Global Information Assurance Certification Paper

Security Considerations for HP-UX and MC/ServiceGuard

Frank Carrick

GIAC Security Essentials Certification (GSEC) Practical Assignment

Version 1.4b

Abstract

Hewlett-Packard's MC/ServiceGuard software product improves availability of applications, such as data bases, by providing multiple potential hosts for these applications. The hosts are configured into a "cluster", and the applications into "packages". MC/ServiceGuard can monitor critical processes, networks, or the hosts themselves, and if a failure is detected the packages can be restarted on an alternate host.

Applications selected for a high availability implementation such as MC/ServiceGuard are generally critical to the business. As such, the securing of the availability of the application should go beyond the design of a highly available architecture. In most cases, the data associated with the application is also business critical, and should also be protected from exposure to unauthorized individuals. The security aspects of the application platform should be seriously considered.

The introduction of more than one potential host for a critical application raises additional security considerations. Some of these are host based, and need to be considered individually for each potential host. Some others concern the operation of MC/ServiceGuard itself, and may require additional attention. This paper will explore the issues raised, and offer some potential solutions.

MC/ServiceGuard in More Detail

MC/ServiceGuard software is available for HP 9000 series 800 servers running HP-UX, and for HP Proliant servers running Red Hat Linux. While many of the issues are the same, this paper will focus on the HP-UX operating system platform.

A typical configuration for MC/ServiceGuard will include two or more systems, or nodes. For simplicity, we will assume that two systems are being used, one designated as the primary host for the application, and the other as the secondary, or adoptive host. Each system will have local disks, containing their own operating system structure and any other files that are only needed on that system. There are other disks that are physically connected to both systems, that contain all application related data that is subject to change. MC/ServiceGuard will activate and mount these disks exclusively on the system that is going to run the application package. Static application files, such as executable binary files, can either be placed on these "shared" disks, or can reside on the local disks of each system. In this case, these files on the two systems should be exact duplicates.

Each system will have a unique IP address for each active network interface. These addresses are known as the "stationary IP addresses", because they are not transferable to any other system. Normally there are one or more unique IP addresses assigned to each application package. These are known as "relocatable IP addresses", because they will be assigned by MC/ServiceGuard to the appropriate LAN interface card in the system that is running the package. These relocatable IP addresses, rather than the stationary IP addresses, are used by clients to connect to the application software, because the relocatable IP addresses will be managed by MC/ServiceGuard to always be identified with the system that is running the package.

The application packages will be configured with all resources that are necessary for the application to run. These usually include the disk volumes and relocatable IP addresses mentioned above and scripts to start and stop the application. There may also be services configured into the package, typically to monitor the application software and/or related hardware. In the event of the loss of a critical resource, MC/ServiceGuard will initiate the failover of the application package to an alternate node.

HP-UX Security Issues and Solutions

"The majority of the successful attacks on operating systems come from only a few software vulnerabilities." This quote is from a document published by the SANS Institute and the FBI's National Infrastructure Protection Center (NIPC), titled "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus ". It can be found at many security-related sites across the internet. The document lists the ten most commonly exploited vulnerable services in Unix, along with the ten most commonly exploited vulnerable services in Windows. Those listed for Unix are:

- Remote Procedure Calls (RPC)
- Apache Web Server
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- File Transfer Protocol (FTP)
- R-Services – Trust Relationships
- Line Printer Daemon (LPD)
- Sendmail
- BIND/DNS
- General Unix Authentication

The document, which includes more information about the specific vulnerabilities, can be found at http://www.sans.org/top20/.

For HP-UX, as well as for other Unix variants, one of the most important security related tasks for an administrator is to install the latest vendor supplied security

patches. Many of the known vulnerabilities in the above list can be corrected by staying current with security patches. Vulnerabilities are being discovered all the time, and patches are released frequently to deal with these new vulnerabilities. Hewlett-Packard has provided a tool, Security Patch Check, that compares the security patches installed on a system to a list of currently available security patches, and generates a report of recommended patches. This tool is available at no cost from http://www.software.hp.com/ISS_products_list.html.

Another resource available from Hewlett-Packard is the IT Resource Center (http://www.itrc.hp.com). You will have to register at this site, but there is no cost for this registration. Once registered, you will be able to subscribe to various support information digests, including the HP-UX security bulletins digest. You will also be able to access the HP Security Bulletins Archive which contains a list of all previously published HP Security Bulletins, and the HP-UX Security Patch Matrix, which contains an index of bulletins with up-to-date patch IDs.

In addition, best practices to reduce vulnerabilities include, but are not limited to:

- Installing the Operating System from a known and trusted source
- Removing or disabling unnecessary software products
- Enforcing strong password policies, and educating users on good password practice
- Setting proper permissions on critical files and directories
- Disabling unnecessary network services
- Configuring logging as appropriate, and regularly reviewing and trimming log files.

These best practices are as important for systems in an MC/ServiceGuard cluster as they are for any other critical system.

HP also provides the ability to convert an HP-UX system to a trusted system. Important additional security features available with a trusted system are:

- Protected password database
- Enhanced login configuration
- Auditing
- Terminal restrictions
- Serial port restrictions
- Access time restrictions
- Password generation
- Password aging (Wong, 31)

MC/ServiceGuard is fully compatible with trusted systems, however, not all applications are. There are known problems with some legacy software and software that does not use the Pluggable Authentication Module (PAM) to authenticate users (Skagen and Jones, 11). It is recommended that a test

environment be set up, converted to a trusted system, and thoroughly tested to assure that all applications are compatible with trusted systems.

For additional information on the more general topic of securing HP-UX, there are a number of papers available at the SANS Information Security Reading Room, at http://www.sans.org/rr/unix/.

Additional Security Issues and Solutions for an MC/ServiceGuard Cluster

Since there are multiple hosts that can be used to run applications in an MC/ServiceGuard cluster, concerns such as those listed above that apply to a typical system hosting the application must be considered for all potential hosts. Sometimes this is complicated by the fact that when the packaged application is running on the primary host, the adoptive host may be performing other, less critical work. Typically, when this is the case the adoptive host will shut down this less critical work before starting the production application. The other workload may require some differences between the primary and adoptive application hosts. These differences should be reduced to as few as possible.

All hosts in the cluster should be kept at the same patch level, with another system that is not a potential host for the production application package used to test the patch bundles before they are applied to the cluster nodes. As mentioned above, particular attention should be paid to security related patches.

Users who need the ability to log onto the HP-UX host to access the application will need this ability on all potential hosts. A mechanism should be devised and used to allow a user to change his password on all nodes at once. If it is left to the user to remember to change passwords on each system individually, problems will inevitably occur with stale passwords remaining on some hosts. This could lead to users having problems logging in to their accounts. More seriously, it could lead to an exploitable vulnerability of the system.

MC/ServiceGuard needs the ability to have some trusted root capabilities among all nodes in the cluster. The capabilities that are required for “normal” cluster activities have been implemented through ServiceGuard daemons, rather than relying on the “r” commands. A file (/etc/cmcluster/cmclnodelist) should be created to define the nodes permitted this access. This file should not allow write access except for the owner, which should be root. If the cmclnodelist file exists, it is the only mechanism used to grant MC/ServiceGuard the root capabilities it needs within the cluster. All cluster nodes should be listed in this file, with root as the user. If the cmclnodelist file does not exist, the .rhosts file in the root user’s home directory will be used to determine if this access should be granted. It is more secure to use the cmclnodelist file rather than .rhosts, because only the necessary MC/ServiceGuard functions are authorized through cmclnodelist. Spoofing an entry in cmclnodelist will not grant any other type of root access.

An entry for a non-root user can also be put in the cmclnodelist file. This would allow that user to view the status of the cluster by running the “cmviewcl” command, while not allowing that user to run any other cluster commands. This

may prove useful to allow certain users to monitor the cluster and packages without giving them the root password.

The scripts that are run by MC/ServiceGuard to start, stop, and monitor the applications within its packages are run as root. If any commands need to be run by a different user, this can easily be accomplished through use of the "su" command. No password will need to be entered in the script, since the root user requires no password to switch to another user. This also clearly means that these scripts need to be just as well protected as any other commands that are executable by root. They should be owned by root, and write and execute permission should only be granted to root. Typically read access should be only granted to root as well, since allowing other users to see these command strings may provide important information to an unauthorized person. Care must also be taken that the correct permissions are set on the directory containing these scripts, to prevent their being replaced with versions that may contain Trojan Horse functionality. Further, any commands or scripts executed by the package start up, shut down, or monitoring scripts, as well as the directories containing these files must also be restricted in the same way.

One of the maintenance tasks associated with MC/ServiceGuard is assuring that all scripts and configuration files needed by the application that reside on each system's local disks are identical on each potential host. Typically this includes at least the MC/ServiceGuard cluster configuration file, along with a package configuration file and control script for each application package. In many cases additional application configuration files, or additional scripts that are executed by package control scripts, are stored on the local disks as well. Whenever these files are changed the changes must be propagated to the other nodes in the cluster. In most MC/ServiceGuard clusters, this is enabled through .rhosts files. A better solution, not only for MC/ServiceGuard related files, but for all files, is to install and use SSH. SSH for HP-UX is also available at no cost from http://www.software.hp.com/ISS_products_list.html. This version of Secure Shell is based on OpenSSH 3.1p1.

Whenever possible, the same network services should be enabled and disabled on all cluster nodes. If additional network services are required on the adoptive host, the inetd.sec file should be configured to restrict access to these services to only those hosts that require such access. If necessary, this access could be taken away by MC/ServiceGuard when the application package is started on the adoptive node.

MC/ServiceGuard requires 10 entries in /etc/services, listed in the table below.

Network Service	Port/Protocol	Function
clvm-cfg	1476/tcp	High Availability (HA) LVM Configuration
hacl-hb	5300/tcp	HA Cluster Heartbeat
hacl-gs	5301/tcp	HA Cluster General Services

hacl-cfg	5302/tcp	HA Cluster TCP Configuration
hacl-cfg	5302/udp	HA Cluster UDP Configuration
hacl-probe	5303/tcp	HA Cluster TCP Probe
hacl-probe	5303/udp	HA Cluster UDP Probe
hacl-local	5304/tcp	HA Cluster Commands
hacl-test	5305/tcp	HA Cluster Test
hacl-dlm	5408/tcp	HA Cluster Distributed Lock Manager

Three of these services need entries in /etc/ inetd.conf: hacl-cfg/tcp, hacl-cfg/udp and hacl-probe/tcp. The /etc/services and /etc/inetd.conf file entries will be created automatically when MC/ServiceGuard is installed. The /etc/inetd.sec file should be used, and should be configured so that each cluster node is allowed to access the hacl-cfg and hacl-probe services. The loopback address (127.0.0.1) should also be specified for these services.

MC/ServiceGuard interacts with the kernel hard clock safety timer through a device file, /dev/kepd. The safety timer is reset on each node when a heartbeat signal is sent to the other nodes. If the system hangs, or for some other reason the heartbeat signal cannot be sent for an extended period of time, a timeout value will be exceeded and the kernel hard clock safety timer will cause the node to perform a Transfer of Control, or to fail and attempt to reboot. This is to prevent more than one node from attempting to run the application package due to a loss of communication between the nodes. This device file must not be deleted or modified.

The same care should be taken when reviewing system log files on all cluster nodes, since a compromise on one node may also compromise the other cluster nodes. Where possible, use of a remote consolidated logging server should be considered. This has the advantage of providing a single location for analyzing log file entries, and it also reduces the possibility that an intruder could cover his tracks by altering the log files.

MC/ServiceGuard also logs information in a variety of places. Cluster related information that is logged goes to syslog.log. Package related information is logged to a file that is usually in the same directory as the package control file. Debugging information may be requested through different means, depending on the type of information wanted, and this information may be written to additional files. All of these log files should be monitored to assure that their permissions are set appropriately to prevent unnecessary information being made available to unauthorized users. Additionally, their sizes should also be monitored to prevent a growing log file from causing a denial of service.

Additional Security Issues and Solutions for ServiceGuard Manager

ServiceGuard Manager is another software tool available from Hewlett-Packard at no cost. This is a GUI based tool, with versions for HP-UX, Linux and Windows, used to display and manage MC/ServiceGuard clusters. All three versions can be downloaded from http://www.software.hp.com/HA_products_list.html. ServiceGuard Manager makes it easy to see the status of all objects that comprise the MC/ServiceGuard cluster, and can be utilized by any user that is authorized to view the status of the cluster. The root user can also manipulate the status of objects. This useful tool also carries with it a few more security considerations.

When ServiceGuard Manager is run, the user logs on to an Object Manager server. This could be the system running ServiceGuard Manager, or one of the MC/ServiceGuard cluster nodes, or an entirely different system. In order for ServiceGuard Manager to access information on a cluster, the Object Manager host system must be included in either /etc/cmcluster/cmclnodelist or the user's .rhosts file on each cluster node. As above, if the cmclnodelist file exists, this is the only mechanism used to validate the user. Clearly, host names should be entered into cmclnodelist with as much caution as entering them into .rhosts. Although cmclnodelist does not authorize root access for other than MC/ServiceGuard information and commands, by running ServiceGuard Manager on an authorized Object Manager node a user who knows the root password on that node could affect the operation of packages or the cluster itself.

On the positive side, when a user logs in to the Object Manager, the supplied password is encrypted before it is sent to the host for validation. On the negative side, the password can be saved on the client. Even though this is stored in encrypted form, saving passwords, especially for the root user, is almost always a bad idea. Someone who has compromised the client would be able to gain control over the MC/ServiceGuard cluster and its applications.

ServiceGuard Manager opens a log file on the computer that initiated the ServiceGuard Manager session. Levels of logging may be specified. Old log files are not automatically deleted. As mentioned above, log files that are not protected can be a source of information for unauthorized users, and log files that are allowed to grow unchecked can consume available disk space and result in a denial of service.

Additional Security Issues and Solutions for Extended Distance Clusters

Typically, nodes in an MC/ServiceGuard cluster reside in the same data center. In the event that geographically dispersed systems are required, this can be accomplished by configuring what Hewlett-Packard calls an Extended Distance Cluster, Metropolitan Cluster, or Continental Cluster. Separating potential hosts for an application into different data centers, or possibly even different cities, may allow for the continued availability of the application during disaster situations like fire or flood. It also adds to the list of security concerns. The configuration of these clusters require data to be available in the different locations, either through disk mirroring or replication. This potentially exposes the data to

unauthorized access in each location where it is kept. Physical security for the facilities, systems and backup media in all locations is critical.

Multiple host sites also complicate the maintenance of all security related topics. Coordination of efforts between different operations staffs will most likely be required to assure that patches are maintained at the same level for all potential applications hosts. It is even more likely that the hosts residing in different data centers from the primary host will have other tasks to run while the critical application is on the primary host. Coordination between the operations staffs, and possibly between different groups of applications administrators will also be required to keep the enabled and disabled network services as similar as possible in the different locations. Reviewing of log files is another issue to be worked out between the operations staffs. Finally, the issue of synchronization of users' passwords also is made more complex by the physical separation of the hosts.

Summary

MC/ServiceGuard software allows critical applications to be made highly available. It should not be overlooked that the use of this software to provide multiple potential hosts for these applications also creates additional security concerns.

Any security review involving the primary host of the application should also be done on the adoptive hosts. Any implementation of techniques for securing the primary host should be also be applied to the adoptive hosts. Adoptive hosts may require differences from the primary host based on other tasks that they perform. These differences should be evaluated with care to assure that they do not leave the adoptive host more vulnerable than the primary.

Functions such as the starting, stopping, and monitoring of the application that are under the control of MC/ServiceGuard are performed differently than they would be without the use of MC/ServiceGuard. This means that any security review of the application host must be done in a way that considers these differences.

Finally, there are aspects of the operation of MC/ServiceGuard itself, and tools such as ServiceGuard Manager, that create their own security considerations. Care must be taken to assure that increasing the availability of a critical application by implementing MC/ServiceGuard does not increase the vulnerability of that same critical application.

References

Hewlett-Packard Company. Managing MC/ServiceGuard. 9th ed. Hewlett-Packard, 2002. URL: http://docs.hp.com/hpux/pdf/B3936-90065.pdf

---. Managing Systems and Workgroups: A Guide for HP-UX System Administrators. 5th ed. Hewlett-Packard, 2001.
URL: http://docs.hp.com/hpux/pdf/B2355-90742.pdf

Skagen, Martin and Walt Jones. "How-to" Secure HP-UX 11i for use in a DMZ Environment. Version 1.6. White Paper, 2002

Wong, Chris. HP-UX 11i Security. Upper Saddle River: Prentice Hall, 2002

"hp-ux secure shell". Internet and Security Solutions. 2003.
URL: http://www.software.hp.com/ISS_products_list.html

"IT Resource Center". 2003. URL: http://www.itrc.hp.com/

"SANS Information Security Reading Room". December 5, 2002.
URL: http://www.sans.org/rr/unix/

"security patch check". Internet and Security Solutions. 2003.
URL: http://www.software.hp.com/ISS_products_list.html

"serviceguard manager". High Availability. 2002.
URL: http://www.software.hp.com/HA_products_list.html

"The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus". Version 3.21. October 17, 2002.
URL: http://www.sans.org/top20/

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor