RSF-I
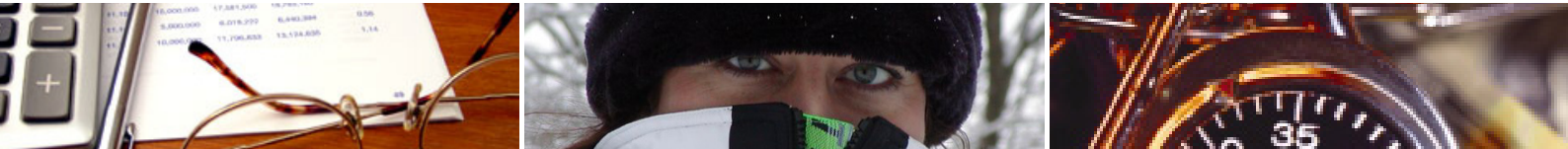
HIGH-AVAILABILITY

Cluster Audit

Overview

Clusters are deployed to improve availability and clustering software provides a solution to work around many of the possible causes of downtime, helping to keep a service running 24x7.

Using a cluster solution reduces most outages to very short spells. However, many potential problems could be pre-empted by ensuring systems are well designed, implemented and maintained.

Environments change over time and that can affect the optimal design for a given solution. New technologies and methods emerge and best practices change to adopt these. However, your existing system may not have kept pace with the changes.

To ensure that your clustered solution is a robust as it was when first deployed you should carry out a full audit annually, ideally by someone other than the regular administration staff.

This annual audit now constitutes part of our Code of Best Practice for cluster solutions and we now include this service as part of our annual maintenance programme, at a cost. Customers can opt out if they prefer to conduct the audit themselves.

The audit is a two day process, one day on site and one day documenting the installation and recommendations. Clusters of greater than two nodes may require additional time which will be identified prior to commencement of the audit.

An example of the audit report is available on request and the general process and level of detail is described within this document. The audit can be completed on non-clustered machines and with an additional scope of work on request, at an additional cost.

A set of simulated failover tests are recommended and these will be performed, which will need careful scheduling, normally out of hours. However, some customers elect not to conduct these tests during the audit.

The focus of the audit process is to identify changes that should be made, rather than to conduct those changes. However, where an immediate change should be made to ensure operational reliability the audit consultant will identify this and will offer to perform the change if practicable in the time available. Other changes can be made by the audit consultant if required but are outside the scope of the audit process.

Scope of the Audit

The audit report will briefly describe the history of HAC's involvement with the customer and detail the cluster being audited in particular. A high level description of the current installation along with the services it provides and the user community helps to 'set the scene' and will be included.

Any known problems or concerns will be noted in the introduction to the report and given special attention during the process and report.

The report will set out the high level scope of work conducted and identify recommended testing if the customer elects not to test failover during the audit process. Typically the report will cover the following topics:
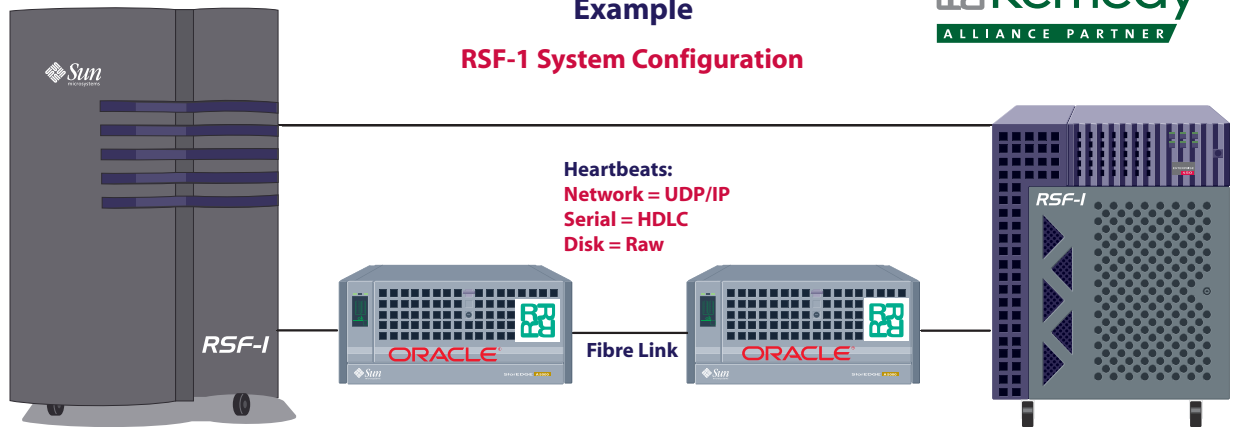
Physical Inspection

- Description of all directly relevant components
- Diagrams of the connections of all that equipment

Remedy®
ALLIANCE PARTNER

Heartbeats:
Network = UDP/IP
Serial = HDLC
Disk = Raw

RSF-1

ORACLE   **Fibre Link**   ORACLE

RSF-1

RSF-1

System Administration Health

- Conducted on each machine
- Inspection of the following;
  - Various system log files
  - log files
  - cron jobs
  - user & password files
  - basic security
  - system admin Email handling
  - unnecessary processes
  - file system health
  - eeprom setting incl. - MAC & boot params
  - name service setup - DNS etc
  - RAID device configuration, logs and state
  - mirror state tables, layout, SPOFs
  - Clock synchronisation
  - OS version and patch revision

High-Availability Product Setup

Clearly we are extremely well placed to be able to review and advise on the ideal configuration of our own products in the customer environment and a thorough inspection will be completed.

- RSF-1™
- NetMon™
- ResMon™

  - configuration and review of resilience
  - log file review; events & what data is being recorded
  - collection of hac_diag logs
  - identify possible benefits of upgrading

Network Design

The audit will identify and SPOFs and will identify how some of those could be eliminated. The routing and configuration of interfaces and MAC addresses will be checked.

Third Party Software

Software products that are integrated with or controlled by RSF-1 will be reviewed for their configuration and ongoing cluster compatibility. We are not experts in every 3rd party product and the extent of the advice we can offer is sometimes limited as a result. However, our broad knowledge often enables us to identify small changes that can be made to dramatically simplify the configuration.

Additional Work

The audit can be expanded to include tests over time on performance as well as identifying possible bottle necks with CPU, IO, memory etc. This work is normally only undertaken if there are known problems and an initial audit has not been 'deep' enough to identify the cause of a specific problem.

Extended security testing and the introduction of a regular automated security audit process is another service that is offered to customers expressing concerns about security.

Report Summary

The audit report will summarise the overall health of the system and refer to any urgent tasks that should be completed.

Sun microsystems   *Partner Advantage*

Mac   Universal

Sun microsystems
iForce™ Partner

hp invent ®

IBM Business Partner

solaris

Java

Linux