurieren einer Wandanzeige	7
2.1 Vorbereitungen	7
2.2 Konfigurieren der IP-Verbindung für eine Wandanzeige	7
3 Konfigurieren des Unternehmens-E-Mail-Servers	9
3.1 Anforderungen des Unternehmens-E-Mail-Servers	9
3.2 Planen der Microsoft Office 365-Installation	10
3.3 Planen der Bereitstellung von Google GSuite	11
3.4 Planen der Microsoft Exchange-Installation	11
3.4.1 Definieren benutzerdefinierter Kopfzeilen (nur Microsoft Exchange Server 2007, 2010 und 2013)	13
3.5 Planen der IBM Lotus Domino-Installation	14
3.5.1 Komprimieren der Datenbank	15
3.6 Einrichten einer sicheren Verbindung für einen E-Mail-Server	16
3.7 Verwenden der Authentifizierung: auf einem E-Mail-Server	17
3.8 Unterstützung des Leistungsmerkmals Reports per E-Mail versenden	17
4 Konfigurieren des Unternehmens-Webservers	19
4.1 Systemvoraussetzungen für das Verwenden von Webkomponenten	19
4.1.1 Voraussetzungen für den Unternehmens-Webserver	19
4.1.2 Webbrowser-Voraussetzungen	20
4.2 Konfigurieren von Webkomponenten	20
4.2.1 Konfigurieren eines IIS-Servers	20
4.2.2 Konfigurieren eines Tomcat-Servers	23
4.2.3 Konfigurieren eines Sun Java System Web-Servers	26
4.3 Einrichten einer sicheren Verbindung für einen Web-Server	28
4.3.1 Aktivieren von TLS auf einem IIS-Server	29
4.3.2 Aktivieren von TLS auf einem Tomcat- bzw. Sun Java-Server	30
4.4 Web Callback-Fehlercodes	31
5 Konfigurieren der Anwesenheitsintegration	33
5.1 Konfigurieren eines OpenScape UC Application-Benutzerkontos	33
5.2 Konfigurieren des externen LDAP-Verzeichnisses	34
6 Verwalten des Systems	35
6.1 Herunterfahren eines Server-Computers für die Systemwartung	35
6.2 Ändern des OpenScape Contact Center- oder Informix-Kennworts	36
6.3 Sichern der Datenbank	38
6.3.1 Planen einer Datenbanksicherung	39
6.3.2 Sichern der Datenbank mit dem ontape-Dienstprogramm	40
6.3.3 Wiederherstellen der Datenbank mit dem ontape-Dienstprogramm	42
6.3.4 Wiederherstellen einer mit dem ontape-Dienstprogramm erstellten Level-0-Sicherung	44
6.3.5 Sichern der Datenbank mit dem onbar-Dienstprogramm	44
6.3.6 Wiederherstellen der Datenbank mit dem onbar-Dienstprogramm	45
6.4 SNMP-Unterstützung	46
6.4.1 OpenScape Contact Center SNMP Extension Agent	46

Inhalt

6.4.2 OpenScape CAP Fault Management-Software	47
Index	49

1 Informationen zu diesem Handbuch

Dieses Handbuch beschreibt, wie Sie Drittanbieter-Hardware, wie z. B. Wandanzeigen, Unternehmens-E-Mail-Server und Unternehmens-Webserver, für die Integration mit dem Unify OpenScape Contact Center Agile V11 R1-System konfigurieren. Außerdem wird beschrieben, wie die regelmäßige Wartung des Unify OpenScape Contact Center Agile V11 R1 Systems durchzuführen ist, einschließlich der Sicherung und Wiederherstellung der Datenbank.

1.1 An wen richtet sich dieses Handbuch?

Dieses Handbuch richtet sich an Benutzer in der Organisation, die für die Verwaltung, Überwachung und Wartung des Status des Unify OpenScape Contact Center Agile V11 R1-Systems zuständig sind.

1.2 Formatierungskonventionen

In diesem Handbuch werden folgende Formatierungskonventionen verwendet:

Fettdruck

In dieser Formatierung erscheinen Unify OpenScape Contact Center Agile V11 R1 Komponenten, Fenster- und Dialogfeldtitel sowie Elementnamen.

Kursiv

In dieser Formatierung erscheinen Verweise auf verwandte Dokumentationen.

`Nichtproportionale Schrift`

In dieser Schrift erscheint Text, den Sie eingeben müssen oder der vom Computer in einer Meldung angezeigt wird.

HINWEIS: Hinweise heben Informationen hervor, die nützlich, aber nicht wesentlich sind, zum Beispiel Tipps oder alternative Methoden zum Durchführen einer Aufgabe.

WICHTIG: Wichtige Hinweise machen auf Aktionen aufmerksam, die den Betrieb der Anwendung beeinträchtigen oder zum Verlust von Daten führen können.

1.3 Feedback zur Dokumentation

Wenn Sie Probleme im Zusammenhang mit diesem Dokument mitteilen möchten, wenden Sie sich bitte an das Kundendienst-Center.

Bitte halten Sie bei Ihrem Anruf folgende Angaben bereit. Dadurch können wir das Dokument, mit dem Sie Schwierigkeiten haben, schneller identifizieren.

- **Titel:** Systemverwaltungshandbuch
- **Sachnummer:** A31003-S22B1-S101-01-0020

2 Konfigurieren einer Wandanzeige

Dieses Kapitel beschreibt, wie Sie eine Wandanzeige konfigurieren. Eine Wandanzeige ist eine elektronische Nachrichtentafel, über die Echtzeit-Statistikdaten und allgemeine Systeminformationen zum Contact-Center laufen und so für mehrere Benutzer gleichzeitig sichtbar sind. Das OpenScape Contact Center-System unterstützt Spectrum IP-Wandanzeigen (Version 4200 R) sowie kundenspezifische Wandanzeigen, die dem EZ Key II-Protokoll entsprechen.

WICHTIG: Wandanzeigen sollten nur von entsprechend geschultem Personal konfiguriert werden. Sollte nicht korrekt geschultes Personal versuchen, eine Wandanzeige zu konfigurieren, kann sich dies negativ auf den Betrieb des OpenScape Contact Center-Systems auswirken.

2.1 Vorbereitungen

Bevor Sie die Wandanzeige installieren und konfigurieren können, müssen Sie Folgendes tun:

- Wenn Sie über eine Serielle Spectrum-Wandanzeige verfügen, benötigen Sie ein Seriell-IP-Konverter-Kit (Nordamerika: NIU, Internationaler Markt: UDS100).
- Beschaffen Sie sich eine statische IP-Adresse für die Wandanzeige.
- Stellen Sie sicher, dass Sie unterstützte Firmware-Versionen haben, die mit dem OpenScape Contact Center-System kompatibel sind.

2.2 Konfigurieren der IP-Verbindung für eine Wandanzeige

Diese Prozedur beschreibt, wie Sie die IP-Verbindung für eine Wandanzeige konfigurieren. Es wird vorausgesetzt, dass Sie die Lantronix Device Server Configuration Utility 2.0-Software für die Wandanzeige bereits auf dem OpenScape Contact Center-Haupt-Server-Computer installiert haben.

WICHTIG: Es werden nur grundlegende Konfigurationsschritte beschrieben. Ausführliche Anweisungen und Vorsichtsmaßnahmen finden Sie in der Herstellerdokumentation.

Konfigurieren einer Wandanzeige

Konfigurieren der IP-Verbindung für eine Wandanzeige

So konfigurieren Sie die IP-Verbindung für eine Wandanzeige:

1. Schließen Sie die Wandanzeige an das LAN (Local Area Network) an.
2. Starten Sie die Lantronix Device Server Configuration Utility-Anwendung.
3. Klicken Sie im Menü **Datei** auf **Netzwerk suchen**.
4. Um das Netzwerk nach einer vorhandenen Wandanzeige zu durchsuchen, gehen Sie folgendermaßen vor:
 - a) Klicken Sie auf **Suche starten**.
 - b) Sobald die Wandanzeigegeräte im Netzwerk gefunden wurden, klicken Sie auf **Speichern**.
 - c) Wenn das System meldet, dass die Geräte gespeichert wurden, klicken Sie auf **OK**.
 - d) Klicken Sie auf **Zurück**.
5. Wählen Sie die IP-Adresse der zu konfigurierenden Wandanzeige aus.
6. Klicken Sie im Menü **Extras** auf **Devicemanager**.
7. Klicken Sie auf **Webkonfiguration**.
8. Klicken Sie auf **OK**. Damit wird der Lantronix Web-Manager gestartet.
9. Geben Sie unter **Reservierte Verbindung** die Portnummer der Wandanzeige in das Feld **Lokaler Port** ein, und klicken Sie auf **Einstellungen aktualisieren**.

HINWEIS: Um eine neue Baugruppe zu konfigurieren, die nicht bereits eine IP-Adresse hat, klicken Sie im Menü **Extras** auf **IP-Adresse zuweisen**. Lesen Sie die Hardware- bzw. Ethernet-Adresse auf der Rückseite der Wandanzeige ab, und geben Sie sie in das entsprechende Feld ein. Weisen Sie der Wandanzeige eine IP-Adresse zu, und klicken Sie auf **IP-Adresse festlegen**.

3 Konfigurieren des Unternehmens-E-Mail-Servers

Dieses Kapitel beschreibt, wie Sie den Unternehmens-E-Mail-Server so konfigurieren, dass er das OpenScape Contact Center-Leistungsmerkmal E-Mail und das Versenden von Reporten per E-Mail unterstützt. E-Mail-Nachrichten werden über den Unternehmens-E-Mail-Server an den OpenScape Contact Center E-Mail-Server weitergeleitet. Alle E-Mail-Nachrichten werden in einer einzelnen Mailbox auf dem Unternehmens-E-Mail-Server gespeichert.

Der OpenScape Contact Center E-Mail-Server und der Unternehmens-E-Mail-Server kommunizieren über das IMAP4-Protokoll. Die OpenScape Contact Center-Clientanwendungen und der Unternehmens-E-Mail-Server verwenden das IMAP4-Protokoll auch zum Abrufen und Verarbeiten von E-Mail-Nachrichten. Nachrichten-Anlagen werden mittels separater IMAP4- und MIME-Funktionen abgerufen. E-Mail-Antwortnachrichten werden vom E-Mail-Server über eine SMTP-Schnittstelle an Kunden gesendet.

HINWEIS: In der Manager-Anwendung wird der Hauptfirmenserver verwendet, um Berichte für Supervisoren und den Keep-Alive-Prozess zu senden

3.1 Anforderungen des Unternehmens-E-Mail-Servers

Folgende E-Mail-Server wurden zusammen mit dem OpenScape Contact Center-System getestet:

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

Weitere Informationen zu diesen Servern finden Sie in der Dokumentation der jeweiligen Hersteller.

HINWEIS: Es wird empfohlen, die Inhalte auf dem Unternehmens-E-Mail-Server zu schützen, um das Risiko zu verringern, dass E-Mail-Nachrichten versehentlich gelöscht werden.

Stellen Sie sicher, dass der Unternehmens-E-Mail-Server folgendermaßen konfiguriert ist:

- **Client-Zugriffslizenzen** – Stellen Sie sicher, dass Sie über ausreichende Client-Zugriffslizenzen verfügen. Jeder Benutzer, der auf den OpenScape Contact Center E-Mail-Server zugreifen kann, benötigt eine Client-Zugriffslizenz.

- **Benutzerdefinierte Kopfzeilen** – Da die E-Mail-Funktion von OpenScape Contact Center benutzerdefinierte Kopfzeilen verwendet, müssen Sie sicherstellen, dass der Unternehmens-E-Mail-Server benutzerdefinierte Kopfzeilen in E-Mail-Nachrichten weder herausfiltert noch entfernt.
- **IMAP-Sitzungen** – Für jeden Tag, dem aktive Nachrichten zugeordnet sind, wird eine IMAP-Sitzung benötigt. Jeder Benutzer benötigt eine IMAP-Sitzung, um eine E-Mail-Nachricht zu versenden oder den Inhalt einer E-Mail-Nachricht abzurufen.
- **Gleichzeitige Verbindungen** – Stellen Sie sicher, dass das E-Mail-Konto von OpenScape Contact Center mit einer ausreichenden Anzahl von Verbindungen konfiguriert wurde, um die Anzahl der Benutzer zu unterstützen, die gleichzeitig auf das Konto zugreifen werden.
- **Spamfilter und E-Mail-Adressblockierung** – Dies verhindert, dass unerwünschte E-Mail-Nachrichten an Benutzer weitergeleitet werden.
- **Antiviren-Software** – Ankommende E-Mail-Nachrichten und Anlagen vom Unternehmens-E-Mail-Server müssen auf Viren geprüft werden.

3.2 Planen der Microsoft Office 365-Installation

Planen Sie die Microsoft Office 365-Installation sorgfältig. Berücksichtigen Sie beim Konfigurieren der Nachrichten-Speicherdauer im OpenScape Contact Center E-Mail-Server unbedingt die Verfügbarkeit der Microsoft Office 365-Datenbank. Bei weiteren Informationen zu dieser sowie anderen in diesem Abschnitt beschriebenen Aufgaben ist die Vertragsvereinbarung zu Microsoft Office 365 zurate zu ziehen.

Sie müssen Folgendes konfigurieren:

- **Benutzerkonten** – Erstellen Sie ein neues Benutzerkonto zur Verwendung durch den OpenScape Contact Center E-Mail-Server. Sie müssen ein Kennwort für das neue Benutzerkonto angeben.
- **Einschränkungsrichtlinie** – Bei der Microsoft Office 365 Einschränkungrichtlinie wird die Nachrichtenrate für SMTP-Nachrichten auf maximal 30 Nachrichten pro Minute begrenzt. Um diese Einschränkung zu berücksichtigen, muss der OSCC-Parameter "Max. Nachrichtenrate" in den E-Mail-Einstellungen auf 30 (oder weniger) gesetzt werden.
- **IMAP-Sitzungen** – Microsoft Office 365 begrenzt die Anzahl der aktiven IMAP-Sitzungen auf 20 Sitzungen pro Konto. Um diese Einschränkung zu einzuhalten, muss der OSCC-Parameter "Max. Anzahl IMAP-Sitzungen" in den E-Mail-Einstellungen auf 20 gesetzt werden.

3.3 Planen der Bereitstellung von Google GSuite

Planen Sie die Google GSuite-Bereitstellung sorgfältig. Berücksichtigen Sie beim Konfigurieren der Nachrichten-Speicherdauer im OpenScape Contact Center E-Mail-Server unbedingt die Größe der Google GSuite-Datenbank. Bei weiteren Informationen zu dieser sowie anderen in diesem Abschnitt beschriebenen Aufgaben ist die Vertragsvereinbarung zu Google GSuite zurate zu ziehen.

Sie müssen die folgenden Konfigurationen vornehmen:

In Google GSuite:

- Erstellen Sie ein neues GMail-Benutzerkonto zur Verwendung durch den OpenScape Contact Center E-Mail-Server.
- Aktivieren Sie in den Gmail-Einstellungen auf den Registerkarten Weiterleitung und POP/IMAP die Option „IMAP-Zugriff“.
- In den Google Account-Sicherheitseinstellungen:
 - Erstellen Sie ein „Anwendungskennwort“ und verwenden Sie es im OpenScape Contact Center.
 - Aktivieren Sie die Option „allow less secure applications“ (weniger sichere Anwendungen zulassen).

Im OpenScape Contact Center:

- **IMAP-Sitzungen** - Google GSuite begrenzt die Anzahl der aktiven IMAP-Sitzungen auf 15 Sitzungen pro Konto. Damit der OSCC-Parameter gemäß dieser Beschränkung operieren kann, setzen Sie **Max. Anzahl IMAP-Sitzungen** in den E-Mail-Einstellungen auf 15, wovon fünf Sitzungen für den OSCC-E-Mail-Server reserviert sind.

3.4 Planen der Microsoft Exchange-Installation

Planen Sie die Microsoft Exchange-Installation sorgfältig. Berücksichtigen Sie beim Konfigurieren der Nachrichten-Speicherdauer im OpenScape Contact Center E-Mail-Server unbedingt die Größe der Microsoft Exchange-Datenbank. Weitere Informationen zu dieser und weiteren in diesem Abschnitt beschriebenen Aufgaben finden Sie in der Dokumentation zu Microsoft Exchange.

WICHTIG: Die Konfiguration von Microsoft Exchange muss von einem entsprechend geschulten Microsoft Exchange-Administrator durchgeführt werden.

Sie müssen Folgendes konfigurieren:

- **Benutzerkonten** – Erstellen Sie ein neues Benutzerkonto zur Verwendung durch den OpenScape Contact Center E-Mail-Server. Sie müssen ein Kennwort für das neue Benutzerkonto angeben.
- **Aliase (optional)** – Falls erforderlich, konfigurieren Sie zusätzliche SMTP-E-Mail-Adressen, die als Aliase für das neue Benutzerkonto verwendet werden.

Wenn Sie Ihren Kunden mehrere Kontakt-E-Mail-Adressen präsentieren möchten, müssen Sie für jede zusätzliche E-Mail-Adresse einen Aliasnamen konfigurieren, der auf das neue Benutzerkonto verweist. Durch Erstellen eines Alias wird sichergestellt, dass E-Mail-Nachrichten, die an den Unternehmens-E-Mail-Server gesendet werden, an das Postfach des OpenScape Contact Center E-Mail-Servers zur Bearbeitung durch einen Agenten weitergeleitet werden. Weitere Informationen finden Sie in der *Manager-Hilfe*.

Da Microsoft Exchange Server 2007 bei Nachrichten mit internem und externem Ursprung Aliase in die Hauptbenutzerkonto-Adresse konvertiert, müssen Sie ein Exchange-Postfach für jeden Alias konfigurieren, den Sie verwenden möchten, und veranlassen, dass das Postfach Nachrichten an das Hauptbenutzerkonto weiterleitet. Dadurch wird sichergestellt, dass eine E-Mail-Nachricht, die ein Kunde an einen Alias wie z. B. sales@company.com sendet, korrekt weitergeleitet werden kann. Außerdem wird sichergestellt, dass die eingehende E-Mail-Adresse beim Antworten nicht in die Hauptkontoadresse konvertiert wird.

- **Einschränkungsrichtlinie (Microsoft Exchange Server 2013)** – Bei Verwendung von Microsoft Exchange Server 2013 können die Werte ImapMaxBurst und ImapRechargeRate in der Einschränkungsrichtlinie den E-Mail-Durchsatz des OpenScape Contact Center E-Mail-Kontos negativ beeinflussen. Um einen maximalen Durchsatz zu erreichen, sollten Sie für das OpenScape Contact Center E-Mail-Konto eine eigene Einschränkungsrichtlinie erstellen und dort die Werte für ImapMaxBurst und ImapRechargeRate auf 8000000 oder höher setzen.
- **Shadow-Redundanz (Microsoft Exchange Server 2013)** – Bei Verwendung von Microsoft Exchange Server 2013 können das Leistungsmerkmal Shadow-Redundanz und die Transportkonfigurations-Einstellungen den E-Mail-Durchsatz des OpenScape Contact Center E-Mail-Kontos negativ beeinflussen. Um einen maximalen Durchsatz zu erreichen, sollten Sie das Flag ShadowRedundancyEnabled auf false setzen.

3.4.1 Definieren benutzerdefinierter Kopfzeilen (nur Microsoft Exchange Server 2007, 2010 und 2013)

In Microsoft Exchange Server 2007, 2010 und 2013 sind benutzerdefinierte Kopfzeilen, die von der E-Mail-Funktionalität von OpenScape Contact Center benötigt werden, möglicherweise nicht über die Microsoft Exchange IMAP-Schnittstelle verfügbar. Wenn Sie Microsoft Exchange Server 2007, 2010 oder 2013 als Ihren unternehmensweiten IMAP-E-Mail-Server verwenden möchten, müssen Sie ein Dienstprogramm (`osccmseheaders.exe`) ausführen, das eine spezielle E-Mail-Nachricht über die Microsoft Exchange SMTP-Schnittstelle sendet. Nachdem die spezielle E-Mail-Nachricht gesendet wurde, sind die erforderlichen benutzerdefinierten Kopfzeilen über die Microsoft Exchange IMAP-Schnittstelle verfügbar.

Bevor Sie das Dienstprogramm ausführen, müssen Sie Folgendes tun:

- Konfigurieren Sie Microsoft Exchange Server darauf, authentifiziertes SMTP zu unterstützen. Das Dienstprogramm verwendet eine authentifizierte SMTP-Sitzung, um die benutzerdefinierten Kopfzeilen zu definieren. Falls erforderlich, können Sie authentifiziertes SMTP deaktivieren, nachdem das Dienstprogramm erfolgreich ausgeführt wurde.
- Wenn Sie Microsoft Exchange Server 2007 SP2 oder höher verwenden, führen Sie in der Exchange-Verwaltungsshell auf dem Microsoft Exchange Server Computer folgenden Befehl aus:

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

Falls erforderlich, können Sie nach der Ausführung des Dienstprogramms zu dem vorherigen Wert der `HeaderPromotionModeSetting`-Eigenschaft zurückkehren.

So definieren Sie benutzerdefinierte Kopfzeilen:

1. Navigieren Sie auf dem Haupt-Server-Computer zu dem Ordner, in dem die OpenScape Contact Center-Software installiert ist, und doppelklicken Sie auf die Datei **osccmseheaders.exe**. Ein Eingabeaufforderungsfenster wird geöffnet.
2. Drücken Sie die **Eingabetaste**, um fortzufahren.
3. Geben Sie an der Eingabeaufforderung **From address** (Von-Adresse) die E-Mail-Adresse ein, die Sie beim Senden der speziellen E-Mail-Nachricht als Absenderadresse verwenden möchten, und drücken Sie anschließend die **Eingabetaste**. Dies muss die E-Mail-Adresse sein, die mit dem Benutzerkonto verbunden ist, das zur Authentifizierung bei Microsoft Exchange Server verwendet wird, zum Beispiel das Standardkonto "OSCEmail".

4. Geben Sie an der Eingabeaufforderung **To address** (An-Adresse) die E-Mail-Adresse ein, an die Sie die spezielle E-Mail-Nachricht senden möchten, und drücken Sie anschließend die **Eingabetaste**. Dies muss eine bekannte E-Mail-Adresse auf dem Microsoft Exchange Server sein.
5. Geben Sie an der Eingabeaufforderung **Subject** (Betreff) einen Betreff für die spezielle E-Mail-Nachricht ein, und drücken Sie anschließend die **Eingabetaste**.
6. Geben Sie an der Eingabeaufforderung **SMTP server host name** (Hostname des SMTP-Servers) den Hostnamen des Microsoft Exchange Server-Computers ein, und drücken Sie die **Eingabetaste**.
7. Geben Sie an der Eingabeaufforderung **SMTP server port number** (Portnummer des SMTP-Servers) die Portnummer ein, die auf dem Microsoft Exchange Server-Computer für SMTP konfiguriert wurde, und drücken Sie die **Eingabetaste**.
8. Geben Sie an der Eingabeaufforderung **SMTP user name** (SMTP-Benutzername) den Benutzernamen für das Microsoft Exchange Server-Konto ein, von dem aus die spezielle E-Mail-Nachricht gesendet wird, und drücken Sie die **Eingabetaste**. Das Konto muss in der Lage sein, eine E-Mail-Nachricht unter Verwendung der in Schritt 3 definierten Absenderadresse zu versenden.
9. Geben Sie an der Eingabeaufforderung **SMTP password** (SMTP-Kennwort) das Kennwort für das Microsoft Exchange Server-Konto ein, von dem aus die spezielle E-Mail-Nachricht gesendet wird, und drücken Sie die **Eingabetaste**.

3.5 Planen der IBM Lotus Domino-Installation

Damit das OpenScape Contact Center-System Lotus Domino verwenden kann, müssen Sie ein IMAP-fähiges Postfach konfigurieren, an das E-Mail-Nachrichten von Benutzern übermittelt werden. Stellen Sie sicher, dass Sie die Option **Format preference for incoming mail** auf dem Postfach als **Prefers MIME** konfigurieren. Informationen zum Durchführen von dieser und weiteren in diesem Abschnitt beschriebenen Aufgaben finden Sie in der Lotus Domino-Dokumentation.

WICHTIG: Die Konfiguration von Lotus Domino muss von einem entsprechend geschulten Lotus Domino-Administrator durchgeführt werden.

Wenn Sie Ihren Kunden mehrere Kontakt-E-Mail-Adressen präsentieren möchten, müssen Sie für jede zusätzliche E-Mail-Adresse einen Aliasnamen konfigurieren, der auf das IMAP-fähige Postfach verweist. Durch Erstellen eines Alias wird sichergestellt, dass E-Mail-Nachrichten, die an den Unternehmens-E-

Mail-Server gesendet werden, an das Postfach des OpenScape Contact Center E-Mail-Servers zur Bearbeitung durch einen Benutzer weitergeleitet werden. Weitere Informationen finden Sie in der *Manager-Hilfe*.

Informationen zu den folgenden Themen finden Sie in der Lotus Domino Administrator-Hilfe:

- Sicherheit für konfigurierte Aliase
- Konfigurieren des SMTP-Routing

WICHTIG: Stellen Sie sicher, dass auf der von Ihnen erstellten Datenbank **sofortige Volltextindizierung** aktiviert ist. Wenn Sie die automatische Volltextindizierung nicht aktivieren, schlagen IMAP-Suchen fehl, und die Leistung des OpenScape Contact Center E-Mail-Servers wird erheblich beeinträchtigt.

3.5.1 Komprimieren der Datenbank

Wenn Sie die Lotus Domino-Datenbank komprimieren, identifiziert der OpenScape Contact Center E-Mail-Server den Unternehmens-E-Mail-Server als nicht betriebsbereit, weil der IMAP-Zugriff auf die Datenbank unterbrochen ist. Die Art der verwendeten Datenbankkomprimierung beeinflusst, wie lange der OpenScape Contact Center E-Mail-Server auf die Lotus Domino-Datenbank zugreifen kann. Es wird empfohlen, die Option **In-place compacting with space recovery only** (Flag -b) auszuwählen. Dies ist die schnellste Methode und wirkt sich nur minimal auf das System aus.

WICHTIG: Es wird nachdrücklich empfohlen, die Unternehmens-E-Mail-Server-Datenbank während der Wartung der OpenScape Contact Center-Daten zu komprimieren. Andernfalls könnte die Verarbeitung von E-Mail-Nachrichten im OpenScape Contact Center-System nachteilig beeinflusst werden.

3.6 Einrichten einer sicheren Verbindung für einen E-Mail-Server

Um eine sichere SSL-Verbindung zwischen dem Unternehmens-E-Mail-Server und dem OpenScape Contact Center E-Mail-Server einzurichten, müssen Sie folgende Schritte durchführen:

- Installieren Sie ein SSL-Zertifikat und aktivieren Sie SSL-Sicherheit für auf dem Unternehmens-E-Mail-Server eingehende (IMAP4) und/oder ausgehende (SMTP) E-Mail-Nachrichten. Befolgen Sie die Anweisungen des Herstellers oder kontaktieren Sie Ihren E-Mail-Anbieter, falls Sie Hilfe benötigen.

HINWEIS: Lotus Domino-Server ermöglichen SSL-gesicherte Verbindungen auf einem bestimmten Port, auch wenn der Port nicht darauf konfiguriert ist, die Verwendung von SSL zu erfordern. Dies führt zu keinerlei Betriebsproblemen. Administratoren sollten jedoch beachten, dass OpenScape Contact Center zwar eine sichere Verbindung zum Domino-Server aufbauen kann, dies jedoch kein eindeutiges Anzeichen dafür ist, dass die Verwendung von SSL auch für Verbindungen erzwungen wird, die von anderen E-Mail-Clients hergestellt werden. Falls Sie eine sichere Domino-Umgebung benötigen, müssen Sie dazu sorgfältig Ihre Domino-Konfiguration überprüfen.

- Aktivieren Sie SSL-Sicherheit für den entsprechenden IMAP-Server und/oder SMTP-Server in der Manager-Anwendung. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

Es wird empfohlen, das Zertifikat von einer anerkannten Zertifizierungsstelle, wie z. B. VeriSign, zu beziehen. Es werden jedoch auch selbstsignierte Zertifikate unterstützt. In beiden Fällen muss das Zertifikat ein vertrauenswürdiges Zertifikat sein.

Hinweis: Wenn Sie ein Zertifikat verwenden, das selbst generiert wurde oder von einer Zertifizierungsstelle generiert wurde, und das nicht mit dem standardmäßigen Java-Schlüsselspeicher verbunden ist, und Sie ein neues SSL-Zertifikat auf den unternehmenseigenen E-Mail-Servern installieren möchten, müssen Sie möglicherweise das entsprechende Root- und Intermediate-Zertifikat im Schlüsselspeicher des JAVA-Pakets hinzufügen, das von Agenten-Portal verwendet wird. Das Zertifikat kann mit folgendem Befehl zum Schlüsselspeicher hinzugefügt werden (aus dem Verzeichnis <Java>\bin):

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

3.7 Verwenden der Authentifizierung: auf einem E-Mail-Server

Beim OpenScape Contact Center-System ist die Authentifizierung für den IMAP-Server obligatorisch und für den SMTP-Server optional. Die Authentifizierungseinstellungen auf dem Unternehmens-E-Mail-Server müssen denen im OpenScape Contact Center-System entsprechen.

So aktivieren Sie die Authentifizierung in Microsoft Exchange:

- Wählen Sie **Standardauthentifizierung** aus.
- Wenn Sie SSL aktiviert haben, denken Sie daran, die Option Verschlüsselung erforderlich zu aktivieren.

So aktivieren Sie die Authentifizierung in IBM Lotus Domino:

- Das OpenScape Contact Center-System verwendet weder keine Clientzertifikate. Stellen Sie also sicher, dass in den SSL-Authentifizierungsoptionen **Clientzertifikat** auf **Nein** und **Name und Kennwort** auf **Ja** gesetzt sind.

3.8 Unterstützung des Leistungsmerkmals Reporte per E-Mail versenden

Um das Leistungsmerkmal Reporte per E-Mail versenden nutzen zu können, muss der OpenScape Contact Center E-Mail-Server in der Lage sein, E-Mail-Nachrichten über den Unternehmens-E-Mail-Server zu senden, wobei eine andere Von-Adresse verwendet wird als die, mit der sich der OpenScape Contact Center E-Mail-Server beim Unternehmens-E-Mail-Server anmeldet.

Der Zweck dieser Konfiguration ist, dass der OpenScape Contact Center E-Mail-Server E-Mail-Nachrichten für andere SMTP-E-Mail-Konten versenden kann. Wenn der OpenScape Contact Center E-Mail-Server zum Beispiel als "oscc@company.com" beim Unternehmens-E-Mail-Server angemeldet ist, und es wird eine E-Mail-Nachricht für "manager@company.com" gesendet, soll der Empfänger der Nachricht als Absender "Von: manager@company.com" und nicht "Von: oscc@company.com für manager@company.com" sehen.

Konfigurieren des Unternehmens-E-Mail-Servers

Unterstützung des Leistungsmerkmals Reporte per E-Mail versenden

Wenn der Unternehmens-E-Mail-Server für SMTP-Authentifizierung konfiguriert ist und SMTP-Relaying eingeschränkt ist, kann diese Funktionalität wie folgt hergestellt werden:

- **Microsoft Exchange Server 2007, 2010 und 2013** – Wenn Sie E-Mail-Nachrichten von E-Mail-Adressen senden müssen, die in derselben Domäne sind, können Sie dem OpenScape Contact Center E-Mail-Server-Konto auf dem Unternehmens-E-Mail-Server über Active Directory die volle Berechtigung für jedes der Postfächer des OpenScape Contact Center-Benutzers erteilen. Sie müssen außerdem einen neuen Kontakt im Active Directory mit der SMTP-E-Mail-Adresse OSCCEmail@company.com erstellen und anschließend dem E-Mail-Konto des OpenScape Contact Center-Server-Computers die Berechtigung Senden als für den neuen Kontakt erteilen. Einzelheiten hierzu finden Sie in der Microsoft Exchange Server-Dokumentation.
- **Nur Microsoft Exchange Server 2007, 2010 und 2013** – Wenn Sie E-Mail-Nachrichten von E-Mail-Adressen senden müssen, die sich außerhalb der Domäne befinden, können Sie einen benutzerdefinierten Empfangsconnector konfigurieren. Einzelheiten zum Konfigurieren eines Empfangsconnectors finden Sie in der Dokumentation zu Microsoft Exchange Server.
- **Lotus Domino 8.0 und 8.5** – Als einzige Voraussetzung müssen Sie sicherstellen, dass der Wert des Parameters SMTPVerifyAuthenticatedSender 0 ist. Einzelheiten zu dieser Einstellung finden Sie in der Dokumentation zu Lotus Domino.

4 Konfigurieren des Unternehmens-Webservers

Dieses Kapitel enthält detaillierte Anleitungen zum Konfigurieren der für die Unterstützung des OpenScape Contact Center-Leistungsmerkmals Web Callback notwendigen Webkomponenten-Dateien auf dem Unternehmens-Webserver. Es beschreibt außerdem, wie Sie eine sichere Verbindung für den Unternehmens-Webserver-Computer einrichten, die Standarddateien lokalisieren und anpassen und allgemeine Probleme behandeln.

WICHTIG: Bevor Sie die Dateien auf dem Unternehmens-Webserver-Computer aktualisieren, kopieren Sie alle angepassten Webkomponenten-Dateien an einen sicheren Ort, sodass Sie sie nach erfolgter Aktualisierung wieder anwenden können. Wenn Sie dies unterlassen, gehen alle angepassten Dateien verloren, da diese beim Upgradevorgang nicht übernommen werden.

HINWEIS: Wenn Sie Webseiten erstellen oder anpassen, um diese mit den Webfunktionen von OpenScape Contact Center zu nutzen, sollten Sie angemessene Vorkehrungen treffen, um die Gefahr von Sicherheitslücken zu minimieren.

4.1 Systemvoraussetzungen für das Verwenden von Webkomponenten

Damit die Webkomponenten-Dateien ordnungsgemäß funktionieren, müssen Sie sicherstellen, dass der für den Zugriff auf die Leistungsmerkmale verwendete Unternehmens-Webserver und Webbrowser die in diesem Abschnitt genannten Voraussetzungen erfüllen.

4.1.1 Voraussetzungen für den Unternehmens-Webserver

Der Unternehmens-Webserver kann einen beliebigen der folgenden Web-Server mit den entsprechenden Betriebssystemen verwenden:

- Microsoft Internet Information Server (IIS) 8 und 8.5
- Apache Tomcat 6.0 auf Red Hat Enterprise Linux 6 Server
- Apache Tomcat 7.0.63 auf Red Hat Enterprise Linux 6 Server

4.1.2 Webbrowser-Voraussetzungen

Folgende Webbrowser wurden zusammen mit dem OpenScape Contact Center-System getestet:

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

Weitere Informationen zu diesen Servern finden Sie in der Dokumentation der jeweiligen Hersteller.

Stellen Sie sicher, dass der Webbrowser wie folgt konfiguriert ist:

- Sicherheitseinstellung für das Internet ist auf mittel oder niedrig gesetzt
- Javascript ist aktiviert
- Popups sind aktiviert (der Popup-Blocker ist deaktiviert oder so konfiguriert, dass Popups von dieser Webseite zugelassen sind)

4.2 Konfigurieren von Webkomponenten

Dieser Abschnitt beschreibt, wie Sie die Webkomponenten abhängig vom Typ des installierten Web-Servers konfigurieren.

HINWEIS: Als Folge der Konfiguration des Web Interaction-Servers müssen Sie möglicherweise die Webkomponenten zusätzlich konfigurieren. So müssen Sie möglicherweise eine sichere Verbindung für einen Webserver einrichten. Einzelheiten hierzu finden Sie unter Abschnitt 4.3, "Einrichten einer sicheren Verbindung für einen Web-Server", auf Seite 28.

4.2.1 Konfigurieren eines IIS-Servers

In diesem Abschnitt ist das Konfigurieren der Webkomponenten auf einem IIS-Server beschrieben. Informationen zu Installation und Konfiguration des IIS-Servers finden Sie in der Windows-Dokumentation.

HINWEIS: OpenScape Contact Center verwendet eine Systemüberwachungsfunktion, um die Verbindung zwischen dem Unternehmens-Webserver und dem Web Interaction-Server zu überwachen. Auf einem IIS-Server gibt es mehrere Konfigurationen, z.B. Anwendungspool-Recycling, die bewirken können, dass die OpenScape Contact Center-ISAPI-Komponente deaktiviert wird. Wenn dies eintritt, weist die System Monitor-

Anwendung darauf hin, dass die Verbindung unterbrochen wurde. Um dieses Problem zu vermeiden, ändern Sie die Konfiguration wie in der Windows-Dokumentation beschrieben.

HINWEIS: Wenn der IIS-Server auf einem 64-Bit-Betriebssystem ausgeführt wird, muss der IIS-Server darauf konfiguriert werden, 32-Bit-Webanwendungen auszuführen, weil die OpenScape Contact Center ISAPI-DLL eine 32-Bit-Datei ist.

4.2.1.1 Konfigurieren der Webkomponenten-Dateien auf einem IIS-Server

Sie müssen die Webkomponenten-Dateien von der OpenScape Contact Center-DVD auf den Unternehmens-Server-Computer kopieren und die Dateien anschließend aktualisieren.

So konfigurieren Sie die Webkomponenten-Dateien auf einem IIS-Server:

1. Legen Sie auf dem Unternehmens-Webserver-Computer einen Ordner für die Webkomponenten-Dateien an. Beispiel:
`c:\HPPC`
2. Legen Sie die OpenScape Contact Center-DVD in das DVD-ROM-Laufwerk ein.
3. Gehen Sie auf der DVD zum Ordner **OpenScape Contact Center Web Components\IIS**.
4. Kopieren Sie die Datei **HPPCAgileWeb.zip** auf den Unternehmens-Webserver-Computer, und dekomprimieren Sie die Datei in den in Schritt 1 erstellten Ordner. Die folgende Dateistruktur wird erstellt:

`c:\HPPC\Default.htm`

`c:\HPPC\hppcwis.dll`

`c:\HPPC\HPWC.ini`

`c:\HPPC\html`

`c:\HPPC\html\WCCallbackMain.htm`

`c:\HPPC\html\english` (und entsprechende Dateien)

c:\HPPC \images (und entsprechende Dateien)

WICHTIG: Ändern Sie diese Dateistruktur nicht, da sie für die korrekte Ausführung der Dateien erforderlich ist.

5. Öffnen Sie die Datei **HPWC.ini** in einem Texteditor, und ändern Sie unter **[HPPCSETTINGS]** die Einstellung **Address** in den Hostnamen bzw. die IP-Adresse des OpenScape Contact Center-Haupt-Server-Computers.

WICHTIG: Stellen Sie sicher, dass die Einstellung für **Port** der in der Manager-Anwendung konfigurierten Portnummer entspricht und dass der Port in der Firewall zwischen dem Unternehmens-Webserver-Computer und dem OpenScape Contact Center-Haupt-Server-Computer geöffnet ist. Die standardmäßige Portnummer ist 6021. Wenn Sie die Portnummer ändern, müssen Sie den Unternehmens-Webserver-Computer und den Web Interaction-Server neu starten.

6. Speichern und schließen Sie die Datei.
7. Erstellen Sie in IIS ein neues virtuelles Verzeichnis für die Standard-Website. Einzelheiten finden Sie in der Windows-Dokumentation. Achten Sie beim Erstellen des virtuellen Verzeichnisses auf Folgendes:
 - Geben Sie ein Alias wie z.B. HPPC an.
 - Wählen Sie den in Schritt 1 angelegten Ordner, wenn das System Sie zur Angabe des Verzeichnisses für die Website-Inhalte auffordert.
 - Aktivieren Sie folgende Zugriffsberechtigungen:
 - Lesen
 - Skripts ausführen (z.B. ASP)
 - Ausführen (z.B. ISAPI-Anwendungen oder CGI)

WICHTIG: Stellen Sie im IIS-Manager für IIS im Knoten Webdienstenerweiterungen sicher, dass ISAPI-Erweiterungen den Status **zulässig** haben. Andernfalls wird der Fehler 404 zurückgegeben, wenn das System versucht, die OpenScape Contact Center-ISAPI-Funktionalität aufzurufen. Wenn Sie die ISAPI-Erweiterungen einzeln aktivieren oder deaktivieren möchten, suchen Sie in der Hilfe der Microsoft Management Console nach Informationen zum Aktivieren oder Deaktivieren von dynamischen Inhalten bei Server-Konfigurationen.

4.2.1.2 Testen von Web Callback auf einem IIS-Server

Dieser Abschnitt beschreibt, wie Sie die Web Callback-Funktionalität auf einem IIS-Server testen.

So testen Sie Web Callback auf einem IIS-Server:

1. Öffnen Sie einen Webbrowser und geben Sie die URL ein, mit der Sie auf die Demoseite WCCallbackMain.htm zugreifen. Das Format des URL ist:

`http://<Hostname>/<VirtuellerPfad>/html/WCCallbackMain.htm`

dabei gilt:

- <Hostname> ist der Hostname oder die IP-Adresse des Unternehmens-Webserver-Computers.
- <VirtuellerPfad> ist der Pfad zu dem virtuellen Verzeichnis, das Sie eingerichtet haben.

Beispiel:

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

2. Klicken Sie auf der Seite WCCallbackMain.htm auf die Schaltfläche **Web Callback versuchen**. Wenn eine Seite geöffnet wird, die Felder mit Kontaktinformationen eines Kunden anzeigt, haben Sie die Seite **WebCallback.htm** geladen und Web Callback in einer Standardkonfiguration auf dem Web-Server erfolgreich konfiguriert.

HINWEIS: Wenn Sie an diesem Punkt auf **WebCallback.htm** auf die Schaltfläche **Abschicken** klicken, kann eine Fehlermeldung angezeigt werden. Sie können auf diese Schaltfläche klicken, nachdem die Webserver-Konfiguration abgeschlossen ist.

3. Konfigurieren Sie den Web Interaction-Server auf dem OpenScape Contact Center-Haupt-Server-Computer. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

4.2.2 Konfigurieren eines Tomcat-Servers

In diesem Abschnitt ist das Konfigurieren der Web Collaboration-Einstellungen auf einem Tomcat-Server beschrieben. Informationen zum Installieren und Konfigurieren des Tomcat-Servers selbst oder zum Verbinden von Tomcat mit dem Apache-Server finden Sie in der Dokumentation zum Tomcat-Server.

4.2.2.1 Konfigurieren der .war-Datei auf einem Tomcat-Server

Dieser Abschnitt beschreibt die Konfiguration und Verwendung der WAR-Datei auf einem Tomcat-Server.

So konfigurieren Sie die WAR-Datei auf einem Tomcat-Server:

1. Legen Sie die OpenScape Contact Center-DVD in das DVD-ROM-Laufwerk ein.
2. Gehen Sie auf der DVD zum Ordner **OpenScape Contact Center Web Components\Apache Tomcat**.
3. Kopieren Sie die Datei **HPPCAgileWeb.war** auf den Unternehmens-Webserver-Computer.
4. Benennen Sie die .war-Datei Ihrer Umgebung entsprechend um. In der folgenden Anleitung wurde der Name der .war-Datei in **HPPC.war** geändert. Hierdurch wird dieselbe Web-Beispielanwendung namens HPPC bereitgestellt. Der Name der .war-Datei muss wie gezeigt in Großbuchstaben angegeben werden, damit die Beispielkonfiguration funktioniert.
5. Stellen Sie sicher, dass der Java Development Kit (JDK) installiert ist.
6. Um die Datei config.properties in einen neuen Ordner mit der Bezeichnung hpwcapp zu extrahieren, öffnen Sie ein Eingabeaufforderungsfenster, wechseln Sie zu dem Verzeichnis, das die Datei HPPC.war enthält, geben Sie an der Eingabeaufforderung Folgendes ein, und drücken Sie anschließend die **Eingabetaste**:

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

7. Öffnen Sie die Datei **hpwcapp/config.properties** in einem Texteditor, und gehen Sie folgendermaßen vor:
 - Ändern Sie die Einstellung **servlet.name** in den Namen der in Schritt 4 angegebenen .war-Datei. In der Beispielkonfiguration lautet die Einstellung `servlet.name=/HPPC/hppcwebchat`.
 - Ändern Sie die Einstellung **socket.server.name** in den Hostnamen oder die IP-Adresse des OpenScape Contact Center-Haupt-Server-Computers.

HINWEIS: Stellen Sie sicher, dass die Einstellung für **socket.server.port** der in der Manager-Anwendung konfigurierten Portnummer entspricht und dass der Port in der Firewall zwischen dem Unternehmens-Webserver-Computer und dem OpenScape Contact Center-Haupt-Server-Computer geöffnet ist. Die standardmäßige Portnummer ist 6021. Wenn Sie die Portnummer ändern, müssen Sie den Unternehmens-Webserver-Computer und den Web Interaction-Server neu starten.

8. Speichern und schließen Sie die Datei.
9. Um die Datei HPPC.war zu aktualisieren, geben Sie an der Eingabeaufforderung im selben Verzeichnis wie in Schritt 6 Folgendes ein:

```
jar ufv HPPC.war hpwcapp/config.properties
```
10. Stellen Sie die Datei HPPC.war auf dem Tomcat-Server bereit. Einzelheiten hierzu finden Sie in der Dokumentation zu Tomcat Web Application Manager.

4.2.2.2 Testen von Web Callback auf einem Tomcat-Server

In diesem Abschnitt wird das Testen der Web Callback-Funktionalität auf einem Tomcat-Server beschrieben.

So testen Sie Web Callback auf einem Tomcat-Server:

1. Öffnen Sie einen Webbrowser und geben Sie die URL ein, mit der Sie auf die Demoseite WCCallbackMain.htm zugreifen. Das Format des URL ist:

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

Dabei ist <Hostname> der Hostname oder die IP-Adresse des Unternehmens-Webserver-Computers.

Beispiel:

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

2. Klicken Sie auf der Seite WCCallbackMain.htm auf die Schaltfläche **Web Callback versuchen**. Wenn eine Seite geöffnet wird, die Felder mit Kontaktinformationen eines Kunden anzeigt, haben Sie die Seite **WebCallback.htm** geladen und Web Callback in einer Standardkonfiguration auf dem Tomcat-Server erfolgreich konfiguriert.

HINWEIS: Wenn Sie an diesem Punkt auf **WebCallback.htm** auf die Schaltfläche **Abschicken** klicken, kann eine Fehlermeldung angezeigt werden. Sie können auf diese Schaltfläche klicken, nachdem die Webserver-Konfiguration abgeschlossen ist.

3. Konfigurieren Sie den Web Interaction-Server auf dem OpenScape Contact Center-Haupt-Server-Computer. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

4.2.3 Konfigurieren eines Sun Java System Web-Servers

Dieser Abschnitt beschreibt die Konfiguration der Webkomponenten auf einem Sun Java System Web Server. Informationen zur Installation und Konfiguration des Sun Java System Web Servers finden Sie in der Sun-Dokumentation.

4.2.3.1 Konfigurieren der WAR-Datei auf einem Sun Java System Web Server

Dieser Abschnitt beschreibt die Konfiguration und Verwendung der WAR-Datei auf einem Sun Java System Web Server.

So konfigurieren Sie die WAR-Datei auf einem Sun Java System Web Server:

1. Legen Sie die OpenScape Contact Center-DVD in das DVD-ROM-Laufwerk ein.
2. Gehen Sie auf der DVD zum Ordner **OpenScape Contact Center Web Components\Sun Java System Web Server**.
3. Kopieren Sie die Datei **HPPCAgileWeb.war** auf den Unternehmens-Webserver-Computer.
4. Benennen Sie die .war-Datei Ihrer Umgebung entsprechend um. In der folgenden Anleitung wurde der Name der .war-Datei in **HPPC.war** geändert. Hierdurch wird dieselbe Web-Beispielanwendung namens HPPC bereitgestellt. Der Name der .war-Datei muss wie gezeigt in Großbuchstaben angegeben werden, damit die Beispielkonfiguration funktioniert.
5. Um die Datei config.properties in einen neuen Ordner mit der Bezeichnung hpwcapp zu extrahieren, öffnen Sie ein Eingabeaufforderungsfenster, wechseln Sie zu dem Verzeichnis, das die Datei HPPC.war enthält, geben Sie die folgende Befehlszeile ein, und drücken Sie anschließend die **Eingabetaste**:

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

6. Öffnen Sie die Datei **hpwcapp/config.properties** in einem Texteditor, und gehen Sie folgendermaßen vor:
 - Ändern Sie die Einstellung **servlet.name** in den Namen der in Schritt 4 angegebenen .war-Datei. In der Beispielkonfiguration lautet die Einstellung `servlet.name=/HPPC/hppcwebchat`.
 - Ändern Sie die Einstellung **socket.server.name** in den Hostnamen oder die IP-Adresse des OpenScape Contact Center-Haupt-Server-Computers.

HINWEIS: Stellen Sie sicher, dass die Einstellung für **socket.server.port** der in der Manager-Anwendung konfigurierten Portnummer entspricht und dass der Port in der Firewall zwischen dem Unternehmens-Webserver-Computer und dem OpenScape Contact Center-Haupt-Server-Computer geöffnet ist. Die standardmäßige Portnummer ist 6021. Wenn Sie die Portnummer ändern, müssen Sie den Unternehmens-Webserver-Computer und den Web Interaction-Server neu starten.

7. Speichern und schließen Sie die Datei.
8. Um die Datei HPPC.war zu aktualisieren, geben Sie an der Eingabeaufforderung im selben Verzeichnis wie in Schritt 5 Folgendes ein:

```
jar ufv HPPC.war hpwcapp/config.properties
```
9. Gehen Sie zur Administrator-Website für Sun Java System Web Server und richten Sie eine neue Server-Instanz ein. Um auf die Administratorseite zuzugreifen, öffnen Sie einen Webbrowser, und geben Sie den URL ein. Das Format des URL ist:

`http://<Hostname>/https-admserv/bin/index`

Dabei ist `<Hostname>` der Hostname oder die IP-Adresse des Unternehmens-Webserver-Computers.

Nutzen Sie beim Einrichten der Serverinstanz **HPPC** als Server-ID. Damit wird automatisch ein Ordner mit dem Namen **/https-HPPC** angelegt. Einzelheiten finden Sie in der Sun-Dokumentation.

HINWEIS: Wenn Sie das Kontrollkästchen **Never attempt to resolve IP addresses into host names** aktivieren, müssen Sie bei Ihrer Konfiguration konsistent vorgehen. Das bedeutet, dass Sie entweder IP-Adressen oder Hostnamen, nicht jedoch beides verwenden können.

10. Starten Sie die neue Server-Instanz.

Konfigurieren des Unternehmens-Webservers

Einrichten einer sicheren Verbindung für einen Web-Server

11. Stellen Sie die Datei HPPC.war auf dem Sun Java System Web-Server bereit. Einzelheiten finden Sie in der Sun-Dokumentation. Der Anwendungs-URL zum Bereitstellen der .war-Datei ist **/HPPC**.

4.2.3.2 Testen von Web Callback auf einem Sun Java System Web-Server

Dieser Abschnitt beschreibt das Testen von Web Callback auf dem Sun Java System Web Server.

So testen Sie Web Callback auf einem Sun Java System Web Server:

1. Starten Sie die in Abschnitt 4.2.3.1, "Konfigurieren der WAR-Datei auf einem Sun Java System Web Server", auf Seite 26 eingerichtete Server-Instanz.
2. Öffnen Sie einen Webbrowser und geben Sie die URL ein, mit der Sie auf die Demoseite WCCallbackMain.htm zugreifen. Das Format des URL ist:

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

Dabei ist <Hostname> der Hostname oder die IP-Adresse des Unternehmens-Webserver-Computers.

Beispiel:

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

3. Klicken Sie auf der Seite WCCallbackMain.htm auf die Schaltfläche **Web Callback versuchen**. Wenn eine Seite geöffnet wird, die Felder mit Kontaktinformationen eines Kunden anzeigt, haben Sie die Seite **WebCallback.htm** geladen und Web Callback in einer Standardkonfiguration auf dem Sun Java System Web Server erfolgreich konfiguriert.

HINWEIS: Wenn Sie an diesem Punkt auf **WebCallback.htm** auf die Schaltfläche **Abschicken** klicken, kann eine Fehlermeldung angezeigt werden. Sie können auf diese Schaltfläche klicken, nachdem die Webserver-Konfiguration abgeschlossen ist.

4. Konfigurieren Sie den Web Interaction-Server auf dem OpenScape Contact Center-Haupt-Server-Computer. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

4.3 Einrichten einer sicheren Verbindung für einen Web-Server

Das System kann so konfiguriert werden, dass es zum Sichern der Verbindung zwischen dem Web Interaction-Server und dem Unternehmens-Webserver die auf TLS-Zertifikaten basierende Authentifizierung verwendet.

Dieser Abschnitt beschreibt, wie Sie die TLS-Sicherheit auf dem Unternehmens-Webserver abhängig vom Typ des eingesetzten Unternehmens-Webserver aktivieren.

Zum Abschließen der TLS-Konfiguration müssen Sie außerdem folgende Schritte durchführen:

1. Installieren Sie ein TLS-Zertifikat auf dem Haupt-Server-Computer. Einzelheiten hierzu finden Sie im *Installationshandbuch*.
2. Wählen Sie in der Manager-Anwendung einen TLS-fähigen Port für die Webverbindung aus. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

HINWEIS: Es wird empfohlen, die TLS-Sicherheit auf dem Unternehmens-Webserver erst zu aktivieren, nachdem alle anderen Konfigurationen für den Web Interaction-Server abgeschlossen sind.

4.3.1 Aktivieren von TLS auf einem IIS-Server

Dieser Abschnitt beschreibt, wie Sie die TLS-Sicherheit auf einem IIS-Server aktivieren.

So aktivieren Sie TLS auf einem IIS-Server:

1. Öffnen Sie die Datei **HPWC.ini** in einem Texteditor.
2. Stellen Sie unter **[HPPCSETTINGS]** sicher, dass **Address** auf den Hostnamen des OpenScape Contact Center Haupt-Server-Computers gesetzt ist, der dem allgemeinen Namen des TLS-Zertifikats entspricht.
3. Setzen Sie die Einstellung **TLSPort** auf die Portnummer, die von den sicheren Webfeatures verwendet wird, zum Beispiel:

SSLPort=443

HINWEIS: Stellen Sie sicher, dass die hier konfigurierte Portnummer mit der in der Manager-Anwendung konfigurierten TLS-Portnummer übereinstimmt. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

Konfigurieren des Unternehmens-Webservers

Einrichten einer sicheren Verbindung für einen Web-Server

4. Setzen Sie das Callback-Flag auf den Wert true (wahr):

```
CallbackUsesSSL=true
```

HINWEIS: Ist das TLS-Flag auf Wahr gesetzt, ist das Leistungsmerkmal nur über TLS an dem Port verfügbar, der durch die Einstellung TLSPort angegeben ist.

5. Klicken Sie im Menü **Datei** auf **Speichern** und klicken Sie anschließend auf **Beenden**.

4.3.2 Aktivieren von TLS auf einem Tomcat- bzw. Sun Java-Server

Dieser Abschnitt beschreibt, wie Sie TLS-Sicherheit auf einem Tomcat Web-Server oder einem Sun Java System Web Server aktivieren.

Falls erforderlich, laden Sie zunächst JSSE (Java Secure Socket Extension) herunter. Eine detaillierte Anleitung finden Sie in der Dokumentation des Herstellers.

So aktivieren Sie TLS auf einem Tomcat- bzw. Sun Java-Server:

1. Installieren Sie "keystore" gemäß der Anleitung des Herstellers.
2. Öffnen Sie die Datei **config.properties** in einem Texteditor.
3. Setzen Sie die Einstellung **socket.server.name** auf den Hostnamen des OpenScape Contact Center Haupt-Server-Computers, der dem allgemeinen Namen des TLS-Zertifikats entspricht.
4. Setzen Sie die Einstellung **socket.server.port.ssl** auf die Portnummer, die von den sicheren Webfeatures verwendet wird, zum Beispiel:

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

HINWEIS: Stellen Sie sicher, dass die hier konfigurierte Portnummer mit der in der Manager-Anwendung konfigurierten TLS-Portnummer übereinstimmt. Ausführliche Informationen finden Sie in der *Manager-Hilfe*.

5. Setzen Sie das Callback-Flag auf den Wert true (wahr):

```
socket.webcallback.ssl=true
```

HINWEIS: Ist das TLS-Flag auf Wahr gesetzt, ist das Leistungsmerkmal nur über SSL an dem Port verfügbar, der durch die Einstellung **socket.server.port.ssl** angegeben ist.

6. Klicken Sie im Menü **Datei** auf **Speichern** und klicken Sie anschließend auf **Beenden**.

4.4 Web Callback-Fehlercodes

In der folgenden Tabelle sind die Fehlercodes aufgelistet, die beim Verwenden des Leistungsmerkmals Web Callback auftreten können. Wenn das System einen der in der Tabelle aufgelisteten Fehlercodes zurückgibt, wird der Callback nicht eingerichtet.

Neben den in der Tabelle aufgelisteten Fehlercodes können auch verschiedene Callback-Serverfehler auftreten, die in der System Monitor-Anwendung beschrieben sind.

Fehlercode	Beschreibung
1000	Ein allgemeiner Fehler ist aufgetreten.
1002	Es konnte keine Verbindung zum IVR-Server hergestellt werden.
1003	Die Verbindung zum Web Interaction-Server ist fehlgeschlagen.
1006	Auf die Webseite kann nicht zugegriffen werden.
1007	Es wurde eine ungültige Sitzungs-ID erkannt.
1008	JavaScript ist nicht aktiviert.
1010	Ein Pflichtparameter ist falsch.
1011	Ein Parameter ist falsch.
1012	Beim Web Interaction-Server ist ein interner Fehler aufgetreten.
1013	Zuordnungsfehler.
17006	In der Datenbank wurde ein doppelter Callback gefunden.
17021	Der Callback-Server kann eine Anforderung aufgrund eines internen Fehlers nicht bearbeiten.
17025	Ein allgemeiner Fehler ist aufgetreten.
17027	Die Callback-Warteschlange existiert nicht.
17028	Ein Callback-Plan ist ungültig.
17029	Ein Callback-Plan liegt außerhalb des für das Contact Center konfigurierten Callback-Routingplans.
17030	Der Name des Kunden ist zu lang, um gespeichert zu werden. Es sind maximal 75 Zeichen zulässig.

Tabelle 1 Web Callback-Fehlercodes

Konfigurieren des Unternehmens-Webservers

Web Callback-Fehlercodes

Fehlercode	Beschreibung
17031	Eine Telefonnummer ist eine der als ausgeschlossen definierten Nummern.
17032	Die Callback-Beschreibung ist zu lang. Es sind maximal 100 Zeichen zulässig.
17033	Die Kontaktdaten sind zu lang. Es sind maximal 1000 Zeichen zulässig.
17035	Die Priorität ist ungültig. Die Priorität muss zwischen 1 und 100 liegen.
17040	Ein Callback-Plan ist abgelaufen.
17047	Ein Start- oder Endedatum eines Callback-Plans ist ungültig. Ein Callback kann nicht weiter als 180 Tage in die Zukunft geplant werden.

Tabelle 1

Web Callback-Fehlercodes

5 Konfigurieren der Anwesenheitsintegration

Dieses Kapitel beschreibt die Elemente, die für die Unterstützung des Leistungsmerkmals Anwesenheitsintegration konfiguriert werden müssen. Das Leistungsmerkmal Anwesenheitsintegration ermöglicht Client Desktop-Benutzern, die Anwesenheit verschiedener Benutzer über das Leistungsmerkmal Verzeichnis anzuzeigen.

Wenn das Leistungsmerkmal Anwesenheitsintegration in der Manager-Anwendung aktiviert ist und der Client Desktop-Benutzer eine Verzeichnissuche durchführt, versucht das System, die Anwesenheit jedes Eintrags in den Suchergebnissen wie folgt abzurufen:

- Das System versucht zunächst, den Anwesenheitsstatus des Benutzers und den Anwesenheitsstatus des Sprachmediums von OpenScape UC Application abzurufen (nur wenn das Leistungsmerkmal OpenScape UC-Anwendungsintegration aktiviert und konfiguriert ist).
- Wenn der Benutzer kein OpenScape UC Application-Benutzer ist oder das Leistungsmerkmal OpenScape UC-Anwendungsintegration nicht aktiviert oder nicht verfügbar ist, versucht das System den Anwesenheitsstatus des Benutzers vom OpenScape Contact Center-System abzurufen.

5.1 Konfigurieren eines OpenScape UC Application-Benutzerkontos

Um dem System die Integration mit der OpenScape UC Application zu ermöglichen, müssen Sie ein Benutzerkonto in der OpenScape UC Application konfigurieren, mit dem das OpenScape Contact Center-System auf die OpenScape UC Application zugreifen und die Verbindung mit dieser aufrechterhalten kann. Dieses Benutzerkonto wird angegeben, wenn Sie die Optionen für die Anwesenheitsintegration in der Manager-Anwendung konfigurieren. Einzelheiten zum Konfigurieren eines neuen Benutzerkontos finden Sie in der Dokumentation zu OpenScape UC Application.

5.2 Konfigurieren des externen LDAP-Verzeichnisses

Damit Client Desktop-Benutzer die Anwesenheit anderer Benutzer anzeigen können, müssen Sie das externe LDAP-Verzeichnis darauf konfigurieren, die Anzeige von Anwesenheitsinformationen zu unterstützen.

Insbesondere müssen Sie eines oder mehrere der folgenden Felder in dem Verzeichnis konfigurieren:

- **Anwesenheits-ID** (die OpenScape UC Application-Benutzer-ID)
- **Benutzername** (der OpenScape Contact Center-Benutzername)

Einzelheiten zum Konfigurieren der Felder finden Sie in der Dokumentation zu dem LDAP-Verzeichnis.

6 Verwalten des Systems

Dieses Kapitel beschreibt, wie Sie die regelmäßige Wartung des OpenScape Contact Center-Systems durchführen, einschließlich Herunterfahren des Haupt-Server-Computers, Ändern der Passwörter und Sichern der Datenbank.

Für den Remote-Servicezugriff auf einen Haupt-Server-Computer wird das Service-Plug-In Smart Services Delivery Platform (SSDP) verwendet. Die Software für das SSDP Service-Plug-In wird als Teil des Installationsvorgangs automatisch auf dem Server-Computer installiert. Um das SSDP Service-Plug-In zu konfigurieren, gehen Sie nach der Anleitung in der Dokumentation für das SSDP Service-Plug-In vor, die sich auf der OpenScape Contact Center-DVD im Ordner Utilities\OpenScape Service Plug-in befindet.

HINWEIS: Wenn Sie allgemeine Systemwartungsprozeduren ausführen, zum Beispiel Aktualisierungen des Netzwerks, wird empfohlen, den OpenScape Contact Center Haupt-Server-Computer herunterzufahren, bevor Sie fortfahren. Spezielle Anweisungen hierzu finden Sie unter Abschnitt 6.1, "Herunterfahren eines Server-Computers für die Systemwartung".

6.1 Herunterfahren eines Server-Computers für die Systemwartung

Wenn Sie einen OpenScape Contact Center-Server-Computer, der Informix ausführt, zu Wartungszwecken herunterfahren oder neu starten müssen, hat Informix manchmal nicht genügend Zeit, um den Dienst Informix IDS zu beenden, bevor das Windows-Betriebssystem heruntergefahren ist. Wenn dies geschieht, kann die Datenbank beschädigt werden. Um dieses Problem zu verhindern, sollte der Dienst Informix IDS immer beendet werden, bevor der Server-Computer heruntergefahren oder neu gestartet wird.

HINWEIS: Um sicherzustellen, dass die Datenbank nicht beschädigt wird, beenden Sie immer erst den Dienst Informix IDS, bevor Sie einen Server-Computer herunterfahren oder neu starten.

6.2 Ändern des OpenScape Contact Center- oder Informix-Kennworts

Wenn Sie aus irgendeinem Grund die Kennwörter für OpenScape Contact Center oder Informix ändern müssen, muss die Kennwortänderung an den folgenden drei Stellen vorgenommen werden:

- Fenster Dienste
- Fenster Computerverwaltung
- OpenScape Contact Center-Fenster Startkonfiguration (oder System Monitor-Anwendung)

WICHTIG: Die Kennwörter für OpenScape Contact Center und Informix sollten nur unter Anleitung Ihres Servicevertreters geändert werden.

Das Informix-Kennwort kann maximal 16 Zeichen lang sein und darf keine Leerzeichen enthalten.

So ändern Sie das Kennwort für OpenScape Contact Center und Informix:

1. Öffnen Sie das Fenster **Dienste**.
2. Gehen Sie folgendermaßen vor, um das OpenScape Contact Center-Kennwort zu ändern:
 - a) Stoppen Sie die Dienste **OpenScape Contact Center** und **OpenScape Contact Center AutoPA**.
 - b) Öffnen Sie jeden einzelnen Dienst und geben Sie das neue Kennwort auf der Registerkarte **Anmelden** ein.
3. Gehen Sie folgendermaßen vor, um das Informix-Kennwort zu ändern:
 - a) Beenden Sie die folgenden Dienste: **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_Servername** (wobei *Servername* der Name des OpenScape Contact Center-Server-Computers ist) und **Informix Server Discovery Process for SNMP**.
 - b) Öffnen Sie den Dienst **Informix IDS - ol_Servername** und geben Sie das neue Kennwort auf der Registerkarte **Anmelden** ein.
 - c) Öffnen Sie den Dienst **Informix Server Discovery Process** für SNMP und geben Sie das neue Kennwort auf der Registerkarte **Anmelden** ein.
4. Schließen Sie das Fenster **Dienste**.
5. Öffnen Sie das Fenster **Computerverwaltung**.
6. Erweitern Sie unter **Systemprogramme Lokale Benutzer und Gruppen** und klicken Sie anschließend auf **Benutzer**.

7. Um das OpenScape Contact Center-Kennwort zu ändern, klicken Sie mit der rechten Maustaste auf **hppc**, klicken Sie auf **Kennwort festlegen** und geben Sie das neue Kennwort ein.
8. Um das Informix-Kennwort zu ändern, klicken Sie mit der rechten Maustaste auf **informix**, klicken Sie auf **Kennwort festlegen** und geben Sie das neue Kennwort ein.
9. Schließen Sie das Fenster **Computerverwaltung**.
10. Öffnen Sie ein Fenster mit der Eingabeaufforderung.
11. Geben Sie in der Befehlszeile `tcfmain` ein und drücken Sie anschließend die **Eingabetaste**. Das Fenster **OpenScape Contact Center Startkonfiguration** wird angezeigt.
12. Um das Informix-Kennwort zu ändern, klicken Sie auf die Registerkarte **Administrationsserver** und geben Sie das neue Kennwort in das Feld **Kennwort für Datenbankserver** ein.

HINWEIS: Wenn das System in Betrieb ist, können Sie das Informix-Kennwort auch ändern, indem Sie die Startdaten für den Administrationsserver mithilfe der System Monitor-Anwendung konfigurieren. Ausführliche Informationen finden Sie in der *System Monitor-Hilfe*.

13. Schließen Sie das Fenster **OpenScape Contact Center Startkonfiguration**.
14. Starten Sie die folgenden Dienste: **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_Servername** (wobei *Servername* der Name des OpenScape Contact Center-Server-Computers ist) und **Informix Server Discovery Process for SNMP**.
15. Starten Sie die Dienste **OpenScape Contact Center** und **OpenScape Contact Center AutoPA**.

6.3 Sichern der Datenbank

Sie sollten die OpenScape Contact Center-Datenbank in regelmäßigen Abständen und bei jeder Änderung der Systemkonfiguration sichern, um sicherzustellen, dass die Daten vor Ausfall und Beschädigung geschützt sind. Da die Datenbank recht groß sein kann, sollte eine Sicherung nur während Perioden mit sehr niedrigem Kontaktvolumen durchgeführt werden.

HINWEIS: Neben der OpenScape Contact Center-Datenbank sollten Sie auch alle Daten auf dem Server-Computer mithilfe eines Sicherungsprogramms sichern. Stellen Sie sicher, dass die Sicherung die Systemstatus-Daten des Server-Computers enthält; hierzu gehören zum Beispiel die Registrierung und die Startdateien.

Es können zwei Arten der Sicherung durchgeführt werden:

- **Vollständige Sicherung** – Um den potentiellen Datenverlust auf höchstens einen Tag zu beschränken, wird dringend empfohlen, täglich eine vollständige Sicherung durchzuführen. Zumindest sollte die Datenbank einmal wöchentlich gesichert werden.
- **Inkrementelle Sicherung** – Um den potentiellen Datenverlust zwischen vollständigen Datenbanksicherungen zu minimieren, können Sie eine inkrementelle Sicherung durchführen. Wenn Sie zum Beispiel nachts eine vollständige Sicherung vornehmen, können Sie während des Tages eine inkrementelle Sicherung durchführen. Die inkrementelle Sicherung benötigt weniger Zeit, da nur die Änderungen seit Beginn der letzten vollständigen Sicherung gesichert werden.

HINWEIS: Einige der Prozeduren in diesem Abschnitt setzen voraus, dass Sie mit der Verwendung von Informix vertraut sind. Eine detaillierte Anleitung finden Sie in der Informix-Dokumentation auf der folgenden Website:
<http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

6.3.1 Planen einer Datenbanksicherung

Sie können den Taskplaner in Windows Server 2012/2012 R2, 2008 R2 verwenden, um eine Task zur Sicherung der OpenScape Contact Center-Datenbank zu planen. Dieser Abschnitt enthält Richtlinien zum Planen einer Task. Eine detaillierte Anleitung finden Sie in der Microsoft-Dokumentation.

WICHTIG: Bei geplanten Sicherungen werden die Batchdateien FULLBACKUP.BAT und INCREMENTALBACKUP.BAT verwendet, um mithilfe des Dienstprogramms Informix ontape die Sicherung durchzuführen. Daher müssen Sie, bevor die erste geplante Sicherung ausgeführt wird, die ontape-Parameter wie in Schritt 2 auf Seite 41 beschrieben bearbeiten.

So planen Sie eine Datenbanksicherung:

1. Mit dem Taskplaner in Windows Server 2012/2012 R2, 2008 R2 können Sie gemäß den folgenden Richtlinien eine Task planen:
 - Wählen Sie die Aktion **Programm starten** und wählen Sie anschließend eine der folgenden Batchdateien aus, die sich im Installationsordner der OpenScape Contact Center-Software befinden:
 - Zum Planen einer vollständigen Sicherung wählen Sie **FULLBACKUP.BAT**.
 - Zum Planen einer inkrementellen Sicherung wählen Sie **INCREMENTALBACKUP.BAT**.
 - Geben Sie je nach dem verwendeten Betriebssystem das Benutzerkonto und das Kennwort an, unter dem die Task ausgeführt werden soll:
 - Geben Sie bei Windows 2012/2012 R2, 2008 R2 ein lokales Administratorkonto an.
 - Um die Ergebnisse der Sicherung in eine Textdatei zu schreiben, fügen Sie in den Eigenschaften der Task das Argument **<return.txt>results.txt** hinzu. Stellen Sie sicher, dass auf den Ordner, in den die Datei "results.txt" geschrieben wird (normalerweise der Installationsordner der OpenScape Contact Center-Software) alle Benutzer ("Jeder") Lesezugriff haben. Bei Windows Server 2012/ 2008 oder Windows Server 2012 R2/ 2008 R2 müssen Sie beim Hinzufügen des Arguments auch den Startpfad angeben. Achten Sie darauf, bei der Angabe des Pfades keine Anführungszeichen zu verwenden.

6.3.2 Sichern der Datenbank mit dem ontape-Dienstprogramm

Sie können die OpenScape Contact Center Datenbank mit dem Dienstprogramm Informix ontape auf ein lokales Bandlaufwerk oder ein lokales Laufwerk oder Netzlaufwerk sichern.

6.3.2.1 Sichern der Datenbank auf einem lokalen Laufwerk

Dieser Abschnitt beschreibt, wie Sie die OpenScape Contact Center Datenbank mit dem Dienstprogramm Informix ontape auf ein lokales Bandlaufwerk sichern.

So sichern Sie die Datenbank auf ein lokales Bandlaufwerk:

1. Melden Sie sich wie folgt bei dem Server-Computer an, auf dem Informix installiert ist:
 - Melden Sie sich bei Windows Server 2008 R2 als Administrator an.
2. Legen Sie ein leeres Band in das Bandlaufwerk des Server-Computers ein.
3. Öffnen Sie über die Verknüpfung **ol_Servername** ein Informix-Eingabeaufforderungsfenster, wobei *Servername* der Name des OpenScape Contact Center Server-Computers ist.
4. Wählen Sie eine der folgenden Vorgehensweisen, um die Sicherung zu starten:
 - Für eine vollständige Sicherung der gesamten Informix-Datenbank geben Sie am Befehlsprompt `ontape -s -L 0` ein, und drücken Sie die **Eingabetaste**.
 - Für eine inkrementelle Sicherung der gesamten Informix-Datenbank geben Sie am Befehlsprompt `ontape -s -L 1` ein, und drücken Sie die **Eingabetaste**.

HINWEIS: Der Parameter `-s` weist das ontape-Dienstprogramm an, eine Sicherung zu erstellen, und der Parameter `-L` gibt den Level des Archivs an, entweder 0 für vollständige oder 1 für inkrementelle Sicherung.

5. Wenn auf diesem Band nicht genügend Platz ist, fordert das System Sie auf, ein weiteres Band einzulegen. Wenn Sie dazu aufgefordert werden, entnehmen Sie das Band aus dem Laufwerk und beschriften Sie es mit Datum, Uhrzeit, Level und laufender Nummer des Bandes. Legen Sie ein neues Band ein und drücken Sie die **Eingabetaste**. Wiederholen Sie diesen Vorgang gegebenenfalls mit weiteren Bändern.

6.3.2.2 Sichern der Datenbank auf einem lokalen Laufwerk

Dieser Abschnitt beschreibt, wie Sie die OpenScape Contact Center Datenbank mit dem Dienstprogramm Informix ontape auf ein lokales Laufwerk oder Netzlaufwerk sichern.

So sichern Sie die Datenbank auf ein lokales Laufwerk oder Netzlaufwerk:

1. Melden Sie sich wie folgt bei dem Server-Computer an, auf dem Informix installiert ist:
 - Melden Sie sich bei Windows Server 2008 R2 als Administrator an.
2. Bearbeiten Sie die ontape-Parameter wie folgt:
 - Öffnen Sie die Datei **ONCONFIG.ol_Servername** in einem Texteditor, z. B. in Notepad; dabei steht *Servername* für den Namen des OpenScape Contact Center-Server-Computers, auf dem Informix installiert ist. Diese Protokolldatei finden Sie normalerweise im Ordner \Programme\Informix\etc.
 - Geben Sie im Parameter TAPEDEV den Pfad und den Dateinamen der Sicherungsdatei auf dem lokalen Laufwerk oder Netzlaufwerk im 8.3-Format (Kurzform) an, zum Beispiel C:\Backups\Backup.001. Sie müssen sicherstellen, dass die Sicherungsdatei in dem angegebenen Verzeichnis vorhanden ist, bevor Sie die Sicherung starten, und dass der angemeldete Benutzer mindestens über die Berechtigung "Ändern" für die Sicherungsdatei verfügt. Wenn die Sicherungsdatei nicht vorhanden ist, können Sie mit einem Texteditor, wie zum Beispiel Notepad (Editor), eine leere Datei erstellen.
 - Geben Sie im Parameter TAPESIZE den Wert 0 an, um festzulegen, dass die Sicherungsdatei keine maximale Größe hat.
3. Öffnen Sie über die Verknüpfung **ol_Servername** ein Informix-Eingabeaufforderungsfenster, wobei *Servername* der Name des OpenScape Contact Center Server-Computers ist.

4. Wählen Sie eine der folgenden Vorgehensweisen, um die Sicherung zu starten:
 - Für eine vollständige Sicherung der gesamten Informix-Datenbank geben Sie am Befehlsprompt `ontape -s -L 0` ein, und drücken Sie die **Eingabetaste**.
 - Für eine inkrementelle Sicherung der gesamten Informix-Datenbank geben Sie am Befehlsprompt `ontape -s -L 1` ein, und drücken Sie die **Eingabetaste**.

HINWEIS: Der Parameter `-s` weist das `ontape`-Dienstprogramm an, eine Sicherung zu erstellen, und der Parameter `-L` gibt den Level des Archivs an, entweder `0` für vollständige oder `1` für inkrementelle Sicherung.

6.3.3 Wiederherstellen der Datenbank mit dem `ontape`-Dienstprogramm

Dieser Abschnitt beschreibt, wie Sie zuvor gesicherte OpenScape Contact Center Daten mit dem Dienstprogramm Informix `ontape` wiederherstellen.

HINWEIS: Wenn Sie eine inkrementelle Sicherung durchgeführt haben, benötigen Sie sowohl die jüngste vollständige Sicherung als auch die inkrementelle Sicherung.

HINWEIS: Wenn Sie das Backup L0 mit einer sauberen Installation von OSCC wiederherstellen möchten, vergewissern Sie sich, dass alle vom Bandhilfsprogramm aufgeführten Blockdateien im Ordner „Contact Center Data“ vorhanden sind. Wenn das nicht der Fall ist, erstellen Sie diese Datei ohne Erweiterung durch einen Rechtsklick, navigieren Sie zu **Neu -> Textdokument**, benennen Sie sie um und löschen Sie die Erweiterung. Der Import funktioniert nicht richtig, wenn diese Dateien nicht vorhanden sind.

So stellen Sie die Datenbank mit dem `ontape`-Dienstprogramm wieder her:

1. Melden Sie sich wie folgt bei dem Server-Computer an, auf dem Informix installiert ist:
 - Melden Sie sich bei Windows Server 2008 R2 als Administrator an.
2. Beenden Sie folgende Dienste:

- **OpenScape Contact Center**
 - **Informix IDS - ol_Servername**, wobei *Servername* der Name des OpenScape Contact Center Server-Computers ist
3. Wählen Sie eine der folgenden Vorgehensweisen:
 - Wenn Sie die Daten von einem Band wiederherstellen, legen Sie das erste Band des vollständigen Archivs, das Sie wiederherstellen möchten, in das Bandlaufwerk des Server-Computers ein.
 - Wenn Sie die Daten von einer Sicherungsdatei auf einem lokalen Laufwerk oder Netzlaufwerk wiederherstellen, stellen Sie sicher, dass der Pfad und der Dateiname der Sicherungsdatei in der Datei `ONCONFIG.ol_Servername` korrekt konfiguriert ist.
 4. Öffnen Sie über die Verknüpfung **ol_Servername** ein Informix-Eingabeaufforderungsfenster, wobei *Servername* der Name des OpenScape Contact Center Server-Computers ist.
 5. Geben Sie an der Eingabeaufforderung `ontape -r` ein, und drücken Sie die **Eingabetaste**.
 6. Wenn Sie dazu aufgefordert werden, ein Band einzulegen, drücken Sie die **Eingabetaste**.
 7. Wenn die Frage **Continue restore (Y/N)?** erscheint, drücken Sie **Y**.
 8. Wenn Sie gefragt werden, ob die Protokolle gesichert werden sollen, drücken Sie **N**.
 9. Wenn Sie ein inkrementelles Archiv erstellt haben und die Meldung **Restore a level 1 archive** angezeigt wird, drücken Sie **Y**. Wenn Sie kein inkrementelles Archiv erstellt haben, drücken Sie **N**.
 10. Wenn Sie gefragt werden, ob Protokollbänder wiederhergestellt werden sollen, drücken Sie **N**.
 11. Wenn der Wiederherstellungsprozess abgeschlossen ist und Sie die Daten von einem Bandlaufwerk wiederhergestellt haben, entnehmen Sie das letzte Band aus dem Bandlaufwerk.
 12. Geben Sie in der Befehlszeile `onmode -m` ein, und drücken Sie die **Eingabetaste**. Durch diesen Befehl wird Informix in den normalen Modus zurückgesetzt. Dieser Vorgang kann einige Minuten dauern.
 13. Geben Sie in der Befehlszeile `onstat -r` ein und drücken Sie anschließend die **Eingabetaste**. Es werden Informationen zur Informix-Server-Umgebung angezeigt. Die erste Zeile gibt den Informix-Anwendungsmodus an und sollte **On-Line** lauten. Um den `onstat`-Prozess anzuhalten, drücken Sie **Strg+C**.
 14. Um das Eingabeaufforderungsfenster zu schließen, geben Sie `exit` ein, und drücken Sie die **Eingabetaste**.

15. Schließen Sie alle sonstigen offenen Fenster und Anwendungen.
16. Starten Sie den Dienst **OpenScape Contact Center** neu.

6.3.4 Wiederherstellen einer mit dem ontape-Dienstprogramm erstellten Level-0-Sicherung

Dieser Abschnitt beschreibt, wie Sie zuvor mit Level 0 gesicherte OpenScape Contact Center-Daten automatisch wiederherstellen.

1. Um das Level-0-Wiederherstellungsskript zu verwenden, kopieren Sie die Dateien FullRestore.bat, fullrestore.in und replace.vbs auf den Server-Computer. Sie finden die Dateien auf der DVD.
2. Öffnen Sie als Informix-Benutzer ein Eingabeaufforderungsfenster
3. Führen Sie die Datei FullRestore.bat unter Angabe der Argumente /tapedev <Pfad> /tapesize <Größe> aus (wobei <Pfad> der Pfad mit der Informix-Level-0-Sicherung ist) und geben Sie unter <Größe> den Wert 0 ein, sofern Sie kein externes Bandgerät verwenden.

6.3.5 Sichern der Datenbank mit dem onbar-Dienstprogramm

Dieser Abschnitt beschreibt, wie Sie die OpenScape Contact Center Datenbank mit dem Dienstprogramm Informix onbar auf ein lokales Laufwerk sichern. Das Dienstprogramm Informix onbar hat eine direkte Schnittstelle zum Informix Storage Manager (ISM) oder einer anderen Drittanbieter-Speicherverwaltung (zum Beispiel Veritas), um eine flexible Sicherungslösung bereitzustellen.

HINWEIS: Sie müssen die Speicherverwaltungs-Anwendung konfigurieren, bevor Sie das onbar-Dienstprogramm ausführen. Eine ausführliche Anleitung finden Sie im *IBM Informix Storage Manager Administratorhandbuch* oder in der Dokumentation der Drittanbieter-Speicherverwaltung. Die Informix-Dokumentation finden Sie auf der folgenden Website:
<http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

So sichern Sie die Datenbank auf ein lokales Laufwerk:

1. Melden Sie sich wie folgt bei dem Server-Computer an, auf dem Informix installiert ist:
 - Melden Sie sich bei Windows Server 2008 R2 als Administrator an.

2. Öffnen Sie über die Verknüpfung **ol_Servername** ein Informix-Eingabeaufforderungsfenster, wobei *Servername* der Name des OpenScape Contact Center Server-Computers ist.
3. Wählen Sie eine der folgenden Vorgehensweisen, um die Sicherung zu starten:
 - Für eine vollständige Sicherung der gesamten Informix-Datenbank geben Sie am Befehlsprompt `onbar -b -L 0` ein, und drücken Sie die **Eingabetaste**.
 - Für eine inkrementelle Sicherung der gesamten Informix-Datenbank geben Sie am Befehlsprompt `onbar -b -L 1` ein, und drücken Sie die **Eingabetaste**.

HINWEIS: Der Parameter `-b` weist das onbar-Dienstprogramm an, eine Sicherung zu erstellen, und der Parameter `-L` gibt den Level des Archivs an, entweder 0 für vollständige oder 1 für inkrementelle Sicherung.

6.3.6 Wiederherstellen der Datenbank mit dem onbar-Dienstprogramm

Dieser Abschnitt beschreibt, wie Sie zuvor gesicherte OpenScape Contact Center Daten mit dem Dienstprogramm Informix onbar wiederherstellen.

HINWEIS: Wenn Sie eine inkrementelle Sicherung durchgeführt haben, benötigen Sie sowohl die jüngste vollständige Sicherung als auch die inkrementelle Sicherung.

So stellen Sie die Datenbank mit dem onbar-Dienstprogramm wieder her:

1. Melden Sie sich wie folgt bei dem Server-Computer an, auf dem Informix installiert ist:
 - Melden Sie sich bei Windows Server 2008 R2 als Administrator an.
2. Öffnen Sie über die Verknüpfung **ol_Servername** ein Informix-Eingabeaufforderungsfenster, wobei *Servername* der Name des OpenScape Contact Center Server-Computers ist.
3. Geben Sie in der Befehlszeile `onbar -r` ein und drücken Sie anschließend die **Eingabetaste**.

6.4 SNMP-Unterstützung

Das System unterstützt zwei Methoden der Generierung von Informationen, die durch ein SNMP-Verwaltungssystem angezeigt werden können:

- **OpenScape Contact Center SNMP Extension Agent** – Zeigt OpenScape Contact Center-spezifische Informationen an, die sich auf den Status von durch OpenScape Contact Center verwaltete Objekte beziehen.
- **OpenScape CAP Fault Management-Software** – Agiert als SNMP Extension Agent, um SNMP-Trap-Nachrichten für die OpenScape Contact Center-Software über Windows-Ereignisprotokolle zu generieren.

Zur Unterstützung dieser Methoden muss der Windows-Dienst SNMP auf dem Haupt-Server-Computer installiert und aktiv sein.

HINWEIS: Sie müssen den Windows-Dienst SNMP so konfigurieren, dass die Liste der Community-Namen weder "public" noch "private" enthält und die Liste der Hosts nur die Hosts enthält, die für den Zugriff auf die Informationen erforderlich sind.

6.4.1 OpenScape Contact Center SNMP Extension Agent

Der OpenScape Contact Center SNMP Extension Agent (osccsnmp.dll) unterstützt Standard-SNMP-Anfragen nach Objekt-IDs (OIDs). Der SNMP Extension Agent zeigt OpenScape Contact Center-spezifische Informationen an, die sich auf den Status von durch OpenScape Contact Center verwaltete Objekte beziehen. Die Informationen können dann von jedem SNMP-Verwaltungssystem angefordert werden.

HINWEIS: Der Benutzer des SNMP-Verwaltungssystems muss sicherstellen, dass Informationen aus dem OpenScape Contact Center SNMP Extension Agent angefordert und abgerufen werden können.

Die OpenScape Contact Center-spezifischen Informationen, die durch den OpenScape Contact Center SNMP Extension Agent angezeigt werden, sind in der Datei "sen-oscc-mib.mib" definiert, die die verwalteten Objekte ihren jeweiligen OIDs zuordnet. In den angezeigten Informationen sind die Nutzung von Call Director-Nebenstellen, die Anzahl der angemeldeten Benutzer und die Anzahl der aktuellen und letzten Kontakte enthalten. Einzelheiten zu allen verfügbaren Informationen finden Sie in der Datei "sen-oscc-mib.mib", die mit einem Texteditor angezeigt werden kann.

Die OpenScape Contact Center-spezifischen Informationen können verwendet werden, um den Status des Systems zu überwachen. Beispielsweise kann ein Techniker im Netzwerkbetriebszentrum eine Ansicht erstellen, die einen Alarm generiert, wenn die Anzahl der betriebsbereiten Sprachprozessor-Nebenstellen unter einen konfigurierten Schwellwert-Prozentsatz der Gesamtzahl der konfigurierten Sprachprozessor-Nebenstellen fällt. Der Techniker kann dann den Kunden benachrichtigen, sodass dieser Zeit hat, das Problem zu beheben, bevor nicht mehr ausreichend Nebenstellen vorhanden sind.

Die Dateien "osccsnmp.dll" und "sen-oscc-mib.mib" befinden sich im Standard-Installationsordner auf dem Haupt-Server-Computer.

HINWEIS: Die Datei "osccsnmp.dll" wird während der Installation der OpenScape Contact Center-Server-Software automatisch auf dem Server-Computer registriert. Bei einer Deinstallation des Windows-Dienstes SNMP wird die Datei "osccsnmp.dll" deregistriert. Um die DLL-Datei erneut zu registrieren, verwenden Sie das Dienstprogramm "osccregistersnmpextension.exe", das sich im Standard-Installationsordner auf dem Haupt-Server-Computer befindet.

6.4.2 OpenScape CAP Fault Management-Software

Die OpenScape CAP Fault Management-Software ist eine optionale Komponente, mit der OpenScape Contact Center SNMP-Trap-Nachrichten generiert werden können. Die OpenScape CAP Fault Management-Software kann entweder automatisch während des OpenScape Contact Center-Installationsvorgangs oder manuell aus dem Ordner \OpenScape CAP\Fault Management auf der OpenScape Contact Center-DVD installiert werden.

HINWEIS: Einzelheiten zum Konfigurieren der OpenScape CAP Fault Management-Software finden Sie in der Dokumentation zum OpenScape CAP Fault Management.

Es gibt zwei Konfigurationsdateien für das OpenScape CAP Fault Management:

- **capfm_procenter.ini**: Dies ist die Standardkonfigurationsdatei, die bei der Installation der OpenScape Contact Center-Server-Software installiert wird. Sie löst die Generierung von SNMP-Trap-Nachrichten bei allen OpenScape Contact Center-Meldungen aus.
- **capfm_procenter_service.ini**: Dies ist die Dienstkonfigurationsdatei, die verwendet werden sollte, wenn nur für die Teilmenge der Meldungen, die für das Netzwerkbetriebszentrum bedeutsam sind, SNMP-Trap-Nachrichten generiert werden sollen.

Beide Konfigurationsdateien befinden sich im Ordner \Utilities\Install auf der OpenScape Contact Center-DVD.

Index

A

Anwesenheitsintegration, konfigurieren 33
 Apache Tomcat-Version 19
 Authentifizierung, E-Mail-Server 17

B

benutzerdefinierte E-Mail-Nachrichtenkopfzeilen
 einfügen 13
 Info über 10

C

config.properties
 auf einem Sun Java System Web Server
 konfigurieren 27
 auf einem Tomcat-Server konfigurieren 24

D

Datei HPWC.ini
 konfigurieren 22
 SSL aktivieren 29
 Datenbanksicherungen
 auf ein lokales Bandlaufwerk (ontape) 40
 auf ein lokales Laufwerk (onbar) 44
 auf ein lokales Laufwerk oder Netzlaufwerk
 (ontape) 41
 inkrementelle Sicherungen 38
 mit dem onbar-Dienstprogramm
 wiederherstellen 45
 mit dem ontape-Dienstprogramm
 wiederherstellen 42
 Planung 39
 vollständige Sicherungen 38
 Dienstprogramme
 osccmseheaders 13
 osccregistersnmpextension 47
 Dokumentation
 Feedback geben 6
 Formatierungskonventionen 5
 Zielgruppe 5

E

E-Mail-Nachrichtenkopfzeilen
 benutzerdefinierte einfügen 10, 13
 E-Mail-Server 9
 Authentifizierung verwenden 17
 sichere Verbindung einrichten 16

F

Fehlercodes, für Web Callback 31

G

geplante Sicherungen 39

I

IBM Lotus Domino-Installation 14
 IIS-Server
 Datei HPWC.ini konfigurieren 22
 Einrichten eines virtuellen Verzeichnisses 22
 sichere Verbindung einrichten 29
 Web Callback testen 23
 Webkomponenten konfigurieren 21
 IMAP4-Protokoll 9
 Informix
 Kennwort ändern 36
 onbar-Dienstprogramm verwenden 44
 ontape-Dienstprogramm verwenden 40
 ontape-Parameter konfigurieren 39, 41
 IP-Verbindungen, für Wandanzeigen konfigurieren 7
 ISAPI-Nebenstellen 22

K

Kennwörter, ändern 36

L

LDAP-Verzeichnis, für Anwesenheitsintegration
 konfigurieren 34
 Leistungsmerkmal Reporte per E-Mail versenden,
 Unterstützung 17
 Lotus Domino-Installation 14

M

Microsoft Exchange-Installation 11
 MIME-Funktionen 9

O

OpenScape Contact Center-Kennwort, ändern 36
 OpenScape UC Application-Benutzerkonto, für
 Anwesenheitsintegration konfigurieren 33

R

Remote-Servicezugriff 35

S

Server-Computer, für Wartung herunterfahren 35
 sichere Verbindung

- für Unternehmens-E-Mail-Server 16
 - für Unternehmens-Webserver 28
- Sicherungen, siehe Datenbanksicherungen
- SMTP-Protokoll 9
- SNMP-Unterstützung, Methoden 46
- SSDP Service-Plug-In 35
- SSL
 - auf einem IIS-Server aktivieren 29
 - auf einem Sun Java Server aktivieren 30
 - auf einem Tomcat-Server aktivieren 30
 - für Unternehmens-E-Mail-Server aktivieren 16
 - für Unternehmens-Webserver aktivieren 28
- Sun Java System Web Server
 - config.properties bearbeiten 27
 - sichere Verbindung einrichten 30
 - WAR-Datei konfigurieren und verwenden 26
 - Web Callback testen 28
 - Webkomponenten konfigurieren 26
- Sun Java System Web Server-Version 19

T

- Tomcat-Server
 - config.properties bearbeiten 24
 - sichere Verbindung einrichten 30
 - WAR-Datei konfigurieren und verwenden 24
 - Web Callback testen 25
 - Webkomponenten konfigurieren 23

U

- Unternehmens-E-Mail-Server
 - Anforderungen 9
 - Authentifizierung verwenden 17
 - konfigurieren 9
 - sichere Verbindung einrichten 16
- Unternehmens-Webserver
 - angepasste Dateien und Aktualisierung 19
 - Apache Tomcat-Version 19
 - konfigurieren 19, 20
 - sichere Verbindung einrichten 28
 - Sun Java System-Version 19
 - unterstützte Betriebssysteme 19
 - Voraussetzungen 19

V

- virtuelles Verzeichnis, IIS-Server 22

W

- Wandanzeigen, konfigurieren 7
- WAR-Datei
 - auf einem Tomcat-Server konfigurieren 24
 - auf einem Sun Java System Web Server konfigurieren 26
- Web Callback

- auf einem IIS-Server testen 23
 - auf einem Tomcat-Server testen 25
 - auf Sun Java-Server testen 28
 - Fehlercodes 31
- Webbrowser, Voraussetzungen 20
- Webkomponenten
 - auf einem IIS-Server konfigurieren 21
 - auf einem Tomcat-Server konfigurieren 23
 - auf Sun Java-Server konfigurieren 26
 - konfigurieren 20
 - sichere Verbindung einrichten 28
 - Systemvoraussetzungen 19
 - Voraussetzungen für Webbrowser 20
- Web-Server
 - angepasste Dateien und Aktualisierung 19
 - Apache Tomcat-Version 19
 - konfigurieren 19, 20
 - sichere Verbindung einrichten 28
 - Sun Java System-Version 19
 - unterstützte Betriebssysteme 19
 - Voraussetzungen 19

