



CATE Backup and Storage Engineering
CATE Database Engineering
Citigroup Architecture & Technology Engineering

Actifio CDS 6.1

CBSE-15034-SG

Solutions Guide

Version 0.6

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

1 Version Control

Version	Date	Author	Reviewed	Comments
0.5	15 th October 2015	Simon Davey		Initial version; Headings only
0.6	22 nd December 2015	Simon Davey	Elizabeth Abraham	RFT

2 Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Arc Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

3 Contact

Please address any comments or questions regarding the information contained in this document via email to the [*GT Global Distributed Backup Engineering](#) distribution list.

4 Latest Versions

It is recommended that the latest version of the document be used from the CATE Storage Engineering website <http://catecollaboration.citigroup.net/domains/platstor/gdse/products/default.aspx>. Newer versions may include certification on additional platforms, or comments on issues discovered after deployment.

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

5 Regional Reviewers

The purpose of this section is to list all the stakeholders who reviewed this document during the Release for Testing process.

Region	Reviewed by
Asia Pacific	-
EMEA	-
Japan	-
Latin America / Mexico	-
North America	-

6 Table of Contents

1	Version Control.....	2
2	Legal Notice	2
3	Contact	2
4	Latest Versions.....	2
5	Regional Reviewers	3
6	Table of Contents	4
7	Introduction	5
7.1	Scope	5
7.2	Applicable Environments	5
7.3	References.....	5
8	Architecture	5
9	Installation Overview	7
9.1	Actifio CDS Sizing Guidelines	7
9.2	Appliance Installation Overview	7
9.3	Oracle Server Preparation	9
10	Appliance Physical Requirements	11
11	Configuration Guidelines	13
11.1	Appliance Configuration Checklist.....	13
11.2	Add User Interface Certificates	14
11.3	Add Active Directory Certificates	21
11.4	Configure LDAP/AD User Authentication	22
11.5	Add Administrators	26
11.6	Configure AD Group to Role Mappings.....	28
11.7	Configure Command Line Access	28
11.8	Configure Notifications	32
12	Appliance Operations	34
12.1	Create Organizational Units.....	34
12.2	Create Policy Templates	35
12.3	Create Resource Profiles	36
12.4	Create Hosts	36
12.5	Discover Host Applications	37
12.6	Adding Storage.....	39
12.7	Monitoring Overview	41
13	Oracle Operations.....	41
14	Appendix A.....	41
14.1	Actifio GUI.....	41
14.2	Actifio CLI	42

7 Introduction

The Actifio CDS (Copy Data Storage) product is a solution designed to enable the fast creation and access of application data copies. It is a data storage management product that provides efficient management of copies of data from database products and other data centric solutions. It can also provide file system protection. The product is provided in an appliance form factor. The appliance comprises two nodes configured in an HA configuration.

7.1 Scope

The Actifio product for Citi is positioned to provide data protection and access for short term copies of data. Typically the expected lifecycle of the data is up to thirty days. Data retention requirements for longer than this will need to use other existing technologies in Citi.

7.2 Applicable Environments

The first release of Actifio in Citi is restricted to the OraaS environment. Later releases will also provide protection for other environments. Suitable candidates for Actifio storage are databases that are in a fast development cycle and require frequent access to previous instances of the data set in order to develop the supported product or resolve problems. Other databases that have similar requirement to re-play batches or refresh UAT environment would also benefit from Actifio.

The Citi OraaS environment will access the Actifio storage through the iSCSI storage network.

7.3 References

Actifio vendor site: <http://www.actifio.com/>
CATE Actifio site: [Actifio CDS 1.6](#)
CATE OraaS site: [Citi OraaS](#)
CATE Oracle site: [Citi Oracle](#)
CATE iSCSI on RHEL: [SANgria 2.0](#)

8 Architecture

The Actifio CDS product is a specialist copy data management solution. This means that it is optimized to provide fast and efficient access to copies of data for certain data centric applications. For Citi, the Oracle application was in scope for this evaluation.

Actifio works by providing storage to a server to be used for writing copies of application data which are then managed by the Actifio Appliance. These copies are made available to hosts that need access to them so the administrators can go back in time and select the required version to recover or use. The data is accessed from the Oracle host via fibre channel or iSCSI storage and is therefore theoretically as fast as the primary database storage. As new data copies are created, and based on retention rules, older data is processed through a deduplication engine, to reduce its size.

In addition to the improvements to the traditional backup and recovery scenario, the copies created through this technology can also be used to quickly provision new environments, based on the Actifio snapshots. Because those copies will only require storage for the new or changed blocks, and not the original database footprint, the amount of storage required is reduced dramatically. This cloning capability allows the creation of new copies very quickly, regardless of the database size, which represents a big improvement over the traditional approach, which can take several hours or even days in some environments.

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

The following diagram shows at a high level the component interaction between a physical server and an Actifio Appliance. The grey arrows show the usable data storage allocated to the physical host and the Actifio Appliance from the EMC/Hitachi storage arrays. The blue arrows show the path taken when backing up or protecting data from the physical host to the Appliance. Multiple copies/deltas of this data can be taken. The first copy is always a complete block for block copy, and subsequent copies are just deltas that can be merged with the preceding one and the original full to make a full copy.

The storage used by the Actifio is Citi provided SAN storage and contains the data copies. The copy data is presented to the application host over the Citi iSCSI networks.

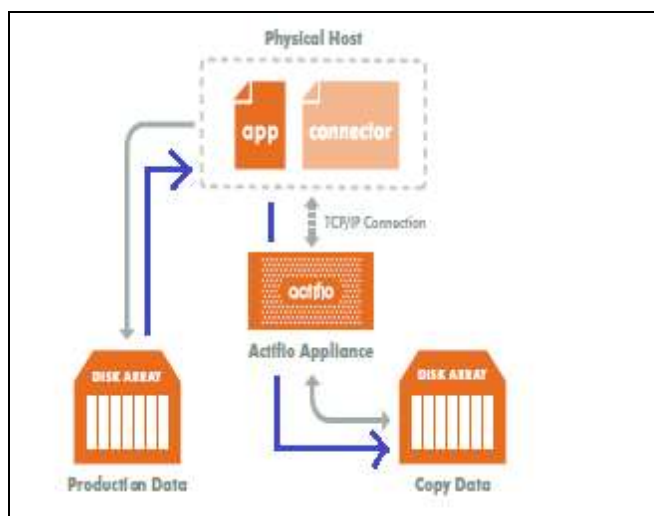


Figure 1: Data Protection Path

The Actifio CDS Appliance comes as a hardware solution in the form of a pair of 2U servers in a highly available configuration. The model is the **M4** series. There is no data storage by the M4 so this will have to be provisioned from the Citi SAN.

The following diagram shows how multiple copies are kept of the application (e.g. Oracle) data image. All applications require a full base copy to be created from which additional snapshot can reference.

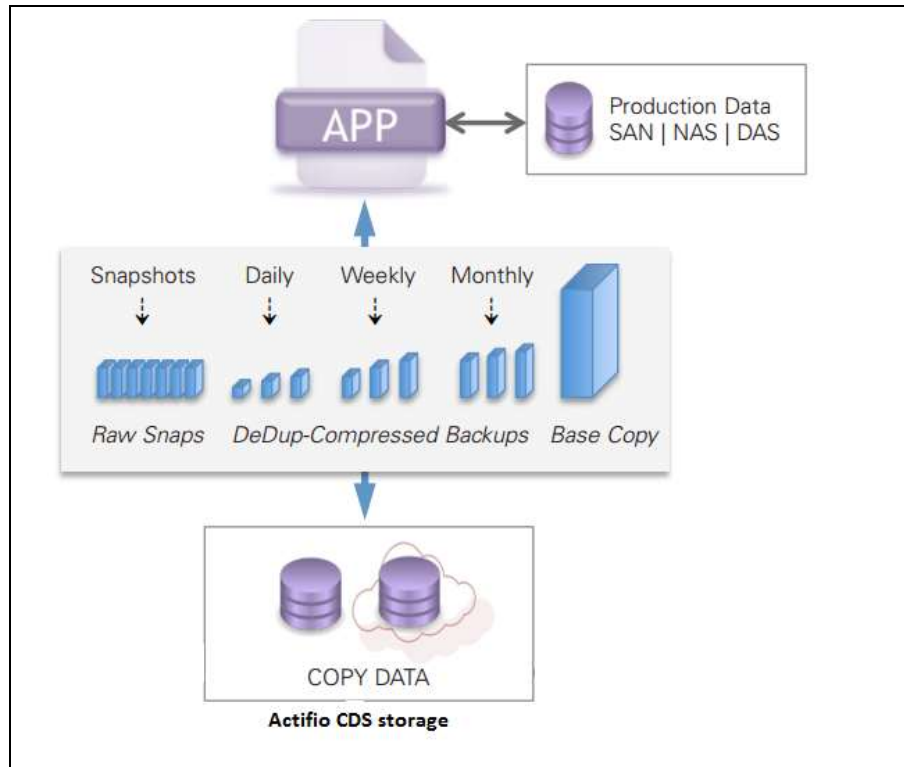


Figure 2: Data Copies

The number of data copies retained will depend on the nature of the databases protected.

9 Installation Overview

Review the following sections and plan the work accordingly.

9.1 Actifio CDS Sizing Guidelines

This release of Actifio CDS at Citi uses SAN bronze level storage to store the data copies. The sizing of this storage is dependent on the following factors:

- Size of database to be protected
- Number of copies retained
- Change rate of the database

A high level sizing guide is to provision four to five times the original data set size on the Actifio Appliance. This factor is still subject to change during the **RFT** period.

9.2 Appliance Installation Overview

The following steps detailed in the table below need to be planned before installing and configuring the Actifio **M4** Appliance. The initial configuration and installation of the Appliance will be done by the vendor, so arrangement must be made for them to access the Citi site for the physical work and then via WebEx for the further preparation before handing over the Citi.

Task	Detail	Implementation
Physical installation request	Raise request to the relevant data centre team. The space and power information is provided in section 10. The M4 unit will need	Data centre site management to allocate rack space and power cabling in

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

	to be in a location where both SAN fibre channel and iSCSI network connectivity is available. Also, the SAN storage array may need to be different to the Actifio client SAN arrays for resilience.	the appropriate location. The hardware must
Raise change for physical install of M4 appliance pair.	It is required in some data centres that the hardware is pre-configured and tested in a local staging room prior to physical installation in production racks. Once the location is confirmed, the network and fibre channel cabling requests can be raised.	Data centre site management will advise on the installation procedure to the Appliance for the local data centre. The vendor will have to be present to ensure the Appliance is functional and that the batteries are fully charged. They will also have to ensure the batteries do not discharge during before the final configuration in the production rack. The fibre channel WWPNs will also be recorded at this time and passed to Citi.
Network cabling request	Raise the request/workflow for the required network cabling. Typically this will be 8 cables total with 10 IP address. See table x in Section 10. This will need to be done prior to the date of the Appliance installation into the production racks.	Data centre cabling team to provision cables once the units are installed in the production racks
Fibre channel cabling request	Raise the request/workflow for the required fibre channel cabling. This will be for 8 cables in total. See table x in Section 10. This will need to be done prior to the date of the Appliance installation into the production racks.	Data centre cabling team to provision cables once the units are installed in the production racks
Confirm production rack installation date and arrange for Actifio engineer to attend site.	The M4 units will be installed in the required racks and powered on.	The Actifio engineer will be present to ensure the network connections are plugged into the correct ports in order to bring the Appliance on to the Citi network. After this has been completed successfully, the rest of the configuration and testing can be done remotely.
Raise fibre channel zoning request to storage team.	On each M4 node, there are two FC connections to each SAN fabric as shown Figure x in Section 10. In addition to this, the ports on each node need to be zoned together across the associated fabrics. This is to enable the M4 cluster to 'heartbeat' over the fibre channel.	Citi storage team to implement request and verify M4 initiators are visible on the fabric. The Actifio engineer with verify this over Webex with the Citi integration team.
Raise a storage allocation request to the storage team.	Both M4 nodes need to have the same storage provisioned from the SAN. For data storage, this will usually be in 1.2TB luns, up to the licensed storage limit. In additions to this, two smaller quorum luns of 20GB	Citi storage team to implement request and verify M4 SAN storage groups are present. The Actifio engineer with verify this over Webex

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

	minimum need to be allocated. This is for the cluster functionality.	with the Citi integration team.
Arrange with Actifio to complete the build and cluster installation.	Arrange a WebEx with the vendor who will log in to the Appliance and complete this task.	Actifio to verify the zoning and to configure the cluster. The Actifio software will also need to be updated as required. Licenses will also be added.
Arrange with Actifio to configure the two iSCSI network connections on the Citi storage IP network	Arrange a WebEx with the vendor who will log into the Appliance and complete this task.	Actifio to configure the network connections and the required routes. This also includes some local scripting to enable the networks to recover correctly from link failures.
Verify that the cluster host names are added/updated in Aperture (or the current datacenter inventory system)	As of version 0.6 of this document, the host names of data centre installed units (servers, appliances etc.) are created in TCRS and then flow into Aperture. This must complete before the Appliance can be fully configured.	Check Aperture for the correct information. Contact support if not present.
Add storage to the Appliance for data use	The initial storage configuration on the Appliance should be done by the vendor. Arrange a WebEx with Actifio for the vendor to complete this	Actifio will add the Citi SAN luns to the Appliance and create the storage pools as required.

Table 1: Actifio Installation Overview

The Actifio M4 Appliance is maintained by the vendor and Citi staff do not have root access to do the initial configuration. All the tasks listed above should be completed with the help of Actifio.

Further Citi specific configuration is detailed in section **11**.

9.3 Oracle Server Preparation

For the first release of Actifio at Citi, data protection is only offered to Oracle 11g databases in the OraaS environment. This environment should be running RHEL 6.4 or greater and also have the SANgria 2.0 SAN stack installed. For details, see the following document:

[SANgria 2.0](#)

Each server in the OraaS environment should have two 10GigE network connections to the Citi storage network. These should be configured using standard networking commands and routes to the Appliance networks configured. This will have to be done after the Appliance installation has been completed.

The following shows how one of the two 10GigE interfaces is configured on a RHEL server. The static route is detailed in the route-eth3 file as shown

```
[guest@oraas-sw-tp6 network-scripts]$
[guest@oraas-sw-tp6 network-scripts]$ pwd
/etc/sysconfig/network-scripts
[guest@oraas-sw-tp6 network-scripts]$
[guest@oraas-sw-tp6 network-scripts]$ ifconfig eth3
eth3      Link encap:Ethernet  HWaddr 00:50:56:9A:4D:52
          inet addr:10.124.64.58  Bcast:10.124.64.63  Mask:255.255.255.192
          UP BROADCAST RUNNING MULTICAST  MTU:8800  Metric:1
          RX packets:7819528 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19101756 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

```
RX bytes:2052884130 (1.9 GiB) TX bytes:52736338947 (49.1 GiB)
```

```
[guest@oraas-sw-tpp6 network-scripts]$  
[guest@oraas-sw-tpp6 network-scripts]$ cat ifcfg-eth3  
DEVICE=eth3  
BOOTPROTO=static  
IPADDR=10.124.64.58  
NETMASK=255.255.255.192  
MTU=8800  
NM_CONTROLLED=yes  
ONBOOT=yes  
TYPE=Ethernet  
[guest@oraas-sw-tpp6 network-scripts]$  
[guest@oraas-sw-tpp6 network-scripts]$ cat route-eth3  
10.124.95.192/26 via 10.124.64.1  
[guest@oraas-sw-tpp6 network-scripts]$
```

The following shows the complete routes

```
[guest@oraas-sw-tpp6 /]$ netstat -r  
Kernel IP routing table  
Destination Gateway Genmask Flags MSS window irtt Iface  
192.168.4.0 * 255.255.255.248 U 0 0 0 eth2  
192.168.3.0 * 255.255.255.248 U 0 0 0 eth1  
10.124.31.192 10.124.0.1 255.255.255.192 UG 0 0 0 eth4  
10.52.32.64 * 255.255.255.192 U 0 0 0 eth0  
10.124.64.0 * 255.255.255.192 U 0 0 0 eth3  
10.124.95.192 10.124.64.1 255.255.255.192 UG 0 0 0 eth3  
10.124.0.0 * 255.255.255.192 U 0 0 0 eth4  
169.254.128.0 * 255.255.128.0 U 0 0 0 eth2  
link-local * 255.255.128.0 U 0 0 0 eth1  
default 10.52.32.65 0.0.0.0 UG 0 0 0 eth0  
[guest@oraas-sw-tpp6 /]$
```

Where the Appliance destination networks are the 10.124.31.192 and 10.124.95.192 subnets shown above.

Following this, the Actifio connector needs to be installed on the RHEL server via the DMA infrastructure. The connector is the Actifio agent. Then the server can be added to the appliance and the iSCSI storage can be discovered. This will have to be done after the configuration work in section 11 has been completed.

The following example shows the storage discovery procedure. Note that there will only be one iSCSI target listed per node, even if there are two or more paths to the storage.

```
[IDENbuild root @ oraas-sw-tpp6 ~]  
# iscsiadm -m discoverydb -t sendtargets -p 10.124.31.250:3260 --discover -P1  
Target: iqn.1986-03.com.ibm:2145.actm4swdc0100-1-vip.actm4swdc0100  
Portal: 10.248.147.103:3260,1  
Iface Name: default  
Portal: 10.124.95.250:3260,1  
Iface Name: default  
Portal: 10.124.31.250:3260,1  
Iface Name: default  
[IDENbuild root @ oraas-sw-tpp6 ~]  
#
```

Note there are three interfaces to the storage as one route is via the virtual iSCSI network. Then print a summary of the visible targets.

```
[IDENbuild root @ oraas-sw-tpp6 ~]  
# iscsiadm -m node -P1  
Target: iqn.1986-03.com.ibm:2145.actm4swdc0100-1-vip.actm4swdc0101  
Portal: 10.124.95.251:3260,1  
Iface Name: default  
Portal: 10.124.31.251:3260,1
```

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

```

Iface Name: default
Target: iqn.1986-03.com.ibm:2145.actgtcdc01.actgtcdc0101
Portal: 168.72.71.25:3260,1
Iface Name: default
Target: iqn.1986-03.com.ibm:2145.actm4swdc0100-1-vip.actm4swdc0100
Portal: 10.248.147.103:3260,1
Iface Name: default
Portal: 10.124.95.250:3260,1
Iface Name: default
Portal: 10.124.31.250:3260,1
Iface Name: default
[IDENbuild root @ oraas-sw-tpp6 ~]
#

```

Note in the example above, there is one target for each of the nodes in the cluster (starting actm4swdc) plus a node for another Appliance used in earlier testing on this particular server.

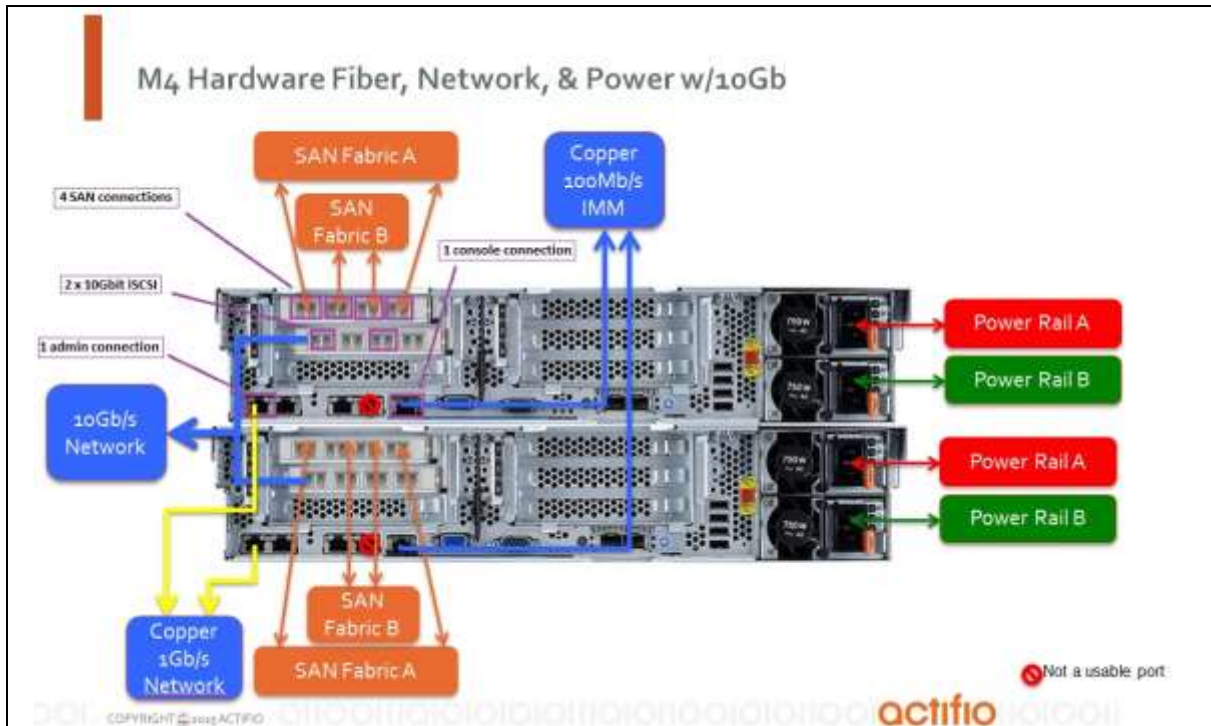
10 Appliance Physical Requirements

The following table provides the information required to allocate data centre space for the planning and installation of the M4 Appliance.

Dimension or Rating	Value
Weight	30kg max
Dimensions	Height: 86.5mm (2U) Width: 445mm Depth: 746mm
Electrical Power	100 – 240v AC 50 – 60Hz
Power	100 to 127 (nominal) VAC: 50 or 60Hz; 8.9A 200 to 240 (nominal) VAC: 50 or 60Hz; 4.5A Two power inputs for cluster node
BTU Heat Output	Maximum 3480 Btu/hour (780 watts)
Operating Temperature	5 to 40 degrees Celsius, altitude 0 – 960 m
Operating Humidity	Server on: 8 to 80%, maximum dew point 24 degrees Celsius, maximum rate of change 5 degrees Celsius per hour

Space and Power Requirements

The following graphic shows an example of the rear view of an M4 cluster complete with the interfaces required. This is taken from a vendor manual with some additional Citi mark-ups.



Actifio M4 Cluster Layout

Each M4 cluster pair will require 2 x 100Mbit interfaces and 2 x 1GigE interfaces on the corporate network (GRN) and 4 x 10GigE interfaces on the Arista storage IP network. There will be one IP address for each interface plus two additional IP addresses for shared addresses for the cluster on the 1GigE network, making a total of ten.

The suggested cluster naming conventions are as follows:

Naming Component	Vendor	Model	Location	Instance number	Node number
Example	act	m4	gtcdc	02	00
Explanation	Actifio	Cluster model	Data centre location	Starting 01	00 and 01 only

Actifio M4 Cluster Naming

The following table provides information on the network patches and IP address allocations for the M4 appliance as well as examples of the naming convention. The names are a guideline only.

Network Interface	IP addresses required	Purpose	Suggested Naming
IMM @100 100mb	2 - One per node	Hardware management and vendor installation	actm4swdc0100-imm actm4swdc0101-imm
Node Interface @ 1GigE	2 - One per node	Cluster node address	actm4swdc0100-mgt actm4swdc0101-mgt
Virtual Interfaces	1 - Cluster address	Cluster address for functional access (-vip stands for cluster virtual IP)	actm4swdc01-vip
	1 - iSCSI address	This address is required at	actm4swdc01-ci

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

		the build stage only (-ci stands for cluster iSCSI)	
iSCSI @10GigE	4 - Two per node These must be on the Arista storage network	For storage data protection traffic only. These interfaces must be on separate subnets with no bonding of failover.	actm4swdc0100-iscsi0 actm4swdc0100-iscsi1

Actifio M4 Cluster Network Connections and IP Requirement

11 Configuration Guidelines

Once the Actifio Appliance build has been completed, the copy management functional configuration and testing can be started.

11.1 Appliance Configuration Checklist

The following table provides and overview of the tasks required.

Task	Detail	Implementation
Add web certificates from the Citi certificate authority (CA)	In order to make the Appliance a trusted host for Citi web browsers and the Adobe AIR based user interface, a customized certificate must be installed on the Appliance. The Appliance must be registered in Aperture for the certificate to be generated.	The installation must be done as the root user, and therefore a WebEx with the vendor must be arranged as the root account is not accessible to Citi staff. Details are provided belows
Add the certificates for LDAP operation	The Appliance also requires AD certificates to be installed in order to query Active Directory for user and group information.	Another WebEx must be arranged with the vendor to install the required certificates. Note that these one go into a separate certificate store.
Configure the Appliance to use LDAP.	All users must be linked to LDAP.	Use the GUI to configure and test LDAP as shown in below.
Add Appliance administrators	Add the Citi administrative users to the appliance. Use the SOE ids as they exist in AD.	Add the required users using the GUI as shown in detail below.
Configure Appliance notifications	Configure email and SNMP reporting on the Appliance. This will be used for both alerting via Service Now and informational messages.	Use the GUI to configure this as shown in detail below.
Configure command line access to the Appliance for key users	The Appliance administrators must have command line access to the Appliance to perform some operations.	Configure command line access for users as shown in detail below.
Configure Organizations	The applications (e.g. Oracle databases) that are protected by the Appliance can be organized into Organizations within the Appliance in order to separate the data access between business units and users	Create high level Organizations and then agree with the user community how to name the sub organizations within these.
Configure policies	Configure Policies on the Appliance.	The Polices govern the type

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

		and frequency of data protection. Agree with the user community what types of protection are required.
Add users	Configure the application users needed and add them to the required organizations.	Add users to the appropriate organizations and with the minimum required permissions.

The tasks in the checklist about are shown in more detail in the sections below:

11.2 Add User Interface Certificates

In order for the Actifio user interface to work without constant authentication warnings, a certificate must be installed on the Appliance cluster that has been signed by the Citi certificate authority (CA). The procedure is outlined below, note however that this example is for the development environment. For an Appliance deployed in a Citi datacenter, all the network interfaces must be in both DNS and Aperture (the current Citi inventory application).

1. Arrange a WebEx with the vendor to enable a root terminal session on the Appliance. This level of privilege is required in order to access the Java key stores.
2. Generate a certificate signing request as shown below. Note that the values shown below are just an example.

```
[09:54:35] citiact01n1:/tmp #
[09:57:03] citiact01n1:/tmp # /act/jre/bin/keytool -genkeypair -alias
warren_actifio1 -keyalg RSA -keysize 2048 -keypass actifio1 -keystore
/act/certs/.keystore
Enter keystore password: actifio1
What is your first and last name?
[Unknown]: 11b4-actifio-01-mgt3.nam.nsroot.net
What is the name of your organizational unit?
[Unknown]: 153826
What is the name of your organization?
[Unknown]: Citigroup Inc.
What is the name of your City or Locality?
[Unknown]: warren
What is the name of your State or Province?
[Unknown]: NJ
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=11b4-actifio-01-mgt3.nam.nsroot.net, OU=153826, O=Citigroup Inc.,
L=Warren, ST=NJ, C=US correct?
[no]: yes
[09:58:26] citiact01n1:/tmp #
```

List the generated CSR and output to a file.

```
[09:58:39] citiact01n1:/tmp # /act/jre/bin/keytool -list -keystore
/act/certs/.keystore
Enter keystore password: xxxxxxxx

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

tomcat, Sep 15, 2014, PrivateKeyEntry,
Certificate fingerprint (SHA1):
09:28:6F:52:09:E8:62:6C:A7:D7:4E:FC:67:BF:97:37:F0:96:F1:55
warren_actifio1, Oct 8, 2015, PrivateKeyEntry,
```

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.


```
xQHh1b9oIU8Sn+310NNGCoa9Ac30XoQnqMsJZOK3UcfoodQxHZPpa2bHm1KSCA0V1Cdt/xLIOSE9
LQkt+btjPkUZIH/o9TNOoc64zn1EnYt0TRY9qJPg5NCny8Pw+FZPdMXCAyXFn40BDdvTKwGzxMcJ
NpAnOENK0GnAukWer+WN6GJAht7kgVLLkVuxRPSC+SqDp/qVoTjVuUf1D1LSJACjqTKYsR0YmEgc
a2HSxsdjbULre8fmj95TVyDitmS2Q8pHJCUsr5z4gzym+00aq+lvxadZ7HAV8K7RfVoLiDCln1pc
/BalzuIQecjXK0dbBGlBHftZXJrzZ9fc
-----END NEW CERTIFICATE REQUEST-----
[10:16:59] citiact01n1:/tmp #
```

Record the CSR in a text file and save on the Citi network. This complete the step required via WebEX. Another WebEX will be required later.

3. Raise a Citi Marketplace (CMP) request for a certificate. Search for the following item: Venafi MS-PKI On Demand Device Certificate - 163513 - Create/Revoke Certificate.AUTO

Complete the request with the following values, note some will be updated automatically on lookup.

Field	Selection or input
CSI ID	169060
Organization Unit by Region	e.g. NA
Action	Create
Which Certificate Authority	Prod
Target Hostname	Select host from pick list. If it is not there, check that the host is linked to the CSI in Aperture
Type Required	MS CA Web Server
Port	443
Service Generated or User provided CSR	CSR
Enter CSR	Paste the CSR from the Java key store generated in step 2 above.
Generate the output in Base64	Base64
Certificate Subject Alternative Name (SAN) DNS name(s)	List all host names for the cluster separate by commas with no spaces.

4. When the CMP request has been submitted, the user will receive an automatic email from CMP containing a signed certificate. This needs to be installed on the appliance along with the relevant certificate chain. An example process is shown below, but the certificate and chain will be different in production.

The certificate chain can be downloaded as a single file from the following SharePoint site:

https://catercollaboration.citigroup.net/domains/security/isp_standards/dpstds/stdshmpgs/MicrosoftPKI.aspx

On the right hand side of this page are the latest certificate packages for the Citi environments. For production, select Production CA Certificates in PEM format. This will download a file which will need to be copied to a RHEL host. This file comprises a number of linked certificates (in a functional chain). The suggested method is to use the standard UNIX vi text editor to create discreet certificate files from the combined certificate file. Create the files as cert1.pem, cert2.pem in the reverse order in which they appear in the file, so the last certificate is cert1.pem.

The certificates will need to be added to the store as shown below. A WebEx will be required with the vendor for this step.

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

5. Create the Citi signed certificate on the Appliance by copying the contents of the email into a text file.

[illegible]

Check the certificate is readable using the openssl command on the Appliance.

```
[07:40:42] citiact01n1:/tmp #
[07:40:43] citiact01n1:/tmp # openssl x509 -in actifio1.cer -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            19:d0:96:4d:00:00:00:10:c0
        Signature Algorithm: sha1withRSAEncryption
        Issuer: DC=net, DC=nsroot, CN=Citi Internal DeviceCA Untrusted
        Validity
            Not Before: Oct  9 10:29:38 2015 GMT
            Not After : Oct  8 10:29:38 2017 GMT
        Subject: C=US, ST=NJ, L=warren, O=Citigroup Inc., OU=153826, CN=11b4-
        actifio-01-mgt3.nam.nsroot.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
```

©Citigroup Inc. 2015. All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

```

Modulus:
00:b8:f4:d3:66:01:88:80:5e:57:ac:c5:f2:3e:44:
5b:2e:ba:12:4a:38:4a:a4:bf:c1:93:8b:c5:27:fe:
1f:cc:6a:b4:53:10:d6:c4:f2:6c:d1:af:40:14:2e:
5d:1e:b2:27:94:fa:ed:f6:09:b2:87:6d:d4:69:3a:
d4:ec:18:26:aa:8a:97:09:68:e1:24:91:06:3b:cb:
4d:ff:b2:0c:07:1b:91:75:f6:00:73:25:8f:27:31:
67:a7:b7:c4:ae:88:69:85:9e:62:0b:b9:75:bf:87:
d5:d3:f1:dc:70:03:48:fb:0c:a5:93:91:80:78:99:
f6:2d:9f:91:9e:6b:74:4d:ce:43:31:f2:9e:9d:a9:
1b:e1:b9:3e:d9:20:83:28:1a:b7:bd:04:a4:13:7d:
c5:b6:f0:9f:68:72:3c:89:41:17:aa:c5:15:ea:87:
43:d7:1b:bd:5a:33:fc:55:3d:11:4e:b9:a5:aa:dc:
62:fd:54:59:bc:15:6c:65:9a:e7:bd:a9:0b:31:70:
f6:5e:93:35:92:65:cc:de:72:fd:53:1d:53:18:b5:
ba:57:20:fa:fb:d7:1c:39:25:c8:d9:01:d6:54:d2:
c6:92:19:9f:90:0a:5d:61:59:75:4e:52:b0:26:e7:
a6:f7:ce:c8:1e:40:09:77:23:60:eb:b6:47:ee:a5:
ee:2b
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
62:4D:69:19:FB:D9:25:D0:00:C2:B2:04:9A:4C:8D:52:F7:BE:F7:C2
X509v3 Authority Key Identifier:

keyid:44:D3:DF:9C:FB:0C:0F:D6:E5:E3:1F:99:FB:C0:C9:77:27:B7:BA:30

X509v3 CRL Distribution Points:

Full Name:
URI:http://certificaterevocationlist.certificates.ti.citigroup.net/PKIRoot/Citi
%20Internal%20DeviceCA%20Untrusted.crl
URI:ldap:///cn=Citi%20Internal%20DeviceCA%20Untrusted,CN=ucagtdccadpp1,CN=CDP,C
N=Public%20Key%20Services,CN=Services,CN=Configuration,DC=nsroot,DC=net?certifi
cateRevocationList?base?objectClass=cRLDistributionPoint

Authority Information Access:
CA Issuers -
URI:http://certificaterevocationlist.certificates.ti.citigroup.net/PKIRoot/Citi
%20Internal%20DeviceCA%20Untrusted.crt
CA Issuers -
URI:ldap:///cn=Citi%20Internal%20DeviceCA%20Untrusted,CN=AIA,CN=Public%20Key%20
Services,CN=Services,CN=Configuration,DC=nsroot,DC=net?CACertificate?base?objec
tClass=certificationAuthority

X509v3 Key Usage: critical
Digital Signature, Key Encipherment
1.3.6.1.4.1.311.21.7:
0-.%+.....7.....,.../.....N..B....
...[.d...
X509v3 Extended Key Usage:
TLS Web Server Authentication
1.3.6.1.4.1.311.21.10:
0.0
...+.....
S/MIME Capabilities:
.....0...+....0050...*.H..
..*.H..

X509v3 Subject Alternative Name:
DNS:11b4-actifio-01-mgt3.nam.nsroot.net
Signature Algorithm: sha1withRSAEncryption
80:53:bb:17:3c:25:94:2d:5f:b7:01:0c:04:a5:e7:35:82:b2:
02:e8:ba:e3:02:8d:a0:7e:a8:dc:e5:5e:38:0b:e5:d4:4c:ff:
e2:63:1b:a3:72:5e:c8:3b:8c:df:cb:b2:49:cf:22:50:97:23:
dc:8c:07:6b:f2:91:ed:32:94:19:d2:fb:b4:14:79:2d:c1:d3:
a1:86:b7:8d:82:3e:03:fc:53:af:39:1a:35:18:6f:21:14:20:
1c:74:85:8f:c0:79:e6:99:ef:c0:00:1c:47:0f:a1:cd:a2:eb:
ff:4b:b1:64:0d:b3:8a:6c:a4:9e:a9:dc:b7:f0:a8:5e:2b:79:
60:4e:47:9c:c2:3c:f8:93:ff:25:9f:2d:d4:8e:74:58:69:ea:
c9:73:a8:70:50:e0:5d:18:40:12:8c:ce:77:d3:11:51:23:3d:

```

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

```
d0:af:d6:9a:8d:ae:22:30:07:b1:64:5e:b7:a9:8f:39:67:f9:
f9:50:8e:94:8f:be:6c:a2:33:bb:64:01:2f:ff:b2:1e:57:ae:
9d:94:6f:57:47:9b:21:43:2a:55:57:93:77:23:d0:68:d0:59:
e4:50:0a:42:d6:70:e2:9b:76:c0:f2:8b:cc:74:4d:09:cb:1e:
99:fc:6d:f1:5d:f9:d6:7e:d7:e0:f4:8a:f7:a8:2e:dd:62:f2:
1e:b0:01:62
[07:41:21] citiact01n1:/tmp #
```

6. Create the other certificates for the Citi CA chain.

```
[08:55:58] citiact01n1:/tmp # cd devcerts/
[08:56:02] citiact01n1:/tmp/devcerts # cat > cert1.pem
-----BEGIN CERTIFICATE-----
MIIghDCCBwygAwIBAgIKF4fXhgAAAAABjANBgkqhkiG9w0BAQUFADBWMRMwEQYK
CZImiZPyLGBGRYDmV0MRQWEgYKZImiZPyLGBGRYEQ2l0aTEpMCCGA1UEAxBG
Q2l0aSBjbnRlcm5hbCBQb2xpy3lDQSBVbnRydnXN0ZWQwHhcnMTQWODEZMTU0OTE4
whcnMjAwODEZMTU0OTE4WjBjYMRMwEQYKZImiZPyLGBGRYDmV0MRYWFAFKCZIm
iZPyLGBGRYGBnNyb290MSkwYjYDVQDEYBDAXRPEludGvYbmFsIERldm1jZUNB
IFVudHJlc3RlZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL0Jdjrf
f/Q6/j5sv1clLKsjmc3x2x8jwkmnADbaEpFo4PePBgji6jy6rZYWIJTYYJNpfCrj
rYk4SxqICg5Mo+th3Fr0l4Yguxfy8cu1XL4zHpN6IDhwvXzamdMnx8QQSNPb8gm7
+GGGJa87t1+7T0CPo/QQUED/gtFvzRX8M+kGkdmQX+5mvjm2JaUrB6XLLyha/TVA
+9B2/B1Nxf++i460Jldgj1od4ln77bth7AU4eQ8ABqzzN34G/SJda1vvtEBfKG8A
bDwYXKx1JEfmxkFpbi0GdveIuzLt3zwmK66Goc9wazg8BAVn/ru0xMJ3Ys5pA2R
L9ryqiwsavi3xn8CAwEAAoCA1AwggNMA8GA1udEWEB/wQFMAMBAf8WHQYDVR00
BBYEFETT35z7DA/w5emfmfvAYXcnt7owMASGA1udDwQEAwIBhjAQBgkrBgEEAYI3
FQEEAwIBADABgkrBgEEAYI3FAIEDB4KAFMADQBiAEMAQTAfBgNVHSMEGDAwBS6
KnIrZqsJYwzd3+2Hos1imlgFNTCCAWEGA1udHwSCAVgggFUMIIBUKCCAuygggFI
hnFodHRwOi8vY2VydG1maWNhdGvYXZvY2F0aw9ubG1zdC5jZXJ0awZpy2F0ZXMu
dGkuY2l0awdyb3VwLm5ldC9QSO1sb290L0NpdGklMjBjbnRlcm5hbCUyMFBvbG1j
eUNBjTIwVW50cnVzdGVkLmNybiAB0mxkYXA6Ly8vY249Q2l0aSUyME1udGvYbmFs
JTIwUG9sawN5Q0E1MjBvbnRydXN0ZWQsQ049dWnhZ3RkY2NhchBwMSxDTj1DRFAS
Q049UHvibG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uzmln
dXJhdGlvbiXEQz1uc3Jvb3QsREM9bmV0P2N1cnRpbm1jYXRlUmV2b2NhdGlvbkxp
c3Q/YmFzZT9vYmp1Y3RDbGFzc21jUkxeaxN0cm1idXRpb25Qb2ludDCCAVgGCCSg
AQUBFBwEBBIIBSjCCAUYwFQYIKwYBBQUHMAKGchw0dHA6Ly9jZXJ0awZpy2F0ZXJl
dm9jYXRpb25saXN0LmN1cnRpbm1jYXRlc3Q5aXN0aXN0aXN0aXN0aXN0aXN0aXN0
b3QvQ2l0aSUyME1udGvYbmFsJTIwUG9sawN5Q0E1MjBvbnRydXN0ZWQy3J0MIHE
BggrBgEFBQcwAoABT2xkYXA6Ly8vY249Q2l0aSUyME1udGvYbmFsJTIwUG9sawN5
Q0E1MjBvbnRydXN0ZWQsQ049Q2l0aSUyME1udGvYbmFsJTIwUG9sawN5Q0E1MjBv
LENOPVn1cnZpy2VzLENOPUNvbmZpZ3VyYXRpb24sREM9bnNyb290LERDPW5ldD9j
QU1cnRpbm1jYXRlc3QvQ2l0aSUyME1udGvYbmFsJTIwUG9sawN5Q0E1MjBvbnRydXN0
cm10eTANBgkqhkiG9w0BAQUFAAOCAQEAS852GgokRTpJQ9Z7y1JEcbe5Ge5RYrVC
YfQfK9M4Cj0tt9lor7CDPJZU/r9rJnnF/PALq/F5KE3ufQcaHmVubq34DQwLGT1z
wkibpJ90z7PU4Cxs6waqvwwtFwNQAONQ9tJPepB2g2d/ac1LjksY3ZthjsY20VE
255Bhk4AgMrLqgB1plovRUVcg1Tjp2GM9yvDD79MEUqv/vovUwTML+4YTYpoF9r
4+KufkklawpIIQ8HaALE1aEO6CJD9DWXKROUoSqudbo3ezuCKkMuAKaotNBX/bM3
JAFkjhRG/ktxfgzPbFj0mNsPOEGo8luwscib09vZrtD92euctSApeQ==
-----END CERTIFICATE-----
[08:56:48] citiact01n1:/tmp/devcerts #
```

And repeat this step for the other certificates required. Note there may be up to seven of these.

Check the title of the certificates, as this will be needed to create the alias when importing them into the Java key store.

```
[09:04:38] citiact01n1:/tmp/devcerts # openssl x509 -text -in cert1.pem | grep
Issuer
Issuer: DC=net, DC=Citi, CN=Citi Internal Root CA Untrusted
[09:04:47] citiact01n1:/tmp/devcerts #
```

7. Then import the certificates into the Java key store.

```
[09:06:23] citiact01n1:/tmp/devcerts # /act/jre/bin/keytool -import -alias
citiinternalrootcauntrusted -keystore /act/certs/.keystore -trustcacerts -file
cert3.pem
```

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

```

Enter keystore password:
Owner: CN=Citi Internal Root CA Untrusted, DC=Citi, DC=net
Issuer: CN=Citi Internal Root CA Untrusted, DC=Citi, DC=net
Serial number: 62e8b8c0d672d6ad4da6b6f23d524c92
Valid from: Thu Mar 20 19:16:31 EDT 2014 until: Tue Mar 20 19:26:25 EDT 2029
Certificate fingerprints:
    MD5: 51:48:7A:B3:10:4D:BE:45:08:9A:28:E3:8A:0F:52:2A
    SHA1: 5B:74:CA:A1:68:FE:9B:D5:4C:C8:DF:39:AF:50:1D:C9:E6:8C:3E:0A
    SHA256:
1A:DD:DA:22:38:B6:71:04:7F:63:20:AF:29:4E:A1:4D:E3:6C:4D:5C:87:2B:07:FC:97:D5:8
6:F3:F5:C0:3F:E8
    Signature algorithm name: SHA1withRSA
    Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 04 00 43 00 41 ...C.A

#2: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00 ...

#3: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
    CA:true
    PathLen:2147483647
]

#4: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
    Key_CertSign
    Crl_Sign
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
    keyIdentifier [
0000: 52 84 FD 42 43 CE 84 F3 75 DD 40 F2 D0 7B B1 9A R..BC...u.@.....
0010: 83 A6 6B 22 ..k"
    ]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
[09:09:34] citiact01n1:/tmp/devcerts #

```

Repeat this for all certificates in the chain. Then import the signed certificate.

```

[09:25:10] citiact01n1:/tmp # /act/jre/bin/keytool -import -alias
warren_actifio1 -keystore /act/certs/.keystore -trustcacerts -file actifio1.cer
Enter keystore password:
Certificate reply was installed in keystore
[09:26:08] citiact01n1:/tmp #

```

8. List the certificates in the Java keystore. The certificate names are highlighted. Then delete the **tomcat** certificate

```

[06:46:55] citiact01n1:/act/certs # /act/jre/bin/keytool -list -keystore
/act/certs/.keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 5 entries

citiinternaldevicecauntrusted, Oct 12, 2015, trustedCertEntry,
Certificate fingerprint (SHA1):

```

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

```

20:B6:21:27:14:E5:B9:42:F3:3A:A0:74:0E:A7:B3:F1:4E:6B:8B:6F
tomcat, Sep 15, 2014, PrivateKeyEntry,
Certificate fingerprint (SHA1):
09:28:6F:52:09:E8:62:6C:A7:D7:4E:FC:67:BF:97:37:F0:96:F1:55
citiinternalpolicycauntrusted, Oct 9, 2015, trustedCertEntry,
Certificate fingerprint (SHA1):
20:B6:21:27:14:E5:B9:42:F3:3A:A0:74:0E:A7:B3:F1:4E:6B:8B:6F
citiinternalrootcauntrusted, Oct 9, 2015, trustedCertEntry,
Certificate fingerprint (SHA1):
5B:74:CA:A1:68:FE:9B:D5:4C:C8:DF:39:AF:50:1D:C9:E6:8C:3E:0A
warren_actifio1, Oct 9, 2015, PrivateKeyEntry,
Certificate fingerprint (SHA1):
96:38:8D:68:42:8A:67:D3:C7:6E:CB:27:8B:3A:FC:8B:DF:EE:1D:A6
[06:47:18] citiact01n1:/act/certs #
[06:48:29] citiact01n1:/act/certs # /act/jre/bin/keytool -delete -alias tomcat
-keystore /act/certs/.keystore Enter keystore password:
[06:49:13] citiact01n1:/act/certs #
[06:49:15] citiact01n1:/act/certs #
[06:49:15] citiact01n1:/act/certs # /act/jre/bin/keytool -list -keystore
/act/certs/.keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 4 entries

citiinternaldevicecauntrusted, Oct 12, 2015, trustedCertEntry,
Certificate fingerprint (SHA1):
20:B6:21:27:14:E5:B9:42:F3:3A:A0:74:0E:A7:B3:F1:4E:6B:8B:6F
citiinternalpolicycauntrusted, Oct 9, 2015, trustedCertEntry,
Certificate fingerprint (SHA1):
20:B6:21:27:14:E5:B9:42:F3:3A:A0:74:0E:A7:B3:F1:4E:6B:8B:6F
citiinternalrootcauntrusted, Oct 9, 2015, trustedCertEntry,
Certificate fingerprint (SHA1):
5B:74:CA:A1:68:FE:9B:D5:4C:C8:DF:39:AF:50:1D:C9:E6:8C:3E:0A
warren_actifio1, Oct 9, 2015, PrivateKeyEntry,
Certificate fingerprint (SHA1):
96:38:8D:68:42:8A:67:D3:C7:6E:CB:27:8B:3A:FC:8B:DF:EE:1D:A6
[06:49:27] citiact01n1:/act/certs #

```

It is then necessary to restart the tomcat process on the server. This will cause the certificate store to be re-read by the tomcat web server.

```

[06:50:23] citiact01n1:/act/certs # monit restart tomcat
[06:50:40] citiact01n1:/act/certs #
[06:50:45] citiact01n1:/act/certs # monit summary
The Monit daemon 5.5.1 uptime: 20d 17h 59m

File 'node.trc.exists'           Accessible
Process 'omd'                    Running
Process 'adhd'                   Running
Process 'postgres'               Running
Process 'psrv'                   Running
Process 'tomcat'                 Running
Process 'udppm'                  Running
System 'citiact01n1'             Running
[06:50:52] citiact01n1:/act/certs #
[06:51:20] citiact01n1:/act/certs #

```

The Actifio AIR GUI should now work without constantly having to confirm the trusted identity of the server.

11.3 Add Active Directory Certificates

This process is similar to the one described in the previous section. Obtain the combined certificate file from the SharePoint and then create the individual certificates, starting from the root. Arrange a WebEx with Actifio and import the certificates. Note however, that the Java

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

keystore is different for the AD certificates. The location is shown below, after the example certificates have been imported.

```
[04:40:19] citiact01n1:/ #  
[04:40:20] citiact01n1:/ # cd /act/jre/lib/security  
[04:40:33] citiact01n1:/act/jre/lib/security #  
[04:40:35] citiact01n1:/act/jre/lib/security # /act/jre/bin/keytool -list -  
keystore cacerts | grep citi  
Enter keystore password: xxxxxxx  
citiinternaldeviceca03lab, Nov 10, 2015, trustedCertEntry,  
citiinternaldeviceca01, Nov 10, 2015, trustedCertEntry,  
citiinternaluserca03lab, Nov 10, 2015, trustedCertEntry,  
citiinternalpolicyca, Nov 10, 2015, trustedCertEntry,  
citiinternaluserca01, Nov 10, 2015, trustedCertEntry,  
citiinternaldevrootca, Nov 10, 2015, trustedCertEntry,  
[04:40:49] citiact01n1:/act/jre/lib/security #
```

After this process has completed, root access to the Appliance will no longer be required.

11.4 Configure LDAP/AD User Authentication

The Actifio Appliance can be configured to use the Citi Ac
This step can be done using the Actifio GUI as shown below.

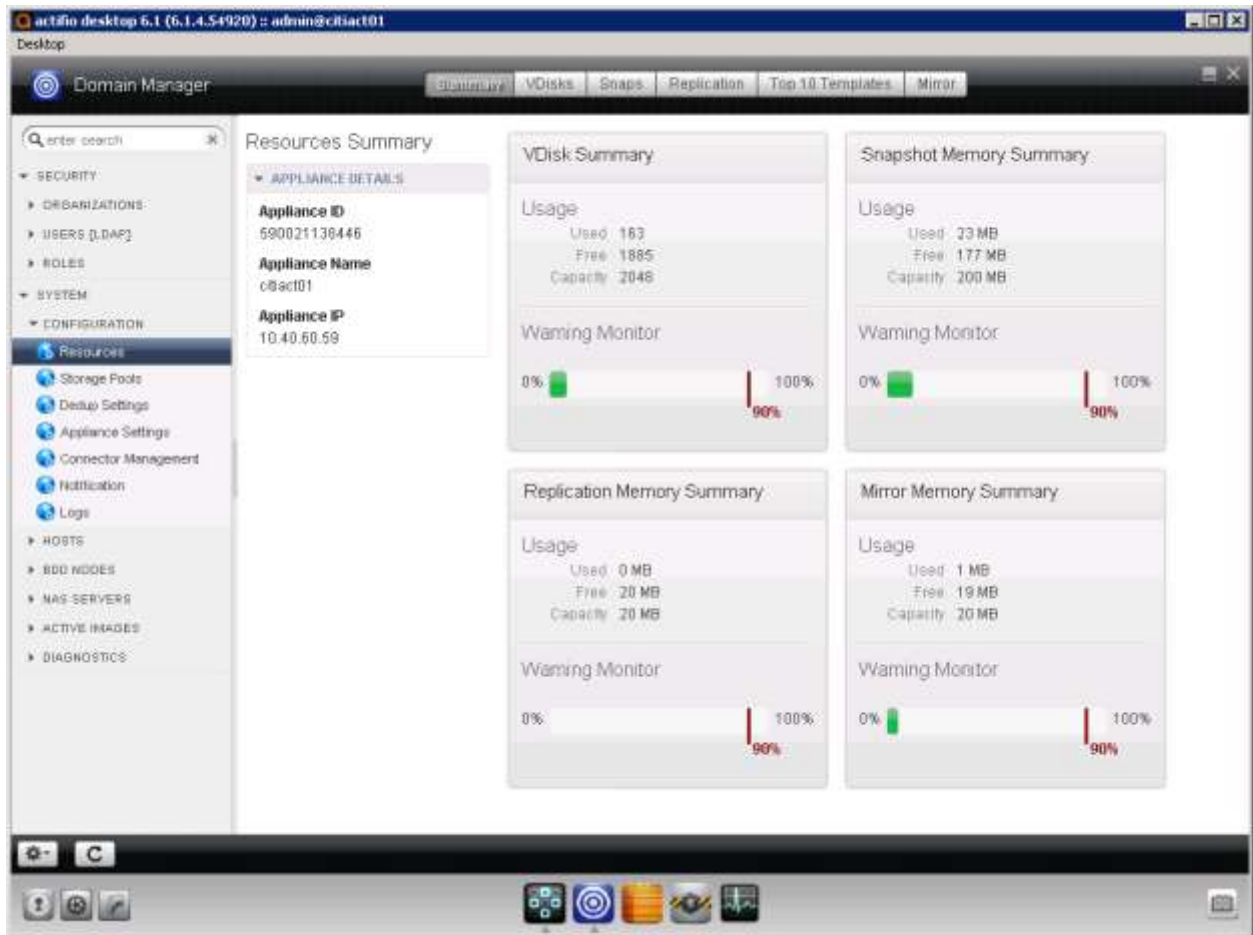
1. Open the GUI. If this is not yet installed, see Appendix B for instructions of how to do this. Go to the Domain Manager Button at the bottom of the window and click on this.



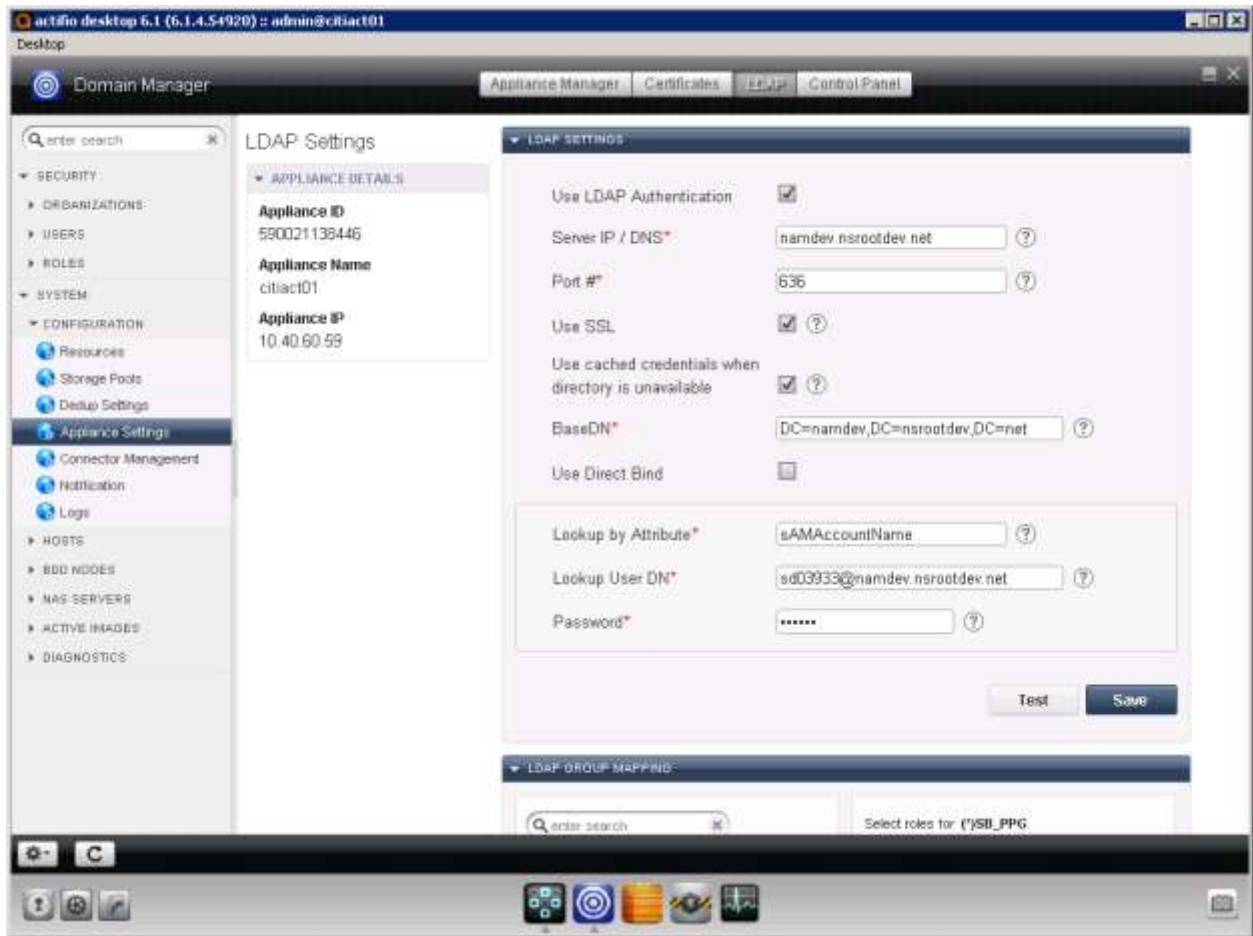
©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

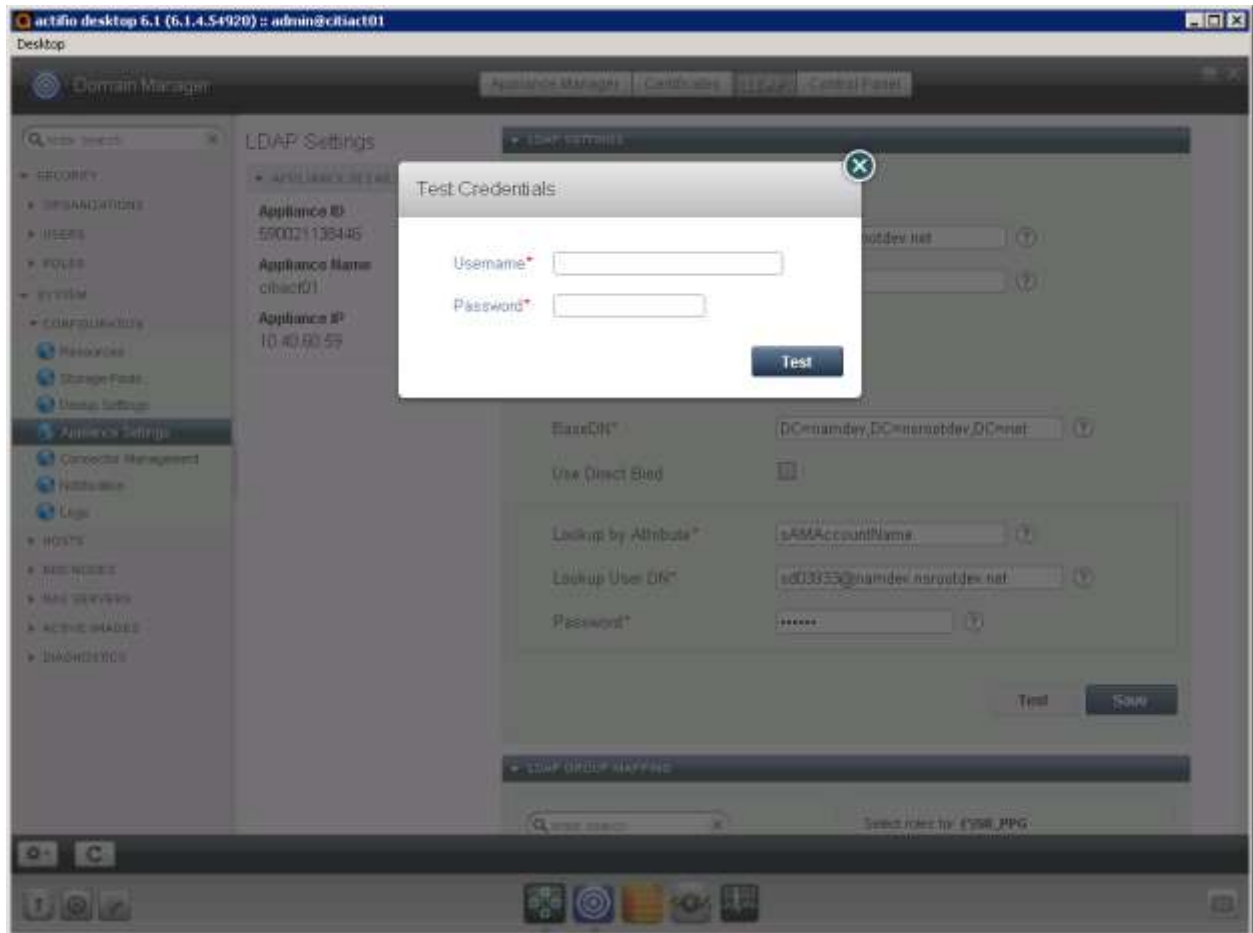
This takes you to the configuration screen shown below.



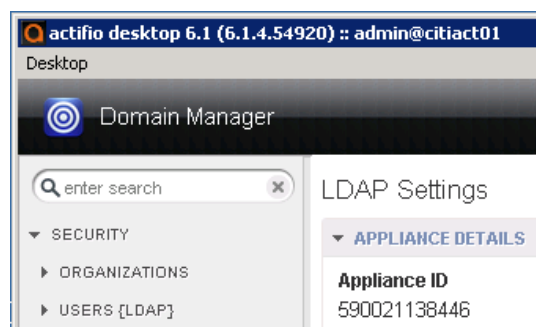
2. From the Domain Manager screen, select Configuration from the left hand pane and the Appliance Settings. Then, select the LDAP button from the top of the pane, as shown below.



3. Complete the details under the LDAP Settings as shown above. Note that this will vary between AD domains. Also note that a functional user will need to be available before this process can be done.
4. Click the Test button to verify AD connectivity. This brings up a Test Credentials window as shown below.



Enter the credentials of a user for that AD domain and hit the Test button. It is recommended that this test is performed for at least two different users in order to ensure the correct functioning of the configuration. If the tests are successful, the configuration can be saved. After this, the Users menu in the Domain Manager screen will show {LDAP} to indicated AD is now being used for all users, except the built in admin user, as show below:

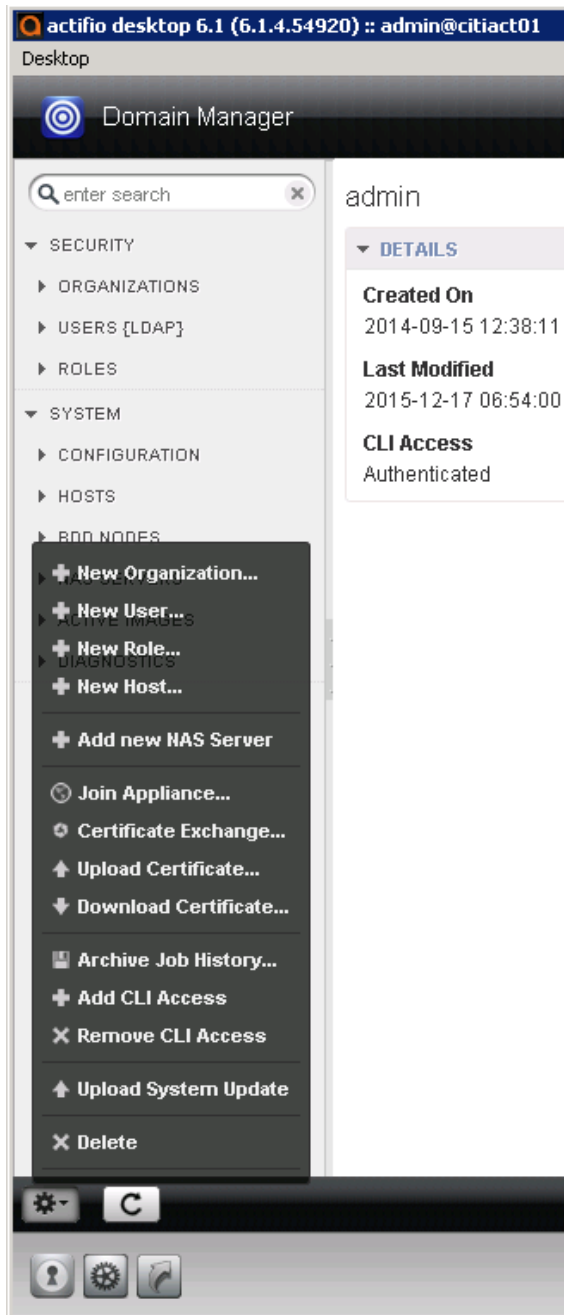


This completes the configuration. Before logging out, it is necessary to add some Administrators to the Appliance as detailed in the next section.

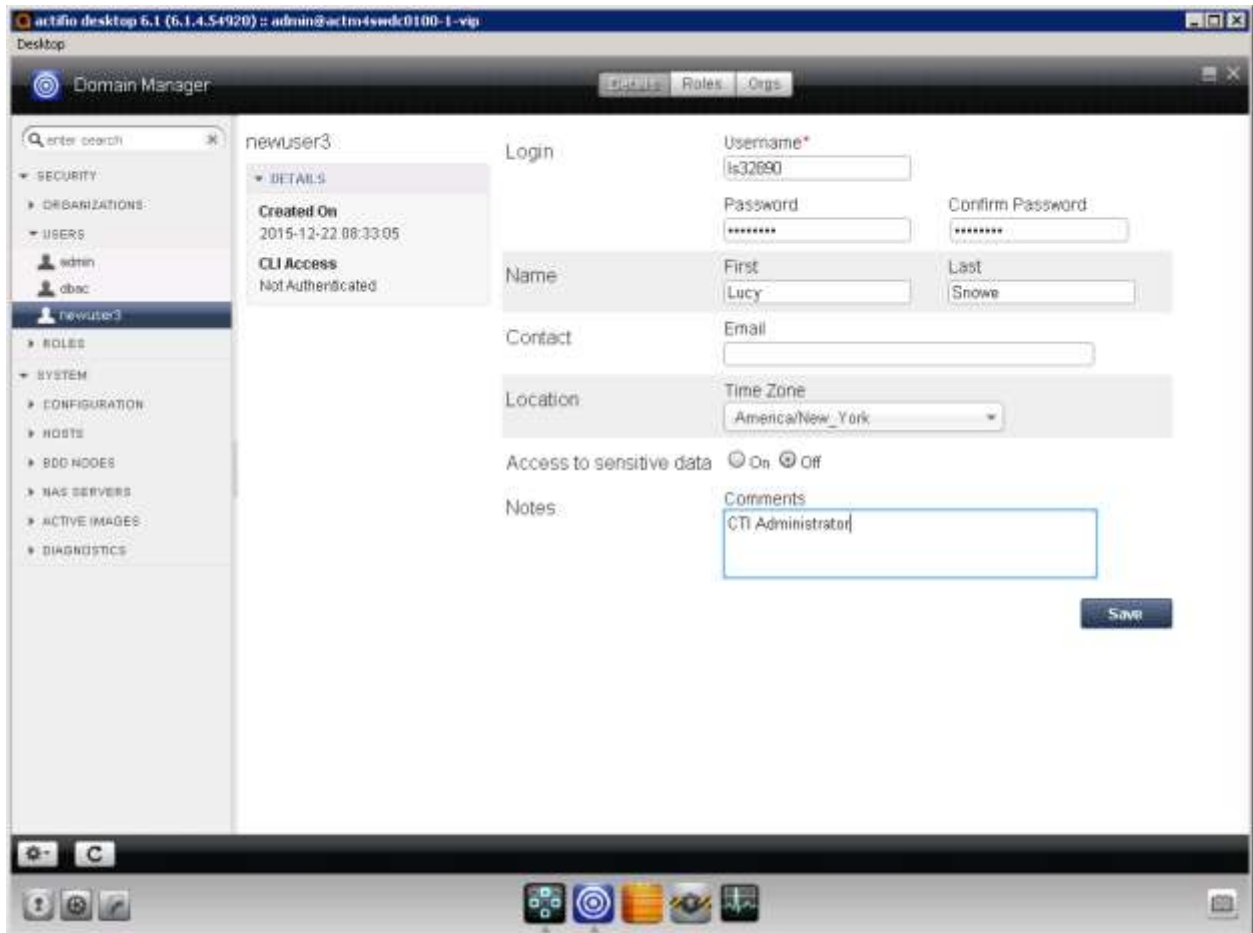
11.5 Add Administrators

Following the AD configuration above, users with Administration privileges need to be added to the environment.

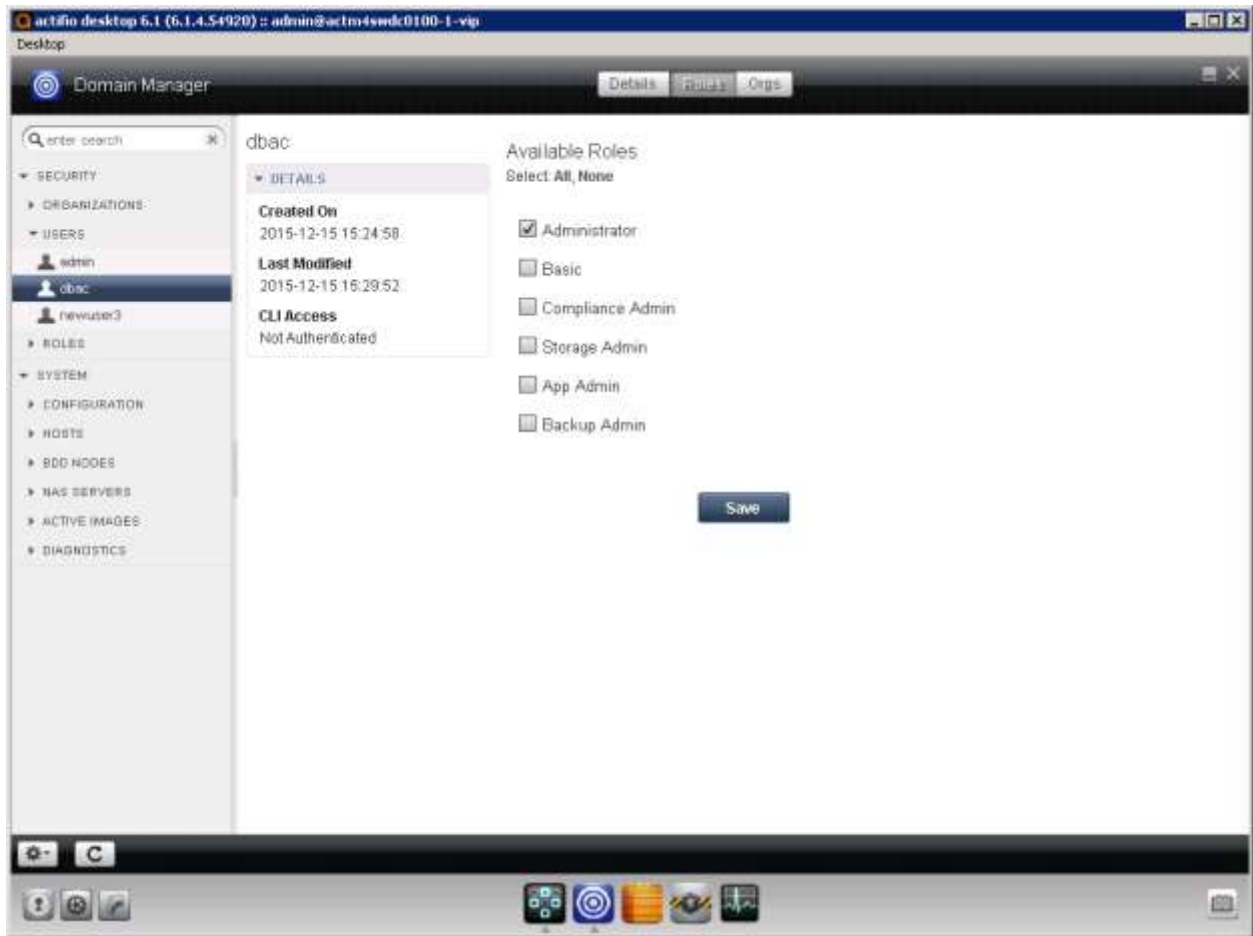
1. From the Domain Manager screen, select the New User option from the “cog wheel” menu on the bottom left as shown below:



This operation will create a new user immediately. The details need to be added as shown below



2. Edit the user details as required. The password can be left blank as AD is being used. It is good practice to put the role in the Comments box at the bottom.
3. Click on the Roles button at the top of the screen and check the Administrator role as shown below:



This completes the user addition.

11.6 Configure AD Group to Role Mappings

The feature has been tested successfully, but the Citi implementation details are still to be decided.

11.7 Configure Command Line Access

As of version **0.6** of this document, command line access is available on the Windows platform only using either Tectia or PuTTY. Note that Tectia is the Citi supported tool for ssh connectivity. The RHEL Tectia access is under investigation.

The following shows an example configuration using Tectia on Windows 2008. Note that the user must already be added to the Appliance and the account verified.

1. On Windows, open a Tectia SSH terminal and go to Tectia Connections...

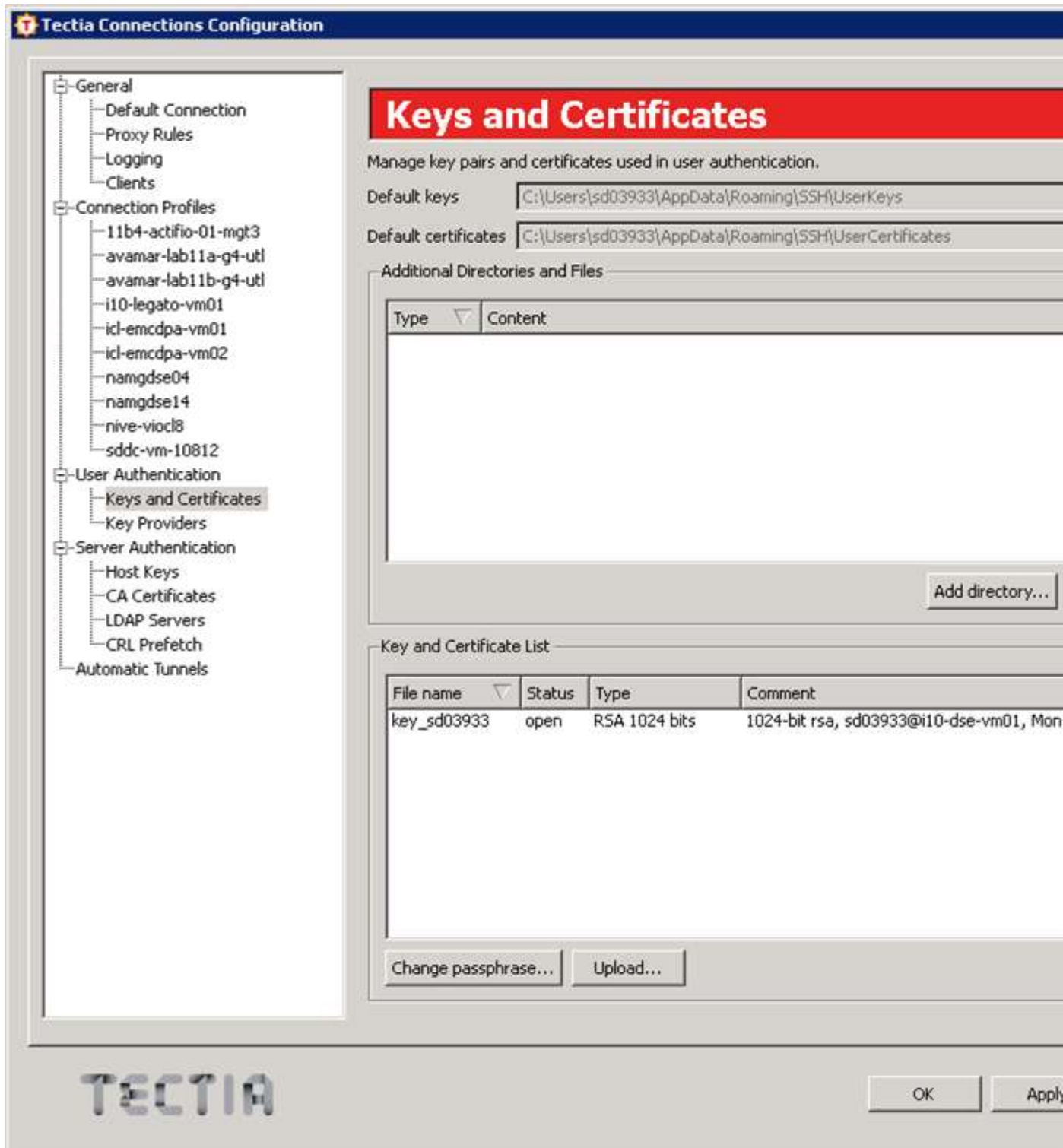
©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.



2. Then select Keys and Certificates on the left hand pane and click New key...
3. In Advanced Options select RSA/1024
Enter a passphrase (although it will work without) and hit next
Then hit Cancel

You should then see the key in the bottom pane (example below)



This key exists in the following folder in a user's home area

\users\<soeid>\appdata\roaming\ssh\userkeys

4. Copy the .pub key with a text editor (or use type at the cmd prompt on windows)

©Citigroup Inc. 2015, All Rights Reserved.

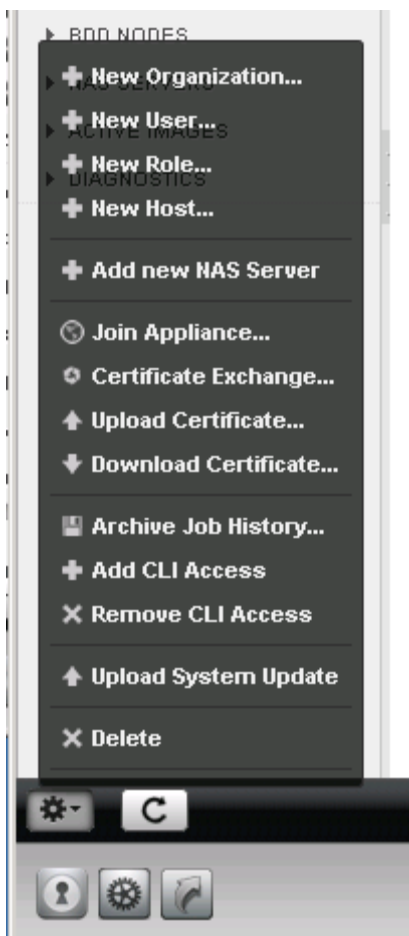
This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

5. You then need to log into the Actifio interface and go to the Domain Manager screen



Under Users on the left hand pane, find your user name and highlight it. The details should appear in the right hand pane.

6. Then click on the gear wheel at the bottom left and select Add CLI Access (as shown below)



You then need to paste you key into the window provided.

7. To test the access, open a new SSH Terminal and enter the Actifio cluster name and the user name with the default port 22. This should then bring up a terminal with the Actifio

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

command prompt. If a pass key was selected during the configuration process (step 3 above), then the user will be prompted for this before access is granted. Otherwise the user will be logged in automatically

11.8 Configure Notifications

This feature has been tested successfully, but the Citi implementation details are still to be decided. To add email notification and a trap receiver, go to the Domain Manager view and then from the left hand pane expand Configuration and select Notification

1. Under the SMTP Server tab, enter the details following the format below:

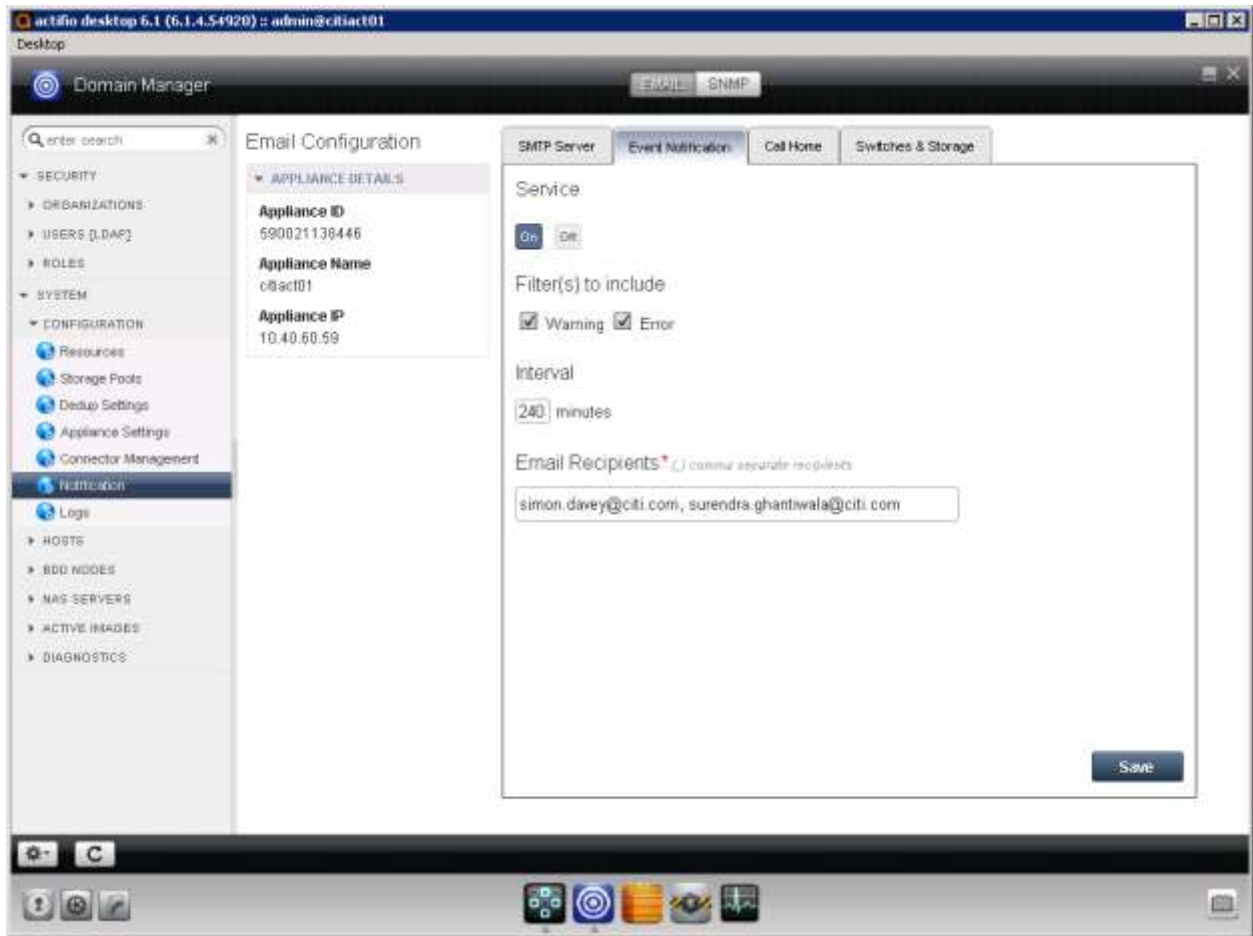
The screenshot shows the 'Domain Manager' application window. The left sidebar contains a navigation menu with categories: SECURITY, ORGANIZATIONS, USERS (LDAP), ROLES, SYSTEM, CONFIGURATION, and LOGS. Under CONFIGURATION, 'Notification' is selected. The main area is titled 'Email Configuration' and has four tabs: SMTP Server, Event Notification, Call Home, and Switches & Storage. The 'SMTP Server' tab is active, displaying the following fields:

- Server Name/IP*: mailhub-ss01.nam.nsroot.net
- Port*: 25 (with a checkbox for 'Use SSL')
- Host Name: 1b4-actio-01-mgt3@nam.nsroot.net
- Email*: lucy.snowe@citi.com
- Password: (empty field)
- Message Limit: 5 MB

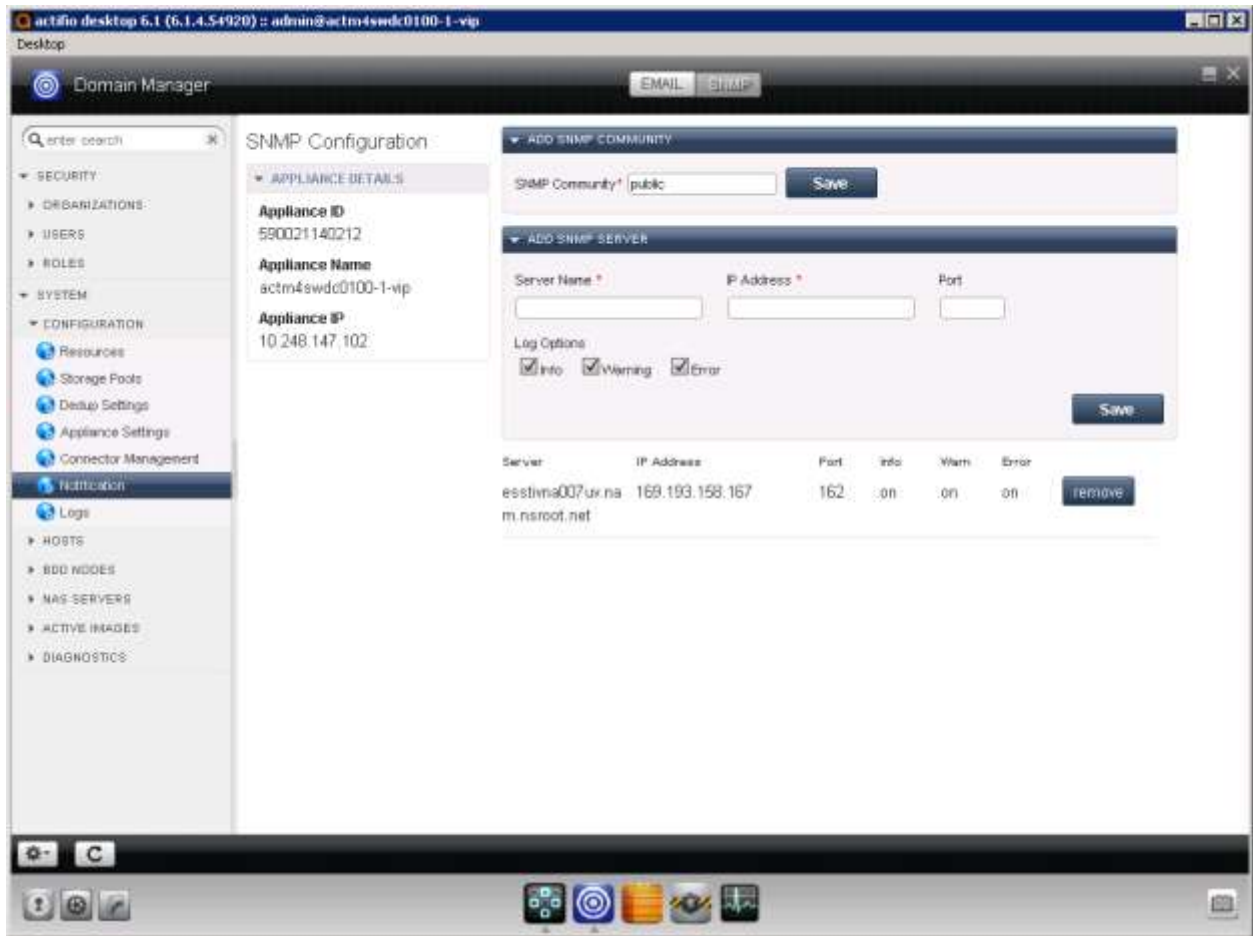
At the bottom right of the form are 'Test Email' and 'Save' buttons. The top of the window shows the user 'admin@citiact01' and the version '6.1 (6.1.4.54920)'.

Use the Test button to verify the connectivity values.

2. Under the Event Notification tab, switch the service on and set the other values shown as required.



3. To configure SNMP notifications, click on the SNMP button at the top of the window and add the details as directed by the Monitoring team. As of 0.6 of this document, this feature is working, but the Tivoli workflow is not yet completed. An example of the UAT trap received configuration is shown below

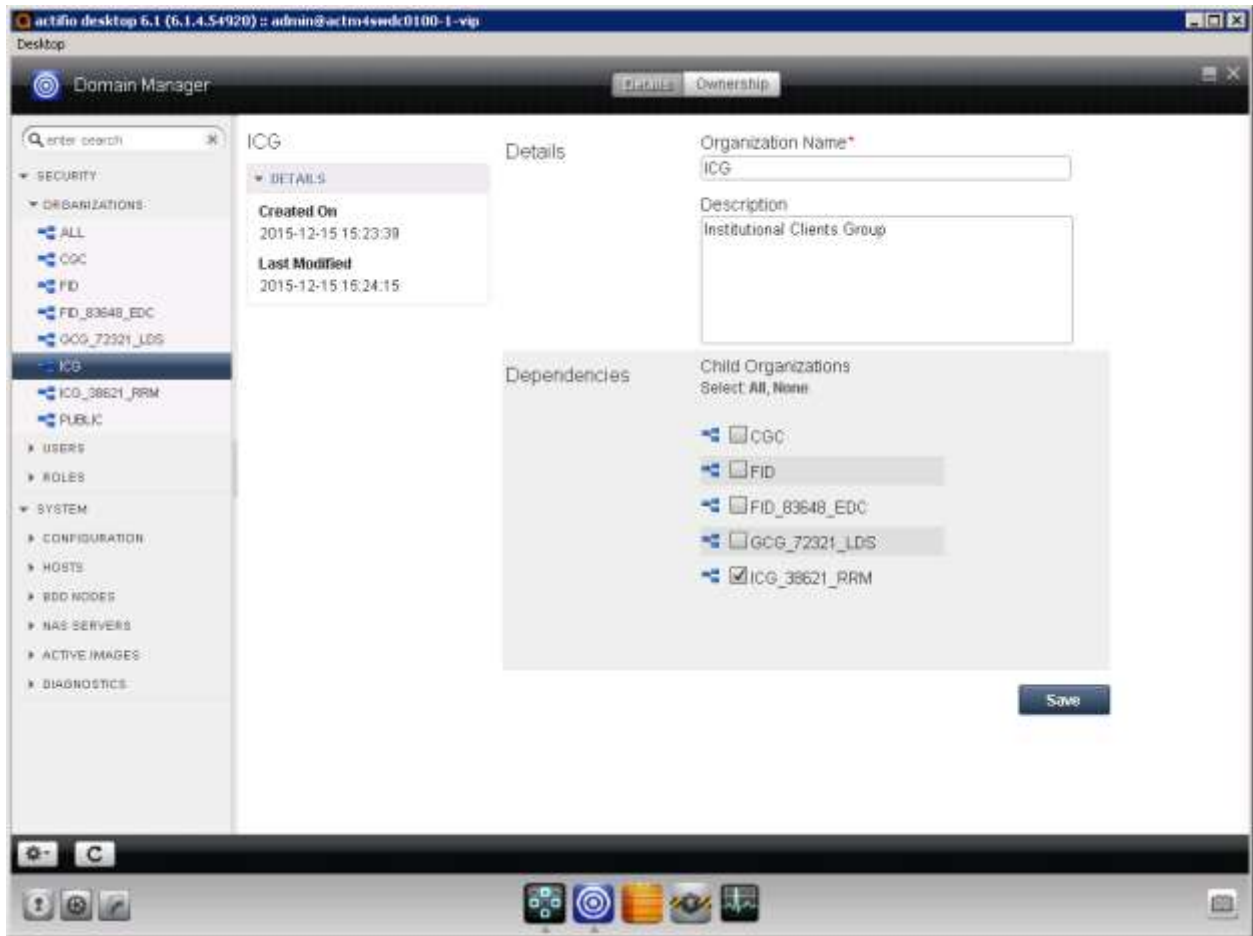


12 Appliance Operations

The following steps will need to be completed at least once on the Appliance and they may have to be repeated as the usage of the environment increases. The sections below just give an overview of what is necessary and recommended for Citi. The vendor reference manuals should be consulted for more details.

12.1 Create Organizational Units

In order to separate data access between business units and applications, Organizations must be created. These should be done in a hierarchical manner with the main Citi businesses at the top and sub businesses and applications beneath them, as shown in the following example.



Note that there is a Child Organization of ICG above. This child Organization will contain hosts and applications.

12.2 Create Policy Templates

Policy Templates are used to govern how an application on a server is protected. For example, whether the snapshots are also stored in the de-dupe pool, and how frequently application protection is performed. There are some preconfigured Templates provided. As of version **0.6** of this document, the Profile usage is not finalized.

The following shows the details of a snapshot and de-dupe policy



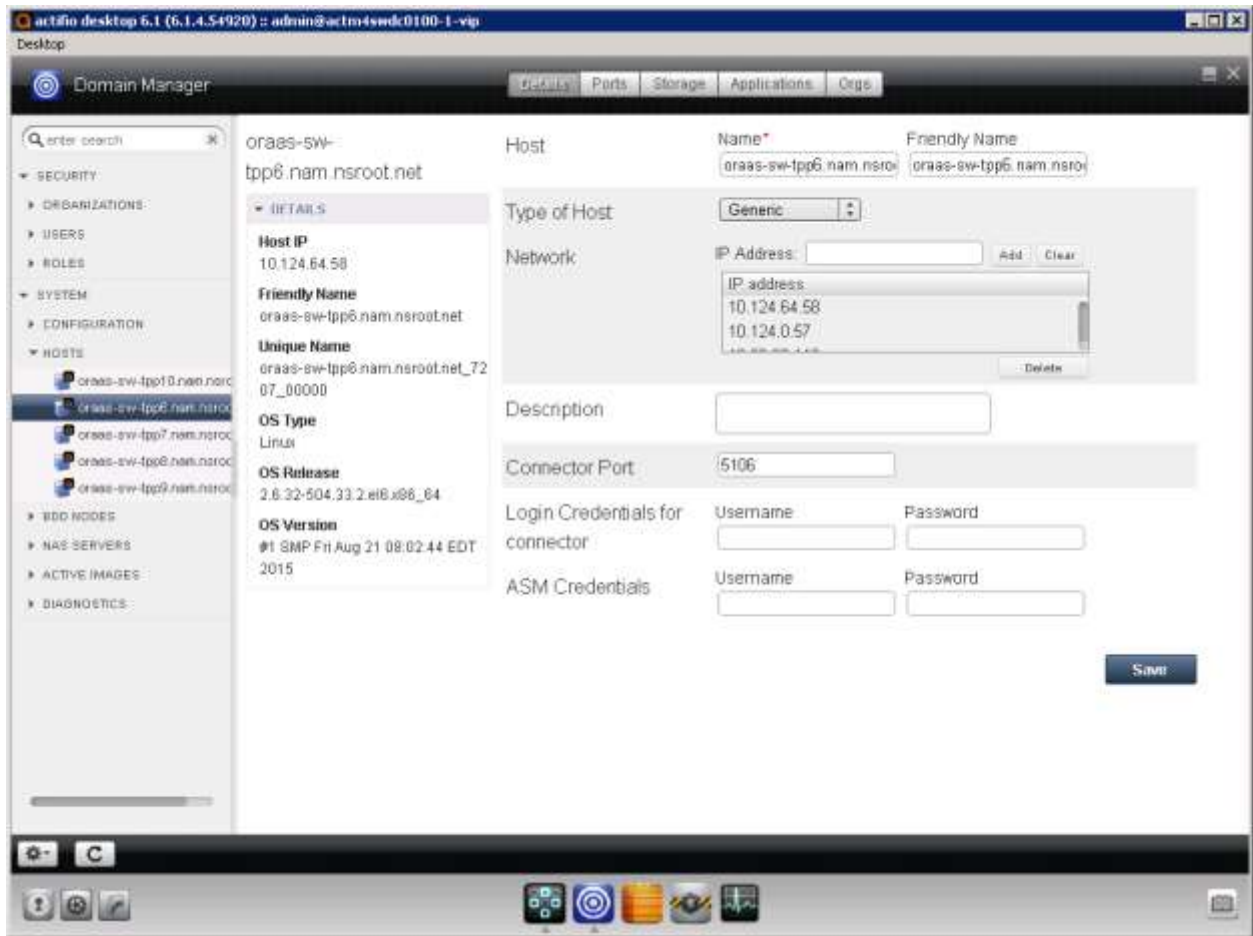
To view and create Policies, go to the SLA Architect screen and select the Policy from the left hand panel. This will show the data flow on the local Appliance and if a Dedup Backup is used or not.

12.3 Create Resource Profiles

Resource Profiles are used to allocate storage again a Policy. This can be used if storage on the Appliance is segregated between applications. As of version **0.6** of this document, the Profile usage is not finalized.

12.4 Create Hosts

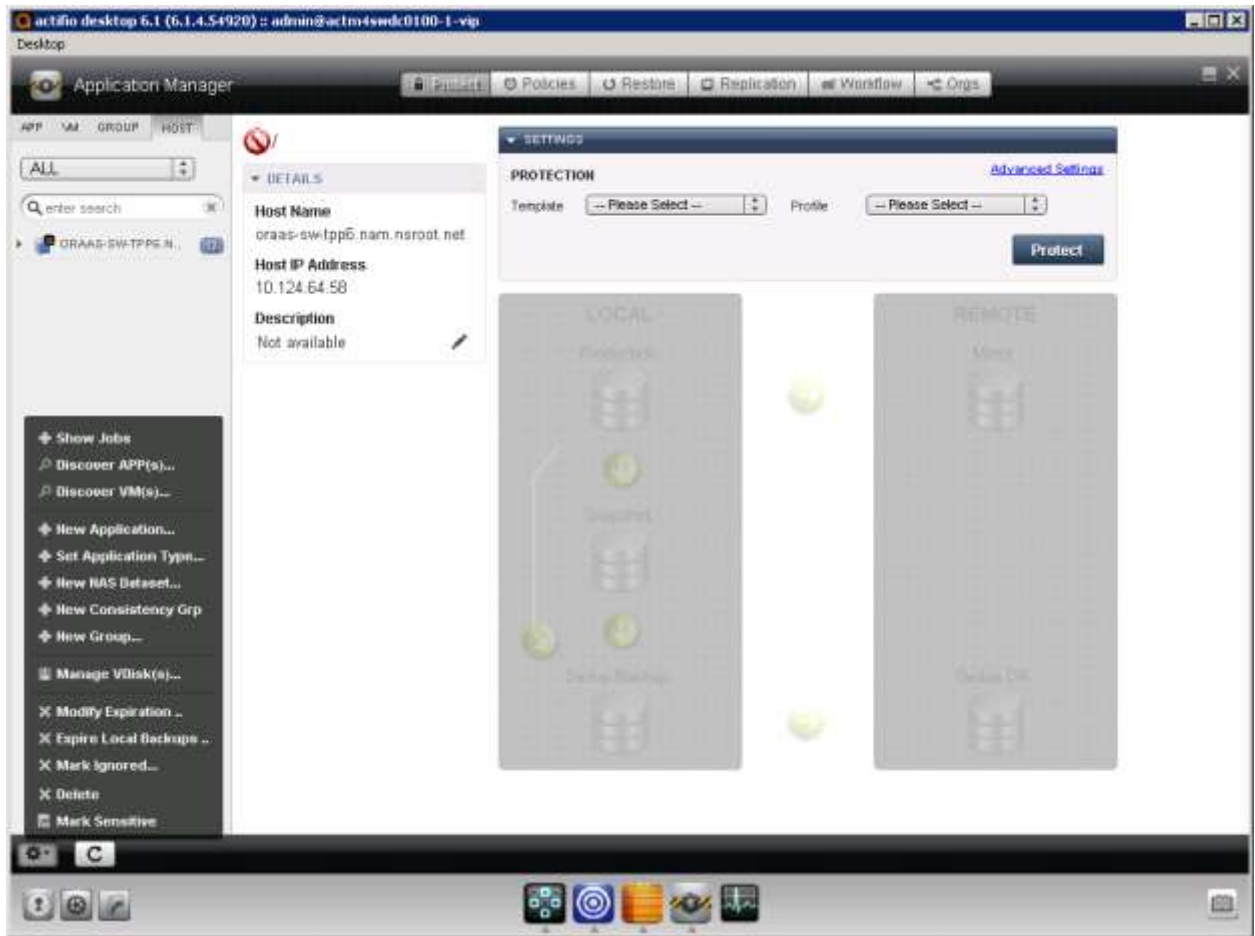
Before creating a host, ensure that the connector has been deployed. This is the client Actifio agent. To add a host, go to the Domain Manager screen and select New Host from the “cog wheel” menu on the bottom left of the screen. This will automatically add a template host and the details can be changed as appropriate.



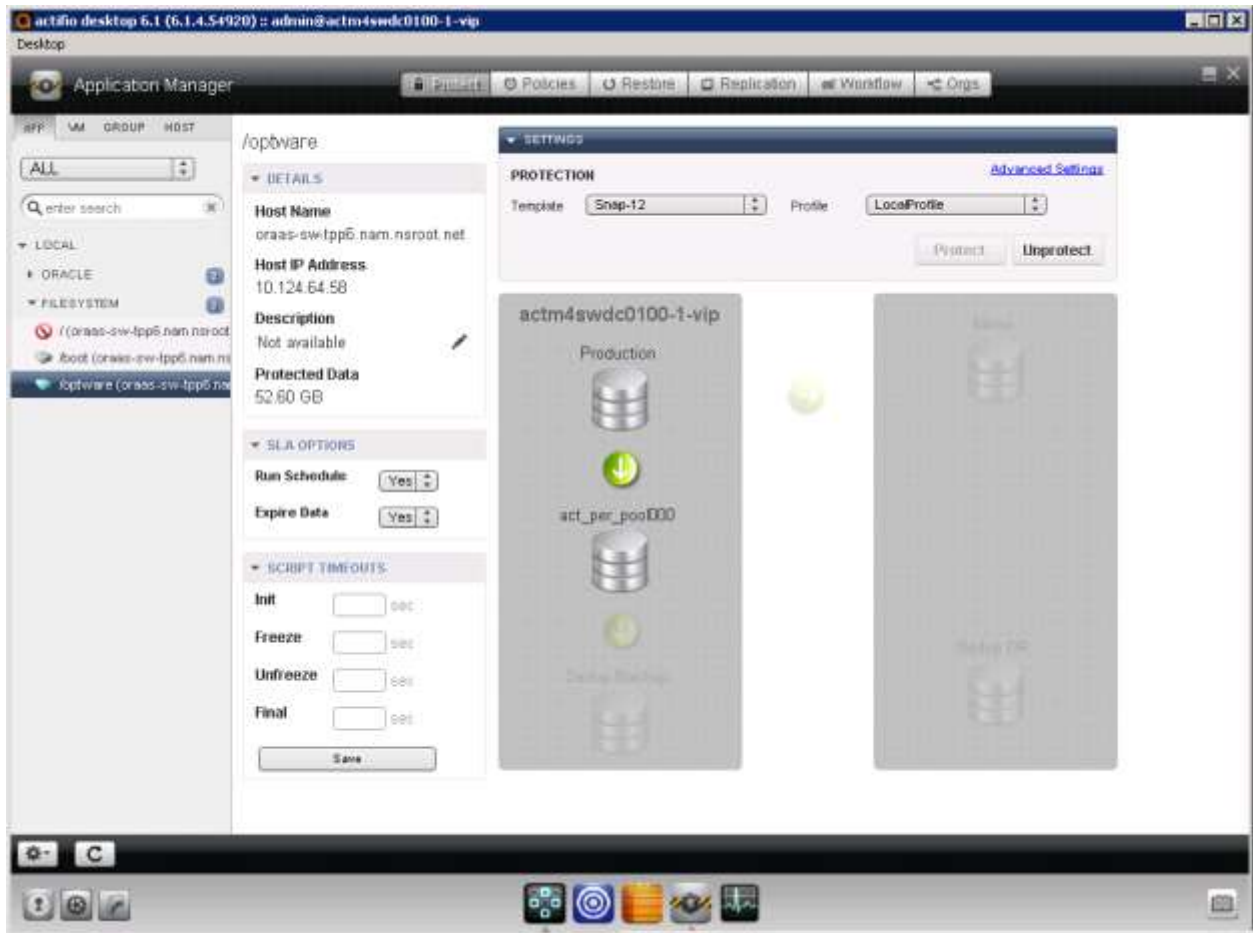
Ensure that all iSCSI network interfaces are included in the client definition. Also ensure that it is put into the correct Organization. This can be done by clicking the Orgs button at the top of the screen.

12.5 Discover Host Applications

After a host has been added to Actifio, the applications on the host can be discovered via the client connector installed on the host. To do this, go to the Application screen (yellow button at the bottom of the window and then select Discover Apps from the “cog wheel” menu, as shown below.



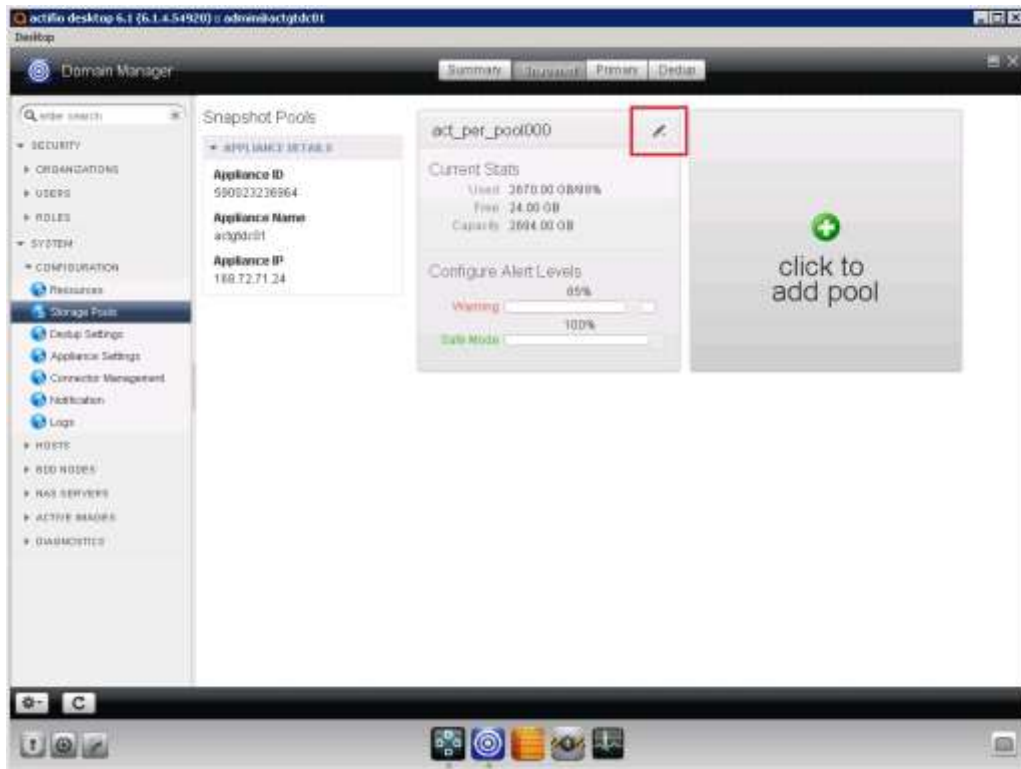
Once the applications on a host have been discovered, they can be protected by selecting the application from the left hand pane and the assigning a Template and Profile as shown below and clicking the protect button.



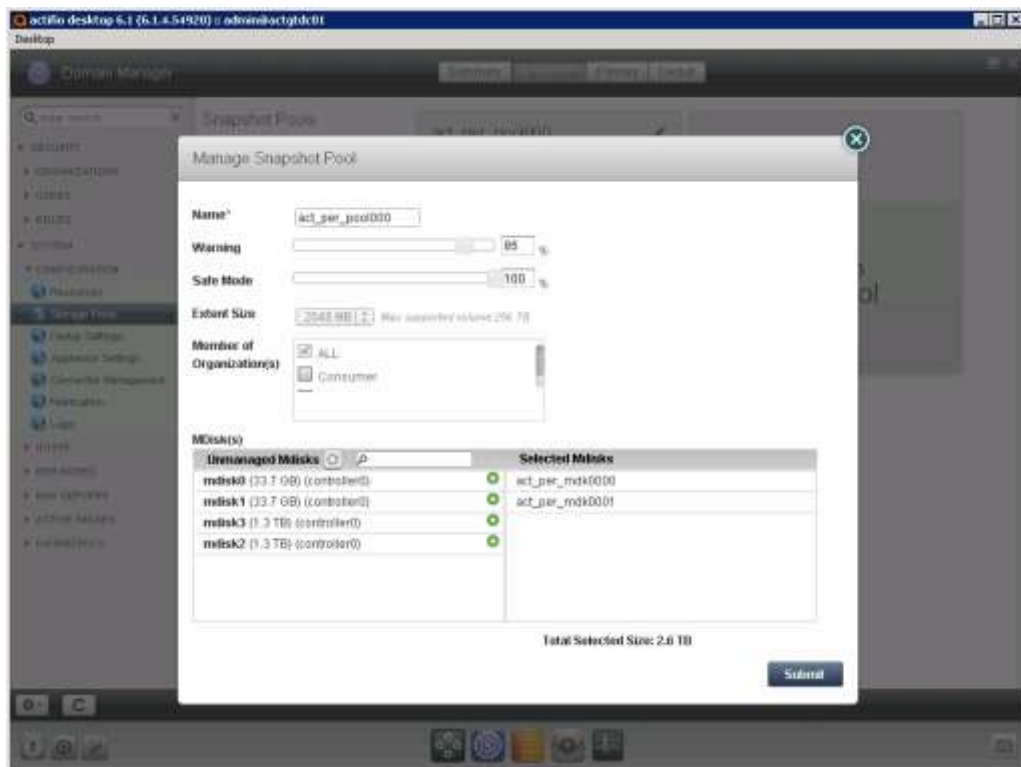
In the above example, the /optware filesystem is protect with a snapshot only template.

12.6 Adding Storage

Additional storage for the Appliance will need to be added in the usual way for SAN clients at Citi. To utilize the new allocated storage on the Appliance, go to the Domain Manager window and select the Snapshot Pool for which storage needs to be added. Then click on the “pencil” icon to edit the pool as shown below.

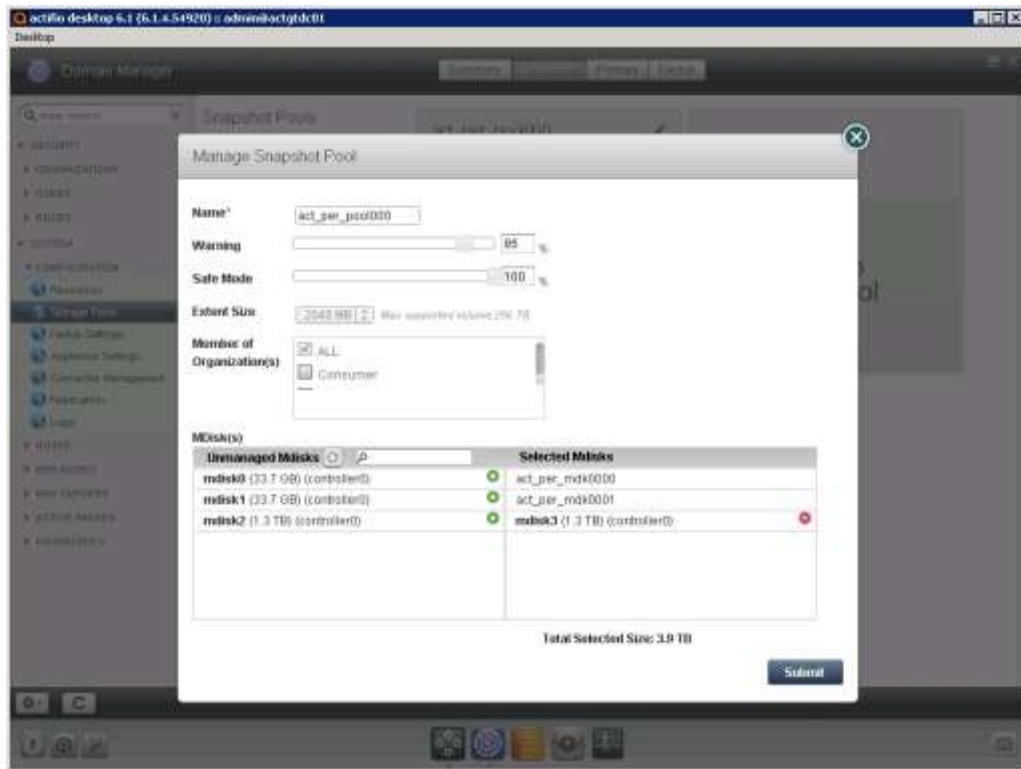


This brings up a new window in which the new mdisks can be listed and added.



©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.



Click the green + button to add them to the pool and click Submit. The new storage will become available immediately.

12.7 Monitoring Overview

Monitoring from the Actifio GUI is document at length in the vendor documentation. See the references section.

13 Oracle Operations

This topic is still under development by CATE Database Automation and is currently documented elsewhere. References will be provided by the end of January 2016.

The OraaS environment is operated via a web portal.

14 Appendix A

14.1 Actifio GUI

The main interface for Actifio is via the AIR based GUI. This can be downloaded directly from the Appliance cluster interface as shown below:

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.



To install the AIR Player, Administrator rights are required on the desktop or server. Note that the AIR installation will prompt the user to upgrade the installation directly from Adobe as and when the vendor releases updates. When the AIR installation is complete, download and install the Actifio Desktop Air File. This also requires Administrator rights.

14.2 Actifio CLI

The command line option is available to all users. The commands available on the cluster depend upon the privileges a particular user has.