Redundancy

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). 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

Mitel is a trademark of Mitel Networks Corporation.

Windows and Microsoft are trademarks of Microsoft Corporation.

Adobe Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

CONTENTS

1 INTRODUCTION

This document describes the redundancy capabilities of the Mitel InAttend solution.

1.1 REDUNDANCY SOLUTIONS

There are two supported redundancy solutions for the InAttend solution:

- VMware High Availability (recommended)
- Hot-standby servers, without using VMware High Availability

These solutions are described in more detail in this document, and applies both to InAttend installations with and without CMG. This document doesn't include CMG Speech redundancy and no multi-site scenarios are described.

1.1.1 SOLUTION COMPARISION

The table below compares the two redundancy solutions.

	VMware High Availability	Hot-standby servers
Full CMG functionality (e.g. activity management) on primary server failure	Yes	No Directory search only.
Full presence and line state on primary server failure	Yes	No
Automatic failover for directory searches in InAttend	Yes	No Each attendant need to switch to the backup directory
Only one set of InAttend and CMG licenses required	Yes	No Multiple licenses required for InAttend, not CMG
Support redundant multi-site deployments with centralized CMG server and local backup servers.	Yes	No
InAttend solution configuration complexity	Low (VMware handles redundancy complexity)	High

1.1.2 LIMITATIONS

Both redundancy solutions have limitations, and don't provide a solution for the following problems:

- Physical network failures that prevents communication between clients and server components

- Physical network failures that prevents communication between server components and call manager

- Software errors

2 INTRODUCTION TO REDUNDANCY

This chapter describes redundancy for the solution in general and applies to both VMware High Availability and Hot-standby server redundancy solutions.

2.1 INATTEND CLIENT

InAttend is connecting to ACS Queue Manager for queues and call control, ACS Media server for soft phone RTP stream, CMG for directory search and activity management or an LDAP server for directory search. InAttend also connects to AnA, TCS and the InAttend server component DAL Service.

When running InAttend with CMG, the CMG database is typically the main directory, even if LDAP servers can be added as additional directories. When running InAttend stand alone, no CMG server is used and an LDAP server is used as main directory. The CMG server redundancy is described in the chapter for Hot-standby redundancy.

2.1.1 STARTUP

In order for InAttend to connect to ACS Queue Manager, InAttend will request an AnA token from the AnA service and use this to get the NCLA configuration from the TCS service. The connection to AnA and TCS is only used during startup of InAttend, and if the client can't connect, it will use the settings saved from last time the connection was successful.

InAttend acquires licenses by contacting BluStar License Manager during startup. The client cannot be started unless licenses are available.

2.1.2 LDAP DIRECTORY REDUNDANCY

InAttend can connect to one or more LDAP servers for directory search. The LDAP server can either be BluStar Directory Server, Active Directory, a CRM system or any other LDAP compatible data source.

When using an LDAP server outside the InAttend solution, it's recommended to add an additional backup LDAP server to be used if the primary LDAP server isn't working. When using the BluStar Directory Server, the redundancy can either be taken care of by VMware High Availability, or by having a backup instance of the BluStar Directory Server running on another server.

In case of failover, the backup LDAP system data source and views will be automatically activated by the client if the primary server is not responding. The InAttend client will however not automatically switch back to the primary server until the client has been restarted.

2.2 LICENSE SERVICES

Enterprise License Manager (ELM) is a client/server license-control application used by several Mitel applications.

BluStar License Manager is used by CMG and InAttend to acquire licenses from ELM. License management is one of the factors that need to be considered when evaluating the redundancy solution to deploy.
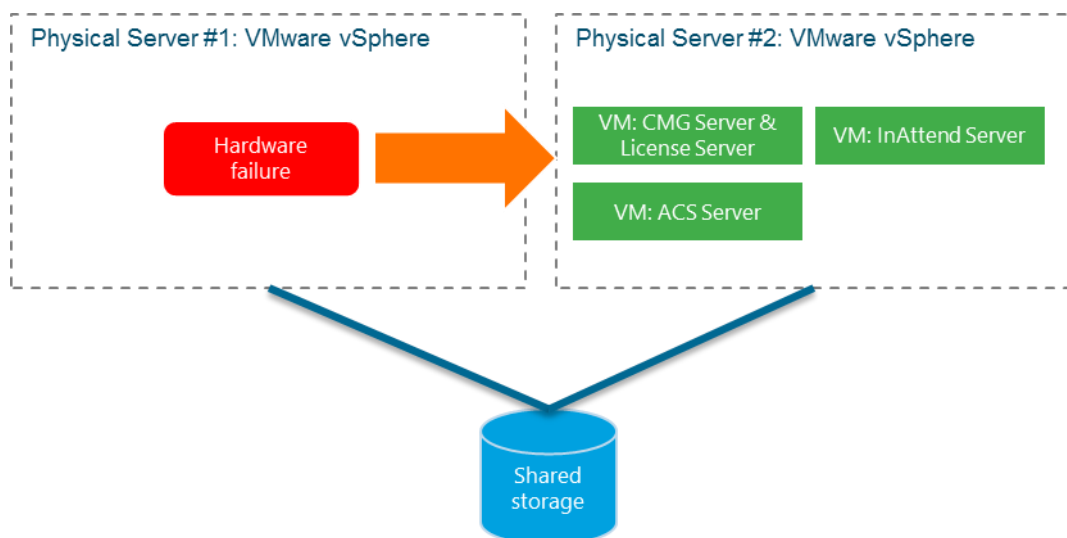
3 REDUNDANCY USING VMWARE HIGH AVAILABILITY

3.1 VMWARE OVERVIEW

The InAttend solution can run in a VMware High Availability environment. VMware High Availability requires more than one VMware server and a shared storage area for the servers. This concept is illustrated below.
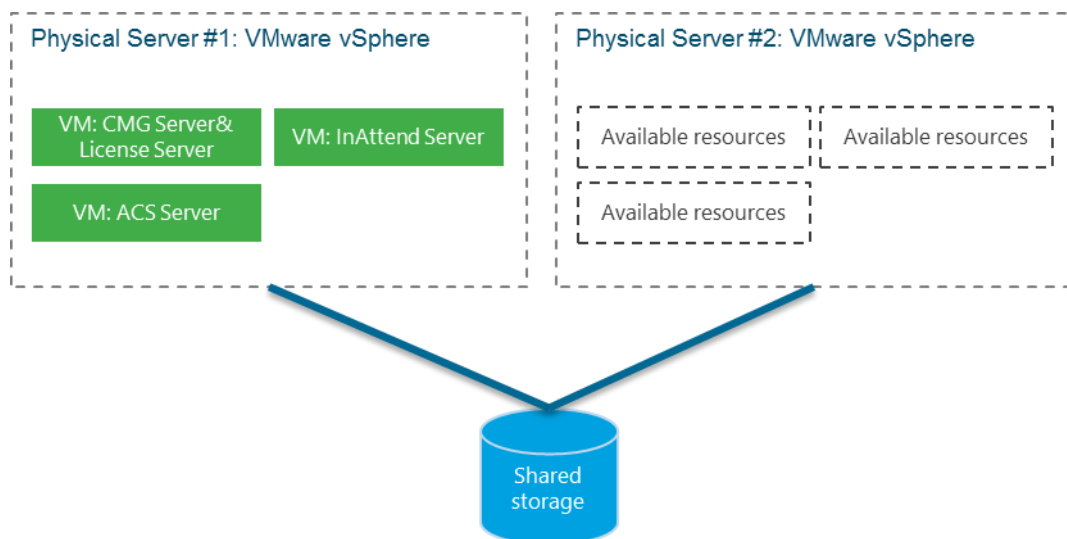
VMware High Availability will detect if a VMware server is failing, and immediately start up the virtual machines on another server. This will result in a down time of a few minutes until the virtual machines are up and running again. The failover concept is illustrated below.

The concepts described above are simplified, as they only include two VMware servers. There may be more VMware servers, and all virtual machines in the

InAttend solution may not run on the same VMware servers, resulting in failover of only certain services in case of failure of a VMware server.

When using VMware High Availability, there are no requirements of installing several instances of each software component to achieve redundancy. Additional instances can be however be added for performance reasons, for example multiple virtual machines running the ACS Media server.

The call managers can either be running on physical servers or in the same VMware High Availability environment as the InAttend solution. From a call manager point of view, only a single SIP trunk needs to be configured for ACS NeTS when using VMware High Availability.

3.2 LICENSES

The licenses will not be affected by using VMware High Availability. The licenses installed on a virtual machine will continue to work even if the virtual machine is restarted on another VMware server. No additional set of licenses will be required.

3.3 ACS

If the ACS Media server is running in a virtual machine, it's important to allocate dedicated CPU and network resources to this virtual machine to ensure that the virtualized environment doesn't have a negative impact on the real time media processing. It's not recommended to use VMware vMotion and automatic load balancing for this reason.

An alternative way of deploying the ACS Media server is to install two instances on physical servers outside the VMware environment.

3.4 SERVER FAILURE

This section describes the result of a server failure from a client and service perspective.

3.4.1 INATTEND CLIENT

In case of a server failure, the InAttend clients will not be able to communicate with the services until the virtual machines have been restarted on another VMware server. All calls, both queued and ongoing, will be dropped and no new calls will be received until the virtual machine has restarted.

Once the virtual machines for the services are running again, the InAttend client will automatically reconnect to the services and continue receiving calls.

3.4.2 SERVICES

If all services in the InAttend solution are running on the same virtual machine or on the same VMware server, a server failure will result in that the virtual machine(s) will be restarted on another VMware server. Once the restart has been completed, all services will be operational.

If the services are running on separate virtual machines, and a VMware server containing one of these virtual machines are failing, this virtual machine will be

restarted on another VMware server. The services running on a virtual machine unaffected by the failure will try to reconnect to the services that failed, and once the virtual machine has been restarted, all services will reconnect and the system will be fully operational again.

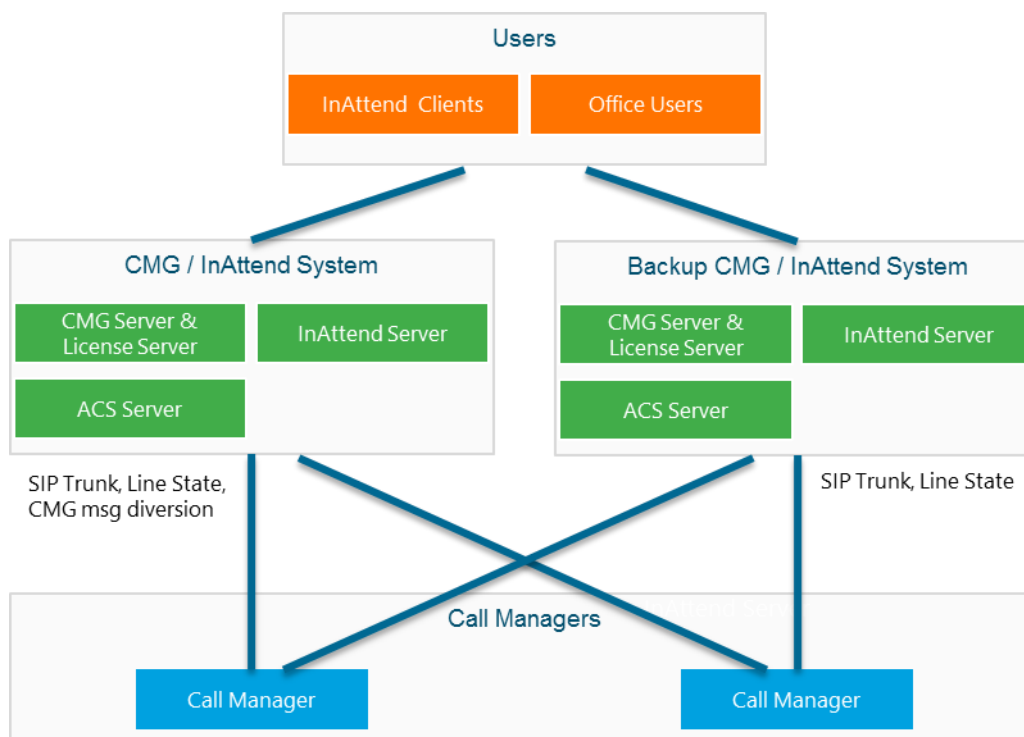# 4 REDUNDANCY USING HOT-STANDBY SERVERS

4.1 OVERVIEW

The illustration below gives an example what a typical installation look like for an InAttend solution without redundancy. Depending on the size of the system, some of the software components can be co-located and run on the same server.
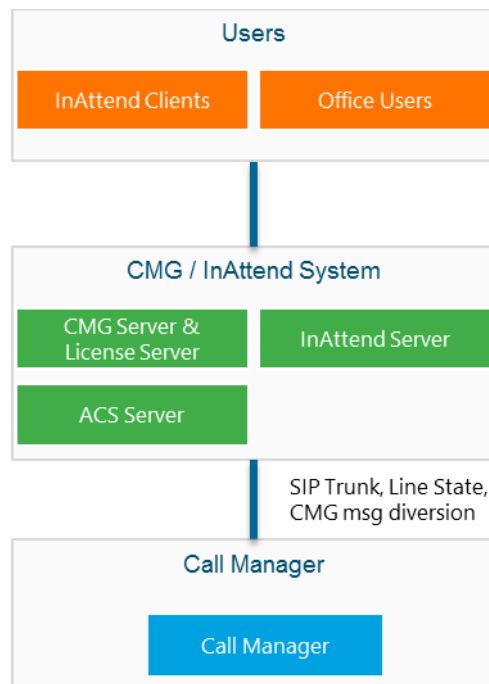
The CMG Server is an optional component. The License Server, including ELM and BluStar License Service, is typically installed on the CMG Server if available, otherwise on the InAttend Server.

The next illustration shows a typical setup of a redundancy solution using hot-standby servers without using VMware High Availability. The servers can either be physical servers or run in a VMware environment (without High Availability).

The next chapters will describe the redundancy solution in more detail.

Note! During Hot standby redundancy if the Hard phone per session doesn't work in the secondary server, and the primary server goes down. It is recommended for the users to use the softphone during redundancy for the smoothest experience.

4.2 REDUNDANCY DESCRIPTION

4.2.1 CMG

A backup CMG server can be installed to provide directory access to InAttend even if the primary CMG server is unavailable. The backup CMG server is however not providing full CMG functionality, as it's not connected to the call manager and only indented to be used to provide search capabilities for the attendants. Operations for viewing and setting CMG activities will not be available.

4.2.2 INATTEND CLIENT

4.2.2.1 Connection to multiple ACS Queue Managers

InAttend can connect to several ACS Queue Managers. The attendant can continue working as usual as long as a connection to at least one ACS Queue Manager exists. If the primary server is unavailable, the calls will still be distributed from the backup server. When the primary server is available again, the calls will be distributed from the primary server.

If the connection to all ACS Queue Manager servers are lost, the open queues will change status indication to be closed. Once the connection to at least one server has been established, the queues will be opened again.

4.2.2.2 Connection to multiple DAL Services

When BluStar Server is installed on redundant servers, the DAL service component will be running on each of these servers.

In case of a failure of the primary DAL service the InAttend client will automatically switch over to the backup DAL service to secure the continuous operation of the InAttend client.

When the connection to the primary DAL service is re-established, the client will automatically switch back.

4.2.2.3 Presence

Presence and line state will only be available when both the primary CMG server running BluStar Web service is available and the primary InAttend server running the BluStar Presence Server is available.

In case of a failure of any of these primary servers, presence and line state will not be available in the InAttend client. Line state will however still be available for Queue Manager.

4.2.3 INATTEND SERVER

The InAttend Server can be installed for redundancy with a second instance of the BluStar Server installation and if CMG isn't used, also a second instance of the license services and BluStar Web service.

4.2.3.1 DAL Service

When installing a redundant InAttend server, a backup DAL service will be running on the backup server. The clients will automatically failover to the secondary DAL service if the primary service is down.

4.2.3.2 CTI Server

The BluStar CTI Server creates redundancy by having the possibility to connect to several line state servers.

If several BluStar CTI Servers have connections to a call manager, this might require additional licenses in the call manager (like CSTA licenses and monitor licenses).

If the connection to the telephone system fails the BluStar CTI Server starts an automatic reconnect to reestablish the connection.

Set operation to set basic forwarding will work even if the primary server is unavailable.

4.2.4 ACS

In the basic ACS setup without redundancy the system is connected according to the simplified system overview below. Each ACS server is comprised of NeTS and a Queue Manager. NeTS is responsible for call and media control. The Queue Manager maintains the queues and handles attendant requests. Each attendant console connects to Queue Manager using TCP connections. In this setup, without redundancy, the InAttend clients cannot be used if the ACS server isn't working.
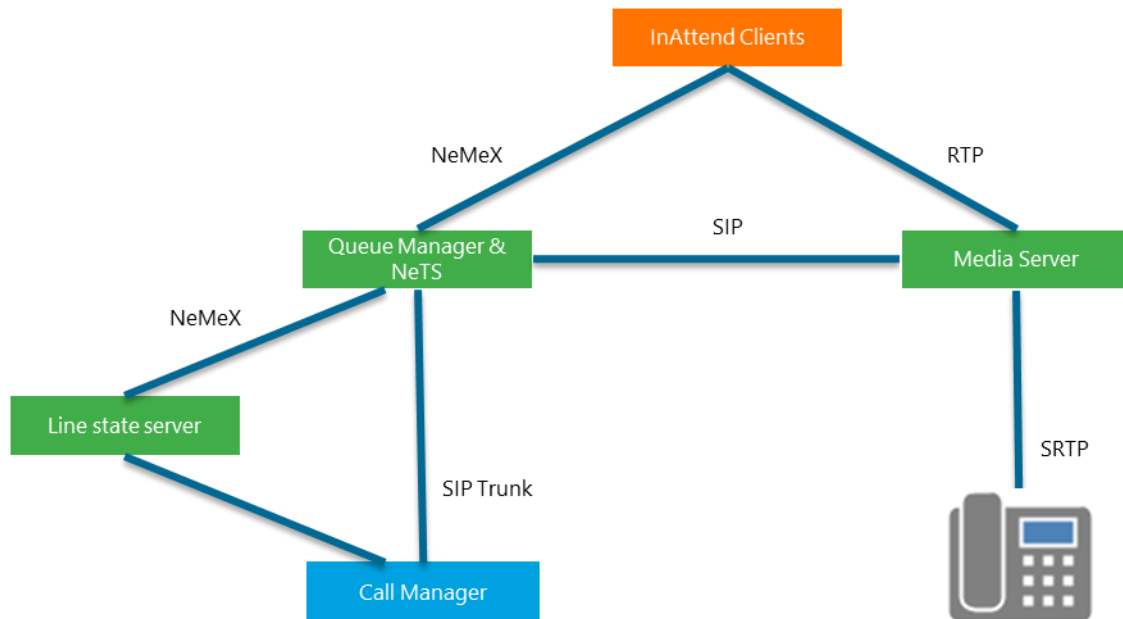
Adding backup servers for redundancy is illustrated below.
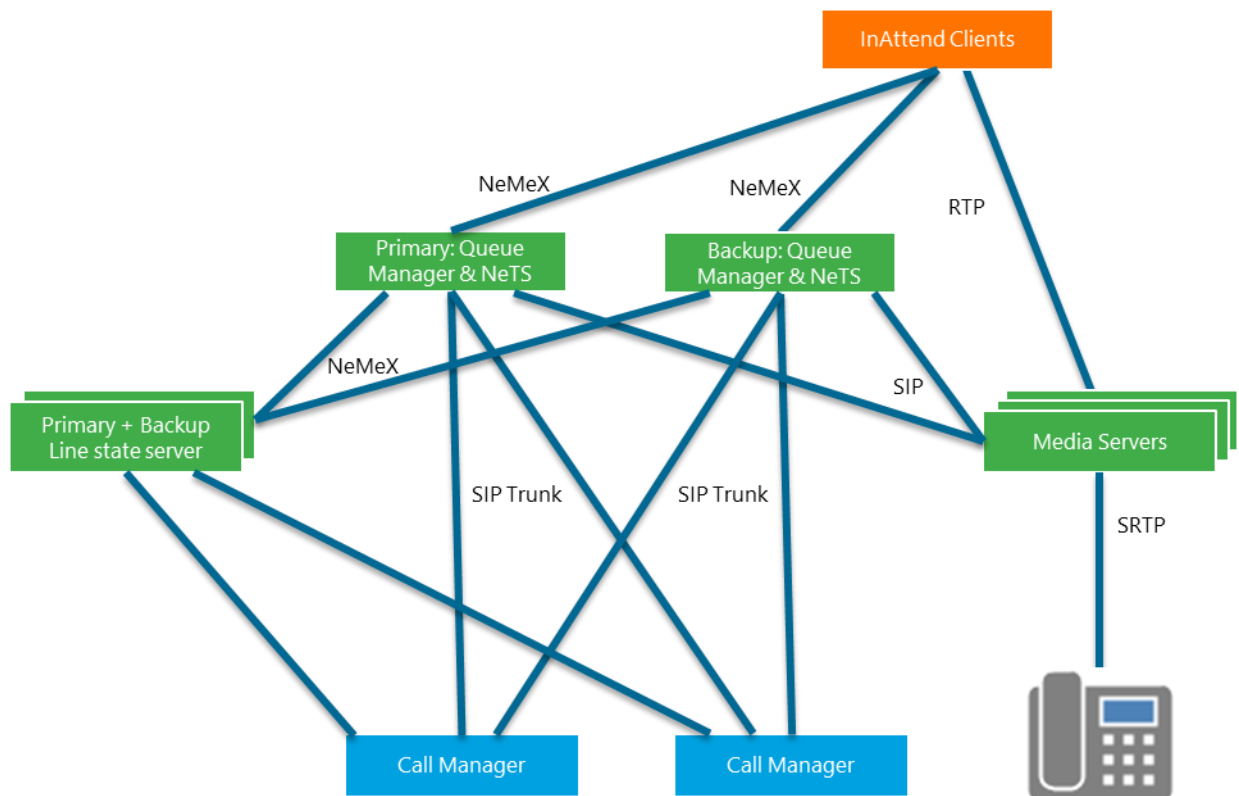
4.2.4.1 NeTS

In order to use redundancy with ACS, the call manager must be configured to manage the backup NeTS server in case the primary server is unavailable. The call manager is assumed to be capable of performing a failover routing of the SIP calls.

Note! Unless the call manager can redirect calls already connected to the primary server (calls in queue) to the secondary server, these calls will be lost.

NeTS has a failover mechanism when connecting to the call manager. NeTS can choose between several SIP nodes for the outbound requests and can failover in case of a missing response from the target or a closed socket port.

4.2.4.2 Media server

Media servers can be installed on several machines for resource distribution and network topology reasons. But it is also possible for several media servers to work as backup nodes for each other.

All calls from the call manager to the NeTS result in twin SIP sessions between NeTS and a media server. All RTP from the SIP end point, behind the call manager, will be routed to the media server. When an operator is connected with the caller, RTP will stream between operator and the caller through the media server. This is necessary for in call media control.

The redundancy is accomplished by a failover mechanism in NeTS. NeTS will use the TCA configuration to select one of the configured media servers for a specific call. These media servers will be contacted in listed order. If a media server fails to respond, or responds with an error code, the next media server in the list will be contacted. If media server node becomes unavailable, all media streams on that server will be disconnected. New RTP streams will however be connected to a working media server automatically.

4.2.4.3 Quality Manager

Quality Manager can connect to multiple Queue Managers and collect statistics from all of them. If the primary Queue Manager stops working, the attendants will connect to the secondary Queue Manager and Quality Manager will continue to collect statistics because it's already connected to the secondary Queue Manager

When using SQL Server Failover Clustering, the Quality Manager data will be stored in a redundant way, across more than one SQL Server.

4.2.5 LICENSES

If CMG is used; both ELM and BluStar License Manager should be installed on the CMG servers (both the primary and backup server). If InAttend is used in stand-alone mode, these services should be installed on the InAttend servers (both the primary and backup server). This is according to the default deployment when using the installation wizards for installing the software.

The primary license server needs a full set of licenses. The backup license server only needs InAttend client licenses, but no CMG licenses

The CMG database is only intended to be used for searches from InAttend when the primary CMG server has failed. Operations to add or remove users will not be available on the backup CMG server. These operations are not indented to be performed on the backup server, and the lack of licenses will also prevent this.

5 CONFIGURE HOT-STANDBY SERVERS

This chapter describes how to configure a system for hot-standby redundancy.

5.1 CMG

Install the CMG Server software on two servers. The primary server should have all services running while the backup server must be configured to not connect to the call manager.

The PBXSTD service must be disabled on the backup server using the SPMAN tool. The reason for this is to avoid conflicts and confusion with activity information, as the activity information cannot be updated correctly on the backup server.

5.1.1 CMG DATABASE REDUNDANCY

This section describes how to configure the CMG database to be restored to the backup server on a regular interval.

The files referred to below are part of the media kit for CMG.

1. Create the folder C:\Restore on the CMG Backup Server

2. Copy 'stopniceservice.bat', 'singleusermode.bat', 'singleusermode.txt' and 'Restore_nice.bat' to C:\Restore on the CMG Backup Server

3. Edit the batch file 'Restore_nice.bat' to suit your needs

4. Copy the nightly backup of the main CMG database nice to the C:\Restore folder on the CMG Backup Server.

5. Run the batch file 'stopniceservice.bat' which will stop the nice server 01 service

6. Run the batch file 'singleusermode.bat' which executes the command in 'singleusermode.txt' and set the SQL Server in single user mode

7. Run the batch file 'Restore_nice.bat' which restores the nice database into the backup CMG Server and alters a few parameters and removes all activities. Activities are removed as they may be outdated because the backup server doesn't have a connection to the call manager.

8. Schedule point 4 to 7 to run in that order each night

The database backup and restore procedure described above is compatible with all editions of Microsoft SQL Server, including Express Edition.

5.2 INATTEND SERVER

Install the BluStar Server software on two servers. Run the DAL Configuration tool on both the primary server and backup server and configure them using the same settings for the DAL Service, where the primary server name should be in the "IP / Host Address" field on the left hand side and the backup server name should be in the "Backup IP / Host Address" field on the right hand side.

The settings for "Connection to SQL DB's" shouldn't be configured identical for the primary and backup server. For this section of configuration, the primary server

should be configured with the primary server settings on the left hand side and the backup server settings on the right hand side. For the backup server, the configuration should instead use the backup server name on the left hand side and the primary server name on the right hand side.

The DAL Configuration tool is illustrated below.

The next configuration tool to be used is CMG Configuration for WebAdmin, to configure the location of the CMG database and the web services for ACS. This configuration must be applied on both the primary and backup InAttend Server in order for WebAdmin to configure the system.

5.2.1 CONFIGURE CMG DIRECTORY

This section describes how to add two CMG data sources using WebAdmin.

Click New CMG Data source to point to the CMG Backup Server, as illustrated below.

If the main CMG Server goes down the operator will not get any flashes and there is no possibility to search for users in CMG. The operator can then press Alt+F2 to change the source to be the backup CMG Server. Name the data sources wisely.

'Main CMG Server' is the name of the view in CMG CM (see screenshot below) that will be displayed in the InAttend client below. There can be more views, usually one for each customer group. Name the views wisely.

5.2.2 CONFIGURE INATTEND WITH LDAP DIRECTORY

Multiple LDAP directory sources can be added for LDAP redundancy.

The backup LDAP directory can be added as a second data source in the Attendant Directory Profile configuration in WebAdmin.

5.2.3 CONFIGURE INATTEND LICENSE SERVER

In order to access the profiles in WebAdmin on the backup server, the option to display InAttend related settings must be enabled. This can be enabled in Tools, Administration settings by adding a new parameter with the following properties:

- Section: UserRights
- Parameter name: BluStarServerForInAttend

- Value: 1

In order for the changes to take effect, log out and log in again in WebAdmin.

Note! Because of database replication from the primary database server to the backup database server, the setting BluStarServerForInAttend described above will be required to be set on the backup server each time the server needs to be configured with a new License Manager location.

Use WebAdmin to configure the Server Profile where the License Manager location can be specified. Specify both the primary server and the backup server.

5.2.4 CONFIGURE INATTEND SQL SERVER REDUNDANCY

There are mainly two options to implement the SQL database redundancy for the InAttend configuration database.

5.2.4.1 SQL Server Failover Clustering (recommended option)

Using SQL Server Failover Clustering means having no databases on the InAttend servers and only addressing one SQL server; the database redundancy is managed within this cluster. For setting up a SQL Server Failover Cluster please refer to the Microsoft SQL Server documentation.

5.2.4.2 SQL snapshot replication

An alternative solution is to implement a simple snapshot-like backup procedure. It can be configured on two SQL servers inside the InAttend server environment. This will require the Microsoft SQL Server Standard edition or above. Microsoft SQL Express doesn't support this setup.

In case of a failure of the primary database server the DAL service will automatically switch over to the secondary database server to enable InAttend clients to continue working. In a failover case the database restore job on the secondary database server should be disabled until the primary database server is available again.

The administration interface (WebAdmin) will display if connected to the secondary database server.

5.3 INATTEND CLIENT

5.3.1 INSTALLATION

During the installation of the InAttend client, the hostname to the InAttend server (Data Access Service) can be specified. To setup redundancy, both the primary and backup server needs to be specified.

The settings for the server locations can also be configured after InAttend has been installed, by using the DAL Configuration tool (DALConfigurationTool.exe) located in the same folder as the InAttend Client.

## 5.3.2 INATTEND CLIENT CONFIGURATION OF CMG DIRECTORY

If the InAttend Server has been configured with multiple data sources for CMG, the InAttend Client must also be configured to support this.

The dialog below shows the two CMG servers to search in, corresponding to the views defined in the CMG CM. Only one should be selected.
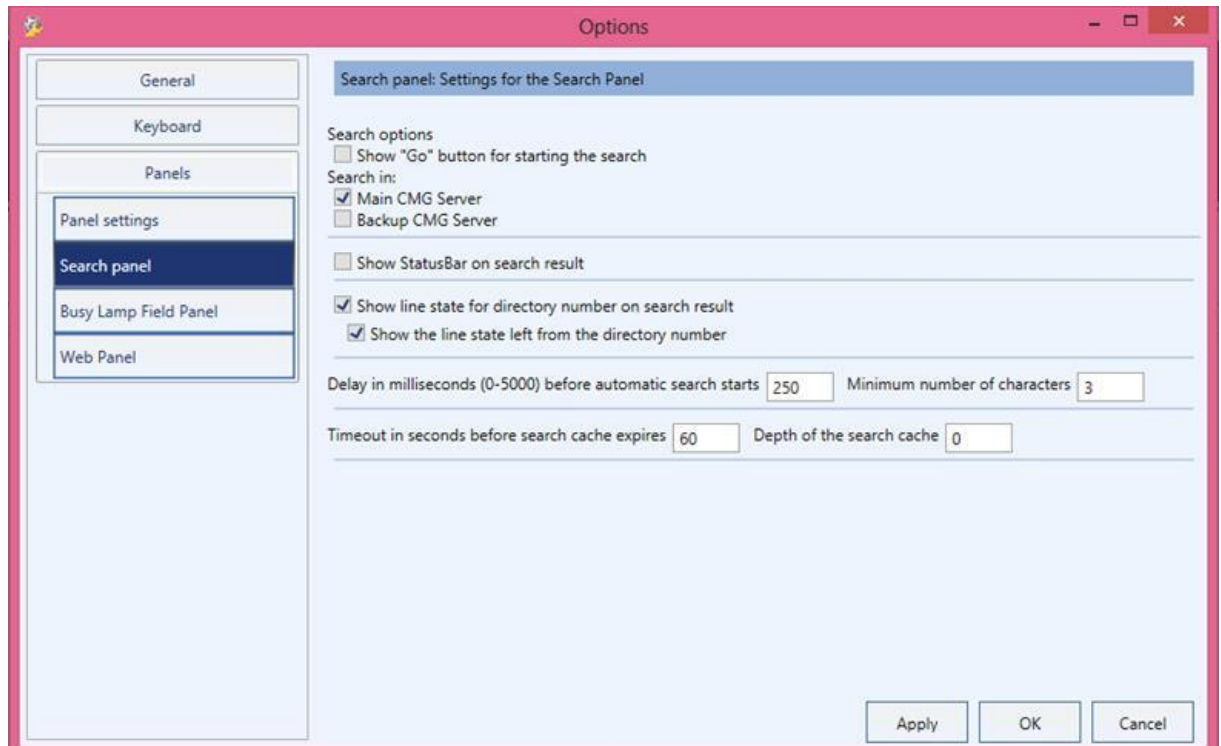
Pressing Alt+F2 gives the choice to switch between the data sources.

The name of the data source is generated by CMG CM and the CMG data source name in the InAttend CMG profile.
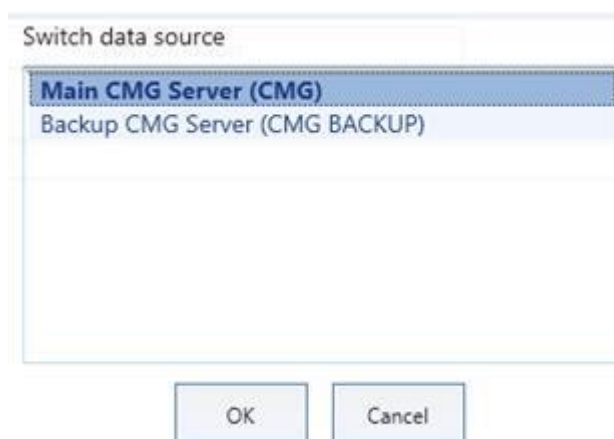
5.4 ACS

ACS redundancy is configured in TCA by first defining more than one host, then adding additional instances of Queue Manager, NeTS, Media server and Line state servers and assign these to each host. These additional instances of the ACS

components should be installed on separate servers and will be used as backup for redundancy.

An ACS system is partitioned into domains, and can be configured using TCA. For each domain a number of media servers can be specified. NeTS will allocate a media server in the list of media servers for the callee's domain, in specified order. It's possible to configure a media server to belong to several domains.

6 CONFIGURE SIP TRUNK AND CALL MANAGER

This chapter applies to both VMware High Availability and Hot-standby server redundancy solutions.

When more than one ACS is used, the call manager SIP trunk configuration must be configured to allow fallback to the secondary ACS server if the primary server is unavailable. The next sections describe how to make this configuration in ACS, Mitel MiVoice MX-ONE and Cisco Unified Call Manager.

For call managers that don't have native support for this, the DNS server can be configured with SRV records that point to the NeTS instances.

6.1 ACS

Use TCA to configure NeTS to use both a primary and secondary SIP trunk for call manager connectivity.

The first step is to add both the primary and secondary call manager to the Hosts configuration. The next step is to open the site configuration, and add SIP ports for both call managers to the private network settings as illustrated below.

The final step is to add the defined SIP ports to the domain, as illustrated below.

NeTS must be able to detect if a SIP trunk is alive or not. This can be configured in the Network Telephony Services Configuration tool. In the SIP tab, the setting *Option to check alive interval* should be set to 30 seconds as illustrated below.
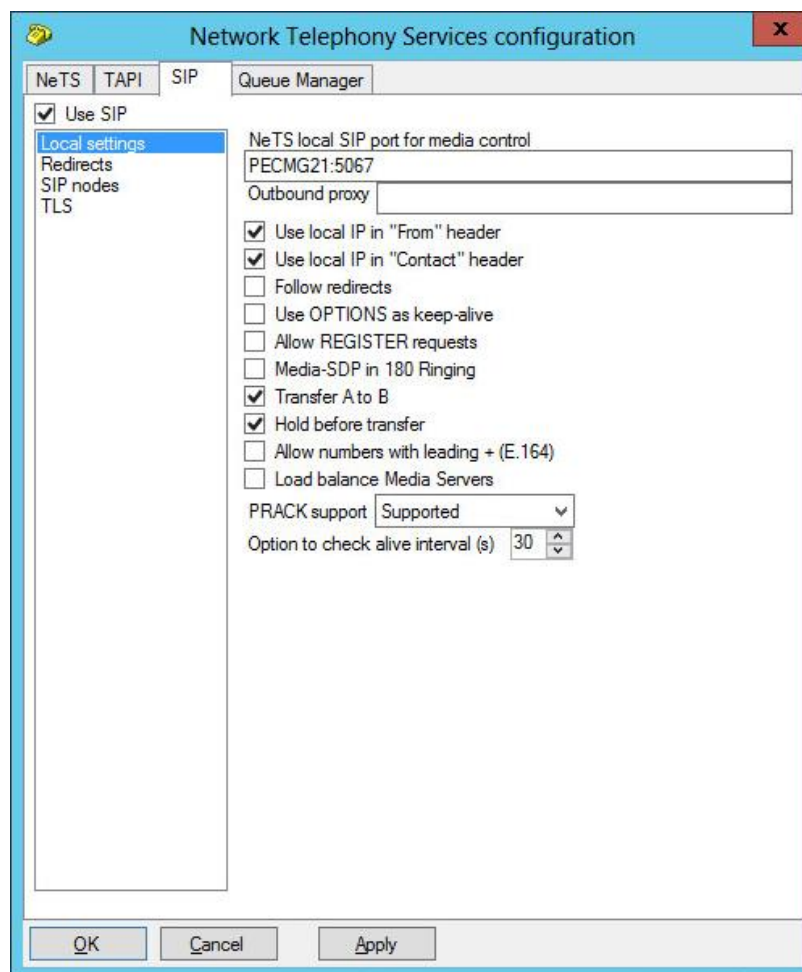
6.2 MITEL MIVOICE MX-ONE

In MX-ONE it's possible to initiate the external destination with alternative routing, so when the first choice is not available the alternative route will be used.

Note! License consideration for MX-ONE v6; TRUNK-SIP-CHANNEL (1/trunk initiated) and TRUNK-SIP-PRIVATE-SERVICES (1/route initiated), MX-ONE v5; EXTERNAL-LINE-SIP (1/route initiated), for the alternative route.

Add new route towards the redundancy ACS server using Manager Telephony Server MTS, in the same way as for the primary ACS route, under MTS / Telephony / External Lines / Route.

1. Add a new SIP Route using the InAttend profile.

2. Add a new Destination:

   a. Select Destination, the external number towards ACS, Click Next.

   b. Change:

- "Type of Seizure of External Line:" to "Seizure when minimum length attained".
- "Type of Called Number:" to "Unknown private"
- Click "Advanced" and check the checkbox for "Enable Enhanced Sent A-Number Conversion:"

c. Click Apply.

6.3 CISCO UNIFIED CALL MANAGER

This section describes how to configure redundant SIP trunks for Cisco Unified Call Manager.

Device - Trunk

Create your trunks to each ACS server

Call Routing - Rout/Hunt - Route Group

Create the Route Group to the ACS system and add the trunks to the Route group in the preferred order use Distribution Algorithm -Top Down

Call Routing - Rout/Hunt - Route List

Create a Route list and add the Route group to the list and check, *Enable this Route List*

Route List Configuration

Save | Delete | Copy | Reset | Apply Config | Add New

Route List Information

Registration:	Registered with Cisco Unified Communications Manager 10.105.87.7
IPv4 Address:	10.105.87.7

☑ Device is trusted

Name* `Blustar_121_122_Routlist`

Description `Blustar_121_122_Routlist`

Cisco Unified Communications Manager Group* `Default ▼`

☑ Enable this Route List (change effective on Save; no reset required)

☐ Run On All Active Unified CM Nodes

Call Routing - Rout/Hunt - Route Pattern

Create a route pattern for the numbers to the ACS system and choose the Route List created above

Route Pattern Configuration

Save | Delete | Copy | Add New

Status

ⓘ Status: Ready

Pattern Definition

Route Pattern*	`102X`
Route Partition	`< None > ▼`
Description	`ACS_10_105_87_121_Pattern_102X`
Numbering Plan	`-- Not Selected -- ▼`
Route Filter	`< None > ▼`
MLPP Precedence*	`Default ▼`
☐ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	`< None > ▼`
Route Class*	`Default ▼`
Gateway/Route List*	`Blustar_121_122_Routlist ▼` (Edit)
Route Option	⦿ Route this pattern
	◯ Block this pattern `No Error ▼`
Call Classification*	`OffNet ▼`
External Call Control Profile	`< None > ▼`

☐ Allow Device Override ☑ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority

SIP Profile Configuration

In the profile used for the trunk - SIP Option ping can be enabled by checking

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"