Pure1™

FlashArray Port Assignments

This article is to serve as a reference for which ports Pure Storage uses by service. Please keep in mind that firewall rules may apply to the management IPs of both controllers as well as the Virtual IP, and should be configured as such, such as for Pure1 Connectivity.

Ports Used by Purity for Services

The following table lists the Purity Services and the associated ports that must be open on the FlashArray. Unless otherwise noted, all service ports must be open on the specified interface. Note that some services use more than one port.

Please note, if any of these services are being accessed over a WAN, you will need to open these ports to the Public Network.

Service	Port	Network Interface	Transport Protocol	Application Protocol	Direction	Additional Information
iSCSI Service	3260	Host Port	TCP	iSCSI	Inbound	
Management Service	22	Management Port	TCP	SSH	Inbound	
	80	Management Port	TCP	HTTP	Inbound	Redirects to HTTPS port 443
	161	Management Port	UDP	SNMP	-	Used by the SNMP MIB to collect array information.
	443	Management Port	TCP	HTTPS	Inbound	Used to access the Purity GUI & REST API
Replication Service	8117	Replication Port	TCP	-	Inbound (Target) Outbound (Source)	Default bond, named "replbond", used to receive replication data. Open this port on the target array. NOTE: In order to replicate data between two arrays, open ports 443 and 8117 on the firewall so that they are reachable

Outgoing Ports to a Public Network

After Purity 4.9, when FlashArray connects to Pure1 Cloud, it will first try connecting via the new methods of HTTPS and SSH over HTTPS. The FlashArray must be able to connect to these ports to do the following:

- Send array diagnostic, log, and performance data to Pure1 Cloud (via HTTPS).
- Enable Pure Storage Support, when given permission from the customer, to view and administer the FlashArray via remote assist sessions (via SSH over HTTPS).

If the FlashArray fails to connect Pure1 Cloud via the new methods, by default, it will fall back to using the connection methods of SSH and SSH over HTTPS used before Purity 4.9. These ports are summarized in the table below. In order to connect to Pure1 Cloud even when the new connection methods fail, the FlashArray should enable these ports. However, if the FlashArray does not want any non-HTTPS outgoing connection, the following ports should be disabled.

Component	Purity Version	Port	Transport Protocol	Application Protocol	Direction	Additional Information
Pure1 Cloud	4.9.0+	443	TCP	HTTPS	Outbound	For IPv4, use the following IP block and hostnames: • IP block 52.40.255.224/27 [1] • Hostnames: ◦ *.cloud-support.purestorage.com For IPv6, we currently do not support static IPs. Use the following hostnames:
Pure1 Cloud	4.9.0+	443	TCP	SSH over HTTPS	Outbound	• *.cloud-support.purestorage.com Please add all of the above to your whitelist. [1] This is an IP CIDR block. This refers to 32 IPs (52.40.255.224 - 52.40.255.255). Most firewalls will accept the whole block, so it can be entered as one-line in most cases.
Pure1 Cloud	4.8.x-	22	TCP	SSH	Outbound	Use with the following hostnames / IP addresses:
Pure1 Cloud	4.8.x-	443	TCP	SSH over HTTPS	Outbound	• phlb1.purestorage.com (50.112.109.24)

Component	Purity Version	Port	Transport Protocol	Application Protocol	Direction	Additional Information

						• phlb2.purestorage.com (50.112.109.205)
						• *.cloud-support.purestorage.com (52.40.255.224/27) [1]
						• Additional IP's used (Prior to 4.9.x only)
						  ◦ 50.112.109.24
						  ◦ 50.112.109.205
						  ◦ 52.64.175.227
						  ◦ 52.64.233.172
						  ◦ 52.11.11.2
						  ◦ 52.11.27.144
						  ◦ 52.76.11.29
						  ◦ 52.74.190.195
						  ◦ 52.17.31.75
						  ◦ 52.30.94.237
						  ◦ 54.232.253.142
						  ◦ 54.94.198.85
						
						Please add all of the above to your whitelist.
						
						[1] This is an IP CIDR block. This refers to 32 IPs (52.40.255.224 - 52.40.255.255). Most firewalls will accept the whole block, so it can be entered as one-line in most cases.

Outgoing Ports to Internal Services (Private Network)

The following table lists the ports that must be open in order to allow the FlashArray to reach other services.

Component	Port	Transport Protocol	Application Protocol	Direction	Additional Information
Email	25	TCP	SMTP	Outbound	Used to route alert and other email messages. The default port here is 25, but it can be user-defined. If your environment has a different port, please update your firewall settings accordingly.
DNS	53	UDP	DNS	Outbound	Directory Name Services
Directory Service (LDAP)	389	TCP	LDAP	Outbound	Used to manage array integration with a directory service using LDAP. Only required if integrating with a directory service. Can be user-defined.
Directory Service (LDAPS)	636	TCP	LDAPS	Outbound	Used to manage array integration with a directory service using LDAPS (LDAP over TLS/SSL). Only required if integrating with a directory service. Can be user-defined.
NTP	123	-	UDP	Outbound	Used to synchronize the array time to the NTP sever.
Proxy Server	80, 443	TCP	HTTP	Outbound	Used for HTTP proxy. Can be user-defined.
REST API	443	TCP	HTTPS	Inbound + Outbound	Required by replication to communicate between two arrays. Open port 443 on the firewall. Pure Storage's Plug-Ins and SDKs utilize the REST API service for communication to the array. So, if you are using any plug-ins / SDKs, please ensure this port is open.
SNMP Trap	162	TCP	UDP	Outbound	Used to send SNMP trap messages
Syslog	514	TCP	-	Outbound	Used for system logging. Can be user-defined

Other Ports

Please note that destination ports 44444 through 44507 (UDP) may be used by Purity for diagnostic purposes.

Internal Information: Do not share externally.

So to summarize: By experimentation, UDP ports 44444-44507 are used by tracepath whenever gather_diagnostics is run (e.g. during hourly phonehome). Other UDP ports are randomly used for DNS queries.