



Education

Get ready for support

Erwin van Londen, Hitachi Data Systems

- ◆ The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- ◆ Member companies and individual members may use this material in presentations and literature under the following conditions:
 - ◆ Any slide or slides used must be reproduced in their entirety without modification
 - ◆ The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- ◆ This presentation is a project of the SNIA Education Committee.
- ◆ Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- ◆ The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

➤ Get ready for support

- ◆ This session will guide the reader/attendee how to include vendor requirements into business continuity procedures. Data collections, time stamp registrations, sequence of events and up to date information are most often overseen or are not available so that vendor support organizations lose a lot of time in diagnosing problems.

- On average administrators lose between 4 to 72 hours before effective troubleshooting can start after a critical event has happened.
- Is your business ready for this?

TOP TEN PAIN POINTS

		2007		2004
Most Painful	1	Reliability/availability		Cost
	2	Managing Growth		Managing Growth
	3	SAN Management		SAN Management
	4	Cost		Interoperability
	5	Complexity		Complexity
	6	Human error		Service/Support from Vendors
	7	Interoperability		Lack of Functions and Features
	8	Upgrades		Justifying Costs
	9	New Technology		Undelivered Promises
Least Painful	10	Vendor Support		Lack of Automated Provisioning

Source: SNIA EUC TTPP Survey October 2008

- How far does your Business Continuity plan reach?
- What is your RTO?
- How much time do you allow your vendor to troubleshoot a particular problem?
- When do you expect your vendor to start troubleshooting?
 - ◆ Immediately !!!!
- Make sure you are ready and have the correct information.

Some case descriptions

- Help, my data-centre went down.
 - ◆ Why did you put it in an elevator?
- Help, I lost all my disks.
 - ◆ OK, file a missing disk report and claim it on the insurance.
- Help, my computer is slow.
 - ◆ Add a V8 supercharged engine and check if this helps.

- **Statements do not add useful information to the case.**
 - ◆ They state frustration and urgency but do not contribute to fast resolution.

- **Sometimes even aggression or verbal threats**
 - ◆ Be aware that people on the other side of the phone are trying to help.
 - ◆ All vendors have guidelines which might even lead to total disengagement.

Examples

- I want you to treat this with the highest priority.
- This needs to be worked on around the clock.
- I want this resolved A.S.A.P.
- I want updates every 15 minutes.
- I want Root Cause yesterday.
- I'll have a chat with your boss.
- Do you want to work there tomorrow.
- Our lawyers will be in touch.

➤ Projects and operations.

- ◆ Only implementation and delivery is signed off.
- ◆ No procedures are defined during testing and/or production which include vendor escalation.

➤ Lack of knowledge

- ◆ How to collect information from various parts in the infrastructure.
- ◆ How to interpret the information.
- ◆ Bad decisions are made based on misinterpretation.

➤ Entitlement

- ◆ Maintenance contracts expired
- ◆ Lose valuable time with vendors to sort this out.
- ◆ Multi vendor infrastructure.

➤ The right people at the right time in the right place

- ◆ Decision authorisation for change.
- ◆ Delegation of authorisation.
- ◆ No focal point or problem manager available.

- Storage implementation project was very successful
- Test have been completed and are successful.
- All data has been migrated.
- Environment has been taken into production.
- So far day to day operations have shown no sign of any issue.

- Murphy's law always applies.
 - ◆ Issues arise at the worst possible moments.
 - ◆ They are often concurrent. One problem leads to another.

➤ Administrator start troubleshooting

- ◆ This occurs on multiple levels.

- › Applications
- › Servers
- › Networks
- › Storage
- › Etc.

➤ Important information might get lost.

- ◆ Log files often wrap on timeframe or size
- ◆ Use circular logging.

➤ Access to datacentre ??

- ◆ Are vendor engineers cleared to access the datacentre.
 - › Physical access.
 - › Virtual access (Webex, Remote Desktop etc.)
 - › Serial console access.
- ◆ Is personnel available and on site.
 - › May be needed to verify statuses of equipment.
 - › Does this also work when operational management is out-sourced/off-shored.

- Documentation is not up to date
 - ◆ Massive spreadsheets with topology diagrams
 - ◆ Connection diagrams
 - ◆ Array, ports, raid group, pools etc are incorrect

- Sequence of events not documented
 - ◆ What did you do? -> “Nothing!!!”

- Topology diagrams.
- Time settings.
 - ◆ Time zones.
 - ◆ Offsets.
 - ◆ Differences between equipment.
- Logs from non-related equipment or software.
- Incorrect data collection procedures followed.

Effect on resolution

- Support organisations do not know your environment
 - ◆ Applications
 - ◆ Servers
 - ◆ Operating Systems
 - ◆ Network infrastructure
 - ◆ Storage infrastructure
 - ◆ Security guidelines
 - ◆ Operational restrictions
 - ◆ etc

- Storage infrastructures have a vertical view
 - ◆ Shared infrastructure
 - ◆ All components between application and physical disk influence the behaviour of a storage network.
 - ◆ Even when, at first glance, a component might seem unimportant this might be the cause of the problem.
 - ◆ Maintain a change log to back-track where things might have gone wrong.

- Four very important things to consider
 - ◆ Time
 - › Use NTP !!!!
 - › Configure correct time zones / DST !!!!!
 - ◆ Infrastructure overview.
 - › Prepare Visio or other visual diagrams.
 - Identify where the problem manifests itself.
 - ◆ Fast data collection with “un-contaminated” logs.
 - › Do NOT start troubleshooting before ALL data-collection procedures have been finished.
 - › Treat your infrastructure as a “crime-scene”.

- Prepare performance data collection.
 - ◆ Regular baseline resets.
 - ◆ Short term and long term.
 - ◆ Depending on equipment capabilities.
 - ◆ Describe timelines or the problem.
 - › When did it start.
 - › Is it current or has the problem ceased.
 - › Is it reoccurring.
 - › Can it be re-created on demand.
 - › What has changed before, during and after the problem.
- Verify with your vendor.

➤ Tools.

- ◆ System collection tools.
- ◆ OS collection tools.
- ◆ Vendor collection tools.
- ◆ Application collection tools.

➤ In general framework based products are not useful.

- ◆ Lack of technical depth.
- ◆ Collect only a subset of information.
- ◆ Same for SNMP based collection products.

- Check error messages and counters daily
 - ◆ Fix any kind of physical issue. (SFP, Cabling)
- Maintain weekly performance baseline.
 - ◆ Collect and save logs every week.
 - ◆ Reset all counters on all equipment.
 - ◆ Embedded platforms have limited space to save data.
 - › Circular or time based logging.
- Use fencing technology if possible.
 - ◆ Prevents one bad device having impact on entire fabrics.

➤ Problem areas

- ◆ Font-end ports (FC/FCoE/iSCSI etc)
- ◆ Controller CPU
- ◆ Cache
- ◆ Back-end connectivity
- ◆ Disks
- ◆ Tape libraries and devices
- ◆ Performance

➤ Check with your vendor on collection procedures

➤ Replication scenarios

- ◆ Synchronous / a-synchronous / journal based.
- ◆ Long distance. (50km +)
- ◆ Technologies. (DWDM/CWDM,FCIP etc)
- ◆ Compatibility. (speeds, protocols, mappings etc)
- ◆ Multiple vendors, service and network providers involved.

- **Keep your equipment up-to-date !!!**
 - ◆ Vendors do actually fix software and hardware issues.
 - ◆ Maintain consistency across your environment.
 - ◆ Check EOL and EOS notifications..
 - ◆ Subscribe to vendor tips and alerts.

- Rehearse collection procedures and escalations.
- Incorporate vendor requirements.
- Maintain history of logs.
- Use correct time and up-to-date change logs.
- Involve all people who need to know.
 - ◆ This may even include building managers.

- **Manage and Maintain your environment !!!**

- Please send any questions or comments on this presentation to SNIA: trackstoragemgmt@snia.org

**Many thanks to the following individuals
for their contributions to this tutorial.**

- SNIA Education Committee

**Erwin van Londen
John Pyle
Steve Lockrey**