

### Introduction

Companies across the globe are faced with rapidly changing, sophisticated attacks against their IT infrastructure from both inside and outside of their organizations. Governments have not ignored the increasing threat to commerce and have enacted or are preparing legislation to require business attention to information security issues.

To help businesses conform to new regulations and combat the increasingly complex threats of attackers, HP is incorporating the next generation of security features called Security Containment into the mainstream HP-UX 11i v2 Operating Environment. HP-UX 11iv2 Security Containment introduces four core technologies: Compartments, Fine-Grained Privileges, Role Based Access Control and audit. These combine to provide a highly secure operating environment without requiring applications to be modified to take advantage of these new features.

---

## Security Containment Features

### Compartments

Similar to the design of a submarine, compartments on HP-UX 11iv2 are designed to provide isolation between unrelated resources to prevent catastrophic damage should a compartment be penetrated. When configured in a compartment, applications (processes, binaries, data files and communication channels used) have restricted access to those resources outside its compartment. This restriction is enforced by the HP-UX 11iv2 kernel and can not be overridden unless configured to do so. Because the application is isolated from other applications and system resources, if the application is compromised it will not be able to damage other parts of the system.

---

### Fine-Grained Privileges

Traditional UNIX operating systems grant "all or nothing" administrative privileges based on the effective UID of the process running. If the process is running with the effective UID number of 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" are able to 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 administrative commands are required to be run by a "superuser" (root). Like access to kernel level system calls, access is usually "all or nothing" based on the user's effective UID. RBAC allows common/related tasks to be grouped into a role, for example User and Group Administration. Once the role is created, users are assigned a role (or set of roles) that enable them to run the commands defined by those roles. By implementing RBAC non-root users are able to perform tasks previously requiring root privileges without granting the user complete root privileges.

---

### Audit

The current auditing system has been de-coupled from the Trusted Mode of HP-UX 11i and will be available while running in Standard Mode as well as Trusted Mode. Auditing provides selective recording of events for analysis and detection of security breaches.

---

### Introduction

## Standard Mode Security Enhancements

In addition to the Security Containment features HP-UX 11iv2 is also enhanced to support many of the security features previously available only in Trusted Mode. These features are distributed within Security Containment or separately as Standard Mode Security Enhancements.

---

### User Security Database

Previously many security attributes and password policy restrictions could be configured only on a system wide basis. These security features could be enforced only for all of the users or for none of the users. The user database being is used to store per-user information to support security features such as RBAC, password history, auditing, time-of-day login restrictions, etc. This per-user information allows security features to optionally be configured uniquely for each user. This information is accessed by the commands and libraries that enforce system security.

---

### Audit

The current auditing system has been de-coupled from the Trusted Mode of HP-UX 11i and will be available while running in Standard Mode as well as Trusted Mode. Auditing provides selective recording of events for analysis and detection of security breaches.

---

### Per-User Security Attributes

HP-UX SMSE introduced number of new security attributes that can be set on a per-user basis. For more information about the new security attributes, refer to the *HP-UX 11i Security Containment Administrator's Guide*.

---

## HP-UX 11iv2 Foundation OE Enhanced

### Shadow Passwords

Shadow Passwords enhance system security by hiding user encrypted passwords in a shadow password file, thwarting "brute-force" attacks to decrypt user passwords. Shadow Password is included with the in HP-UX 11i v2 Foundation Operating Environment. With Shadow Passwords, you now have the ability to have hidden passwords in both standard and trusted mode.

---

## Secure Resource Partitions

Security Containment can be combined with HP Process Resource Manager (PRM) or HP-UX Workload Manager (WLM) to create Secure Resource Partitions. As a part of the HP Virtual Server Environment, Secure Resource Partitions provide a powerful mechanism for consolidating applications within a single operating system image. Entitlement (fixed size) resource partitions can be created with PRM. HP-UX Workload Manager (WLM), the intelligent policy engine of the VSE, resizes resource partitions, hardware partitions with utility pricing and virtual partitions. WLM allows the partitions to be resized based on business policies or in goal-based mode where the partitions are sized based on actual application performance. The HP Virtual Server Environment (VSE) is an integrated solution for both HP 9000 and HP Integrity server platforms that delivers the highest degree of integrated virtualization for allowing your business to quickly respond to changing business demands.

Using security containment, customers can ensure that application instances can not access processes or files from other applications or the system. This ensures that multiple application instances run securely in a consolidated environment, providing the benefits of consolidation while preserving the security of a scale out environment.

Security Containment and HP-UX WLM provide an environment where the secure resource partitions are automatically resized based on business policy or application performance. This allows customers to take advantage of consolidation and virtualization techniques to improve server utilization and reduce operating system management costs while still maintaining or improving on the security benefits that are inherent in a standalone, scale out environment.

---

### *Introduction*

#### **Customer Benefits**

By combining the new features of Security Containment with the enhanced features available in the standard operating system, HP-UX 11iv2 provides a highly secure, easy to maintain and backwards compatible environment to deploy business applications. Existing application software does not have to be modified to take advantage of these security features. HP-UX 11iv2 is the trusted foundation of the adaptive enterprise and is a common release operating environment used to power the HP 9000 and HP Integrity lines of 64bit server hardware.

By using the features of Security Containment, customers can be assured that compromised applications will not be allowed unauthorized access to other applications/files on the system. Security Containment lowers TCO by ensuring that unplanned downtime due to server compromise is practically eliminated. On application and database servers processing high value transactions unplanned downtime reductions can add up in the millions of dollars.

Administrative tasks can now be broken up into logical role groupings and delegated to users without granting all administrative capabilities. Enhanced features of HP-UX 11iv2 make unauthorized system access even tougher than before by closing known points of attack as well as giving administrators the ability to tighten security policy enforcement. In the unlikely event of a security breach the audit trail provided by the HP-UX 11iv2 audit subsystem maintains excellent forensic data to track down the intruder.

Security Containment is integrated with the HP-UX 11iv2 virtualization continuum to form Secure Resource Partitions (SRP). Virtualization in many instances shows dramatic improvements in lowering the TCO of a company's IT infrastructure. While most servers today are underutilized, many operating in the 30% range, virtualization has shown to improve utilization to more than 80%. Using SRPs, customers will be able to use Security Containment to isolate entire applications or individual processes within partitions, providing them with the confidence that the virtual server environment and partitioning is both secure and cost effective.

### Hardware and Software Requirements

#### Hardware Requirements

HP-UX 11i v2 security containment operates as a common operating environment for HP 9000 and HP Integrity Servers.

---

#### Software Requirements

Security containment is a no charge feature of the HP-UX 11iv2 operating environment.

---

#### Distribution Media

Security Containment is available for download from [Software Depot](#). The Security Containment distribution also includes the following individual distributions that are available separately.

- Role-based Access Control from [Software Depot](#)
  - Standard Mode Security Extensions from [Software Depot](#)
- 

#### For More Information

HP-UX 11i Operating Environment [www.hp.com/go/hpux](http://www.hp.com/go/hpux)

HP-UX 11i Security [www.hp.com/go/hpux11isecurity](http://www.hp.com/go/hpux11isecurity)

HP-UX 11i Security Containment [www.hp.com/go/securitycontainment](http://www.hp.com/go/securitycontainment)

HP Virtual Server Environment [www.hp.com/go/vse](http://www.hp.com/go/vse)

---

© Copyright 2005 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.