Nortel Communication Server 1000 Communication Server 1000E High Scalability Installation and Commissioning

7.0
NN43041-312, 01.03

July 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release

This is a new document created to support Nortel Communication Server1000 Release 7.0.

Other Changes

This release contains no other changes.

Revision History

July 2010 Standard 01.03. Up-issued to reflect changes in technical content.

June 2010 Standard 01.02. Up-issued to reflect changes in technical content.

June 2010 Standard 01.01. This is a new document created to support Communication Server1000 Release 7.0.

Chapter 2: How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://support.nortel.com/go/main.jsp

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

http://www.nortel.com/help/contact/global/index.html

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/help/contact/erc/index.html

Getting help through a Nortel distributor or re-seller

If you purchased a service contract for your Nortel product from a distributor or authorized re-seller, contact the technical support staff for that distributor or re-seller.

Chapter 3: Communication Server1000 High Scalability System Management overview

A Communication Server1000 High Scalability System (HS System) contains multiple Communication Server1000E High Availability Groups (HA Groups), associated Signaling Servers, Media Cards, and Communication Server1000 Element Manager to provide centralized Unified Communications Services and Multimedia Services to large-scale enterprise customers having more than 100000 telephony accounts.

HS System Data

HS System data is divided into two categories: common data and unique data.

HS System common data is a set of identically configured data blocks across multiple HA Groups within an HS System. Because you can view the HS System as a single Unified Communications Services and Multimedia Services entity, internal HA Groups must share a set of system configuration data, such as Customer, Route, and ESN data blocks, to provide a single system view.

HS System unique data is a group of individually configured data blocks, or attributes, for each HA Group. For example, station data is unique on a per server basis.

Communication Server1000 High Scalability System Management

An HS System is managed through a Web interface. The Web-based management application is called Communication Server1000 Element Manager (EM) High Scalability (HS). EM HS presents the multiple HA Groups as a single system and replicates common data to all HA Groups within an HS System. An administrator uses also configures specific or unique data for an individual HA Group within an HS System.

EM HS uses Nortel Unified Communications Management Common Services (UCM Common Services) as the navigation and launch point, the UCM Common Services security framework as the access control laye, and UCM Deployment Manager as the deployment point. For more information on UCM Common Services and the UCM Common Services security framework,

see *Unified Communications Management Common Services Fundamentals, NN43001-116* and *Security Management Fundamentals, NN43001-604*.

Communication Server1000 Element Manager High Scalability Services

Common Data Definition

HS System common data is a group of identically configured data blocks across multiple HA Groups within the same HS System. Data that are common across multiple HA Groups are configured once and automatically propagated to all groups within the same HS System, so that the HS System appears as a single entity from a common data management perspective.

Appendix Common Data on page 57 summarizes the loads that contain common data blocks. For a complete list of attributes (prompts) in the default definition of common data, see *Software Input Output Reference — Administration, NN43001-611*.

Common Data Replication Services

One HA Group in an HS System is designated as a reference HA Group for data replication services.

The Communication Server1000 Element Manager HS provides two common data replication services: Common Data Bulk Provision Service for a new HA Group and Common Data Automatic Update Service.

- Common Data Bulk Provision Service:

  Common Data Bulk Provision Service applies to the initial configuration of a new HA Group within an HS System. The Common Data Bulk Provision Service transfers the entire system common data from the reference HA Group as a bulk provision into a target HA Group.

- Common Data Automatic Update Service

  When common data in one of the managed HA Groups is changed through Communication Server1000 Element Manager HS, the Common Data Automatic Update Service propagates the change to all other HA Groups within the HS System.

Note:
You must not change common data, managed by EM HS, by using the CLI.

Common data managed by Communication Server1000 Element Manager HS must not be changed through the CLI. Changes to common data made through the CLI are not propagated to other HA Groups within the HS System.

Common Data Service Replication Flexibility

An HS System is installed with a default definition of common data. Administrators can modify the default definition. An entire default data block, or specific attributes (prompts) within a data block, can be set as unique. Data that has been set as unique data can be reset as common data. Data not in the default definition of common data can not be set as common data.

- If a data type is common data, the Common Data Automatic Update Service replicates the entire data type attributes (data block prompts) among the multiple HA Groups within the HS System during provisioning.
- If a data type is set as unique data, none of the data type attributes (data block prompts) are replicated among the multiple HA Groups within the HS System during provisioning.
- If a specific attribute (prompt) within a data block is set as unique, it will not be replicated among the multiple HA Groups within the HS System during provisioning.

Common Data Service Replication Reliability

A generic mechanism is used to reliably retrieve and transfer load data across multi-HA Groups by the Common Data Bulk Provision and Common Data Automatic Update Services.

In EM HS, a common data transaction is a set of common data replication operations performed within all HA Groups in an HS System. In EM HS, a common data transaction operation is a common data replication against a single HA Group under a common data transaction. All common data transactions and associated transaction operations are recorded. Administrators can review the common data replication report and rerun failed transactions.

Common Data Bulk Provision Service for a new HA Group

Common Data Bulk Provisioning is used to bring a newly deployed HA Group to the same level of service as the other HA Groups in the HS System. It is assumed that the configuration on the reference HA Group is not changed during the bulk provisioning process.

- If data retrieval from the reference HA Group is successful and replication to the destination HA Group fails, the failed transaction requests can be re-replicated.
- If critical failures occur, you must remove all partially transferred data on the destination HA Group and restart the transfer from the beginning. For more information on restarting bulk provisioning after a critical failure, see Re-replicating Bulk Provisioning on page 50.

A critical failure occurs, if data retrieval from the reference HA Group fails, or if the bulk replication process unexpectedly stops before successful completion.

Common Data Automatic Update Service

If data retrieval from the reference HA Group is successful and replication to one or more destination HA Groups fails, the failed transaction requests can be re-replicated.

Common Data Audit Services

The Communication Server1000 HS Management Audit Services focus on:

- Common data integrity preservation: the audit services preserve the integrity of common data provisioning. The audit services screen the last common data transaction between the HS management system and an individual HA Group to determine the integrity of the common data provisioning sequence.
- Common data transaction audit: the audit services go through all common data transactions from the last committed point in the database to find failed transactions and associated transaction operations.
- Audit reports: the audit services generate comprehensive reports, including the Common Data Replication Report and the Common Data Audit Report.
- Possible common data provisioning error correction: the audit services integrate a generic mechanism to handle common data re-replication and provide hints for unique data reconfiguration.

Element Manager High Scalability Redundancy Model

The EM HS redundancy model is depicted in Figure 1: EM HS redundancy with two way replication and monitoring on page 13. For more information on deploying the EM HS application with the redundancy option, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

In normal conditions one of the servers, for example server one, is in active mode and has all the clients connections. If server one becomes unavailable, server two becomes active and updates the element registry for the EM HS URL in the primary UCM Common Services to point to server two. It may take up to 10 seconds for the update to the element registry for the EM HS URL. After a switchover event, all new connections will be redirected to the active server two. If server one becomes available, upon reconnecting with server two, server one will switch to backup mode.

Note:

If there is no response when clicking the EM HS link, login to UCM Common Services again. An EM HS redundancy switchover event may have occurred.

It is assumed that the EM HS application does not co-reside with other applications, such as Personal Directory or Network Routing Service. The database replication and heart beat between the two servers does not support IPV6.

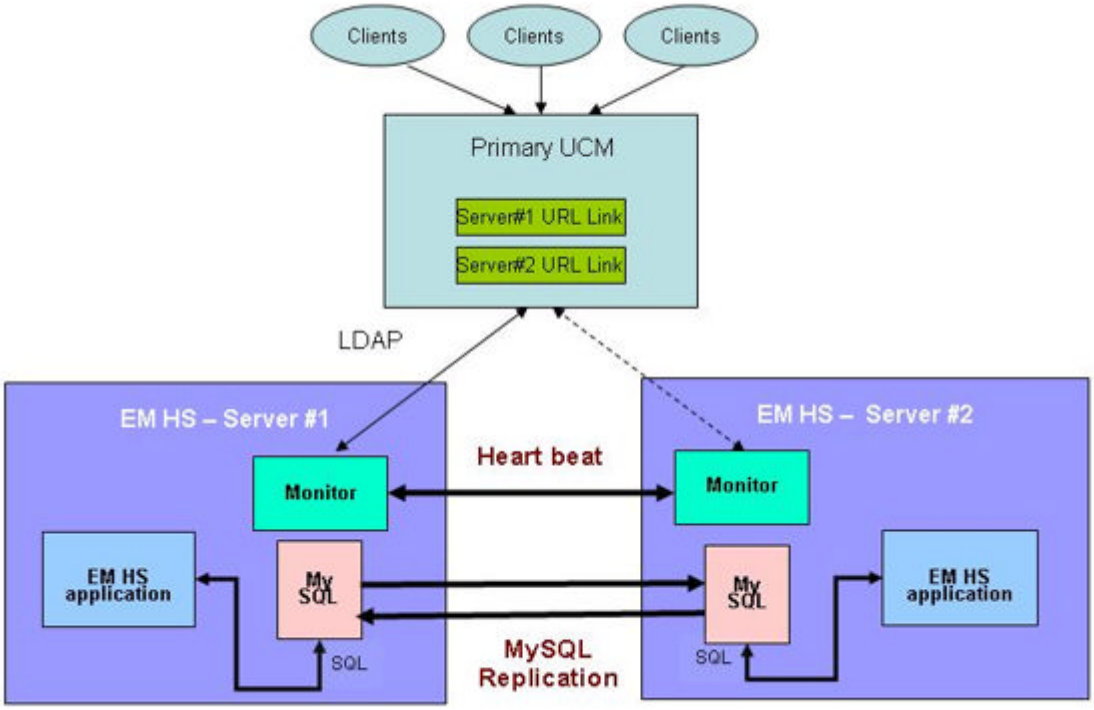


Figure 1: EM HS redundancy with two way replication and monitoring

Operation, Administration, and Maintenance Transaction Audit and Security Event logging

Communication Server1000 Element Manager HS log files are incorporated into the Operation, Administration, and Maintenance (OA&M) Transaction logging system. UCM Common Services provides log viewer and file download functions to retrieve log files. The log viewer is available from the UCM Common Services navigation tree.

Communication Server1000 High Scalability System Management Security

Communication Server1000 High Scalability System Management uses the UCM Common Services framework for security. The UCM Common Services framework provides the following security features:

- centralized logon and user authentication
- centralized security management with levels of user access
- lists the joined HS System under UCM security domain in structure view
- patch management and other security aspects
- underlying user access name and password to connected a HA Group

Chapter 4: Migrating the Communication Server1000 High Scalability System

This chapter provides a high-level task flow for migrating two or more Communication Server1000E systems to a Communication Server1000 High Scalability System (HS System).

Communication Server1000 task flow

This section provides a high-level task flow for the installation or upgrade of a Communication Server1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the NTP number that contains the detailed procedures required for the task.

High Scalability Solution

For more information refer to the following NTPs, which are referenced in the High Scalability Solution task flow diagram:

- *Network Routing Service Fundamentals, NN43001-130*
- *Dialing Plans Reference, NN43001-283*
- *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Security Management Fundamentals, NN43001-604*
- *Element Manager System Reference - Administration, NN43001-632*
- *Communication Server 1000E Planning and Engineering – High Scalability Solutions, NN43041-221*

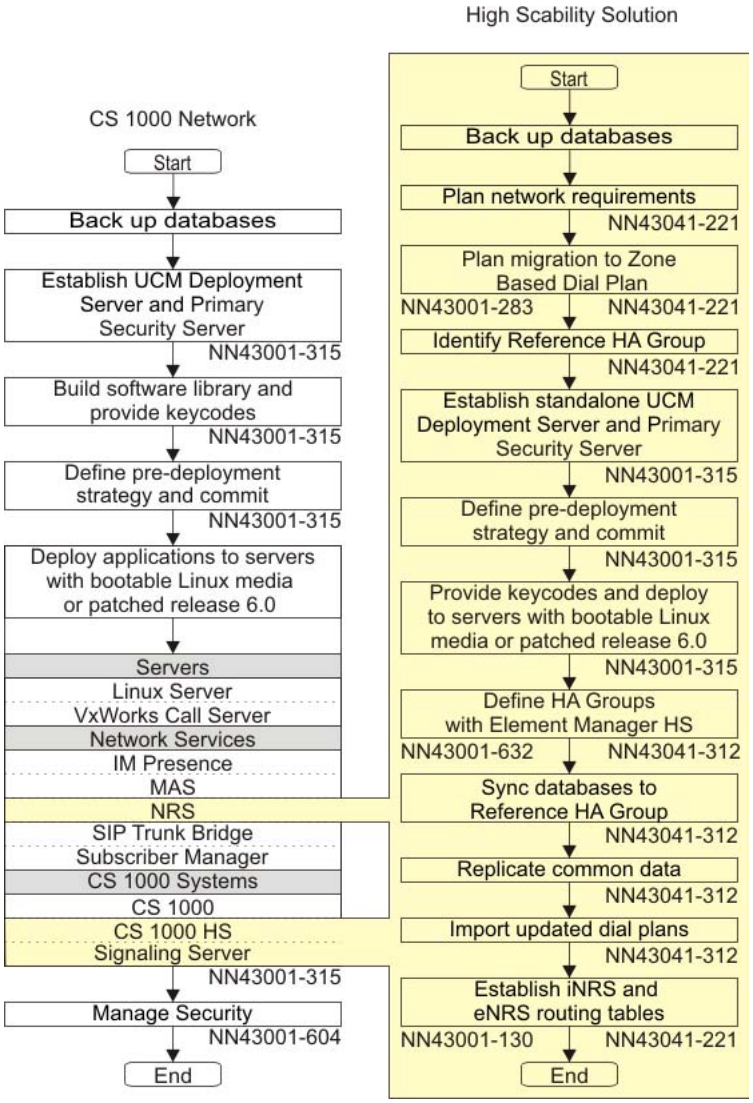


Figure 2: High Scalability Solution task flow

Survivable SIP Media Gateway

For more information refer to the following NTPs, which are referenced in the Survivable SIP Media Gateway task flow diagram:

- *Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Network Routing Service Fundamentals, NN43001-130*
- *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Security Management Fundamentals, NN43001-604*

- *Communication Server 1000E Installation and Commissioning, NN43041-310*
- *Communication Server 1000E Software Upgrades, NN43041-458*

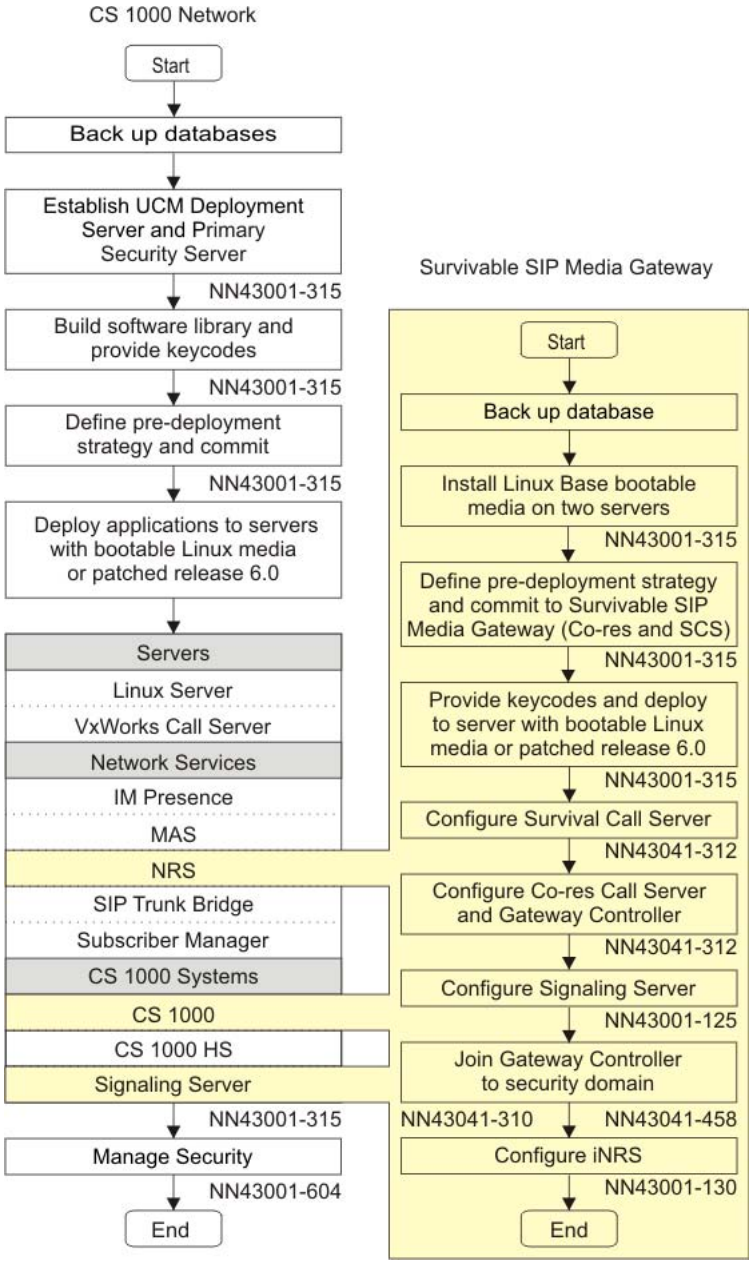


Figure 3: Survivable SIP Media Gateway task flow

Planning

There are a number of factors and questions to consider prior to the deployment of an HS System, including

- Dial Plan analysis and migration to Zone Based Dialing design
- Migration of existing Media Gateway Controllers
- Total capacity of all existing Communication Server1000E systems must be considered. This will determine the number of HA Groups needed in the HS System.
- Physical configuration of the HS System

For more information on planning and engineering an HS System, see *Communication Server 1000E Planning and Engineering – High Scalability Solutions, NN43041-221*.

Recommendations

For large network deployment, Nortel recommends that the UCM Primary Server and the UCM Backup Server be installed on dedicated standalone servers, with no other applications co-residing on the servers. In particular, the Communication Server1000 Element Manager (EM) High Scalability (HS) application should not be installed on the same server as the UCM Primary or Backup Servers. The UCM Servers must be the first elements to upgrade. Thus, if EM HS is co-residing with the UCM Servers, it will be upgraded as well and it cannot be used to manage the Call Server which has not been upgraded yet.

For more information on UCM Common Services and the UCM Common Services security domain, see *Unified Communications Management Common Services Fundamentals , NN43001-116* and *Security Management Fundamentals, NN43001-604*.

Requirements

- The EM HS application must be installed on a dedicated standalone Linux server. If the EM HS application is installed with the redundancy option, the redundant EM HS application must be installed on the same type of Linux server as the primary EM HS application.

  For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.
- Subscriber Manager is a mandatory component of an HS System.

For more information on Subscriber manager, see *Subscriber Manager Fundamentals, NN43001-120*.

Communication Server1000 High Scalability System task flow

The task flow makes the following assumptions about the configuration of the HA Groups that are migrating to the HS System.

Assumptions

- The reference HA Group at the centralized location will be deployed with new hardware.
- Existing HA Groups will be migrated individually.
- The existing HA Groups are running Release 6.0 software.
- All components have registered to the same UCM Common Services security domain.
- Zone Based Dialing (ZBD) has not been configured on any of the HA Groups.
- Survivable Media Gateways will be converted to Survivable SIP Media Gateways. (Optional.)
- Most of the existing phones are IP phones (Unistim), or most of the existing TDM phones will be replaced by IP phones (Unistim).

General task flow

1. Upgrade UCM Common Services to Release 7.0.
    a. Backup the UCM Common Services database prior to migration of the HA Groups to the HS System.
    b. If Element Manager is deployed on the UCM Primary Server or UCM Backup Server, remove it from the UCM Server prior to the upgrade.
    c. Install a new stand alone UCM Primary Server first, followed by the UCM Backup Server. Certain UCM Common Services management capability will be impacted while the UCM Primary Server is being installed. For example, an administrator cannot add new accounts or new servers.

    For more information on upgrading UCM Common Services to Release 7.0, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

After UCM Common Services is upgraded, there should be no impacts to existing Release 6.0 systems.

The Release 7.0 Deployment Manager will be installed on the UCM Primary Server.

2. Configuration using Deployment Manager.

   Release 7.0 Deployment Manager provides the capability to group servers into a system view. For example, the following could be included in a system view:

   - HA groups
     - HA Call Server pairs
     - Signaling Servers (TPS, GW, SIPL, PD)
   - EM HS
   - Internal NRS for the HS System

   Other components, such as the following, could be included at this stage or later.

   - Survivable SIP Media Gateways
   - SIP Media Gateways and their associated EM
   - Media Gateways
   - Geographic Redundancy Counterparts for the HS System, if any

   For more information on Deployment Manager, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

3. Preparation for upgrade.

   Backup all system configuration data, including Call Server data and Signaling Server data (Network Routing Service and Personal Directory), prior to upgrade.

4. Install hardware and software for the reference HA Group.

   a. Install the dedicated standalone Linux server for the EM HS application.

      For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

   b. Deploy the EM HS application.

      For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

   c. Install the hardware and deploy the software for the reference HA Group, including

      - High Availability Call Server pair. For more information, see *Communication Server1000E Installation and Commission, NN43041-310*.
      - associated Signaling Server for High Availability Call Server pair.
      - Media Gateways, Survivable Media Gateways, or Survivable SIP Media Gateways. For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

- Signaling Server for the Internal NRS. For more information, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Note:

This workflow example assumes that new hardware is used to build the reference HA Group at the Data Center. Thus, during the configuration of the HS System, all existing Communication Server1000E systems will continue to operate and existing systems can be migrated to the HS System in stages. With this approach, the reference HA Group Call Server can be installed with a default database initially. Proper configuration of the Call Server will be done at the next stage.

Note:

The High Scalability software package 421 and the Geographic Redundancy Primary System software package 404 must be included in the keycode for all the HA Groups, including the reference HA Group Call Server.

Note:

It is also possible to upgrade an existing Communication Server1000E system to Release 7.0 and convert it to the reference HA Group. In this case, the existing hardware and customer database can be re-used. There may be significant modifications required in the configuration, if the existing customer database has not already incorporated the Zone Based Dialing design, or the existing Zone Based Dialing design does not fit the overall Zone Based Dialing design for the HS System.

5. Configure the Reference HA Group Call Server.

   Use EM HS to configure the reference HA Group Call Server. This includes

   - system configuration data
   - customer data
   - route and trunk data
   - numbering zone and bandwidth zone data
   - ESN routing data
   - Network Time Protocol

6. Configure the associated Signaling Servers.

   Use EM HS to configure the associated Signaling Servers for the reference HA Group Call Server. This includes

   - IPL configuration
   - SIP gateway configuration
   - Personal Directory

Note:

There will be a Personal Directory server for each HA Group.

7. Configure the Internal Network Routing Service.

   Configure the Internal NRS that will be used for routing inter-HA Group calls based on private numbers (UDP and CDP). Routing entries for user phone data must be configured manually as user phone data are migrated to the HS System.

Migration and Consolidation of existing Communication Server1000E systems into the HS System

Migration and consolidation of existing Communication Server1000E systems will be done one system at a time. There will be service interruption during the migration process.

1. Planning

   a. Map the existing dial plan into the new centralized Zone Based Dialing plan.

   b. Determine the hardware migration strategy.

   c. Determine to which HA Group the Communication Server1000E system should be migrated.

   d. Determine the TN mapping

   e. Print out existing data before migration.

      If possible, existing data (for example, CFN, CDB, RDB, ESN, trunk data blocks) should be printed and kept for future reference.

   For more information on planning and engineering an HS System, see *Communication Server1000E Planning and Engineering – High Scalability Solutions, NN43041-221*.

2. MGC migration

   If MGC must be migrated, the MGC data must be configured on the reference HA Group Call Server and the data must fit into the TN space of this HA Call Server (for example, Tone loop, Conference loop, digital trunk loops, analog trunks, MGC loop and shelf).

   The TDM sets on the MGC can be migrated together with IP sets in the next step.

3. User data migration

   Extract the user set data from the existing Communication Server1000E system into a CSV format file.

Use the PC based Migration Tool to make any modifications required for the new ZBD design, for example

- TN changed to the TN for the new HA Group
- DN changed to add zone prefix
- CFWDN and HUNT changed to add zone prefix

Use Subscriber Manager to import the modified and converted data into the controlling HA Call Server of the HS System.

4. Other database migration

   The data stored in the Unicode Name Directory have to be modified according to the new numbering plan (that is, ZBD prefix added to users DN have to be considered for different Numbering Groups).

   Because of the changes for phone DN involved in converting to ZBD design, the personal data (caller list, redial list) stored in the Personal Directory will not be retrievable. New data will be stored against the new DN once the user phone data is migrated to the HS System.

5. Migrating an existing Release 6.0 Survivable Media Gateway to a Release 7.0 Survivable SIP Media Gateway. (Optional.)

   Nortel recommends deploying Survivable SIP Media Gateways (SSMG) in the HS System as secondary call servers in the GR-n way redundancy model.

   The SSMG separates the Media Gateway component from the Survivable Call Server component. The physical separation of these two components enhances the scalability of the Geographic Redundancy network. Release 7.0 allows up to 511 secondary servers to be provisioned on the Primary Call Server for database replication and redundancy, if the secondary servers are SSMGs. This architecture also removes the 80 msec round trip delay restriction in Geographic Redundant networks, since the local media controller communicates only with its local call server and not with the Primary Call Server.

   The TDM resources (Media Gateway Controller card, DSPs on other Media Cards) register to the Media Gateway Call Server while the Survivable Call Server provides redundant Communication Server1000 services for the IP Phones. The Media Gateway communicates with the Primary Call Server or the Survivable Call Server using SIP trunking.

   For more information, see Migrating an existing Release 6.0 Survivable Media Gateway to a Release 7.0 Survivable SIP Media Gateway on page 25.

   Once installed and deployed, the Survivable Call Servers and the SIP Media Gateways are part of the UCM Common Services security domain. However, manual registration with the UCM Common Services is required to enable Central Authentication.

6. Hardware Conversion

   Conversion of the existing hardware to the new HS System architecture depends on the architecture chosen for the HS System.

   The preferred architecture for the HS System is to have Survivable SIP Media Gateways at the regional or branch locations. Phones for the users are upgraded

to Unistim phones or SIP phones. Only a small number of TDM phones are supported at the regional or branch locations, for example FAX and test phones. This will provide the maximum number of users supported on each HA Group in the HS System.

If a large number of TDM phones are needed after the migration, SMGs would still be required. This will affect the number of HA Groups needed in the HS System.

7. NCS Configuration

   Configure NCS for redirection of Unistim phones from the branch or regional locations to the HS System Call Servers.

8. Decommission the old hardware and commission the new hardware

   a. Migrate the sets to the new hardware configurations and decommission the old hardware.

   b. Unregister all the obsolete elements from the old hardware.

   c. Delete any obsolete elements from the UCM Common Services security domain.

9. Testing

   a. Ensure that the phones are functional.

   b. Make test calls (internal and PSTN calls).

   c. Test survival mode operations.

10. Consolidation of the next Communication Server1000E system

    Repeat each of the above steps for each Communication Server1000E system that must be migrated to the HS System.

Note:

To consolidate Communication Server1000E systems that are running pre-Release 6.0 software, follow he general task flow for consolidating Release 6.0 systems. Since these systems are not registered to the UCM Common Services, it is not necessary to unregister or delete the elements.

Task flow for adding an HA Group to the HS System

1. Use Deployment Manager to add a new HA Group to the Communication Server1000E system.

   • HA Call Server pair

   • Signaling Servers (TPS, SIPL, SIP GW, PD)

2. Install the hardware and software.
3. Use EM HS to replicate the common data to the new HA Call Server pair.

4. Use EM HS to define any additional Numbering Zones and BW Zones.
5. Configure the appropriate nodes for this HA Call Server pair.
6. Configure NRS for routing to this new HA Call Server pair.

After this HA Group is configured and deployed, consolidation of existing Communication Server1000E systems to the HS System can continue.

Migrating an existing Release 6.0 Survivable Media Gateway to a Release 7.0 Survivable SIP Media Gateway

Hardware considerations:

Survivable Call Server

CPDC or CPPM platform for running the Co-res CS/SS; CPPM only for running VxWorks CS with SS applications running on COTS. The decision to run Co-res or VxWorks is dependent on the number of users at the site. A Co-res system can only support 1000 IP users.

SIP Media Gateway

The CS, SS and MGC run in the SIP Media Gateway (CPMG/CPPM /CPDC/COTS). Here, CPMG is a combination of CPPM and MGC hardware in one single hardware package providing equivalent functionality.

Migration work flow

This section outlines the work flow in migrating an existing Release 6.0 SMG to a Release 7.0 SSMG.

When migrating a SMG to a SSMG, additional server(s) will be needed depending on the hardware option chosen. The following sections illustrate the possible hardware migration paths.

Preparation for upgrade

Back up all system configuration data prior to migration, including Call Server data and Signaling Server data.

Hardware Migration based on CPPM

1. The existing CPPM card serves as the Survivable Call Server. A new CPMG card is added to the gateway chassis. The existing MGC card is not used.
2. The existing CPPM card serves as the Survivable Call Server. An additional CPPM card is added to the gateway chassis, with the existing MGC card serving as the SIP Gateway.
3. A new CPPM card, serving as the Survivable Call Server, is added to the gateway chassis. The existing CPPM and MGC cards serve as the basic SIP Media Gateway.

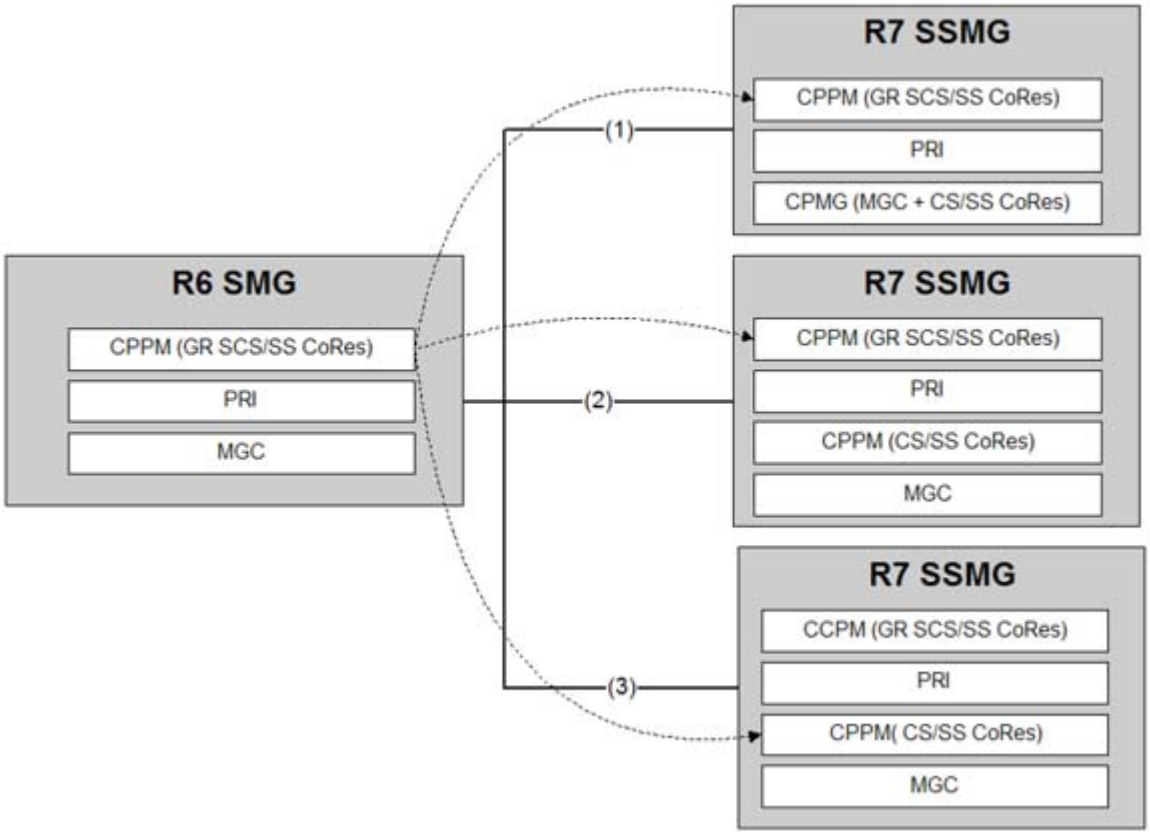


Figure 4: Migration based on CPPM

Hardware Migration based on CPDC

1. A new CPDC card, serving as the Survivable Call Server, and a new CPMG card, serving as the basic SIP Media Gateway, are added to the gateway chassis.
2. The existing CPPM card serves as the Survivable Call Server. A new CPDC card is added to the gateway chassis to serve as the SIP Media Gateway with the existing MGC card.
3. The existing CPPM card serves as the SIP Media Gateway with the existing MGC. A new CPDC card, serving as the Survivable Call Server, is added to the gateway chassis.

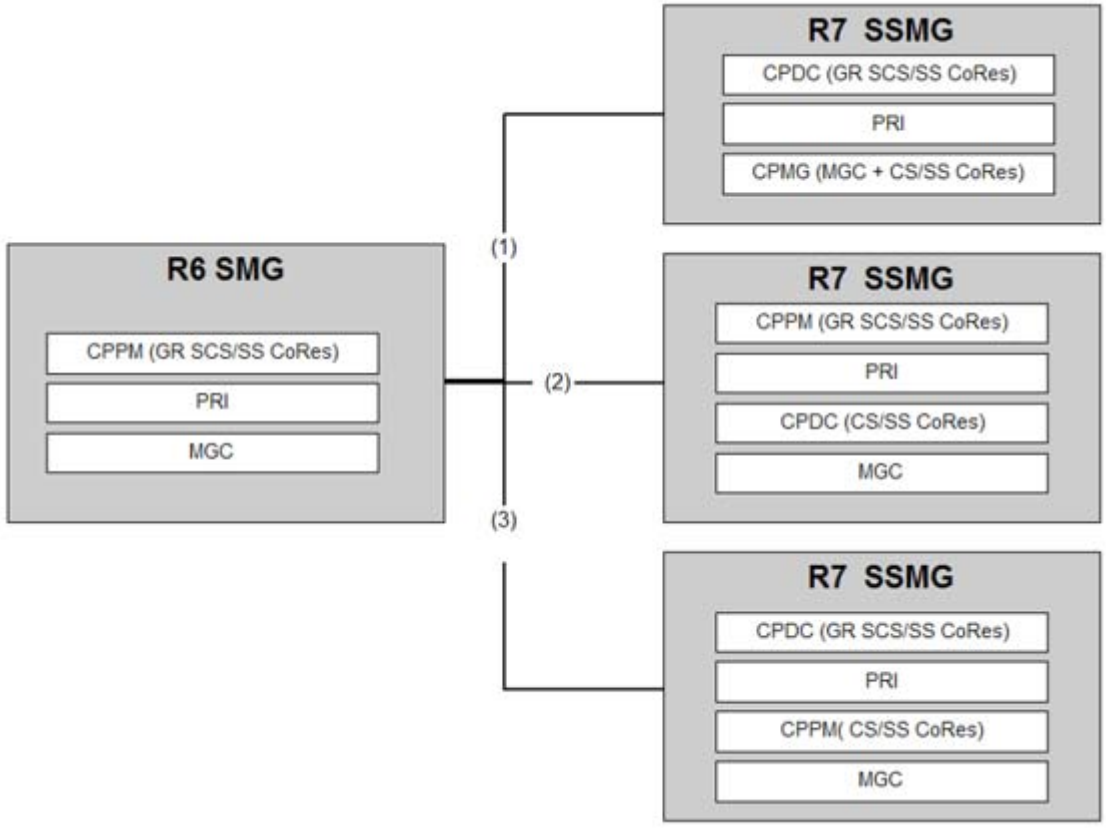


Figure 5: Migration based on CPDC

Hardware Migration based on COTS

1. A new COTS card, serving as the Survivable Call Server, and a new CPMG card, serving as the SIP Media Gateway, are added to the gateway chassis.
2. The existing CPPM card serves as the Survivable Call Server. A new COTS card is added to the gateway chassis to serve as the SIP Media Gateway with the existing MGC.
3. The existing CPPM card serves as the SIP Media Gateway with the existing MGC. A new COTS card, serving as the Survivable Call Server, is added to the gateway chassis.

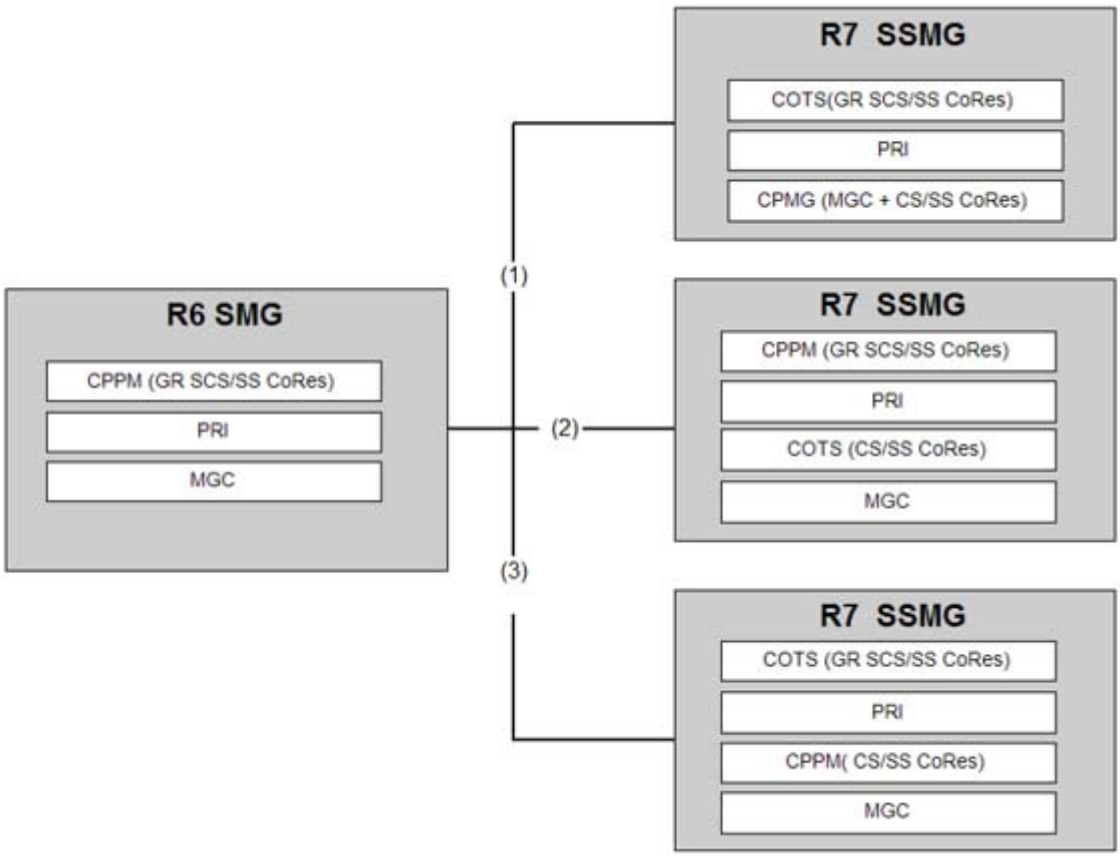


Figure 6: Migration based on COTS

Software Configuration

The configuration of the Survivable Call Server for the SSMG is similar to the configuration of the Survivable Call Server for the SMG. The SIP Media Gateway controller has to be configured independently.

Table 1: Call Server Package Requirements on page 29 summarizes the Call Server package requirements for the Survivable Call Server and the SIP Media Gateway in an HS System.

Table 1: Call Server Package Requirements

Package	Mnemonic	Survivable Call Server (CPPM/ CPDC/COTS)	SIP Media Gateway (CPMG/CPPM/ CPDC/COTS)
404	GRPRIM		X
405	GRSEC	X	
406	SIP	X	X
410	HIGH_AVAIL	X (Optional)	
420	ZBD	X	X

Once installed and deployed, the Survivable Call Server and the SIP Media Gateways are part of the UCM Security Domain. However, manual registration with the UCM Security Domain is required to enable Central Authentication.

There may be extra modifications required in the configuration, if the existing customer database has not incorporated the Zone Based Dialing design, or if the existing Zone Based Dialing design does not fit the overall Zone Based Dialing design for the HS System.

Configuration of the Survivable Call Server

The CS, SS, and the Local NRS run in the Survivable Call Server (CPPM/CPDC/COTS).

Note:

To configure the Survivable Call Server, use the EM deployed with the SIP Media Gateway. Do not use EM HS.

- Configure the GR Database Restoration Policy. The database for the Secondary Call Server is replicated from the Primary Call Server using the existing GR database. Manually invoke database download at the Primary Call Server.
- Configure Node ID

- Configure IPL/TPS
- Configure SIP Gateway, which should register with the network Primary NRS by default. For WAN outage, it could register with a local NRS or point directly to the Survivable Call Server.

Note:

Application ID field in EM: When configuring the node on the Survivable system, the application Node ID field in the Gateway (H.323 and SIP) settings should be set to the Node ID on the Primary Call Server, which is used in the Primary Call Server database against the SIP route. For example, SIP route 1 on the Primary database is configured with Node ID 4444. The Survivable Call Server is configured with Node ID 3333. The Survivable Call Server gets the database from the Primary Call Server. The Survivable Call Server defines application Node ID 4444, so that in survivable mode the SIP trunks associated with route 1 can register.

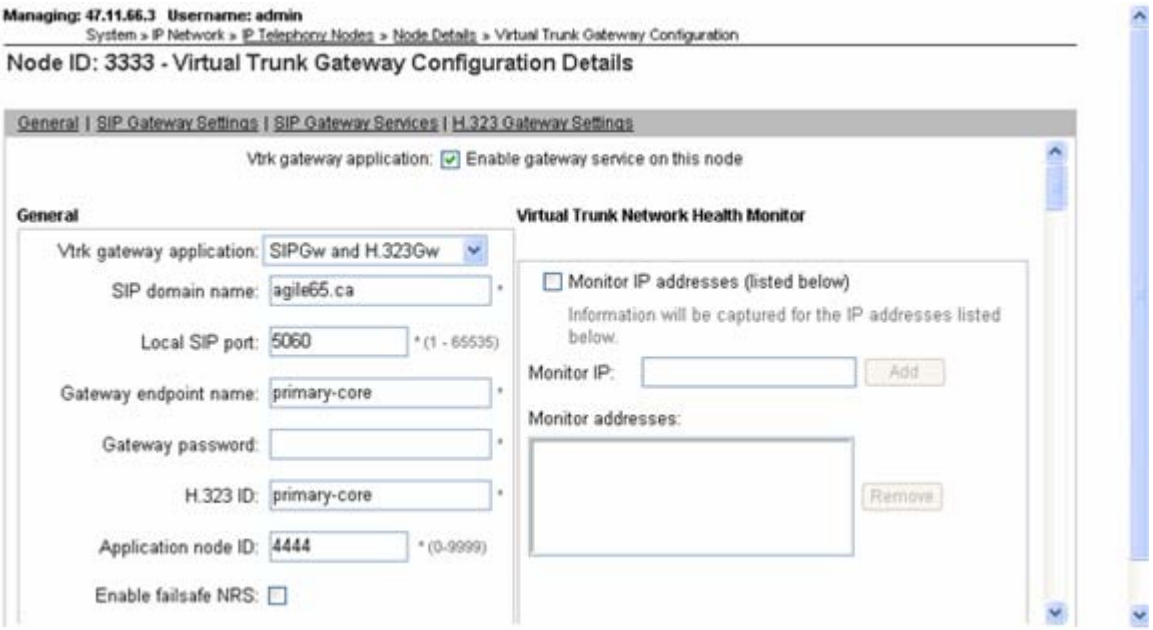


Figure 7: Virtual Trunk Gateway Configuration

- Configure Local NRS for WAN outage

Configuration of the SIP Media Gateway

The SIP Media Gateway is not a GR Secondary Call Server, so it does not receive a replicated database from the Primary Call Server (PCS). The configuration for the SIP Media Gateway is independent of the PCS.

Note:

To configure the SIP Media Gateway, use the EM deployed with it. Do not use EM HS.

- Configure basic customer configuration and basic networking data
- Configure the Numbering Zone according to the overall Zone Dial Plan.
- Configure bandwidth zone for this SIP Media Gateway
- Configure digital trunks for PSTN access.
- Configure ESN routing
- Configure TDM sets as required
- Configure SIP gateway component
- Configure MGC data

Chapter 5: Configure and manage the Communication Server1000 High Scalability System

Communication Server1000 High Scalability System Management Web UI

An administrator starts Communication Server1000 Element Manager HS from UCM Common Services. Communication Server1000 Element Manager High Scalability is a Web-based management application to configure and provision aspects of an HS System. It extends Element Manager (EM) for management of a single Communication Server1000 element:

- EM HS shows a list of HA Groups that are part of the HS System.
- When an administrator uses EM HS to update any of the common data in one of the managed HA Groups, the Common Data Automatic Update Service propagates the change to all other HA Groups within the HS System.
- An administrator can update data that is specific to an HA Group by selecting that group from the list of HA Groups and performing the relevant operation.

The procedures in this section describe the functions available in EM to manage an HS System.

Task Flow

This section provides the following high-level task flow for managing an HS System:

- Set the reference HA group.

  You must set a reference HA group before you configure EM HS Common or Unique data.

  The reference HA group is used to provide the common data configuration view and specifies the HS System common data baseline.

- Common Data View and Unique Data View.

  Common Data is a set of identically configured data blocks across multiple HA groups within an HS System. Since an HS System is viewed as a single Unified Communication

entity, its internal HA groups must share a set of system configuration data, such as Customer, Route, and ESN data blocks, to provide a single system view.

Unique Data is a group of individually configured data blocks for each HA group. For example, station data is unique on a per server basis.

To configure Common Data in an HS System, the administrator must select Common Data View in EM HS, so that the common data configuration will automatically replicate from the reference HA group into all other HA groups belonging to the same HS System.

To configure Unique Data in an HS System, the administrator must select the individual Unique Data View in EM HS, so that the unique data configuration will apply only to the specified HA group.

- Bulk Provision a new HA group.

  Bulk Provisioning replicates all the defined common data from the reference HA group into a target HA group, providing a common data baseline within an HS System.

  Common Data Bulk Provisioning is used to bring a newly deployed HA Group to the same level of service as the other HA Groups in the HS System. Except for the reference HA group, every HA group that joins an HS System must be Bulk Provisioned.

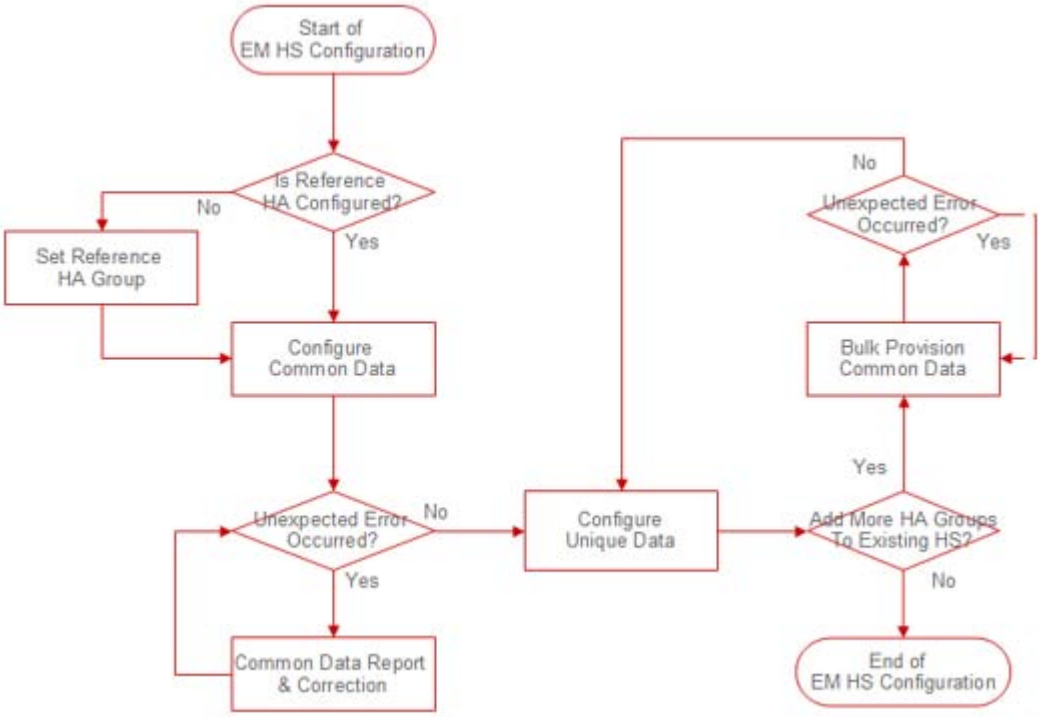


Figure 8: Task flow

Configuration Prerequisites

1. Overall HS System configuration

    a. All HA Groups should register to the same security domain.

    b. Create a user in UCM Common Services with the CS1000 role. Give all permissions related to the CS1000 role to the user. This user should be used to log in to UCM Common Services.

    c. All CS1000 HA groups in the HS system should be of the same system type (CS1000E), the same software load and have the same packages enabled. The HS package should be enabled in all HA groups.

    d. Don’t perform a Bulk Provision operation while scheduled backups are in progress.

    e. Don’t perform a Bulk Provision operation while an audit message is in progress.

2. Bulk Provisioning

    For Bulk Provision to work properly, there are certain unique data elements which need to be set prior to the replication:

    a. The same TTY configurations should be present on both reference and destination HA Groups. The same TTY configurations are required in case there are LD data block dependencies on the TTYs. For example, configure a TTY with USER as CTY on both reference and destination HA groups to successfully replicate the CDR_DATA block.

    b. Pkg-168 is an obsolete package. However, Pkg-168 may be unrestricted, especially when using a database from an earlier release. Ensure that Pkg-168 is restricted and that TMON is set to NO in LD 15 FTR_DATA..

    c. There are number of dependencies when configuring certain data blocks:

        i. To replicate Night Number Table (NNT prompt), the Speed Called List associated with the Reference HA Group must be configured with DNSZ to 4 and SIZE to 10, within the unique data of the new HA group prior to Bulk Provision. To add Speed Call List, MSCL in PARM of LD 17 needs to have sufficient number.

        ii. To replicate CDR_DATA data block in LD 15, a port type ADAN in LD 17 and USER as CTY must be configured within the unique data of the new HA group prior to Bulk Provision.

        iii. To replicate ATT_DATA data block which has the option configured as ILE in LD 15, SETN in LD 12 must be configured within the unique data of the new HA group prior to Bulk Provision.

iv. To replicate NSCL data block in LD 90, LSNO in SSC of LD 18 must be configured within the unique data of the new HA group prior to Bulk Provision.

3. Auto Update

   Bulk Provision must be applied to a new HA Group before the Auto Updates operation occurs.

Set Reference HA Group

Set a reference HA Group within the HS System.

Setting Reference HA Group

1. From the UCM Common Services navigation tree, click **Network, Elements**.

   The Elements page appears.

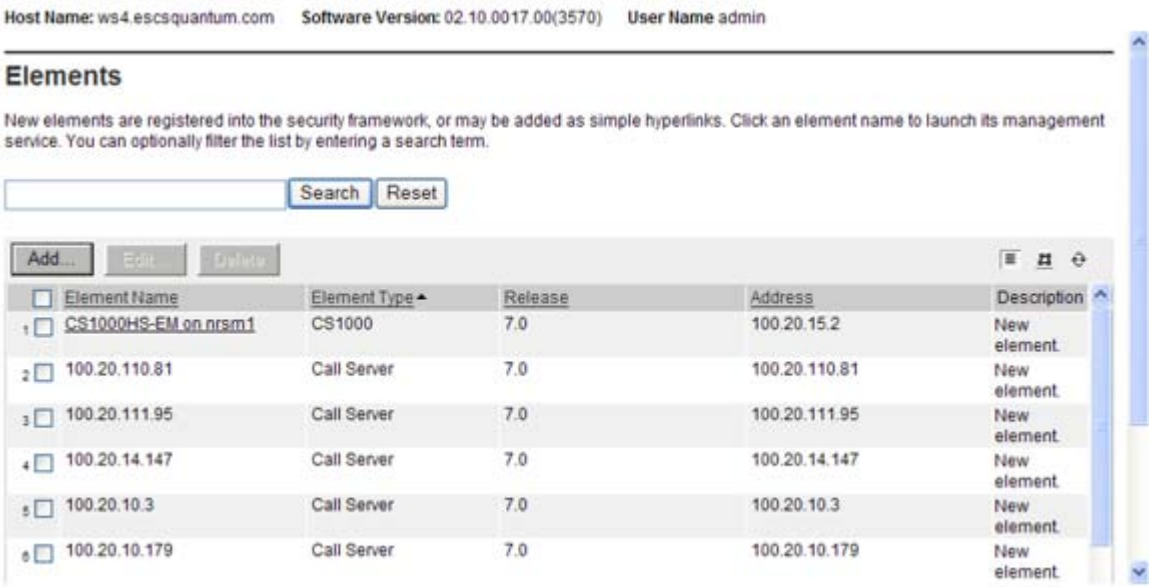


Figure 9: Elements page Table View

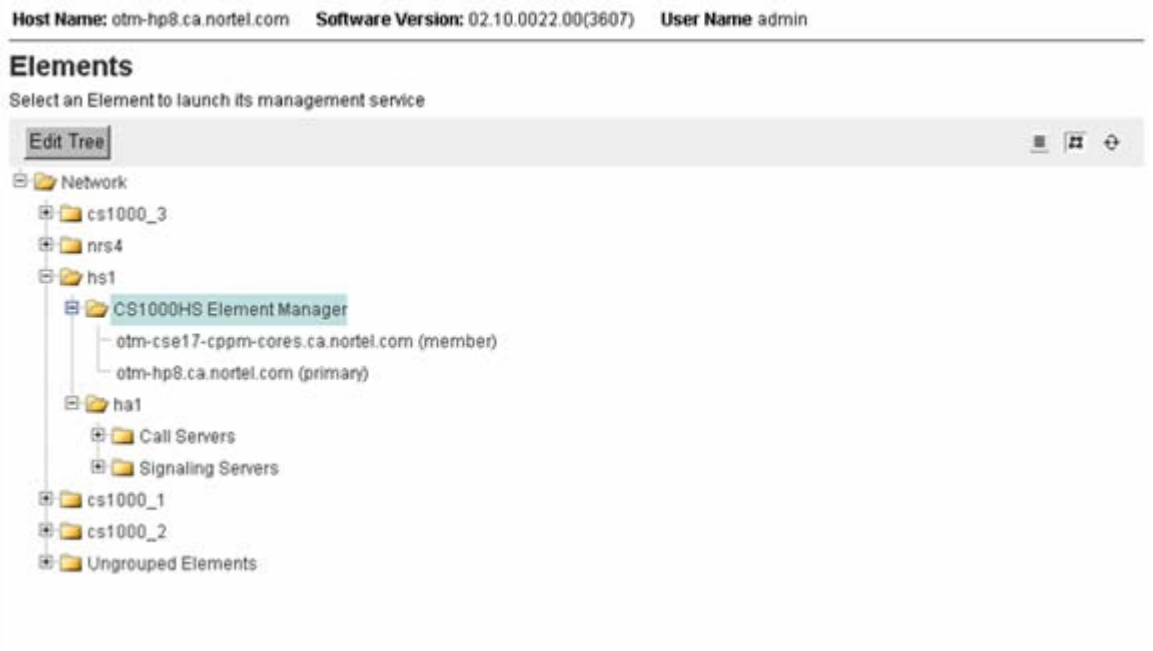


Figure 10: Elements page Tree View

2. Click on the link corresponding to the EM HS System in the **Element Name** column. For example, in Figure 9: Elements page Table View on page 37 the link is "CS1000HS-EM on ibmss9".

   The System Overview page appears.

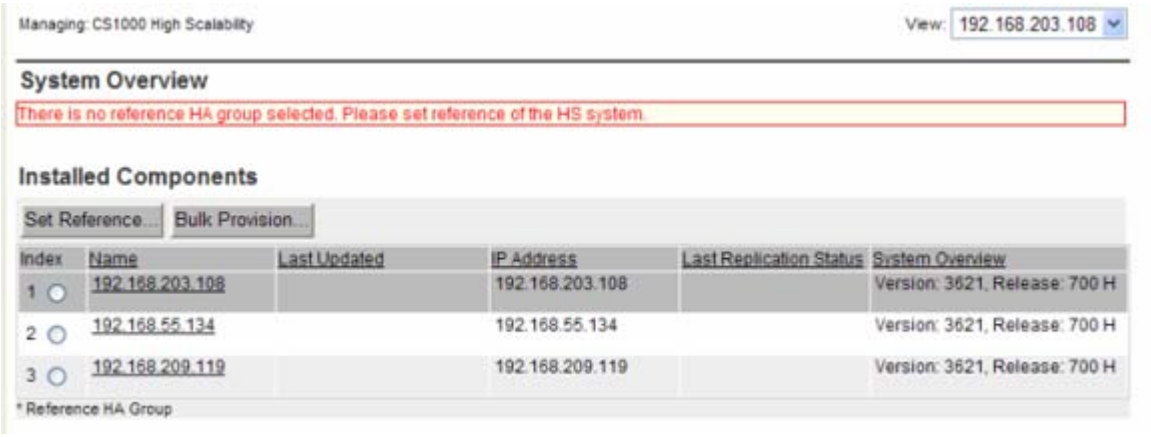


Figure 11: System Overview

3. Select the radio button beside a Call Server in the **Name** column and click the **Set Reference** button.

   Note:
   If the Reference HA Group has been set, the Set Reference button is disabled.

   The Set Reference page appears.

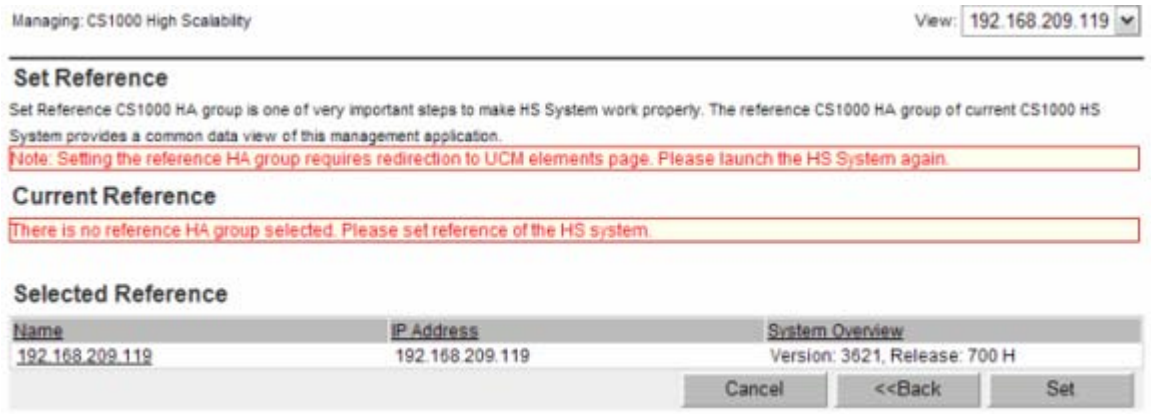


Figure 12: Set Reference

4. Verify the **Selected Reference** HA Group setting. Once the Reference HA Group is set, it can not be unset.
5. Click the **Set** button.

   A confirmation box stating "After successful set reference operation, UCM elements page will be launched. Re-launch Element Manager HS application to continue using. Click OK to continue with setting reference operation." appears.

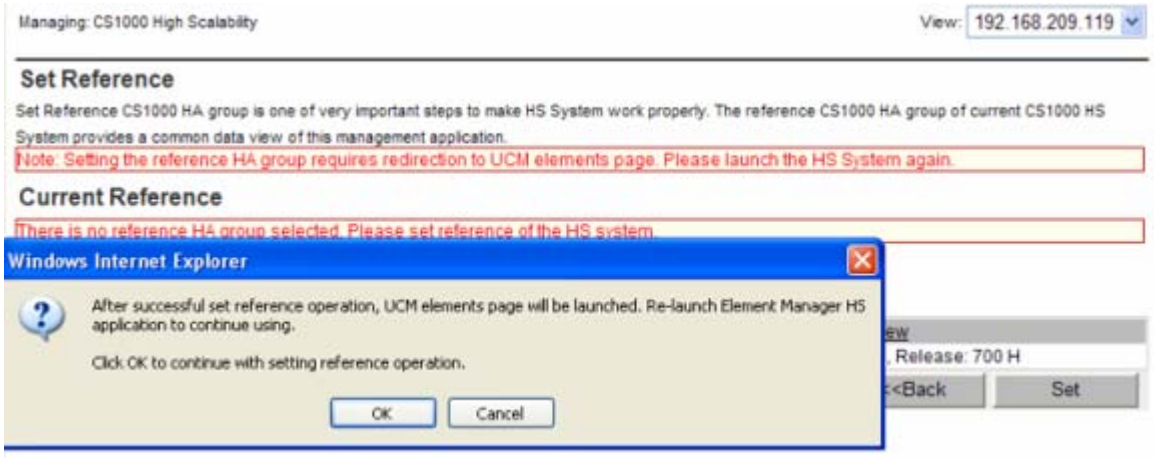


Figure 13: Leaving EM HS application and launching UCM elements page confirmation box

6. Verify the **Selected Reference** HA Group setting and click the **OK** button.

   Note:

   Once the reference HA Group is set, it can not be unset. To set another HA Group as the reference HA Group, the administrator must delete the current reference HA Group from the HS System. After the reference HA Group has been deleted, another Call Sever can be set as the reference HA Group. For more information on deleting an HA Group from an HS System, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

   The Elements page appears. (See Figure 9: Elements page Table View on page 37.)

7. Click on the link corresponding to the EM HS System in the **Element Name** column. For example, in Figure 9: Elements page Table View on page 37 the link is "CS1000HS-EM on ibmss9".

   The System Overview page appears with an updated Installed Components table and an updated View drop down list. Common Data is the first row in the Installed Components table. The Common Data row is high lighted. The name of the reference HA Group is denoted with an asterisk (*).

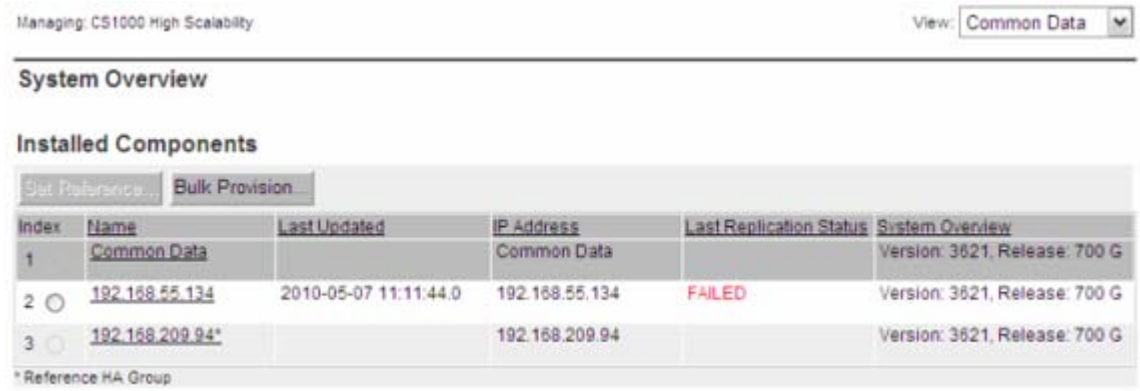


Figure 14: System Overview with Reference HA Group Set

Common Data Configuration

Configure HS System common data.

Set Common Data or Unique Data View

Each HA Group, including the reference HA Group, may have unique data. Setting view sets the data context: common or unique. There are two navigation trees: a Common navigation tree and a Unique navigation tree.

The Common navigation tree only lists links which belong to common data configuration. The Unique navigation tree only lists links which belong to unique data configuration.

Setting Common Data or Unique Data View

1. To configure common data, set Common Data view. To set Common Data view, click on Common Data in the **Name** column of the **Installed Components** table of the System Overview page.

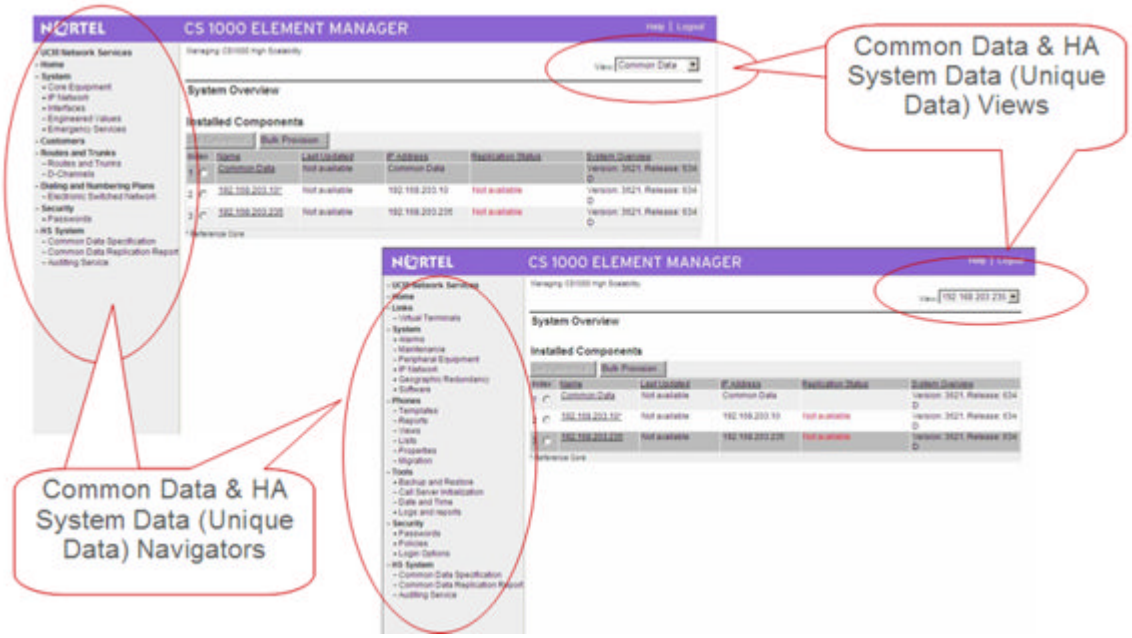


Figure 15: System Overview - Set Common Data or Unique Data View

2. To configure unique data, set Unique Data view. To set Unique Data view, click on an item in the **Name** column of the **Installed Components** table of the System Overview page. For example, in Figure 15: System Overview - Set Common Data

or Unique Data View on page 40 click on **192.168.203.235** to set the Unique Data View for the HA group with IP address 192.168.203.235.

The System Overview page refreshes. The row for the HA group with IP address 192.168.203.235 is high lighted in the Installed Components table and 192.168.203.235 is displayed in the View drop down list.

Or

3. From any EM page, select an item from the **View** drop down list.

   The System Overview page refreshes. The row corresponding to the selected component is high lighted in the Installed Components table and displayed in the View drop down list.

   The navigation tree for the selected installed component is loaded. If the Common Data component was chosen, the common data view has been set and the Common navigation tree is loaded. If any component other than Common Data was chosen, the unique data view has been set and the Unique navigation tree is loaded.

View Context of Data Fields

When the Common Data View is selected, only common data fields should be edited on an EM web page. Exceptional Unique Attributes are highlighted and the warning message "Highlighted field(s) must be filled in from the individual HA Group view" is displayed. The highlighted unique data field(s) must be configured from the individual HA Group view.

If an administrator edits a unique data field when Common Data View is selected, the unique field value will be transferred to the reference HA Group (in New and Change cases). The edited unique field value will NOT be transferred to other HA Groups in the "Change" case, but the value will be transferred to other HA Groups in the "New" case. For an example, see Figure 16: Location Code Common Data View on page 42.

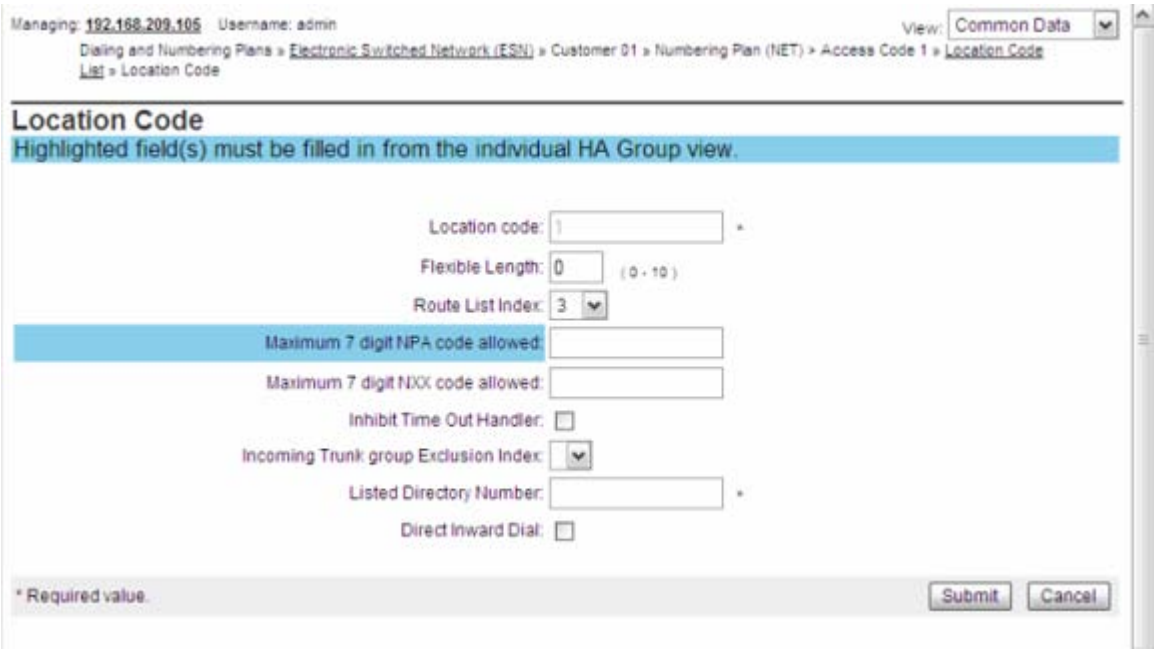


Figure 16: Location Code Common Data View

When the Unique Data View is selected, only unique data fields should be edited on an EM web page. Unique data fields are highlighted and the warning message "Highlighted field(s) should be filled in this HA Group View. Other non-highlighted fields should be filled in Common View" is displayed. The non-highlighted common data fields must be configured from the Common Data view. If the common data fields are modified from the Unique Data view, the modifications will overwrite the existing common data. For an example, see Figure 17: Location Code Unique Data View on page 43.

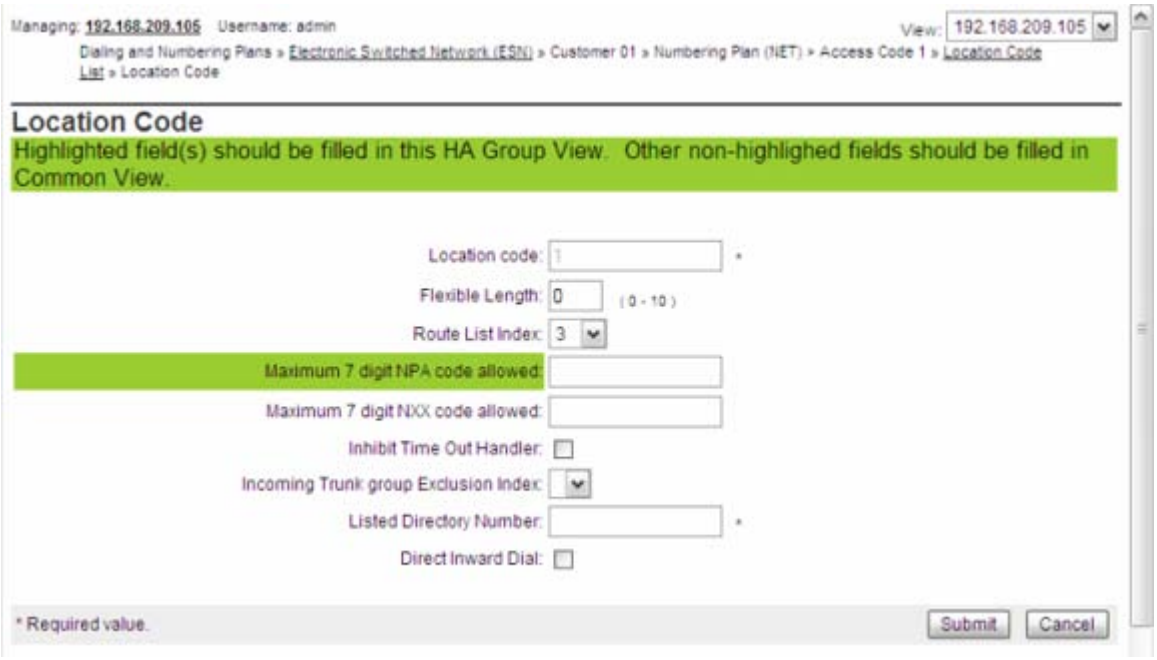


Figure 17: Location Code Unique Data View

Common Data Auto Update Error Report

The Common Data Auto Update Error Reports page appears upon the first occurrence of a transaction failure during a Common Data Automatic Update for a particular HA Group.

Common Data Auto Update Error Reporting

1. If a transaction fails during a Common Data Automatic Update, the Common Data Auto Update Error Reports page appears.

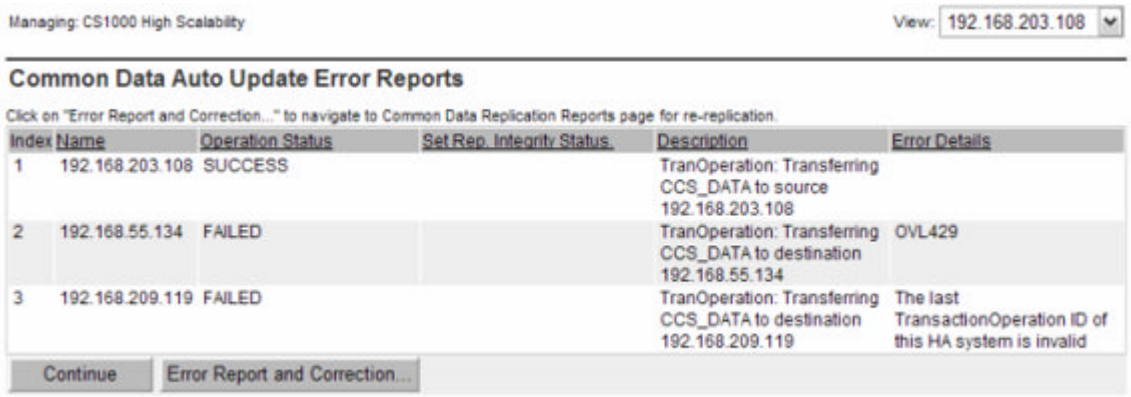


Figure 18: Common Data Auto Update Error Reports

2. Perform one of the following actions:

   - Click the **Continue** button.

     The Element Manger page that was open when the Common Data Automatic Update transaction failed appears. Element Manager continues the operation that was in progress when the transaction error occurred. The transaction error can be corrected at a later time.

   - Click the **Error Report and Correction** button.

     The Common Data Replication Reports page appears with a summary of the Last transaction's operations.

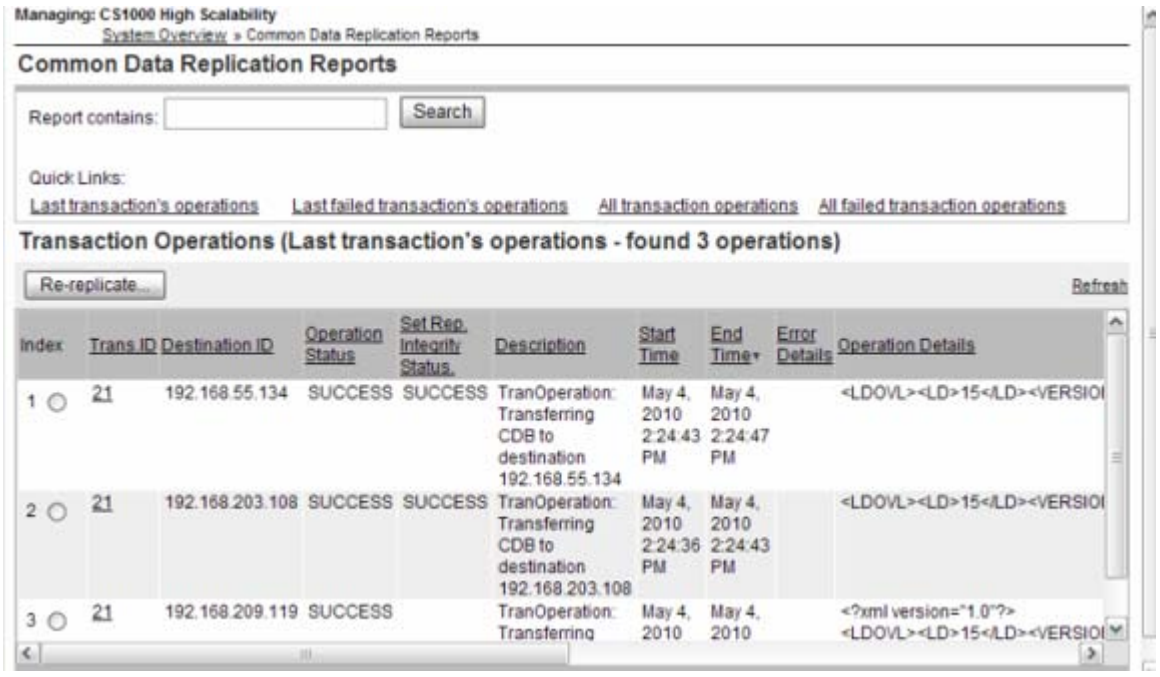


Figure 19: Common Data Replication Reports

An Operation Status has four states:

- Success - the common data was successfully replicated to the destination HA Group.
- Failed - the common data was not successfully replicated to the destination HA Group.
- Outstanding - a transaction operation has failed. The outstanding operation is pending the correction of a transaction error and the re-replication of the failed transaction operation.
- Obsolete - the status of a Failed or Outstanding operation is set to Obsolete after it has been corrected and re-replicated. A new transaction record is created with status Success.

If there are failed transaction operations, the data will not be replicated to the other HA Groups. Correct the transaction error and re-replicate the failed auto update transaction request.

Re-replicate Auto Update

Re-replicate failed auto update transaction requests.

Re-replicating Auto Update

1. From the UCM Common Services navigation tree, click **HS System, Common Data Replication Report**.

The Common Data Replication Reports page appears with a summary of the Last transaction's operations. (See Figure 19: Common Data Replication Reports on page 45.)

2. Click the **List all failed transaction operations** link.

   The Common Data Replication Reports page refreshes with a summary of List all failed transaction operations.

3. Click the **List all transaction operations** link.

   The Common Data Replication Reports page refreshes with a summary of List all transaction operations.

4. Select the radio button in the **Index** column for the transaction to be re-replicated and click the **Re-replicate** button.

   The Auto Update Re-replication page appears.

Figure 20: Auto Update Re-replication

5. Verify all selected transaction operations in the list and click **Execute**.

   The selected transaction is executed and the Auto Update Re-replication page refreshes.

Common Data Specification Configuration

An HS System is installed with a default definition of common data. Within the default definition of common data, an entire data block, or specific attributes (prompts) within a data block, can be set as unique. Data that has been set as unique data can be reset as common data.

To change the default definition of common data, follow the steps in Configuring Common Data Specification on page 47.

Configuring Common Data Specification

1. From the UCM Common Services navigation tree, click **HS System, Common Data Specification**.

   The Common Data Specification page appears displaying a list of the common data blocks.

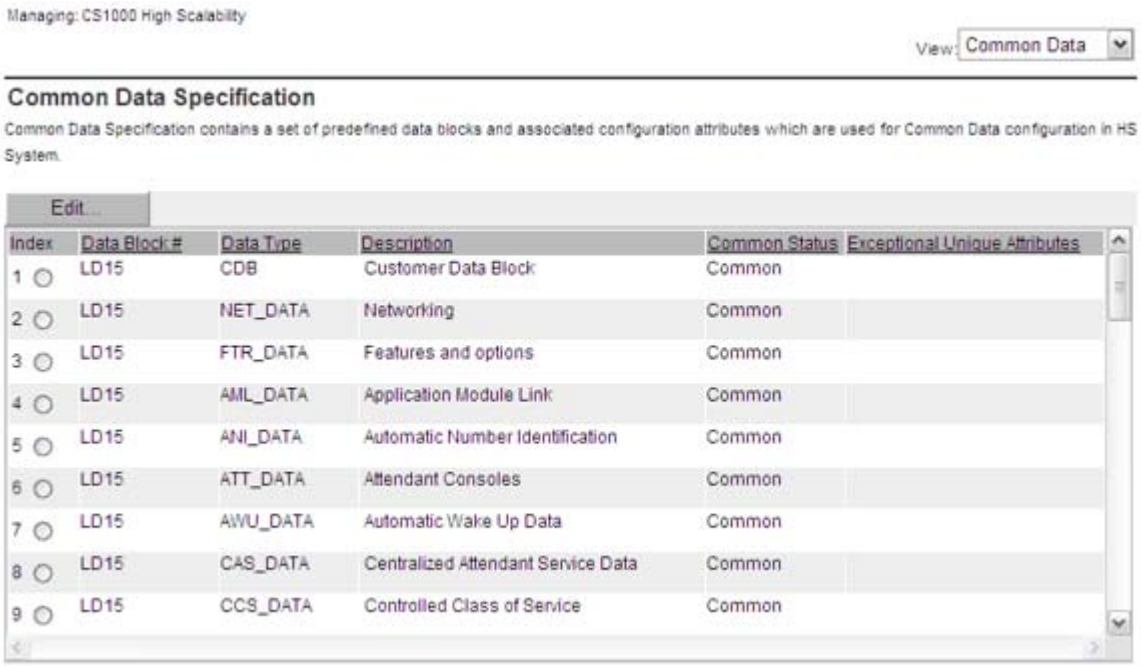


Figure 21: Common Data Specification

2. Select a radio button in the **Index** column of a data block and click the **Edit** button.

   The Common Data Specification Configuration page for the selected data block with its associated configuration attributes appears.

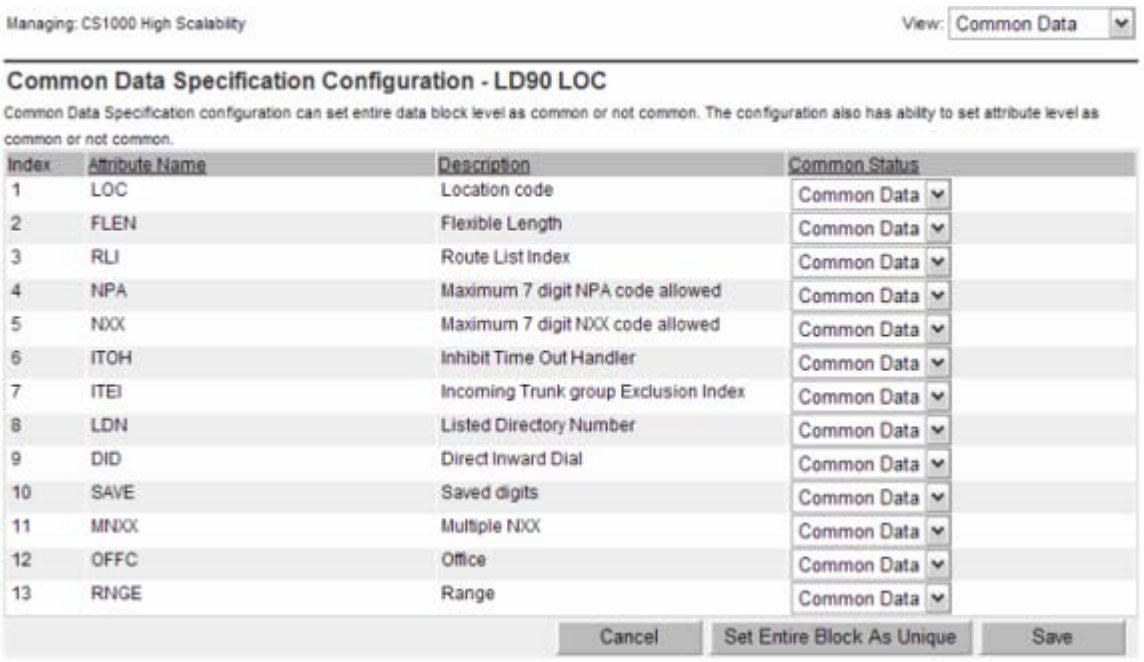


Figure 22: Common Data Specification Configuration - LD 90 LOC

3. Perform one of the following actions:

   - To set one or more attributes (prompts) to unique, select **Unique Data** from the **Common Status** drop down list for the attribute(s) and click the **Save** button.

     The Common Data Specification page appears with the attribute(s) set to unique high lighted in red in the Exceptional Unique Attributes column.

   - If the data block has been set to common, the Common Data Specification Configuration page for the selected data block has three buttons:

     - **Cancel**
     - **Set Entire Block as Unique Data**
     - **Save**.

     To set the entire data block to unique, click the **Set Entire Block as Unique Data** button.

     The Common Data Specification page appears with the row corresponding to the selected data block high lighted in red.

   - If the data block has been set to unique, the Common Data Specification Configuration page for the selected data block has three buttons:

     - **Cancel**
     - **Set Entire Block as Common Data**
     - **Save**.

To set the entire data block to common, click the **Set Entire Block as Common Data** button.

The Common Data Specification page appears.

Bulk Provision a new HA Group

Common data bulk provisioning is used to bring a newly deployed HA Group to the same level of service as the other HA Groups in the HS System.

Bulk Provisioning

Transfer common data as a bulk provision into a target HA Group.

Bulk Provisioning

1. From the UCM Common Services navigation tree, click **Network, Elements**.

   The Elements page appears. (See Figure 9: Elements page Table View on page 37.)

2. Click on the link corresponding to the EM HS System in the **Element Name** column. For example, in Figure 9: Elements page Table View on page 37 the link is "CS1000HS-EM on ibmss9".

   The System Overview page appears. (See Figure 14: System Overview with Reference HA Group Set on page 39.)

3. Select the radio button in the **Name** column for the target HA Group to be provisioned and click the **Bulk Provision** button.

   The Bulk Provision page appears.

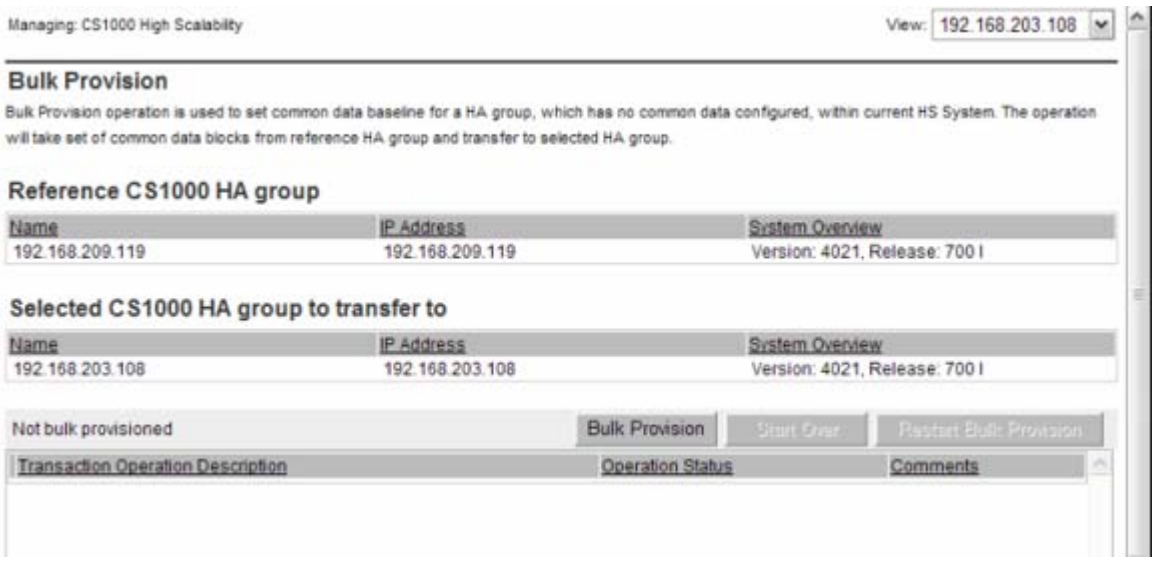


Figure 23: Bulk Provision

4. Verify the **Bulk Provisioning** settings.
5. Click the **Bulk Provision** button.

   The Bulk Provision page refreshes, and displays the status of the Bulk Provision operation and a summary of the Transaction Operations.

Re-replicate Bulk Provisioning

If a Transaction Operation fails during Bulk Provisioning, the Bulk Provisioning process will stop and display the Operation Status. An administrator can re-replicate failed bulk provisioning transaction requests. For more information on re-replicating failed bulk provisioning transactions, see Common Data Bulk Provision Service for a new HA Group on page 11.

Re-replicating Bulk Provisioning

1. From the UCM Common Services navigation tree, click **Network, Elements**.

   The Elements page appears. (See Figure 9: Elements page Table View on page 37.)
2. Click on the link of the HS System in the **Element Name** column.

   The System Overview page appears. (See Figure 11: System Overview on page 38.)
3. Select the radio button beside a Call Server in the **Name** column and click the **Bulk Provision** button.

   The Bulk Provision page appears, and displays the status of the Bulk Provision operation and a summary of the Transaction Operations. (See Figure 23: Bulk Provision on page 50.)

An Operation Status has three states:

- Success - the common data was successfully replicated to the destination HA Group.
- Failed - the common data was not successfully replicated to the destination HA Group.
- Obsolete - the status of a Failed operation is set to Obsolete after it has been corrected and a new transaction record is created with status Success.

Note:

If a Transaction Operation fails during Bulk Provisioning, the Bulk Provisioning process will stop and display the Operation Status. The administrator can correct improper operations, or errors, and restart the Bulk Provisioning process.

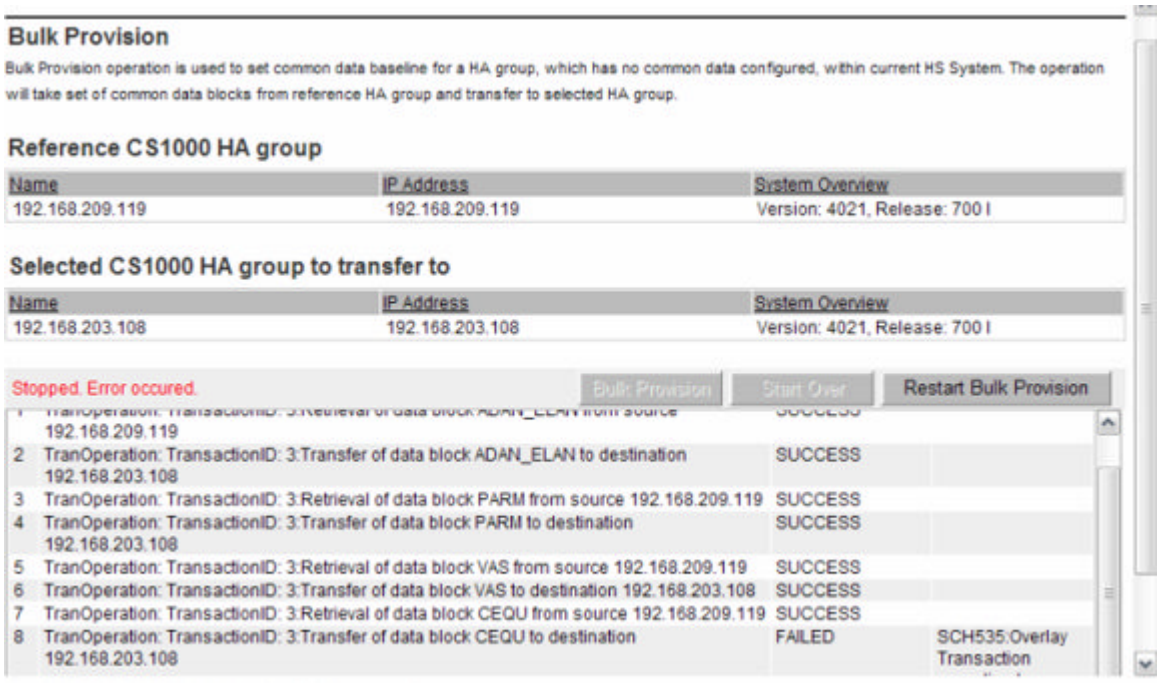


Figure 24: Bulk Provisioning Failure

Note:

If a critical error occurs, the **Start Over** button will be active and the **Restart Bulk Provision** button will be inactive. Click the Start Over button to re-replicate bulk provisioning after a critical failure. The Call Server in the HA Group will be rebooted and all partially transferred data on the destination HA Group will be erased.

4. Click the **Restart Bulk Provision** button.

   The Bulk Provision page refreshes and displays the status of the Restart Bulk Provision operation.

Review Common Data Replication Reports

All common data transactions and associated transaction operations are recorded. Once a transaction has been performed, an administrator can review the common data replication report and rerun failed transactions. For more information on rerunning failed transactions, see Common Data Service Replication Reliability on page 11.

Reviewing Common Data Replication Reports

1. From the UCM Common Services navigation tree, click **HS System, Common Data Replication Report**.

   The Common Data Replication Report pages appears with a summary of the Last transaction's operations. (See Figure 19: Common Data Replication Reports on page 45.)

2. Perform one of the following actions:

   - Enter a search string in the **Report contains** box and click **Search**.

     There are no restrictions on the search string. For example, the search string could be an IP address, load number, prompt name, error message or error code.

     The Common Data Replication Reports page refreshes with a summary of the transaction operations containing the search string.

   - Click one of the **Quick Links**.

     The Quick Links target frequently used high-run queries.

     - Last transaction's operations: lists all the operations of the last transaction. It is the default query when the Common Data Replication Reports page appears.
     - Last failed transaction's operations: lists all the transaction operations associated with the last failed transaction.
     - List all transaction operations: lists all the transaction operations.
     - List all failed transaction operations: lists all the failed transaction operations.

     The Common Data Replication Reports page refreshes with a summary of the corresponding transaction operations.

Common Data Audit Services

The common data audit services screen the last common data transaction between the HS management system and an individual HA Group to determine the integrity of the common data provisioning sequence.

Schedule Daily Audit Services

To schedule a daily audit service report, follow the steps in Scheduling Daily Audit Services on page 53.

Scheduling Daily Audit Services

1. From the UCM Common Services navigation tree, click **HS System, Audit Services**.

   The Common Data Auto Service Configuration page appears.

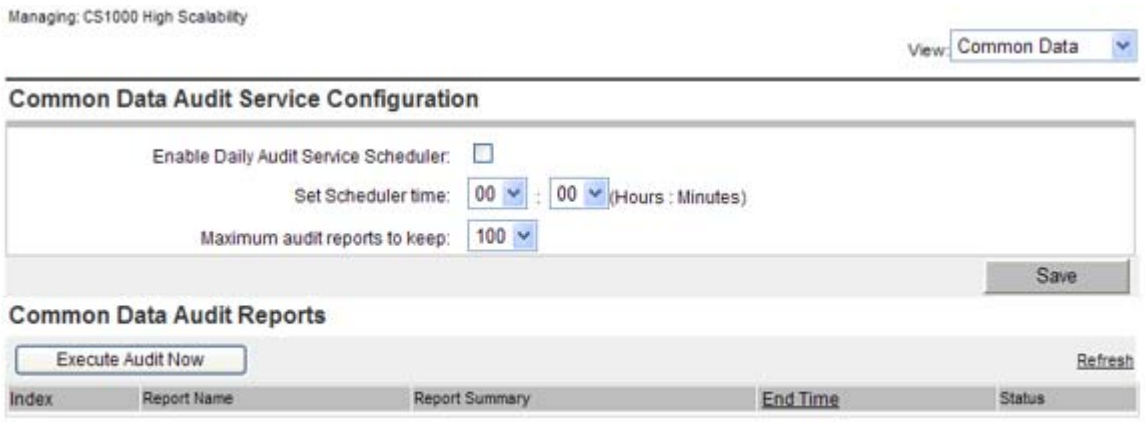


Figure 25: Common Data Auto Service Configuration

   The default Audit Service Scheduler values are:

   - Enabled - not enabled
   - Scheduler time - 00:00 (Hours : Minutes)
   - Maximum audit report to keep - 100

2. Click the **Enable Daily Audit Service Scheduler** check box to enable the Audit Service Scheduler.
3. Set **Scheduler time** and **Maximum audit reports to keep**.

4. Click the **Save** button.

   The Common Data Auto Service Configuration page refreshes.

5. Click the **Refresh** link on the Common Data Audit Reports table to update the table.

Manual Audit

To update the common data audit services reports table manually, follow the steps in Performing Manual Audit on page 54.

Performing Manual Audit

1. From the UCM Common Services navigation tree, click **HS System, Audit Services**.

   The Common Data Auto Service Configuration page appears. (See Figure 25: Common Data Auto Service Configuration on page 53.)

2. Click the **Execute Audit Now** button.

   The Common Data Auto Service Configuration page refreshes.

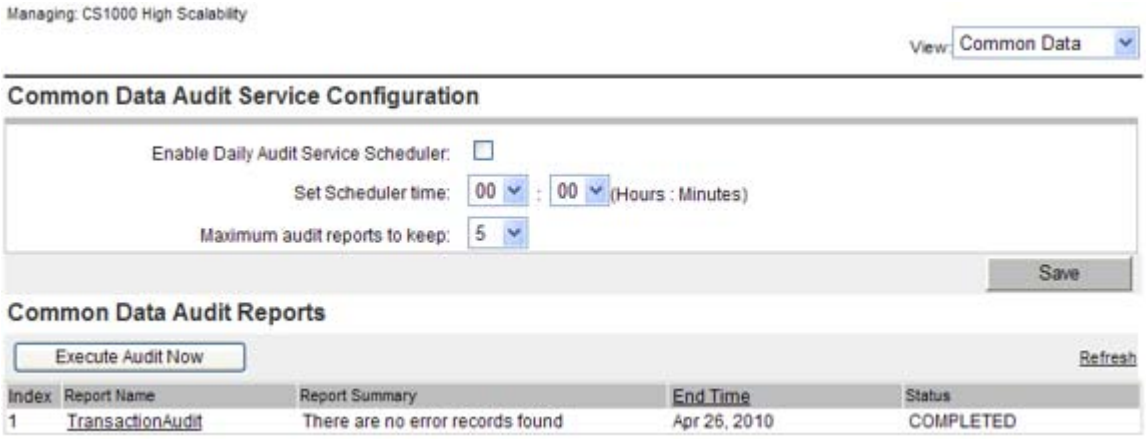
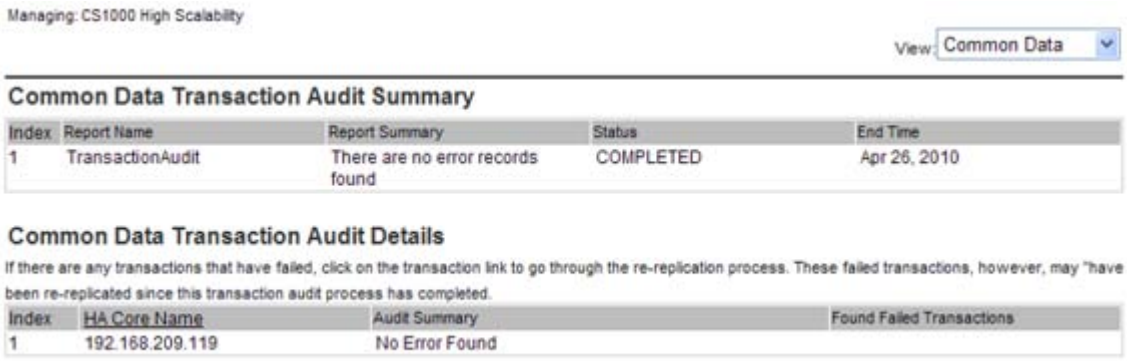


Figure 26: Common Data Audit Reports Table

3. Click on a link to an audit report in the **Report Name** column of the Common Data Audit Reports table

   The Common Data Transaction Audit Summary page opens with a summary of Common Data Transaction Audit Details.


Managing: CS1000 High Scalability

View: Common Data

Common Data Transaction Audit Summary

Index	Report Name	Report Summary	Status	End Time
1	TransactionAudit	There are no error records found	COMPLETED	Apr 26, 2010

Common Data Transaction Audit Details

If there are any transactions that have failed, click on the transaction link to go through the re-replication process. These failed transactions, however, may "have been re-replicated since this transaction audit process has completed.

Index	HA Core Name	Audit Summary	Found Failed Transactions
1	192.168.209.119	No Error Found	

Figure 27: Common Data Transaction Audit Summary

Chapter 6: Appendix Common Data

With the exception of the following prompts

- the SPVC prompt in the ATT_DATA block of LD 15
- the ALDN and PREO prompts in the FTR_DATA block of LD 15
- the VNR prompt in the NET_DATA block of LD 15

all prompts in the data blocks listed in Table 2: Default definition of common data on page 57 are included in the default definition of common data.

Table 2: Default definition of common data

Load Number	Data Block Type	Description
14	IPTI	IP TIE trunk data block
15	CDB	Customer data block
15	DEFAULT	Default customer data block
15	AML_DATA	Application Module Link options
15	ANI_DATA	Automatic Number Identification numbers
15	ATT_DATA	Attendant Console options (Except prompt SPVC)
15	CAS_DATA	Centralized Attendant Service options
15	CCS_DATA	Controlled Class of Service options
15	CDR_DATA	CDR and Charge Account options
15	FCR_DATA	New Flexible Code Restriction options
15	FFC_DATA	Flexible Feature Code options
15	FTR_DATA	Features and options (Except prompts ALDN and PREO)
15	INT_DATA	Intercept treatment options
15	LDN_DATA	Departmental Listed Directory Numbers
15	MPO_DATA	Multi-Party Options
15	NET_DATA	ISDN and ESN Networking options (Except prompt VNR)
15	PWD_DATA	Customer related Passwords
15	RDR_DATA	Call Redirection
15	ROA_DATA	Recorded Overflow Announcement options

Load Number	Data Block Type	Description
16	RDB	Route data block and Meridian 911
16	AWR	Automatic Wake Up trunk block for RAN/Music
16	CAA	Common Control Switching Arrangement
16	CAM	Central Automatic Message Accounting trunk
16	CBCT	Call by call master route cbc_pkg-23
16	COT	Central Office Trunk data block
16	CSA	Common Control Switching Arrangement access
16	DIC	Dictation trunk data block basic-1
16	DID	Direct Inward Dialing trunk data block
16	FEX	Foreign Exchange trunk data block basic-1
16	FGDT	Feature Group D trunk fgd-17
16	IDA	Integrated Digital Access
16	ISA	Integrated Service Access route or Call-by-Call
16	MCU	Meridian Communications Unit port basic-18
16	MUS	Music trunk data block
16	PAG	Paging trunk data block basic-1
16	R232	DAC for NT7D16 on RS-232 port basic-18
16	R422	DAC for NT7D16 on RS-422 port basic-18
16	RAN	Recorded Announcement trunk data block
16	RCD	Emergency Recorder trunk data block
16	RLM	Release Link Main trunk data block
16	RLR	Release Link Remote trunk data block
16	TIE	TIE trunk data block
16	TIE ATL	TIE ATL data block for Sweden supp-15
16	TIE SEMI	Semi-automatic TIE trunk data block opcb-14
16	TIE AUTO	Automatic TIE trunk data block opcb-14
16	TIE TONE	Tone TIE trunk data block opcb-14
16	WAT	Wide Area Telephone Service trunk data block basic-18
17	ADAN	All input/output devices (includes D-channels) basic-19
17	CEQU	Common Equipment parameters basic-19
17	PARM	System Parameters basic-19

Load Number	Data Block Type	Description
17	VAS	Value Added Server
24	ESA	Emergency Services Access data block
86	DGT	Digit manipulation data block
86	ESN	ESN data block
86	ITGE	Incoming Trunk Group Exclusion data block
86	RLB	Route List data Block
87	FCAS	Free Calling Area Screening
87	FSNS	Free Special Number Screening
87	NCTL	Network Control
90	NET	Network translation tables
90	HNPA	Home NPA translation code
90	LOC	ESN Location Code translation data block
90	NPA	Numbering Plan Area code translation data block
90	NSCL	Network Speed Call List data block
90	NXX	Central Office Code Translation data block
90	SPN	Special code translation data block
117	ERL	Emergency response location
117	NumZone	Numbering Zone