

# HP Open View Data Protector for Security Containment



|   |   |
|---|---|
| Introduction.....                         | 2 |
| HP Open View Storage Data Protector ..... | 2 |
| Data Protector Concept .....              | 3 |
| Security Containment Concepts .....       | 3 |
| Software Infrastructure.....              | 5 |
| Writing Security Policy backup.....       | 5 |
| RBAC policy.....                          | 6 |
| Bastille Policy:.....                     | 7 |
| IP Filter Policy: .....                   | 7 |
| Appendix A .....                          | 8 |
| For more information.....                 | 9 |

## Introduction

This document helps you deploy a backup application in a Security Containment environment that will protect your backup applications from other application security threats. HP-UX Security Containment provides a highly secure operating system environment. Security containment uses three core technologies (compartments, privileges, and authorizations) to provide platform level security which is essential for enterprises and small and medium enterprises (SME) to host their business applications securely. This document demonstrates how to deploy HP Open View Data Protector applications in an HP-UX Security Containment environment.

Traditionally, enterprises deployed different applications in a single operating system environment. For example, a backup application that runs along with other enterprise applications. In a highly hostile internet environment, there is a possibility of a system being compromised. In addition if one application in the system is compromised, there is a high probability that other applications will get compromised. In the traditional UNIX environment, there is no mechanism to mitigate this scenario.

This document explains a way to isolate a backup application from other applications running in a system using HP-UX Security Containment. In today's enterprise, backup applications play a vital role since many applications and databases frequently make small changes to existing files or produce many new files containing business-critical data throughout the day. These files need to be backed up immediately to guarantee that no data is lost. Therefore, the backup application should be protected at all times from internet threats in order to perform real-time application data backup and restore functions.

The following sections explain how to isolate HP Open View Data Protector (omni) in a security containment environment.

## HP Open View Storage Data Protector

HP OpenView Storage Data Protector is a backup solution that provides reliable data protection and high accessibility for your fast growing business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments. Data Protector is an effective back up and restore tool for environments that range from a single system to multiple (thousand) systems at different locations.

The Data Protector cell is the basic management unit in the data protector. It consists of a network environment with a Cell Manager system, one or more Installation Servers, client systems, and devices. The Cell Manager and Installation Server can be on the same system (default setting) or on different systems. Data Protector has the following features:

- Scalable and highly flexible architecture
- Easy central administration
- High performance backup
- Easy installation, backup, and restore

See [HP Open View Storage Data Protector Concepts Guide](#) (B6960-96001) for more information on the features that Data Protector offers.

## Data Protector Concept

A backup is a process that creates a copy of the data on a backup device. During backups on a network environment, the data is transferred over the network from systems that need to be backed up on systems with backup devices. A restore is a process that recreates the original data from a backup copy. This process consists of the preparation and actual restore of data, and some post-restore actions that make that data ready for use.

Though Data Protector supports different types of backup and restore operations, this document discusses disk backup (also known as disk-to-disk backup). Many applications and databases frequently make small changes to existing files or produce many new files containing business-critical data throughout the day. These files need to be backed up immediately to guarantee the data in them will not be lost. This requires a fast medium that can store large amounts of data and that works without interruption. Today, more and more businesses are augmenting their tape storage backup solutions with faster disk-based backup solutions because disks are cheaper, more reliable, and faster than the traditional tape devices. See [HP Open View Storage Data Protector Concepts Guide](#) (B6960-96001) for more information on the advantages of disk backup.

Data protector has three disk-based devices: file library devices, standalone file devices, and file jukebox devices. This document uses the file library devices while performing backup and restore operations. The file library device is the most sophisticated disk-based backup device. The device's maximum capacity is the same as the maximum that can be saved on the filesystem on which the device resides. Each file depot has a maximum capacity of up to 2 TB. The file library device has intelligent disk space management; it anticipates potential problems. A warning message is written in the event log file if the amount of free disk space approaches the configured minimum amount required for the device to work. This enables you to free more disk space in time for the device to continue saving data. If all the space allocated to the file library device is completely used, a warning message appears on the screen with instructions on how to solve the problem. HP recommends using the file library device as the preferred disk-based backup device. See [HP Open View Storage Data Protector Concepts Guide](#) (B6960-96001) for more information on other devices.

Data Protector uses the default port number 5555. Therefore, this particular port number should not be used by another program. If the port number 5555 is already in use, you should make it available for Data Protector or you can change the default port number to an unused port number. See *Changing the Default Port Number* on page B-28 of [HP Open View Storage Data Protector Installation and Licensing Guide](#) (B6960-96002).

## Security Containment Concepts

Security Containment primarily consists of three core technologies: compartments, fine-grained privileges, and Role-Based Access Control.

### Compartments

The compartments feature of the HP-UX Security Containment software isolate unrelated resources on a system, to prevent catastrophic damage to the system if one compartment is compromised. When an application is configured in a compartment, it has restricted access to system resources (processes, binaries, data files, and communication channels used) outside its compartment. This restriction is enforced by the HP-UX kernel and cannot be overridden unless specifically configured to do so. If the application is compromised, it will not be able to damage other parts of the system because it is isolated by the compartment configuration.

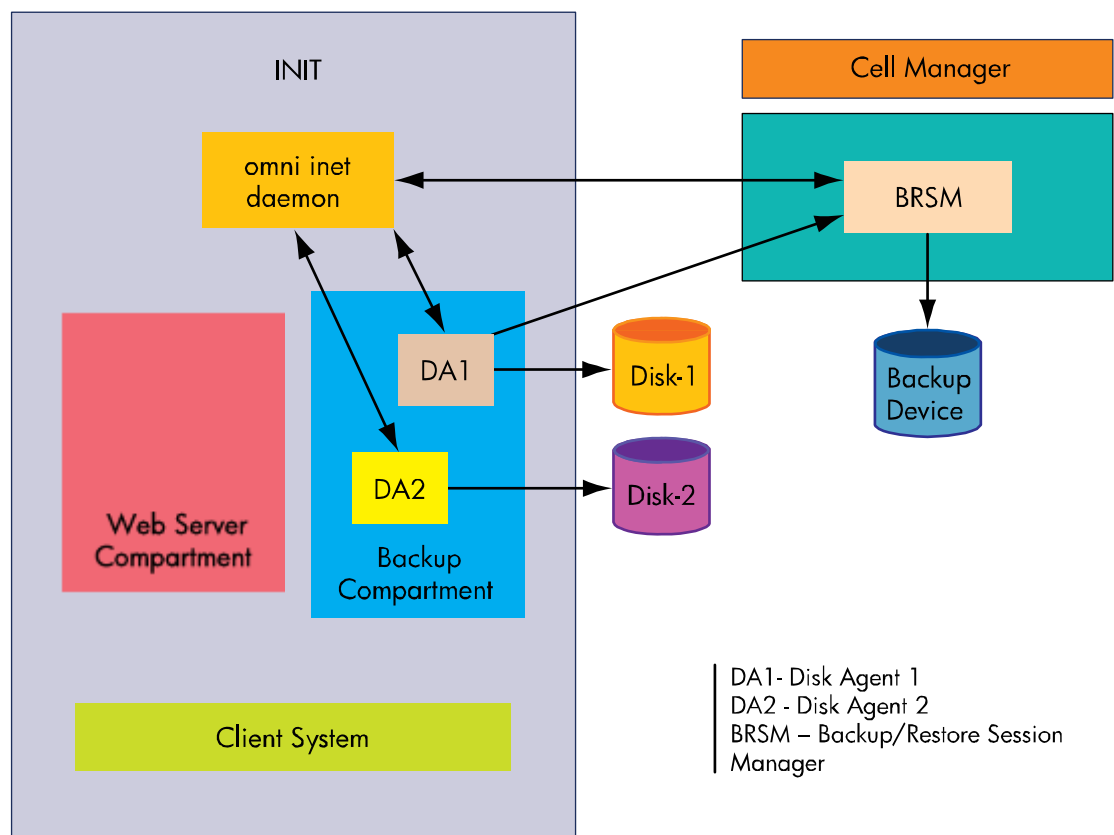
## Fine Grained Privileges

Traditional UNIX operating systems grant "all or nothing" administrative privileges based on the effective `UID` of the process that is running. If the process is running with the effective `UID=0`, it is granted all privileges. With fine-grained privileges, processes are granted only the privileges needed for the task and, optionally, only for the time needed to complete the task. Applications that are privilege-aware can elevate their privilege to the required level for the operation and lower it after the operation completes.

## Role-Based Access Control (RBAC)

Typical UNIX system administration commands must be run by a superuser (`root` user). Similar to kernel level system call access, access is usually "all or nothing" based on the user's effective `UID`. HP-UX Role-Based Access Control (HP-UX RBAC) enables you to group common or related tasks into a role. For example, a common role might be `User` and `Group` administration. Once the role is created, users are assigned a role or set of roles that enables them to run the commands defined by those roles.

The following figure shows the architecture for an `omni` backup configured in a Security Containment environment.



The architecture illustrates a client system and a cell manager. The cell manager is the central control point where the Data Protector Software is installed. After installing the Data Protector Software, you can add systems (client system) to be backed up. The client system is installed and configured with the

HP-UX Security Containment product. In this figure, the client system is configured with three different compartments:

- Web server compartment
- backup compartment
- INIT, the default system compartment

The Data Protector backup and restore agent's runs in the backup compartment.

## Software Infrastructure

Install Open View Data Protector software on the system designated as the Cell Manager. See [HP Open View Storage Data Protector Installation and Licensing Guide](#) (B6960-96002) for more information on the installation.

The Security Containment product is located on the HP-UX 11iv2 December 2006 Software Pack DVD for HP-UX 11iv2, and is an integral part of HP-UX 11iv3. See [HP-UX 11i Security Containment Administrator's Guide](#) for installation instructions for Security Containment, Role-Based Access Control, and Standard Mode Security Enhancements on HP-UX 11iv2.

On the client system, perform the following installation steps:

- Successfully install Security Containment, Role-Based Access Control, and Standard Mode Security Enhancements
- Install Data Protector Disk agent on the client system. You can install disk agent from Cell Manager's GUI. HP recommends that you to install disk agents over a secure connection. To do this, refer to the *Setting up OpenSSH* section of the [HP Open View Storage Data Protector Installation and Licensing Guide](#). Typically, most systems configured in a secure environment disable other services, except for Secure SHell (SSH). For example, the HP Protected Systems. Successful installation of disk agent on the client system adds an `omni inetd` entry to the `/etc/inetd.conf` file. It also updates the `/etc/services` file to ensure that port 5555 is mapped to `omni` if necessary.

## Writing Security Policy backup

The compartments feature of the HP-UX Security Containment software enables you to isolate processes, or subjects, from each other and also from resources, or objects. In this architecture we have defined two different compartments: backup and Web server. As illustrated in the architecture, there are two disk agents: DA1 and DA2 that are running in the backup compartment. Data protector's `inet` process runs in INIT compartment. The `inet` process is responsible for the communication between systems in the cell and starts other processes needed for backup and restore. The Data Protector `inet` service is started when Data Protector is installed on a system. For the purposes of this document, we assume that the client communicates with the DNS servers and that the cell servers use the interfaces in the compartment `in_iface` (for example, this compartment contains one or more interface rules such as `interface lan2` and `interface lan3` where the client uses either or both `lan2` and `lan3` to resolve DNS requests and to communicate with the cell server).

Data Protector processes communicate using TCP/IP connections. Every Data Protector client system accepts connections on port 5555 by default. In addition, some processes dynamically allocate ports on which they accept connections from other Data Protector processes. The incoming connections are accepted by `inetd`—which is running in the INIT compartment—before handing them to the data

protector product. Therefore, the `INIT` compartment needs to be able to accept such incoming connections. If you have redefined the `INIT` compartment on your system, add the following rules to it:

```
grant bidir udp peer port 53 in_iface /* DNS client */
grant server tcp port 5555 in_iface /* Data Protector inet
      backup/restore daemon */
```

Define a new compartment `backup` as follows:

```
sealed compartment backup {
    disallowed privileges Policy
    perm all /
    grant client tcp in_iface /* Data Protector backup and restore
      processes */
    grant bidir udp peer port 53 in_iface /* DNS client */
}
```

The rule “`grant client tcp in_iface`” is necessitated by the internal organization of `omniback`: recall that the `omniback` client uses dynamically allocated ports to communicate back to the cell server.

As we shall see later on in RBAC policy section, the following processes run in the `backup` compartment:

```
/opt/omni/sbin/fsbrda and /opt/omni/sbin/vbda
```

To view the process running in the `backup` compartment, you need to add `ps -ef` to the RBAC commands (`cmd_priv`) database. See [Appendix A](#) for more information.

## RBAC policy

Deployment of an application in RBAC environment requires planning. You need to following

1. Identify a user runs an application. Create the user account using the `useradd` command if the user does not already exist.
2. Identify a role for the user created in step 1. Create the role using the `roleadm` command if the role does not already exist.
3. Identify and assign the authorizations that the role created in step 2 should have to run an application. Use the `authadm` command to create and assign the authorization if it does not already exist.
4. Define an authorization-to-application mapping using the `cmdprivadm` command.

To create a user, do the following:

```
# useradd -m backup
```

This step creates the user with the name `backup` to manage the `omniback`. This is an otherwise unprivileged user who would be configured to enter the `backup` compartment while running the `omniback` software using RBAC.

To create a new role called `DP` (“Data Protector”) that the user `backup` belongs to, do the following:

```
# roleadm add DP "Data Protector role"
# roleadm assign backup DP
```

To create a new authorization called `hpux.backups.omni` and assign it to the above role, do the following:

```
# authadm add hpux.backupsw.omni
# authadm assign DP hpux.backupsw.omni
```

Add the `cmd_priv` entry such that the command gets executed with `eid=ruid=0` with the compartment keyword `backup`.

```
# cmdprivadm add cmd="/opt/omni/sbin/inet \
-log /var/opt/omni//log/inet.log" op=hpux.backupsw.omni \
compartment=backup eid=0 ruid=0
```

When the omni disk agent software gets installed, the following `inet` entry gets added to the `/etc/inetd.conf` file:

```
"omni stream tcp nowait root /opt/omni/sbin/inet inet -log \
/var/opt/omni//log/inet.log"
```

Replace the above entry in the `/etc/inetd.conf` file with the following:

```
"omni stream tcp nowait backup /usr/bin/privrun privrun -c backup \
/opt/omni/sbin/inet -log /var/opt/omni//log/inet.log"
```

The above change ensures that the `/opt/omni/sbin/inet` process starts in the `backup` compartment. Execute `/usr/sbin/inetd -c`. This ensures that the `inetd` reads the changes made to the `inetd.conf` file.

## Bastille Policy

HP-UX Bastille is a security hardening and lockdown tool that can be used to enhance the security of the HP-UX operating environment. If your system is already configured with Bastille's demilitarized configuration file `DMZ.conf`, then Bastille configures the IPFilter rule which denies every connection other than the rules defined explicitly for specific applications. You should add an IPfilter rule for the Data Protector application to make sure that the client receives connections through the configured port. The next section explain how to add an IPFilter rule for Data Protector (omni) applications.

## IP Filter Policy

This section describes how to configure Data Protector in an environment where the Data Protector processes communicate across an IPFilter firewall that is configured either independently or using Bastille.

Add the following IPFilter rule (for the omni software) in the IPFilter configuration file, `/etc/opt/ipf/ipf.conf`.

```
"pass in quick proto tcp from any to any port = omni flags S keep state
keep frags"
```

Reload the IPFilter rules:

```
# /sbin/init.d/ipfboot stop
# /sbin/init.d/ipfboot start
```

## Appendix A

The following steps add a new authorization to view the processes running in the `backup` compartment:

1. Add the new authorization to view the processes running in the `backup` compartment, as follows:  
# `authadm add hpux.backupsw.omni.ps`
2. Assign the authorization to the role `DP`, as follows:  
# `authadm assign DP hpux.backupsw.omni.ps`
3. Add the `cmdpriv` entry, as follows:  
# `cmdprivadm add cmd="/usr/bin/ps" op=hpux.backupsw.omni.ps \ compartment=backup`
4. Once the `/usr/bin/ps` entry gets added to the `cmd_priv` database, you can view the processes running in the `backup` compartment by executing the following command:  
# `privrun -c backup ps -ef`

You can repeat steps **1**, **2**, and **3** to add more commands.

## For more information

You can find additional information about security and HP-UX at:

<http://docs.hp.com>

In particular, the following documents are available:

- [Bastille](#)
- [IPFilter](#)
- [Security Containment](#)
- [HP-UX 11i Protected Systems Web Server](#)
- [HP Open View Storage Data Protector Concepts Guide \(B6960-96001\)](#)
- [HP Open View Storage Data Protector Installation and Licensing Guide](#)

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Itanium is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

June 2007

