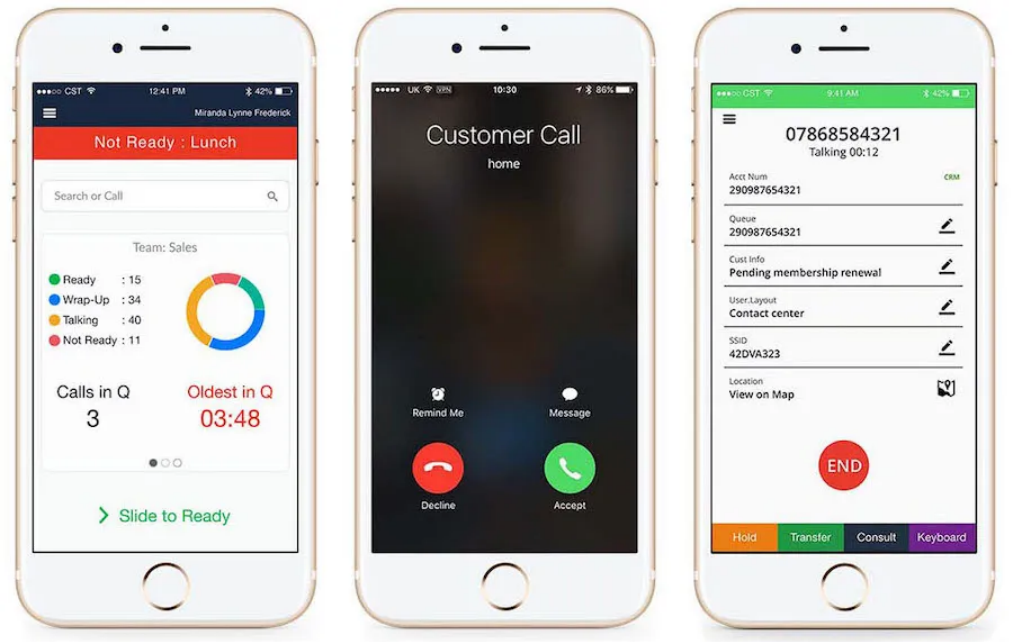
Comstice

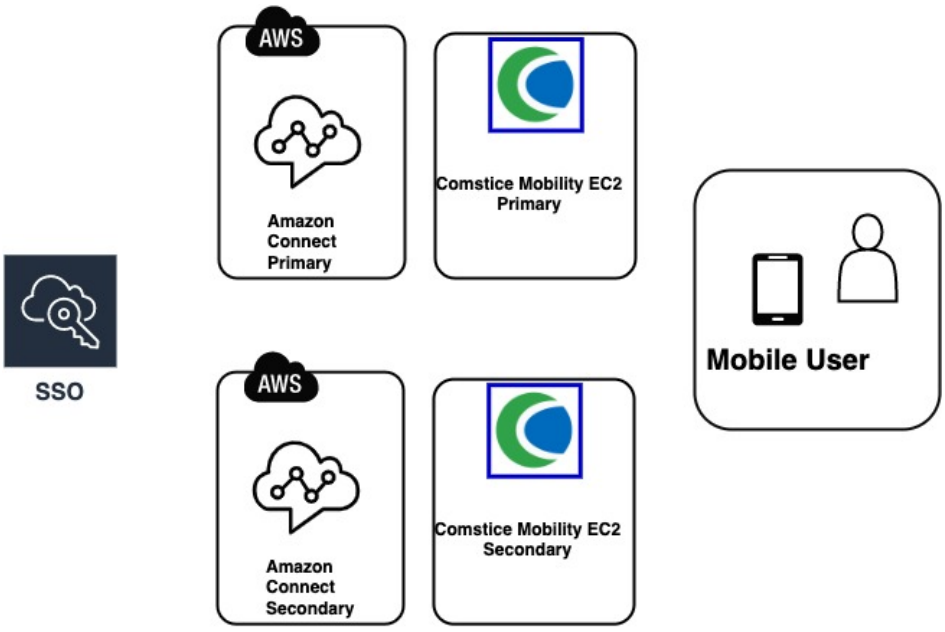
Amazon Connect Mobile Softphone by Comstice

High Availability Guide



Comstice Mobility Solution

Comstice Mobility solution helps to login to Amazon Connect, make and receive calls using mobile devices. Mobile app communicates with the Comstice Mobility Server running on EC2 and this communication is extended to Amazon Connect and SSO.



There are two types of failover for the mobile user;

- Login failover
- Failover while logged in

Amazon Connect instance can have a secondary identical instance which can be used as a failover instance. Comstice Mobility server as well can have a secondary EC2 as a failover option.

Failover during Login

Mobility Server Failover

In a high availability setup where there are at least two Mobility servers, login process starts with the primary. User settings retrieved by the company code on the mobile app have primary and secondary Mobility Server information. The mobile app will try the primary, if inaccessible, then it will failover to secondary Mobility server and try to login.

Amazon Connect Instance Failover

Each Mobility server can communicate with the Amazon Connect instances. It will first try to connect the primary, then fail over to secondary if the primary server does not respond to the login request.

In case of SSO, it will communicate the SSO Enterprise Application of the relevant Connect instance using their Access Login URL.

If SSO and Amazon Connect instance do not have any high availability /failover setup, SSO provider can still redirect the login request to the unavailable Amazon Connect instance. In this case, login will fail and the user will be asked to initiate a login to the secondary server by the mobile app.

Once the user taps on "OK", the new login process will start to the secondary Amazon Connect instance SSO login URL. User will enter the credentials for the second time and validate MFA, if used. SSO will grant the token to login to Amazon Connect and Mobility server will login to secondary Amazon Connect.

If SSO and Amazon Connect instance do have a high availability / failover setup, then SSO will fail the login request before entering the username/password, and the mobile app will try to login to the secondary Amazon Connect instance SSO URL.

Failover After Login - No Active Call

Mobility Server Failover

If the mobile user is logged in and there has been a failover, the user does not need to relogin to SSO. Existing SSO session tokens will be preserved by the second Mobility server.

In case of a failover, secondary Mobility server will send mobile notification to logged in mobile users to bring the mobile app into active state to update the latest (mobile apps may not update the data while in the background). Secondary Mobility Server will still try to connect to the primary Amazon Connect first using the available tokens. If the primary Amazon Connect instance is still working, mobile user will use the secondary Mobility server to connect to the primary Amazon Connect instance.

There is no fail-back mechanism to the primary Mobility Server for the logged-in users. Only if they log out and log back in, mobile app will try primary Mobility server first.

Amazon Connect Failover

If primary Amazon Connect instance goes down, Mobility Server will send mobile notification to the mobile app users who are currently logged in to relogin due to Amazon Connect instance failure. Since different Amazon Connect instances will have different login URLs, there must be a new login to the secondary Amazon Connect instance via SSO.

Once the Amazon Connect primary comes back up, the users must log out and relogin. For this, Comstice Mobility server can send ad-hoc notifications for the users to bring back the mobile app to active state on the screen and relogin.

Failover After Login - Active Call

Mobility Server Failover

If there is an active call and Mobility server failed over, the active call is preserved. Also the active login session is preserved since Mobility servers share the existing SSO session tokens.

IAfter each call, mobile app checks which Mobility server is currently active and. This will help to fail over after the active call. Secondary Mobility Server will still try to connect to the primary Amazon Connect first using the available tokens. If the primary Amazon Connect instance is still working, mobile user will use the secondary Mobility server to connect to the primary Amazon Connect instance.

There is no fail-back mechanism to the primary Mobility Server for the logged-in users. Only if they log out and log back in, mobile app will try primary Mobility server first. Ad-hoc mobile notifications can be sent to request relogin.

Amazon Connect Instance Failover

If there is a Connect instance failover while there is an active call, the call will fail, since Amazon Connect instances can not fail over the calls. Also, Mobility server will send a mobile notification to relogin. Since different Amazon Connect instances will have different login URLs, there must be a new login to the secondary Amazon Connect instance via SSO.

Once the Amazon Connect primary comes back up, the users must log out and relogin. For this, Comstice Mobility server can send ad-hoc notifications for the users to bring back the mobile app to active state on the screen and relogin.

Failover Mechanism: Conclusion

There are different scenarios in different topologies for the failover;

- SSO vs Non-SSO
- Single Amazon Connect instance vs two separate instances
- Failover of Third-party integrations

The key here is that Amazon Connect already has a certain level of high availability using AWS Availability Zones (AZ). Comstice Mobility servers must be monitored and potential issues can be resolved before causing an outage.

In some scenarios, a mobile notification may be sent to request user to bring the application back to main view so that the mobile app can update the latest service state or relogin if needed due to the nature of the failover.