Best practices for production-based clusters and backup environments

Santosh Arunachalam,
santosh.a@hp.com

OpenVMS Technical Journal V18

Table of contents

About this document

This document provides you information about the OpenVMS best practices and its usages.

Intended audience

This document is intended for:

- Administrators who have implemented OpenVMS based production clusters in their environment
- Administrators/users who look forward to use the best practices for their environment thereby increasing their organization's productivity
- Leads, project or program managers

Prerequisite for using this document

- Knowledge of OpenVMS System Administration (Refer: OpenVMS system manager Manual)
- Knowledge of taking backup using archive backup system (ABS) saves and restoring data using ABS/data protector (DP) restore operations (Refer: ABS Operation Guide)
- Knowledge of taking backup using DP saves and restoring data using ABS/DP restore operations (Refer: HP Data protector User Manual)

Introduction

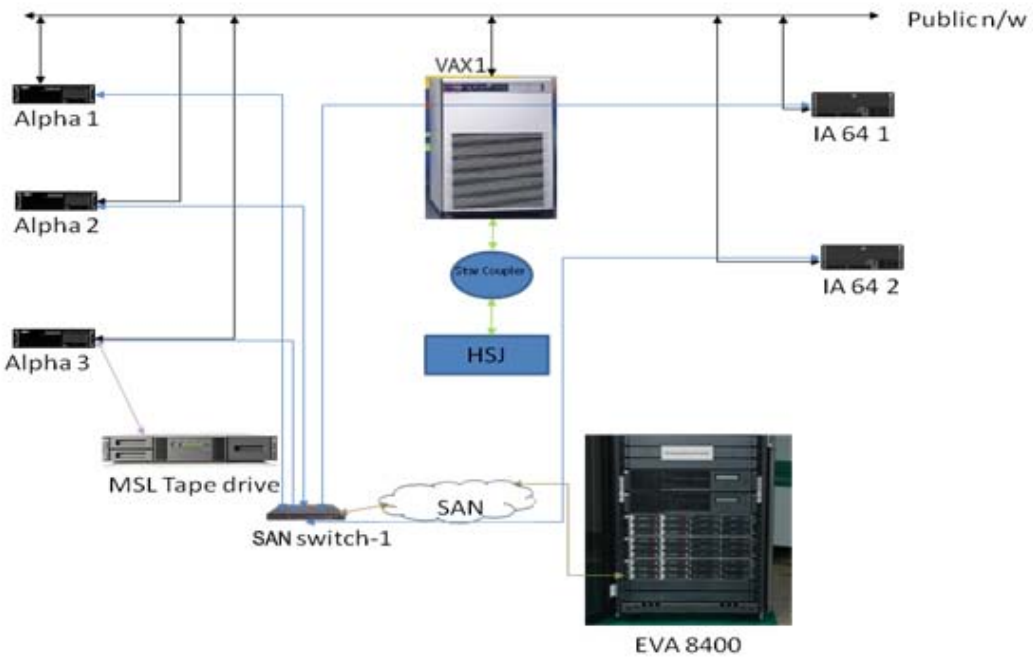
Overview

This environment explains the best practices in using the redundant setup associated with SAN environment and backup environment using the private switch setup. It uses the method of using both the public production cluster and private IP address for the backup based environment.

Problem statement:

As shown in this example, generally an OpenVMS cluster with three alpha and two Itanium boxes with EVA8400 storage, along with one Virtual Address Extension (VAX) 7000 node is connected to a HSJ storage through star coupler. This would be Scenario 1, which offers very less redundancy, and cluster becomes highly unstable because of large IO (based on the user access) along with routine backup operations.

Figure 1. Pictorial representation (traditional) of Scenario 1



Black line represents public network, blue line represents FC connectivity between the servers and SAN switch-1, green line represents Cluster Interconnect (CI) connectivity between VAX 7000 server and HSJ through star coupler. Tan color represents interconnectivity between SAN switch and EVA8400.

In case of ABS setup with latest LTO 3 or LTO 4 drives the ABS server is installed and configured on alpha-3 server.

Purple line represents connectivity between the alpha servers and the tape library.

To overcome this scenario, if we have a combination of the public production cluster with redundancy and private address-based backup environment, there can be a highly stable production cluster environment with EVA Continuous Access and good backup environment without affecting the public network.

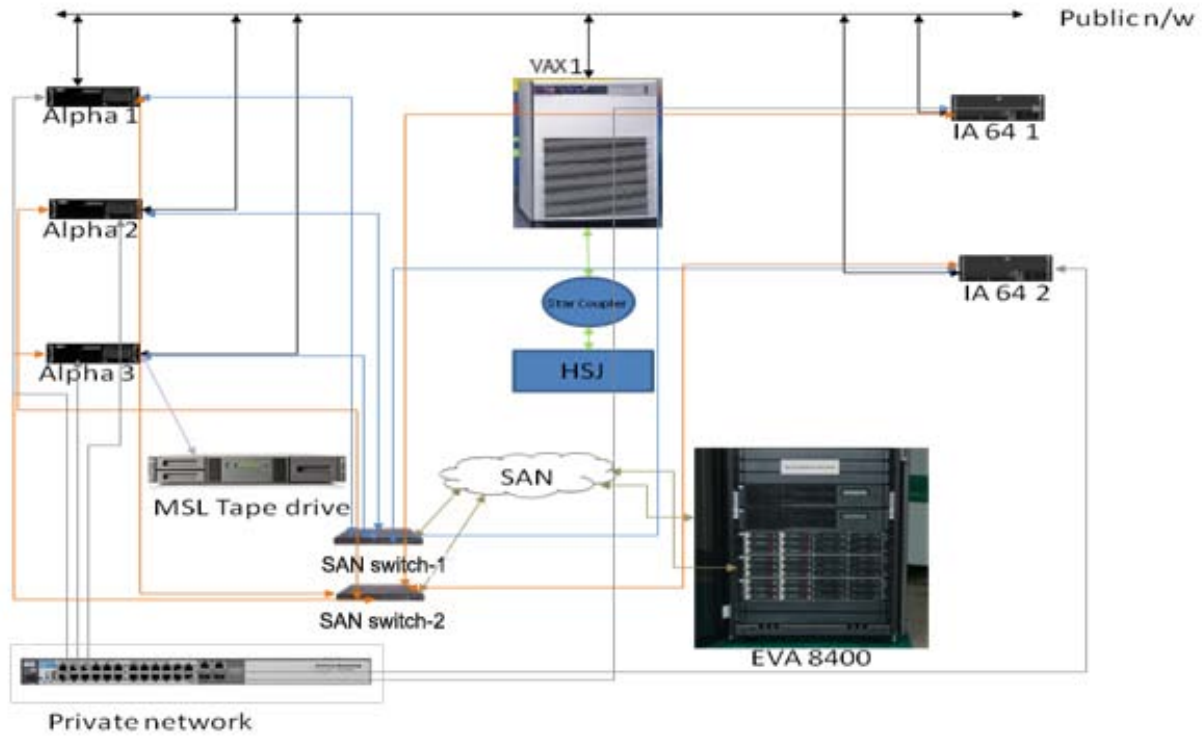
Solution statement:

To apply a straightforward scenario on substitution, insert additional Fibre Channel (FC) cards in all the alpha and Itanium nodes with each of the FC cables going to either of the FC switches, and two FC connections from the EVA also doing the same, which gives more redundancy.

On the other hand, we need to have additional NIC cards (not NIC ports on the same card like dual or combo cards) for more efficiency to route the public and private data separately.

Since VAX 7000 server comes with single NIC card and joins the cluster, the disks are Mass Storage Control Protocol (MSCP) served—this has not been taken into consideration. It will be the last node in our cluster that will be booted. Please see Scenario 2 for better understanding.

Figure 2. Pictorial representation of Scenario 2



Black line represents public n/w, blue line represents FC connectivity between the servers and SAN switch-1, orange line represents FC connectivity between the servers and SAN switch-2, green line represents CI connectivity between VAX 7000 server and HSJ through star coupler. Tan color line represents interconnectivity between SAN switch and EVA8400 through SAN network.

ABS software-based encryption or decryption methodology comes with the key management facility for backed up data to be safe. Please refer manual, Data encryption using Archive Backup System.

In case of DP installation, it is done on separate server (UNIX® or Microsoft® Windows®) and the DP client will be installed on the main node of the cluster. The tape library is connected to the DP server and configured for taking backup.

Device support:

The Media Device and Management Services (MDMS) portion of ABS/MDMS manages tape devices and volumes. It is part of the application installation and no additional software is needed to ensure that connectivity is available to OpenVMS tape devices. ABS/MDMS documentation explains how to set up the drives to be used for backups.

DP is based on a non-OpenVMS operating system. In order to use devices locally attached to the OpenVMS system, an additional software package, the Data Protector Media Agent, must be installed. Data Protector README.TXT files have more information on installing this software.

Both products follow the OpenVMS device support matrix to help ensure that any recently purchased libraries or tape drives are usable. Check the OpenVMS software product description (SPD), Release Notes, or online support pages for the latest supported devices.

Summary

Which software to use in a particular environment will be dependent on a number of factors:

- What operating system is predominant in the environment? Environments that have mostly OpenVMS servers may find ABS/MDMS more feasible for them.
- Are your libraries and devices used by more than one operating system? DP can be the application that can manage multiple systems—a library or device. ABS/MDMS requires a library to be dedicated to an OpenVMS system.
- On which operating system does most of the data reside? If it is mostly on OpenVMS, ABS/MDMS may prove most efficient. However, if there are large SQL, Exchange, or other applications or databases on other operating systems, DP can back those up along with your OpenVMS system.
- What type of operating skills does your staff have? If your staff is OpenVMS centric, ABS/MDMS may prove to be the best choice. You should do an analysis of how much it will cost to hire new skills such as those required for HP-UX.
- How fast must a disaster recovery take place? If OpenVMS is the primary operating system in the data center and quick, flexible restores are required, ABS/MDMS may be the best choice. If there are other operating systems, however, their restore time and criticality need to be considered.
- Is there particular OpenVMS backup functionality that is needed or required? DP can be a cultural change for users and the list of qualifiers that backup owns is not available. You should carefully consider what types of backups and their associated functionality are required before deciding on an application.

Another deciding factor is the cost of the application. Your choice of one product or the other depends on your environment, current applications, and future growth considerations.

Some useful links

- Firmware links
  www.hp.com/support
- About security
  http://h71028.www7.hp.com/enterprise/us/en/technologies/information-security-home-overview.html
- About encryption
  www.hp.com/go/dataencryption
- Enterprise Backup Solutions
  www.hp.com/go/EBS
- Advanced Encryption Standard at the website
  http://csrc.nist.gov/archive/aes/rijndael/
- Encryption Technology for the HP StorageWorks Ultrium LTO 4 tape drive white paper at the website
  http://h71028.www7.hp.com/ERC/downloads/4AA1-4878ENW.pdf
- ABS Support Matrix
  http://h71000.www7.hp.com/openvms/storage/smstape_matrix.html

Reference

- ABS documents
  http://h71000.www7.hp.com/doc/abs.html
- Secure Key Manager
  http://h18000.www1.hp.com/products/storageworks/secure_key/additional.html
- Secure Key Manager white paper
  http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA2-0797ENW.pdf
- Federal Information Processing Standards Publications—1996
  www.itl.nist.gov/fipspubs
- Data protector reference Manual
  http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c01632065/c01632065.pdf

4AA4-0529ENW, Created April 2012