Asterisk High Availability Design Guide

VoIP Conference – High Availability
January 27, 2016

® The Asterisk speech bubble is a registered trademark of Digium

Autonomy

Peers must be fully autonomous

Failure or data corruption of one peer must not adversely affect the other

Must Have	Avoid
✓ Fully autonomous peers	✗ Shared hardware (e.g. channel bank)
✓ Support for system configuration differences between peers	✗ Shared logical devices
	✗ Locally attached trunks / phones

Synchronization

Peers must remain in sync so they can take over immediately without needing to copy data

Peers must not sync if either peer is not in optimal health

Must Have	Avoid
✓ Synchronization of programs, data, and configuration	✗ Common disk (DRBD, iSCSI)
✓ Synchronization of non-Asterisk files / databases	✗ Network share (NFS / CIFS)

Failure Detection

Detect ability of Asterisk to bridge calls and serve the needs of internal and external callers

Must Have	Avoid
✓ Internal process awareness	✗ Simple process monitoring
✓ Hardware awareness	✗ Dependence on Asterisk to reports its own health
✓ External environment awareness	

Geographic Separation

Peers must be able to operate equally well whether in a single data center or in separate data centers on different continents

Must Have	Avoid
✓ Network latency compensation	× LAN based device sharing (DRBD, NFS)
✓ Adjustable latency fluctuation control	× USB based device sharing

Transparency

Upstream trunks must not be aware of failover

Downstream phones must not be aware of failover

Must Have	Avoid
✓ VoIP IP address moves with active peer	× Dependence on multiple server registration by phone
✓ Rapid failover	× Introduction of single point of failure (device) in front of Asterisk peers
✓ Complete transparency	

Single Point of Failure

Peers should not be dependent on a single device in front of cluster (e.g.: for ‘call survival’ on failover)

These devices introduce more problems (single point of failure) than they solve. They also don’t work in real world scenarios.

Must Have	Avoid
✓ Direct access to trunks and/or phones	× Any shared device in front of cluster × Claims of proprietary call salvage devices

Encryption

Communications between peers must be fully encrypted

Essential where NG911 and Sarbanes Oxley regulations apply

Common sense in era of ubiquitous hacking

Must Have	Avoid
✓ Encryption of peer control channel	✗ Unencrypted network storage (DRBD, NFS)
✓ Encryption of data synchronization protocol	

Cost vs Capabilities

Broad spectrum of products ranging in capabilities and performance

Beware of vendors charging for open source tools (e.g.: DRBD + Heartbeat) rebranded as their own

Try before you buy!

Free	Commercial
• Flipit • DRBD + Heartbeat • Ultramonkey • More	• HAAst (High Availability for Asterisk) • Stratus • Shmooze

Conclusions

- A number of products on the market
- Almost all are at the low-end of the capability and performance spectrum
- Vendors rebranding free tools is concerning
- Vendors hiding use of unsuitable technology (DRBD) in their products to solve synchronization problem
- All solutions perform great in simplest tests
- Only one product (HAAst) actually survived continuous failover and extreme tests
- The “right” product depends on the cost of an outage to your telephony environment
- If you don’t need the high-end product (HAAst) consider building your own with ‘flipit’ and NFS share/DRBD – but understand what you are trading off
- Don’t pay a vendor for a rebranded open source product

Thank you!

Robert Knowles
Vice President VoIP Solutions
Globe Telecom