Building a high availability ArcSight solution

Paul Brettle – Presales Manager, Americas Pacific Region

#HPProtect
What is high availability?

High availability system design approach and associated service implementation that ensures a prearranged level of operational performance will be met during a contractual measurement period.

1. Elimination of single points of failure. This means adding redundancy to the system so that failure of a component does not mean failure of the entire system.
2. Reliable crossover. In multithreaded systems, the crossover point itself tends to become a single point of failure. High availability engineering must provide for reliable crossover.
3. Detection of failures as they occur. If the two principles above are observed, then a user may never see a failure. But the maintenance activity must.
What is disaster recovery?

Disaster recovery (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

[1] Disaster recovery focuses on the IT or technology systems supporting critical business functions

Critical differentiation

• What do I need?
• How do I approach it?
• What is the minimum that I will accept?
But what is high availability?

Understand what is required, approach and differences

• Data
• Systems
• Usage
• Resilience
• Processing

Understand differences between hot, warm, and cold!
Prioritize and organize

What are the drivers for this?

• Regulation?
• Legislation?
• Compliance?
• Good governance/best practice?

Start examining the critical components

Look at systems, processes and models to assist you

• More on this later!
What do I get by default?

**Communications**
- Reliable communications

**Cache**
- Built in once collected for all SmartConnectors

**Commit**
- Commit model for storage of data (SmartConnector -> ESM)

**Recovery**
- Archive files

**Hardware**
- Dual power supply, reliable hardware, hot swap components and storage
ArcSight Architecture

Enriched events from ESM will be forwarded to Logger for long-term event storage.

Events from all SmartConnectors will be forwarded to the ESM Instance.

All SmartConnectors are managed remotely via the ArcSight Connector Appliance or ESM Manager.

Analysts will leverage the ArcSight Console or a web browser to access ESM, Logger, and CA.
ArcSight Architecture

Events of interest will be forwarded from Logger to ESM for real-time correlation. Correlated events will be forwarded back to Logger for long-term storage.

Analysts will leverage the ArcSight Console or a web browser to access ESM, Logger, and CA.

Events from all SmartConnectors will be forwarded to separate Loggers for load balancing purposes.

All SmartConnectors are managed remotely via the ArcSight Connector Appliance.
Analysts will leverage the ArcSight Console or a web browser to access the Global or Regional ESM and Logger Instances.

Globally correlated and base events will be forwarded from the Global ESM Instance to Logger for long-term storage.

All SmartConnectors are managed remotely via the ArcSight Connector Appliance.

Loggers can be configured in a Peer Network for a holistic view of all events in the environment.

Events of interest will be forwarded from Logger to ESM for real-time correlation. Correlated events will be forwarded back to Logger for long-term storage.

Events from all SmartConnectors will be forwarded to the Regional ESM Instances.
Connector layer

- Push connector type
- Load balanced
- Needs consistency
- Typically used for
  - Syslog
  - Large volumes

Each SmartConnector forwards on the encrypted, compressed and processed events to the ArcSight solution.

Here a two-node load balancing solution can be deployed. The load balancing system can be used to spread the load between two or more nodes for processing. There is no need for clustering here as we simply want to process the logs and events and this represents the most efficient method to do this.

The source devices send their logs and events directly to the load balancing IP address using their native protocol, such as Syslog.
Connector layer

- Pull connector type
- Log messages not lost
- Active HA needed
  - Require consistency
- Typically not implemented

Two-node active/passive cluster for the SmartConnector. Should the active node fail for any reason, the passive node can continue where it left off. Since the shared disk is used, all current events are processed with no loss or duplication.

SmartConnector forwards on the encrypted, compressed and processed events to the ArcSight solution.

SmartConnector connects to the sources directly from the active node. All processing is done by the active node but state information stored on shared drive.
Log storage layer

- Dual feed strategy
- Duplicate in two Loggers
- No replication needed

Connector receives/pulls the events and forwards on to configured Loggers.

Devices send/receive their logs and events to and from the Connector in their native formats as required. Typically this will be via Syslog, which uses UDP.
Log storage layer

- Warm standby model
- Backup configuration
- Access archives
- Provide cache at connectors

Main Logger

Configuration restored to access stored data and assume role of main Logger.

Devices send/receive their logs and events to and from the shared IP in their native formats as required. Typically this will be via Syslog, which uses UDP.

Storage device used for archived daily logs. Secondary Logger can retrieve archives as necessary.
Log storage layer

- Most effective solution
- Dual feed and dual archive
  - Easy to restore
  - Little impact
  - **No** replication needed
- Be aware of network

- **Connector** receives/pulls the events and forwards on to configured Loggers.
- Devices send/receive their logs and events to and from the Connector in their native formats as required. Typically this will be via Syslog, which uses UDP.

- Loggers auto-archive to storage system for resilient long-term storage.

- Main Logger
  - Remote site
  - Connector
  - Logger DR site
Correlation layer

- ESM with Oracle
  - Simple fail-over to single DB
  - Use commercial solutions
  - Tried and trusted

- Replicate database
  - Several technologies available

- Fail-over manager starts
- Console re-connects

Here a primary Manager is used as the single processing server for the correlation etc. of the ESM solution. All communications to the database come from the single primary Manager.
Correlation layer

- ESM with CORRe
  - No one single DB
  - Need to replicate DB
  - Consider options

- Consider ESM/Express
- Look at options
- Work out difference
  - HA or DR
Options?

Hardware
- Power
- Disk
- Network

Software
- HA/fail-over/cluster software

Operating system
- HA/fail-over/cluster software

Virtualization
- Don’t forget what you can get here
- Usually a cost option
Summary

Lots of options
• Consider what is needed and how to address

HA deployed at a lot of customers
• Using in-built and external technologies

Only as strong as weakest link
Plan and understand issues
Please give me your feedback

Session TT3058  Speaker Paul Brettle

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you
Make it matter.