MSA1000 Best Practices document

Below is a list of 'Best Practices' for the MSA1000. A short explanation is added to each bullet as needed. For full details, please refer to the Documentation tab on the MSA1000 WEB page (www.hp.com/go/msa1000)

Released: 4/27/2004

All configurations:

- **Only HP/Compaq branded HBAs are supported.**
  - One ore more HBAs is tested and qualified for each supported Operating System. Refer to the Compatibility Matrix on the WEB page.
- **HBA firmware can be upgraded via vendor specific utilities or Device Manager in Windows.**
  - Refer to the release notes for the firmware upgrade.
- **HBA driver installation;**
  - For a new installation; first set up the server from SmartStart, then install the HBA driver form the MSA Support Software CD.
  - To add MSA1000 support on a current server, insert the MSA Support Software CD and follow the on-screen installation procedure.
- **HBA drivers need to be loaded with HP specific parameters.**
  - This is done automatically if drivers are installed via MSA Support Software CD.
  - If any other method is used, please refer to the release notes for the driver to ensure proper configuration for your OS.
- **For Windows systems, HBA drivers should be installed via the MSA Support Software CD, not Device Manager**
  - To ensure proper configuration and parameter settings, all drivers should be installed via the MSA Support Software CD.
  - Always check the WEB for the latest drivers and firmware.
- **The latest version of ACU should be used to configure the MSA.**
  - If your server is running an old version of ACU, it should be upgraded to ensure compatibility with the MSA.
  - The latest version can be found on the MSA Support Software CD.
  - As of version 6.10, ACU-XE became simply ACU.
  - If your OS doesn't support ACU, you can use the CLI to configure the MSA.
- **In general, Localized OS versions are not supported with SecurePath.**
  - SecurePath was developed and tested with the English version of the Operating Systems. In most cases, localized or translated versions of the OS will not work.
- **Software and Firmware upgrades may need to be done synchronized.**
  - New drivers and firmware are available on the MSA Support Software CD and on the WEB. To assure compatibility, check the release notes for the upgrade you plan to install to verify if there are any dependencies.
- **MSA Support Software CD can be used to create LUNs before the OS is installed on the server.**
  - If using this method, the server must be booted from the CD.
  - A supported HBA must be installed in the server.
  - Alternatively; LUNs can be created via the Command Line Interface (CLI); a special cable is provided to connect to the MSA controller.
- **Boot to SAN**
  - To install the boot partition for your server on the MSA (remote boot), first boot the server from the MSA Support Software CD, configure the LUN and set it up as a boot device. LUNs can also be created via CLI. Then continue with the SmartStart assisted install.
  - For details and restrictions, please refer to the Boot to SAN white paper on the WEB page pertaining to your operating system.

- **Migrating drives from an RA4100**
  - If you are replacing the RA4100 with an MSA1000, you must also replace the HBA in the server.
  - You can access both the RA4100 and the MSA1000 from the same server; they require separate HBAs and drivers. If you have SecurePath, this configuration is not supported.
  - For further details, refer to the Migration white paper on the WEB site.
- **The embedded MSA SAN switch 2/8 takes 5-7 minutes to initialize. This is normal.**
  - The switch goes through an extensive self-test at power up.
  - This function can be disabled via setup.
- **Firmware on the MSA controller, EMU and the discontinued MSA fabric switch 6 can be upgraded via MSA flash (Windows, Linux, NetWare)**
- **The MSA SAN switch 2/8 firmware must be upgraded via vendor specific application.**
  - This switch is comparable to HP's B-series external switches, and uses the same firmware and software utilities.
- **With fibre direct connect (I/O module or HUB), the MSA controller will show error: "516 - fibre subsystem link failure" if the attached server is rebooted.**
  - The link is automatically reestablished when the server comes back up, and the message "517 – fibre subsystem link OK" is displayed.
- **MSA controller Amber light will stay on until all error messages have been read.**
  - Use up and down arrows to read the messages.
- **To clear the errors on the MSA controller, press the <left> and <right> arrows simultaneously when the error message is displayed on the LCD panel.**
- **All controller messages are erased when the controller is restarted.**
  - There is currently no way to save the messages in the controller buffer.
- **The controller stores the last 100 messages (wrap around buffer).**
  - When the buffer is filled up, the oldest messages will be erased.
- **If the controller logs several 401/400 message pairs (Storage box fan failed/fan OK), or 410/409 message pairs (Storage box power supply failed/power supply OK), the most probable source of the problem is the EMU module.**
- **Currently the MSA supports a maximum of 32 LUNs.**
- **Blade servers support connection via Fibre Channel Switch (Not direct).**
  - The switch can be internal to the MSA or external.
- **Backup of the LUNs on the MSA must be done from each individual server.**
  - One server cannot have access to all LUNs while other servers accessing data.
- **In a cluster configuration, parity initialization of LUNs will not finish.**
  - Parity Initialization is done when the controller is idle. The cluster software will poll the controller continuously, preventing parity initialization from finishing. Disable clustering SW until this is done.
- **To clear a connection from the memory on the controller, you first have to delete the connection name (CLI or ACU) then reboot the MSA.**
- **To clear an error message from the controller LCD, use the up or down arrows until the message is displayed, then press left and right arrow simultaneously.**

Single Controller Configurations:

- **Two or more servers cannot share LUNs without software support (Clustering, etc.)**
  - This is a limitation in the Operating System, not the MSA1000.
- **SSP (Selective Storage Presentation) or CLI can be used to give access to specific LUNs.**
  - SSP is enabled via ACU.

- **If using ACU to name the connections and set the profile, SSP must be enabled first.**
    - This must be done even if you don't plan to restrict access to specific LUNs.
    - When connection names and profiles have been set, SSP can be disabled.
    - Alternatively, connections and profiles can be set via the CLI.
- **In a Single Controller configuration, the controller must be in the right slot, the I/O module or switch directly behind it.**
- **2 I/O modules cannot be used to connect two servers; you need hub or switch.**
- **Two internal MSA SAN 2/8 switches cannot be cascaded for additional port count within the same MSA1000.**
    - It can be cascaded to an MSA SAN switch 2/8 in another MSA1000.
- **The discontinued Fabric Switch 6 cannot be cascaded to external switches.**
    - If additional ports are needed, use external switches only, or replace the internal switch with the MSA SAN switch 2/8.
- **The MSA SAN switch 2/8 supports cascading to external HP B-series switches.**

Dual Controller configurations:

- **Only Active/Standby is supported, not Active/Active.**
    - Need Software support on server side (SecurePath).
- **Load balancing is not available.**
    - Both controllers can not be active simultaneously. (Active/Standby)
- **The whole path from server to storage must be duplicated and isolated (separate SAN/zoning)**
- **SSP must be enabled to set host mode (profile) for each connection.**
    - Default is Windows.
- **Cache modules must match in size and configuration between the two controllers.**
    - Different cache configurations will lead to the redundant controller being disabled.
- **Fibre I/O configuration must match.**
    - You cannot mix I/O modules, HUBs and switches.
- **SecurePath is the only supported failover mechanism.**
- **Tape backup solution :**
    - To backup data on an MSA shared between several servers, each server must backup its data to the tape device.
    - In a dual path configuration, if a failover occurs, the servers will lose connection to the tape device.
- **If a second controller is hot added with a different firmware level, the active controller will try to clone its firmware to the new controller.**
- **If the MSA is cold booted with two different firmware versions, the newest will try to clone itself to the oldest.**
- **If cloning is not performed or is unsuccessful, the second controller will be disabled.**
- **If a single path server (W2K, NT, NetWare) is attached to an MSA that also has dual-path servers with Secure Path, the single path servers will lose access to the MSA should the primary controller become inactive.**