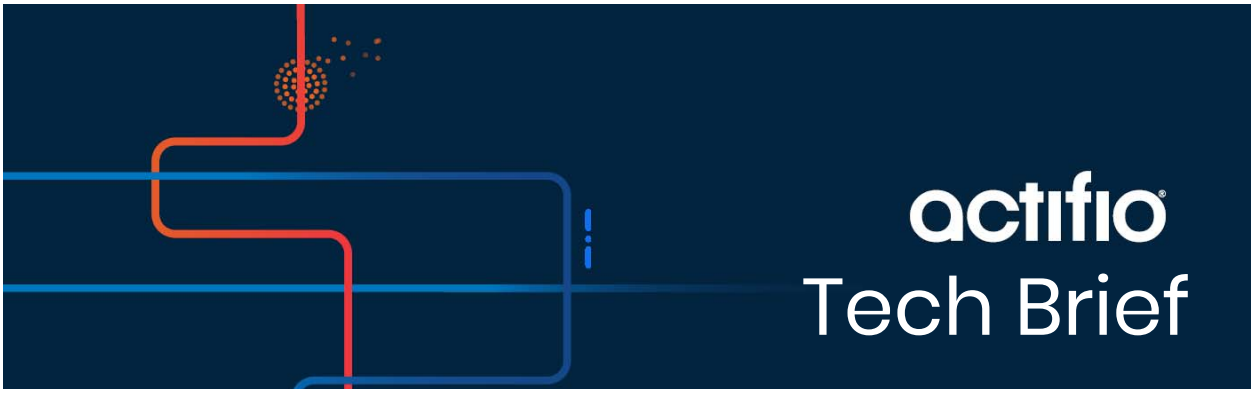


Data Security

All components of the Actifio Virtual Data Pipeline have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

This chapter describes:

Secure Operating System Access to Actifio Appliances

Actifio systems run on a hardened Linux software stack. Linux user accounts and direct access to the operating system are not required nor employed for normal operations and support of the Actifio systems. Direct access to the operating system can only be obtained via the use of time and system-limited cryptographic credentials obtainable by select users within Actifio support and engineering who have been undergone extensive background checks. Certificates are stamped with the identity of the user to whom they are issued, the issuing is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. Actifio employs a locked-down operating system that minimizes the possibility of unauthorized access. Even privileged users with direct access to the appliance's operating system can not access customer data unless they have access to a host on the storage fabric which can mount and understand the data.

Actifio VDP in a vSphere Environment

When Actifio VDP is deployed on a public cloud, the instance itself is protected by the cloud's security architecture. When deployed in an on-premises vSphere environment, the security of the instance is dependent on the configuration of the vSphere environment which hosts it. Insufficient security controls of the vSphere environment could allow an attacker to perform a side-channel or side-loading attack and gain unauthorized access to data or privileges on the Actifio Appliance(s).

While specific vSphere hardening is outside of the scope of this document, Actifio recommends customers follow VMware's best practices including, but not limited to, ensuring that the server BIOS and firmware be kept up-to-date along with the ESXi and vCenter versions to mitigate the "Meltdown/Spectre" class of side-channel vulnerabilities. Additionally, virtual machine encryption (available in vSphere 6.5+), can mitigate unauthorized tampering or side-loading of the Actifio Appliance(s) virtual disks. Customers should consult with their internal IT and/or security teams, VMware, or other resources with regard to security of a vSphere environment.

Internet Protocol (IP) Network Security

All components of Actifio VDP have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

Standard Network Services

The following services are deployed and listening on open network ports:

- HTTP (80): Actifio Appliance resource center, provides local downloads of the Connector software. No appliance control or data access is possible on this portal.
- HTTPS (443): Provides TLS-encrypted communication between Actifio GUI clients and the appliance, as well as some appliance-to-appliance communication. SSL certificates may be customer replaced.
- ssh (22): for user CLI
- ssh (26): for support CLI
- Actifio replication (5103): encrypted appliance-to-appliance data replication traffic. Both sides of this link utilize strong mutual authentication of the partner appliance.
- iSCSI, iSNS (3260, 3205): iSCSI target
- cimserver (5989): SSL encrypted WBEM (CDS Appliance only and utilized for SRM integration)
- svrloc (427): service location for WBEM (CDS Appliance only)

Appliance Outbound Connections

The appliance may make outbound connections to the following services, but not does not listen on or run a service for these ports unless listed above:

- LDAP/LDAPS (389/tcp, 636/tcp) Authentication of users against a central directory if configured
- DNS (53/udp) Resolution of addresses for hosts, VMs, vCenters, and other infrastructure
- NTP (udp/123) Clock synchronization against a customer-provided or public source
- SMTP (25/tcp, 465/tcp) Optional transmission of events via a customer-provided SMTP email relay server, can optionally utilize SSL encryption.
- SNMP (162/udp) Optional delivery of events in the form of SNMP traps to a trap receiver
- SSH (26/tcp) Encrypted intra-cluster communication between CDS Appliance nodes
- vSphere API (443/tcp) Required to communicate with vCenter servers and ESX hosts for snapshot and image management during backup and mounts over an encrypted link.
- ESXi data connectivity (902/tcp) Encrypted connectivity to VMware ESXi hosts for data movement operations.

- Actifio Connectors (5106/tcp) Encrypted control channel between Actifio Appliance and hosts running the Actifio Connector.
- Appliance-to-appliance Replication (5103/tcp, 5107/tcp) Encrypted replication data and control between two Actifio Appliances.
- SecureConnect (optional feature) remote support (1194/udp, 443/tcp) Encrypted remote support access to Actifio Connector data centers. As the connection is mutually authenticated with strong cryptography, it is recommended that the destination not be limited by a firewall.

SNMP

Most SNMP code on Actifio Appliances is outgoing only, sending traps to a configured receiver to notify events and failures.

The exception is when integrated with Actifio Connector Optimized Storage or SAN Fabric, CDS Appliances and CDX Appliances listen on UDP 162 for SNMP traps from specified IPs that are whitelisted for CDS Appliance Integrated Storage components.

A list of whitelisted IP's can be viewed with the following commands. Currently SNMP v1 and v2 are supported.

```
udsinfo
lsmonitoreddevice
id
name
type
address
5847
Brocade--SAN
switch
X.X.X.X
5850
DS3512--A
storage
X.X.X.X
5852
DS3512--B
storage
X.X.X.X
```

No Actifio configuration will ever accept any SNMP walk or write (e.g. GetRequest, SetRequest, GetNextRequest, GetBulkRequest) and this configuration of community names is not required or supported.

Cross Cluster Communication and Replication

All Actifio Appliances utilize strong mutual authentication of the partner appliance with verification of 2048-bit RSA public keys.

Once authenticated, data in flight between appliances is encrypted using 256-bit AES encryption with session keys protected by Diffie-Hellman algorithms affording Perfect Forward Secrecy (PFS) over a TLS v1.2 channel.

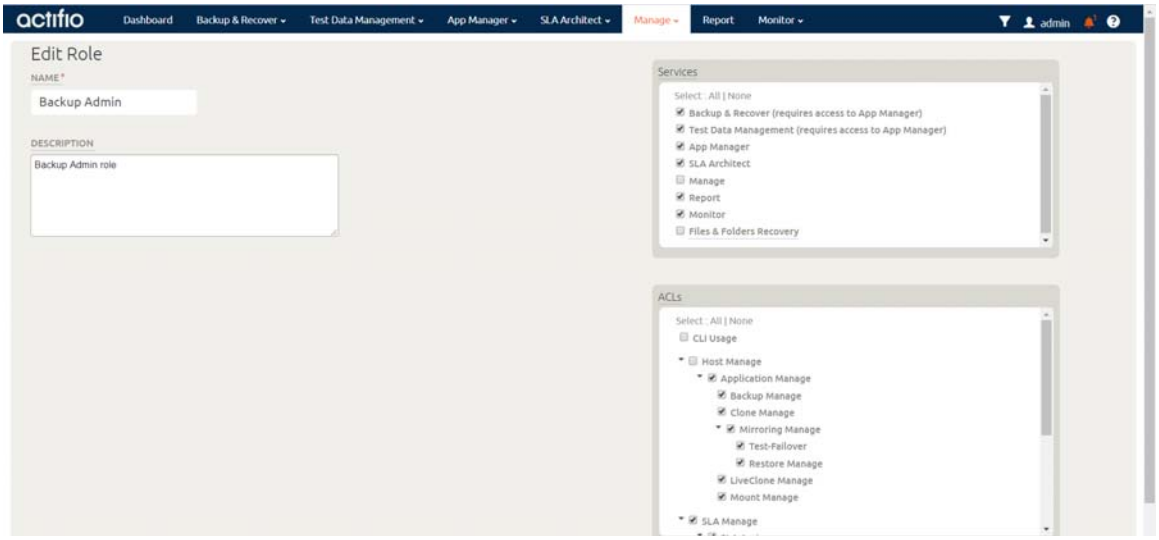
Access Control on Actifio Systems

Actifio Connector uses a very rich role-based access control mechanism that allows an administrator to assign rights to users to operate on objects. These users and rights are constrained to operating on objects owned by 'Organizations' of which they are members.

A role consists of a group of rights. Roles are assigned to users to use those rights on specific objects.

Users, Roles, Rights, and Organizations can all be modified and managed from either the CLI or the AGM.

Coupled together, roles and organizations allow the customer to define a specific group of servers/hosts/applications that a given user can perform specific actions on.



A Role Called Backup Admin

Authentication and Authorization

Actifio Appliance can either utilize an internal user directory or integrate with an external LDAP source, including Active Directory. This allows users to leverage their existing usernames and passwords, ensuring compliance with corporate password standards such as complexity and expiration. SSL encryption may optionally be utilized between the Actifio Appliance and the external LDAP server. LDAP/AD groups may be mapped to specific user-defined roles within the appliance.

Access Logging and Auditing

Actifio maintains a full audit log of every command that has been executed on the platform, including logging requester's IP address and method of access (CLI or AGM). The audit log can also be retrieved via the Actifio REST API for automatic ingestion into a central log or event correlation repository.
The audit log can be viewed from the CLI using the following command:

```
sa--hq1:~
$
udsinfo
lsaudit
id username stat status component issuedate proxy command ipaddress privileged
172675 admin 0 UI 13/12/2013 03:24:13.707 loginadmin 192.168.225.2 true
172675 admin 0 CLI 13/12/2013 03:24:25.707 loginadmin 192.168.225.2 true
172676 admin 0 UI 13/12/2013 03:24:14.124 lsprincipaldata1 192.168.225.2 false
172677 admin 0 CLI 13/12/2013 03:24:26.578 lsdiskpooldatamdiskgrpLIKE'act_ded% 192.168.225.2 false
172678 admin 0 CLI 13/12/2013 03:24:28.469 lsdiskpooldatamdiskgrpLIKE'act_pri% 192.168.225.2 false
172679 admin 0 UI 13/12/2013 03:24:18.737 lsdiskpooldatamdiskgrpLIKE'act_per% 192.168.225.2 false
172680 admin 0 UI 13/12/2013 03:24:19.037 lsdiskpooldatamdiskgrpLIKE'act_ded% 192.168.225.2 false
172681 admin 0 UI 13/12/2013 03:24:24.579 appgroupingregular 192.168.225.2 false
172682 admin 0 UI 13/12/2013 03:24:25.384 appgroupingremote 192.168.225.2 false
172683 admin 0 UI 13/12/2013 03:24:25.900 appgroupingorphan 192.168.225.2 false
```

Actifio Secure Connectivity and Data Movement with iSCSI in the Public Cloud

When Actifio Connector is deployed in the public cloud, iSCSI is utilized to transfer data between instances and the Actifio Appliance(s). Actifio establishes in-depth secure data transfer at multiple levels to ensure that no Connector-equipped Host or Appliance can access unauthorized data.

Actifio recommends that both the appliance(s) and instances communicate over the provider's private network, using non-routable IP addresses. Under these conditions, the traffic will be protected by the provider's software-defined network and subject to all of the protections and external accreditations (e.g. SOC2 and ISO27001) most public cloud providers offer.

Actifio also recommends:

- Firewall rules at the Public Cloud level that restrict iSCSI and/or control channel communication (5106/tcp) between the authorized appliance(s) to authorized instances only.
- Enable bi-directional iSCSI authentication (CHAP) utilizing pre-shared secrets that must be known to both the appliance(s) and the authorized instances before any data can be accessed.
- Install the appliance(s) certificate(s) in the Connector's trusted certificate directory on each instance.
- Some providers automatically encrypt all data at-rest (e.g. Google Cloud). On public clouds where such encryption is optional (e.g. EBS encryption on Amazon Web Services), it should be enabled to protect the appliance(s) virtual disks.

When properly configured, multiple levels of cryptographic authentication and security protect both the control and data movement channels. Additionally, only instances that have been pre-registered with the appliance(s) will be able to access data. All data operations are subject to the appliance(s) Role Based Access Control (RBAC) that validate that a user is authorized to perform a certain operation, with certain data, on a specific instance or host.

Data Encryption

Encryption In Flight

Data inflight traveling between Actifio Appliances and to OnVault, as well as SecureConnect remote support sessions, is encrypted in flight using AES-256 with session keys exchanged via Diffie-Hellman.

Management (GUI or CLI) sessions are protected utilizing the highest cipher negotiated between the client computer and the Actifio Appliancee.

Data traveling between Actifio and VMware environments is protected using the strongest cipher negotiated between the Actifio Appliance and VMware ESXi/vCenter hosts up to and including AES-256.

For hosts protected out-of-band using the Actifio Connector, the control channel between the appliance and the host is encrypted utilizing TLS and strongest cipher negotiated between the host and the appliance, however data movement occurs over iSCSI, which is not encrypted. If sensitive data is being transmitted via this mechanism it is recommended that this traffic be isolated to a given VLAN or subnet, or configured to use Fibre Channel, so that it cannot be intercepted. Traffic between an appliance and a host over iSCSI is not encrypted in flight.

Encryption At Rest

Administrative end-user credentials are hashed with a strong one-way salted SHA256 hash in the appliance database. Credentials used by the appliance to access other systems (vCenters, databases, etc) are stored in an AES256 encrypted form.

Sky Appliances encrypt customer data (snapshots and dedup) utilizing AES 256-bit encryption. Actifio CDS Appliances and CDX Appliances rely on optional encryption at the hardware layer through the use of Self Encrypting Drives (SED)-containing storage arrays. Internal system drives on CDS Appliances, including optional SSD cache, do not store customer data.

Note: *Actifio CDX Appliances have a heartbeat connection between the two nodes. This connection is not encrypted.*

Command Line (CLI) Access to Actifio VDP

Following the security principle of separation of duties, Actifio uses two command line (CLI) interfaces for customer end-users and Actifio support personnel. These are described in detail below.

User CLI Access

One CLI interface is for general user access and is only accessible by users defined in the Actifio Appliance. This is accessible via an SSH based login via port 22 on either the primary cluster IP address or node IP addresses. All CLI access is via key based authentication only. This avoids the threat of brute force password attacks and social engineering of password theft.

A user must generate an SSH public key, and that public key must be installed on the user's account by an administrator before CLI access is granted.

The User CLI login allows authenticated users access to a heavily restricted shell where only Actifio-specific commands are available to be run. The full list of commands is documented in the Actifio Documentation Library available from the Actifio Resource Center on each Actifio Appliance (http://<cluster-IP>). Users (including admin) have no ability to upload and execute arbitrary binaries, nor can users escape the restricted shell to escalate their privileges.

Support CLI Access

The second CLI interface is for use by Actifio Support only. The time and system-limited login certificates required to use this service can only be acquired via a secure portal. The username of the user who generated the SSH certificate is embedded within the certificate and all actions are audited with this information allowing all activity to be positively tied to a specific individual.

Any employee granted authorization to generate these access certificates is subject to rigorous scrutiny including a background check for every individual.

The nature of this access mechanism means it's both very secure and fully traceable making it easy to identify which individuals have logged in using the support credentials and what actions they have performed.

Console CLI Access

Access to the Actifio CLI is also available the console on the Actifio Appliance. Use of this is restricted to Actifio staff who can leverage the key based login approach described above with the key loaded on a USB stick to gain a support login to the system.

Vulnerabilities with Actifio VDP

Actifio Engineering routinely monitors multiple sources for vulnerability information and makes available to all customers hotfixes to mitigate any discovered vulnerability in a component utilized by the appliance:

- Common Vulnerabilities and Exposures
- Security Focus - Vulnerabilities Search - http://www.securityfocus.com/bid
- National Vulnerabilities Database (NVD).

The Actifio Connector

The Actifio Connector is a highly optimized service that runs as root (or the system account on Windows) that accepts connections from Actifio Appliances (CDS/CDX/Sky) and performs operations on the host to support backup, mount, and restore activities.

The Actifio Connector runs with elevated privileges as it performs a significant amount of low-level system functions including manipulating the SCSI bus, manipulating the LVM subsystem (where applicable), mounting/unmounting/formating volumes, loading and managing kernel modules (when change block tracking is enabled), copying any file on the host to the backup staging volume including protected OS files, accessing the MFT (on Windows NTFS), and more. As a C/C++ program, many of these operations are performed via native system calls and functions.

Because Actifio recognizes the risk of running any process as root, a significant amount of security architecture exists. The Connector utilizes statically linked libraries, it can validate with 2048-bit RSA certificates the identity of any Appliance that connects to it and reject any untrusted connections, and it has built-in "sudo"-like functionality to downgrade its privileges to other user accounts when it runs user-specified scripts or interacts with databases such as Oracle.

Classified as a backup agent by most companies, the Connector has been deployed across tens of thousands of customer systems in highly secure and regulated environments such as global financial institutions and banks, airlines, health care, and government agencies.