

Implementing a MiVoice 5000 Cluster Server

05/2020

AMT/PTD/PBX/0143/3/2/EN

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.

©Copyright 2015, Mitel Networks Corporation. All rights reserved.

Mitel® is a registered trademark of Mitel Networks Corporation.

Any reference to third party trademarks is for reference only and Mitel makes no representation of ownership of these trademarks.

CONTENTS

1	INTRODUCTION	3
1.1	REFERENCE DOCUMENTS	3
1.2	TERMINOLOGY	3
1.3	DEFINITION	4
2	OVERVIEW	5
2.1	ARCHITECTURE	5
3	APPLICATION	8
3.1	RESTRICTIONS.....	8
3.2	RULES AND PREREQUISITES	8
3.3	PRELIMINARY OPERATIONS	9
3.4	SUMMARY OF CLUSTER IMPLEMENTATION PHASES	9
3.5	DECLARING THE CLUSTER SERVER ID AND LICENCE	11
3.6	DECLARING THE ID ON MIVOICE 5000 SERVER TYPE NODES	11
3.7	DECLARING THE LDAP DIRECTORY	12
3.8	DEPLOYING THE CLUSTER SERVER	14
3.8.1	CHECKING SYNCHRONISATION WITH MIVOICE 5000 MANAGER.....	14
3.8.2	CREATING AND IDENTIFYING THE CLUSTER SERVER.....	14
3.9	DEPLOYING A NODE	19
3.9.1	INTRODUCTION	19
3.9.2	PREREQUISITES.....	19
3.9.3	PRELIMINARY OPERATIONS.....	20
3.9.4	CREATING AND IDENTIFYING THE NODE	21
3.10	SYNCHRONISING COMMON DATA BETWEEN THE CLUSTER SERVER AND NODES.....	25
3.11	DISTRIBUTING SIP LINK AND MEDIA SERVER LICENCES.....	26
3.11.1	DISTRIBUTION OF SIP LINK LICENCES	26
3.11.2	DISTRIBUTION OF MEDIA SERVER LICENCES	26
3.12	CONFIGURING MIVOICE 5000 MANAGER WITHOUT COMMUNITY MODE	27
3.12.1	CONFIGURING DIALLING RANGES (SDN MODE).....	27
3.12.2	CONFIGURING INSTALLATION NUMBERS (SDN MODE)	27
3.12.3	GENERATION	27
3.12.4	MANAGING PLACE AND DID NUMBERS FOR SUBSCRIBERS (SDN MODE)	28
3.12.5	CONFIGURING THE CLUSTER SERVER AND NODES (SDN MODE)	28
3.13	CONFIGURING MIVOICE 5000 MANAGER WITH COMMUNITY MODE.....	29
3.13.1	ACTIVATING COMMUNITY MODE	29
3.13.2	MANAGING COMMUNITIES.....	29
3.13.3	MANAGING "COMMUNITY" RIGHT IN OPERATOR MANAGEMENT	30
3.13.4	ASSIGNING COMMUNITIES TO SITES.....	30
3.13.5	CONFIGURING NUMBERING RANGES.....	30
3.13.6	CONFIGURING INSTALLATION NUMBERS	31
3.13.7	GENERATION	31
3.13.8	MANAGING PLACE AND DID NUMBERS FOR SUBSCRIBERS.....	31
3.13.9	CONFIGURING THE CLUSTER SERVER AND NODES (SDN MODE).....	31
3.14	MASSIVE CLUSTER SERVER SUBSCRIBER CREATION	32
3.15	MANAGING ENCRYPTION	33
3.15.1	INTRODUCTION	33
3.15.2	SELF-SIGNED CERTIFICATE	34
3.15.3	EXTERNAL CERTIFICATE	34
3.15.4	PREREQUISITES.....	34
3.15.5	IMPLEMENTING ENCRYPTION BY SELF-SIGNED CERTIFICATE	35
3.15.6	IMPLEMENTING ENCRYPTION BY EXTERNAL CERTIFICATE	37
3.15.7	IMPLEMENTING SITE-BASED ENCRYPTION	37
3.15.8	DEACTIVATING ENCRYPTION ON A MULTI-SITE NETWORK	38
3.15.9	ACTIVATING/DEACTIVATING ENCRYPTION ON A SITE	38
3.16	MAINTENANCE OPERATIONS ON A WORKING CLUSTER.....	40
3.16.1	ADDING A NODE TO A CLUSTER.....	40
3.16.2	DELETING A NODE FROM A CLUSTER	40
3.16.3	UPDATING CLUSTER SOFTWARE	41

3.16.4	CASE OF DEFENCE FOLLOWING A FAILED SOFTWARE UPDATE OR AFTER A ROLLBACK	41
3.16.5	BACKING UP THE CLUSTER DATA	42
3.16.6	RESTORING THE CLUSTER DATA	42
3.17	WORKING IN DUAL HOMING MODE IN A CLUSTER	44
3.17.1	DEFINING THE BACKUP NODE	44
3.17.2	CREATING UPDATING BACKUP SUBSCRIBERS ON THE NODES	45
3.18	REDUCED DIRECTORY DATABASE IN THE NODES	46
3.18.1	ACTIVATING AND CONFIGURING THE REDUCED DIRECTORY DATABASE	46
3.19	MANAGING SPECIAL NUMBERS ON A CLUSTER	48
3.20	MANAGING USER ACCOUNTS BY NODE	49
3.20.1	CREATING A USER ACCOUNT ON A NODE	49
3.20.2	OPERATION, RESTRICTIONS AND CASE OF DEFENCE	49
4	IMPLEMENTING SURVIVABILITY IN CLUSTER MODE	50
4.1	OVERVIEW	50
4.2	PRINCIPLE OF THE CONFIGURATION	53
4.3	RULES AND PREREQUISITES	53
4.4	IDENTIFYING THE TYPE OF NODE (SURVIVAL OR CLIENT)	53
4.5	DEACTIVATING A SURVIVAL NODE	54
4.6	DEACTIVATING A SURVIVAL NODE	54
4.7	DELETING A CLIENT NODE	54
4.8	ADDING A CLIENT NODE TO A COMMUNITY	54
4.9	REASSIGNING A SURVIVAL NODE IN A COMMUNITY	54
4.10	CHANGING THE COMMUNITY OF A SURVIVAL NODE	55
4.11	CHANGING THE COMMUNITY OF A CLIENT NODE	55
4.12	DELETING A COMMUNITY	55

1 INTRODUCTION

This document describes how to install and configure a MiVoice 5000 Cluster Server or XXL network from a MiVoice 5000 Manager.

1.1 REFERENCE DOCUMENTS

- XD - XL - XS - XS12 - XS6 - MiVoice 5000 Server - Functional description and hardware installation:
 - AMT/PTD/PBX/0150/EN
- Mitel 5000 Gateways and MiVoice 5000 Server - Commissioning:
 - AMT/PTD/PBX/0151/EN
- MiVoice 5000 Web Admin XD-XL-XS-XS12-MiVoice 5000 Server – Operating manual:
 - AMT/PTD/PBX/0080/EN
- Upgrading by Repository
 - AMT/PTD/PBX/0155 (minimum edition for R6.5)
- MiVoice 5000 Manager Installation manual
 - AMT/PTD/NMA/0040/EN
- MiVoice 5000 Manager User manual
 - AMT/PUD/NMA/0003/EN
- MiVoice 5000 - Multi-site management - Operating manual
 - AMT/PTD/PBX/0081/EN
- Mitel EX Controller and Mitel GX Gateway - Installation and Configuration
 - AMT/PTD/PBX/0173

1.2 TERMINOLOGY

Web Admin: MiVoice 5000 Web Admin.

User Portal: MiVoice 5000 User Portal.

BLF: Busy Lamp field.

CS: Cluster Server

DHCP: Dynamic Host Configuration Protocol.

DND: Do Not Disturb.

EX Controller: System integrating a deployment tool and a MiVoice 5000 Server.

ICG: Interconnection Management

HTTP: HyperText Transfer Protocol.

HTTPS: HTTP Secure.

Operating system: Operating System

SIP: Session Initiation Protocol.

TMA: Terminal Management Application.

URI: Uniform Resource Identifier.

URL: Uniform Resource Locator.

XML: eXtended Markup Language.

1.3 DEFINITION

Cluster: MiVoice 5000 telephony systems comprising physical systems (Mitel 5000 Gateways, Mitel 500, MiVoice 5000 Server or C2IC) or virtual systems (MiVoice 5000 Server) connected to a central MiVoice 5000 Server dedicated to general control, called Cluster Server.

Cluster Server: Physical or virtual MiVoice 5000 Server systems dedicated to global Cluster control. This system can be duplicated.

Node: Mitel 5000 Gateways, MiVoice 5000 Server, EX Controller or Mitel 500 system belonging to a Cluster and managed by the Cluster Server.

Cluster Server mode: Operating mode of an MiVoice 5000 Server dedicated to controlling the cluster after automatic configuration of MiVoice 5000 Manager.

Node mode: Operating mode which takes an Mitel 5000 Gateways, Mitel 500 or MiVoice 5000 Server in a cluster suite after MiVoice 5000 Manager is automatically configured.

Standalone mode: Node temporarily isolated from the Cluster Server and working in standalone mode.

Standalone node: Operating mode of an Mitel 5000 Gateways, Mitel 500 or MiVoice 5000 Server, a in single-site or multi-site configuration. A standalone system is a site in the sense of MOVACS.

Location: This attribute is added to the MiVoice 5000 Manager LDAP directory in order to assign a (geographic) location to each internal number.

2 OVERVIEW

2.1 ARCHITECTURE

The MiVoice 5000 Cluster Server solution is based on a star architecture made up of one cluster server and several nodes communicating via an IP network infrastructure.

The cluster server contains all the subscriptions (IP, TDM, analogue) as well as all the licences with a centralised configuration and common features on the entire cluster.

Each node is supervised by the cluster server. Adding a node to the architecture does not require reconfiguring the entire network like in the multi-site node; only one IP link is created between the cluster server and the node and the entire configuration is pushed by the cluster server to the node.

It forms a single-site, multi-node unit that can be deployed in a multi-site configuration.

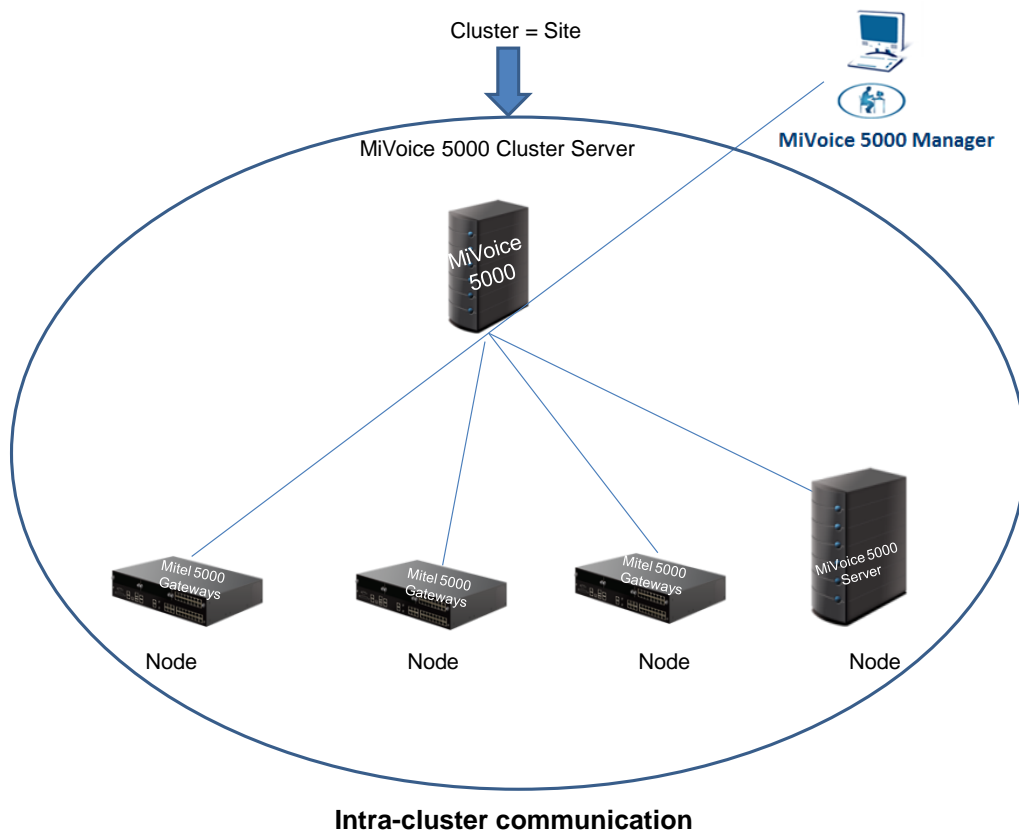
A cluster server always refers to an MiVoice 5000 Server type iPBX. A node refers to a MiVoice 5000 Server, Mitel 5000 Gateways, EX Controller or Mitel 500-type iPBX.

It is possible to duplicate the cluster server locally or geographically (LAN or WAN). This duplication is identical to multi-site mode.

When an MiVoice 5000 Server is configured as node, it may be made redundant (MiVoice 5000 Server duplication).

A MiVoice 5000 Manager is required to configure and manage a cluster which is seen as a site.

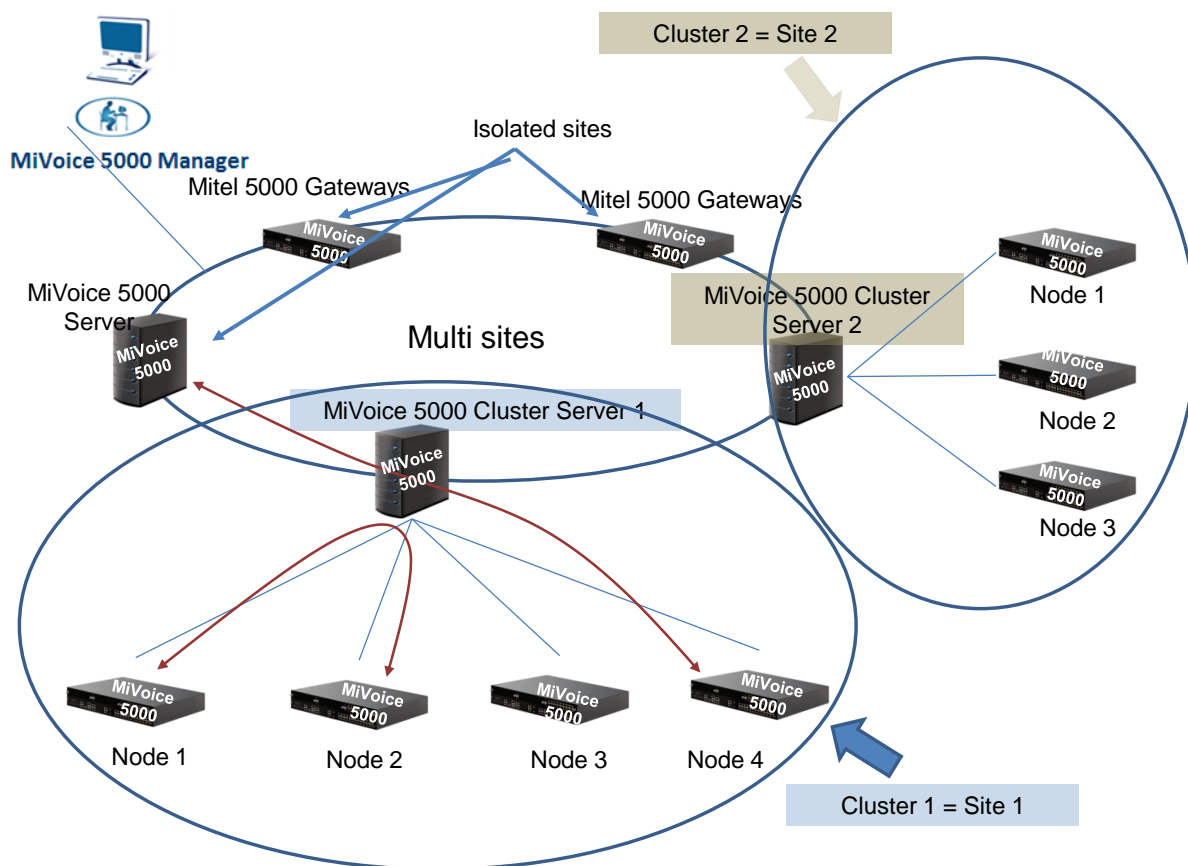
Architecture of a simple cluster



In the operating phase, the cluster server is the transit point for information exchanged between all the cluster nodes.

Multi-site architecture with several cluster servers

An MiVoice 5000 Cluster Server may be part of a multi-site network. In this case, the multi-site network is called **XXL network**.



Only the cluster server is interconnected to the other sites on the multi-site network. MOVACS inter-site signalling links are set up from the cluster server.

An XXL network architecture has the same characteristics as a multi-site architecture and, in particular, it supports interoperation with heterogeneous R6.1, R6.2, R6.3, R6.4 or R6.5.

➤ Before R6.5

In the same cluster, all systems (MiVoice 5000 Cluster Server and node) must be in the same software version. This software version must be greater than or equal to R6.1.

➤ From R6.5

In a Cluster, up to two different versions can coexist but must be at least R6.4.

A node can not have a lower version than the Cluster.

All the nodes of a cluster share the same "MOVACS site" number as the cluster server.

The XXL network architecture does not support SVL mode. (An SVL cannot be set up between a cluster server and a remote site)

A cluster server can be connected to 230 nodes maximum (Mitel 5000 Gateways, MiVoice 5000 Server, Mitel 500 and C2IC).

Each node is connected to the cluster server, but the nodes are not interconnected.

The nodes centralise accesses to the TDM networks and the TDM terminal connections.

Messages are broadcast inside the cluster (MOVACS signalling) by the cluster server.

Messages are broadcast to the multi-site network (MOVACS signalling via inter-site gateways) by the cluster server.

3 APPLICATION

3.1 RESTRICTIONS

The following subscriptions cannot be configured on a cluster server:

- Digital attendant console 6757 and the i2070 application.



Note: It is possible to meet the special needs to deploy an attendant console 6757 or i2070 on an additional Mitel 5000 Gateways set to multi-site with the cluster sever.



Note: The attendant console available in cluster mode is the CCMitel 5000 Web Attendant application.

- ISDN S0 and S2 subscriptions



Note: If these subscriptions must be used, they must be declared on a Mitel X Series R6.1 connected on a multi-site network with the cluster server. In R6.1, the ISDN S0 and S2 terminals may look like an IP terminal and set up an IP call with a remote terminal declared on the cluster server.

- DISA subscriptions
- HSCX subscription

3.2 RULES AND PREREQUISITES

The minimum MiVoice 5000 Manager version required to configure and manage a cluster is:

Before R6.5

MiVoice 5000 Manager: R6.1 – V3.1A

iPBX compatibility

- **R6.1:** cluster server, node and remote site in multi-site architecture with a cluster
- **R5.4:** remote site in a multi-site architecture with a cluster
- **R5.3:** remote site in a multi-site architecture with a cluster

From R6.5

MiVoice 5000 Manager: R6.5 - V3.3

The version of the nodes in a Cluster can be different from that of the Cluster Server but at least R6.4

IPBX Compatibility

- R6.1 minimum: Cluster Server, Node and Remote Site in Multisite with a Cluster

MiVoice 5000 Manager must be configured in such a way that the DID numbers are managed in directory characteristics (SDN mode). This mode is activated by default in the cluster server when a cluster is created via MiVoice 5000 Manager in the multi-site architecture.

SDN mode must be configured on the cluster before deployment by MiVoice 5000 Manager. When this SDN mode is activated on the cluster, all the nodes are automatically set to this mode.

Each iPBX is started in standalone mode and then configured by MiVoice 5000 Manager.

All the cluster components must be:

- In the same country
- Within the same time range

- Working with the same software release.



WARNING: All the components of a cluster must be synchronised on the same date and time. This must be done before any configuration (cluster server and node).

A cluster server always refers to an MiVoice 5000 Server type iPBX.

If the cluster is set to multi-site mode with one or more remote sites, this configuration must be performed after deploying the cluster. This multi-site configuration must be made on the cluster server only.

All the cluster subscriptions are declared on the cluster server, except IVR type subscriptions.

Software unlocking is centralised and must be implemented on the cluster server only.

In the case of a heterogeneous Cluster Server (R6.4 / R6.5), the Cluster Server in R6.5 adapts the licenses in the nodes (minimum version R6.4).

For WAN configurations between a node and the cluster server, it is very advisable to configure the geographic location (of the CAC server) on the node.

3.3 PRELIMINARY OPERATIONS

No subscriber should be declared on the iPBX nodes, except general-purpose subscribers and IVRs (if necessary).



WARNING: All the components of a cluster must be synchronised on the same date and time. This must be done before any configuration (cluster server and node).

3.4 SUMMARY OF CLUSTER IMPLEMENTATION PHASES

This paragraph gives a summary of the phases of the procedure.

For full details about each phase see the following sections.

On the Cluster Server

- Declaring the cluster server ID and licence. This ID is cluster-server specific.

On MiVoice 5000 Server nodes

- Declaring the ID

On MiVoice 5000 Manager

- Declaring the LDAP on MiVoice 5000 Manager
- Deploying the cluster server
 - Checking time synchronisation with MiVoice 5000 Manager
 - Creating and identifying the cluster server
- Deploying the nodes
 - Checking time synchronisation with MiVoice 5000 Manager
 - Starting the system in TOTAL mode, without subscriber creation
 - Creating and identifying nodes
- Synchronising common data automatically between the cluster server and nodes

On the Cluster Server

- Distributing SIP LINK and MEDIA SERVER licences

On MiVoice 5000 Manager

- Configuring MiVoice 5000 Manager SDN mode **without community mode**
 - Configuring dialling ranges (SDN mode).
 - Configuring installation numbers (SDN mode)

- Generation (updating the MiVoice 5000 Manager LDAP database)
- Managing place and DID numbers for subscribers (SDN mode)
- Configuring the cluster server and nodes (SDN mode)

OR

- Configuring MiVoice 5000 Manager SDN mode **with community mode**
 - Activating community mode in MiVoice 5000 Manager
 - Managing communities
 - Managing community right in operator management
 - Assigning communities to sites (cluster server, node, remote site)
 - Configuring dialling ranges (SDN mode)
 - Configuring installation numbers (SDN mode)
 - Generation (updating the MiVoice 5000 Manager LDAP database)
 - Managing place and DID numbers for subscribers (SDN mode)
 - Configuring the cluster server and nodes (SDN mode)
- Creating subscribers massively via the MiVoice 5000 Manager Excel form
- Managing encryption
- Carrying out maintenance operations on a working cluster
- Working in dual homing mode in a cluster
- Reduced directory database in the nodes
- Special numbers in a cluster server

3.5 DECLARING THE CLUSTER SERVER ID AND LICENCE

Menu **System>Info>Licences**

- Enter the cluster server ID provided with the system.

This ID is specific to the cluster server and starts with the code 0302xxxxxxxxxx to distinguish it from other standalone node and site type IPBXs.

- Declare the licence obtained from the installation code. Refer to MiVoice 5000 Installation document AMT/PTD/PBX/0151/EN.

Reminder:

- No other licence must be declared on the cluster nodes.
- The administrator enters the license into the Cluster Server. The license is copied to all nodes.
- As of R6.5, to manage multiple versions of MiVoice 5000 in the Cluster, the Cluster Server adapts the license to the node version when it copies it to the node

3.6 DECLARING THE ID ON MIVOICE 5000 SERVER TYPE NODES

Menu **System>Info>Licences**

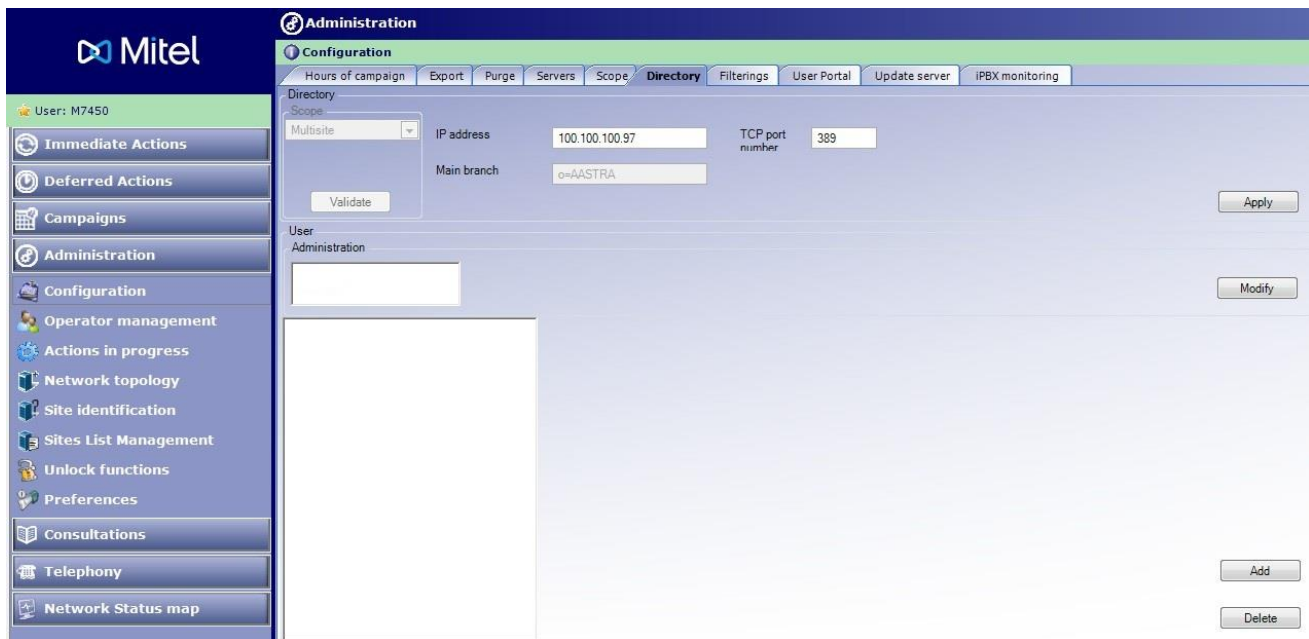
- Enter the ID on the MiVoice 5000 Server nodes as well as their IP address and IID number. Click Generate installation code to back up the ID.



Note: No check is made on the IID number or on the MiVoice 5000 Server type node.

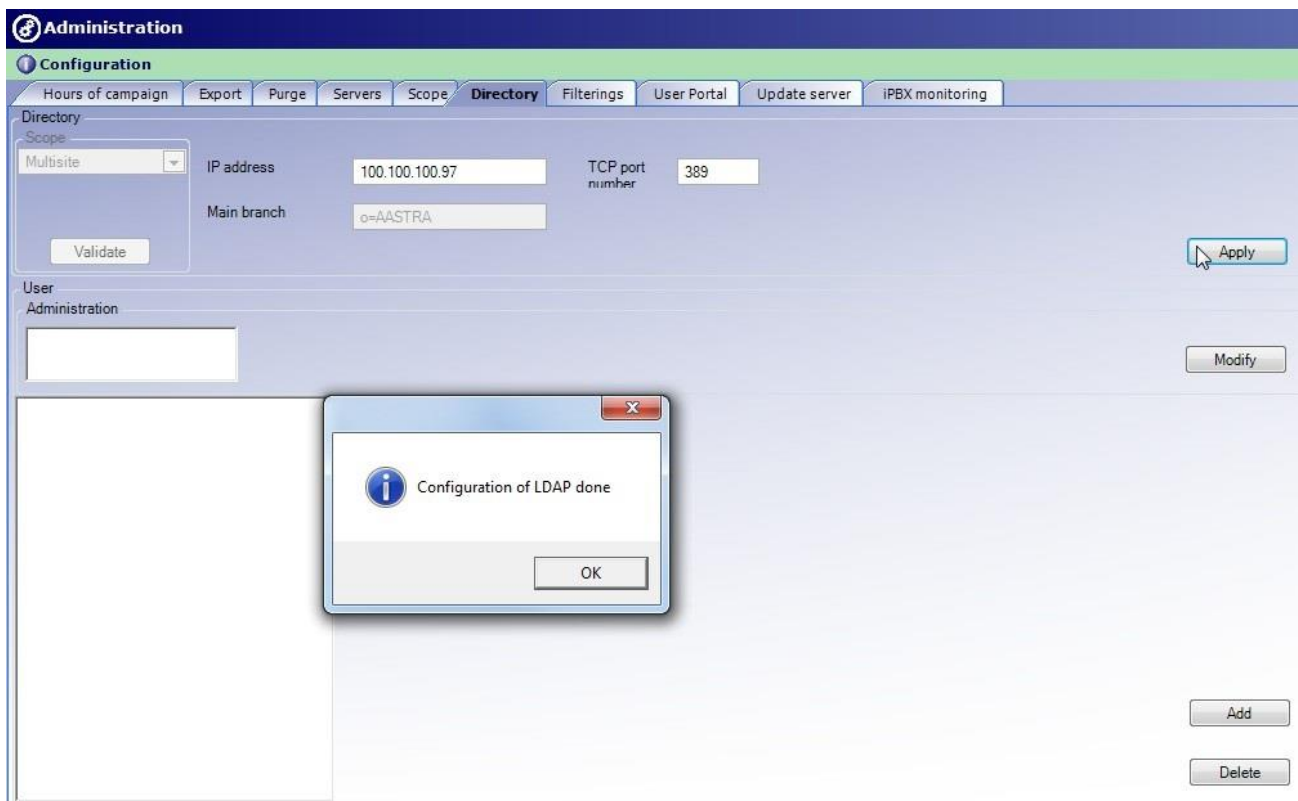
3.7 DECLARING THE LDAP DIRECTORY

The directory must first be configured in Menu **Administration>Configuration – Directory** tab, and the IP address defined (that of MiVoice 5000 Manager).



The screenshot shows the Mitel Administration interface. The left sidebar contains a menu with options: Immediate Actions, Deferred Actions, Campaigns, Administration, Configuration, Operator management, Actions in progress, Network topology, Site identification, Sites List Management, Unlock functions, Preferences, Consultations, Telephony, and Network Status map. The main area is titled 'Administration' and 'Configuration'. The 'Directory' tab is selected, showing fields for 'Scope' (Multisite), 'IP address' (100.100.100.97), 'TCP port number' (389), and 'Main branch' (o=Aastra). There are 'Validate', 'Apply', 'Add', and 'Delete' buttons. A 'User' section is also visible with a text input field and a 'Modify' button.

- Click **Apply**.



This screenshot shows the same Mitel Administration interface as the previous one, but with a mouse cursor clicking the 'Apply' button. A small dialog box is overlaid on the screen, displaying an information icon and the text 'Configuration of LDAP done'. The dialog has an 'OK' button.

- Click **OK**.

Result

Administration

Configuration

Hours of campaignExportPurgeServersScopeDirectoryFilteringsUser PortalUpdate serverIPBX monitoring

Directory

Scope

Multisite

Validate

IP address

100.100.100.97

TCP port number

389

Main branch

o=AASTRA

Apply

User

Administration

ROOT
CONFIG

Modify

i2052
i2070
twp
acp
billing
light Management

Add

Delete

3.8 DEPLOYING THE CLUSTER SERVER

Reminder: a Cluster Server can only be an MiVoice 5000 Server.



WARNING: If the cluster is set to multi-site configuration with one or more remote sites and the cluster server "site" number is bound to change, change it now.

3.8.1 CHECKING SYNCHRONISATION WITH MIVOICE 5000 MANAGER

All the cluster components must be synchronised on the same NTP server.

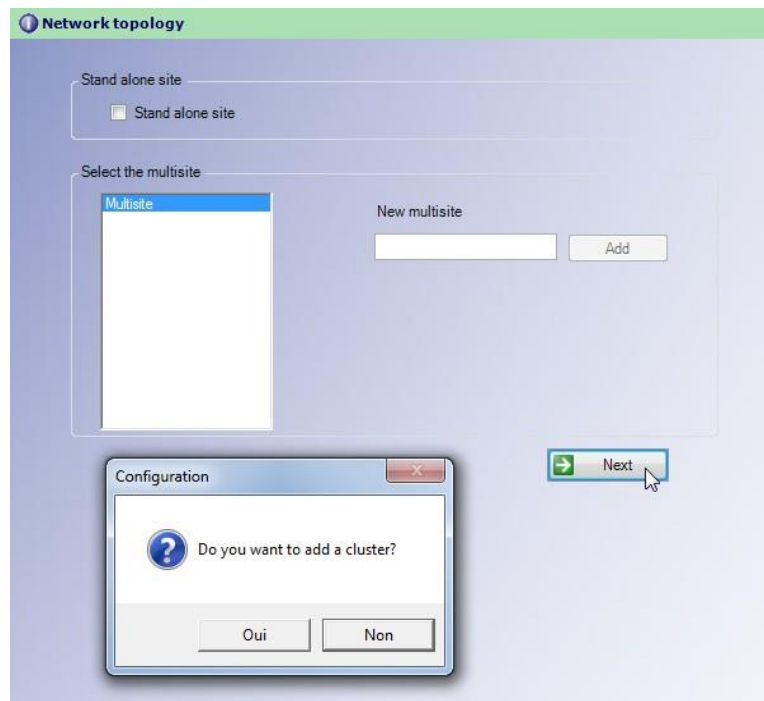
3.8.2 CREATING AND IDENTIFYING THE CLUSTER SERVER

Menu **Administration>Topology**

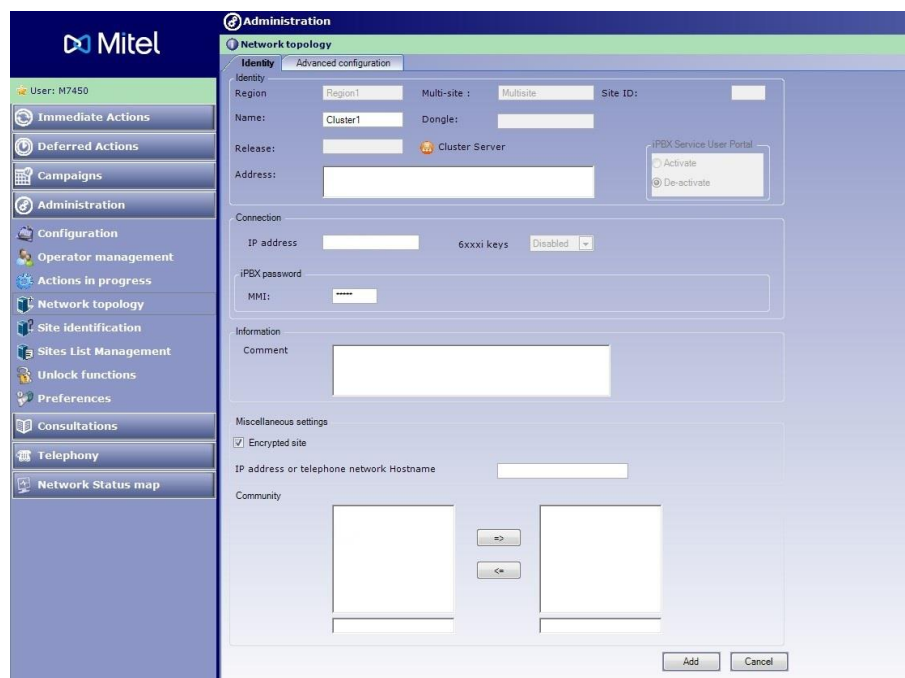
- Create a region (Region1)

- Create a multisite (Multisite1)

- Click **Next**.



- Answer **Yes** when asked whether to create a cluster server in this multi-site configuration.



Fill in the compulsory fields for creation:

- Name (Cluster1)
- IP address in the connection box (10.102.42.121)

Mitel

User: M7450

Immediate Actions

Deferred Actions

Campaigns

Administration

Configuration

Operator management

Actions in progress

Network topology

Site identification

Sites List Management

Unlock functions

Preferences

Consultations

Telephony

Network Status map

Administration

Network topology

IdentityAdvanced configuration

RegionRegion1Multi-site :MultisiteSite ID:

NameCluster1Dongle:

Release:Cluster ServerPBX Service User PortalActivateDe-activate

Address:

IP address10.102.42.1216xxxx keysDisabled

IPBX passwordMMI:

Information

Comment

Miscellaneous settings

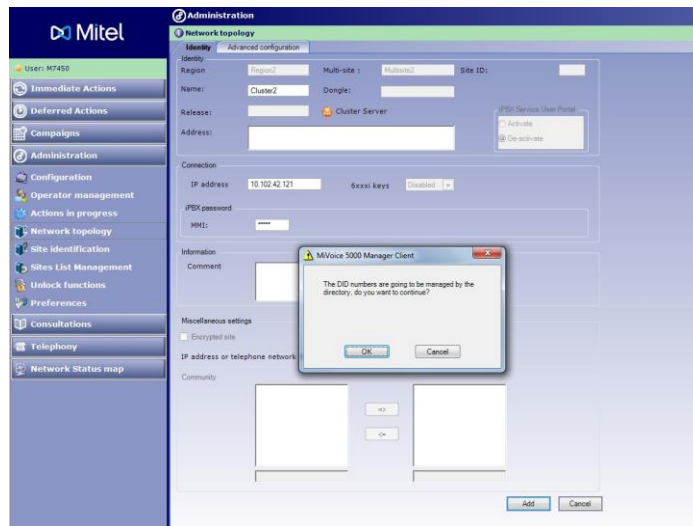
Encrypted site

IP address or telephone network Hostname

Community

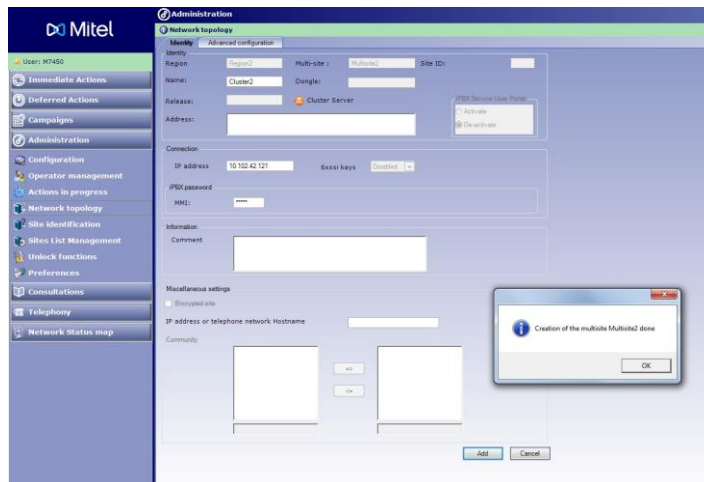
AddCancel

- Click **Add**.



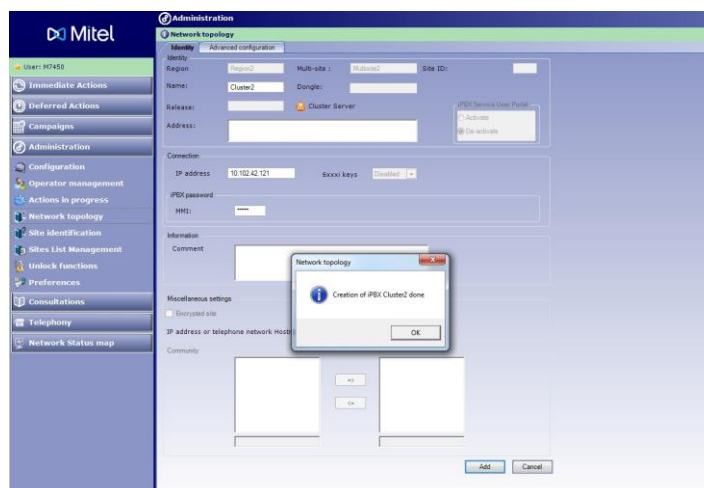
In a cluster server, calls and dialling must be managed in SDN mode, which corresponds to the default configuration of MiVoice 5000 R6.1.

- Click **OK**.



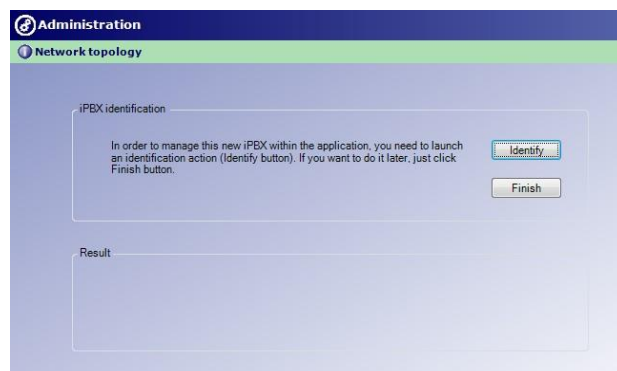
The multi-site network has been created.

- Click **OK**.



The cluster server has been created on the multi-site network.

- Click **OK**.
- Then start identifying the cluster server by clicking **Identify**.



The identification is made, and the cluster server information displayed:

Software version: R6.1 (an error message is displayed if the version is below R6.1)

Hardware type: MiVoice 5000 Server

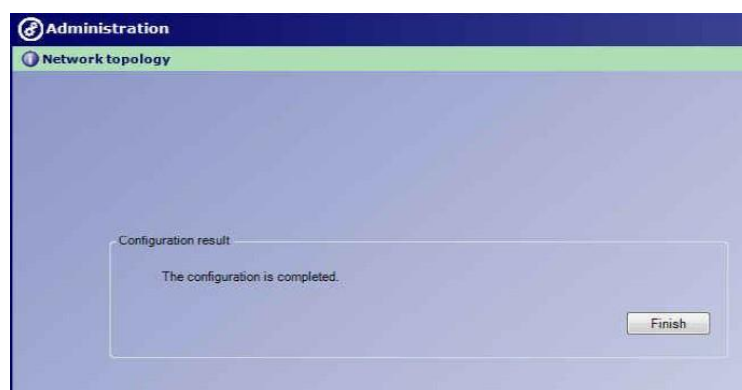


- Click **Continue**,

The following operations are carried out automatically by MiVoice 5000 Manager:

- MiVoice 5000 Manager is configured as SNMP manager in MiVoice 5000 Server (Menu Telephony service>System>Configuration>Alarms>Parameters).
- Configuring MiVoice 5000 Server in **Cluster Server** management mode (Menu 2.7 by manufacturer access)

The screen below is displayed, indicating that the operation has been successful.



- Click **Finish**.

The cluster server configuration has been completed and the topology screen is displayed again.



Note: After the configuration in Cluster Server management mode, the cluster server restarts.



WARNING: If necessary, the multi-site can be configured as from this moment.

3.9 DEPLOYING A NODE

3.9.1 INTRODUCTION

A node may be:

- A MiVoice 5000 Server
- A EX Controller
- A Mitel 5000 Gateways (with at least one VoIP card)
- A Mitel 500 (with at least one VoIP card)

The link between cluster server and node may be a LAN or WAN.

3.9.2 PREREQUISITES

Each node must contain a dongle ID (without licence).

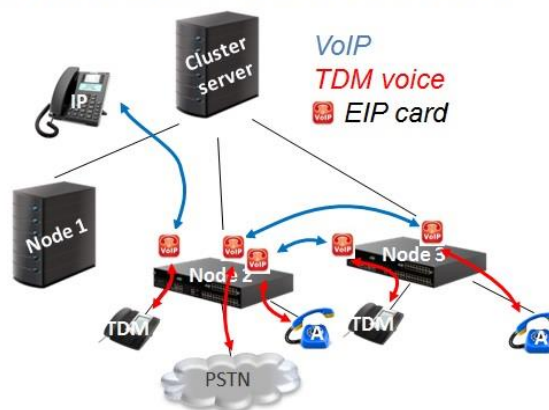


WARNING: The dongle ID on a MiVoice 5000 server type node must be declared (see Chapter 3.6).

If the node is a Mitel X Series or Mitel 500 type node, it must be fitted with a VoIP daughter card on the CPU card.

This VoIP card is compulsory because communications between a TDM terminal and IP terminal or TDM terminals and/or operator access on some distinct nodes use some VoIP resources on the nodes and voice is conveyed over IP.

Call processing with VoIP and TDM flows



The cluster server must be working before the nodes are deployed.

Since subscribers are managed from MiVoice 5000 Manager, no subscriber must be declared on the nodes except the general-purpose subscriber.

Subscriptions are centralised on the cluster server.



Note: Only one IVR subscription may be declared on a node after it is deployed via MiVoice 5000 Manager.

The software releases of the cluster server and node must be strictly identical.

On Mitel 5000 Gateways type nodes, the IVB must be **Disabled** (Menu 2.3.3.8).

3.9.3 PRELIMINARY OPERATIONS

3.9.3.1 *Checking synchronisation with MiVoice 5000 Manager*

All the components of the cluster, cluster server and nodes must be synchronised on the same date and time (NTP server).

3.9.3.2 *Starting the system in total mode, without subscriber creation*

No subscriber may be created except the IVR subscriber (if necessary).



Note: The IVR subscriber may be created after the node is deployed via MiVoice 5000 Manager.

On the system (MiVoice 5000 Server, Mitel 5000 Gateways, Mitel 500 or C2IC) implement a start in **Total** mode with Ctrl + I. For the complete procedure, see the MiVoice 5000 commissioning document AMT/PTD/PBX/0151.

With CTL + i, on the configuration screen for automatic start of the services set the value of the TMA service to 0.

With CTL + i, in Menu **Configuration / Subscribers**, reset all the subscriber creation parameters:

MITEL 5000 CONFIGURATION / Subscribers

| Do you want to change configuration Y/[N] ? Y |

- Answer **Y**
- Enter **0** for all the creation parameters as indicated below.

MiVoice 5000 Configuration / Subscribers

Creation (0/1) * :	0	
IVB creation (0/1) :	0	
Unified IVB (0/1) :	0	
First :		
Last :		
DID numbering length :		
First DID :		
First Public DID :		
Modem :		
IVB :		
HSCX Creation (0/1) :	0	
HSCX :		
DID HSCX :		
Common Subscriber :		
Common Bell :		
Additional Subscriptions :		
Subscriber password :	0000	

* : Mandatory field-----

Do you confirm (Y/N) (Press enter to reconfigure) ? **Y**

Only the general-purpose subscriber will be automatically created.

Check that only the general-purpose subscriber is declared in the iPBX menu **Subscribers>Subscriptions>Display by local number**.

3.9.4 CREATING AND IDENTIFYING THE NODE

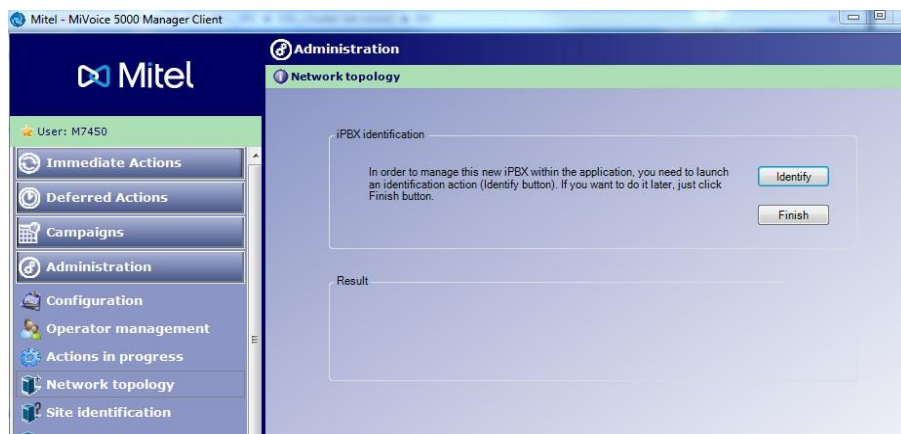
Menu **Administration>Network topology**

- Select the cluster in the multi-site configuration.
- In the column New **Multisite/Site/Node**, click **Add**.
- On the site configuration screen: enter the site/node name, and the corresponding IP address.

- Click **Add**.

The node has been created in Cluster1.

- Click **OK**.
- Then start identifying the node by clicking **Identify**.



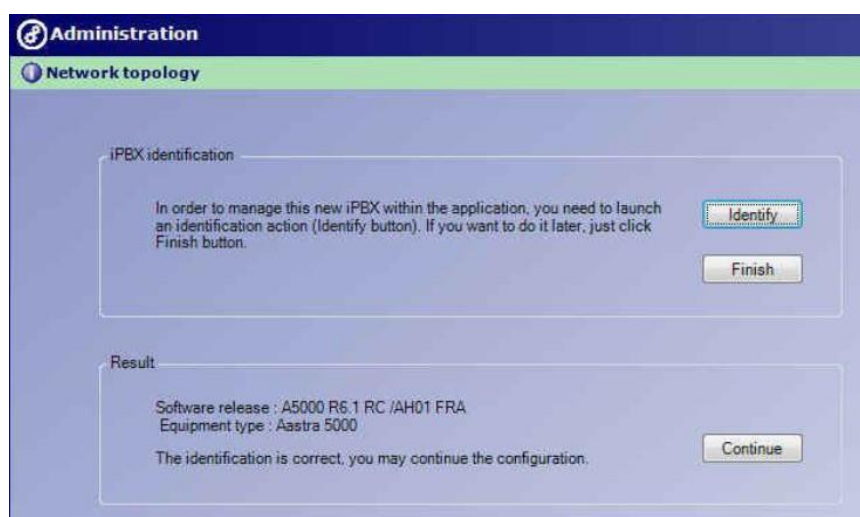
The identification is made, and the node information displayed:

Software version: R6.1 (an error message is displayed if the version is below R6.1)

Hardware type: MiVoice 5000 Server or Mitel 5000 Gateways.



WARNING: The node is only identified by MiVoice 5000 Manager if the cluster server on which depends this node had first been successfully identified.



- Click **Continue**.

The following operations are carried out automatically by MiVoice 5000 Manager:

- Checking that the node does not contain any subscriber except the general-purpose subscriber (otherwise, an error message appears and the node configuration is interrupted)
- Configuring the node number associated with the dongle ID in the cluster server Web Admin (Menu 2.7. by manufacturer access). The node number is automatically chosen by MiVoice 5000 Manager.



Note: The node number will be visible at the end of this procedure in the Web Admin banner and also in the MiVoice 5000 Manager topology.

- Configuring the cluster server IP address in the node Web Admin (Menu 2.7 by manufacturer access)
- Configuring the MiVoice 5000 Server or Mitel 5000 Gateways in **Node** management mode (Menu 2.7 by manufacturer access)

After this configuration, the node restarts. After the node is restarted, a start trap (PBX_INFOS) is sent to MiVoice 5000 Manager to inform it that the node has been correctly configured, and at the node's initiative a TCP connection is set up between the node and cluster server.

The automatic synchronisation tool for the common data between the cluster server and node will trigger a second restart of the node to take into account these common data which have just been updated on the node.

After the node has reconnected to the cluster server, the dual homing process starts five minutes later. The subscriber backed up on the server declared on this node is created (general-purpose subscriber).



Note: Later in the life of the cluster, all the backup subscribers of the cluster declared on this node will be created.

The node's general-purpose subscriber is updated so it is consistent with the one declared on the cluster server (the same phone number and the same technical parameters).



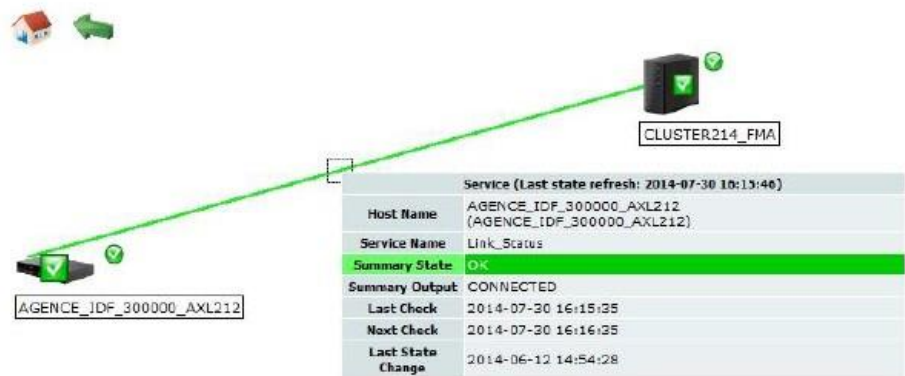
WARNING: If the directory number of the general-purpose subscriber is modified on the cluster server side, wait for (or trigger) dual homing realignment so it is taken into account on the nodes.

The screen below is displayed, indicating that the operation has been successful.

- Click **Finish**.

The node configuration has been completed.

Wait for the end of the second node restart. The status of the cluster server, node and the link between the cluster server and node is then visible from MiVoice 5000 Manager via Menu **Network supervision > Map**.



3.10 SYNCHRONISING COMMON DATA BETWEEN THE CLUSTER SERVER AND NODES

To facilitate the configuration of a cluster, a new mechanism automatically synchronises the common data between the cluster server and all the nodes attached to the cluster server.

The common data concerned are as follows (list not exhaustive):

- Feature classes
- PSTN and TL categories
- configuration data (DCF)
- Calendars
- Extension numbering plan
- Special numbers
- Barred numbers
- Encoding laws
- Intercom groups (ICG)
- Definition of centres and sites
- Message routing
-

These common data can only be modified via the cluster server Web Admin. Any modification made on the cluster server is taken into account in real time on all the nodes.

The corresponding nodes are hidden on the nodes (on the nodes, this data can only be displayed).

If the node cannot be reached during the modification of common data on the cluster server, the common data synchronisation tool automatically starts when the node reconnects. In this case, an automatic node restart will allow the common data updated on the node to be taken into account during synchronisation with the cluster server.

The following data must have been configured on each node, if necessary, according to network topology (list not exhaustive and configuration specific to each node):

- Call distribution management
- IVS scripts
- Attendants
- Incoming call numbering plan
- messages and announcements
- Equipment (external line, etc.)
- Network (routing, trunk group, etc.)
-

During maintenance operation on the cluster server or node (software upgrade, rollback to the valid version, code + data restore, data restore only), all the common data are synchronised between the cluster server and all the nodes attached to this cluster server.

3.11 DISTRIBUTING SIP LINK AND MEDIA SERVER LICENCES

On a cluster, the SIP LINKS and MEDIA SERVER licences may be distributed on the cluster server and on each node.

By default, these two licences are centralised on the cluster server. In this case, only the SIP links declared on the cluster server are working and only the ANNOUNCEMENT, CONFERENCE, IVR and IVB activated on the MEDIA SERVER of the cluster server are working.

If some SIP TRUNKs must be used on one or more nodes, the SIP TRUNK licences must be distributed over the cluster server and on these nodes.

If some MEDIA SERVER resources must be used on one or more MiVoice 5000 Server type nodes, the MEDIA SERVER licences must be distributed over the cluster server and on these MiVoice 5000 Server type nodes.

3.11.1 DISTRIBUTION OF SIP LINK LICENCES

On the cluster server, from Web Admin:

- Menu **Telephony service>System>Info>Licences**,
- **SIP links distribution** tab,
- Untick **Centralised licences**.
- Distribute the licences between the **Cluster Server** and each **Node** concerned.
- Click **Validation**.

These licences are used by the node in nominal mode (node connected to the cluster server) and also in standalone mode (node disconnected from the cluster server).



Note : An increase in SIP Trunk licenses on a cluster server may require a new distribution of licenses on the nodes.

3.11.2 DISTRIBUTION OF MEDIA SERVER LICENCES

On the cluster server, from Web Admin:

- Menu **Telephony service>System>Info>Licences**,
- **Media Server Distribution** tab,
- Untick **Centralised licences**.
- Distribute the licences between the **Cluster Server** and each MiVoice 5000 Server type **Node** concerned (first check that the ANNOUNCEMENT, CONFERENCE or IVR services are activated on the node).
- Click **Validation**.

These licences are used by the node in nominal mode (node connected to the cluster server) and also in standalone mode (node disconnected from the cluster server) for the following services:

- Network announcement (SIP TRUNK declared on an MiVoice 5000 Server type node)
- Subscriber announcement in standalone mode (dual homing function activated)
- Conference in standalone mode (dual homing function activated)
- IVR

3.12 CONFIGURING MIVOICE 5000 MANAGER WITHOUT COMMUNITY MODE

This procedure is used to configure MiVoice 5000 Manager (in SDN mode) without community mode.

This procedure is a summary of the operations described in detail in the document *DID number management AMT/PTD/PBX/0099/EN*.



WARNING: If you wish to create some communities in MiVoice 5000 Manager, go directly to Chapter 3.13.



Note: SDN mode is compulsory on a cluster server.

3.12.1 CONFIGURING DIALLING RANGES (SDN MODE).

Menu **Telephony>Numbering plan>Numbering range**

The numbering ranges are configured through an import/export operation.

Import is always global.

To add a numbering range, the administrator exports the current configuration and adds the new ranges to the file before re-exporting it.

3.12.2 CONFIGURING INSTALLATION NUMBERS (SDN MODE)

Menu **Telephony>Numbering plan>Installation numbers**

The installation numbers are configured through an import/export operation.

For the first configuration, click Export to retrieve the file frame and, thus, fill it in and then import it.

The import/export file is used to fill in the different **Places** (IID). A **Place** explicitly describes a site, and this generally corresponds to a geographic location.

3.12.3 GENERATION

Prerequisites on the Cluster Server:

- From the cluster server Web Admin, feature class and TL management must be set to **AUTO YES** in the **System** tab of Menu **Telephony service>Subscribers>Rights>General settings**.
- All the subscribers to be deployed must have at least one directory record (at this stage, this only concerns general-purpose subscribers).

From MiVoice 5000 Manager:

- Then start multi-site generation via MiVoice 5000 Manager from Menu **Administration>Network topology**.

3.12.4 MANAGING PLACE AND DID NUMBERS FOR SUBSCRIBERS (SDN MODE)

Each subscriber must be assigned a **Place**.



Note: At this stage, only the general-purpose subscription must be assigned a place via the MiVoice 5000 Manager subscriber management menu.

For a new installation and for all the subscriptions to be created on the cluster server, this assignment is made via the MiVoice 5000 Manager massive creation Excel form (see Chapter 3.14).

3.12.5 CONFIGURING THE CLUSTER SERVER AND NODES (SDN MODE)

Proceed as follows:

- Activate SDN mode on the cluster server:
Menu **Telephony service>Subscribers>Rights>General settings**
Tick the parameter **DID number managed by MiVoice 5000 Manager**

At the end of the cluster server configuration in SDN mode, the different nodes are automatically configured in this mode (menu hidden on the nodes).

- Configure the LDAP database connections.
Menu **Telephony service>Subscribers>Directory>Parameters>Connections**
Check the configuration of the **Configuration**, **Name resolution** and **Dialling service**

tabs. The parameters for connection to the LDAP databases are automatically configured on the different nodes (menu hidden on the nodes). Activate the different directory services on the nodes as well as the reduced database, if necessary.

- Locate the number dialling service:
Menu **Telephony service>Network and links>Multi-sites>Location of the services>Other services**
Check the configuration of the **TRANSLATION OF NUMBERS** parameter.
- Activate Directory search for calls arriving on the SIP TRUNK used on the cluster server:
Menu **Telephony service>Network and links>Network>Trunk groups>Characteristics**.
Check that the **Search via directory** parameter is ticked.



Note: If necessary, make this check on the different SIP or TDM TRUNKS configured or used on the different nodes.

- Activate Directory search for outgoing calls presented on the SIP TRUNKs used on the cluster server:
Menu **Telephony service>Network and links>Network>AID handling>Outgoing handling**.
Check that the parameter **AID SET USING DID NUMBER** is set to **YES**.



Note: If necessary, make this check on the different SIP or TDM TRUNKS configured or used on the different nodes.

- Configure the number translators: it may be necessary to translate the number received or sent.

3.13 CONFIGURING MIVOICE 5000 MANAGER WITH COMMUNITY MODE

This procedure is used to configure MiVoice 5000 Manager (in SDN mode) with community mode activated. This procedure is a summary of the operations described in detail in the document *DID number management AMT/PTD/PBX/0099/EN*.



Note: SDN mode is compulsory on a cluster server.

Community mode is optional and a concept introduced in MiVoice 5000 Manager only.

Community = community of subscribers sharing the same numbering range and the same place

Community mode is basically used to:

- Limit the perimeter of MiVoice 5000 Manager operators to a subgroup of subscribers defined on the same site
- Facilitate the choice of subscriber number during creation, by filtering the corresponding number ranges
- Facilitate the configuration of the backup site (dual homing)
- Facilitate the choice of hardware resources for analogue and digital subscribers.

Each Community is, for instance, linked to a geographic area.

The Community is assigned to systems (cluster server, node, remote site) which share the same numbering range.

3.13.1 ACTIVATING COMMUNITY MODE

Community mode is activated from the multi-site configuration in Menu **Administration>Topology**.

- Select the multi-site configuration (Cluster1).
- In the Type of DID number management area:
- Modify the DID plan number (if necessary).
- Tick the **Community mode** box to activate the mode on the multi-site network then click **Apply**. Confirm the message by clicking **OK**.

3.13.2 MANAGING COMMUNITIES

A Community is defined by key and a label, and possibly one or more aliases.

Possible actions on Communities are:

- Add Community.
- Modify Community (only for the label and alias).
- Delete Community.
- Export the parameters of configured Communities to a .csv file.
- Import a .csv file: This import only adds or modifies a Community. Deletions can only be made through an individual action in the MiVoice 5000 Manager Community management menu.

Communities are always defined from the multi-site, in Menu **Administration>Topology**.

- Select the multi-site configuration (Cluster1).
- Click Community.

Add one or more associated communities to the multi-site configuration (Cluster1) by clicking **Community**.

3.13.3 MANAGING "COMMUNITY" RIGHT IN OPERATOR MANAGEMENT

Community is subject to operator right.

Menu **Administration>Operators management**.

- Select the operator from the list.
- Click **Community rights**.
- Grant the user in question rights over one or more communities then click **Apply**.
- Then click **Apply** on the operator management screen to validate the assigned rights.
- Repeat this operation for each operator.

3.13.4 ASSIGNING COMMUNITIES TO SITES

After creating the communities, assign them to the systems (cluster server, node, remote site) before importing the numbering plan.

Depending on system type, some rules apply.

Cluster Server:

- Several Communities may be assigned to it.
- The Cluster Server also inherits the Communities assigned to the nodes of this same cluster.

Node: only one Community may be assigned to it.

Multi-site site: several Communities may be assigned to it.

Menu **Administration>Topology**

- Select the site (cluster server, node or standalone site)
- Click **Configuration**
- In the **Miscellaneous parameters – Community** area:
 - Select the Community concerned from the list.
 - Click on =>.
 - The list on the right is filled in.
- Click **Modify**.

3.13.5 CONFIGURING NUMBERING RANGES

Number ranges are configured (like in SDN mode) through import/export.

The differences in terms of import/export compared to SDN mode without community are:

- Deletion of the site associated with the numbering range
- Addition of the Community key
- Addition of the notion of default numbering range.

During file import, a check is made to ensure that:

- The file format is correct
- All the sites have a community
- All the communities have at least one numbering segment
- All the communities have one default numbering range
- The numbering ranges are not overlapping.
- The subscribers available in the database have a number belonging to a numbering range
- There is a consistency between the subscribers' numbers and community.

3.13.6 CONFIGURING INSTALLATION NUMBERS

Installation numbers are configured (like in SDN mode) through import/export.

The differences in terms of import/export compared to SDN mode without community are:

- Addition of the Community key
- Addition of the notion of default place.

During file import, a check is made to ensure that:

- The file format is correct
- All the communities have a place
- All the communities have a default place
- No place used in a subscription is deleted.

3.13.7 GENERATION

This phase is necessary for updating the MiVoice 5000 Manager database.

Prerequisites on the Cluster Server:

- Feature class and TL management must be set to **AUTO YES** in the **System** tab of Menu **Telephony service>Subscribers>Rights>General settings**.
- All the subscribers to be deployed must have at least one directory record (at this stage, this only concerns general-purpose subscribers).

Then start multi-site generation from Menu **Administration>Network topology**.

3.13.8 MANAGING PLACE AND DID NUMBERS FOR SUBSCRIBERS

The Community is linked to a Place. It is while configuring the Place in the subscription that the Community is initialised in the subscription.



Note: At this stage, only the general-purpose subscription must be assigned a place via the MiVoice 5000 Manager subscriber management menu.

For a new installation and for all the subscriptions to be created on the cluster server, this assignment is made via the MiVoice 5000 Manager massive creation Excel form (see Chapter 3.14).

3.13.9 CONFIGURING THE CLUSTER SERVER AND NODES (SDN MODE)

Proceed as follows:

- Activate SDN mode on the cluster server:
Menu **Telephony service>Subscribers>Rights>General settings**
Tick the parameter **DID number managed by MiVoice 5000 Manager**

At the end of the cluster server configuration in SDN mode, the different nodes are automatically configured in this mode (menu hidden on the nodes).

- Configure the LDAP database connections.
Menu **Telephony service>Subscribers>Directory>Parameters>Connections**
Check the configuration of the **Configuration**, **Name resolution** and **Dialling service**

tabs. The parameters for connection to the LDAP databases are automatically configured on the different nodes (menu hidden on the nodes). Activate the different directory services on the nodes as well as the reduced database, if necessary.

- Locate the number dialling service:
Menu **Telephony service>Network and links>Multi-sites>Location of the services>Other services**
Check the configuration of the **TRANSLATION OF NUMBERS** parameter.

- Activate Directory search for calls arriving on the SIP TRUNK used on the cluster server:
Menu **Telephony service>Network and links>Network>Trunk groups>Characteristics**.
Check that the **Search via directory** parameter is ticked.



Note: If necessary, make this check on the different SIP or TDM TRUNKS configured or used on the different nodes.

- Activate Directory search for outgoing calls presented on the SIP TRUNKs used on the cluster server:
Menu **Telephony service>Network and links>Network>AID handling>Outgoing handling**.
Check that the parameter **AID SET USING DID NUMBER** is set to **YES**.



Note: If necessary, make this check on the different SIP or TDM TRUNKS configured or used on the different nodes.

- Configure the number translators: it may be necessary to translate the number received or sent.

3.14 MASSIVE CLUSTER SERVER SUBSCRIBER CREATION

All the cluster server subscribers are declared from the massive MiVoice 5000 Manager creation form:

From Menu **Telephony>Subscribers management>Massive creation – Massive creation** tab.

Massive creation is site-based and is performed through import/export.

- Select the Cluster Server.
- Click **New** to export the file to be configured.
- Then fill in the different tabs.

In the **DIRECTORY** tab, the **Place** column is used to assign a geographic location to each subscriber. The Community/place combo box corresponds to the configuration made in the previous phases.

- Click **Import** in the Import area to import the configured file again.
- Click **Next** to start the massive action.
- Click **Program**.

The maximum number of subscribers that can be declared for an Excel form is limited to 500. Depending on the number of subscribers to be declared on the cluster server, define as many Excel forms as necessary.

3.15 MANAGING ENCRYPTION

3.15.1 INTRODUCTION

As of R3.1, signal encryption is managed from MiVoice 5000 Manager.

Signal encryption is based on:

- Inter-site links (especially between a cluster server and a remote site)
- Links between the cluster server and nodes (intra-cluster links)

The TLS protocol is used carry out this encryption.

Two encryption modes are proposed by MiVoice 5000 Manager:

- Encryption through self-signed certificate
- Encryption through external certificate

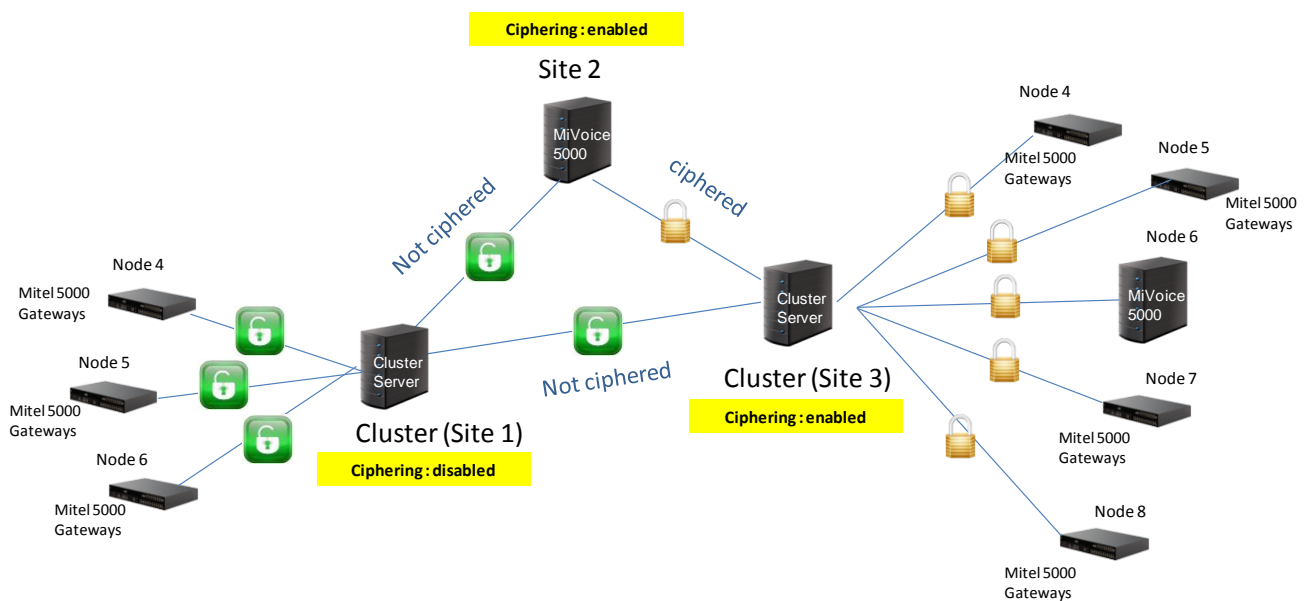
In MiVoice 5000 Manager, encryption is a multi-site-based configuration parameter, but the administrator may or may not allow site-by-site encryption.



WARNING: In case of encryption inside the cluster, the nodes adopt the properties of the cluster server. If encryption is activated on the cluster server from MiVoice 5000 Manager, it is then implicitly activated on the nodes.



WARNING: Encryption works between two systems (cluster server and remote site) only if it is activated on the systems concerned.



3.15.2 SELF-SIGNED CERTIFICATE

In this operating mode, the certificate is fully managed by the systems (cluster server, remote sites). When the certificate expires, an expiration alarm is sent to MiVoice 5000 Manager for information, and a new self-signed certificate automatically generated by the system.

3.15.3 EXTERNAL CERTIFICATE

In this operating mode the external certificate is imported into MiVoice 5000 Manager. The import file (file p12) contains the private key and certificate for MiVoice 5000 Manager, as well as the certificate from the certification authority.

MiVoice 5000 Manager generates system certificates (cluster server and remote sites) and private keys from the information contained in the external certificate and sends them to the systems.



Note: The certificate import file format is PKCS#12..

3.15.4 PREREQUISITES

MiVoice 5000 Manager, the cluster (Cluster Server and all the nodes) as well as all the remote sites must be synchronised via an NTP server:

- Same date
- Same time
- Same minute

In case of malfunction due to certificate deployment, check the date / time / minute synchronisation.



Note: As a precautionary measure, in case of encryption via external certificate, the certificate generated is backdated by 24 hours in order to limit the problems.

The status of the **encryption** licence must be **AUTHORISE** on the Cluster Server and the remote sites on which encryption will be configured as of MiVoice 5000 Manager (Menu Telephony service>System>Info>Licences).

On the cluster server and remote sites on which encryption has been configured, the alarms **AlmLocPers** and **IN ALARM** must be configured to generate some traps returned to MiVoice 5000 Manager:

- Menu Telephony service>System>Configuration>Alarms>Individualized configuration:
 - Detection in **LOCAL SITE**
 - BY SBL GROUP **MANAGEMENT**
 - Of alarm **.....**
 - Routed to **SNMP TRAP**
- Click **Select item**.
- Check that the alarms **AlmLocPers** and **IN ALARM** are actually sent.

A first trap will be issued when the external or self-signed certificate expires, and a second trap will be issued daily two weeks before the external certificate expires.

3.15.5 IMPLEMENTING ENCRYPTION BY SELF-SIGNED CERTIFICATE

This procedure is used to activate encryption by self-signed certificate for all the sites on the multi-site network: cluster server, nodes and remote sites belonging to the same multi-site network.

On MiVoice 5000 Manager, Menu **Administration>Network topology**

- Select the multi-site on which encryption through self-signed certificate must be configured then click **Configuration**.
- Tick **encryption** to authorise encryption on the multi-site network.
- Set **Type of encryption** to **Self signed**.
- Click **Apply** then **OK**: this enables the Generate certificates button.



- Click **Certificate generation**.



- To the question asked, select **Generate certificates for all the sites on the multi-sites** then click **Confirm**.
- In the MiVoice 5000 Manager operations log, a message is used to check the success of the certificate generation operation.

MiVoice 5000 Manager sends the certificate generation command to the systems defined in MiVoice 5000 Manager (Cluster Server, nodes and remote sites), and the certificate is generated locally on each system.

Encryption through self-signed certificate is then operational on all the multi-site systems.

3.15.5.1 Checking the encryption configuration on each system

- Go to Menu Telephony service>Network and links>Quality of service>Encryption and IP parameter of Web Admin.
- Check that:
 - The parameter **dates of active certificate validity** is correct.
 - The parameter **name of the certification authority** corresponds to the system IP address.
 - The parameter **inter iPBX encryption** is ticked.
 - The parameter **self-signed certificate** is ticked.

Ciphering and IP settings

Telephony service>Network and links>Quality of service>Ciphering and IP settings (4.4.5)

IP parameters and ciphering Certificates

bytes TOS voice (hexa)	B8
bytes TOS signaling (hexa)	A0
VLAN voice priority	6
VLAN signaling priority	6
time to live of the IP datagram	64

Signalling and voice ciphering

function state FORBIDDEN BETWEEN SETS

dates of active certificate validity :

start 20/03/15 19:42

end 19/03/16 19:42

name of the certification authority :

100.40.81.40

voice terminals ciphering ☐

inter iPBX ciphering ☒

self signed certificate ☒

Certificate regeneration

Voice ciphering (i7xx)

function state KEY NON EXISTENT

updated on: ed:

working mode SLAVE ▼

encryption ALLOWED ▼

3.15.6 IMPLEMENTING ENCRYPTION BY EXTERNAL CERTIFICATE

This procedure is used to activate encryption by external certificate for all the sites on the multi-site network: cluster server, nodes and remote sites belonging to the same multi-site network.

On MiVoice 5000 Manager, Menu **Administration>Network topology**

- Select the multi-site on which encryption through external certificate must be configured then click **Configuration**.
- Tick **encryption** to authorise encryption on the multi-site network.
- Set **Type of encryption** to **Import**.
- Select the external certificate to be imported.
- Enter and confirm the password associated with the certificate.
- Click **Import** to import the certificate into MiVoice 5000 Manager.
- Click **Apply** then **OK**: this enables the Generate certificates button.
- Click **Certificate generation**.
- To the question asked, select **Generate certificates for all the sites on the multi-sites** then click **Confirm**.
- In the MiVoice 5000 Manager operations log, a message is used to check the success of the certificate generation operation.

MiVoice 5000 Manager generates system certificates (cluster server, nodes and remote sites) and private keys from the information contained in the external certificate and sends them to each system.

Encryption through external certificate is then operational on all the multi-site systems.

3.15.6.1 *Checking the encryption configuration on each system*

- Go to Menu Telephony service>Network and links>Quality of service>Encryption and IP parameter of Web Admin.
- Check that:
 - The parameter **dates of active certificate validity** is correct.
 - The parameter **name of the certification authority** is correct.
 - The parameter **inter iPBX encryption** is ticked.
 - The parameter **self-signed certificate** is unticked.

3.15.7 IMPLEMENTING SITE-BASED ENCRYPTION

This procedure is used to activate site-based encryption through self-signed or external certificate. This activates encryption on certain sites only.

On MiVoice 5000 Manager, Menu **Administration>Network topology**

- Select the multi-site on which encryption must be configured then click **Configuration**.
- Tick **encryption** to authorise encryption on the multi-site network.
- Set **Type of encryption** to **Self signed** or **Import**.
- Import the external certificate if necessary.
- Click **Apply** then **OK**.
- Click **Certificate generation**.
- To the question asked, select **Generate certificates only for the sites which already have the encryption property** then click **Confirm**.
- Click **Return**.

- Select the site on which encryption must be configured then click **Configuration**.
- Tick the parameter **Encrypted site** to activate encryption on the site concerned, then click **Modify**. Click **OK** to confirm the modification.
- Validate the modification confirmation message by clicking **OK**.
- Validate the message confirming the encryption activation on the site by clicking **OK**.
- In the MiVoice 5000 Manager operations log, a message is used to check the success of the certificate generation operation.
- For each site, repeat the last five operations.



WARNING: Encryption works between two systems (cluster server and remote site) only if it is activated on the systems concerned.



Note: You can regenerate the certificate on a site on which encryption is already active by clicking **Certificate**.

3.15.8 DEACTIVATING ENCRYPTION ON A MULTI-SITE NETWORK

This procedure is used to deactivate encryption for all the sites of the multi-site network: cluster server, nodes and remote sites belonging to the same multi-site network.

On MiVoice 5000 Manager, Menu **Administration>Network topology**

- Select the multi-site on which encryption must be deactivated then click **Configuration**.
- Untick **encryption** to deactivate encryption on the multi-site network.
- Click **Apply** then **OK**.
- Validate the message confirming the encryption deactivation on the multi-site network by clicking **OK**.

3.15.9 ACTIVATING/DEACTIVATING ENCRYPTION ON A SITE

3.15.9.1 *Deactivating encryption on a site*

If encryption has been activated on all the sites of the multi-site network, this procedure is used to deactivate encryption on a site basis.

On MiVoice 5000 Manager, Menu **Administration>Network topology**

- Select the site (cluster server or remote site) of the multi-site network on which encryption must be deactivated then click **Configuration**.
- Untick the parameter **Encrypted site** to deactivate encryption on the site concerned, then click **Modify**. Click **OK** to confirm the modification.
- Validate the modification confirmation message by clicking **OK**.
- Validate the message confirming the encryption deactivation on the site by clicking **OK**.



WARNING: Encryption works between two systems (cluster server and remote site) only if it is activated on the systems concerned.

3.15.9.2 *Activating encryption on a site*

If site-based encryption has been activated, this procedure is used to activate encryption on a non-encrypting site. This also activates encryption on a new site.

On MiVoice 5000 Manager, Menu Administration>Network topology

- Select the site (cluster server or remote site) of the multi-site network on which encryption must be activated then click **Configuration**.
- Tick the parameter **Encrypted site** to activate encryption on the site concerned, then click **Modify**. Click **OK** to confirm the modification.
- Validate the modification confirmation message by clicking **OK**.
- Validate the message confirming the encryption activation on the site by clicking **OK**.



WARNING: Encryption works between two systems (cluster server and remote site) only if it is activated on the systems concerned.



Note: You can regenerate the certificate on a site on which encryption is already active by clicking **Certificate**.

3.16 MAINTENANCE OPERATIONS ON A WORKING CLUSTER

3.16.1 ADDING A NODE TO A CLUSTER

This procedure is used to add a new node to a working cluster.



WARNING: The dongle ID on an MiVoice 5000 server type node must be declared (see Chapter 3.6).

- Check the synchronisation of the new node with MiVoice 5000 Manager (see Chapter 3.9.3.1).
- Start the new node in TOTAL mode without creating any subscribers (see Chapter 3.9.3.2).
- Create and identify the node from MiVoice 5000 Manager (see Chapter 3.9.4). While creating the new node, it is possible to attach it to a community by selecting this community before clicking **Add**.



Note: If encryption is activated on the cluster server, encryption will also be automatically activated on the new node attached to this cluster server.

The node restarts after the system is configured in node mode. After the node is restarted, a start trap (PBX_INFOS) is sent to MiVoice 5000 Manager to inform it that the node has been correctly configured, and at the node's initiative a TCP connection is set up between the node and cluster server.

The synchronisation tool for the common data between the cluster server and node will trigger a second restart of the node to take into account these common data which have just been updated on the node.

3.16.2 DELETING A NODE FROM A CLUSTER

On a working cluster, this procedure is used to delete a node from MiVoice 5000 Manager and reconfigure the corresponding system in standalone mode.

On MiVoice 5000 Manager, Menu **Administration>Network topology**

- Select the cluster server in the multi-site configuration then the node to delete.
- Click **Configuration**.
- Click **Delete** then confirm the deletion by clicking **OK**.
- A message appears, indicating that the node has been successfully deleted.

From Web Admin, Menu **Telephony service>System>Operation mode configuration**

- Set the parameter **Mode** to **Standalone** then confirm.
- The system restarts in TOTAL mode.



Note: If necessary, the system may be fully reconfigured in standalone mode via a restart procedure through **Ctrl + I**.

3.16.3 UPDATING CLUSTER SOFTWARE

This procedure is used to update a cluster software release from MiVoice 5000 Manager.

The update concerns the cluster server and all the nodes attached to this cluster server.

3.16.4 CASE OF DEFENCE FOLLOWING A FAILED SOFTWARE UPDATE OR AFTER A ROLLBACK

- Processing the nodes with a wrong software release (below that of the cluster server):
 - The administrator must restart, on the Web Admin of the node in question, an update of the node software.
- Processing the cluster server with a wrong software release (below that of the nodes or certain nodes):
 - The administrator must restart, on the Web Admin of the cluster server in question, an update of the cluster server software.

As for R6.5, the update can be carried out gradually and selectively by list of sites.

This is due to the possibility of heterogeneity between the Cluster Server versions and the nodes (minimum R6.4 required for each of the nodes to be updated by the Repository method).

This procedure is described in a specific document Updating by Repository AMT/PTD/PBX/0155/2/ (R6.5 Minimum Edition 2).

3.16.5 BACKING UP THE CLUSTER DATA

This procedure is used to back up cluster data from MiVoice 5000 Manager.

The data backup concerns the cluster server and all the nodes attached to this cluster server.

From MiVoice 5000 Manager, Menu **Immediate actions > Upgrade/restore**

- Select the cluster in the multi-site configuration.
- Click **Start action**.
- Select the type of information to back up on the cluster:
 - Application and PBX data
 - IVR
 - Spoken announcements
 - Application code



WARNING: The disk space occupied by a backup, including the application code, is very large. This option must be used with precaution and occasionally.

- In the operations log, a message indicating that the operation on the cluster server and on all the nodes must appear.

3.16.6 RESTORING THE CLUSTER DATA

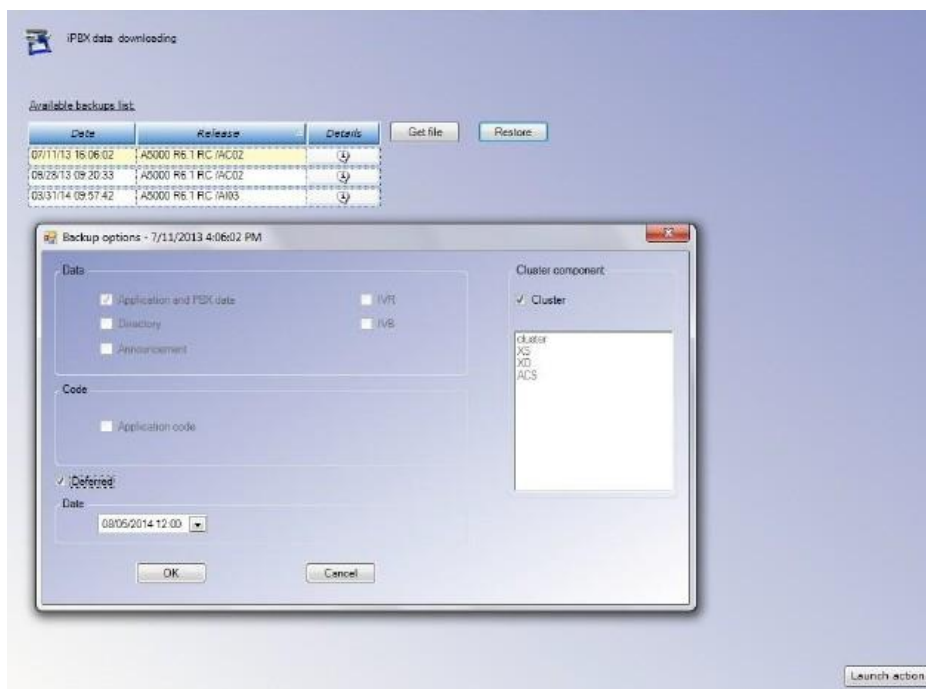
This procedure is used to restore cluster data from MiVoice 5000 Manager.

An option allows you restore:

- Only the cluster server data
- The data of a specific node
- The cluster data (cluster server + all the nodes attached to it).

From MiVoice 5000 Manager, Menu **Immediate actions > Upgrade/restore**

- Select the cluster in the multi-site configuration.
- From **List of available backups** select the data to be restored, then click **Restore**.
- Select the components to restore (by default, the cluster data is restored).
 - Cluster
 - Cluster Server
 - Specific node
- Indicate whether the action is deferred or immediate, then click **OK**.



- In the operations log, a message indicating that the operation has been successful must appear.

3.17 WORKING IN DUAL HOMING MODE IN A CLUSTER

When communication between the node and cluster server is cut, the node automatically switches to standalone mode without restarting. In this mode:

- The backup subscriptions available on the node are activated (dual homing mode).
- The node regularly tries to restore the connection with the cluster server.

The screenshot shows the Mitel Telephony service web interface. The left sidebar contains navigation links: Web Admin home, Subscribers, Rights, General settings, System, Dialing plan, Network and links, Reception, Voice mail and tones, and Fast links. The main content area is titled 'Subscribers miscellaneous settings' and includes a breadcrumb trail: Telephony service > Subscribers > Rights > General settings (1.4.1). Below this is a tabbed interface with tabs for Subscriber, System, Rights, Application, and Network. The 'Subscriber' tab is selected, displaying various configuration options. These include 'Com abbreviated dialing' (number of numbers: 1000, numerous prefixes: checkbox), 'Subscriber forwarded to exterior' (Charging: CALLING, send ident: CALLING NUMBER), 'Feature class management' (TL class management: NO, Partition class management: NO), 'Partition class management' (checkbox), 'DID numbers handled by the Manager' (checkbox), 'N* without external prefix for SIP set' (checkbox), 'Subscription lock duration(min)' (5), 'Routing of EXT calls' (LOCALISATION SITE), 'Check password when opening TAPI session' (checkbox), 'Power saving function' (checkbox), and 'Dual homing settings' (daily realignment (hh:mm): 01:37, immediate realignment of: dropdown). At the bottom left, there is a status bar showing 'XS - R6.1 RC / E301 FRA', 'Site: 088 - SITE LOC', and a timestamp '31/03/16 11:41:57'.

When connection with the cluster server is restored, the node automatically returns to its normal mode and the backup subscriptions are no longer active.

3.17.1 DEFINING THE BACKUP NODE

The backup node of a cluster serve subscription is defined statically:

From MiVoice 5000 Manager

- Menu **Telephony > Subscriber management**
- **Search** for the subscription to configure with the right filter criteria.
- Open the subscription via the **Management** button **then modify the Backup site** parameter in the technical record of the subscription declared on the cluster server.
- Assign the backup node according to the following rules:
 - For the IP terminals, the backup node may be any cluster node (preferably the one geographically closer to the IP terminal).
 - For a TDM terminal, the backup node must be the node to which it is physically connected.
- Validate the modification.



WARNING: A node must be the backup site of a subscription declared on the cluster server. A node cannot be the backup site of a remote site or of another node.

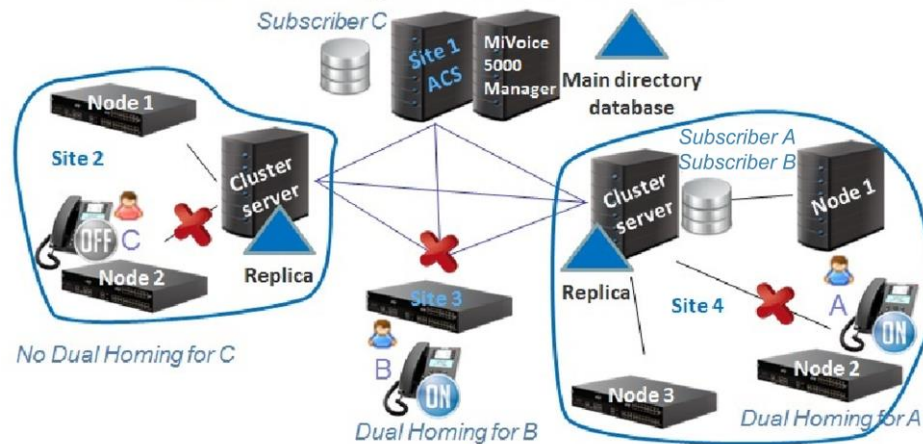
If one or more communities are defined in MiVoice 5000 Manager, only the nodes belonging to the same community as the cluster server subscription will be proposed as the backup site for this subscription.

If community mode is not enabled, all the cluster server nodes will be proposed as backup site for the subscription declared on the cluster server.

In an XXL architecture, if no community is defined in MiVoice 5000 Manager, the backup site of a subscriber in dual homing mode may be any site on the XXL multi-site network.

In the example below, a node on the site 4 cluster can only offer backup for subscribers declared on the site 4 cluster. Moreover subscriber C of site 1 cannot be backed up by node 5 of site 2 cluster.

Dual Homing in an XXL architecture



3.17.2 CREATING UPDATING BACKUP SUBSCRIBERS ON THE NODES

Backup subscribers are automatically created/updated on the cluster server backup node(s) in the following cases:

- After a node reconnects to the cluster server (case of a node which was occasionally in standalone mode), the dual homing process (creating/updating backup subscribers) starts automatically five minutes later.
- When a new node is deployed from MiVoice 5000 Manager (after the last node restart and five minutes after its connection to the cluster server). In this case, only the general-purpose subscriber is concerned.
- Everyday at a time defined in the cluster server menu
Telephony service>Subscribers>Rights>General parameters, System tab, Dual homing parameters, daily realignment.

This creation may be immediate:

- From the cluster server menu
Telephony service>Subscribers>Rights>General parameters, System tab, Dual homing parameters, daily realignment,

Dual homing settings

- daily realignment (hh:mm)

01:37

- immediate realignment of

001-SITE LOC

- Select the cluster server then click **Confirmation**.



WARNING: The dual homing function requires the presence of a dual homing licence on the cluster server:
Menu Telephony service>System>Info>Licences.

3.18 REDUCED DIRECTORY DATABASE IN THE NODES

R6.1 improves the directory resilience with the possibility to activate a reduced directory database in the nodes.

On a node, the reduced directory database contains:

- The backup subscriber records and subscribers inside the node (only the general-purpose subscriber and possibly the IVR subscriber are declared)

When the node belongs to a community, the reduced directory database contains:

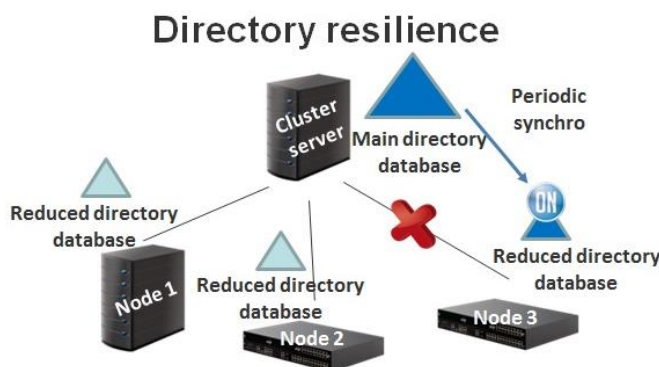
- The community's subscriber records.

The reduced directory database is limited to 3000 directory records when the node is a Mitel 5000 Gateways or Mitel 500. The reduced directory database is limited to 80000 directory records when the node is a MiVoice 5000 Server.

The reduced directory database is automatically accessible when the node no longer accesses the priority 0, 1 or 2 remote LDAP databases defined on the cluster server.



WARNING: If a directory replica is configured on the cluster server, it is henceforth forbidden to use the address 127.0.0.1 during directory configuration on the cluster server (access to priority 0, 1 or 2 LDAP databases). The actual cluster server IP address must be used so the nodes can use this address



3.18.1 ACTIVATING AND CONFIGURING THE REDUCED DIRECTORY DATABASE

On each node, activate the reduced directory database:

- Menu **Telephony service>Subscribers>Directory>Parameters>Connections, Configuration** tab
- Tick **Reduced directory**.

Directory connections settings
Telephony service>Subscribers>Directory>Settings>Connections (1.1.1.1)

Configuration | Name resolution | Dialing service

Directory configuration base EXP

Type of server

Regeneration of internal records ☐

- The reduced directory database is created and synchronised immediately with the priority 0 LDAP database configured on the cluster server.



Note: The reduced directory database may be synchronised from time to time by ticking the parameter immediate realignment then clicking Validation.



WARNING: The reduced directory database synchronisation tool automatically starts immediately after the backup subscriber creation process (see Chapter 3.17 for more information about the backup subscriber creation process).

The reduced directory database offers the following directory features: call by name, name resolution, SDN routing.

On each node, configure the following directory services used by the reduced directory database:

- Menu **Telephony service>Subscribers>Directory>Parameters>Connections, Name resolution** tab
- Check that this service is working (box ticked).



- Menu **Telephony service>Subscribers>Directory>Parameters>Connections, Dialling service** tab
- Check that this service is working (box ticked).



The reduced directory database does not require any additional licence. The licence used to unlock the number of directory records that can be used on the main LDAP database is entered on the cluster server.

3.19 MANAGING SPECIAL NUMBERS ON A CLUSTER

On a cluster the content of the special number lists is defined on the cluster server only.

The geographic location service is activated in the parameters of the CAC server on the cluster server: Menu **Telephony service>Network and links>Quality of service>CAC and localisation>CAC server settings**

Each location is defined on the cluster server: Menu **Telephony service>Network and links>Quality of service>CAC and localisation>Locations>Names**

Each location is assigned a location code: Menu **Telephony service>Network and links>Quality of service>CAC and localisation>Locations>characteristics**

Then the special number lists are associated with the location code: Menu **Telephony service>Numbering plan>Special numbers>Special numbers definition**

There is no location service in the nodes. Therefore, location 0 must be used.

On each node, assign location 0 the location code corresponding to the special number lists defined on the cluster server.

3.20 MANAGING USER ACCOUNTS BY NODE

As of R6.1 SP1, it is possible to manage user accounts by node.

3.20.1 CREATING A USER ACCOUNT ON A NODE

To create a user account on node 4, proceed as follows:

From the Web Admin of node 4,

- Menu **Telephony service>System>Configuration>Users>Operators definition**
 - Enter the user account login.
 - Enter the user account password.
 - Select the language.
 - Hide the picture on the welcome page if you wish.
 - Assign a profile to the account.



Note: The profiles remain the same for the nodes and cluster server, and are defined on the cluster server only.

- Define the execution mode if necessary (basic or advanced).



Note: The execution mode is used to hide (basic mode) or leave visible (advanced mode) some parameters in SIP TRUNK characteristics.

3.20.2 OPERATION, RESTRICTIONS AND CASE OF DEFENCE

Between the "main accounts" defined on the cluster server and the "local accounts" defined by node, the login must be unique. On the other hand, the same local user account login defined by node may exist on several nodes.

It is impossible to log on with the login A1 defined on Node A to another node apart from A (if the passwords are different) or to the cluster server.

It is not allowed to create on a node a login defined already on the cluster server.

Creating on the cluster server a login defined already on Node A deletes this login (local account) on Node A.

The function 'reset password' via CTRL + I on a node does not have any impact on the password of the admin account defined locally on the node or on the cluster server.

A local account defined on the survival node does not give access to the nodes connected to this survival node.

Special defence:

- Creating a login B1 (main account) on the cluster server whereas Node A is disconnected and this login B1 exists on Node A (local account)
- When node A reconnects, login B1 is automatically deleted (local account) on Node A.

4 IMPLEMENTING SURVIVABILITY IN CLUSTER MODE

4.1 OVERVIEW

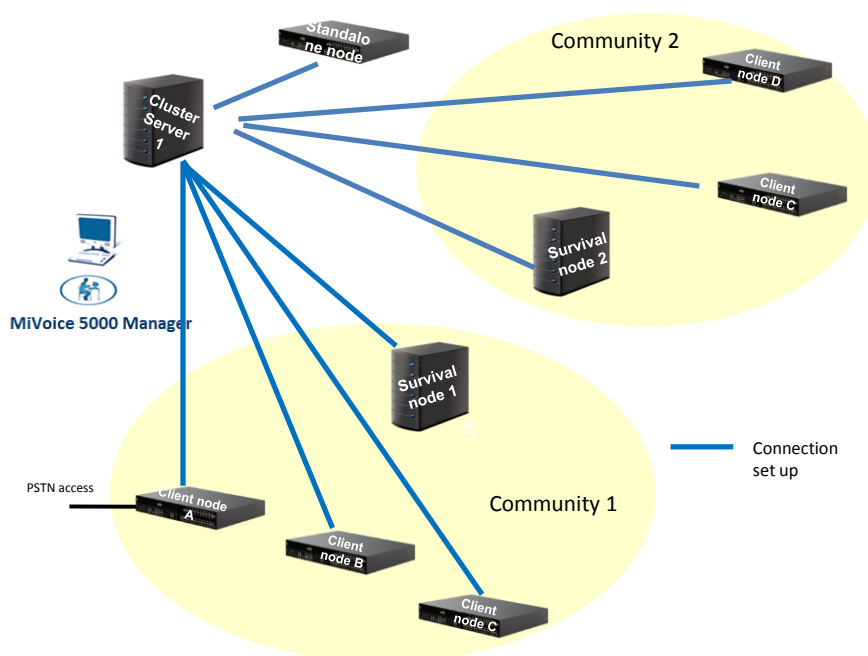
Survivability is an optional operating mode which enables nodes of the same community and the same cluster whose link with the cluster server has been cut, to work independently in an architecture similar to a "backup cluster".

In this degraded operating mode, the node playing the role of cluster server is called "Survival node".

The other nodes in this community are called (survival) client nodes.

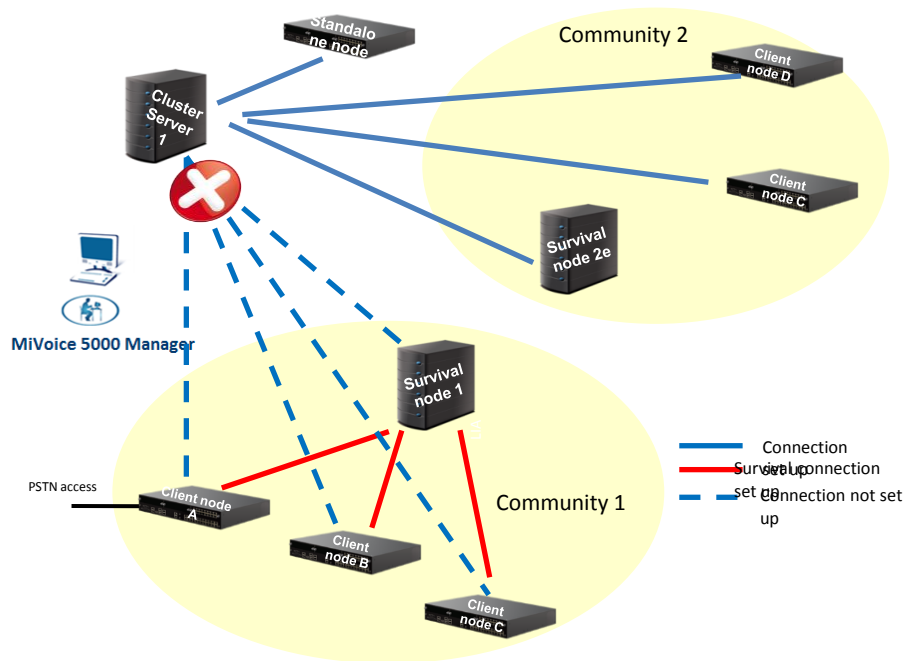
Example:

Nominal operation



Operation in survival mode

Links of nodes for community 1/ cluster server 1 are cut (case of network problem). The community changes to "survival" mode. Node 1, defined as survival node in MiVoice 5000 Manager, becomes the backup cluster for the nodes of community 1 managed by cluster server 1.



Principles

All the client nodes are configured by MiVoice 5000 Manager to reach the survival node which contains the reduced LDAP database for the community.

When the disconnection from the cluster server is confirmed, each node regularly tries to set up a connection to the survival node and cluster server.

The survival node is unique for each community.

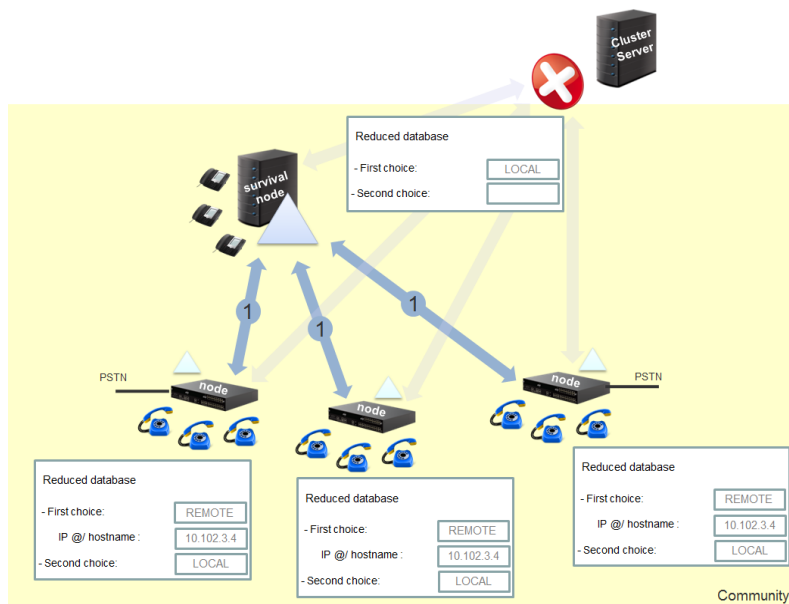


Note: As long as the nodes remain connected to the cluster server, they do not change to "survival" mode; this applies to both the survival node and the other nodes. This point must be taken into account while configuring the IP network.

Concerning the directory database:

A main reduced directory is defined in the survival node and contains all the subscribers in the community.

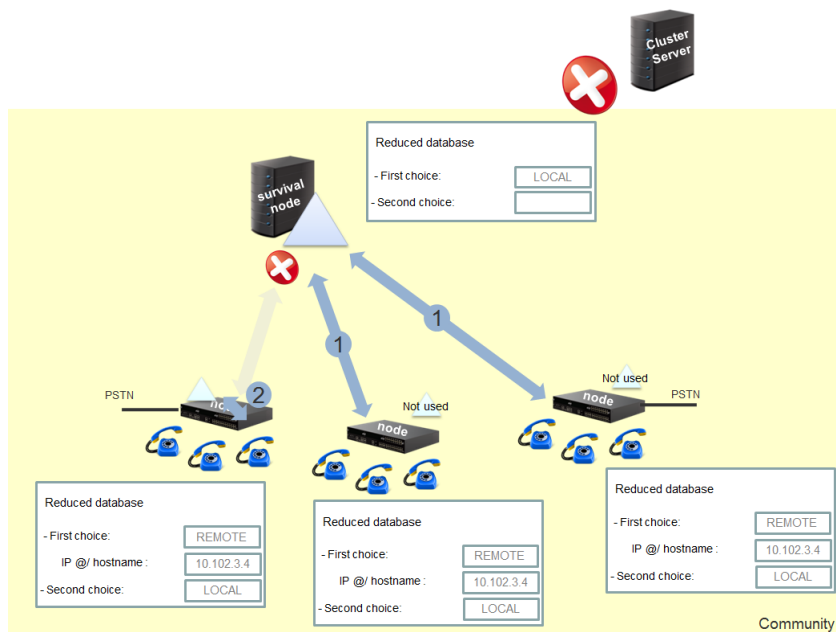
When connection to the cluster server is confirmed, each (survival) client node accesses this remote directory database.



If the link between a client node and the survival node is cut and the link between this client node is still not restored, the inaccessible client node uses the local reduced directory database.

This database contains only the internal records of local subscribers.

Refer to Section 3.18.1.



4.2 PRINCIPLE OF THE CONFIGURATION

The configuration consists in identifying the survival node for each community in MiVoice 5000 Manager.

The IP address/host name for this node identified as survival node is then automatically sent to the other client nodes in the community.

The reduced directory database in the survival node is then dynamically configured in the Web Admin by MiVoice 5000 Manager.

4.3 RULES AND PREREQUISITES

MiVoice 5000 Manager must be configured in such a way that the DID numbers are managed in directory characteristics (SDN mode).

Community mode is mandatory in the infrastructure of the cluster concerned.

Each community must correspond to a local geographic area (no WAN in this area).

The minimum MiVoice 5000 Manager version required to configure survivability mode in a cluster is:

- MiVoice 5000 Manager: V3.1C

iPBX compatibility

- Cluster Server and nodes: R6.1 SP1

It may be either a MiVoice 5000 Server or an Mitel 5000 Gateways system.

If the survival node is a Mitel 5000 Gateways system:

- The maximum number of client nodes is 5.
- The maximum number of directory records is 3000.

If the survival node is a MiVoice 5000 Server:

- The maximum number of client nodes is 10.
- The maximum number of directory records is 10000.



Note: However, it is advisable to define an MiVoice 5000 server in the community as survival node for a large number of client nodes to manage.

4.4 IDENTIFYING THE TYPE OF NODE (SURVIVAL OR CLIENT)

Menu **Administration>Network topology**

- Select the node in the cluster concerned.
- If necessary tick the **Survival node** box.
- Click **Modify**.

4.5 DEACTIVATING A SURVIVAL NODE

When the administrator deactivates the survival feature on the node in question, MiVoice 5000 Manager updates the other nodes in the community; the survival node ID (IP address/hostname) is deleted from the other nodes in the community.

4.6 DEACTIVATING A SURVIVAL NODE

When the administrator deletes the survival node in the community, MiVoice 5000 Manager updates the other nodes in the community; the survival node ID (IP address/hostname) is deleted from the other nodes in the community.

4.7 DELETING A CLIENT NODE

When a client node is deleted in the cluster community, this has no impact on the other nodes of this same community.

4.8 ADDING A CLIENT NODE TO A COMMUNITY

When a (client) node is added to a community, MiVoice 5000 Manager automatically configures on this node the survival node IP address/hostname of this same community.

4.9 REASSIGNING A SURVIVAL NODE IN A COMMUNITY

When the administrator wishes to reassign a new node as survival node inside a community:

Menu **Administration>Network topology**

- Select the current survival node in the cluster concerned.
- Untick the **Survival node** box.
- Click **Modify**.
- Select the new survival node in the cluster concerned.
- Tick the **Survival node** box.
- Click **Modify**.

The reduced directory database is then transferred by MiVoice 5000 Manager to the new survival node.

4.10 CHANGING THE COMMUNITY OF A SURVIVAL NODE

When the administrator wishes to change the survival node's community, he must first deactivate the survival node function.

4.11 CHANGING THE COMMUNITY OF A CLIENT NODE

When the administrator wishes to change the community of a client node, this node is reconfigured to be connected to another survival node if it exists in the new community:

- Updating the IP address / hostname of the survival node

When there is no survival node in the new community, the IP address /hostname of the survival node is deleted for the moved node.

In both cases, the node configuration update is monitored by MiVoice 5000 Manager.

4.12 DELETING A COMMUNITY

A community cannot be deleted if a subscriber, administrator or iPBX is using it.

Therefore, there is no additional impact on the management of community deletion.