

FLASHARRAY™ ACCESS SECURITY

How Pure Storage™ FlashArrays protect against unauthorized local and remote access

FLASHARRAY ACCESS POINTS

FlashArrays connect to the external environment in four ways:

STORAGE NETWORK

Fibre Channel, iSCSI, or NVMe-oF links between arrays and storage networks or host computers.

REPLICATION NETWORK

TCP/IP connections between FlashRecover asynchronous replication source and target arrays, and between ActiveCluster synchronously replicating *partner* arrays.

ARRAY ADMINISTRATION

TCP/IP connections between an array and a GUI or CLI running on a workstation or mobile device, or administrative applications that use the Purity//FA REST interface.

SUPPORT

TCP/IP connections for transmitting logs to the Pure1® cloud-based support framework and for conducting RemoteAssist diagnosis and remediation sessions with Pure Storage Technical Services Engineers.

This brief describes how FlashArray protects against threats of misappropriation, alteration, or destruction of stored data by unauthorized access on each of these paths.

SECURING ACCESS TO STORED DATA

FlashArray presents *volumes* to hosts via Fibre Channel, iSCSI, or NVMe-oF storage network fabrics. Many fabrics are internal to the data center and so are physically secure. For routed connections, however, and to prevent access by unauthorized hosts, users should configure zones or VLANs to restrict access to data in transit.

Regardless of storage network type, FlashArray administrators must *connect* volumes to hosts, effectively whitelisting them, before arrays will respond to their I/O commands. Internally, FlashArray represents hosts as *host*

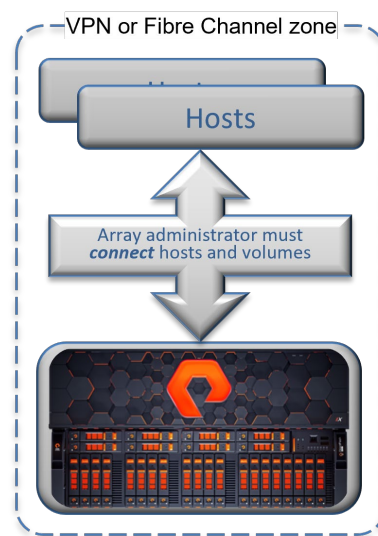


Figure 1: Data Access Security

object data structures—lists of the hosts’ storage network addresses. Arrays only respond to commands from storage network addresses associated with hosts that an administrator has connected to the volumes their commands address.¹

Technical Brief TB-160201 describes how FlashArray protects the data at rest in an array from misappropriation.

SECURING COMMUNICATIONS BETWEEN ARRAYS

Because the usual reason for replicating data between arrays is disaster protection, replication often takes place over routed connections that pass through firewalls. FlashArray encrypts locally stored data, but does not encrypt replicated data during transit. Where “on the wire” encryption is required, it is performed by network gateways and/or VLANs. Network administrators must permit TCP/IP connections through firewalls for the ports that arrays use to make replication connections and to transfer data.

To minimize the possibility of a remote computer impersonating a replication target or peer array and misappropriating data, pairs of replicating arrays exchange a credential called a *replication connection key* before establishing the replication TCP/IP connections. One array’s administrator uses the CLI or GUI to generate a replication connection key and communicates it (securely) to the other administrator, who installs it in the partner array. Either administrator can establish a replication connection between arrays with matching keys.

Once replication connections are established, both arrays’ administrators must explicitly permit replication to occur. With FlashRecover, for example, source array administrators *enable* replication; target administrators *allow* it. Either administrator can stop replication at any time. These protections help administrators limit exposure to network breaches, and in addition they make it possible to suspend replication temporarily, for example if network load becomes too high or a target array’s available storage becomes dangerously low.

SECURING ADMINISTRATIVE ACCESS TO ARRAYS

Administrators interact with arrays using either a command line interface (CLI) accessed from a virtual console such as PuTTY or ssh, a Graphical User Interface (GUI) in a web browser, or a

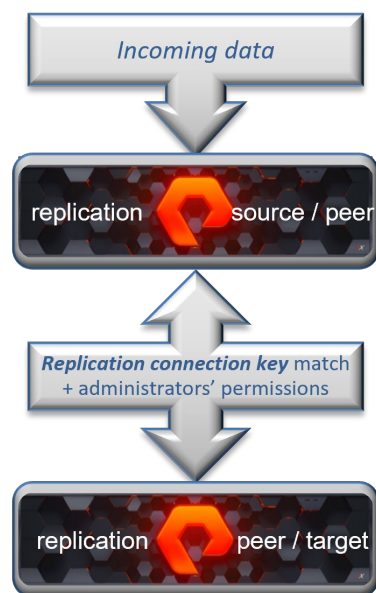


Figure 2: Replication Security

¹ For iSCSI connections, array administrators may additionally configure *Challenge Handshake Authentication Protocol (CHAP)* to prevent an unauthorized host from impersonating an authorized one.

mobile device application. In addition, Purity//FA supports a REST API for software-based administration and for VMware's *vStorage APIs for Storage Awareness (VASA)*.

CLI access is validated either by a *public/private key* (PPK) pair or an account name and password. GUI access uses account name and password for validation. Arrays may validate passwords themselves, or they may optionally be configured to query an Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) service for validation.

Array administrators generate account-specific *API tokens* that are used to validate REST exchanges. With VASA, vCenter administrators manage FlashArray systems in vSphere environments using interfaces with which they are familiar. FlashArray administrator credentials validate an array's first interaction with vCenter; thereafter, certificates generated and validated by vCenter authenticate interactions.

Each FlashArray account is associated with one of four roles:

- ▶ **Read-Only:** can perform operations that report array state but cannot alter it.
- ▶ **Ops Admin:** Read-Only operations plus plus controlling RemoteAssist sessions.
- ▶ **Storage Admin:** Read-Only operations plus operations on volumes, hosts, and host groups, but not global or array configuration operations.
- ▶ **Array Admin.** All administrative operations.

FlashArrays are delivered with a pre-installed **pureuser** account that has the **Array Admin** role. The **pureuser** account password can be changed, but its role cannot, nor can it be deleted.

Administrators, REST applications, and vCenter use secure connections between arrays and workstations, mobile devices, and management servers to create, resize, organize, copy, and destroy storage volumes, to manage host-volume connections, to schedule snapshots and replications, and to monitor array performance and storage utilization.

Arrays log all administrative interactions, including successful and unsuccessful logins, in a circular buffer that overwrites the oldest entries with the newest ones when it fills. Logs cannot be deleted, except by a Pure Storage Technical Services engineer resetting an entire array. Administrators can view logs via the GUI or CLI and can optionally configure arrays to send them to syslog servers.



Figure 3: Administrative Access

None of the FlashArray administrative interfaces provides access to stored data. Purity//FA software has no facilities for an administrator to read stored data or to write data to an array's volumes. While an administrative access breach might enable an attacker to masquerade as an array or storage administrator and obliterate data by eradicating volumes, it would not enable data alteration or other misappropriation. Purity//FA provides robust mechanisms for limiting access to arrays to authorized administrators, but it is incumbent on array owners to manage administrator authorizations.

SECURING ACCESS FOR SUPPORT

Except where it is technically infeasible or prohibited by user policy, arrays regularly use a REST API to upload performance, utilization, log, and alert information to Pure1, a feature colloquially called *phonehome*. The Pure Storage Technical Services organization uses phonehome information for diagnosis and remediation, fingerprint analysis and development, and for routine monitoring and statistics collection.

Pure Storage Technical Services engineers use the *RemoteAssist* (RA) facility to perform hands-on diagnosis and remediation. Array administrators must *enable* RemoteAssist and initiate RA sessions. Sessions are often accompanied by phone or video communication with the Technical Services Engineer, whose every action is indelibly logged by the array.

Phonehome and RA do not access user data. Nevertheless, their communication paths between array and Pure1 must be secure to avoid exposing tangential information such as volume properties, utilization, I/O activity, storage network addresses, host identities, snapshot and replication schedules, and so forth.

When an array is installed, generates a *public-private key* (PPK) pair and signs and sends its public key securely to a Pure1 database. Pure1 uses the array's public key to verify its identity in subsequent interactions.

The array also creates a generic self-signed digital certificate. When a GUI user attempts to connect to the array through a browser, the array confirms its identity by presenting its certificate for validation. Administrators in the array role can change certificate attributes and import additional certificates from recognized signing authorities. For optimal access security, Pure Storage strongly recommends the latter. Arrays automatically update their digital certificates when necessary, for example shortly prior to expiration.

At time of publication, current releases of Purity//FA software secure phonehome exchanges and RA sessions with TLS Mutual Authentication and HTTPS encryption. With TLS Mutual Authentication, encrypted message exchanges are not susceptible to the "man in the middle"

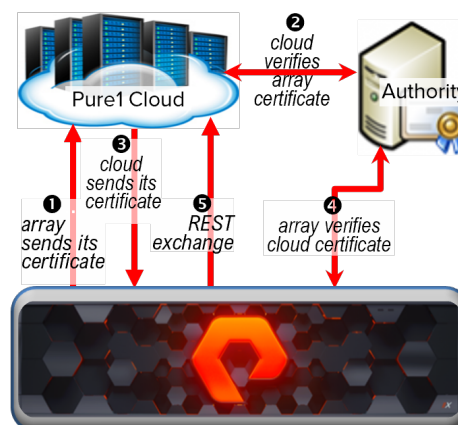


Figure 4: Mutual Authentication

SSL interception that some organizations use to audit traffic leaving their internal networks. (Earlier Purity//FA versions did not use TLS Mutual Authentication, so interception was possible.)

SECURING REMOTEASSIST SESSIONS

When an array administrator initiates an RA session, the array and a remote Pure1 server perform TLS Mutual Authentication. The array then generates a one-time password which it sends to the Technical Services engineer via a secure network path (separate from the path used by the session). The engineer echoes the password to the array, thus verifying his or her authenticity. Communication during the session uses ssh within an HTTPS encrypted tunnel. As with phonehome exchanges, interactions between Support Engineers and arrays cannot be intercepted. Arrays log every Technical Services engineer action.

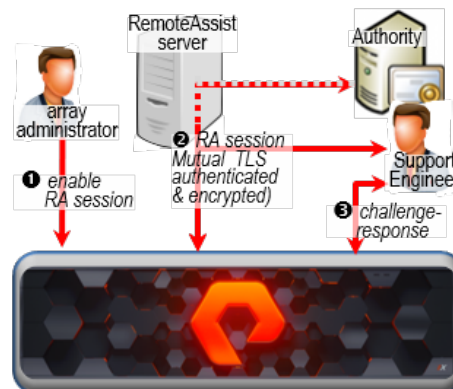


Figure 5: RemoteAssist Authentication

FlashArray administrators control RA sessions. Arrays automatically terminate sessions after 48 hours of inactivity, but an administrator can terminate a session at any time by disabling RemoteAssist with the CLI or GUI. RA sessions enable Technical Services engineers to view internal array information for diagnosis and to perform certain maintenance operations not available with any of the administrative roles.

SECURING USER ACCESS TO PURE1®

Pure1 Manage (often referred to simply as Pure1) is a comprehensive management platform for Pure Storage products. It is a distributed cloud application available to Pure customers with current support agreements at no incremental cost. It. With Pure1, customers' authorized representatives can use artificial intelligence-based models to forecast storage capacity and I/O performance needs for individual workloads, analyze full-stack performance down to the virtual machine level, manage volume group snapshots stored either locally or in a public cloud service, view the utilization, performance history, and alert status of their arrays, and manage support cases through a browser or mobile application.

Pure1 distills information from the logs it receives from arrays; it does not access the arrays directly.² The information visible to Pure1 users includes array and host object names, alert and support case status, volume properties, replication schedules and status, historical and projected utilization and performance, and so forth, *for their arrays only*.

² Pure1 does provide one-click access to arrays' GUI login pages, from which administrators can log in with their credentials and manage their arrays directly.

When a Pure Storage product is installed, a company representative creates a record of the array's security certificate in a Pure1 private database. Pure1 uses the database to restrict organizations' access to information about their own arrays.

Pure Storage representatives create a *Pure1 administrative user* (**Pure1 Admin**) account for each of their customers. Users with **Pure1 Admin** accounts can create and delete additional accounts, including **Pure1 Admin** ones, for their organization. Pure1 supports single sign-on (SSO) access through recognized identify providers that support the *Security Assertion Markup Language* (SAML 2.0). For organizations that do not use SSO, Pure authenticates Pure1 logins via a recognized credentialing authority.³ **Pure1 Admin** users create and delete additional **Pure1 Admin** accounts (e.g., when an employee's role no longer requires **Pure1 Admin** access) upon customer or partner request.

PURE STORAGE AND PARTNER ACCESS TO PURE1

Pure Storage employees whose job functions require access to Pure1 data have access to information pertaining to the entire installed base. Pure Storage extends Pure1 access, except for support case information, to its *Authorized Service Providers* (ASPs) automatically. Organizations that acquire their arrays through other partners can create accounts to enable the partners to access Pure1 information about their arrays. ASPs and other partners can only access information pertaining to arrays for which they are responsible.

In addition, Pure Storage sales engineers and account executives regularly use Pure1 information for capacity planning and preemptive diagnosis.

Pure1 makes about a month of performance history and a year of storage utilization history available to users. It retains certain information indefinitely for internal use to resolve problems, to develop "fingerprints" of issues for preemptive diagnosis and remediation, and to conduct research leading to product improvements and enhancements.

FLASHARRAY AND COMMON CRITERIA

The Common Criteria Recognition Arrangement (CCRA) is an international agreement that defines criteria for specifying and evaluating security in information technology products. Published under the aegis of CCRA, the *Common Criteria for Information Technology Security Evaluation* (commonly known as CC) and related specifications define product profiles, security features, and testing criteria. Each CCRA signatory is represented by a national agency whose responsibility is IT security. The United States, for example, is represented by the National Information Assurance Partnership (NIAP, <https://www.niap-ccevs.org/>). These agencies approve security evaluation laboratories,⁴ which test IT products and issue certificates of compliance with criteria specific to product classes. Under the CCRA, signatory nations agree in principle to

³ At the time of publication, Salesforce.com, Inc.

⁴ In the United States, laboratories are certified by the NIST National Voluntary Laboratory Accreditation Program.

recognize each others' certifications, effectively making CC compliance an international IT product security certification.

Increasingly, organizations are using CC compliance to assure that the equipment in their data centers meets consistent, well-defined standards for securing data and access to it. Some, especially in the public sector, require that all IT products they acquire be CC-certified. Recognizing the importance of CC to its customers, Pure engages independent laboratories certified by NIAP,⁵ to evaluate FlashArray hardware and Purity//FA software for compliance to current CC profiles. Evaluations have thus far resulted in certification of most current FlashArray models and Purity//FA software versions against the Common Criteria Network Device Protection Profile, Version 1.1.⁶ Certification of newer array models, Purity//FA versions, and CC Profile versions is constantly in progress.

CC COMPLIANCE AND FLASHARRAY DEPLOYMENT

Strict CC compliance requires that certain FlashArray facilities, such as phonehome and RemoteAssist, be restricted or disabled. Thus, although all FA-400 and FlashArray//M arrays that run Purity//FA version 4.7 are certified CC-compliant, a Pure Storage or Qualified Partner representative must configure an array for full compliance when it is installed. After installation with full compliance configured, phonehome and RemoteAssist, can be enabled by an array administrator, but complete relaxation of CC-compliance requires engagement with Pure Storage Support or with a Qualified Partner.

⁵ For example, UL (<https://ims.ul.com/common-criteriaiso15408>) is one such laboratory.

⁶ <https://www.niap-ccevs.org/Product/Archived.cfm?par303=Pure%20Storage%2C%20Inc%2E> contains a partial list of certified FlashArray models. Certification documents for other models are available from FlashArray Product Management.

Secure access to FlashArray administration

© 2022 Pure Storage

The Pure P Logo, and the marks on the Pure Trademark List at <https://www.purestorage.com/legal/productenduserinfo.html>

are trademarks of Pure Storage, Inc. Other names are trademarks of their respective owners. Use of Pure Storage Products and Programs are covered by End User Agreements, IP, and other terms, available at: <https://www.purestorage.com/legal/productenduserinfo.html>

and <https://www.purestorage.com/patents>

The Pure Storage products described in this documentation are distributed under a license agreement restricting the use, copying, distribution, and decompilation/reverse engineering of the products. The Pure Storage products described in this documentation may only be used in accordance with the terms of the license agreement. No part of this documentation may be reproduced in any form by any means without prior written authorization from Pure Storage, Inc. and its licensors, if any. Pure Storage may make improvements and/or changes in the Pure Storage products and/or the programs described in this documentation at any time without notice.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. PURE STORAGE SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.