



A MITEL
PRODUCT
GUIDE

Mitel OpenScape Contact Center Enterprise V12

Manuale di Gestione del Sistema

Manuale di Gestione del Sistema

Documentazione di servizio

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

Indice

1 Informazioni sul manuale	5
1.1 A chi è dedicato il manuale	5
1.2 Convenzioni di formattazione.	5
1.3 Commenti sulla documentazione.	6
2 Configurazione di una bacheca.	7
2.1 Prima di iniziare	7
2.2 Configurazione della connessione IP per una bacheca	7
3 Configurazione del server e-mail aziendale	9
3.1 Requisiti del server e-mail aziendale	9
3.2 Pianificazione della distribuzione di Microsoft Office 365	10
3.3 Pianificazione della distribuzione di Google GSuite.	10
3.4 Pianificazione della distribuzione di Microsoft Exchange.	11
3.4.1 Come specificare intestazioni personalizzate (solo Microsoft Exchange Server 2007, 2010 e 2013) .	12
3.5 Pianificazione della distribuzione di IBM Lotus Domino.	14
3.5.1 Compattazione del database	15
3.6 Impostazione di una connessione protetta per un server e-mail	15
3.7 Utilizzo di un'autenticazione su un server e-mail.	16
3.8 Supporto della funzione report e-mail	16
4 Configurazione di un server Web aziendale.	19
4.1 Requisiti di sistema per l'utilizzo di componenti Web	19
4.1.1 Requisiti del server Web aziendale	19
4.1.2 Requisiti browser Web	19
4.2 Configurazione di componenti Web.	20
4.2.1 Configurazione di un server IIS	20
4.2.2 Configurazione di un server	25
4.2.3 Configurazione di un Sun Java System Web Server	28
4.3 Impostazione di una connessione protetta per un server Web	32
4.3.1 Attivazione TLS su un server IIS	32
4.3.2 Attivazione TLS su un server Tomcat o Sun Java	33
4.4 Localizzazione e personalizzazione di componenti Web.	34
4.4.1 Localizzazione dei componenti Web	34
4.4.2 Personalizzazione dei componenti Web.	35
4.5 Risoluzione dei problemi di collaborazione Web	37
4.5.1 Problemi di configurazione del server Web	37
4.5.2 Problemi di connessione generali.	37
4.6 Codici errore richiamata Web	38
5 Configurazione dell'integrazione presenze	41
5.1 Configurazione di un account utente per l'Applicazione OpenScape UC	41
5.2 Configurazione dell'elenco LDAP esterno	42
6 Manutenzione del sistema	43
6.1 Arresto di un server per la manutenzione del sistema.	43
6.2 Modifica delle password di OpenScape Contact Center e Informix.	44
6.3 Backup del database	46
6.3.1 Pianificazione di un backup del database.	47
6.3.2 Backup del database tramite l'utilità ontape	48

Indice

6.3.3 Ripristino del database tramite l'utilità ontape	50
6.3.4 Ripristino di un backup di livello zero effettuato con l'utilità su nastro	51
6.3.5 Backup del database tramite l'utilità onbar	52
6.3.6 Ripristino del database tramite l'utilità onbar	52
6.4 Supporto SNMP	53
6.4.1 OpenScape Contact Center SNMP Extension Agent	54
6.4.2 Software OpenScape CAP Fault Management	55
7 Gestione di un ambiente report centralizzati	57
7.1 Gestione della replica per Report centralizzato	57
7.1.1 Il buffer di replica	57
7.1.2 Sospensione della replica per report centralizzato	58
7.1.3 Chiusura di tutte le repliche per report centralizzato	61
7.2 Sincronizzazione dei dati per report centralizzato	63
7.3 Risoluzione dei problemi della configurazione di replica per report centralizzato	65
7.4 Sostituzione di un server principale per i report centralizzati	68
7.4.1 Riconfigurazione delle impostazioni di replica	68
8 Gestione di un ambiente di alta disponibilità (warm standby)	71
8.1 Gestione della replica per l'alta disponibilità (warm standby)	71
8.1.1 Sospensione della replica per l'alta disponibilità (warm standby)	71
8.1.2 Sospensione della replica report centralizzato	73
8.1.3 Arresto della replica per l'alta disponibilità (warm standby)	74
8.1.4 Arresto della replica report centralizzato	77
8.1.5 Chiusura di tutte le repliche	81
8.2 Sincronizzazione dei dati fra il server principale e quello di backup	83
8.3 Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzato	85
8.4 Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato	86
8.5 Risoluzione dei problemi di configurazione della replica per l'alta disponibilità (warm standby)	88
8.6 Ripristino del database	89
8.6.1 Ripristino del database sul server in modalità standby	89
8.6.2 Ripristino del database sul server report centralizzato	90
8.6.3 Ripristino del database su più server	91
8.7 Forzatura di un singolo server nel servizio	92
8.8 Sostituzione di un server nel cluster	93
Indice alfabetico	95

1 Informazioni sul manuale

Questo manuale descrive come configurare l'hardware di terze parti, ad esempio bacheche, server e-mail aziendali e server Web aziendali, per l'integrazione con il sistema OpenScape Contact Center Enterprise V10. Descrive inoltre come eseguire la manutenzione continuativa del sistema, incluse le operazioni di backup e ripristino del database. OpenScape Contact Center Enterprise V10

1.1 A chi è dedicato il manuale

Questo manuale è concepito per gli utenti all'interno dell'organizzazione responsabili della gestione, del monitoraggio e del funzionamento ottimale del sistema OpenScape Contact Center Enterprise V10.

1.2 Convenzioni di formattazione

Nel presente manuale vengono utilizzate le seguenti convenzioni di formattazione:

Grassetto

Questo formato identifica i componenti, i titoli delle finestre e finestre di dialogo e i nomi degli elementi di OpenScape Contact Center Enterprise V10.

Corsivo

Questo formato identifica i riferimenti alla documentazione correlata.

Tipo di carattere a spaziatura fissa

Questo formato distingue il testo da digitare o che il computer visualizza in un messaggio.

NOTA: Le note evidenziano informazioni utili ma non essenziali, quali suggerimenti o metodi alternativi per eseguire un'operazione.

IMPORTANTE: Note importanti: le indicazioni di attenzione sottolineano le azioni che potrebbero influire negativamente sul funzionamento dell'applicazione o causare perdite di dati.

Informazioni sul manuale

Commenti sulla documentazione

1.3 Commenti sulla documentazione

Per notificare problemi in merito al presente documento, rivolgersi al Centro di assistenza clienti.

Al momento di effettuare la chiamata, assicurarsi di poter indicare le informazioni seguenti. Ciò consentirà di identificare il documento pertinente.

- **Titolo:** Manuale di Gestione del Sistema
- **Numero d'ordine:** A31003-S22A-S100-01-7220

2 Configurazione di una bacheca

Questo capitolo descrive come configurare una bacheca. In questo contesto una bacheca è un sistema elettronico che offre contemporaneamente a più utenti una visualizzazione a scorrimento di informazioni generali sul sistema e dati statistici in tempo reale relativi al centro contatti. Il sistema OpenScape Contact Center supporta bacheche IP Spectrum, versione 4200 R, nonché bacheche personalizzate conformi al protocollo EZ Key II.

IMPORTANTE: La configurazione di una bacheca deve essere riservata esclusivamente a personale qualificato a tale scopo. I tentativi di configurazione di una bacheca effettuati da personale non qualificato possono influire negativamente sul funzionamento del sistema OpenScape Contact Center.

2.1 Prima di iniziare

Prima di installare e configurare la bacheca, è necessario effettuare quanto segue:

- Se si utilizza una bacheca seriale Spectrum, è necessario un kit di conversione da seriale a IP (NIU in Nord America e UDS100 negli altri Paesi).
- Ottenere un indirizzo IP statico per la bacheca.
- Assicurarsi di disporre delle versioni del firmware supportate e conformi al sistema OpenScape Contact Center.

2.2 Configurazione della connessione IP per una bacheca

Questa procedura descrive come configurare la connessione IP per una bacheca. Si presuppone che sul server principale OpenScape Contact Center sia già installato il software di configurazione Lantronix Device Server Configuration Utility 2.0 per la bacheca.

IMPORTANTE: Sono riportati solo i passaggi della configurazione di base. Per istruzioni ed avvertenze dettagliate, consultare la documentazione del fornitore.

Per configurare la connessione IP per una bacheca:

1. Collegare la bacheca alla rete LAN (Local Area Network).
2. Avviare l'applicazione Lantronix Device Server Configuration Utility.

Configurazione di una bacheca

Configurazione della connessione IP per una bacheca

3. Nel menu **File**, fare clic su **Search Network**.
4. Per eseguire una ricerca di una bacheca esistente nella rete, procedere come segue:
 - a) Fare clic su **Start Search**.
 - b) Una volta individuate le bacheche nella rete, fare clic su **Save**.
 - c) Quando il sistema informa che i dispositivi sono stati salvati, fare clic su **OK**.
 - d) Fare clic su **Back**.
5. Selezionare l'indirizzo IP della bacheca da configurare.
6. Nel menu **Tools**, fare clic su **Device Manager**.
7. Fare clic su **Web Configuration**.
8. Fare clic su **OK**. Lantronix Web-Manager si avvia.
9. In **Dedicated Connection**, digitare il numero porta della bacheca nella casella **Local Port**, quindi fare clic su **Update Settings**.

NOTA: Per configurare una nuova bacheca, non ancora dotata di indirizzo IP, nel menu **Tools**, fare clic su **Assign IP Address**. Individuare l'indirizzo dell'hardware o Ethernet sul retro della bacheca, quindi digitarlo nel campo disponibile. Assegnare alla bacheca un indirizzo IP, quindi fare clic su **Set IP Address**.

3 Configurazione del server e-mail aziendale

Questo capitolo descrive come configurare il server e-mail aziendale per supportare la funzione e-mail di OpenScape Contact Center e l'invio di report tramite e-mail. I messaggi e-mail inviati dai clienti vengono instradati dal server e-mail aziendale al server e-mail OpenScape Contact Center. + Tutti i messaggi e-mail vengono memorizzati in una singola casella di posta sul server e-mail dell'azienda.

Il server e-mail OpenScape Contact Center e il server e-mail aziendale comunicano utilizzando il protocollo IMAP4. Le applicazioni client OpenScape Contact Center e il server e-mail dell'azienda utilizzano il protocollo IMAP4 anche per ripristinare ed elaborare i messaggi e-mail. Gli allegati dei messaggi vengono recuperati utilizzando funzioni IMAP4 e MIME separate. I messaggi e-mail di risposta vengono inviati ai clienti dal Server e-mail utilizzando un'interfaccia SMTP.

3.1 Requisiti del server e-mail aziendale

I seguenti server e-mail sono stati testati in combinazione con il sistema OpenScape Contact Center:

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

Per ulteriori informazioni su questi server, consultare la documentazione del produttore.

NOTA: Si consiglia di proteggere il contenuto del server e-mail aziendale per ridurre le probabilità di cancellare inavvertitamente i messaggi e-mail.

Assicurarsi che il server e-mail aziendale sia configurato come segue:

- **Licenze di accesso client** – Assicurarsi di disporre di un numero sufficiente di licenze di accesso client. Ogni utente in grado di accedere al server e-mail OpenScape Contact Center richiede una licenza di accesso client.
- **Intestazioni personalizzate** – Poiché la funzionalità e-mail di OpenScape Contact Center utilizza intestazioni personalizzate, è necessario che il server e-mail aziendale non filtri o rimuova le intestazioni personalizzate dai messaggi e-mail.

Configurazione del server e-mail aziendale

Pianificazione della distribuzione di Microsoft Office 365

- **Sessioni IMAP** – una sessione IMAP è necessaria per ciascun giorno con messaggi attivi. Ogni utente necessita di una sessione IMAP quando invia un messaggio e-mail o recupera i contenuti di un messaggio e-mail.
- **Connessioni simultanee** – Assicurarsi che l'account e-mail OpenScape Contact Center sia stato configurato con un numero di connessioni sufficiente per supportare gli utenti che avranno accesso all'account simultaneamente.
- **Filtro anti-spam e blocco indirizzi e-mail** – Impediscono ai messaggi e-mail indesiderati di venire instradati agli utenti.
- **Software antivirus** – È necessario sottoporre al controllo antivirus i messaggi e-mail e i relativi allegati ricevuti dal server e-mail aziendale.

3.2 Pianificazione della distribuzione di Microsoft Office 365

È necessario pianificare con cura la distribuzione di Microsoft Office 365. Quando si configura il periodo di conservazione dei messaggi nel server e-mail OpenScape Contact Center, assicurarsi di prendere in considerazione la disponibilità del database di Microsoft Office 365. Per ulteriori informazioni su questa ed altre attività descritte nella presente sezione, occorre valutare il contratto per Microsoft Office 365.

È necessario configurare quanto segue:

- **Account utente** – Creare un nuovo account utente da utilizzare nel server e-mail OpenScape Contact Center. È necessario specificare una password per il nuovo account utente.
- **Criterio throttling** – Microsoft Office 365 è dotato di un criterio di throttling che limita la velocità dei messaggi SMTP a un massimo di 30 messaggi/minuto. Per garantire la conformità a questa limitazione, il parametro Limite velocità messaggi di OSCC nelle Impostazioni e-mail deve essere impostato su 30 (o meno).
- **Sessioni IMAP** – Microsoft Office 365 limita il numero di sessioni IMAP attive a 20 per account. Per funzionare secondo questa limitazione, il parametro Sessioni IMAP max. di OSCC nelle Impostazioni e-mail deve essere impostato su 20.

3.3 Pianificazione della distribuzione di Google GSuite

È necessario pianificare con cura la distribuzione di Google GSuite. Quando si configura il periodo di conservazione dei messaggi nel server e-mail OpenScape Contact Center, assicurarsi di prendere in considerazione la disponibilità del database di Google GSuite. Per ulteriori informazioni su questa ed altre attività descritte nella presente sezione, occorre valutare il contratto per Google GSuite.

È necessario eseguire le configurazioni seguenti:

In Google GSuite:

- Creare un nuovo account utente GMail da utilizzare nel server e-mail OpenScape Contact Center.
- Nelle impostazioni di Gmail, nella scheda Inoltro e POP/IMAP, verificare che "Accesso IMAP" sia attivato.
- Nelle impostazioni di sicurezza dell'account Google:
 - creare una "password applicazione" e utilizzarla in OpenScape Contact Center.
 - attivare l'opzione "consenti applicazioni meno sicure"

In OpenScape Contact Center:

- **Sessioni IMAP** - Google GSuite limita il numero di sessioni IMAP attive a 15 per account. Per funzionare secondo questa limitazione, il parametro OSCC **Sessioni IMAP max. di OSCC nelle Impostazioni e-mail** deve essere impostato su 15, di cui 5 sessioni sono riservate per il server e-mail OSCC.

3.4 Pianificazione della distribuzione di Microsoft Exchange

È necessario pianificare con cura la distribuzione di Microsoft Exchange. Quando si configura il periodo di conservazione dei messaggi nel server e-mail OpenScape Contact Center, assicurarsi di prendere in considerazione le dimensioni del database di Microsoft Exchange. Per ulteriori informazioni su questa e altre attività descritte nella presente sezione, vedere la documentazione di Microsoft Exchange.

IMPORTANTE: La configurazione di Microsoft Exchange deve essere completata esclusivamente da un amministratore di Microsoft Exchange qualificato.

È necessario configurare quanto segue:

- **Account utente** – Creare un nuovo account utente da utilizzare nel server e-mail OpenScape Contact Center. È necessario specificare una password per il nuovo account utente.
- **Alias (facoltativo)** – Se necessario, configurare ulteriori indirizzi e-mail SMTP da utilizzare come alias per il nuovo account utente.

Configurazione del server e-mail aziendale

Pianificazione della distribuzione di Microsoft Exchange

Se si desidera presentare ai clienti più indirizzi e-mail per i contatti, è necessario configurare un alias per ciascun indirizzo aggiuntivo riferito al nuovo account utente. La creazione di un alias assicura che i messaggi e-mail inviati al server e-mail aziendale vengano instradati alla casella postale del server e-mail di OpenScape Contact Center, per la gestione da parte degli agenti. Per ulteriori informazioni, consultare la *Guida di Manager*.

Poiché Microsoft Exchange Server 2007 converte gli alias nell'indirizzo dell'account utente principale per i messaggi sia in entrata che in uscita, è necessario configurare una casella di posta di Exchange per ogni alias da utilizzare e fare in modo che tale casella inoltri i messaggi all'account utente principale. Ciò è particolarmente importante negli ambienti multi-tenant, dove garantisce che se un cliente invia un messaggio e-mail a un alias, ad esempio sales@company1.com, tale messaggio venga instradato all'unità operativa appropriata. Assicura inoltre che l'indirizzo e-mail in entrata non venga convertito nell'indirizzo dell'account principale al momento di rispondere.

- **Criterio di limitazione (Microsoft Exchange Server 2013)** – Quando si utilizza Microsoft Exchange Server 2013, i valori ImapMaxBurst e ImapRechargeRate nel criterio di limitazione possono influenzare negativamente la produttività e-mail dell'account di posta elettronica OpenScape Contact Center. Per ottenere la massima produttività, si consiglia di creare un criterio di limitazione specifico per l'account di posta elettronica OpenScape Contact Center e di impostare i valori ImapMaxBurst e ImapRechargeRate su 8000000 o su un valore superiore.
- **Ridondanza shadow (Microsoft Exchange Server 2013)** – Quando si utilizza Microsoft Exchange Server 2013, la funzionalità Ridondanza shadow nelle impostazioni della configurazione di trasporto può influenzare negativamente la produttività e-mail dell'account di posta elettronica OpenScape Contact Center. Per ottenere la massima produttività, si consiglia di impostare il flag ShadowRedundancyEnabled su false.

3.4.1 Come specificare intestazioni personalizzate (solo Microsoft Exchange Server 2007, 2010 e 2013)

In Microsoft Exchange Server 2007, 2010 e 2013, le intestazioni personalizzate necessarie per la funzionalità e-mail di OpenScape Contact Center potrebbero non essere disponibili tramite l'interfaccia IMAP Microsoft Exchange. Se si desidera utilizzare Microsoft Exchange Server 2007, 2010 o 2013 come server e-mail IMAP aziendale, occorre eseguire un'utility (osccmseheaders.exe) che invia uno speciale messaggio e-mail utilizzando l'interfaccia SMTP Microsoft Exchange. Una volta che il messaggio e-mail speciale è stato inviato, le intestazioni personalizzate richieste diventeranno disponibili nell'interfaccia IMAP Microsoft Exchange.

Prima di eseguire l'utility, è necessario:

- Configurare Microsoft Exchange Server per il supporto dell' SMTP autenticato. L'utilità impiega una sessione con protocollo SMTP autenticato per specificare le intestazioni personalizzate. Se necessario, è possibile disattivare l' SMTP autenticato una volta eseguita correttamente l'utilità.
- Se si utilizza Microsoft Exchange Server 2007 SP2 o versioni successive, eseguire il seguente comando da Exchange Management Shell nel computer di Microsoft Exchange Server:

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

Se necessario, dopo l'esecuzione dell'utilità è possibile ripristinare il valore precedente della proprietà HeaderPromotionModeSetting.

Per specificare intestazioni personalizzate:

1. Sul server principale, passare alla cartella dove è installato il software OpenScape Contact Center e fare doppio clic su **osccmseheaders.exe**. Viene visualizzata una finestra di prompt dei comandi.
2. Premere **INVIO** per continuare.
3. Al prompt **From address**, digitare l'indirizzo e-mail da utilizzare come mittente (Da) per inviare il messaggio e-mail speciale, quindi premere **INVIO**. Questo deve essere l'indirizzo e-mail associato all'account utente utilizzato per l'autenticazione con Microsoft Exchange Server, ad esempio l'account OSCCEmail predefinito.
4. Al prompt **To address**, digitare l'indirizzo e-mail al quale si desidera inviare (A) il messaggio e-mail speciale, quindi premere **INVIO**. Tale indirizzo e-mail deve essere noto in Microsoft Exchange Server.
5. Al prompt **Subject**, digitare un oggetto per il messaggio e-mail speciale, quindi premere **INVIO**.
6. Al prompt **SMTP server host name**, digitare il nome host del PC Microsoft Exchange Server quindi premere **INVIO**.
7. Al prompt **SMTP server port number**, digitare il numero di porta configurato per SMTP sul PC Microsoft Exchange Server quindi premere **INVIO**.
8. Al prompt **SMTP user name**, digitare il nome utente dell'account Microsoft Exchange Server che verrà utilizzato per inviare il messaggio e-mail speciale, quindi premere **INVIO**. L'account deve essere in grado di inviare messaggi e-mail mediante l'indirizzo specificato al punto 3.
9. Al prompt **SMTP password**, digitare la password dell'account Microsoft Exchange Server che verrà utilizzato per inviare il messaggio e-mail speciale, quindi premere **INVIO**.

Configurazione del server e-mail aziendale

Pianificazione della distribuzione di IBM Lotus Domino

3.5 Pianificazione della distribuzione di IBM Lotus Domino

Se si desidera che il sistema OpenScape Contact Center utilizzi Lotus Domino, è necessario configurare una casella di posta abilitata IMAP per la ricezione dei messaggi e-mail degli utenti. Assicurarsi di configurare **Format preference for incoming mail** sulla casella di posta come **Prefers MIME**. Per informazioni relative a come eseguire questa e altre operazioni descritte nella presente sezione, fare riferimento alla documentazione di Lotus domino.

IMPORTANTE: La configurazione di Lotus Domino deve essere completata solo da un amministratore Lotus Domino qualificato.

Se si desidera presentare ai clienti più indirizzi e-mail per i contatti, è necessario configurare un alias per ciascun indirizzo aggiuntivo riferito alla casella di posta abilitata IMAP. La creazione di un alias assicura che i messaggi e-mail inviati al server e-mail aziendale vengano instradati alla casella postale del server e-mail di OpenScape Contact Center, per la gestione da parte degli utenti. Per ulteriori informazioni, consultare la *Guida di Manager*.

Consultare la Guida di Lotus Domino Administrator per informazioni su:

- Protezione per gli alias configurati
- Configurazione del routing SMTP

IMPORTANTE: Assicurarsi di attivare **immediate full text indexing** sul database creato. Se non si attiva ‘immediate full test indexing’, le ricerche IMAP non riescono e le prestazioni del server e-mail di OpenScape Contact Center risultano insoddisfacenti.

3.5.1 Compattazione del database

Al momento di compattare il database di Lotus Domino, il server e-mail di OpenScape Contact Center ritiene che il server e-mail aziendale sia inattivo poiché l'accesso IMAP al database è interrotto. Il tipo di compattazione del database implementato determina per quanto tempo il server e-mail di OpenScape Contact Center può accedere al database di Lotus Domino. Si consiglia di selezionare l'opzione **In-place compacting with space recovery only** (flag -b). È il metodo più rapido, con un effetto minimo sul sistema.

IMPORTANTE: Si consiglia di compattare il database del server e-mail aziendale durante il periodo di manutenzione dati del server e-mail di OpenScape Contact Center. Se si esegue la manutenzione in un altro momento, si può compromettere l'elaborazione dei messaggi e-mail nel sistema OpenScape Contact Center.

3.6 Impostazione di una connessione protetta per un server e-mail

Per impostare una connessione (SSL) protetta tra il server e-mail aziendale e il server e-mail OpenScape Contact Center, procedere come segue:

- Installare un certificato SSL e attivare la protezione SSL per i messaggi e-mail in entrata (IMAP4) e/o in uscita (SMTP) sul server e-mail aziendale. Attenersi alle istruzioni fornite dal produttore o rivolgersi al provider di posta elettronica per assistenza.

NOTA: I server Lotus Domino permettono connessioni con protezione SSL su una data porta anche se la porta non è configurata in modo da richiedere l'utilizzo di SSL. Ciò non causa problemi operativi. Tuttavia gli amministratori devono essere consapevoli che, anche se OpenScape Contact Center è in grado di stabilire una connessione protetta con il server Domino, non si tratta di un'indicazione affidabile della disponibilità di SSL per le connessioni stabilite da altri client e-mail. Se occorre un ambiente Domino protetto, è necessario controllarlo attentamente nella configurazione Domino.

- Attivare la protezione SSL per il corrispondente server IMAP e/o il server SMTP nell'applicazione Manager. Per ulteriori informazioni, consultare la *Guida di Manager*.

Configurazione del server e-mail aziendale

Utilizzo di un'autenticazione su un server e-mail

Si consiglia di procurarsi il certificato da un'autorità di certificazione riconosciuta, quale VeriSign, benché siano supportati anche i certificati autofirmati. In ogni caso, il certificato deve essere attendibile.

NOTA: Quando si utilizza un certificato autogenerato o generato da un'autorità di certificazione che non è coperta da uno keystore di Java predefinito e si desidera installare un nuovo certificato SSL sui server di posta aziendali, potrebbe essere necessario aggiungere il certificato radice+intermedio corrispondente nel keystore del pacchetto Java utilizzato dal Portale agenti. È possibile aggiungere il certificato al keystore utilizzando la seguente riga di comando (dalla directory bin\<Java>):

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

3.7 Utilizzo di un'autenticazione su un server e-mail

Nel sistema OpenScape Contact Center, l'autenticazione è obbligatoria per il server IMAP e facoltativa per il server SMTP. Le impostazioni di autenticazione specificate sul server e-mail aziendale devono corrispondere a quelle specificate nel sistema OpenScape Contact Center.

Per attivare l'autenticazione in Microsoft Exchange:

- Selezionare **Autenticazione di base**.
- Se SSL è attivo, assicurarsi di selezionare l'opzione che richiede la crittografia.

Per attivare l'autenticazione in IBM Lotus Domino:

- Il sistema OpenScape Contact Center non utilizza certificati client, pertanto per le opzioni di autenticazione SSL, assicurarsi che **Certificato client** sia impostato su **No** e **Nome & password** su **Sì**.

3.8 Supporto della funzione report e-mail

Per utilizzare la funzione report e-mail, il server e-mail OpenScape Contact Center deve essere in grado di inviare messaggi e-mail attraverso il server e-mail aziendale utilizzando un indirizzo “Da” diverso dall’indirizzo del mittente che il server e-mail OpenScape Contact Center utilizza per connettersi al server e-mail aziendale.

L'intenzione è quella di consentire al server e-mail OpenScape Contact Center di inviare messaggi e-mail per conto di altri account e-mail SMTP. Ad esempio, quando il server e-mail OpenScape Contact Center è connesso al server e-mail aziendale come "oscc@company.com" e viene inviato un messaggio e-mail per conto di "manager@company.com", ci si attende che il destinatario del messaggio visualizzi "Da: manager@company.com" e non "Da: oscc@company.com per conto di manager@company.com".

Quando il server e-mail aziendale viene configurato per l'autenticazione STMP e l'inoltro SMTP è soggetto a restrizioni, questa funzionalità può essere ottenuta nel modo seguente:

- **Microsoft Exchange Server 2007, 2010 e 2013** – Se occorre inviare messaggi e-mail da indirizzi e-mail nello stesso dominio, è possibile concedere all'account del server e-mail OpenScape Contact Center sul server e-mail aziendale l'autorizzazione completa per ciascuna delle caselle di posta dell'utente di OpenScape Contact Center, tramite Active Directory. È inoltre necessario creare un nuovo contatto in Active Directory con l'indirizzo e-mail SMTP OSCCEmail@company.com, quindi assegnare l'autorizzazione Invia come per il nuovo contatto all'account e-mail del server OpenScape Contact Center. Per ulteriori informazioni, vedere la documentazione di Microsoft Exchange Server.
- **Solo Microsoft Exchange Server 2007, 2010 e 2013** – Se occorre inviare messaggi e-mail da indirizzi e-mail esterni al dominio, è possibile configurare un connettore di ricezione personalizzato. Per ulteriori informazioni su come configurare un connettore di ricezione, consultare la documentazione di Microsoft Exchange Server.
- **Lotus Domino 8.0 e 8.5** – L'unico requisito è accertarsi che il valore dell'impostazione di SMTPVerifyAuthenticatedSender sia 0. Per ulteriori informazioni su questa impostazione, vedere la documentazione di Lotus Domino.

Configurazione del server e-mail aziendale

Supporto della funzione report e-mail

4 Configurazione di un server Web aziendale

Questo capitolo fornisce istruzioni dettagliate su come configurare i file dei componenti Web necessari sul server Web aziendale per supportare le funzioni OpenScape Contact Center Collaborazione Web, Richiamata Web e integrazione VoiceXML. Descrive inoltre come impostare una connessione protetta per il server Web aziendale, individuare e personalizzare file predefiniti e risolvere i problemi più comuni.

IMPORTANTE: Prima di aggiornare i file sul server Web aziendale, copiare tutti i file dei componenti Web personalizzati in una posizione protetta in modo da poterli riapplicare al termine dell'aggiornamento. In caso contrario, i file personalizzati andranno persi poiché non vengono conservati nel processo di aggiornamento.

NOTA: Al momento di creare o personalizzare pagine Web per utilizzarle con le funzionalità Web di OpenScape Contact Center, adottare precauzioni per ridurre al minimo le potenziali vulnerabilità della sicurezza.

4.1 Requisiti di sistema per l'utilizzo di componenti Web

Per un funzionamento ottimale dei file di componenti Web, è necessario assicurarsi che il server Web aziendale e il browser Web utilizzato per accedere alle funzioni soddisfino i requisiti indicati in questa sezione.

4.1.1 Requisiti del server Web aziendale

Il server Web aziendale può utilizzare uno qualsiasi dei seguenti server Web e dei sistemi operativi corrispondenti:

- Microsoft Internet Information Server (IIS) 8 e 8.5
- Apache Tomcat 6.0 su server Red Hat Enterprise Linux 6
- Apache Tomcat 7.0.63 su server Red Hat Enterprise Linux 6

4.1.2 Requisiti browser Web

I seguenti browser Web sono stati testati in combinazione con il sistema OpenScape Contact Center:

Configurazione di un server Web aziendale

Configurazione di componenti Web

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

Per ulteriori informazioni su questi server, consultare la documentazione del produttore.

Assicurarsi che il browser Web sia configurato come segue:

- Livello di protezione Internet impostato su medio o basso
- Javascript attivo
- Pop-up attivi (il blocco dei pop-up è disattivato o configurato per accettare sempre i pop-up del sito Web)

4.2 Configurazione di componenti Web

Questa sezione descrive come configurare i componenti Web, in base al tipo di server Web installato.

NOTA: A seguito della configurazione del Server di interazione Web, può essere necessario eseguire l'ulteriore configurazione dei componenti Web. Ad esempio, può essere necessario impostare una connessione protetta per un server Web o personalizzare i componenti Web. Per ulteriori informazioni, vedere Sezione 4.3, "Impostazione di una connessione protetta per un server Web", a pagina 32 e Sezione 4.4, "Localizzazione e personalizzazione di componenti Web", a pagina 34..

4.2.1 Configurazione di un server IIS

Questa sezione descrive come configurare i componenti Web su un server IIS. Se occorrono informazioni sull'installazione e la configurazione del server IIS, consultare la documentazione Windows.

NOTA: OpenScape Contact Center utilizza un meccanismo di monitoraggio del sistema per controllare la connessione fra il server Web aziendale e il server di interazione Web. Esistono varie configurazioni in un server IIS, come il riciclo del pool di applicazioni, che determinano lo scaricamento del componente ISAPI di OpenScape Contact Center. In tal caso, l'applicazione System Monitor indica che la connessione non è attiva. Per evitare questo problema, modificare la configurazione in base a quanto descritto nella documentazione di Windows.

NOTA: Quando il server IIS viene eseguito su un sistema operativo a 64 bit, server IIS deve essere configurato per l'esecuzione di applicazioni Web a 32 bit, in quanto la DLL ISAPI di OpenScape Contact Center è a 32 bit.

4.2.1.1 Configurazione dei file dei componenti Web su un server IIS

È necessario copiare i file dei componenti Web dal DVD OpenScape Contact Center sul server Web aziendale, quindi aggiornare i file.

Per configurare i file dei componenti Web su un server IIS:

1. Creare una cartella sul server Web aziendale per memorizzare i file dei componenti Web. Ad esempio:

c :\HPPC

2. Inserire il DVD di OpenScape Contact Center nell'unità DVD-ROM.
3. Nel DVD, passare alla cartella **Web Components OpenScape Contact Center\IIS**.
4. Copiare il file **HPPCEnterpriseWeb.zip** sul server Web aziendale e decomprimerlo nella posizione creata nella fase 1. Viene visualizzata la seguente struttura file:

c:\HPPC\Default.htm

c:\HPPC\hppcwis.dll

c:\HPPC\HPWC.ini

c:\HPPC\html

c:\HPPC\html\WCCallbackMain.htm

c:\HPPC\html\WCMain.htm

c:\HPPC\html\english (e file corrispondenti)

c:\HPPC \images (e file corrispondenti)

c:\HPPC\VXML (e file corrispondenti)

IMPORTANTE: Non modificare questa struttura file, poiché è necessaria per la loro corretta esecuzione.

Configurazione di un server Web aziendale

Configurazione di componenti Web

5. Aprire il file **HPWC.ini** in un editor di testo e, in **[HPPCSETTINGS]**, modificare l'impostazione relativa all'**indirizzo** inserendo il nome host o l'indirizzo IP del server principale OpenScape Contact Center.

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), è necessario modificare l'impostazione relativa all'**indirizzo** inserendo il nome del cluster o l'indirizzo IP virtuale del cluster di server.

IMPORTANTE: Assicurarsi che l'impostazione **porta** sia uguale al numero porta configurato nell'applicazione Manager e che la porta sia aperta nel firewall tra il server Web aziendale e il server principale OpenScape Contact Center. Il numero porta predefinito è 6021. Se si modifica il numero porta, è necessario riavviare il server Web aziendale e il server di interazione Web.

6. Salvare e chiudere il file.
7. In IIS, creare una nuova directory virtuale per il sito Web predefinito. Per ulteriori informazioni, consultare la documentazione Windows. Quando si crea la directory virtuale, assicurarsi di:
 - Fornire un alias come HPPC.
 - Selezionare la cartella creata nella fase 1 quando il sistema richiede di specificare la directory del contenuto del sito Web.
 - Attivare le seguenti autorizzazioni di accesso:
 - Lettura
 - Esecuzione script (ad esempio, ASP)
 - Esecuzione (ad esempio, applicazioni ISAPI o CGI)

IMPORTANTE: Assicurarsi che le estensioni ISAPI siano **consentite** nel nodo Web Service Extensions in IIS Manager per IIS. In caso contrario, quando il sistema tenta di invocare la funzionalità ISAPI di OpenScape Contact Center, viene restituito l'errore 404. Per attivare o disattivare le estensioni ISAPI singolarmente, consultare la guida di Microsoft Management Console per informazioni sull'attivazione e disattivazione del contenuto dinamico nelle configurazioni del server.

4.2.1.2 Verifica della collaborazione Web su un server IIS

Questa sezione descrive come verificare la funzionalità di collaborazione Web su un server IIS.

Per verificare la collaborazione Web su un server IIS:

1. Aprire un browser Web e immettere l'URL per accedere alla pagina demo WCMain.htm. Il formato dell'URL è:

`http://<nomehost>/<percorsovirtuale>/html/WCMain.htm`
dove

- `<nomehost>` è il nome host o l'indirizzo IP del server Web aziendale.
- `<Percorsovirtuale>` è il percorso della directory virtuale creata.

Ad esempio:

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

2. Nella pagina WCMain.htm, fare clic sul pulsante **Sessione Web richiesta**. Se viene visualizzata una pagina con il messaggio "You have requested a live Web Collaboration session", è stato caricato il file **CaptureWCData.htm** ed è stata configurata correttamente la collaborazione Web sul server Web in una configurazione di base predefinita.

NOTA: A questo punto, se si fa clic sul pulsante **Inoltra** in **CaptureWCData.htm** è possibile ricevere un errore. È possibile fare clic su questo pulsante dopo aver completato la configurazione del server Web.

3. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

Configurazione di un server Web aziendale

Configurazione di componenti Web

4.2.1.3 Verifica della richiamata Web su un server IIS

Questa sezione descrive come verificare la funzione richiamata Web su un server IIS.

Per verificare la richiamata Web su un server IIS:

1. Aprire un browser Web e immettere l'URL per accedere alla pagina demo WCCallbackMain.htm. Il formato dell'URL è:

`http://<nomehost>/<percorsovirtuale>/html/WCCallbackMain.htm`
dove

- <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.
- <Percorsovirtuale> è il percorso della directory virtuale creata.

Ad esempio:

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

2. Nella pagina WCCallbackMain.htm, fare clic su **Tenta Richiamata Web**. Se si apre una pagina che mostra campi relativi a informazioni su contatti cliente, si è caricato il file **WebCallback.htm** e si è configurata correttamente la richiamata Web sul server Web in una configurazione di base predefinita.

NOTA: A questo punto, se si fa clic sul pulsante **Inoltra** in **WebCallback.htm** è possibile ricevere un errore. È possibile fare clic su questo pulsante dopo aver completato la configurazione del server Web.

3. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

4.2.1.4 Verifica dell'integrazione VoiceXML su un server IIS

Questa sezione descrive come verificare l'integrazione VoiceXML su un server IIS.

Per verificare l'integrazione VoiceXML su un server IIS:

1. Assicurarsi che VoiceXML sia definito come tipo MIME nelle proprietà dell'elenco virtuale o nel sistema. Ad esempio, per definire il tipo MIME nell'elenco virtuale:
 - a) Fare clic con il pulsante destro del mouse sull'elenco virtuale, quindi scegliere **Proprietà**.
 - b) Selezionare la scheda **HTTP Headers**, quindi fare clic su **MIME Types**.
 - c) Fare clic su **Nuovo**.

- d) Nella casella **Estensione**, immettere **VXML**.
 - e) Nella casella **Tipo MIME**, digitare **application/voicexml+xml**.
 - f) Fare clic su **OK**.
2. Aprire un browser Web e immettere l'URL per accedere alla pagina demo Initialize.vxml. Il formato dell'URL è:
- ```
http://<nomehost>/<percorsovirtuale>/VXML/
Initialize.vxml
```
- dove:
- <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.
  - <Percorsovirtuale> è il percorso della directory virtuale creata.
- Ad esempio:
- ```
http://127.0.0.1:8080/HPPC/VXML/Initialize.vxml
```
3. Nella finestra di dialogo visualizzata, fare clic su **OK** per aprire il file Initialize.vxml. Se viene visualizzato il file Initialize.vxml, VoiceXML è stato configurato correttamente sul server Web in una configurazione di base predefinita.
 4. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

4.2.2 Configurazione di un server

Questa sezione descrive come configurare le impostazioni dei componenti Web su un server Tomcat. Se occorrono informazioni sull'installazione e la configurazione del server Tomcat o sulla connessione di Tomcat al server Apache, fare riferimento alla documentazione del server Tomcat.

4.2.2.1 Configurazione del file .war su un server Tomcat

Questa sezione descrive come configurare e distribuire il file .war su un server Tomcat.

Per configurare il file .war su un server Tomcat:

1. Inserire il DVD di OpenScape Contact Center nell'unità DVD-ROM.
2. Nel DVD, passare alla cartella **Web Components OpenScape Contact Center\Apache Tomcat**.
3. Copiare il file **HPPCEEnterpriseWeb.war** sul server Web aziendale.

Configurazione di un server Web aziendale

Configurazione di componenti Web

4. Rinominare il file .war in un modo appropriato per l'ambiente in uso. Nelle seguenti istruzioni, il nome del file .war è stato modificato in **HPPC.war**. Viene utilizzato per distribuire l'applicazione Web di esempio denominata HPPC. Per garantirne la funzionalità, il nome del file .war deve mantenere le maiuscole e le minuscole indicate nella configurazione di esempio.
5. Assicurarsi che il JDK (Java Development Kit) sia installato.
6. Per estrarre il file config.properties in una nuova cartella denominata hpwcapp, aprire una finestra prompt dei comandi, passare alla directory che contiene il file HPPC.war, digitare quanto segue al prompt dei comandi, quindi premere **INVIO**:

```
jar xfv HPPC.war hpwcapp/config.properties
```
7. Aprire il file **hpwcapp/config.properties** in un editor di testo e procedere come segue:
 - Modificare l'impostazione **servlet.name** in modo da riflettere il nome del file .war specificato nella fase 4. Nella configurazione di esempio, l'impostazione è `servlet.name=/HPPC/hppcwebchat`.
 - Modificare l'impostazione **socket.server.name** con il nome host o l'indirizzo IP del server principale OpenScape Contact Center.

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), è necessario modificare l'impostazione **socket.server.name** inserendo il nome del cluster o l'indirizzo IP virtuale del cluster di server.

NOTA: Assicurarsi che l'impostazione **socket.server.port** sia uguale al numero porta configurato nell'applicazione Manager e che la porta sia aperta nel firewall tra il server Web aziendale e il server principale OpenScape Contact Center. Il numero porta predefinito è 6021. Se si modifica il numero porta, è necessario riavviare il server Web aziendale e il server di interazione Web.

8. Salvare e chiudere il file.
9. Per aggiornare il file HPPC.war, nel prompt dei comandi, nella stessa directory della fase 6, digitare:

```
jar ufv HPPC.war hpwcapp/config.properties
```
10. Distribuire il file HPPC.war sul server Tomcat. Per ulteriori informazioni, consultare la documentazione di Tomcat Web Application Manager.

4.2.2.2 Verifica della collaborazione Web su un server Tomcat

Questa sezione descrive come verificare la funzione di collaborazione Web su un server Tomcat.

Per verificare la collaborazione Web su un server Tomcat:

1. Aprire un browser Web e immettere l'URL per accedere alla pagina demo WCMain.htm. Il formato dell'URL è:

`http://<nomehost>/HPPC/html/WCMain.htm`

dove <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.

Ad esempio :

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

2. Nella pagina WCMain.htm, fare clic sul pulsante **Sessione Web richiesta**. Se viene visualizzata una pagina con il messaggio "You have requested a live Web Collaboration session", è stato caricato il file **CaptureWCData.htm** ed è stata configurata correttamente la collaborazione Web sul server Web in una configurazione di base predefinita.

NOTA: A questo punto, se si fa clic sul pulsante **Inoltra** in **CaptureWCData.htm** è possibile ricevere un errore. È possibile fare clic su questo pulsante dopo aver completato la configurazione del server Web.

3. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

4.2.2.3 Verifica della richiamata Web utilizzando un server Tomcat

Questa sezione descrive come verificare la funzione di richiamata Web su un server Tomcat.

Per verificare la richiamata Web su un server Tomcat:

1. Aprire un browser Web e immettere l'URL per accedere alla pagina demo WCCallbackMain.htm. Il formato dell'URL è:

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

dove <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.

Ad esempio:

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

Configurazione di un server Web aziendale

Configurazione di componenti Web

2. Nella pagina WCCallbackMain.htm, fare clic su **Tenta Richiamata Web**. Se si apre una pagina che mostra campi relativi a informazioni su contatti cliente, si è caricato il file **WebCallback.htm** e si è configurata correttamente la richiamata Web sul server Tomcat in una configurazione di base predefinita.

NOTA: A questo punto, se si fa clic sul pulsante **Inoltra** in **WebCallback.htm** è possibile ricevere un errore. È possibile fare clic su questo pulsante dopo aver completato la configurazione del server Web.

3. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

4.2.2.4 Verifica dell'integrazione VoiceXML su un server Tomcat

Questa sezione descrive come verificare l'integrazione VoiceXML sul server Tomcat.

Per verificare l'integrazione VoiceXML su un server Tomcat:

1. Aprire un browser Web e immettere l'URL per accedere alla pagina demo Initialize.vxml. Il formato dell'URL è:

```
http://<nomehost>/HPPC/VXML/Initialize.vxml
```

dove <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.
Ad esempio:

```
http://127.0.0.1:8080/HPPC/VXML/Initialize.vxml
```
2. Nella finestra di dialogo visualizzata, fare clic su **OK** per aprire il file Initialize.vxml. Se viene visualizzato il file Initialize.vxml, VoiceXML è stato configurato correttamente sul server Tomcat in una configurazione di base predefinita.
3. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

4.2.3 Configurazione di un Sun Java System Web Server

Questa sezione descrive come configurare i componenti Web su un server Web Sun Java System. Se occorrono informazioni sull'installazione e la configurazione del Sun Java System Web Server, consultare la documentazione Sun.

4.2.3.1 Configurazione del file .war su un server Web Sun Java System

Questa sezione descrive come configurare e distribuire il file .war su un server Web Sun Java System.

Per configurare il file .war su un server Web Sun Java System:

1. Inserire il DVD di OpenScape Contact Center nell'unità DVD-ROM.
2. Nel DVD, passare alla cartella **Web Components OpenScape Contact Center\Sun Java System Web Server**.
3. Copiare il file **HPPCEnterpriseWeb.war** sul server Web aziendale.
4. Rinominare il file .war in un modo appropriato per l'ambiente in uso. Nelle seguenti istruzioni, il nome del file .war è stato modificato in **HPPC.war**. Viene utilizzato per distribuire l'applicazione Web di esempio denominata HPPC. Per garantirne la funzionalità, il nome del file .war deve mantenere le maiuscole e le minuscole indicate nella configurazione di esempio.
5. Per estrarre il file config.properties in una nuova cartella denominata hpwcapp, aprire una finestra prompt dei comandi, passare alla directory che contiene il file HPPC.war, digitare quanto segue sulla riga di comando, quindi premere **INVIO**:

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

6. Aprire il file **hpwcapp/config.properties** in un editor di testo e procedere come segue:
 - Modificare l'impostazione **servlet.name** in modo da riflettere il nome del file .war specificato nella fase 4. Nella configurazione di esempio, l'impostazione è **servlet.name=/HPPC/hppcwebchat**.
 - Modificare l'impostazione **socket.server.name** con il nome host o l'indirizzo IP del server principale OpenScape Contact Center.

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), è necessario modificare l'impostazione **socket.server.name** inserendo il nome del cluster o l'indirizzo IP virtuale del cluster di server.

NOTA: Assicurarsi che l'impostazione **socket.server.port** sia uguale al numero porta configurato nell'applicazione Manager e che la porta sia aperta nel firewall tra il server Web aziendale e il server principale OpenScape Contact Center. Il numero porta predefinito è 6021. Se si modifica il numero porta, è necessario riavviare il server Web aziendale e il server di interazione Web.

Configurazione di un server Web aziendale

Configurazione di componenti Web

7. Salvare e chiudere il file.
8. Per aggiornare il file HPPC.war, nel prompt dei comandi, nella stessa directory della fase 5, digitare:

```
jar ufv HPPC.war hpwcapp/config.properties
```
9. Per creare una nuova istanza server, visitare il sito per amministratori di Sun Java System Web Server. Per accedere al sito riservato agli amministratori, aprire il browser Web e digitare l'URL. Il formato dell'URL è:

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

dove <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.
Quando si crea l'istanza del server, utilizzare **HPPC** come identificatore del server. In questo modo si crea automaticamente una cartella denominata / **https-HPPC**. Per ulteriori informazioni, consultare la documentazione Sun.

NOTA: Se si seleziona la casella di controllo **Never attempt to resolve IP addresses into host names**, è necessario mantenere la coerenza con la configurazione. Ciò significa utilizzare indirizzi IP oppure nomi host, non entrambi.

10. Avviare la nuova istanza del server.
11. Distribuire il file HPPC.war nel Sun Java System Web Server. Per ulteriori informazioni, consultare la documentazione Sun. Quando si distribuisce il file .war, l'URL dell'applicazione è /**HPPC**.

4.2.3.2 Verifica della collaborazione Web su un Sun Java System Web Server

Per verificare la collaborazione Web su Sun Java System Web Server.

Per verificare la collaborazione Web su un Sun Java System Web Server:

1. Aprire un browser Web e immettere l'URL per accedere alla pagina demo WCMain.htm. Il formato dell'URL è:

```
http://<nomehost>/HPPC/html/WCMain.htm
```

dove <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.

Ad esempio:

```
http://127.0.0.1:8181/HPPC/html/WCMain.htm
```

2. Nella pagina WCMain.htm, fare clic sul pulsante **Sessione Web richiesta**. Se viene visualizzata una pagina con il messaggio "You have requested a live Web Collaboration session", è stato caricato il file **CaptureWCData.htm** ed è stata configurata correttamente la collaborazione Web sul server Web in una configurazione di base predefinita.

NOTA: A questo punto, se si fa clic sul pulsante **Inoltra** in **CaptureWCData.htm** è possibile ricevere un errore. È possibile fare clic su questo pulsante dopo aver completato la configurazione del server Web.

3. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

4.2.3.3 Verifica della richiamata Web su un Sun Java System Web Server

Questa sezione descrive come verificare la richiamata Web su un Sun Java System Web Server:

Per verificare la richiamata Web su un Sun Java System Web Server:

1. Avviare l'istanza server creata in Sezione 4.2.3.1, "Configurazione del file .war su un server Web Sun Java System", a pagina 29.
2. Aprire un browser Web e immettere l'URL per accedere alla pagina demo WCCallbackMain.htm. Il formato dell'URL è:

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

dove <nomehost> è il nome host o l'indirizzo IP del server Web aziendale.

Ad esempio:

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

3. Nella pagina WCCallbackMain.htm, fare clic su **Tenta Richiamata Web**. Se si apre una pagina che mostra campi relativi a informazioni su contatti cliente, si è caricato il file **WebCallback.htm** e si è configurata correttamente la richiamata Web su Sun Java System Web Server in una configurazione di base predefinita.

NOTA: A questo punto, se si fa clic sul pulsante **Inoltra** in **WebCallback.htm** è possibile ricevere un errore. È possibile fare clic su questo pulsante dopo aver completato la configurazione del server Web.

4. Configurare il server di interazione Web sul server principale OpenScape Contact Center. Per ulteriori informazioni, consultare la *Guida di Manager*.

Configurazione di un server Web aziendale

Impostazione di una connessione protetta per un server Web

4.3 Impostazione di una connessione protetta per un server Web

Il sistema può essere configurato per utilizzare l'autenticazione basata sui certificati TLS per proteggere la connessione fra il server di interazione Web e il server Web aziendale.

Questa sezione descrive come attivare la protezione TLS nel server Web aziendale, in base al tipo di server Web aziendale disponibile.

Per completare la configurazione TLS, è inoltre necessario:

1. Installare un certificato TLS sul server principale. Per ulteriori informazioni, vedere il *Manuale di Installazione*.
2. Nell'applicazione Manager, selezionare una porta abilitata TLS per la connessione Web. Per ulteriori informazioni, consultare la *Guida di Manager*.

NOTA: Si consiglia di non attivare la protezione TLS nel server Web aziendale finché non sono complete tutte le altre configurazioni del server di interazione Web.

4.3.1 Attivazione TLS su un server IIS

Questa sezione descrive come attivare la protezione TLS in un server IIS.

Per attivare la protezione TLS su un server IIS:

1. Aprire il file **HPWC.ini** in un editor di testo.
2. In **[HPPCSETTINGS]**, assicurarsi che **Address** sia impostato sul nome host del server principale di OpenScape Contact Center, che corrisponde al nome comune del certificato TLS.

NOTA: Quando il sistema è configurato per l'alta disponibilità (warm standby), è necessario che **Address** sia impostato sul nome del cluster di server.

3. Impostare **TLSPort** sul numero porta da utilizzare per le funzioni Web protette, ad esempio:

SSLPort=443

NOTA: Assicurarsi che il numero porta qui configurato corrisponda al numero porta TLS configurato nell'applicazione Manager. Per ulteriori informazioni, consultare la *Guida di Manager*.

4. Impostare i flag SSL richiesti su true:

- Per Collaborazione Web, ChatUsesSSL=true
- Per Richiamata Web, CallbackUsesSSL=true
- Per VoiceXML, VoiceXMLUsesSSL=true

NOTA: Quando il flag TLS è impostato su true, la funzione sarà disponibile esclusivamente via TLS sulla porta specificata dall'impostazione TLSPort.

5. Nel menu **File**, fare clic su **Salva**, quindi selezionare **Esci**.

4.3.2 Attivazione TLS su un server Tomcat o Sun Java

Questa sezione descrive come attivare la protezione TLS in un server Web Tomcat o Sun Java System.

Se necessario, prima di iniziare scaricare JSSE (Java Secure Socket Extension). Per istruzioni dettagliate, consultare la documentazione del produttore.

Per attivare TLS su un server Tomcat o Sun Java:

1. Installare il keystore secondo le istruzioni del produttore.
2. Aprire il file **config.properties** in un editor di testo.
3. Impostare **socket.server.name** sul nome host del server principale OpenScape Contact Center, che corrisponde al nome comune del certificato TLS.

NOTA: Quando il sistema è configurato per l'alta disponibilità (warm standby), è necessario che **socket.server.name** sia impostato sul nome del cluster di server.

4. Impostare **socket.server.port.ssl** sul numero porta da utilizzare per le funzioni Web protette, ad esempio:

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

NOTA: Assicurarsi che il numero porta qui configurato corrisponda al numero porta TLS configurato nell'applicazione Manager. Per ulteriori informazioni, consultare la *Guida di Manager*.

Configurazione di un server Web aziendale

Localizzazione e personalizzazione di componenti Web

5. Impostare i flag SSL richiesti su true:
 - Per Collaborazione Web, `socket.webchat.ssl=true`
 - Per Richiamata Web, `socket.webcallback.ssl=true`
 - Per VoiceXML (solo Tomcat), `socket.voicexml.ssl=true`

NOTA: Quando il flag TLS è impostato su true, la funzione sarà disponibile esclusivamente via SSL sulla porta specificata dall'impostazione `socket.server.port.ssl`.

6. Nel menu **File**, fare clic su **Salva**, quindi selezionare **Esci**.

4.4 Localizzazione e personalizzazione di componenti Web

Dopo aver testato il server Web aziendale, è possibile localizzare e personalizzare i file dei componenti Web per il proprio ambiente.

4.4.1 Localizzazione dei componenti Web

Dopo aver testato il server Web aziendale, è possibile localizzare i file dei componenti Web nella lingua supportata sul proprio sito Web. L'esempio sotto mostra una procedura di localizzazione per la lingua tedesca.

Per localizzare i file dei componenti Web:

1. Creare una nuova sottodirectory nella directory html della struttura esistente, mostrata nella fase 4 di Sezione 4.2.1.1, "Configurazione dei file dei componenti Web su un server IIS". Ad esempio:
`c:\HPPC\html\deutsch`
2. Copiare tutti i file predefiniti in `c:\HPPC\html\english` nella nuova directory.
3. Nella nuova directory, utilizzare uno strumento appropriato per aggiornare il testo o i grafici delle pagine, come appropriato, e salvare i file con lo stesso nome. Ad esempio, può essere opportuno aggiornare il testo e i pulsanti in CallMePage.htm in base ai propri requisiti di localizzazione.

IMPORTANTE: Se si utilizzano simboli non-ASCII nelle pagine aggiornate, è necessario salvarli in un formato UTF-8.

4. Creare una copia del file WCMain.htm all'interno della stessa directory e rinominarlo. Ad esempio, è possibile rinominare WCMain.htm come WCDeutsch.htm:
`c:\HPPC\html\WCDeutsch.htm`
5. Aggiornare l'URL utilizzato dalla pagina (nell'esempio, WCDeutsch.htm) per indirizzare alla nuova directory. A tale scopo, sostituire "english" con la lingua corretta. Ad esempio:
`?varUserRequest=REQ_WEBCHAT_MAIN&varUserLanguage=deutsch`
6. Verificare la nuova pagina (ad esempio, WCDeutsch.htm) facendo clic sul pulsante **Occorre la Guida in tempo reale?**. Se la pagina **CaptureWCData.htm** viene visualizzata, la localizzazione della pagina WCMain.htm è stata completata correttamente.

4.4.2 Personalizzazione dei componenti Web

Dopo aver localizzato WCMain.htm, è necessario personalizzare il file CaptureWCData.htm poichè contiene elementi necessari a OpenScape Contact Center per connettere un cliente collaborazione Web con l'utente appropriato. Questo file contiene anche alcuni elementi di presentazione visiva della sessione di collaborazione Web, ad esempio saluti e icone, che possono essere personalizzati.

È necessario avere un file CaptureWCData.htm per ogni lingua localizzata, e ogni file CaptureWCData.htm deve trovarsi nella directory della lingua appropriata. Ad esempio:

`c:\HPPC\html\english\CaptureWCData.htm`

`c:\HPPC\html\deutsch\CaptureWCData.htm`

L'attuale pagina CaptureWCData.htm attivata dipende dalla lingua indicata nella pagina WCMain.htm. Ad esempio:

`?varUserRequest=REQ_WEBCHAT_MAIN&varUserLanguage=english`

`?varUserRequest=REQ_WEBCHAT_MAIN&varUserLanguage=deutsch`

Configurazione di un server Web aziendale

Localizzazione e personalizzazione di componenti Web

La tabella seguente mostra i parametri che possono essere aggiornati in CaptureWCData.htm.

IMPORTANTE: Non è possibile eliminare i parametri nel file captureWCData.htm. Non è possibile modificare o rimuovere il parametro VarUserRequest e i pulsanti standard.

Nome/ID	Descrizione	Dettagli
varUserLanguage	Definisce le pagine utilizzate durante la sessione di collaborazione Web.	Si tratta della sottodirectory della directory html (vedere Sezione 4.4.1, "Localizzazione dei componenti Web").
varHPPCLanguage	Il nome della lingua di collaborazione Web. Utilizzato per definire il gruppo di regole (messaggi standard, emoticon, ecc.) per sessioni di collaborazione Web.	Il valore deve corrispondere a una lingua di collaborazione Web definita nell'applicazione Manager.
varSessionPriority	La priorità del contatto. Utilizzato dal flusso di lavoro collaborazione Web durante il routing.	Il valore deve essere compreso fra 1 e 100.
varCustomerName	Nome cliente.	Senza limiti.
varSource	L'origine del contatto. Utilizzato dal flusso di lavoro collaborazione Web durante il routing.	Il valore deve essere espresso in una delle lingue supportate dal sistema OpenScape Contact Center. Non sono consentiti i caratteri non-ASCII, i caratteri ASCII non stampabili e i seguenti caratteri speciali: accento grave (`), asterisco (*), virgola (,), virgolette doppie ("'), punto esclamativo (!), segno di percentuale (%), barra verticale () e trattino basso (_).
varDestination	La destinazione del contatto. Utilizzato dal flusso di lavoro collaborazione Web durante il routing.	Il valore deve essere espresso in una delle lingue supportate dal sistema OpenScape Contact Center.
varCaption	Domanda del cliente.	Senza limiti.
varBusinessUnitName	In un ambiente multi-tenant, il nome dell'unità operativa a cui appartengono i contatti di collaborazione Web in ingresso.	Il valore deve corrispondere a una delle unità operative definite nel sistema OpenScape Contact Center. In un ambiente non multi-tenant, questo valore può essere ignorato.

Tabella 1

parametri CaptureWCData.htm

È inoltre possibile aggiornare altri elementi, ad es. Codice1 e Codice2, nonché aggiungere nuovi elementi in una delle lingue supportate da OpenScape Contact Center. Tutti gli elementi aggiuntivi aggiungono codici e valori nella raccolta dati contatto relativi alla richiesta di collaborazione Web e vengono utilizzati dal flusso di lavoro collaborazione Web.

4.5 Risoluzione dei problemi di collaborazione Web

Questa sezione fornisce soluzioni ad alcuni dei problemi più spesso riscontrati con collaborazione Web.

4.5.1 Problemi di configurazione del server Web

Durante la configurazione delle impostazioni di collaborazione Web sul server Web aziendale, si consiglia di tenere conto degli aspetti seguenti:

- Assicurarsi che il numero porta sia uguale al numero porta definito nell'applicazione Manager.
- Assicurarsi che l'indirizzo IP per il server Web aziendale sia puntato sul server principale OpenScape Contact Center.

NOTA: Queste impostazioni possono essere configurate nel file `HPWC.ini` sul server IIS o nel file `config.properties` nei server Tomcat o Sun Java System Web Server.

4.5.2 Problemi di connessione generali

Vengono descritti alcuni problemi di connessione generali e le soluzioni corrispondenti.

Problema: Non è possibile caricare la pagina iniziale o si riceve il messaggio di errore 404.

Soluzione: assicurarsi che sia possibile riferire il nome host all'indirizzo IP corretto. Se possibile, assicurarsi che il server Web aziendale sia in esecuzione e che l'URL utilizzato sia corretto.

NOTA: Se si utilizza un server Tomcat e si riceve questo errore, passare alla directory `[tomcat-root]/bin` quindi digitare `./startup.sh` per riavviare il server Web aziendale.

Configurazione di un server Web aziendale

Codici errore richiamata Web

Problema: Si riceve un errore di connessione (codice di errore 1003).

Soluzione: Assicurarsi che il Server di interazione Web sia in esecuzione e che l'indirizzo IP e il numero porta nel file di configurazione siano corretti. Queste impostazioni possono essere configurate nel file `HPWC.ini` sul server IIS o nel file `config.properties` nei server Tomcat o Sun Java System Web Server.

Occorre inoltre assicurarsi che il server Web aziendale sia in grado di risolvere correttamente il nome host del server di interazione Web.

Inoltre un errore di connessione può verificarsi se *non* è stato installato un certificato SSL sul server di interazione Web e l'impostazione di protezione è attiva. In questo caso è necessario installare un certificato server o utilizzare l'applicazione Manager per disattivare l'impostazione di protezione.

NOTA: Sul server Tomcat o in Sun Java System Web Server, è obbligatorio installare la libreria JSSE indipendentemente dal fatto che si utilizzi una connessione normale o protetta. Poiché sul server Web aziendale potrebbero essere installati più JRE (Java Runtime Engine) è necessario assicurarsi che la libreria JSSE sia installata nella stessa directory JRE utilizzata dal server Web aziendale. Ad esempio, Sun Java System Web Server permette di configurare il percorso per il JRE (Java Runtime Engine) nel file `start-jvm` contenuto nella directory `https-admserv` di Sun Java System Web Server. Per ulteriori informazioni, consultare la documentazione del produttore.

4.6 Codici errore richiamata Web

La seguente tabella elenca i codici degli errori che possono verificarsi quando si utilizza la funzione richiamata Web. Se il sistema presenta uno dei codici di errore elencati nella tabella, la richiamata non viene creata.

Oltre ai codici di errore elencati nella tabella, possono verificarsi anche vari errori del Callback Server, descritti nell'applicazione System Monitor.

Codice errore	Descrizione
1000	Si è verificato un errore generale.
1002	Il server di routing non è riuscito a connettersi al server di interazione Web.
1003	Tentativo di connessione al server di interazione Web non riuscito.
1006	Impossibile accedere alla pagina Web.
1007	Rilevato ID sessione non valido.
1008	JavaScript non è attivo.
1010	Parametro obbligatorio non valido.

Tabella 2

Codici errore richiamata Web

Codice errore	Descrizione
1011	Parametro non valido.
1012	Errore interno del Server di interazione Web.
1013	Errore di allocazione.
17006	Richiamata duplicata presente nel database.
17021	Il Callback Server non è in grado di elaborare una richiesta a causa di un errore interno.
17025	Si è verificato un errore generale.
17027	La coda richiamate non esiste.
17028	Piano richiamata non valido.
17029	Piano richiamata esterno al piano di routing richiamate configurato per il centro contatti.
17030	Nome cliente troppo lungo. La lunghezza massima è di 75 caratteri.
17031	Un numero di telefono appartiene all'elenco dei numeri definiti come Numeri esclusi.
17032	Descrizione della richiamata troppo lunga. La lunghezza massima è di 100 caratteri.
17033	Dati contatto troppo lunghi. La lunghezza massima è di 1000 caratteri.
17035	La priorità non è valida. La priorità deve essere compresa fra 1 e 100.
17040	Piano richiamata scaduto.
17047	Una data di avvio o fine di un piano richiamata non è valida. Una richiamata non può essere pianificata a oltre 180 giorni dalla data corrente.

Tabella 2

Codici errore richiamata Web

Configurazione di un server Web aziendale

Codici errore richiamata Web

5 Configurazione dell'integrazione presenze

Questo capitolo descrive gli elementi da configurare per supportare la funzione Integrazione presenze. La funzione di integrazione presenze permette agli utenti Client Desktop di visualizzare la presenza di diversi utenti tramite la funzione Elenco.

Se la funzione di integrazione presenze è attiva nell'applicazione Manager e l'utente Client Desktop effettua una ricerca nell'elenco, il sistema tenta di ottenere la presenza di ciascuna delle voci nei risultati di ricerca, come segue:

- Il sistema prima cerca di ottenere lo stato presenza dell'utente e del supporto voce dall'Applicazione OpenScape Unified Communications (UC), ma solo se la funzione di integrazione dell'Applicazione OpenScape UC è attiva e configurata.
- Se non si è utenti dell'Applicazione OpenScape UC o se la funzione di integrazione dell'Applicazione OpenScape UC non è attiva o non è disponibile, il sistema cerca di ottenere lo stato presenza utente dal sistema OpenScape Contact Center.
- Se non si è utenti di OpenScape Contact Center o lo stato presenza non è disponibile da OpenScape Contact Center e si è connessi a una piattaforma di comunicazione OpenScape Voice, il sistema cerca di ottenere lo stato della linea del dispositivo dell'utente dalla piattaforma di comunicazione OpenScape Voice.

Se si opera in un ambiente di rete, è possibile accedere alla presenza per gli utenti solo nel sito locale.

5.1 Configurazione di un account utente per l'Applicazione OpenScape UC

Per consentire al sistema di integrarsi con l'Applicazione OpenScape UC, è necessario configurare un account utente nell'Applicazione OpenScape UC utilizzabile dal sistema OpenScape Contact Center per accedere e mantenere la connettività con l'Applicazione OpenScape UC. Questo account utente viene specificato quando si configurano le opzioni di integrazione della presenza nell'applicazione Manager. Per dettagli sulla configurazione di un nuovo account utente, consultare la documentazione dell'Applicazione OpenScape UC.

Configurazione dell'integrazione presenze

Configurazione dell'elenco LDAP esterno

5.2 Configurazione dell'elenco LDAP esterno

Per consentire agli utenti Client Desktop di visualizzare la presenza di altri utenti, è necessario configurare l'elenco LDAP esterno in modo che supporti la visualizzazione delle presenze.

In particolare, si devono configurare uno o più dei seguenti campi nell'elenco:

- **ID presenza** (l'ID utente dell'Applicazione OpenScape UC)
- **Nome utente** (il nome utente OpenScape Contact Center)
- **Stato della linea** (lo stato della linea di OpenScape Voice, applicabile solo se il sistema è connesso a una piattaforma di comunicazione OpenScape Voice)

Per dettagli sulla configurazione dei campi, consultare la documentazione dell'elenco LDAP.

6 Manutenzione del sistema

Questo capitolo descrive come effettuare la manutenzione continuativa del sistema OpenScape Contact Center, compresi l'arresto del server principale, la modifica delle password e il backup del database.

L'accesso remoto a un server principale o a un server report centralizzati è fornito dal plug-in Servizio SSDP (Smart Service Delivery Platform). Il software del plug-in Servizio SSDP e la relativa documentazione vengono installati automaticamente sul server durante il processo di installazione generale. Per configurare il plug-in Servizio SSDP, attenersi alle istruzioni fornite nella documentazione corrispondente, disponibile sul DVD di OpenScape Contact Center nella cartella Utilities\OpenScape Service Plug-in.

NOTA: Durante le procedure di manutenzione generale del sistema, ad esempio l'aggiornamento della rete, prima di procedere si consiglia di arrestare il server principale di OpenScape Contact Center. Per istruzioni speciali, consultare Sezione 6.1, "Arresto di un server per la manutenzione del sistema".

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), l'arresto del servizio OpenScape Contact Center dalla finestra Servizi non determina un guasto.

6.1 Arresto di un server per la manutenzione del sistema

Quando occorre arrestare o riavviare un server OpenScape Contact Center che esegue Informix a scopo di manutenzione, talvolta Informix non dispone di tempo sufficiente per interrompere il servizio Informix IDS prima della chiusura del sistema operativo Windows. Se ciò accade, il database può danneggiarsi. Per evitare questo problema, si consiglia di arrestare sempre il servizio Informix IDS prima di arrestare o riavviare il server.

NOTA: Per assicurarsi che il database non venga danneggiato, arrestare sempre il servizio Informix IDS prima di arrestare o riavviare un server.

Manutenzione del sistema

Modifica delle password di OpenScape Contact Center e Informix

6.2 Modifica delle password di OpenScape Contact Center e Informix

Se occorre modificare le password di OpenScape Contact Center o Informix per qualsiasi motivo è necessario aggiornarle nelle tre posizioni seguenti:

- Finestra Servizi
- Finestra Gestione computer
- Finestra Configurazione avvio di OpenScape Contact Center (o applicazione System Monitor)

IMPORTANTE: Le password di OpenScape Contact Center e Informix possono essere modificate solo sotto la supervisione del rappresentante dell'assistenza.

La password Informix non può superare i 16 caratteri e non può contenere spazi.

Per modificare le password di OpenScape Contact Center e Informix:

1. Aprire la finestra **Servizi**.
2. Per modificare la password OpenScape Contact Center, procedere come segue:
 - a) Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA**.
 - b) Per ciascun servizio, aprire il servizio e fornire la nuova password nella scheda **Logon**.
3. Per modificare la password Informix, procedere come segue:
 - a) Arrestare i servizi seguenti: **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_nomeserver** (dove *nomeserver* è il nome del server OpenScape Contact Center) e **Informix Server Discovery Process for SNMP**.
 - b) Aprire il servizio **Informix IDS - ol_nomeserver** e immettere la nuova password nella scheda **Logon**.
 - c) Aprire il processo **Informix Server Discovery** per il servizio SNMP e fornire la nuova password nella scheda **Log On**.
4. Chiudere la finestra **Servizi**.
5. Aprire la finestra **Gestione computer**.
6. In **Utilità di sistema**, espandere **Utenti e gruppi locali**, quindi selezionare **Utenti**.

7. Per modificare la password OpenScape Contact Center, fare clic con il pulsante destro del mouse su **hppc**, quindi selezionare **Imposta password** e fornire la nuova password.
8. Per modificare la password Informix, fare clic con il pulsante destro del mouse su **Informix**, quindi selezionare **Imposta password** e fornire la nuova password.
9. Chiudere la finestra **Gestione computer**.
10. Aprire una finestra prompt dei comandi.
11. Nella riga di comando, immettere `tcfmain`, quindi premere **INVIO**. Viene visualizzata la finestra **Configurazione di avvio di OpenScape Contact Center**.
12. Per modificare la password Informix, fare clic sulla scheda **Server di amministrazione** e digitare la nuova password nella casella **Password server database**.

NOTA: Quando il sistema è in esecuzione, è inoltre possibile modificare la password Informix configurando la data di avvio del server di amministrazione mediante l'applicazione System Monitor. Per ulteriori informazioni, vedere la *guida dell'applicazione System Monitor*.

13. Chiudere la finestra **Configurazione di avvio di OpenScape Contact Center**.
14. Avviare i servizi seguenti: **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_nomeserver** (dove *nomeserver* è il nome del server OpenScape Contact Center) e **Informix Server Discovery Process for SNMP**.
15. Avviare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA**.

6.3 Backup del database

È necessario eseguire il backup del database OpenScape Contact Center regolarmente e ad ogni modifica della configurazione del sistema, allo scopo di proteggere i dati da eventuali guasti o danni. Le dimensioni del database possono diventare molto grandi, pertanto si consiglia di eseguire il backup solo durante i periodi con un traffico di contatti minimo.

NOTA: Oltre al database di OpenScape Contact Center, si consiglia di sottoporre a backup anche tutti i dati sul server, tramite un'utilità di backup. Assicurarsi che il backup contenga i dati di stato del sistema del server, che includono elementi quali il registro di sistema e i file di avvio.

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), assicurarsi di eseguire il backup di server principale, server di backup e server report centralizzati.

Sono disponibili due tipi di backup:

- **Backup completo** – Per evitare qualsiasi perdita di dati (tranne di quelli relativi al giorno corrente) si consiglia di eseguire giornalmente il backup completo del database. In ogni caso è opportuno sottoporre il database a backup almeno una volta a settimana.
- **Backup incrementale** – Per limitare l'eventualità di perdite di dati fra i backup completi del database, è possibile eseguire un backup incrementale del database. Ad esempio, se si esegue un backup completo del database durante la notte, è possibile sottoporre il database a backup incrementale durante il giorno. Il backup incrementale richiede meno tempo, poiché riguarda solo le modifiche dall'inizio dell'ultimo backup completo.

NOTA: Alcune delle procedure presentate in questa sezione sono state redatte presupponendo che l'utente abbia familiarità con l'utilizzo di Informix. Per istruzioni dettagliate, vedere la documentazione Informix all'indirizzo seguente:
<http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

6.3.1 Pianificazione di un backup del database

È possibile avvalersi dell'Utilità di pianificazione di Windows Server 2012/2012 R2, 2008 R2 per pianificare un'attività che eseguirà il backup del database di OpenScape Contact Center. Questa sezione fornisce linee guida relative alla pianificazione di un'attività. Per istruzioni dettagliate, vedere la documentazione Microsoft.

IMPORTANTE: Per i backup pianificati si utilizzano i file FULLBACKUP.BAT e INCREMENTALBACKUP.BAT, entrambi i quali eseguono il backup mediante l'utilità ontape di Informix. Quindi, prima dell'esecuzione del primo backup pianificato, è necessario modificare i parametri ontape come descritto nella fase 2 a pagina 49.

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), si consiglia di pianificare il backup di server principale, server di backup e server report centralizzati nello stesso momento, per garantire la coerenza dei dati.

Per pianificare un backup di database:

1. Mediante l'Utilità di pianificazione in Windows Server 2012/2012 R2, 2008 R2, pianificare un'attività in base alle seguenti linee guida:
 - Selezionare l'azione **Avvio programma**, quindi scegliere uno dei seguenti file batch, contenuti nella cartella dove è stato installato il software OpenScape Contact Center:
 - Per pianificare un backup completo, selezionare **FULLBACKUP.BAT**.
 - Per pianificare un backup incrementale, selezionare **INCREMENTALBACKUP.BAT**.
 - Specificare l'account utente e la password mediante i quali eseguire l'attività in base al tipo di sistema operativo:
 - Per Windows Server 2012/2012 R2, 2008 R2, specificare un account amministratore locale.
 - Per scrivere i risultati del backup su un file di testo, nelle proprietà dell'attività, aggiungere l'argomento <return.txt>results.txt. Assicurarsi che la cartella nella quale viene scritto il file results.txt (normalmente la cartella nella quale è stato installato il software OpenScape Contact Center) sia accessibile in lettura per tutti gli utenti (Everyone). In Windows Server 2012/ 2008 o Windows Server 2012 R2/ 2008 R2, quando si

Manutenzione del sistema

Backup del database

aggiunge l'argomento, è necessario specificare anche il percorso iniziale. Assicurarsi di non utilizzare le virgolette al momento di specificare il percorso.

6.3.2 Backup del database tramite l'utilità ontape

È possibile sottoporre a backup il database OpenScape Contact Center su un'unità nastro locale o su un'unità locale o di rete tramite l'utilità ontape di Informix.

6.3.2.1 Backup del database su un'unità nastro locale

Per sottoporre a backup il database di OpenScape Contact Center su un'unità nastro, è necessario ricorrere all'utilità ontape di Informix.

Per eseguire il backup del database su un'unità nastro locale:

1. Accedere al computer server in cui è installato Informix nel modo seguente:
 - Per Windows Server 2008 R2, accedere come amministratore.
2. Inserire un nastro vuoto nell'apposita unità del server.
3. Aprire un prompt dei comandi Informix utilizzando la scelta rapida **ol_nomeserver**, dove *nomeserver* è il nome del server OpenScape Contact Center.
4. Per avviare il backup, procedere in uno dei modi seguenti:
 - Per eseguire un backup completo del database Informix, al prompt dei comandi, immettere **ontape -s -L 0**, quindi premere **INVIO**.
 - Per eseguire un backup incrementale dell'intero database Informix, al prompt dei comandi immettere **ontape -s -L 1**, quindi premere **INVIO**.

NOTA: Il parametro **-s** istruisce l'utilità ontape a creare un backup e il parametro **-L** specifica il livello di archiviazione: **0** per completa o **1** per incrementale.

5. Se lo spazio disponibile sul nastro utilizzato non è sufficiente, il sistema richiede di inserire un altro nastro. Se richiesto, rimuovere il nastro e l'etichetta con la data, l'ora, il livello e il numero del nastro nella sequenza. Inserire un altro nastro, quindi premere **INVIO**. Ripetere la procedura per tutti i nastri necessari.

6.3.2.2 Backup del database su un'unità locale o di rete

Questa sezione descrive come sottoporre a backup il database di OpenScape Contact Center su un'unità locale o di rete, tramite l'utilità ontape di Informix.

Per eseguire il backup del database su un'unità locale o di rete:

1. Accedere al computer server in cui è installato Informix nel modo seguente:
 - Per Windows Server 2008 R2, accedere come amministratore.
2. Modificare i parametri ontape come segue:
 - Individuare il file **ONCONFIG.ol_nomeserver**, dove *nomeserver* è il nome del computer server OpenScape Contact Center in cui è installato Informix, quindi aprire il file in un editor di testo come Blocco note. Questo file di registro normalmente si trova nella cartella Program Files\Informix\etc.
 - Nel parametro TAPEDEV, specificare il percorso e il nome file del file di backup nell'unità locale o di rete nel formato 8.3 (breve), ad esempio C:\Backups\Backup.001. Prima di avviare il backup, è necessario assicurarsi che il file esista nella posizione specificata e che l'utente connesso sia dotato almeno dell'autorizzazione Modifica per il file di backup. Se il file di backup non esiste, è possibile creare un file vuoto utilizzando un editor di testo come Blocco note.
 - Nel parametro TAPESIZE, specificare 0, in modo che il file di backup non presenti un limite di dimensioni massimo.
3. Aprire un prompt dei comandi Informix utilizzando la scelta rapida **ol_nomeserver**, dove *nomeserver* è il nome del server OpenScape Contact Center.
4. Per avviare il backup, procedere in uno dei modi seguenti:
 - Per eseguire un backup completo del database Informix, al prompt dei comandi, immettere **ontape -s -L 0**, quindi premere **INVIO**.
 - Per eseguire un backup incrementale dell'intero database Informix, al prompt dei comandi immettere **ontape -s -L 1**, quindi premere **INVIO**.

NOTA: Il parametro **-s** istruisce l'utilità ontape a creare un backup e il parametro **-L** specifica il livello di archiviazione: **0** per completa o **1** per incrementale.

6.3.3 Ripristino del database tramite l'utilità ontape

Questa sezione descrive come ripristinare dati OpenScape Contact Center sottoposti a backup in precedenza tramite l'utilità ontape di Informix.

NOTA: Se è stato eseguito un backup incrementale, sono necessari sia il backup completo più recente, sia quello incrementale.

NOTA: Se si desidera ripristinare un backup L0 con un'installazione OSCC pulita, verificare che tutti i file di gruppi di record elencati dall'utilità "ontape" siano presenti nella cartella dati di Contact Center. Se non esistono, creare tali file senza estensione facendo clic con il pulsante destro del mouse, quindi accedere a New -> Text Document (**Nuovo -> Documento di testo**) e rinominarli eliminando l'estensione. L'importazione non funzionerà correttamente se i file di gruppi di record non sono presenti.

Per ripristinare il database tramite l'utilità ontape:

1. Accedere al computer server in cui è installato Informix nel modo seguente:
 - Per Windows Server 2008 R2, accedere come amministratore.
2. Arrestare i servizi seguenti:
 - **OpenScape Contact Center**
 - **Informix IDS - ol_nomeserver**, dove *nomeserver* è il nome del server OpenScape Contact Center
3. Procedere in uno dei modi seguenti:
 - Se si stanno ripristinando dati da un nastro, inserire il primo nastro dell'archivio completo da ripristinare nell'unità nastro del server.
 - Se si sta eseguendo il ripristino dei dati da un file di backup su un'unità locale o di rete, assicurarsi che il percorso e il nome file di backup siano configurati correttamente nel file *nomeserver*.
4. Aprire un prompt dei comandi Informix utilizzando la scelta rapida **ol_nomeserver**, dove *nomeserver* è il nome del server OpenScape Contact Center.
5. Nella riga di comando, immettere **ontape -r**, quindi premere **INVIO**.
6. Quando viene richiesto di caricare un nastro, premere **INVIO**.
7. Quando viene richiesto, **Continue restore (Y/N)?**, premere **Y**.
8. Quando viene richiesto se si desidera eseguire il backup dei registri, premere **N**.

9. Se è stato creato un archivio incrementale, quando viene richiesto se **si desidera ripristinare un archivio di livello 1**, premere **Y**. Se non è stato creato un archivio incrementale, premere **N**.
10. Quando viene richiesto se si desidera ripristinare i nastri dei registri, premere **N**.
11. Al termine del processo di ripristino, se sono stati ripristinati i dati da un'unità nastro locale, rimuovere l'ultimo nastro dall'unità nastro.
12. Nella riga di comando, immettere `onmode -m`, quindi premere **INVIO**. Questo comando riporta Informix alla modalità normale e la sua esecuzione può richiedere vari minuti.
13. Nella riga di comando, immettere `onstat -r`, quindi premere **INVIO**. Vengono visualizzate informazioni sull'ambiente del server Informix. La prima riga indica la modalità dell'applicazione Informix e dovrebbe mostrare **On-Line**. Per arrestare l'esecuzione di `onstat`, premere **CTRL+C**.
14. Per chiudere la finestra del prompt dei comandi, digitare `exit`, quindi premere **INVIO**.
15. Chiudere tutte le altre finestre e applicazioni aperte.
16. Riavviare il servizio **OpenScape Contact Center**.

6.3.4 Ripristino di un backup di livello zero effettuato con l'utilità su nastro

Questa sezione descrive come ripristinare un backup di livello zero dei dati di OpenScape Contact Center utilizzando un processo automatizzato.

1. Per utilizzare lo script di ripristino di livello zero, copiare i file `FullRestore.bat`, `fullrestore.in` e `replace.vbs` sul server. I file sono inclusi nel DVD.
2. Aprire un prompt dei comandi come utente Informix
3. Eseguire `FullRestore.bat` specificando gli argomenti `/tapedev <percorso> / tapesize<dimensioni>`, dove `<percorso>` è il percorso del backup Informix di livello zero; indicare `<dimensioni>` come zero se si utilizza un dispositivo a nastro esterno.

6.3.5 Backup del database tramite l'utilità onbar

Questa sezione descrive come sottoporre a backup il database OpenScape Contact Center su un'unità locale tramite l'utilità onbar di Informix. L'utilità onbar di Informix è in grado di interfacciarsi direttamente con Informix Storage Manager (ISM) o un'altra applicazione di memorizzazione di terze parti, quale Veritas, in modo da fornire una soluzione di backup flessibile.

NOTA: Prima di eseguire l'utilità onbar, è necessario configurare l'applicazione Storage Manager. Per istruzioni dettagliate, consultare il documento *IBM Informix Storage Manager Administrator's Guide* nella documentazione corrispondente. La documentazione Informix viene fornita all'indirizzo:
<http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

Per eseguire il backup del database su un'unità locale:

1. Accedere al computer server in cui è installato Informix nel modo seguente:
 - Per Windows Server 2008 R2, accedere come amministratore.
2. Aprire un prompt dei comandi Informix utilizzando la scelta rapida **ol_nomeserver**, dove *nomeserver* è il nome del server OpenScape Contact Center.
3. Per avviare il backup, procedere in uno dei modi seguenti:
 - Per eseguire un backup completo dell'intero database Informix, al prompt dei comandi immettere **onbar -b -L 0**, quindi premere **INVIO**.
 - Per eseguire un backup incrementale dell'intero database Informix, al prompt dei comandi immettere **onbar -b -L 1**, quindi premere **INVIO**.

NOTA: Il parametro **-b** istruisce l'utilità onbar a creare un backup e il parametro **-L** specifica il livello di archiviazione: **0** per completa o **1** per incrementale.

6.3.6 Ripristino del database tramite l'utilità onbar

Questa sezione descrive come ripristinare dati OpenScape Contact Center precedentemente sottoposti a backup tramite l'utilità onbar di Informix.

NOTA: Se è stato eseguito un backup incrementale, sono necessari sia il backup completo più recente, sia quello incrementale.

Per ripristinare il database tramite l'utilità onbar:

1. Accedere al computer server in cui è installato Informix nel modo seguente:
 - Per Windows Server 2008 R2, accedere come amministratore.
2. Aprire un prompt dei comandi Informix utilizzando la scelta rapida **ol_nomeserver**, dove *nameserver* è il nome del server OpenScape Contact Center.
3. Nella riga di comando, immettere **onbar -r**, quindi premere **INVIO**.

6.4 Supporto SNMP

Il sistema supporta due metodi di creazione delle informazioni visualizzabili da un sistema di gestione SNMP:

- **OpenScape Contact Center SNMP Extension Agent** – Espone informazioni OpenScape Contact Center specifiche pertinenti allo stato degli oggetti OpenScape Contact Center gestiti. Questo metodo è supportato solo dal server principale.
- **Software OpenScape CAP Fault Management** – Agisce come SNMP Extension Agent per generare messaggi trap SNMP per conto del software OpenScape Contact Center tramite il registro eventi di Windows. Questo metodo è supportato dal server principale e dal server report centralizzati (opzionale).

Il servizio SNMP Windows deve essere installato e in esecuzione sul server per supportare questi metodi.

Il servizio SNMP Windows deve inoltre essere installato e in esecuzione sul server principale e sul server report centralizzati per supportare questi metodi.

NOTA: Occorre configurare il servizio SNMP Windows in modo che l'elenco dei nomi delle community non contenga “pubblico” o “privato” e che l'elenco degli host contenga solo quelli che devono accedere alle informazioni.

6.4.1 OpenScape Contact Center SNMP Extension Agent

OpenScape Contact Center SNMP Extension Agent (osccsnmp.dll) supporta le richieste SNMP standard per gli ID oggetto (OID). SNMP Extension Agent espone informazioni OpenScape Contact Center specifiche riguardo lo stato degli oggetti OpenScape Contact Center gestiti. Le informazioni possono quindi essere richieste da qualsiasi sistema di gestione SNMP.

NOTA: È responsabilità dell'utente del sistema di gestione SNMP garantire che le informazioni possano essere richieste e recuperate dall'OpenScape Contact Center SNMP Extension Agent.

Le informazioni specifiche di OpenScape Contact Center che vengono esposte dall'OpenScape Contact Center SNMP Extension Agent sono definite nel file sen-oscc-mib.mib, che associa gli oggetti gestiti agli OID corrispondenti. Le informazioni esposte includono l'utilizzo dell'estensione Call Director, il numero di utenti registrati e il numero dei contatti attuali e recenti. Per ulteriori dettagli su tutte le informazioni disponibili, fare riferimento al file sen-oscc-mib.mib, che può essere visualizzato mediante un editor di testo.

Le informazioni specifiche OpenScape Contact Center possono essere utilizzate per monitorare lo stato del sistema. Ad esempio, un tecnico nel centro operativo di rete può creare una vista che genera un allarme quando il numero di estensioni elaboratore vocale operative scende sotto una percentuale soglia configurata sul totale di estensioni elaboratore vocale configurate. Il tecnico può quindi segnalare l'evento al cliente in modo che questo abbia a disposizione il tempo necessario per risolvere il problema ed evitare l'esaurirsi di estensioni disponibili.

I file The osccsnmp.dll e sen-oscc-mib.mib si trovano nella cartella predefinita di installazione, sul server principale. Il file osccsnmp.dll viene inoltre utilizzato per supportare le licenze su abbonamento.

NOTA: Il file osccsnmp.dll viene registrato automaticamente sul server durante l'installazione del software server OpenScape Contact Center. Se il servizio SNMP di Windows viene disinstallato, il file osccsnmp.dll viene deregistrato. Per registrare di nuovo il file .dll, utilizzare il programma osccregistersnmpextension.exe, presente nella cartella di installazione predefinita sul server principale.

6.4.2 Software OpenScape CAP Fault Management

Il software OpenScape CAP Fault Management è un componente opzionale che può essere utilizzato per generare messaggi trap SNMP OpenScape Contact Center. Il software OpenScape CAP Fault Management può essere installato automaticamente durante il processo di installazione di OpenScape Contact Center o manualmente dalla cartella \OpenScape CAP\Fault Management sul DVD di OpenScape Contact Center.

NOTA: Per ulteriori informazioni su come configurare il software OpenScape CAP Fault Management, consultare la documentazione di OpenScape CAP Fault Management.

Esistono due file di configurazione per OpenScape CAP Fault Management:

- **capfm_procenter.ini** – Si tratta del file di configurazione predefinito, installato al momento dell'installazione del software del server OpenScape Contact Center. Attiva la generazione di messaggi trap SNMP per tutti i messaggi OpenScape Contact Center.
- **capfm_procenter_service.ini** – Si tratta del file di configurazione del servizio che deve essere utilizzato se si desidera creare messaggi trap SNMP solo per il sottogruppo di messaggi associati al centro operativo di rete.

Entrambi i file di configurazione si trovano nella cartella \Utilities\Install sul DVD di OpenScape Contact Center.

Manutenzione del sistema

Supporto SNMP

7 Gestione di un ambiente report centralizzati

Questo capitolo descrive le operazioni possibili se si riscontrano problemi quando il sistema è configurato per i report centralizzati.

7.1 Gestione della replica per Report centralizzato

In caso di problemi con la replica, è possibile utilizzare l'applicazione di configurazione della replica OpenScape Contact Center (trcdbins.exe) per gestire la replica dei dati.

NOTA: Se il sistema è configurato per l'alta disponibilità (warm standby), eseguire le procedure descritte in Sezione 8.1, "Gestione della replica per l'alta disponibilità (warm standby)", a pagina 71.

IMPORTANTE: L'orario del server report centralizzati deve essere sincronizzato con quello dei server OpenScape Contact Center che partecipano al report centralizzato. È necessario sincronizzare gli orari prima di eseguire l'applicazione di configurazione della replica OpenScape Contact Center (trcdbins.exe) e assicurarsi che rimangano sincronizzati. La replica non riesce se gli orari differiscono di oltre 2 secondi.

7.1.1 Il buffer di replica

Potenzialmente esistono due tipi di replica dei dati:

- **Replica per report centralizzato** – Replica dei dati dei report cronologici nel server report centralizzati quando il sistema è configurato per la funzione Report centralizzato.
- **Replica per alta disponibilità (warm standby)** – Replica dei dati di amministrazione ed elaborazione fra il server principale e quello di backup, se il sistema è configurato per l'alta disponibilità (warm standby).

Se la replica si interrompe (ad esempio se si verifica un problema di rete), i dati vengono memorizzati nel buffer di replica. Le dimensioni del buffer di replica sono adeguate per contenere circa due giorni di dati di replica dei report centralizzati e dell'alta disponibilità (warm standby) per un sistema medio.

Gestione di un ambiente report centralizzati

Gestione della replica per Report centralizzato

In base alla capacità del buffer, il sistema effettua le operazioni seguenti:

- **50% del buffer pieno** – Viene generato un messaggio di errore ogni ora per indicare la percentuale di spazio utilizzato nel buffer di replica.
- **75% del buffer pieno** – Viene generato un messaggio di errore ogni 15 minuti. Se il sistema è configurato sia per il report centralizzato che per l'alta disponibilità (warm standby), e solo un tipo di replica determina il riempimento del buffer, tale replica viene interrotta.
- **95% del buffer pieno** – Viene generato un messaggio di avviso ogni 15 minuti e la replica configurata sul server si interrompe.

IMPORTANTE: Se il sistema arresta la replica automaticamente, è necessario attenersi alle procedure appropriate per chiudere e riavviare manualmente la replica, dopo aver risolto il problema. La replica non si riavvia automaticamente. Per ulteriori informazioni, consultare Sezione 7.1.3, "Chiusura di tutte le repliche per report centralizzato", a pagina 61 o Sezione 8.1.5, "Chiusura di tutte le repliche", a pagina 81.

Si consiglia di utilizzare l'applicazione System Monitor al fine di monitorare la capacità del buffer di replica e, se necessario, sospendere la replica causa del problema. Per ulteriori informazioni, vedere Sezione 7.1.2, "Sospensione della replica per report centralizzato", a pagina 58, o Sezione 8.1.1, "Sospensione della replica per l'alta disponibilità (warm standby)", a pagina 71.

NOTA: Il buffer di replica continua a riempirsi anche quando la replica è sospesa.

7.1.2 Sospensione della replica per report centralizzato

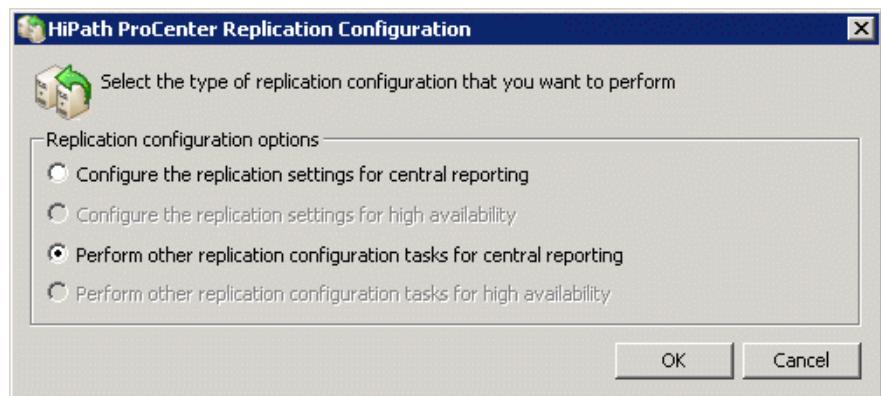
È possibile sospendere il flusso dei dati replicati sul server report centralizzati, ad esempio per eseguire la manutenzione della rete o del server stesso. Si consiglia di sospendere la replica se si prevede che il flusso dei dati replicati verrà interrotto per più di mezza giornata.

Sospendere la replica del server report centralizzati è utile per un paio di ragioni:

- Se una grande quantità di dati si accumula nel buffer durante un'interruzione, alla riattivazione della replica vengono consumate significative risorse di rete e CPU nel computer di destinazione. Se si sospende la replica è possibile riattivarla durante i periodi con un basso volume di contatti, riducendo l'impatto sul sistema.
- Dopo un'interruzione, i dati vengono sincronizzati automaticamente. La sincronizzazione comprende due fasi, una relativa ai dati interni Informix e l'altra ai dati dei report di OpenScape Contact Center. La sospensione della replica dei dati dei report consente di sincronizzare prima i dati interni Informix, in modo che il sistema possa essere riattivato più gradualmente.

Per sospendere la replica report centralizzato:

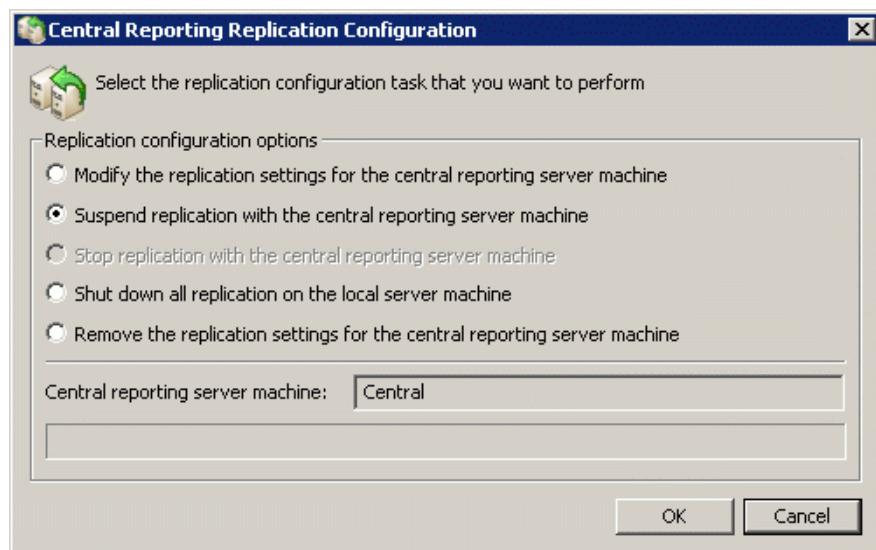
1. Eseguire il logon sul server dove si desidera sospendere la replica.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.



Gestione di un ambiente report centralizzati

Gestione della replica per Report centralizzato

4. Selezionare **Suspend replication with the central reporting server machine**, quindi fare clic su **OK**.



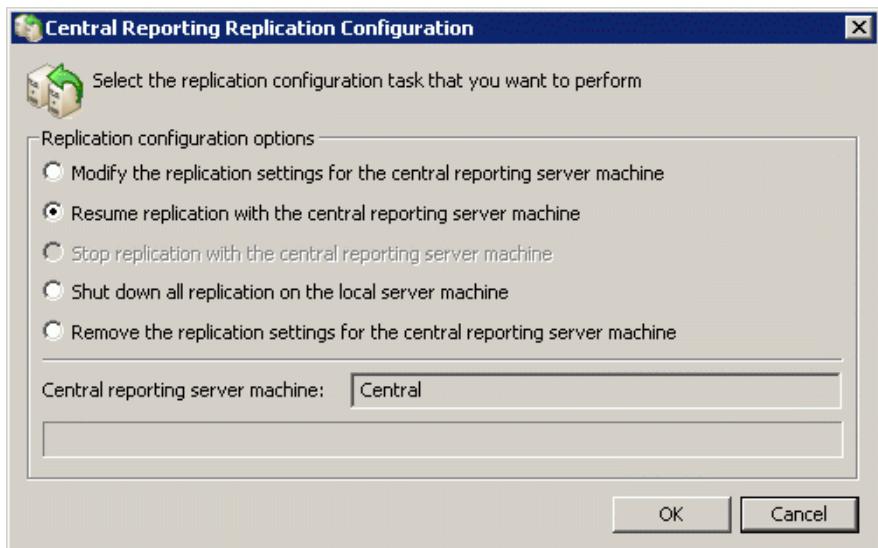
7.1.2.1 Riattivazione della replica report centralizzato

Se il buffer di replica contiene una grande quantità di dati, si consiglia di riattivare la replica durante un periodo con un basso volume di contatti, in modo da ridurre l'impatto sul sistema.

Per riattivare la replica del server report centralizzati:

1. Eseguire il logon sul server dove si era sospesa la replica.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.

4. Selezionare **Resume replication with the central reporting server machine**, quindi fare clic su **OK**.



7.1.3 Chiusura di tutte le repliche per report centralizzato

È possibile terminare la replica del server report centralizzati, ad esempio se si verifica un problema di rete ed è necessario rimuovere le impostazioni di replica (il che richiede accesso alla rete).

IMPORTANTE: Si consiglia di effettuare tale procedura solo se necessario o indicato, dato che potrebbe richiedere di sincronizzare i dati nei report. Per ulteriori informazioni, vedere Sezione 7.2, "Sincronizzazione dei dati per report centralizzato", a pagina 63. Se possibile, si consiglia di sospendere anziché terminare la replica, poiché la sospensione non richiede di sincronizzare i dati nei report.

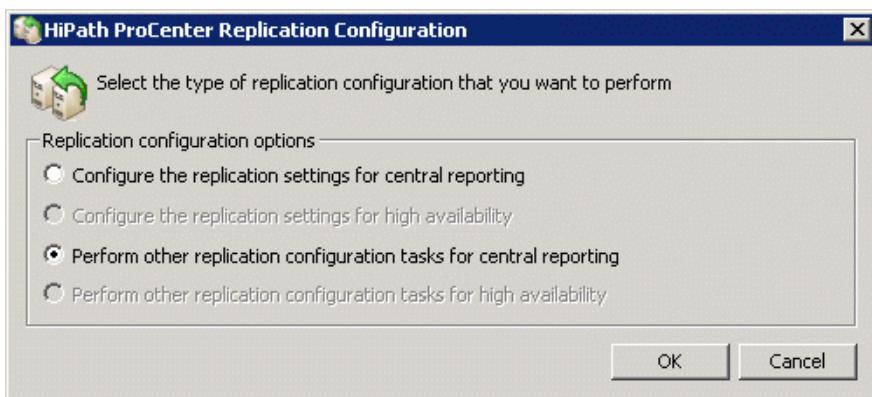
Per terminare la replica report centralizzato:

1. Eseguire il logon sul server dove si desidera terminare la replica.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.

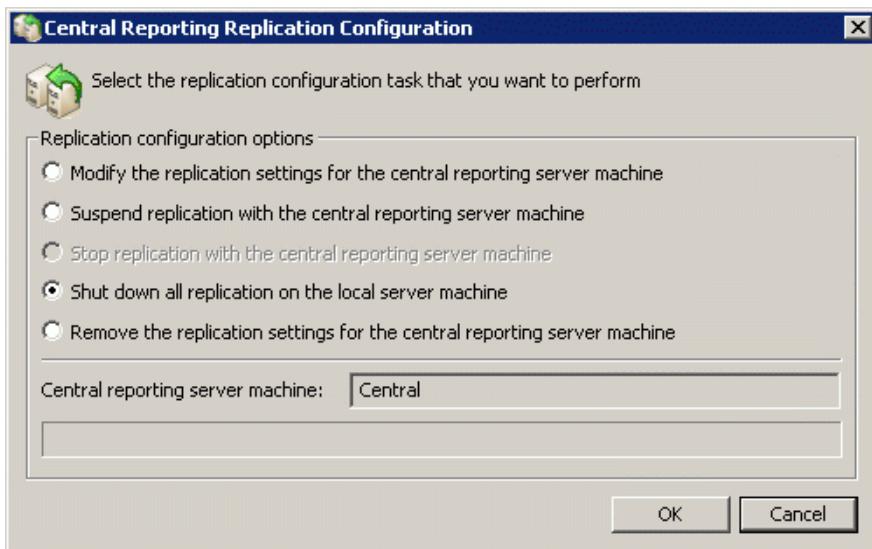
Gestione di un ambiente report centralizzati

Gestione della replica per Report centralizzato

3. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.



4. Selezionare **Shut down all replication on the local server machine**, quindi fare clic su **OK**.



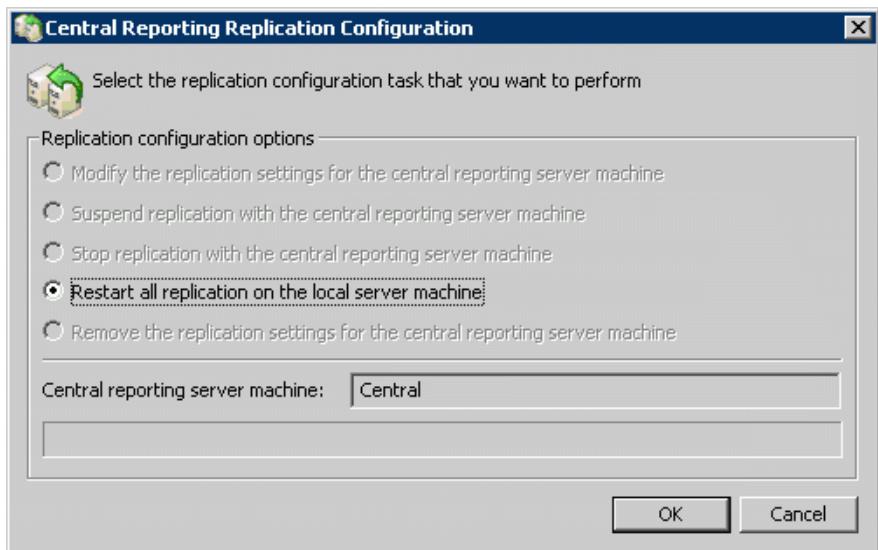
7.1.3.1 Riavvio della replica report centralizzato

La replica del server report centralizzati, una volta terminata, può essere riavviata come descritto in questa procedura. Durante il processo di riavvio vengono cancellati tutti i dati del buffer di replica.

Per riavviare la replica report centralizzato:

1. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** su tutti i server che condividono Report centralizzato. Attendere la chiusura completa dei servizi prima di procedere.
2. Eseguire il logon sul server dove si era terminata la replica.
3. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.

4. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.
5. Selezionare **Restart all replication on the local server machine**, quindi fare clic su **OK**.



6. Sincronizzare i dati nei report solo se veramente necessario. Sezione 7.2, "Sincronizzazione dei dati per report centralizzato", a pagina 63.

7.2 Sincronizzazione dei dati per report centralizzato

Se si riscontrano problemi con i dati dei report cronologici, è possibile sincronizzare i dati dei report. Ad esempio, se mancano dei dati a causa di una prolungata interruzione della rete fra uno dei server OpenScape Contact Center che partecipano al report centralizzato e il server report centralizzato, è possibile sincronizzare i dati nei report tra il server e il server report centralizzati.

NOTA: La sincronizzazione dei dati nei report può richiedere molto tempo. Si consiglia di eseguire la procedura solo se i problemi ai dati nei report cronologici sono veramente inaccettabili per le proprie esigenze.

NOTA: Prima di eseguire la sincronizzazione, si consiglia di controllare i periodi di mantenimento sul server report centralizzati per assicurarsi che non siano più brevi di quelli configurati sul server principale. In caso di periodi di mantenimento più brevi, è possibile perdere alcuni dati dei report sincronizzati durante l'ora successiva di manutenzione dati.

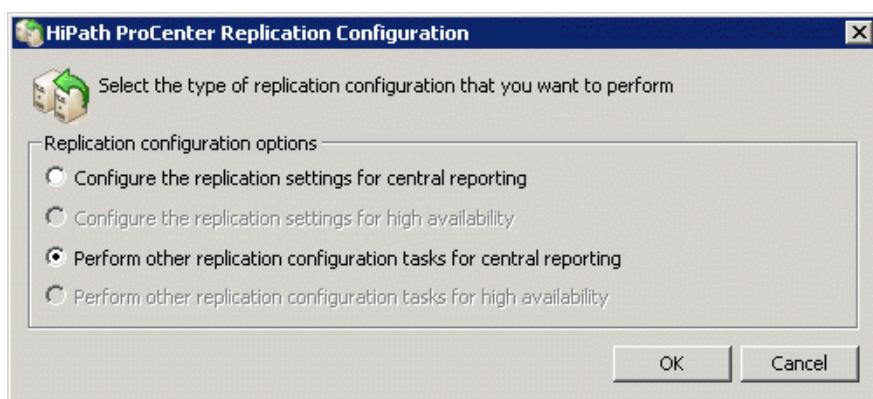
Gestione di un ambiente report centralizzati

Sincronizzazione dei dati per report centralizzato

Se il sistema è configurato per l'alta disponibilità (warm standby), vedere Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86.

Per sincronizzare i dati nei report:

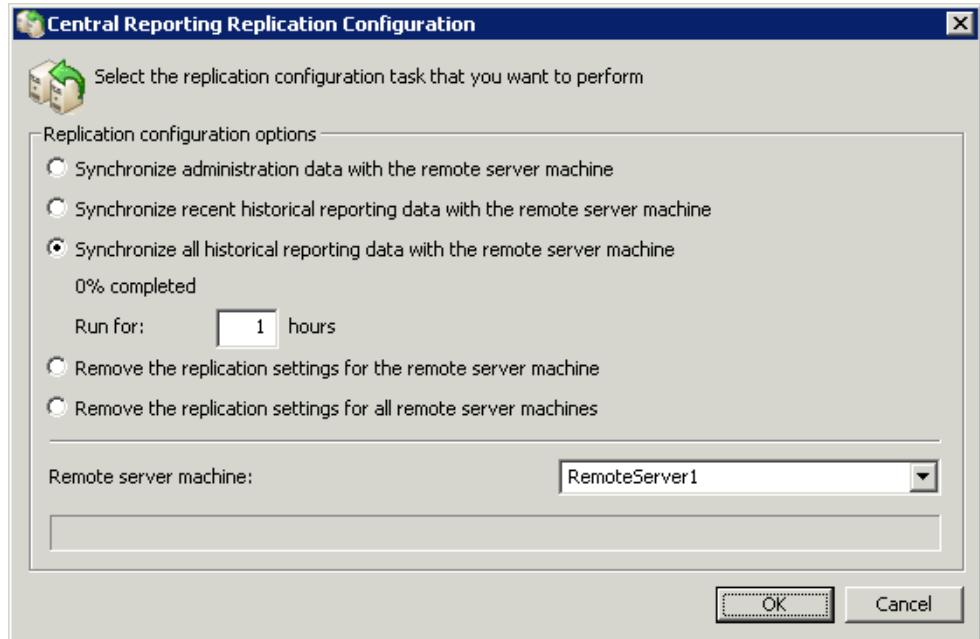
1. Eseguire il logon sul server report centralizzati.
2. Arrestare il servizio **OpenScape Contact Center AutoPA** sul server report centralizzati. Attendere la chiusura completa del servizio prima di procedere.
3. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
4. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.



5. Selezionare una delle seguenti opzioni di installazione, quindi fare clic su **OK**:
 - Per sincronizzare i dati dei report cronologici solo per il mese corrente e quello precedente (questa opzione richiede meno tempo), procedere come segue:
 - Selezionare **Synchronize recent historical reporting data with the remote server machine**.
 - Nell'elenco **Remote server**, selezionare il server con cui ci si desidera sincronizzare.
 - Per sincronizzare tutti i dati dei report cronologici, procedere come segue:
 - Selezionare **Synchronize all historical reporting data with the remote server machine**.
 - Nell'elenco **Remote server**, selezionare il server con cui ci si desidera sincronizzare.
 - Poiché questa opzione richiede molto tempo per essere completata, è possibile specificare la durata della sincronizzazione. Nella casella **Run for** digitare numero di ore che si desidera duri la sincronizzazione. Al termine di questo periodo di tempo, la

sincronizzazione si arresta ed è possibile continuare in un secondo momento. Il valore completo in % mostra in che misura il processo di sincronizzazione è attualmente completo. La barra di avanzamento mostra l'avanzamento nel numero di ore specificato.

- Per riprendere una sincronizzazione precedente, selezionare **Continue to synchronize all historical reporting data with the remote computer server**, quindi specificare il server remoto e la durata della sincronizzazione, come descritto sopra.



6. Quando la sincronizzazione è terminata, avviare il servizio **OpenScape Contact Center AutoPA** nel server report centralizzati.

7.3 Risoluzione dei problemi della configurazione di replica per report centralizzato

L'applicazione di configurazione della replica OpenScape Contact Center (trcdbins.exe) effettua diversi test per assicurarsi che la replica sia stata configurata correttamente. Se si presentano problemi con la configurazione di replica, verificare i file di diagnostica (denominati trcdbins.000, trcdbins.001... trcdbins.025), che si trovano nella cartella da cui è stato eseguito il componente. Questi file di diagnostica possono aiutare a risolvere i problemi più comuni della configurazione di replica.

Se i file di diagnostica non aiutano a risolvere i problemi della configurazione di replica, è possibile eseguire la procedura di risoluzione dei problemi descritta in questa sezione.

Gestione di un ambiente report centralizzati

Risoluzione dei problemi della configurazione di replica per report centralizzato

Questa procedura può essere utilizzata anche per risolvere i problemi di configurazione della replica dei report centralizzati quando il sistema è configurato per l'alta disponibilità (warm standby).

NOTA: Questa sezione è stata redatta presupponendo che l'utente abbia familiarità con l'utilizzo di Informix. Per istruzioni dettagliate, vedere la documentazione Informix all'indirizzo seguente:
<http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp>

Per risolvere un problema della configurazione di replica:

1. Per controllare la configurazione dell'ambiente, sul server report centralizzati e su ciascun server che partecipa al report centralizzato, procedere come segue:
 - a) Nel menu **Start**, scegliere **Programmi**, quindi fare clic su **Pannello di controllo**.
 - b) Fare doppio clic su **Sistema**.
 - c) Fare clic sulla scheda **Avanzate**.
 - d) Fare clic su **Variabili del sistema**.
 - e) In **Variabili del sistema**, assicurarsi che le variabili di ambiente del sistema INFORMIXDIR, INFORMIXSERVER e ONCONFIG siano incluse nell'elenco.
 - f) Se qualche variabile di ambiente del sistema non viene visualizzata nell'elenco, aggiungerla.
2. Utilizzare il comando `ping` per assicurarsi che la connessione di rete tra il server report centralizzati e ciascun report che partecipa al report centralizzato funzioni correttamente. Se qualche connessione di rete non funziona, contattare l'amministratore di rete.
3. Utilizzare il comando `tracert` per controllare la risoluzione dell'indirizzo IP al nome host per il server report centralizzati e ciascun server che partecipa al report centralizzato. Se qualche indirizzo IP non viene risolto correttamente al nome host, contattare l'amministratore di rete.
4. Sul server report centralizzati e su ciascun server che partecipa al report centralizzato, assicurarsi che il file `hosts.equiv` si trovi nella cartella `windows\system32\drivers\etc`. Se il file `hosts.equiv` non viene visualizzato nella cartella, assicurarsi di disporre delle autorizzazioni di accesso in scrittura alla cartella.

5. Sul server report centralizzati e su ciascun server che partecipa al report centralizzato, assicurarsi che il file hosts.equiv contenga le righe seguenti:

```
<local_host>
<fully_qualified_local_host_name>
<remote_host>
<fully_qualified_remote_host_name>
```

dove:

- I nomi host validi completi specificano il dominio, ad esempio, perfect.com.
- Sul server report centralizzati, gli host remoti sono i server che partecipano al report centralizzato.
- Su un server che partecipa al report centralizzato, l'host remoto è il server report centralizzati.

6. Sul server report centralizzati e su ciascun server che partecipa al report centralizzato, connettersi ai server del database per assicurarsi che l'ambiente sia attendibile per l'utente **Informix**, come segue:

- a) Connettersi al server tramite l'account **Informix**.
- b) Nel menu **Start**, scegliere **Esegui**, quindi digitare **dbaccess** e premere **OK**.
- c) Selezionare **Connessione**.
- d) Selezionare **Connett**.
- e) Specificare il database del server al quale connettersi.
- f) Quando viene richiesto di specificare un nome utente, premere **INVIO**.
- g) Sul server deve essere visualizzato l'elenco dei database. Se si verifica un errore, contattare l'amministratore di rete. Le possibili cause di errore sono: problemi di ricerca DNS (tabella di ricerca DNS in avanti e indietro sul controller di dominio) oppure il sistema è configurato per l'alta disponibilità (warm standby), ordine di binding TCP/IP non valido per le schede di interfaccia di rete. Per l'alta disponibilità (warm standby) è necessario che la scheda di interfaccia di rete del cliente si trovi all'inizio dell'elenco dei binding TCP/IP, seguita dalla scheda di interfaccia di rete privata del cluster, quindi dalla scheda di interfaccia di rete del PABX (se richiesta).

Gestione di un ambiente report centralizzati

Sostituzione di un server principale per i report centralizzati

7.4 Sostituzione di un server principale per i report centralizzati

Se un server principale che partecipa a Report centralizzato deve essere sostituito, procedere come segue.

IMPORTANTE: Un server principale deve essere sostituito solo sotto la supervisione del rappresentante dell'assistenza. La procedura non è valida per un server report centralizzati. Se occorre sostituire il server report centralizzati, è necessario rivolgersi al rappresentante dell'assistenza.

NOTA: Questa procedura richiede di sottoporre a backup tutti i dati sul server. Assicurarsi che il backup contenga i file del database, registro e hosts.equiv. Se non si effettua un backup di tutti i dati presenti sul server, sarà necessario riconfigurare le impostazioni di replica al termine di questa procedura. Per ulteriori informazioni, vedere Sezione 7.4.1, "Riconfigurazione delle impostazioni di replica", a pagina 68.

Prima di iniziare, è necessario richiedere un nuovo file della licenza per il nuovo server. L'ID sistema utilizzato per la licenza di OpenScape Contact Center si basa sull'hardware del server.

Per sostituire un server principale per Report centralizzato:

1. Ripristinare tutti i dati sul nuovo server utilizzando il backup più recente.
2. Assicurarsi che il livello patch del software del server OpenScape Contact Center corrisponda a quello del database da ripristinare.
3. Ripristinare il database sul server. Per ulteriori informazioni, attenersi alla procedura fornita in Sezione 6.3.3, "Ripristino del database tramite l'utilità ontape", a pagina 50 o in Sezione 6.3.6, "Ripristino del database tramite l'utilità onbar", a pagina 52, come appropriato.
4. Utilizzando l'applicazione Manager, attivare la licenza del nuovo server. Per ulteriori informazioni, consultare la *Guida di Manager*.

7.4.1 Riconfigurazione delle impostazioni di replica

Se non si dispone di un backup di tutti i dati del server principale da sostituire, è necessario riconfigurare le impostazioni di replica dopo aver sostituito il server.

Per riconfigurare le impostazioni di replica:

1. Rimuovere le impostazioni di replica per Report centralizzato:
 - Su tutti i server che partecipano a Report centralizzato (escluso il server sostituito), rimuovere le impostazioni di replica.
 - Sul server report centralizzati, rimuovere le impostazioni di replica per tutti i server remoti.
2. Configurare le impostazioni di replica.

NOTA: Per ulteriori informazioni sulla rimozione e la configurazione delle impostazioni di replica, vedere il *Manuale di Installazione*.

Gestione di un ambiente report centralizzati

Sostituzione di un server principale per i report centralizzati

8 Gestione di un ambiente di alta disponibilità (warm standby)

Questo capitolo descrive le operazioni possibili se si riscontrano problemi quando il sistema è configurato per l'alta disponibilità (warm standby).

NOTA: Nel presente capitolo viene utilizzata l'espressione generale "applicazione per i cluster Microsoft". Se si utilizza Windows Server 2008 R2, Windows 2012 e Windows 2012 R2, l'espressione si riferisce all'applicazione Gestione cluster di failover. Per ulteriori informazioni sulle procedure correlate a queste applicazioni, vedere la Guida di Microsoft.

8.1 Gestione della replica per l'alta disponibilità (warm standby)

Se si verificano problemi con la replica, il buffer di replica inizia a riempirsi. Per ulteriori informazioni, vedere Sezione 7.1.1, "Il buffer di replica", a pagina 57. In queste situazioni utilizzare l'applicazione di configurazione della replica OpenScape Contact Center (trcdbins.exe) per gestire la replica dei dati.

IMPORTANTE: Gli orari dei server principale, di backup e report centralizzati opzionale devono essere sincronizzati. È necessario sincronizzare gli orari prima di eseguire l'applicazione di configurazione della replica OpenScape Contact Center (trcdbins.exe) e assicurarsi che rimangano sincronizzati. La replica non riesce se gli orari differiscono di oltre 2 secondi.

8.1.1 Sospensione della replica per l'alta disponibilità (warm standby)

È possibile sospendere il flusso dei dati replicati fra il server principale e quello di backup, ad esempio per eseguire la manutenzione della rete. Si consiglia di sospendere la replica se si prevede che il flusso dei dati replicati verrà interrotto per più di mezza giornata. Non ha importanza quale server si utilizzi per sospendere la replica.

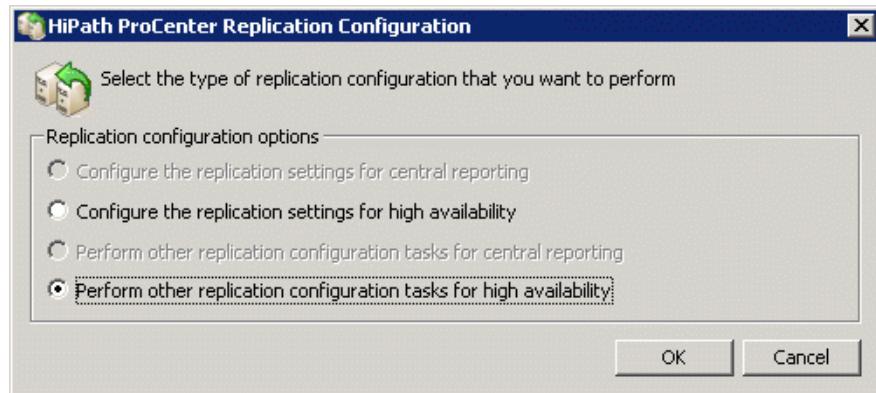
Questa funzione è utile poiché, se una grande quantità di dati si accumula nel buffer durante un'interruzione, alla riattivazione della replica vengono consumate significative risorse di rete e CPU nel computer di destinazione. Se si sospende la replica è possibile riattivarla durante i periodi con un basso volume di contatti, riducendo l'impatto sul sistema.

Gestione di un ambiente di alta disponibilità (warm standby)

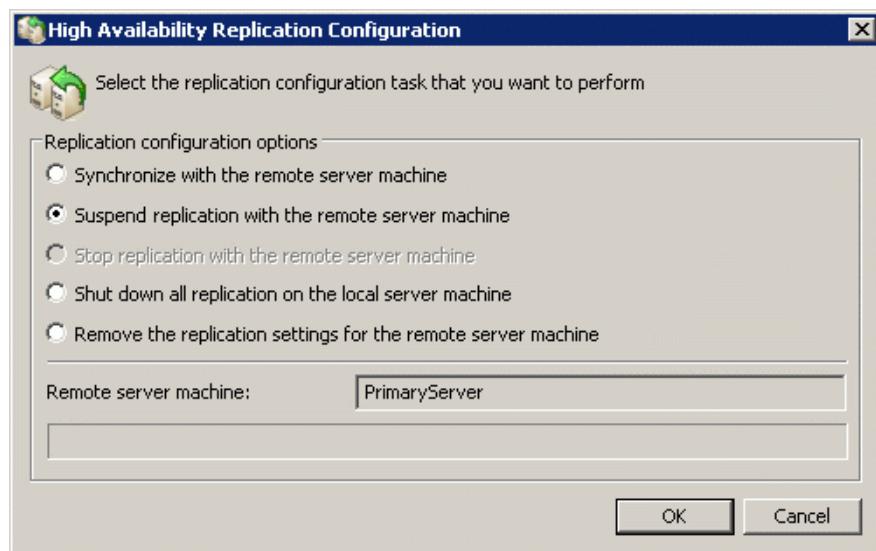
Gestione della replica per l'alta disponibilità (warm standby)

Per sospendere la replica per l'alta disponibilità (warm standby):

1. Eseguire il logon sul server principale o di backup.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.



4. Selezionare **Suspend replication with the remote server machine**, quindi fare clic su **OK**.



8.1.1.1 Riattivazione della replica per l'alta disponibilità (warm standby)

Se il buffer di replica contiene una grande quantità di dati, si consiglia di riattivare la replica durante un periodo con un basso volume di contatti, in modo da ridurre l'impatto sul sistema.

Per riattivare la replica per l'alta disponibilità (warm standby):

1. Eseguire il logon sul server dove si era sospesa la replica.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.
4. Selezionare **Resume replication with the remote server machine**, quindi fare clic su **OK**.



8.1.2 Sospensione della replica report centralizzato

Sospendere la replica del server report centralizzati è utile per le ragioni descritte in Sezione 7.1.2, "Sospensione della replica per report centralizzato", a pagina 58. Attenersi alla procedura descritta in tale sezione per sospendere la replica del server report centralizzati.

NOTA: Se si verifica un failover del sistema quando la replica report centralizzato è sospesa, quest'ultima viene riavviata automaticamente.

8.1.2.1 Riattivazione della replica report centralizzato

Attenersi alla procedura descritta in Sezione 7.1.2.1, "Riattivazione della replica report centralizzato", a pagina 60 per riattivare la replica del server report centralizzati.

Gestione di un ambiente di alta disponibilità (warm standby)

Gestione della replica per l'alta disponibilità (warm standby)

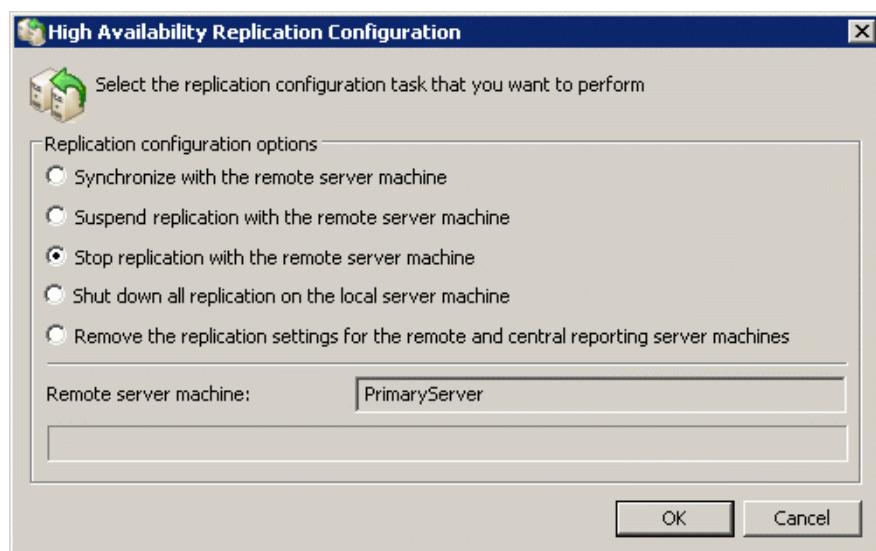
8.1.3 Arresto della replica per l'alta disponibilità (warm standby)

Se il sistema è configurato sia per l'alta disponibilità (warm standby) che per il report centralizzato, è possibile arrestare la replica fra il server principale e quello di backup. Ciò consente di lasciare la replica report centralizzato in esecuzione mentre si risolvono i problemi della rete. Non ha importanza quale server si utilizzi per arrestare la replica.

IMPORTANTE: Si consiglia di effettuare tale procedura solo se necessario o indicato, dato che potrebbe richiedere di sincronizzare i dati nei report. Per ulteriori informazioni, vedere Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86. Se possibile, si consiglia di sospendere anziché arrestare la replica, poiché la sospensione non richiede di sincronizzare i dati nei report.

Per arrestare la replica per l'alta disponibilità (warm standby):

1. Eseguire il logon sul server principale o di backup.
2. Nel menu **Start**, fare clic su **Eseguì**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.
4. Selezionare **Stop replication with the remote server machine**, quindi fare clic su **OK**.

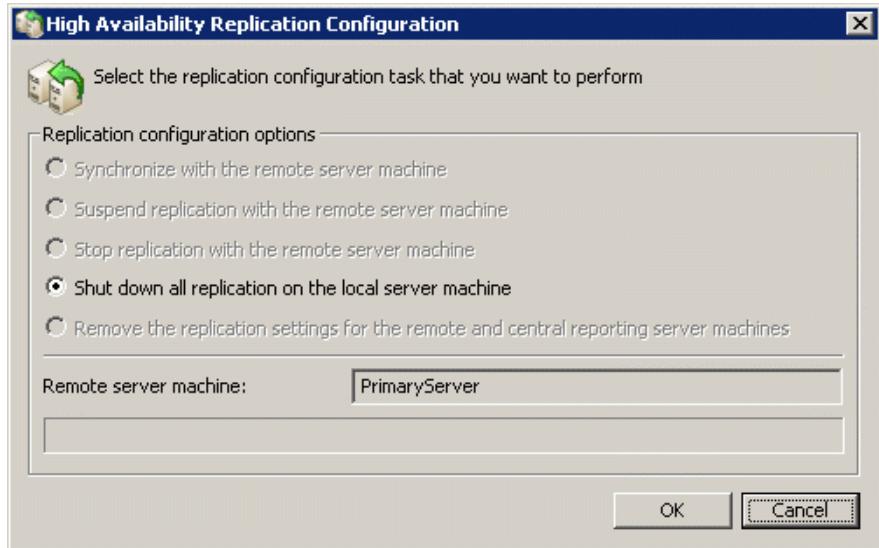


8.1.3.1 Riavvio della replica per l'alta disponibilità (warm standby)

Dopo l'arresto, è prima necessario terminare tutte le replicate, quindi riavviare la replica. Durante il processo di riavvio vengono cancellati tutti i dati del buffer di replica.

Per riavviare la replica per alta disponibilità (warm standby):

1. Utilizzare l'applicazione per i cluster Microsoft per scollegare il **HPPC Group** (Gruppo HPPC). Prima di procedere, attendere che lo stato del server diventi Warm Standby.
2. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** sia sul server principale che su quello di backup. Attendere la chiusura completa dei servizi prima di procedere.
3. Eseguire il logon sul server dove si era interrotta la replica.
4. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
5. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.
6. Selezionare **Shut down all replication on the local server machine**, quindi fare clic su **OK**.

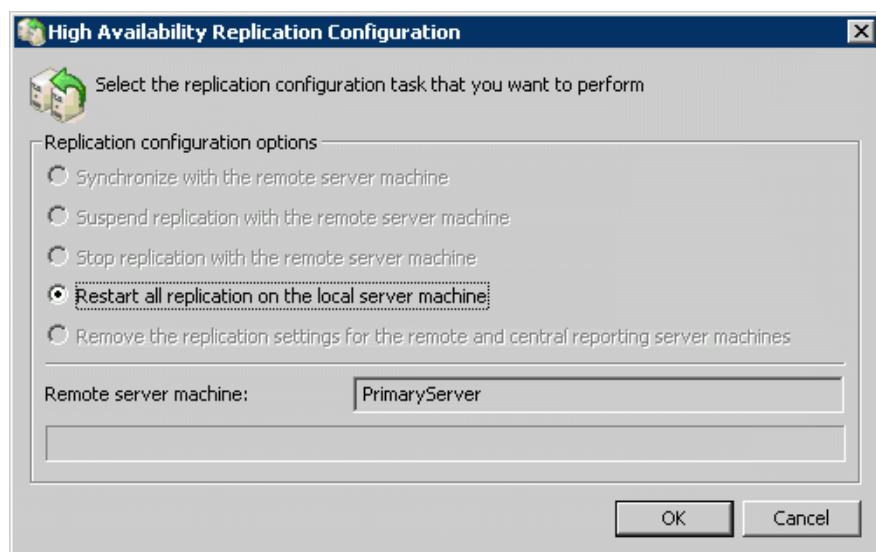


7. Sullo stesso server, eseguire nuovamente **trcdbins.exe**. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins** quindi fare clic su **OK**.
8. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.

Gestione di un ambiente di alta disponibilità (warm standby)

Gestione della replica per l'alta disponibilità (warm standby)

9. Selezionare **Restart all replication on the local server machine**, quindi fare clic su **OK**.



10. Sincronizzare i dati nei report solo se veramente necessario. Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86.
11. Sincronizzare i dati di amministrazione fra i server principale e di backup. Per ulteriori informazioni, vedere Sezione 8.2, "Sincronizzazione dei dati fra il server principale e quello di backup", a pagina 83.
12. Se si stabilisce di non sincronizzare i dati nei report nella fase 10, sincronizzare i dati di amministrazione fra il server principale e il server report centralizzati. Per dettagli Sezione 8.3, "Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati", a pagina 85.

8.1.4 Arresto della replica report centralizzato

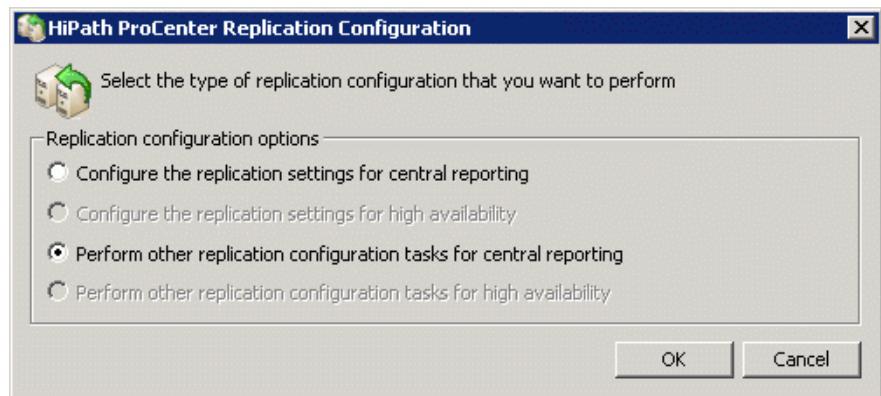
Quando il sistema è configurato sia per l'alta disponibilità (warm standby) che per il report centralizzato, è possibile arrestare la replica del server report centralizzati. Ciò consente di lasciare la replica per l'alta disponibilità (warm standby) in esecuzione mentre si risolvono i problemi della rete o del server report centralizzati.

IMPORTANTE: Si consiglia di effettuare tale procedura solo se necessario o indicato, dato che potrebbe richiedere di sincronizzare i dati nei report. Per ulteriori informazioni, vedere Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86. Se possibile, si consiglia di sospendere anziché arrestare la replica, poiché la sospensione non richiede di sincronizzare i dati nei report.

NOTA: Se si verifica un failover del sistema quando la replica report centralizzato è arrestata, quest'ultima viene riavviata automaticamente.

Per arrestare la replica report centralizzato:

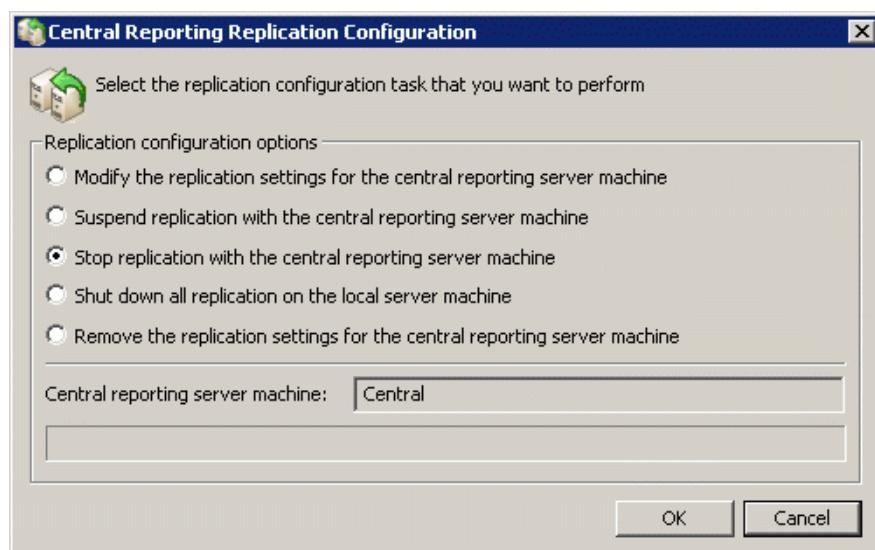
1. Eseguire il logon sul server dove si desidera arrestare la replica con il server report centralizzati.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.



Gestione di un ambiente di alta disponibilità (warm standby)

Gestione della replica per l'alta disponibilità (warm standby)

4. Selezionare **Stop replication with the central reporting server machine**, quindi fare clic su **OK**.



8.1.4.1 Riavvio della replica report centralizzato

In caso di arresto della replica, è prima necessario terminare tutte le repliche, quindi riavviare la replica. Durante il processo di riavvio vengono cancellati tutti i dati del buffer di replica.

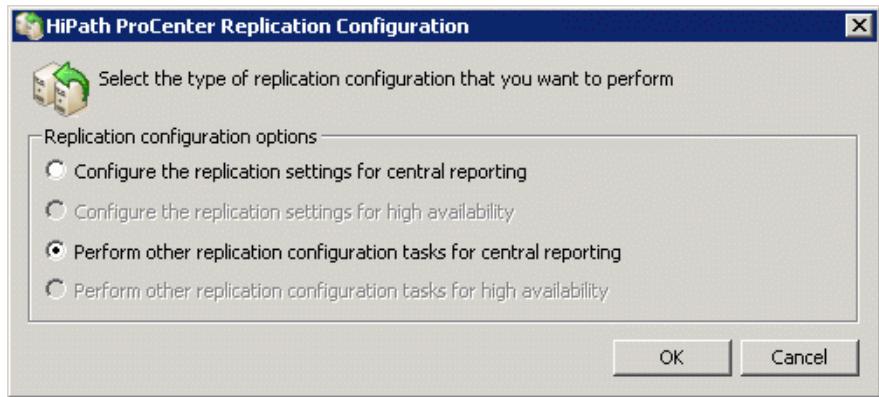
Per riavviare la replica report centralizzato:

1. Utilizzare l'applicazione per i cluster Microsoft per scollegare il **HPPC Group** (Gruppo HPPC). Prima di procedere, attendere che lo stato del server diventi Warm Standby.
2. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** sia sul server principale che su quello di backup. Attendere la chiusura completa dei servizi prima di procedere.
3. Eseguire il logon sul server dove si era interrotta la replica.
4. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.

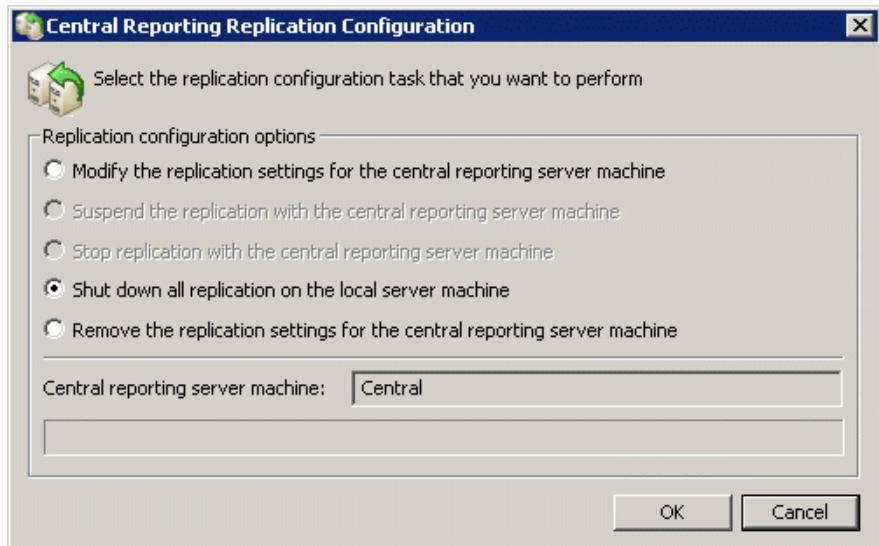
Gestione di un ambiente di alta disponibilità (warm standby)

Gestione della replica per l'alta disponibilità (warm standby)

5. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.



6. Selezionare **Shut down all replication on the local server machine**, quindi fare clic su **OK**.

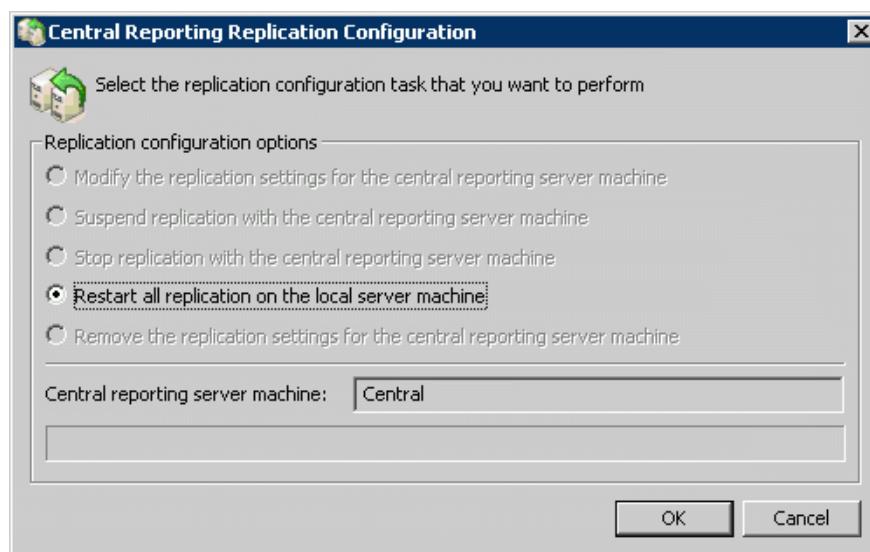


7. Sullo stesso server, eseguire nuovamente trcdbins.exe. Nel menu **Start**, fare clic su **Eseguì**, digitare **trcdbins** quindi fare clic su **OK**.
8. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.

Gestione di un ambiente di alta disponibilità (warm standby)

Gestione della replica per l'alta disponibilità (warm standby)

9. Selezionare **Restart all replication on the local server machine**, quindi fare clic su **OK**.



10. Sincronizzare i dati nei report solo se veramente necessario. Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86.
11. Sincronizzare i dati di amministrazione fra i server principale e di backup. Per ulteriori informazioni, vedere Sezione 8.2, "Sincronizzazione dei dati fra il server principale e quello di backup", a pagina 83.
12. Se si stabilisce di non sincronizzare i dati nei report nella fase 10, sincronizzare i dati di amministrazione fra il server principale e il server report centralizzati. Per dettagli Sezione 8.3, "Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati", a pagina 85.

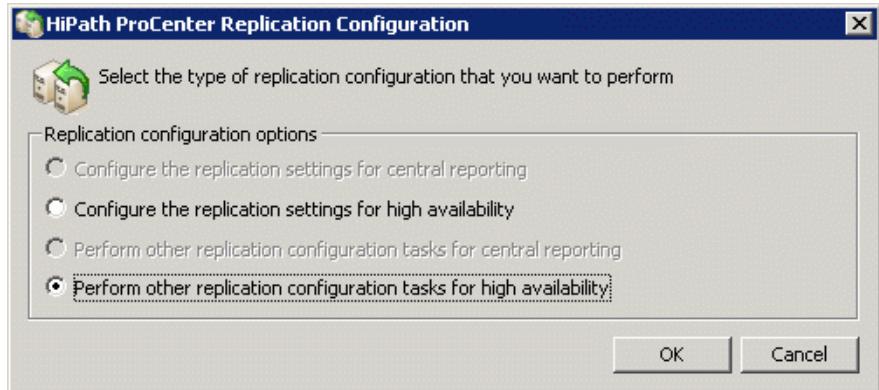
8.1.5 Chiusura di tutte le repliche

È possibile terminare tutte le repliche sul server, ad esempio se si verifica un problema di rete ed è necessario rimuovere le impostazioni di replica (il che richiede accesso alla rete). Quando il sistema è configurato sia per l'alta disponibilità (warm standby) che per il report centralizzato, ciò termina entrambi i tipi di replica.

IMPORTANTE: Si consiglia di effettuare tale procedura solo se necessario o indicato, dato che potrebbe richiedere di sincronizzare i dati nei report. Per ulteriori informazioni, vedere Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86. Se possibile, si consiglia di sospendere anziché terminare la replica, poiché la sospensione non richiede di sincronizzare i dati nei report.

Per terminare tutte le repliche sul server:

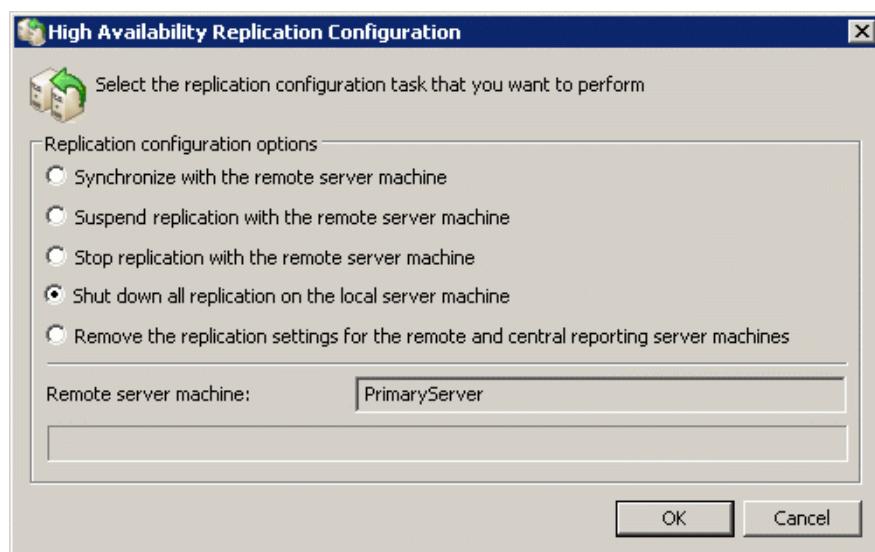
1. Eseguire il logon sul server dove si desiderano terminare tutte le repliche.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.



Gestione di un ambiente di alta disponibilità (warm standby)

Gestione della replica per l'alta disponibilità (warm standby)

4. Selezionare **Shutdown all replication on the local server machine**, quindi fare clic su **OK**.



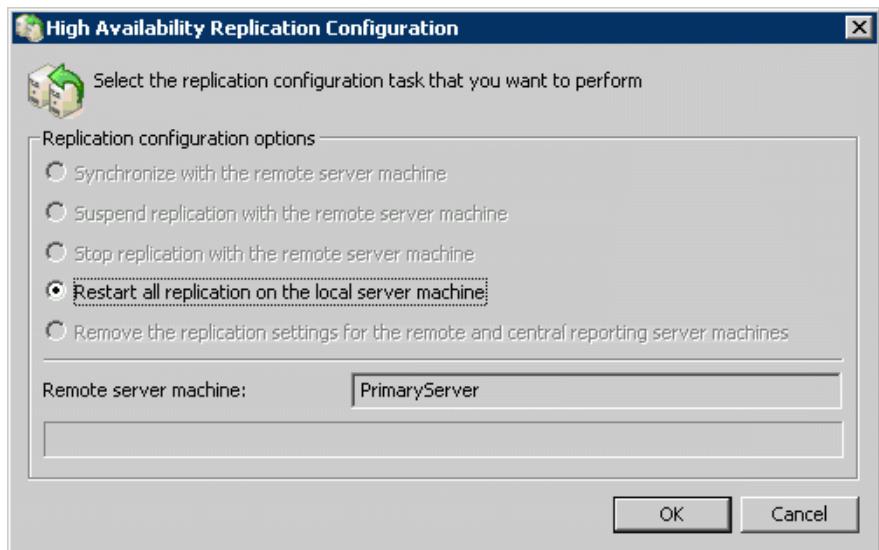
8.1.5.1 Riavvio di tutte le repliche

Tutte le repliche sul server, una volta terminate, possono essere riavviate come descritto in questa procedura. Quando il sistema è configurato sia per l'alta disponibilità (warm standby) che per il report centralizzato, questa procedura riavvia entrambi i tipi di replica. Durante il processo di riavvio vengono cancellati tutti i dati del buffer di replica.

Per riavviare tutte le repliche sul server:

1. Utilizzare l'applicazione per i cluster Microsoft per scollegare il **HPPC Group** (Gruppo HPPC). Prima di procedere, attendere che lo stato del server diventi Warm Standby.
2. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** sia sul server principale che su quello di backup. Attendere la chiusura completa dei servizi prima di procedere.
3. Eseguire il logon sul server dove si era terminata la replica.
4. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
5. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.

6. Selezionare **Restart all replication on the local server machine**, quindi fare clic su **OK**.



7. Sincronizzare i dati nei report solo se veramente necessario. Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86.
8. Sincronizzare i dati di amministrazione fra i server principale e di backup. Per ulteriori informazioni, vedere Sezione 8.2, "Sincronizzazione dei dati fra il server principale e quello di backup", a pagina 83.
9. Se si stabilisce di non sincronizzare i dati nei report nella fase 7, sincronizzare i dati di amministrazione fra il server principale e il server report centralizzati. Per dettagli Sezione 8.3, "Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati", a pagina 85.

8.2 Sincronizzazione dei dati fra il server principale e quello di backup

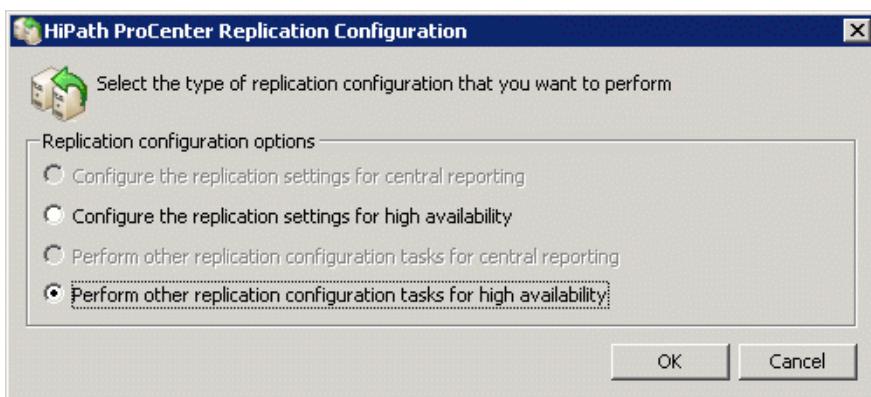
Talvolta può essere necessario sincronizzare i dati di amministrazione e di elaborazione fra i server primario e di backup. Ad esempio, può essere opportuno eseguire questa operazione se uno dei server è inattivo da un lungo periodo (oltre due giorni) poiché il sistema può memorizzare nel buffer solo una quantità limitata di dati. In tal caso, occorre eseguire la procedura sul server rimasto inattivo e che deve essere sincronizzato.

Gestione di un ambiente di alta disponibilità (warm standby)

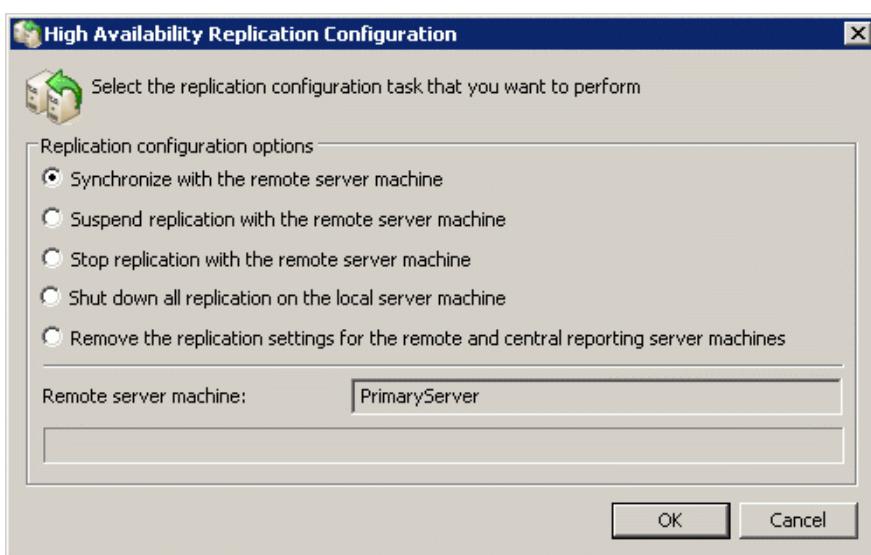
Sincronizzazione dei dati fra il server principale e quello di backup

Per sincronizzare i dati fra il server principale e quello di backup:

1. Utilizzare l'applicazione per i cluster Microsoft per scolare il **HPPC Group** (Gruppo HPPC). Prima di procedere, attendere che lo stato del server diventi Warm Standby.
2. Arrestare il servizio **OpenScape Contact Center** su tutti i server. Attendere la chiusura completa del servizio prima di procedere.
3. Eseguire il logon sul server da sincronizzare.
4. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
5. Se si è dotato della funzione opzionale Report centralizzato, viene visualizzata la finestra di dialogo delle opzioni di configurazione di replica OpenScape Contact Center. Selezionare **Perform other replication configuration tasks for high availability**, quindi fare clic su **OK**.



6. Selezionare **Synchronize with the remote server machine**, quindi fare clic su **OK**.



7. Quando la sincronizzazione è terminata, avviare il servizio **OpenScape Contact Center** su tutti i server.

Gestione di un ambiente di alta disponibilità (warm standby)

Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati

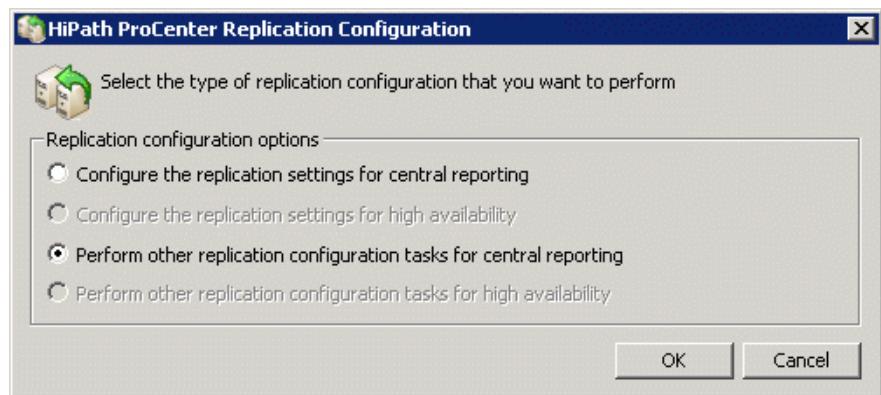
8. Connettere il **HPPC Group** (Gruppo HPPC).

8.3 Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati

Quando il sistema è configurato per l'alta disponibilità (warm standby) con i report centralizzati, si possono riscontrare problemi che richiedono di sincronizzare i dati di amministrazione fra il server primario e quello dei report centralizzati.

Per sincronizzare i dati di amministrazione fra il server principale e il server report centralizzati.

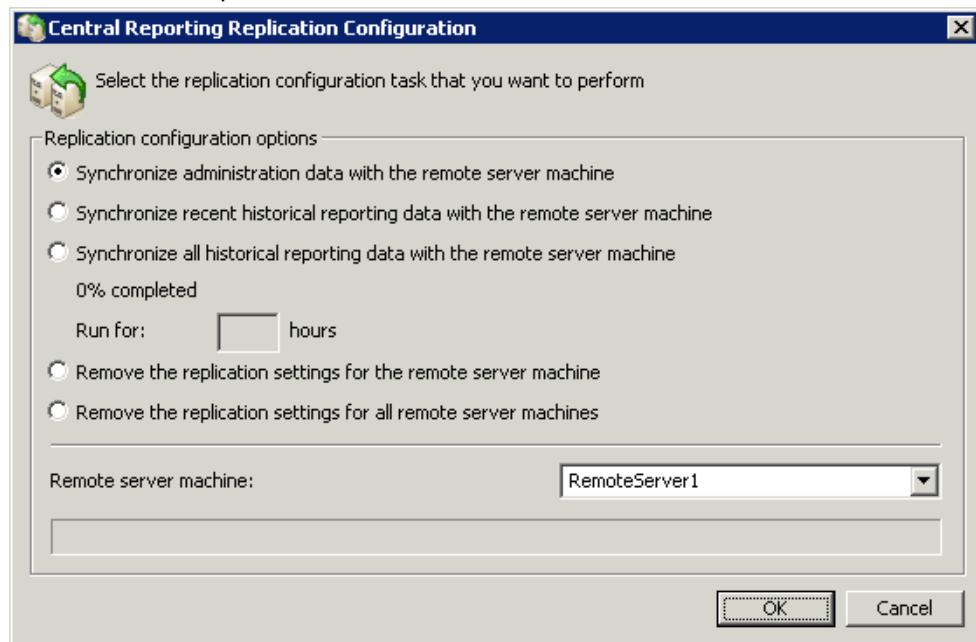
1. Eseguire il logon sul server report centralizzati.
2. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
3. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.



Gestione di un ambiente di alta disponibilità (warm standby)

Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato

4. Selezionare **Synchronize administration data with the remote server machine**, selezionare il server principale nell'elenco **Remote server machine**, quindi fare clic su **OK**.



8.4 Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato

Se si riscontrano problemi con i dati dei report cronologici, è possibile sincronizzare i dati dei report. Ad esempio, se mancano dei dati a causa di una prolungata interruzione della rete fra uno dei server (principale o di backup) e il server report centralizzato, è possibile sincronizzare i dati nei report tra il server e il server report centralizzati. Quando si sincronizzano i dati dei report su un server nel cluster (principale o di backup), è necessario sincronizzare i dati dei report anche sull'altro server.

NOTA: La sincronizzazione dei dati nei report può richiedere molto tempo. Si consiglia di eseguire la procedura solo se i problemi ai dati nei report cronologici sono veramente inaccettabili per le proprie esigenze.

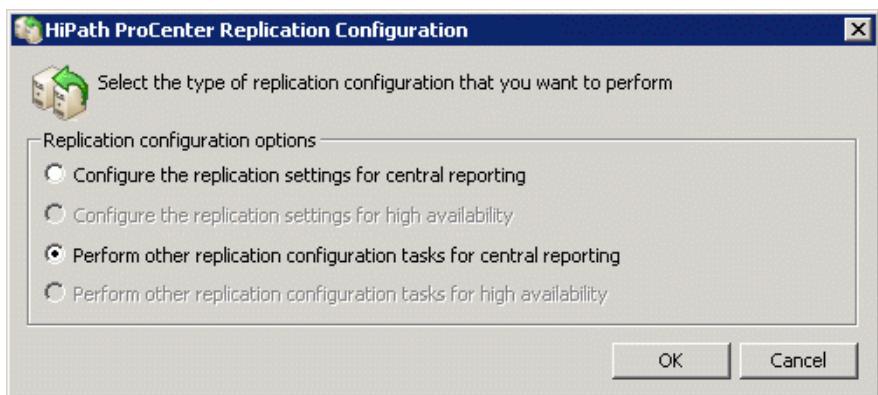
NOTA: Prima di eseguire la sincronizzazione, si consiglia di controllare i periodi di mantenimento sul server report centralizzati per assicurarsi che non siano più brevi di quelli configurati sul server principale. In caso di periodi di mantenimento più brevi, è possibile perdere alcuni dati dei report durante la prima ora di manutenzione dati dopo la sincronizzazione.

Gestione di un ambiente di alta disponibilità (warm standby)

Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato

Per sincronizzare i dati dei report per l'alta disponibilità (warm standby) con report centralizzato:

1. Eseguire il logon sul server report centralizzati.
2. Arrestare il servizio **OpenScape Contact Center AutoPA** sul server report centralizzati. Attendere la chiusura completa del servizio prima di procedere.
3. Nel menu **Start**, fare clic su **Esegui**, digitare **trcdbins**, quindi fare clic su **OK**.
4. Selezionare **Perform other replication configuration tasks for central reporting**, quindi fare clic su **OK**.

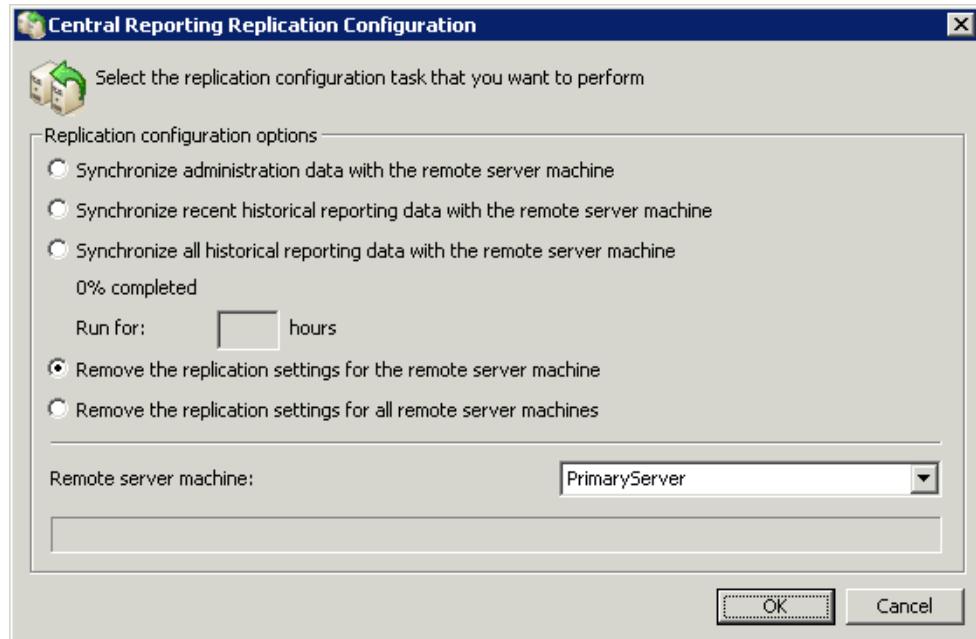


5. Selezionare una delle seguenti opzioni di installazione, quindi fare clic su **OK**:
 - Per sincronizzare i dati dei report cronologici solo per il mese corrente e quello precedente (questa opzione richiede meno tempo), procedere come segue:
 - Selezionare **Synchronize recent historical reporting data with the remote server machine**.
 - Nell'elenco **Remote server**, selezionare il server (principale o di backup) con cui si desidera sincronizzarsi.
 - Per sincronizzare tutti i dati dei report cronologici, procedere come segue:
 - Selezionare **Synchronize all historical reporting data with the remote server machine**.
 - Nell'elenco **Remote server**, selezionare il server (principale o di backup) con cui si desidera sincronizzarsi.
 - Poiché questa opzione richiede molto tempo per essere completata, è possibile specificare la durata della sincronizzazione. Nella casella **Run for** digitare numero di ore che si desidera duri la sincronizzazione. Al termine di questo periodo, la sincronizzazione si interrompe ed è possibile riprendere in un secondo momento. Il valore completo in % mostra in che misura il processo di sincronizzazione è attualmente completo. La barra di avanzamento mostra l'avanzamento nel numero di ore specificato.

Gestione di un ambiente di alta disponibilità (warm standby)

Risoluzione dei problemi di configurazione della replica per l'alta disponibilità (warm standby)

- Per riprendere una sincronizzazione precedente, selezionare **Continue to synchronize all historical reporting data with the remote computer server**, quindi specificare il server remoto (principale o di backup) e la durata della sincronizzazione, come descritto sopra.



6. Ripetere le fasi da 2 a 5 per gli altri server nel cluster.
7. Quando la sincronizzazione è terminata, avviare il servizio **OpenScape Contact Center AutoPA** nel server report centralizzati.

8.5 Risoluzione dei problemi di configurazione della replica per l'alta disponibilità (warm standby)

L'applicazione di configurazione della replica OpenScape Contact Center (trcdbins.exe) effettua diversi test per assicurarsi che la replica sia stata configurata correttamente. Se si presentano problemi con la configurazione di replica, verificare i file di diagnostica (denominati trcdbins.000, trcdbins.001... trcdbins.025), che si trovano nella cartella da cui è stato eseguito il componente. Questi file di diagnostica possono aiutare a risolvere i problemi più comuni della configurazione di replica.

Se i file di diagnostica non aiutano a risolvere i problemi della configurazione di replica, è possibile eseguire la procedura di risoluzione dei problemi descritta in Sezione 7.3, "Risoluzione dei problemi della configurazione di replica per report centralizzato", a pagina 65.

8.6 Ripristino del database

Questa sezione descrive come ripristinare il database di OpenScape Contact Center in un ambiente ad alta disponibilità (warm standby).

Su ciascun server nel quale si desidera ripristinare il database, è necessario verificare che:

- Il software del server OpenScape Contact Center installato sia ancora valido.
- Il livello patch del software del server corrisponda a quello del database da ripristinare.

Se occorre reinstallare il sistema operativo o il software del server OpenScape Contact Center, è necessario attenersi alla procedura descritta in Sezione 8.8, "Sostituzione di un server nel cluster", a pagina 93.

8.6.1 Ripristino del database sul server in modalità standby

Questa procedura descrive come ripristinare il database di OpenScape Contact Center sul server in modalità standby (normalmente il server di backup). Durante gran parte della procedura è possibile lasciare OpenScape Contact Center in esecuzione sul server in modalità attiva. È sufficiente arrestare i servizi OpenScape Contact Center e OpenScape Contact Center AutoPA per un breve periodo di tempo per sincronizzare i dati di amministrazione tra i server principali e di backup.

Per ripristinare il database sul server in modalità standby:

1. Assicurarsi che il server sia in modalità Standby. Se il server è in modalità attiva, utilizzare l'applicazione per i cluster Microsoft per spostare il **HPPC Group** (Gruppo HPPC).
2. Utilizzare l'applicazione per i cluster Microsoft per sospendere il server.
3. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** sul server principale in ripristino. Attendere la chiusura completa dei servizi prima di procedere.
4. Ripristinare il database sul server. Per ulteriori informazioni, attenersi alla procedura fornita in Sezione 6.3.3, "Ripristino del database tramite l'utilità ontape", a pagina 50 o in Sezione 6.3.6, "Ripristino del database tramite l'utilità onbar", a pagina 52, come appropriato.
5. Sincronizzare i dati di amministrazione fra i server principale e di backup. Per ulteriori informazioni, vedere Sezione 8.2, "Sincronizzazione dei dati fra il server principale e quello di backup", a pagina 83.
6. Utilizzare l'applicazione per i cluster Microsoft per riattivare il server.

Gestione di un ambiente di alta disponibilità (warm standby)

Ripristino del database

8.6.2 Ripristino del database sul server report centralizzati

Questa procedura descrive come ripristinare il database esclusivamente sul server report centralizzati. Durante gran parte della procedura è possibile lasciare OpenScape Contact Center in esecuzione sul server in modalità attiva. È sufficiente arrestare i servizi OpenScape Contact Center e OpenScape Contact Center AutoPA per un breve periodo di tempo dopo la sincronizzazione dei dati di amministrazione tra il server principale e il server report centralizzati.

Quando si ripristina il database sul server report centralizzati, i dati non vengono sincronizzati con i server principale e di backup. È necessario decidere se i dati nei report sono accettabili per i propri scopi oppure se si desidera sincronizzarli come descritto in Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86.

Per ripristinare il database sul server report centralizzati:

1. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** sul server report centralizzati. Attendere la chiusura completa dei servizi prima di procedere.
2. Ripristinare il database sul server. Per ulteriori informazioni, attenersi alla procedura fornita in Sezione 6.3.3, "Ripristino del database tramite l'utilità `ontape`", a pagina 50 o in Sezione 6.3.6, "Ripristino del database tramite l'utilità `onbar`", a pagina 52, come appropriato.
3. Sincronizzare i dati nei report solo se veramente necessario. Per ulteriori informazioni, vedere Sezione 8.4, "Sincronizzazione dei dati dei report per alta disponibilità (warm standby) con report centralizzato", a pagina 86.
4. Se si è deciso di non sincronizzare i dati nei report nella fase 3, è necessario procedere come segue:
 - a) Nel server in modalità attiva (normalmente il server principale), aprire una finestra prompt dei comandi, digitare quanto segue e premere **INVIO**:

```
trcdbins -activate
```
 - b) Sincronizzare i dati di amministrazione fra il server principale e il server report centralizzati. Per ulteriori informazioni, vedere Sezione 8.3, "Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati", a pagina 85.
5. Avviare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** sul server report centralizzati.

8.6.3 Ripristino del database su più server

Questa procedura descrive come ripristinare più istanze del database di OpenScape Contact Center sul server principale, di backup e/o sul server report centralizzati opzionale. È necessario arrestare i servizi OpenScape Contact Center e OpenScape Contact Center AutoPA su tutti i server per l'intera durata della procedura.

Per ripristinare il database OpenScape Contact Center:

1. Utilizzare l'applicazione per i cluster Microsoft per scollegare il **HPPC Group** (Gruppo HPPC). Prima di procedere, attendere che lo stato del server diventi Warm Standby.
2. Arrestare i servizi **OpenScape Contact Center** e **OpenScape Contact Center AutoPA** su tutti i server. Attendere la chiusura completa dei servizi prima di procedere.
3. Ripristinare il database su ciascun server che ne abbia la necessità. Per ulteriori informazioni, attenersi alla procedura fornita in Sezione 6.3.3, "Ripristino del database tramite l'utilità ontape", a pagina 50 o in Sezione 6.3.6, "Ripristino del database tramite l'utilità onbar", a pagina 52, come appropriato.
4. Sincronizzare i dati di amministrazione fra i server principale e di backup. Per ulteriori informazioni, vedere Sezione 8.2, "Sincronizzazione dei dati fra il server principale e quello di backup", a pagina 83.
5. Se il sistema è configurato per il report centralizzato, sincronizzare i dati di amministrazione fra il server principale e il server report centralizzati. Per ulteriori informazioni, vedere Sezione 8.3, "Sincronizzazione dei dati di amministrazione fra il server principale e il server report centralizzati", a pagina 85.

Gestione di un ambiente di alta disponibilità (warm standby)

Forzatura di un singolo server nel servizio

8.7 Forzatura di un singolo server nel servizio

La soluzione OpenScape Contact Center ad alta disponibilità (warm standby) utilizza un cluster con quorum di maggioranza nodi definito a due nodi (un server principale e uno di backup) e una condivisione file Witness. Se il server principale e quello di backup rimangono isolati in un cluster a causa di un errore di comunicazione, non è possibile formare una maggioranza e il cluster perde il quorum. Di conseguenza, il servizio cluster e OpenScape Contact Center non vengono più eseguiti. In questo caso, occorre forzare manualmente il quorum su uno dei server in modo che il cluster possa continuare a funzionare.

IMPORTANTE: Prima di eseguire questa procedura, assicurarsi che OpenScape Contact Center non si attivi su entrambi i server (ad esempio, disconnettere l'altro server dalla rete).

Per forzare un singolo server nel servizio:

1. Utilizzando l'applicazione per i cluster Microsoft, arrestare il servizio cluster sul server.
2. Configurare l'opzione “start parameter” del servizio cluster come segue:
`/forcequorum <nome server>`
dove `<nome server>` è il nome del server.
3. Avviare il servizio cluster.

NOTA: Non fare clic su **OK** o su **Applica** prima di avviare il servizio cluster poiché verrebbero sovrascritti i parametri di avvio. Notare inoltre che i parametri di avvio non vengono mantenuti dopo un riavvio del computer.

8.8 Sostituzione di un server nel cluster

Se occorre sostituire un server, è necessario attenersi a questa procedura per aggiungere il nuovo server al cluster.

IMPORTANTE: Un server nel cluster deve essere sostituito solo sotto la supervisione del rappresentante dell'assistenza.

NOTA: Questa procedura richiede di sottoporre a backup tutti i dati sul server. Assicurarsi che il backup contenga i dati di stato del sistema del server, che includono elementi quali il registro di sistema e i file di avvio.

Prima di iniziare, è necessario:

- Assicurarsi che l'hardware del nuovo server sia identico a quello da sostituire. Il nuovo server deve presentare lo stesso indirizzo IP e nome server di quello da sostituire.
- Richiedere un nuovo file della licenza per il nuovo server. L'ID sistema utilizzato per la licenza di OpenScape Contact Center si basa sull'hardware del server.

Per sostituire un server nel cluster:

1. Ripristinare tutti i dati sul nuovo server utilizzando il backup più recente.
2. Utilizzando l'applicazione per i cluster Microsoft, sospendere il nuovo server.
3. Assicurarsi che le connessioni di rete siano riferite alla scheda di rete corrispondente e che l'ordine della rete e quello dei binding TCP/IP siano corretti. L'ordine di rete è cluster privato, cliente, PABX. Al momento di configurare le schede di interfaccia di rete, è importante ricordare che l'ordine dei binding TCP/IP è diverso da quello della rete. La scheda di interfaccia di rete del cliente deve trovarsi all'inizio dell'elenco dei binding TCP/IP, seguita dalla scheda di interfaccia di rete privata del cluster, quindi dalla scheda di interfaccia di rete del PABX (se richiesta).
4. Assicurarsi che il livello patch del software del server OpenScape Contact Center corrisponda a quello del database da ripristinare.
5. Ripristinare il database OpenScape Contact Center. Per ulteriori informazioni, vedere Sezione 8.6.1, "Ripristino del database sul server in modalità standby", a pagina 89.
6. Utilizzando l'applicazione Manager, attivare la licenza del nuovo server. Per ulteriori informazioni, consultare la *Guida di Manager*.

Gestione di un ambiente di alta disponibilità (warm standby)

Sostituzione di un server nel cluster

Indice alfabetico

A

accesso remoto 43
 account utente Applicazione OpenScape UC,
 configurare per integrazione presenze 41
 alta disponibilità (warm standby)
 arrestare la replica 74
 arrestare la replica report centralizzato 77
 chiudere tutte le repliche 81
 forzare il quorum su un singolo server 92
 gestire la replica 71
 informazioni sul buffer di replica 57
 ordine binding TCP/IP 93
 riavviare la replica dopo l'arresto 75
 riavviare la replica report centralizzato dopo
 l'arresto 78
 riavviare tutte le repliche 82
 riprendere la replica 72
 riprendere la replica report centralizzato 73
 ripristinare il database 89
 risolvere i problemi di configurazione della
 replica 88
 sincronizzare i dati 83
 sincronizzare i dati dei report 86
 sincronizzare i dati di amministrazione per il report
 centralizzato 85
 sincronizzazione degli orari dei server 71
 sospendere la replica 71
 sospendere la replica report centralizzato 73
 sostituire un server nel cluster 93
 applicazione Amministrazione cluster Microsoft 71
 applicazione Gestione cluster di failover 71
 autenticazione, server e-mail 16

B

bacheche, configurare 7
 backup database
 backup completi 46
 backup incrementali 46
 pianificare 47
 ripristinare tramite l'utilità onbar 52
 ripristinare tramite l'utilità ontape 50
 su un'unità locale (onbar) 52
 su un'unità locale o di rete (ontape) 49
 su un'unità nastro locale (ontape) 48
 backup pianificati 47
 backup, vedere backup di database
 browser Web, requisiti 19

C

codici errore, per richiamata Web 38
 collaborazione Web
 risoluzione dei problemi 37
 test su Sun Java Server 30
 test sul server IIS 23
 collaborazione Web su server Tomcat 27
 componenti Web
 configurare 20
 configurare su Sun Java Server 28
 configurare sul server IIS 21
 configurare sul server Tomcat 25
 impostare una connessione protetta 32
 localizzare 34
 personalizzare 35
 requisiti browser Web 19
 requisiti del sistema 19
 config.properties
 configurare su un server Web Sun Java System 29
 configurare un server Tomcat 26
 connessione protetta
 per un server e-mail aziendale 15
 per un server Web aziendale 32
 connessioni IP, configurare per bacheche 7

D

dati dei report
 sincronizzare per alta disponibilità (warm standby)
 con report centralizzato 86
 sincronizzare per report centralizzato 63
 dati di amministrazione
 sincronizzare per alta disponibilità (warm standby)
 con report centralizzato 85
 directory virtuale, server IIS 22
 distribuzione di IBM Lotus Domino 14
 distribuzione di Lotus Domino 14
 distribuzione di Microsoft Exchange 11
 documentazione
 convenzioni di formattazione 5
 destinatario previsto 5
 fornire commenti 6

E

elenco LDAP, configurare per integrazione
 presenze 42
 estensioni ISAPI 22

F

file HPWC.ini
attivare per SSL 32
configurare 22
risoluzione dei problemi 37, 38
file .war
configurare su un server Web Sun Java System 29
funzione report e-mail, supporto per 16
funzioni MIME 9

I

Informix
cambiare la password 44
configurare i parametri ontape 47, 49
utilizzare l'utilità onbar 52
utilizzare l'utilità ontape 48
integrazione presenze, configurare 41
integrazione VoiceXML
test su server Tomcat 28
test su un server IIS 24
intestazioni messaggi e-mail
inserimento personalizzate 12
richiesta personalizzate 9
intestazioni personalizzate messaggi e-mail
informazioni su 9
inserire 12

J

Java Runtime Engine 38

L

libreria JSSE 38
localizzare componenti Web 34

P

password OpenScape Contact Center, cambiare 44
password, cambiare 44
plug-in Servizio SSDP 43
protocollo IMAP4 9
protocollo SMTP 9

Q

quorum, forzare su un singolo server 92

R

replica
arrestare per alta disponibilità (warm standby) 74
arrestare per report centralizzato 77
chiudere per report centralizzato 61
chiudere tutte le repliche 81
gestire il report centralizzato 57
gestire per alta disponibilità (warm standby) 71

riavviare dopo l'arresto per alta disponibilità (warm standby) 75
riavviare per report centralizzato 62
riavviare per report centralizzato dopo l'arresto 78
riavviare tutte le repliche 82
riprendere per alta disponibilità (warm standby) 72
riprendere per report centralizzato 60
risolvere i problemi per alta disponibilità (warm standby) 88
risolvere i problemi per report centralizzato 65
sospendere per alta disponibilità (warm standby) 71
sospendere per report centralizzato 58
replica dei dati, vedere replica
Report centralizzato
sostituire un server principale 68
report centralizzato
chiudere la replica 61
gestire la replica 57
informazioni sul buffer di replica 57
riavviare la replica 62
riprendere la replica 60
risolvere i problemi della configurazione di replica 65
sincronizzare i dati nei report 63
sincronizzare orari server 57
sospendere la replica 58
richiamata Web
codici errore 38
test su server Tomcat 27
test su Sun Java server 31
test sul server IIS 24
risoluzione dei problemi
collaborazione Web 37
configurare un server Web 37
file HPWC.ini 37, 38
SSL 38
risolvere i problemi
configurazione della replica per alta disponibilità (warm standby) 88
configurazione di replica per report centralizzato 65

S

server e-mail 9
impostare una connessione protetta 15
utilizzare autenticazione 16
server e-mail aziendale
configurare 9
impostare una connessione protetta 15
requisiti 9
utilizzare autenticazione 16
server IIS

- configurare componenti Web 21
- configurare il file HPWC.ini 22
- creare una directory virtuale 22
- impostare una connessione protetta 32
- test collaborazione Web 23
- test integrazione VoiceXML 24
- test richiamata Web 24
- server Tomcat**
 - configurare componenti Web 25
 - configurare e distribuire il file .war 25
 - impostare una connessione protetta 33
 - modificare config.properties 26
 - test integrazione VoiceXML 28
 - test richiamata Web 27
 - verificare collaborazione Web 27
- server Web**
 - configurare 19, 20
 - file personalizzati e aggiornare 19
 - impostare una connessione protetta 32
 - requisiti 19
 - risoluzione dei problemi 37
 - sistemi operativi supportati 19
 - versione Apache Tomcat 19
 - versione Sun Java System 19
- server Web aziendale**
 - configurare 19, 20
 - file personalizzati e aggiornare 19
 - impostare una connessione protetta 32
 - requisiti 19
 - sistemi operativi supportati 19
 - versione Apache Tomcat 19
 - versione Sun Java System 19
- server Web Sun Java System**
 - configurare e distribuire il file .war 29
 - modificare config.properties 29
- server, arrestare per manutenzione 43
- sincronizzare
 - dati dei report per alta disponibilità (warm standby) 86
 - dati dei report per report centralizzato 63
- sincronizzare i dati
 - dati di amministrazione e elaborazione per alta disponibilità (warm standby) 83
- sincronizzazione dei dati per alta disponibilità (warm standby) con il report centralizzato 85
- SSL**
 - attivare per un server e-mail aziendale 15
 - attivare per un server Web aziendale 32
 - attivare su Sun Java Server 33
 - attivare su un server IIS 32
 - attivare su un server Tomcat 33
 - risoluzione dei problemi 38
- Sun Java System Web Server**
 - configurare componenti Web 28
 - impostare una connessione protetta 33
 - test collaborazione Web 30
 - test richiamata Web 31
 - supporto SNMP, metodi 53
- U**
 - utilità
 - osccmseheaders 12
 - osccregistersnmpextension 54
- V**
 - versione Apache Tomcat 19
 - versione Web Server Sun Java System 19
- W**
 - file .war
 - configurare su server Tomcat 25

