



High Availability Services

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 1](#)
- [AMF High Availability Service, on page 2](#)
- [NGAP and NAS High Availability Service, on page 2](#)

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2021.04.0

Feature Description

High Availability (HA) is the ability of a system to operate continuously for a designated time without significant down time.

HA uses two pods, one as active and other one as standby. Whenever the active pod goes down, the standby pod becomes active and handles the traffic.

This feature supports the following HA services:

- AMF
- NGAP and NAS

AMF High Availability Service

Feature Description

The High Availability feature ensures the following functionalities for AMF-service:

- No session loss when AMF-service pods get killed or restarted.
- During restart, the AMF-service pods don't:
 - Fail any procedures
 - Increase in call processing time
 - Result in call failure of the retried calls
 - Restart or crash other pods
 - Downgrade the performance

NGAP and NAS High Availability Service

Feature Description

The AMF protocol pod maintains the security context cache, NAS UL, and DL counters. Whenever this information is modified in the cache, the same information gets replicated to the peer protocol pod to ensure high availability.

The AMF protocol pods determine among themselves who is the leader by using the Etcd for electing a leader. The leader information gets registered in the topology management module in the Etcd. The leader selection upgradation helps with replicating the security context cache to the other AMF protocol pod. If the leader pod goes down, the other(follower) pod becomes active and handles the traffic. The follower pod works with the replicated security context cache, UL, and DL counters from the leader.

The AMF-SCTP and the AMF-service pods query the leader information for the AMF protocol pod before making any IPC call. When the leader pod goes down, the other pod gets selected as a leader and the subsequent IPC requests goes to the selected protocol pod.

If a pod comes up, the security context cache gets synced with the peer before the pod becomes ready.

This feature supports two AMF protocol replicas.



Note Supported maximum two replicas (recommended) for high availability.
If both protocol pod replicas go down back to back or together, the security context data gets lost.

Feature Configuration

To configure this feature, use the following configuration:

```
config
instance instance-id instance_id
endpoint ngap replicas replica_count
end
```

NOTES:

- **endpoint ngap replicas *replica_count***—Specify the number of NGAP replicas per node.

Configuration Example

The following is an example configuration.

```
config
instance instance-id 1
endpoint ngap replicas 2
end
```

