Technical Explanation of P.A.S.S

Pro-Active Seamless Support is our independent solution to monitoring and managing your storage array. It works much like the original equipment manufacturer's monitoring solution. Our P.A.S.S. client software constantly monitors your system looking for any new alerts or errors. Once a new alert or error is detected, the P.A.S.S. client sends the encrypted information to our Diagnostic PASS Server. From there it automatically opens a new service ticket and sends text and email to all relevant management and engineers.

P.A.S.S. runs on a VM that communicates outbound over SSL on port 9455 and 443.

Section:

1. How Does P.A.S.S. Work

P.A.S.S. runs as a client agent on a virtual machine or the monitored array's physical management server. Setup on a schedule it communicates securely with our P.A.S.S. management framework of servers (home).

The P.A.S.S. client checks for any new errors or alerts on the monitored array. When a new error or alert is detected, the P.A.S.S. client will send home the new information as an encrypted payload where it is decrypted and analyzed. Based on the necessity of the results, a new service ticket is generated and notifications are sent by text and email to the engineers on call and relevant management team members.

The P.A.S.S. client sends multiple heartbeats home daily to ensure the monitoring service is active. When new missing heartbeat(s) are detected, 'missing heartbeat' service tickets are generated.

* Please note: P.A.S.S. monitoring has its own encryption framework and will not work across any proxy services.*

2. P.A.S.S and Your Security

P.A.S.S. uses four levels of encryption to make sure that your array's information is unavailable to view or use by anyone else except our P.A.S.S. management framework.

To protect your infrastructure against outsider intrusion our P.A.S.S client needs TCP Port 9455 OUTBOUND ONLY to our P.A.S.S Management IP Address and traffic travels using HTTPS SSL protocol.

3. DKC500, DKC600, DKC700, and DW700 Series

P.A.S.S. is supported on the following arrays:

DKC500:

Hitachi - USPNSC55, UPS **HP** – XP10000, XP12000 **SUN** – 9985, 9990

DKC600:

Hitachi – USPV-M, USPV **HP** – XP20000, XP24000 **SUN** – 9985V, 9990V

DKC700:

Hitachi – VSP **HP** – P9500

DW700:

Hitachi – HUS-VM **HP** – XP7

DKC800:

Hitachi – VSP- G Series

The P.A.S.S. client is installed and run directly on the storage array's Service Processor (SVP). It actively parses the array log area for new messages and reacts by forwarding the alert codes, timestamps, and customer/array identity into an encrypted payload and sends using HTTPS with SSL certificates.

The P.A.S.S. Management framework receives the encrypted payloads, decrypts, interprets the customer, site and array identifiers and decodes the alerts for ticket processing.

SVP functionality unchanged, the P.A.S.S. client has NO access to customer data of any kind. P.A.S.S., as well as the SVP, can only access the array for maintenance purposes.

Installing P.A.S.S. on the DKC and DW arrays

The P.A.S.S. installation team provides a new customer form to gather the necessary information needed to configure the client.

Remote or local SVP desktop and filesystem access are necessary to upload or copy, and to configure the client. Typically this is being done by the assistance of the customer or a local field engineer utilizing portable drives to copy the installation, Windows Remote Desktop Protocol (RDP), Bomgar Remote Client or customer's preferred remote access are the tools of choice.

To make sure that P.A.S.S. can run correctly, the client will need the outbound TCP Port 9455 and 443 open to 76.190.62.2, and 443 to 74.112.3.220

The Windows Task Manager is used to schedule P.A.S.S. to run periodically. Usually, SVP passwords do not change. If they do change the scheduled task needs to have the password changed also.

4. DF700, DF800, and DF850 Series

DF700:

Hitachi – AMS200, AMS500, AMS1000

DF800:

Hitachi – AMS2100, AMS2300, AMS2500

DF850:

Hitachi – HUS110, HUS130, HUS150

The P.A.S.S. client is installed and run on a virtual machine that we provide for your team to deploy. P.A.S.S. works in conjunction with the array's controllers to collect component status from the array. Local array read-only accounts can be created to use for monitoring purposes.

P.A.S.S. interrogates the array's controllers, this way NO access to the customer data of any kind. P.A.S.S. can only access the for maintenance purposes.

Installing P.A.S.S. on the DF arrays

The P.A.S.S. installation team provides a new customer form to gather the necessary information needed to configure the Virtual Machine and client. Remote access will is necessary to configure and test the client and VM. This can be done by the assistant of the customer. To make sure that P.A.S.S. can run correctly, the client will need the outbound TCP Port 9455(HTTPS) and 443(SSL) open to 76.190.62.2, and 443 to 74.112.3.220

5. HP 3Par Series

3Par:

HP – E-Class, F-Class, 7000, 8000

HP – S-Class, T-Class, V-Class 10000

The P.A.S.S. client is created on a virtual machine that we provide for your team to deploy. P.A.S.S. works in conjunction with the array's nodes to collect service logs and alerts from the array.

P.A.S.S. interrogates the array's controllers, this way NO access to the customer data of any kind. P.A.S.S. can only access the for maintenance purposes.

Installing P.A.S.S. on the 3Par arrays

The P.A.S.S. installation team provides a new customer form to gather the necessary information needed to configure the client. Remote access will be needed to upload and configure the client and VM. This can be done with the assistance of the customer. To make sure that P.A.S.S. can run correctly, the client will need the outbound TCP Port 9455(HTTPS) and 443(SSL) open to 76.190.62.2, and 443 to 74.112.3.220

6. Nimble Series

SC Series:

The P.A.S.S. client is created on a virtual machine that we provide for your team to deploy. P.A.S.S. works in conjunction with the array's nodes to collect service logs and alerts from the array.

P.A.S.S. interrogates the array's controllers, this way NO access to the customer data of any kind. P.A.S.S. can only access the for maintenance purposes.

Installing P.A.S.S. on the Nimble arrays

The P.A.S.S. installation team provides a new customer form to gather the necessary information needed to configure the client. Remote access will be needed to upload and configure the client and VM. This can be done with the assistance of the customer. To make sure that P.A.S.S. can run correctly, the client will need the outbound TCP Port 9455 and 443 open to 76.190.62.2, and 443 to 74.112.3.220

* Please note: P.A.S.S. monitoring has its own encryption framework and will not work across any proxy services.*

7. Support

In the event of a service call on your array, a technician will be dispatched with replacement parts. To ensure the security of your system, only expertly trained backline support engineers are authorized to remotely connect to the management workstation. The backline engineer works in tandem with the on-site technician, sending commands to the SVP/SP/Node via the management workstation while directing the technician's action's need to be taken to diagnose and resolve any issues on your machine.

8. Remote Access

Remote access to the array tools offers the backline capability to check problems and closely investigate, resolve issues quickly, flash and locate components during servicing. These benefits lead to faster responsive service, closely guided hands-on activity and direct problem resolution versus long phone or texting sessions with explanations before actually gathering and resolving issues.

To ensure a smoother service, we offer remote access for the backline support team members. To allow this access the local management workstation would need Outbound access on TCP port 443 (HTTP over SSL) to 76.190.62.2 and 443 to 74.112.3.220 The remote access client that we use is Bomgar.

https://www.bomgar.com/

White Papers:

https://www.bomgar.com/resources/whitepapers#lang=en

9. P.A.S.S. Environment Requirements

The Pass Tool Needs a VM environment. It has been deployed VMware, Hyper-V, VirtualBox, ProxMox, and Xen Server. Any system that supports OVA or VHD Virtual Machines should be sufficient.

The hardware requirements are as follows, 1 CPU core, 1 GB of Memory, 8GB of Storage Space, and 1 or 2 Network Interfaces depending on how you route to the internet and the machine.

The system is a self-contained, stripped-down Debian 9 OS. If you wish to have rolling security updates, then it will need access to the Debian security repository. However, this device is very limited in scope. The only inbound port open is SSH and can be turned off at the customer's request. It is only there for the customer's convenience for remote administration and is not required for monitoring.

To have the P.A.S.S. tool installed for your environment, please send over the answers to following questions below to pass@seamlesssupport.com or your sales representative.

This device is pre-configured before it is sent out. We will need to know your virtual environment so we can send the right version. Also, we will need a static IP address, netmask, and gateway, to pre-set the device.

This P.A.S.S. virtual appliance will need to communicate to your array(s). For pre-configuration, please provide the serial number(s) and management IP address(es) for each array.