July 2020

END USER HOME CLUSTER MOBILITY

Muthuviji Karuppiah

Ashwin Anand

END USER HOME CLUSTER MOBILITY

AUTHORS:

Muthuviji Karuppiah
Ashwin Anand

ABSTRACT

A method is provided for marking an end user with SuperUser access, in order to enable user to seamlessly login to any cluster in a Tactical Corps Network (TCN) during a critical situation when the home cluster is no longer available.

DETAILED DESCRIPTION

In a Tactical Corps Network (TCN) used for communications in military combat situations, it is well known that an emergency is inevitable, and it is more challenging to tackle communication in critical situations. An end user can log in to any cluster using an Extension Mobility Cross Cluster (EMCC) feature. In an extreme case, one of the clusters is not available or is destroyed. In such a situation, at which point, if the primary cluster has failed, the commissioned officers would not be able to login to any other cluster, as EMCC would cease to work. This would hinder all forms of effective communication and causing chaos.

However, consider the advantages if an end user, at this time, could log in to any of the clusters in the Tactical Corps Network and experience all the features as he or she would in their home cluster.

Presented herein is a mechanism to seamlessly synchronize users (commissioned officers such as Generals, Majors, Captains - further addressed as SuperUsers herein) across all clusters of the Tactical Corps Network, thereby enabling the SuperUsers to login to any cluster in the Tactical Corps network at any point of time, while having the same experience as that of his home cluster, thus enabling effective leadership and communication across the corps.

In short, the SuperUser who logs into any roaming/visiting cluster essentially can be contacted at the same directory number (DN) by others. Also, he or she can dial the same patterns to reach out to other end users, and also experience the same capabilities as his home or base cluster across the entire TCN.

Terminology:

Home Cluster / Base Cluster - This is the cluster where the SuperUser's own desk phone is registered.

Roaming/Visiting Cluster - This is the cluster where the SuperUser does not have a designated desk phone, however, the user can EM-login to any EM-capable phone just like in his/her base cluster.

CSS - Calling Search Space

ILS - Inter-Cluster Lookup Service

EM - Extension Mobility

GDPR - Global Dial Plan Replication

DN - Directory Number

CM – Call Manager

AXL - Administrative XML Web Service

TCN - Tactical Corps Network

ACG - Access Control Group

Assumptions:

1. A Tactical Corps Network will typically have around 100 Unified CallManager Cluster, growing over to say 7 or 8 such clusters since a military architecture would be a distributed one.
2. At a given time, at least 15 % of the total users would be deemed as SuperUsers, who would be able to connect to any other cluster in the network.

Design Considerations

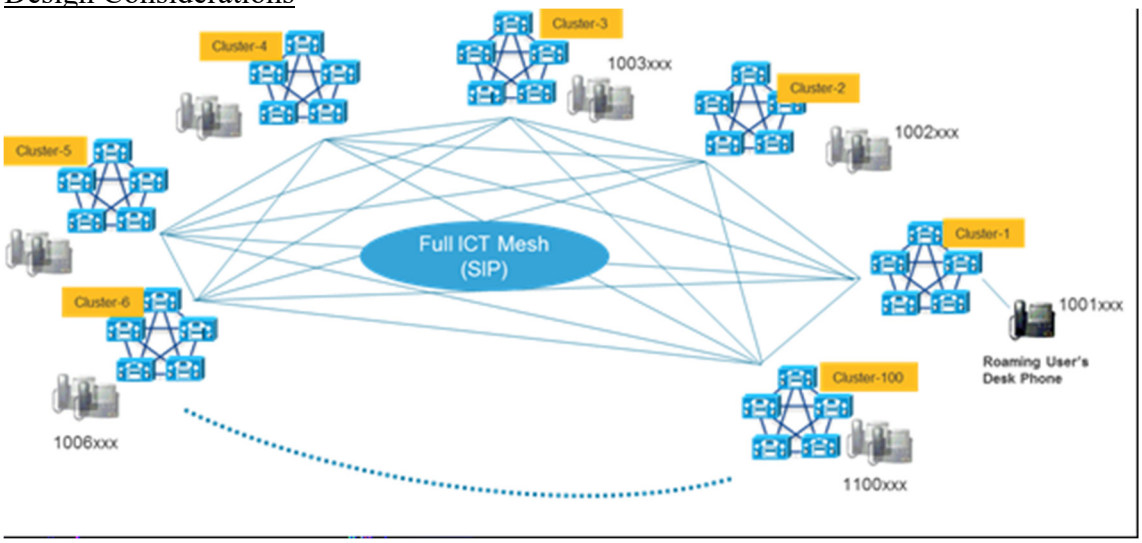

Figure 1

Reference is made to Figure 1 above.

A Primary Intention is only to support Roaming across Clusters and NOT Phone Device Portability.

Phone Device Portability: Roaming user carries his phone everywhere he goes, he can plug in the phone to any cluster, the phone can register and make/receive calls every cluster, with the same end-user experience

Roaming Across Cluster: Roaming user can EM-login to a registered device on any cluster, using identical credentials and profile in every cluster.

A uniform dial plan needs to be maintained across the TCN.

Roaming across clusters is only within the same Tactical Corps Network, not across TCN.

Within the same TCN network, every user must have distinguishable DN (i.e. No two users will have the same primary DN).

The roaming users must keep their own DN after logging into another cluster.

ILS deployment is mandatory.

Functional Description:

Creation of a Super User

CM supports Extension Mobility Login (EM Login) and Inter-Cluster Lookup Service feature for the users who are authenticated as Super User by admin.

A user can be authenticated as a SuperUser if added under a particular Access Control Group (ACG), the **Standard EM Roaming Super Users Across Cluster** access control group.

SuperUser EM Login across clusters – Figure 2

CM to support EM (Extension Mobility) login for a SuperUser created across clusters.

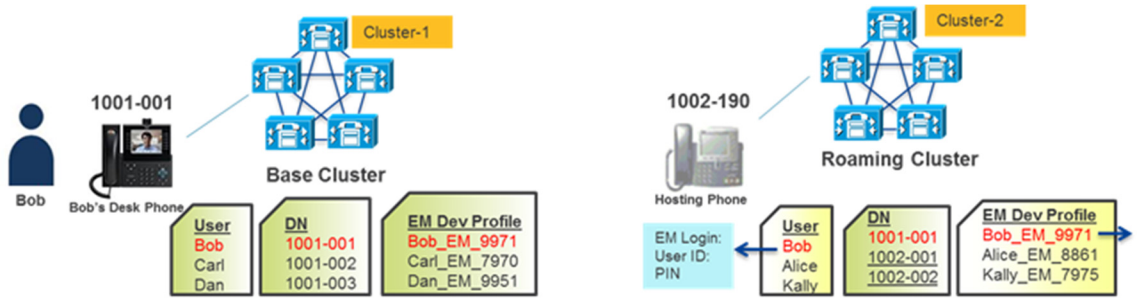

Figure 2

End User (Roaming user) details like the User ID, DN, and Device profile are configured in all the clusters present under a TCN. After EM Login, a SuperUser is able to make calls from the roaming cluster the same way as in the base cluster.

- User Class

If a CSS/Partition is associated with the roaming user's DN in the base cluster, the equivalent CSS/Partition is provisioned to the same DN in all other clusters, so that after EM login to roaming cluster, the user has the same call privileges as that in the base cluster.

- Dial Pattern

The same dial pattern should be maintained for the roaming user. i.e., the calling user dials the same digit string to reach another user in the network, regardless of which cluster (base

or roaming), the user is calling. Dynamic discovery/learning is achieved by deploying ILS (Inter-cluster Lookup Service)

Note: Details are shared with the networks regardless of the cluster in which the user is logging-in. Dynamic discovery can be achieved by ILS (Inter-Cluster Lookup Service).

Dynamic Discovery using ILS -- Figures 3 and 4

The ILS cluster discovery feature automatically populates the list of remote clusters. Each cluster in an ILS network exchanges update message, called peer info vectors, which are designed to inform remote clusters of the status of each cluster in the network. The update messages contain information about the known clusters in the network which includes:

- Cluster IDs
- Cluster descriptions and versions
- The fully qualified domain name of the host
- IP addresses and hostnames for the cluster nodes that have ILS activated
- Since we cannot have a dependency of one cluster to another, every cluster has to be ILS Hub

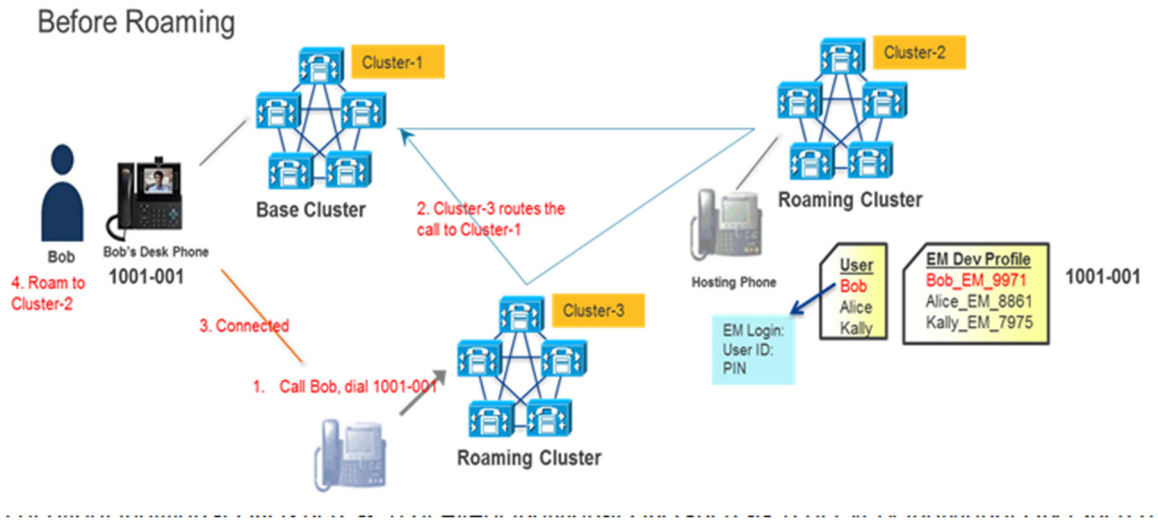

Figure 3

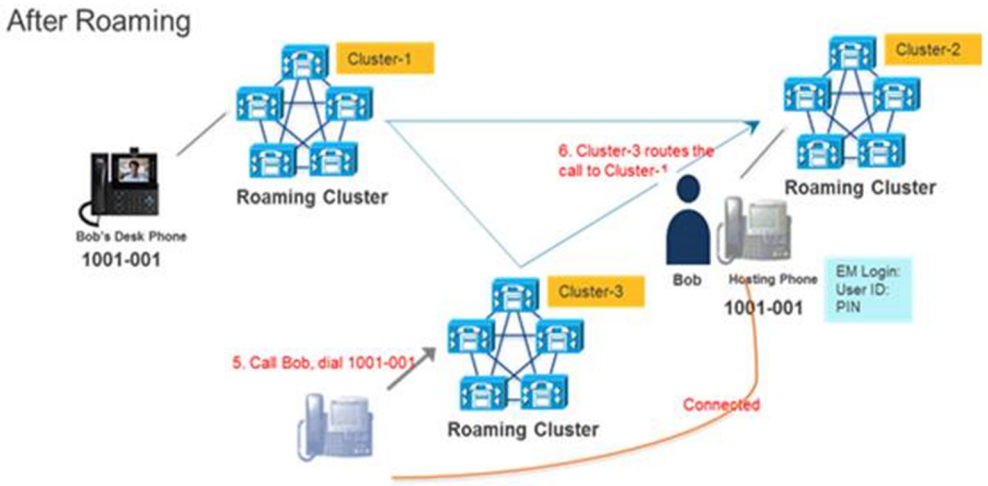

Figure 4

EM and ILS Interaction

If a SuperUser logs into a visiting cluster, a notification is sent which updates the Roaming User logged in details, which triggers a signal to the ILS network under which cluster is associated.

This signal will notify and share the available information with other clusters under the ILS network. Once the information is shared, the User will be able to perform actions like making calls.

- At EM login to roaming cluster, EM Service should trigger an ILS advertisement to add GDPR (Global Dial Plan Replication) record for the user's DN, now associated with the roaming cluster. This allows all clusters to route call toward this user, to this roaming cluster.
- At EM logout from the roaming cluster, EM Service should trigger an ILS advertisement to remove the GDPR record for the user's DN associated with this cluster. This makes sure all clusters stop routing a call to the user to the 'obsolete' roaming cluster.
- At EM login to the roaming cluster, EM Service should trigger an ILS advertisement to remove the existing GDPR record for the user's DN. This is to ensure the obsolete record is removed if the user did not log out properly.

- Above is done for 'SuperUser' only.
- All features of EM like Auto logout or multiple logins are also supported.

SuperUser Synchronization Tool

To visualize the usability of the feature end-to-end, the SuperUsers, User Profiles, Partitions, and the Calling Search Spaces are synchronized across the clusters in the network. Doing this manually, and on a regular basis is a cumbersome process. To ease this effort and to provide additional functionality, the SuperUser Synchronization Tool is employed.

The web-based SuperUser Synchronization Tool synchronizes all the roaming SuperUsers which are present across various CM clusters. All the roaming super users and their end-user details along with their respective device profiles will be available in their respective CM clusters. The Administrator would need to configure all the clusters which are present in their network into this SuperUser Synchronization Tool. The administrator also needs to identify the users in the CM as SuperUsers by placing them under an access control group (ACG) meant to identify the roaming SuperUsers. The Scheduled service in the tool will basically synchronize the SuperUsers and their respective details across all the CM clusters.

The SuperUser Synchronization Tool may be a standalone server. The redundant server can be down and whenever the standalone server goes down, a redundant server can be brought up.

The various functions that the tool supports are:

1. Configuring the Clusters in the SuperUser Synchronization tool.

Tool administrator can configure the required clusters in the TCN where the SuperUsers need to be synced.

2. Elevating the normal users to SuperUsers in the CM Clusters

To identify the super users in the CM clusters, the super users need to be assigned the Access Control Group (ACG) named as "Standard EM Roaming Across Clusters Super Users". This ACG has the following roles:

Access Control Group Name	**Roles Associated with Access Control Group**
Standard EM Roaming Super Users Across Cluster	Standard CM End Users
	Standard CMUSER Administration

As an Administrator, he will need to go to the end user page for the CM Administration, identify the user, and assign the Access Control Group. The Roles mentioned above will be automatically assigned to that user. The Administrator has now elevated the user from a normal user to a SuperUser. When synchronization, happens the same user will be propagated to all the other clusters.

3. Creation of Super Users from the SuperUser Synchronization Tool

In case one wants to configure the SuperUsers from the SuperUser Synchronization Tool, then the administrator needs to get the list of super users with their base cluster-ID in a CSV format and upload that into the tool. Once the upload is finished, the administrator will be navigated to a web page showing the list of the SuperUsers. Whenever the synchronization happens, it will take the users and associate them with the Access Control Group named 'Standard EM Roaming Super Users Across Cluster' in the base cluster and it will sync these users in all the other Clusters.

4. Delete a SuperUser from the SuperUser Synchronization tool

The Administrator can explicitly provide the SuperUser information to be deleted by providing the user identifier in the tool itself. When the Synchronization happens, it will delete the respective user from all the Clusters.

5. Delete a SuperUser from any cluster using the CM Admin interface

When the Administrator deletes the user from the CM Admin and triggers a synchronization process by clicking on the Synchronize now or whenever the synchronization schedule is hit. At that time the Synchronization Service will get the SuperUser from all clusters and compare it with super users stored in tool database. If there is a mismatch, then the corresponding changes are propagated to other clusters.

6. Mark the SuperUser as a normal user from the SuperUser Synchronization tool

In this case, the administrator will explicitly mark the SuperUser as a normal user by providing the user identifier in the tool itself. When Synchronization occurs, it will move the user out of the ACG only in his base cluster and the Synchronization process will delete the user from the clusters.

7. Mark the user as a normal user from his/her base cluster from CM Admin interface

In this case, the administrator moves the user in its base cluster from SuperUsers Access Control Groups to the normal access control group and when synchronization occurs, it will obtain the SuperUser from all clusters and compare it with super users stored in tool database. If the User11 is made as normal user from his/her base cluster (Cluster1), then User11 from all other clusters, except the base cluster.

Before Synchronization

*Users marked in red color are SuperUsers in the CM cluster

Cluster1	**Cluster2**	**Cluster3**
User11	User21	User31
User12	User22	User32
User13	User23	User33
User14	User24	User34
User21	User11	User11
User31	User31	User21

After Synchronization

(User 11 is marked as a normal user in the base cluster) After Synchronization, the User11 is removed from all other clusters.

*Users marked in red color are super users in the CM cluster. The strike-through Users are the ones deleted after synchronization.

Cluster1	Cluster2	Cluster3
User11	User21	User31
User12	User22	User32
User13	User23	User33
User14	User24	User34
User21	~~User11~~	~~User11~~
User31	User31	User21

8. Scheduling the service in the tool which will synchronize the users across the clusters

The Synchronization service can be scheduled daily or weekly as per the administrator's choice. The administrator can also set a particular time when the synchronization will start. The synchronization end time will depend upon the number of clusters and the number of users that are present in the cluster.

9. Synchronization of User Profiles, and the class of control entries

The administrator has the control to synchronize the user profiles from the home cluster to other clusters in the network. The administrator can also include the partitions, and the calling search spaces to be synchronized.

10. Resetting the password and security questions in the tool

The administrator can log in to the tool and go to the Profile Settings section and change the password and security questions and its answers as per his or her choice.

Currently, the deployment requires the clusters to be configured as Hubs in the ILS network. This is because, if configured with a Hub-Spoke topology, and if one of the Hubs goes down, then it would affect the feature utility.

An enhancement in the ILS may be made, wherein, unavailability of a Hub in a Hub-Spoke setup, can elevate one of the Spokes to a Hub, which thereby can perform the required duties. Basically, facilitating an uninterrupted mechanism to provide a failover-fallback mechanism for the ILS network.

In summary, a method is provided for marking an end user with SuperUser access, in order to enable user to seamlessly login to any cluster in the TCN during a critical situation when the home cluster is no longer available.