Configuring Bastille to Operate with Ignite-UX

Table of Contents

Abstract

Ignite-UX for HP-UX addresses the need for system administrators to perform operating system installations, deployment, and recovery, often on a large scale. It provides the means for creating and reusing standard operating system configurations. Additionally, Ignite-UX delivers the ability to archive operating system configurations, and to use these archives to replicate systems, with the added benefit of speeding up the process. Ignite-UX also permits various customizations, and is capable of both interactive and unattended operating modes.

HP-UX Bastille 2.1 is a security hardening/lockdown tool that can be used to enhance the security of the HP-UX operating system. It provides customized lockdown on a system-by-system basis by encoding functionality similar to the Bastion Host and other hardening/lockdown checklists.

The new Bastille technology, available in HP-UX 11i v2, presents some unique considerations when utilizing it simultaneously with Ignite-UX. This document discusses these considerations and the steps necessary to achieve coexistence.

Introduction

Remote operating system installation (ignition), recovery, and all other features of Ignite-UX, require services like `rcp`, `remshd` services for remote execution, and the ability to operate in a `chroot` environment.

In contrast, Bastille configures daemons and system parameters, and sets up an IPFilter-based firewall to increase system security. Additionally, unneeded services such as `pwgrd` and printing are turned off, and client software such as `rcp` and `rlogin` are configured to be more secure. Bastille also helps create *`chroot` jails* that help limit the vulnerability of common Internet services such as Web servers and Domain Name Service (DNS).

Given that these two products operate in diametrically opposite manners, there are additional configuration steps that must be executed on the Ignite-UX server to modify the default Bastille configuration for each of the three levels of security provided. Once Bastille is modified on your Ignite-UX server, each client must be altered to modify the Bastille configuration to use the Ignite-UX functionality.

All of the configuration processes in this document modify the standard Bastille security level settings and careful consideration should be given on the impact to your network security when modifying the protocols and ports that are enabled.

Configuring Bastille on Ignite-UX Servers

Each of the procedures in this section modifies the Bastille security levels on the Ignite-UX server, and requires changes to Bastille, and IPFilter.

Choose the procedure that is applicable to the Bastille security level at which the Ignite-UX server is currently set from the following sections.

Bastille Level 10 Configuration

Note: If Bastille is being run for the first time, you may be required to enter, "accept”, when prompted to complete the installation.

Steps:

1. Change directories into the Bastille management directory:

```
cd /etc/opt/sec_mgmt/bastille
```

2. Copy the HOST.config file into config:

```
cp -p HOST.config config
```

The config file is used by Bastille to configure the lockdown measures on the Ignite-UX server.

3. Edit the config file and change the following three values from "Y" to "N":

```
  – # Q: Would you like to deactivate the NFS server on this system?  [Y]

MiscellaneousDaemons.nfs_server="N"

# Q: Should Bastille ensure inetd's bootp service does not run on this
system?
SecureInetd.deactivate_bootp="N"

# Q: Should Bastille ensure inetd's TFTP service does not run on this
system?
SecureInetd.deactivate_tftp="N"
```

4. To start Bastille with the modified config file, enter:

```
bastille -b
```

Bastille Level 20 or Level 30 Configuration

Note:

– An Ignite-UX server must also be a Network File System (NFS) server. NFS dynamically uses the standard high RPC ports from the range between 49152 through 65535 when igniting a client.

– See Ignite-UX Server Network Ports on page 5 for more information regarding the ports discussed in this procedure.

Steps:

1. Change directories into the Bastille management directory:

```
cd /etc/opt/sec_mgmt/bastille
```

2. Add the port information required by IPFilter by editing the file, ipf.customrules.

3. NFS conversations using network ports are sometimes fragments and these conversations are over UDP so the words, `keep frags`, must be added to the end of third line of `ipf.customrules` as in the following example:

```
pass out quick proto udp all keep state keep frags
```

4. Remove, or comment out, the last line in the file that reads as follows:

```
block in quick proto udp from any to any port = portmap
```

This ensures that `rpcbind` is running and are ready for use by NFS, as described in How Network Ports Are Used.

5. Then look for the message:

```
# End allow outgoing rules

#####################################################
```

Then insert the following lines:

```
# ports required for Ignite-UX
#####################################################
pass in log quick proto udp from any to any port = 69 keep state
pass in log quick proto udp from any port = 68 to any port = 67 keep state
pass in log quick proto tcp/udp from any to any port = 111 keep state
pass in log quick proto tcp from any to any port = 135 keep state
pass in log quick proto udp from any port = 1068 to any port = 1067 keep
state
pass in log quick proto tcp/udp from any to any port = 2049 keep frags
pass in log quick proto tcp from any to any port = 2121
pass in log quick proto tcp/udp from any to any port 49152 >< 65535
pass in log quick proto tcp from any to any port = 20
pass in log quick proto tcp from any to any port = 21
pass in log quick proto tcp from any to any port = 514
pass in log quick proto icmp from any to any icmp-type 8 keep state
pass in log quick proto tcp from any port = 514 to any keep state
pass in log quick proto tcp from any port = 1023 to any keep state
```

The additional lines are the *rules* to Bastille uses to open the necessary network ports. The `icmp-type 8` rule allows the Ignite-UX server to ping clients.

6. Copy the appropriate configuration file into `config` by choosing one of the following commands:

–

for level 20 – `cp -p MANDMZ.config config`

or

for level 30 `cp -p DMZ.config config`

The `config` file is used by Bastille to configure the server lockdown measures.

7. Edit the `config` file and change the following three values from "`Y`" to "`N`":

```
– # Q: Would you like to deactivate the NFS server on this system?  [Y]

MiscellaneousDaemons.nfs_server="N"
```

```
# Q: Would you like to deactivate NIS client programs?  [Y]

MiscellaneousDaemons.nis_client="N"

# Q: Should Bastille ensure inetd's bootp service does not run on this
system?
SecureInetd.deactivate_bootp="N"

# Q: Should Bastille ensure inetd's TFTP service does not run on this
system?
SecureInetd.deactivate_tftp="N"
```

8. To start Bastille with the modified `config` file, enter:

```
bastille –b

–
```

Ignite-UX Server Network Ports

The following describes the network ports that may be used on the Ignite-UX server by Bastille and Ignite-UX, and are applicable to Bastille security levels 20 and 30.

Table 1

Port/Port Range	Service/ Application	Protocol	Description
20	`ftp`	TCP[1]	File Transfer Protocol: Data
21	`ftp`	TCP	File Transfer Protocol: Control
67	`bootpd`	UDP[2]	Bootstrap Protocol Server - This service should function only if the server is a `bootp`/DHCP server. If it is not, disable the service in the `/etc/inetd.conf` file.
68	`bootpd`	UDP	Bootstrap Protocol Client - This service should function only if the server is a bootp server. If it is not, disable the service in the `/etc/inetd.conf` file.
69	`tftpd`	UDP	Trivial File Transfer Protocol - Found on systems that have Ignite-UX installed. This service should function only if the host is being used as a `tftp` server. If you want to disable this service, edit the `/etc/inetd.conf` file.
111	`portmap/sunrpc/ rpcbind`	TCP/UDP	SUN Remote Procedure Call (RPC)
135	`rpcd/dced`	TCP	Distributed Computing Environment (DCE)-based RPC
514	shell	TCP	Remote Command, No Password Used
1067	`instl_boots`	UDP	Installation Bootstrap Protocol Server - Part of the Ignite-UX service. You can disable this service in the `/etc/inetd.conf` file.

[1] Transmission Control Protocol
[2] User Datagram Protocol

Port/Port Range	Service/ Application	Protocol	Description
1068	`instl_bootc`	UDP	Installation Bootstrap Protocol Client - Part of the Ignite-UX service. You can disable this service in the `/etc/inetd.conf` file.
2049	`nfsd`	TCP/UDP	NFS Remote File System
2121	`swagentd`	TCP/UDP	HP Software Distributor Daemon - Used for communication between systems for software installation, listing, or other sw commands.
4000 - 4009	secure `swagent` ports	TCP/UDP	The `swagent` firewall configurable ports.
49152 - 65535	Dynamic or Private Ports	TCP/UDP	Dynamic and Private Ports are used by many applications for dynamic port assignments. UDP ports in this range are often RPC ports.

How Network Ports Are Used

In a normal configuration, Ignite-UX requires that the Ignite-UX server be an NFS server for the following reasons:

1) To allow recovery archives to be placed onto the system (from `make_net_recovery`).
2) To allow clients to write configuration files while creating recovery archives.
3) To allow clients to read configurations and write temporary files during install or recovery.

– Ignite-UX Servers and any Ignite-UX boot helpers must be configured as a `tftp` server to allow the Ignite-UX environment to be loaded on clients during install or recovery

An Ignite-UX server may serve as a boot server or this functionality may be disabled and a boot server used to provide this functionality on another computer on the same network for security reasons. Normally boot servers are used only to boot clients on a different network from the Ignite-UX server.

An Ignite-UX boot helper must provide `bootp` support. An Ignite-UX server must provide `bootp` support if it is to serve as a boot server.

Ignite-UX clients do not require access to all of the other network ports listed in Table 1 depending on which network services the Ignite-UX server is configured to use. For example, if you install clients using SD-UX you do need to allow access to SD-UX ports, or if you use the `ftp` transfer method for archives you will need to allow access to the `ftp` ports.

Configuring Bastille on Ignite-UX Clients

Each of the procedures in this section modifies the Bastille security levels on each Ignite-UX client and each requires changes to: Ignite-UX, Bastille, and IPFilter. These configuration modifications facilitate ignition, media booting, and recovery operations. It is important to note that the configurations described in this section must be performed on each client where Ignite-UX and Bastille are to coexist.

Choose the procedure that is applicable to the security level at which the Ignite-UX client is currently set from the following sections:

Bastille Level 10 Configuration

Note:

- Ensure that the Bastille Level 10 Configuration procedure of

Configuring Bastille on Ignite-UX Servers, on page 3, has been performed on your Ignite-UX server.

- If Bastille is being run for the first time, you may be required to enter, "`accept`", when prompted to complete the installation.

Steps to be executed on each client:

1. Change directories into the Bastille management directory:

```
cd /etc/opt/sec_mgmt/bastille
```

2. Copy the `HOST.config` file into `config`:

```
cp –p HOST.config config
```

The `config` file is used by Bastille to configure the lockdown measures on the client.

3. To allow the client NFS access to the Ignite-UX server, edit the `config` file and change the following value from "Y" to "N":

```
  – # Q: Would you like to deactivate the NFS client daemons?  [Y]
MiscellaneousDaemons.nfs_client="N"
```

4. To start Bastille with the modified `config` file, enter:

```
bastille –b
```

Steps to be executed on the Ignite-UX server for each client:

1. Create a directory for the client, such as `client1`, on the Ignite-UX server:

```
mkdir -p /var/opt/ignite/recovery/archives/client1
```

2. Change the ownership of this directory to `bin:bin`:

```
chown bin:bin /var/opt/ignite/recovery/archives/client1
```

3. Edit `/etc/exports` and add an entry for `client1`:

```
/var/opt/ignite/recovery/archives/client1 root=client1,access=client1
```

4. Export the newly created `client1` directory, enter:

```
exportfs -av
```

–

Bastille Level 20 or level 30 Configuration

Note:

- Ensure that the Bastille Level 20 or Level 30 Configuration procedure of Configuring Bastille on Ignite-UX Servers, on page 3, has been performed on your Ignite-UX server.
- If Bastille is being run for the first time, you may be required to enter, "`accept`", when prompted to complete the installation.

Steps to be executed on each client:

1. Change directories into the Bastille management directory:

```
cd /etc/opt/sec_mgmt/bastille
```

2. Copy the appropriate configuration file into `config` by choose one of the following commands:

–

for level 20 – `cp -p MANDMZ.config config`

or

for level 30 `cp -p DMZ.config config`

The `config` file is used by Bastille to configure the client lockdown measures.

3. Ignite-UX server management (or control) of clients requires NFS client services to be enabled and is accomplished by executing the following steps:

   A. Edit the `config` file and change the following value from "`Y`" to "`N`":

```
  – # Q: Would you like to deactivate the NFS client deamons?
    [Y]
MiscellaneousDaemons.nfs_client="N"

# Q: Should Bastille ensure that the login, shell, and exec
services do not run on this system?
SecureInetd.deactivate_rtools="N"
```

   B. Edit the `ipf.customrules` file and add the words, `keep frags`, to the end of third line as in the following example:

```
pass out quick proto udp all keep state keep frags
```

   Then look for the message:

```
# End allow outgoing rules

####################################################
```

   Then insert the following lines:

```
# ports required for Ignite-UX
####################################################
pass in log quick proto icmp from any to any icmp-type 8 keep stat
pass in log quick proto tcp from any to any port = 512
pass in log quick proto tcp from any to any port = 514
pass in log quick proto tcp/udp from any port = 2049 to any keep frags
pass in log quick proto tcp/udp from any to any port 49152 >< 65535
```

   The additional lines are the *rules* to Bastille uses to open the necessary network ports. The `icmp-type 8` rule allows the client to be pinged by the Ignite-UX server. This functionality also requires `login`, `shell`, and `exec` services are enabled so that remote commands controlling client operations from the Ignite-UX server can be performed.

4. To start Bastille with the modified `config` file, enter:

```
bastille –b
```

This allows the client to be ignited, booted, and recovered via the network.

–

Steps to be executed on the Ignite-UX server for each client:

1. Create a directory for the client, such as `client1`, on the Ignite-UX server:

```
mkdir -p /var/opt/ignite/recovery/archives/client1
```

2. Change the ownership of this directory to `bin:bin`:

```
chown bin:bin /var/opt/ignite/recovery/archives/client1
```

3. Edit `/etc/exports` and add an entry for `client1`:

```
/var/opt/ignite/recovery/archives/client1 root=client1,access=client1
```

4. Export the `client1` directory, enter:

```
exportfs -av
```

–

Ignite-UX Client Network Ports

The following client network ports are used by Bastille security levels 20 and 30.

Table 2

Port/Port Range	Service/Application	Protocol	Description
512	– `exec`	TCP	Remote Execution
514	`shell`	TCP	Remote Command, No Password Used
2049	`nfsd`	TCP/UDP	NFS Remote File System
49152 - 65535	Dynamic or Private Ports	TCP/UDP	Dynamic and Private Ports are used by many applications for dynamic port assignments. UDP ports in this range are often RPC ports.

For More Information

The following relevant documents are available online at the HP Technical Documentation Web site at:

http://www.docs.hp.com/:

- *Ignite-UX Administration Guide*
- *HP-UX 11i v2 Installation and Update Guide*
- *HP-UX 11i Version 2 Release Notes*
- *Managing Systems and Workgroups*
- *Installing and Administering HP-UX IPFilter*
- *HP-UX Networking Ports Reference Guide*

Some or all of these documents are available on the Instant Information media and in printed form.

The *Bastille User's Guide* is delivered in `/opt/sec_mgmt/bastille/docs/user_guide.txt`.

The *Building a Bastion Host Using HP-UX 11* Technical White Paper is available at:

http://www.hp.com/products1/unix/operating/infolibrary/whitepapers/building_a_bastion_host.pdf

Product information regarding Ignite-UX for HP-UX is available at the HP Software Depot at:

http://www.docs.hp.com/en/IUX/

Product information regarding HP-UX Bastille and HP-UX IPFilter is available at the HP Software Depot at:

http://www.software.hp.com/ISS_products_list.html

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.

MPN 5991-0734, 12/2005