

Actifio CDS/Sky Tech Brief

Configuring Hitachi Content Platform and Actifio OnVault for Long-Term Data Retention

Audience

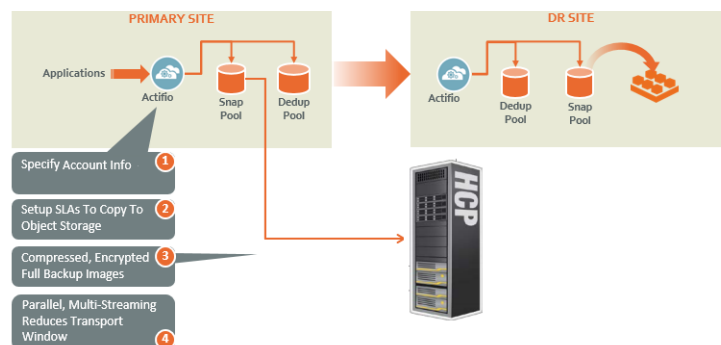
The intended audience for this document is the user who is familiar with Hitachi® Content Platform (HCP) and who has a basic understanding of Actifio processes and procedures.

Overview

Actifio appliances retain data in pools:

- Actifio Snapshot Pools provide short-term data retention i.e. a few days. Snapshot data ensures instant access to the latest production data.
- Actifio Dedup Pools provide medium-term data retention i.e. three to six months. Dedup data is incrementally rehydrated before it is accessed.

Actifio OnVault Pools and Actifio OnVault Policies allow a single Actifio appliance to send compressed, full snapshots of application data to an HCP Name Space where data is retained for the long-term i.e. for months or years. Incremental copies of production data are not sent to OnVault Pools.



Four Steps to Put Application Data into HCP Name Space

Before You Begin

This document assumes that you have a basic understanding of HCP processes and procedures. From HCP, you will be required to obtain:

- A Private key (Secret Access Key) for the S3 storage.
- The Access ID (Access Key ID) for the S3 storage.

Note: The Secret Access Key and Access Key ID must be in S3 format. To convert your HCP credentials to S3 format, see [Converting HCP Credentials](#) on page 8.

- A PEM file if you require HTTPS connectivity to your HCP object storage.
- A bucket name (Name Space) for this Actifio OnVault Pool.
- The URL to your object storage.

Once you have obtained these, then you can:

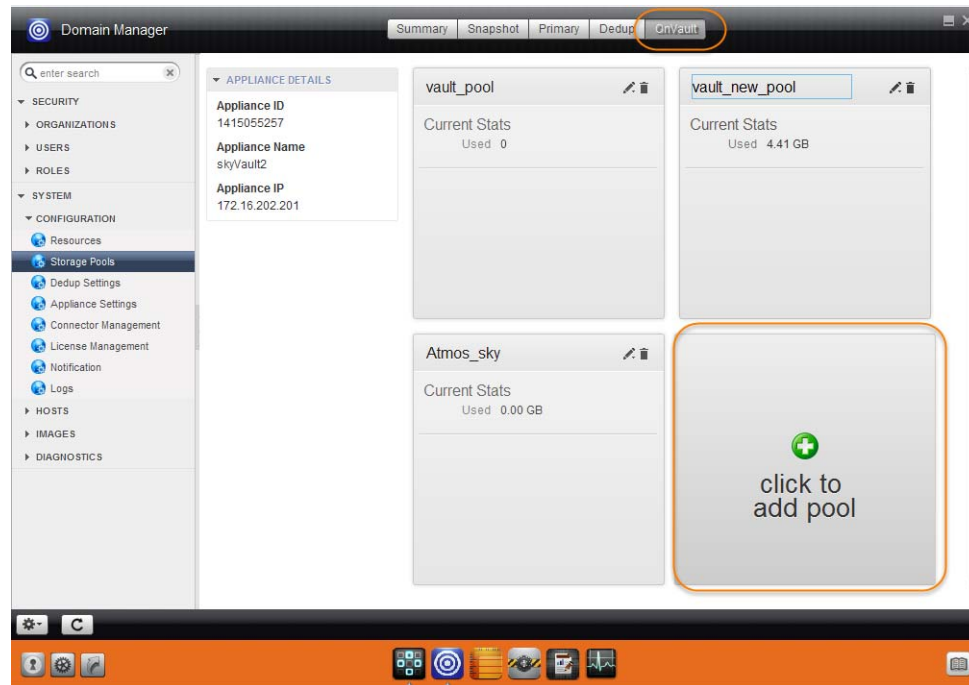
- [Add Actifio OnVault Pools](#) on page 3
- [Create Snapshot to OnVault Policy](#) on page 6
- [Access Data in an Actifio OnVault](#) on page 7

Add Actifio OnVault Pools

Actifio appliances store data in pools. Actifio OnVault Pools store copies of Production Snapshot data in HCP S3 object storage Name Spaces (S3 buckets).

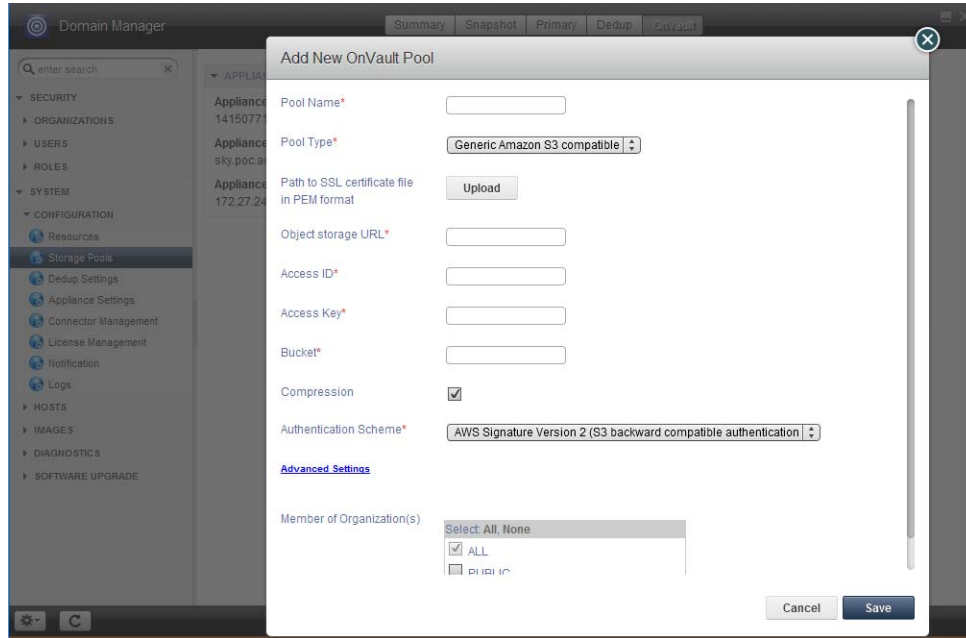
To add an OnVault Pool to an Actifio appliance:

1. Open the **Domain Manager** to **System > Configuration > Storage Pools**.
2. Select the **Vault** tab and the Vault Pools page opens:



Vault Pools

3. Click **Click to add pool** and the Add New OnVault Pool dialog box opens.



Generic Amazon S3 Compatible Storage Settings

4. In the space provided, enter a Pool Name for the OnVault pool.
5. From the **Pool Type** drop down menu, select **Generic Amazon S3 Compatible**.
6. If you want to use an HTTPS connection to your object storage, click **Upload** to upload the SSL Certificate (PEM format) file for your HCP object storage.
7. In the spaces provided enter:
 - o The URL to your HCP S3 object storage
 - o The Access ID (Access Key ID) for the HCP S3 object storage
 - o The Access Key (Secret Access Key) for the HCP S3 object storage

Note: The Secret Access Key and Access Key ID must be in S3 format. To convert your HCP credentials to S3 format, see [Converting HCP Credentials](#) on page 8.

- o The Bucket name (Name Space) created for the HCP S3 object storage
8. In most cases you will want to keep the compression option checked. Compression will keep network traffic to a minimum.
 9. **Advanced Settings** should only be changed from the default 64KB block size at the direction of Actifio Support.
 10. Select the **AWS Signature Version** as needed.
 11. Select the organization memberships for the OnVault pool as needed

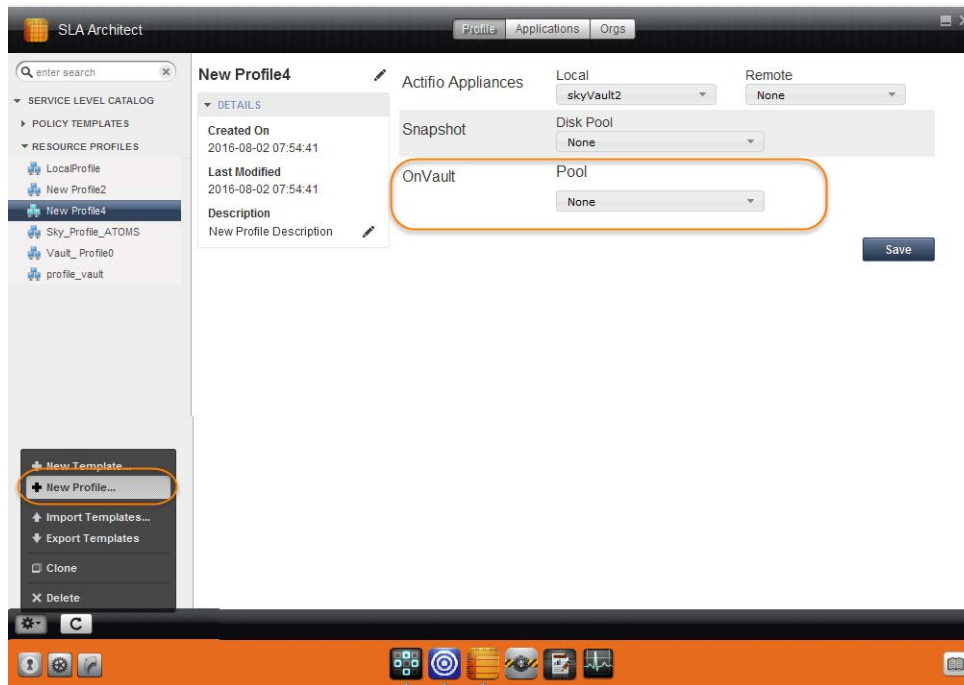
Create a Resource Profile

Resource profiles define in which Actifio pool application data is retained.

Resource Profiles are created in the Actifio Service Level Architect (SLA) service. To create a resource profile:

1. From the SLA Architect select either an existing policy template or from the SLA Architect's service menu, click **New Profile...** and the Resource Profile page is displayed.

Caution! If you select an existing Profile, ALL applications to which the Profile is applied will be impacted by changes to the Profile.



2. Select the local Actifio appliance from **Local** drop-down list. This is the appliance on which the profile is created.
3. Ensure a Snapshot Pool from the **Disk Pool** drop-down list is selected. Data written to this pool will be sent to the OnVault specified according to SLA Template Policy definitions.
4. From the **Vault Pool** drop down menu, select the Actifio OnVault Pool to which production data in the Snapshot Pool will be sent. You can select this option only if this Actifio appliance has defined an OnVault Storage Pool.
5. Click **Save**.

Create Snapshot to OnVault Policy

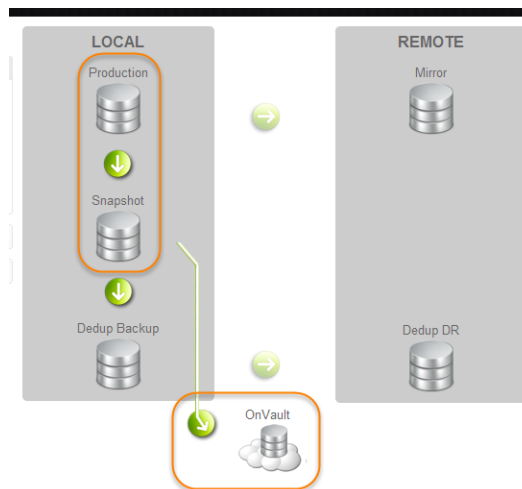
The Snapshot to OnVault policy allows you to schedule when to send Production Snapshot data to an Actifio OnVault Pool.

To create a Production to OnVault Policy, you must either use an SLA Policy Template that already has a Production to Snapshot Policy defined or create a new SLA Policy Template.

Caution! If you add a Snapshot to OnVault Policy to an existing SLA Policy Template, **ALL applications** to which the SLA Policy Template is applied will be impacted by the changes.

Best practices for creating SLA Policy Templates and Policies can be found in the **Developing Service Level Agreements** guide.

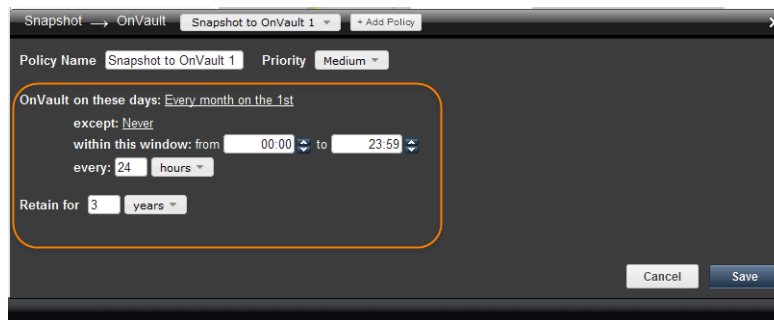
Individual policies within an SLA Policy Template are defined by clicking the green arrows on a new or existing SLA Policy Template:



When creating a Snapshot to OnVault policy to send the SLA Policy Template's most recent Production to Snapshot data to an Actifio OnVault Pool, set the frequency at which data is sent to no less than one week and make other settings as needed.

For example, to send Production to Snapshot data to a OnVault once a month, set:

- Vault on these days to **Every month on the 1st**
- The window to open and close as needed. Typically set to 19:00 to 18:50
- The frequency to **Every 24 Hours**
- Retain for **3 Years**



Capture Application Data

Once you have both a Resource Profile that uses an OnVault Pool and an SLA Policy Template that contains an OnVault Policy, you can, via the Actifio Application Manager apply the Resource profile and SLA Policy Template to applications and VMs.

Access Data in an Actifio OnVault

When accessing data in an Actifio OnVault Pool's object storage:

- Actifio CDS and Sky appliances can create clones from OnVault data.
- Actifio Sky appliances can mount OnVault data.

Note: Mounted data can be accessed directly from a host, but it is not recommended to run workloads directly against this data.

- Actifio CDS appliances **cannot** mount data in an OnVault Pool
- LiveClones cannot be created from data in an OnVault Pool.
- Actifio Application Aware mounts are not supported for data in an OnVault Pool.

For details on how to access data captured by an Actifio appliance, see ***Accessing and Recovering Copy Data with the Application Manager***.

Converting HCP Credentials

The following example Powershell script can be used to convert HCP credentials to S3 style. Actifio does not warrant or provide support for this script. It is provided here as an aid to help you create your own script to convert your Hitachi credentials to S3 format.

```
# Intro
cls
Write-Host "HCP HS3 Access Key Conversion Tool"
Write-Host ""
Write-Host ""

# Function to Convert to Account name to Base64
function ConvertTo-Base64($string) {
    $bytes = [System.Text.Encoding]::UTF8.GetBytes($string);
    $encoded = [System.Convert]::ToBase64String($bytes);

    return $encoded;
}

# Function to convert Password to MD5
Function Get-StringHash([String] $String,$HashName = "MD5")
{
    $StringBuilder = New-Object System.Text.StringBuilder
    [System.Security.Cryptography.HashAlgorithm]::Create($HashName).ComputeHash([System.Text.Encoding]::UTF8.GetBytes($String))|%{
    [Void]$StringBuilder.Append($_.ToString("x2"))
    }
    $StringBuilder.ToString()
}

# Get Tenent Account Name and Password
$accesskey = Read-host "Type the HCP Tenant Account Name"
$SecretKey = Read-host "Type the HCP Tenant Account Password" -AsSecureString

# Convert Secret to plain text
$BSTR = `
    [System.Runtime.InteropServices]::SecureStringToBSTR($SecretKey)
$PlainPassword = [System.Runtime.InteropServices]::PtrToStringAuto($BSTR)
```



```
# Send values to formulas
$aktemp = ConvertTo-Base64($accesskey)
$sktemp = Get-StringHash($PlainPassword)

# Output values
Write-Host ""
Write-host "The HS3 Access Key for $accesskey is: " $aktemp -ForegroundColor Yellow
Write-host "The HS3 Secret Key for $accesskey is: " $sktemp -ForegroundColor Green
Write-Host ""
Write-Host ""
```

