Hewlett Packard Enterprise

HPE Reference Configuration for HPE 3PAR File Persona and Sophos antivirus software for NAS devices

Solution overview and recommendations for secure file sharing

Reference Architecture

Contents

Executive summary

As the need for data storage and access across the enterprise increases every year, the need for dependable, optimized, secure, and scalable storage has become essential. HPE 3PAR StoreServ Storage with HPE 3PAR File Persona introduces the true convergence of block, file, and object access, providing a scale-out network-attached storage (NAS) solution.

However, this centralized consolidation of data requires a shift in approach to data security. This document describes a scalable, high-performance threat detection solution for protecting valuable file and object data by integrating HPE 3PAR File Persona with Sophos antivirus for NAS devices. This solution addresses the increased need for making new data sources available to the enterprise, while simultaneously reducing vulnerability to malicious threats and attacks.

Target Audience: This Reference Configuration is intended for presales consultants, solution architects and engineers. We assume that readers of this Reference Configuration are familiar with HPE 3PAR StoreServ with File Persona and antivirus functionality.

Introduction

HPE 3PAR File Persona

HPE 3PAR StoreServ with HPE 3PAR File Persona offers a unique and efficient storage solution that incorporates multi-protocol support into the system architecture. It delivers a tightly integrated, truly converged solution for provisioning both block storage volumes and file shares from a single storage system. The HPE 3PAR File Persona is a feature of HPE 3PAR OS that enables a rich set of file protocols and core file data services on an HPE 3PAR StoreServ system. As a feature of HPE 3PAR OS, File Persona inherits one of the industry-leading architecture and Block Persona benefits of HPE 3PAR StoreServ. It extends the spectrum of primary storage workloads natively addressed by HPE 3PAR StoreServ from virtualization, databases, and applications via the Block Persona to the following workloads via the File Persona—all with truly Converged Controllers, truly agile capacity, and truly unified management.

The HPE 3PAR File Persona provides continuously available file shares, which allows non-disruptive HPE 3PAR Operating System upgrades and transparent failover of clients in the event of a controller failure. Comprehensive data protection is also delivered by point-in-time file store snapshots for user-driven file recovery, support for third-party antivirus and backup or restore software, and disaster recovery (DR) replication using separately licensed HPE 3PAR Remote Copy. Furthermore, the HPE 3PAR File Persona supports the security of FIPS 140-2 validated data-at-rest (DAR) encryption as an optional additional measure to prevent unauthorized data access.

Only HPE 3PAR StoreServ Storage has the ability to host workload-centric Storage Personas directly on a multi-controller architecture with hardware-accelerated data compaction—delivering a high-performance, low-cost, Management Server tier-1 storage platform to address any application need and data type. Protecting your file data and organization, as well as increasing your uptime, have never been simpler, thanks to the high availability (HA) and resiliency features built into HPE 3PAR StoreServ Storage.

Sophos antivirus software for NAS devices

Sophos antivirus software for NAS devices provides a scalable, high availability, high performance threat detection service that protects valuable data stored on network-attached storage devices against multi-blended threats. Sophos antivirus software features a highly proactive virus scan engine (VSE) technology that provides real-time protection against viruses, adware, worms, spyware, zero-day threats and data stealing malware. Sophos Antivirus for Network Storage protects applications, servers and storage systems from hosting and distributing malware in a networked environment.

Sophos antivirus software provides a scalable solution that allows high-performance security scanning using multiple scanning servers to run in parallel, while utilizing load balancing solutions and failover capability to service one or more storage devices. Sophos antivirus software works with the Sophos Antivirus Dynamic Interface (SAV-DI) to provide a seamless integration and comprehensive storage security scanning to HPE 3PAR File Persona services using the industry-standard Internet Content Adaption Protocol (ICAP).

Sophos Antivirus Dynamic Interface (SAV-DI)

Sophos Antivirus Dynamic Interface provides an interface to Sophos antivirus software enabling scans to take place locally or over the network using the industry-standard ICAP. SAV-DI can be run as a command line process, as a daemon on Linux® or Unix® systems, or as a command line process or service on Windows® systems. SAV-DI communicates requests to the Sophos antivirus scanner installed on the same server to protect network attached storage from viruses, Trojans, worms, spyware and adware. Detection rates are increased by combining detection technologies like Dynamic Code Analysis, pattern matching, heuristics, emulation, and Behavioral Genotype Protection to detect known and unknown threats. SAV-DI automatically updates virus signatures and engine libraries to enable around the clock protection.

Solution overview

To protect NAS systems effectively, it is critical not only to protect the NAS system, but also to protect the rest of the network infrastructure from intrusion and attack. If any parts of the network are open or vulnerable, they can be leveraged for a denial-of-service attack or a blended threat. Since a NAS system is accessed through the network, it is just as vulnerable as the rest of the network devices to being taken offline by these types of attacks. The new breed of threats demands a more integrated, proactive, and layered approach to security that will protect every part of the enterprise network—from gateway to client, server, and storage.

Antivirus software cannot be installed natively on enterprise-class storage arrays. Any files accessed by the users that require virus scanning must be sent over the network to external servers running antivirus software designed to offer virus scanning services to storage systems.

Sophos antivirus software for NAS devices with SAV-DI supports external dedicated servers, thereby offloading the virus scanning task from HPE 3PAR StoreServ Storage. The antivirus feature of HPE 3PAR File Persona integrates with the Sophos virus scan engine (VSE) to provide on-access or on-demand scanning of the files stored in the HPE 3PAR StoreServ Storage array. HPE 3PAR File Persona can scale and support up to 50 scan engines.

Antivirus scanning in HPE 3PAR File Persona can maintain a connection to the Sophos VSE to scan files dynamically as they are opened or closed. Files are scanned before the requesting user gains access to the file. This type of scan is called an on-access scan, and when configured, is done automatically by the HPE 3PAR kernel. File reads and writes from SMB clients trigger the on-access scanning.

It is not enough to use on-access scanning only. Infrequently accessed files are infrequently scanned, which increases the chances of the file becoming infected. Antivirus scanning in HPE 3PAR File Persona can also be a scheduled task, thereby providing additional on-demand protection. This periodical scanning is controlled by administrator configuration. With on-demand scanning, protection is not just at the file level; entire directories or even entire HPE 3PAR File Persona file shares or file stores may be scanned.

Antivirus scanning in HPE 3PAR File Persona will record the results of the scan and quarantine any infected files for subsequent review and action by the administrator. Any file changes and file scans are tracked by the antivirus function of HPE 3PAR File Persona. After a file has been scanned, it is not scanned again until it is modified or until the virus definitions have been updated. If no scan engines are available to perform the scan, HPE 3PAR StoreServ can allow or deny access to the files based on the policy configured for VSE availability.

Solution components and architecture

Sophos virus scan engine (VSE)

The Sophos virus scan engine executes the file scanning and virus and threat detection functions. Scans are relayed to the scan server through SAV-DI via ICAP providing real-time protection. Multiple scan servers can be configured to increase scan performance and reliability.

Sophos Antivirus Dynamic Interface (SAV-DI)

The Sophos Antivirus Dynamic Interface enables communication between HPE 3PAR File Persona and the Sophos antivirus scan server via the ICAP standard. SAV-DI relays the scan requests to the Sophos antivirus scan server installed on the same server. SAV-DI is a general-purpose interface to the Sophos antivirus scan server providing a single copy of the malware database for efficiently increased protection.

Figure 1 illustrates the product architecture for Sophos antivirus software with SAV-DI.

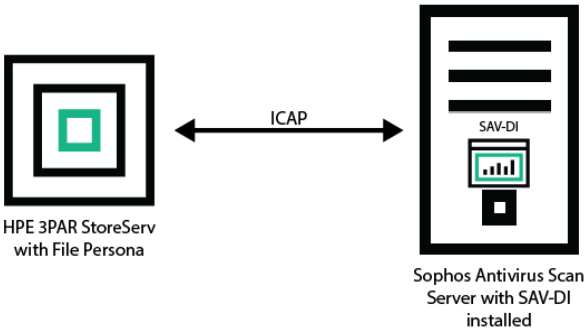

Figure 1. Sophos antivirus software with SAV-DI architecture

Antivirus scanning

Figure 2 illustrates the following flow of information between HPE 3PAR File Persona and Sophos antivirus software for NAS devices:

1. The client requests an open (read) or close (write) of an SMB file, or read of an NFS or HTTP file.
2. HPE 3PAR File Persona determines if the file needs to be scanned based on the policies that have been set and notifies the Sophos antivirus servers. The file is then sent to the Sophos Antivirus Dynamic Interface (SAV-DI) via ICAP. Then requests are relayed to the Sophos antivirus scanner that's installed on the same server.
3. Sophos antivirus software scans the file and reports the scan results back to HPE 3PAR StoreServ system.
4. If no virus is found, access will be allowed to the file. If a virus is found, then there will be an "Access Denied" to an SMB client, a "Permission Denied" to an NFS client, or "transfer closed" to an Object Access API client. HPE 3PAR File Persona then quarantines the file and logs the scan messages.

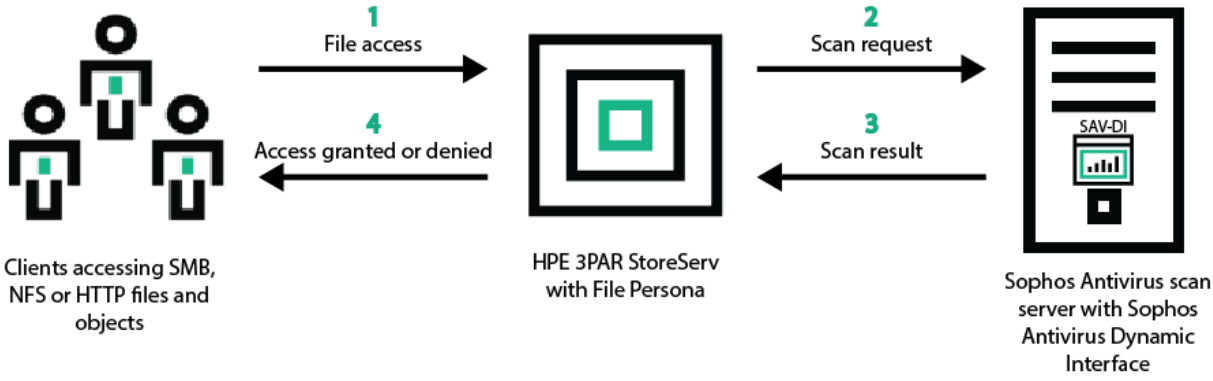

Figure 2. Antivirus scanning and threat detection flow

Capacity and sizing

Sophos savdid.conf parameters

For optimum performance, you must tune parameters in the SAV-DI configuration file. If the parameters are not tuned (`threadcount`, `maxqueuedsessions` and `Allow204`), the scan server can be reported as DOWN in the HPE 3PAR StoreServ Management Console (SSMC). The following parameters need to be changed:

- `Channel: ICAP`
- `Port: 1344`
- `Service: AVSCAN`
- `Allow204: Yes`
- `Keepalive: Yes`
- `Threadcount: 32`
- `Maxqueuedsessions: 1200 (value between 1024 ~ 1280)`

Note
Use a physical machine for Sophos VSE with internet connectivity as suggested by the vendor. For best performance, tune the parameters (`threadcount`, `maxqueuedsessions`, and `allow204`) in the Sophos SAVDI configuration file. The suggested value for `threadcount` is **32**. The suggested value for `maxqueuedsessions` is **1200** (value between 1024 ~ 1280). The `allow204` parameter is set to YES (enabled). HPE recommends these parameter settings based on performance testing (scanning of files with average size of 100 KB) in dual core 48 GB RAM physical machine. Refer the vendor documents for minimum hardware requirement, configuration, and installation steps.

SAV-DI has a single logger for logging events and messages. The log can be sent to the console, a file or on Linux/Unix, the syslog. You can also specify the level of logging. The following parameters can be set in the configuration file based on your requirements:

- Specify the logging mechanism `{CONSOLE | FILE | SYSLOG}:`

  Type: `FILE`

- Specify the level of logging required:

  0 = errors + threats

  1 = (0) + process events

  2 = (1) + session events

  Log level: 0

Analysis and recommendations

Sophos antivirus scanning servers should be installed on a physical machine.

- Locate the Sophos antivirus scanning server that is physically closest to the HPE 3PAR StoreServ Storage system to reduce network latency and maintain optimum file access time.
- Add at least one additional Sophos Antivirus for NAS scanning server to increase the scan engine availability and improve the performance for virus scanning tasks. When multiple scanning server VSEs are added to the cluster, all incoming scan requests are distributed in a round-robin fashion.
- Configure the antivirus feature of HPE 3PAR File Persona for both on-access and on-demand scanning.
- To increase antivirus protection, consider running on-demand scanning during off hours or when the HPE 3PAR StoreServ Storage system is not running priority tasks.
- Antivirus software reads a file and then compares it against a locally stored database of known virus patterns, resulting in the file testing either positive or negative for a virus. The databases of virus patterns are referred to as virus pattern files or virus definitions. The pattern files need to be frequently updated to stay in sync with all the known virus signatures. Be sure to deploy Sophos AutoUpdate to perform scheduled updates of these files, as well as updating the virus definitions in the HPE 3PAR StoreServ Management Console.

Summary

With the HPE 3PAR File Persona, you can unlock the native file and object access capabilities within your HPE 3PAR StoreServ Storage array, made possible by the HPE 3PAR Operating System and your array's Converged Controllers. HPE 3PAR File Persona provides easy, centralized management of user data for home directory consolidation, and group or corporate shares on HPE 3PAR StoreServ Storage systems. Sophos antivirus software for NAS devices protects applications and network-attached storage devices from hosting and distributing malware. Combining the HPE 3PAR File Persona antivirus features with Sophos antivirus software safeguards valuable enterprise data from virus threats.

Resources and additional links

Virus scanning best practices guide for HPE 3PAR File Persona, http://h20195.www2.hpe.com/V2/GetDocument.aspx?docname=4aa5-6079enw

HPE 3PAR StoreServ Storage, https://www.hpe.com/us/en/storage/3par.html

HPE 3PAR File Persona Software, https://www.hpe.com/us/en/product-catalog/storage/storage-software/pip.hpe-3par-file-persona-software.7415887.html

Sophos Antivirus for Network Storage, https://www.sophos.com/en-us/products/server-security.aspx

Sophos Antivirus Dynamic Interface (SAV-DI), https://www.sophos.com/en-us/partners/oem-and-technology/products.aspx#

To help us improve our documents, please provide feedback at hpe.com/contact/feedback.

Learn more at hpe.com/storage

Sign up for updates

a00018112enw, June 2017

Hewlett Packard Enterprise