Novell AppArmor Powered by Immunix Installation and QuickStart Guide

www.novell.com

1.2 | 09/29/2005

Novell AppArmor Powered by Immunix 1.2 Installation and QuickStart Guide

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

AppArmor is a registered trademark of Novell, Inc. in the United States and other countries.
Immunix is a trademark of Novell, Inc. in the United States and other countries.
Novell is a registered trademark of Novell, Inc. in the United States and other countries.
SUSE is a registered trademark of SUSE LINUX Products GmbH, a Novell business.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

1 Introduction to Novell AppArmor

Many security vulnerabilities result from bugs in *trusted* programs. A *trusted* program runs with privilege that some attacker would like to have and the program fails to keep that trust if there is a bug in the program that allows the attacker to acquire that privilege.

Novell AppArmor is an application security solution designed specifically to provide least privilege confinement to suspect programs. AppArmor allows the administrator to specify the domain of activities the program can perform by developing a security *profile* for that application—a listing of files that the program may access and the operations the program may perform.

Effective hardening of a computer system requires minimizing the number of programs that mediate privilege then securing the programs as much as possible. With Novell AppArmor, you only need to profile the programs that are exposed to attack in your environment, which drastically reduces the amount of work required to harden your computer. AppArmor profiles enforce policies to make sure that programs do what they are supposed to do, but nothing else.

Administrators only need to care about the applications that are vulnerable to attacks and generate profiles for these. Hardening a system thus comes down to building and maintaining the AppArmor profile set and monitoring any policy violations or exceptions logged by AppArmor's reporting facility.

Building AppArmor profiles to confine an application is very straightforward and intuitive. AppArmor ships with several tools that assist in profile creation. AppArmor does not require you to do any programming or script handling. The only task that is required from the administrator is to determine a policy of strictest access and execute permissions for each application that needs to be hardened.

Updates or modifications to the application profiles are only required if the software configuration or the desired range of activities changes. AppArmor offers intuitive tools to handle profile updates or modifications.

Users will not notice AppArmor at all. It runs “behind the scenes” and does not require any user interaction. Performance will not be affected noticeably by AppArmor. If some activity of the application is not covered by an AppArmor profile or if some activity of the application is prevented by AppArmor, the administrator needs to adjust the profile of this application to cover this kind of behavior.

This guide outlines the basic tasks that need to be performed with AppArmor to effectively harden a system. For more in-depth information, refer to *Novell AppArmor Powered by Immunix 1.2 Administration Guide*.

2 Installing Novell AppArmor

Users installing either a GNOME or the KDE desktop selection can skip this section, because Novell® AppArmor is installed by default as part of these selections.

If installing neither of these desktops or even going for en entirely text-based environment, do the following to install the required packages using the YaST package manager.

1. Log in as `root` and start YaST.
2. In the YaST Control Center, select *Software* → *Software Management*.
3. Use the search functionality of YaST (keywords "AppArmor" and "subdomain") to install the following packages:

   - subdomain-parser-demo
   - subdomain-parser-common
   - libimmunix
   - libimnxcert
   - subdomain-docs
   - yast2-subdomain
   - subdomain-profiles
   - subdomain-leaf-cert
   - subdomain-utils

4 Select all these packages for installation then select *Accept*. YaST resolves any dependencies and installs all the packages for you.

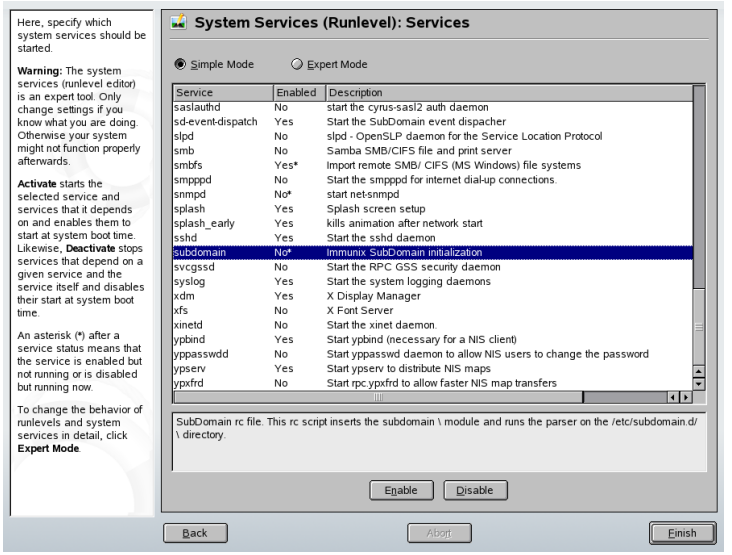
5 After YaST has finished updating the system configuration, select *Finish* to leave the package manager.

3 Enabling Novell AppArmor

After Novell® AppArmor has been installed, explicitly enable it to make sure that it is started whenever your system boots. Use the YaST System Services (Runlevel) module for this task:

1. Log in as `root` and start YaST.
2. Start *System* → *System Services (Runlevel)*.
3. In the list of services displayed, select `subdomain`. See Figure 3.1, “Enabling Novell AppArmor Using YaST” (page 12).
4. Click *Enable* to enable AppArmor permanently.
5. Click *Finish* to accept your settings.

Figure 3.1 *Enabling Novell AppArmor Using YaST*



Using the YaST Runlevel tool, you enable services permanently—these settings survive a reboot of your system. To enable AppArmor temporarily—for the duration of one session only—proceed as follows:

1. Log in as `root` and start YaST.
2. Start *Novell AppArmor → AppArmor Control Panel*.
3. Set the *AppArmor Status* to *AppArmor is enabled* by clicking *Configure → Enable → OK*.
4. Apply your settings with *Done*.

4 Getting Started with Profiling Applications

Prepare a successful deployment of Novell® AppArmor on your system by carefully considering the following items:

1. Determine the applications to profile. Read more on this in Section 4.1, “Choosing the Applications to Profile” (page 13).
2. Build the needed profiles as roughly outlined in Section 4.2, “Building and Modifying Profiles” (page 14). Check the results and adjust the profiles when necessary.
3. Keep track of what is happening on your system by running AppArmor reports and dealing with security events. Refer to Section 4.3, “Configuring Novell AppArmor Event Notification and Reports” (page 16).
4. Update your profiles whenever your environment changes or you need to react to security events logged by AppArmor's reporting tool. Refer to Section 4.4, “Updating Your Profiles” (page 18).

4.1 Choosing the Applications to Profile

You only need to protect the programs that are exposed to attacks in your particular setup, so only use profiles for those applications you really run. Use the following list to determine the most likely candidates:

Network Agents
: Programs (servers and clients) have open network ports and network agents are server programs that respond to those network ports. User clients (such as mail clients and Web browsers) also have open network ports and mediate privilege.

Web Applications
: CGI Perl scripts, PHP pages, and more complex Web applications can be invoked through a Web browser.

Cron Jobs
: Programs that the cron daemon periodically runs read input from a variety of sources.

To find out which processes are currently running with open network ports and might need a profile to confine them, run `unconfined` as `root`.

Example 4.1 *Output of unconfined*

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

Each of the processes in the above example labeled `not confined` might need a custom profile to confine it. Those labeled `confined by` are already protected by AppArmor.

TIP: For More Information

For more information about choosing the the right applications to profile, refer to Chapter *Selecting Programs to Immunize* (↑Novell AppArmor Powered by Immunix 1.2 Administration Guide).

4.2 Building and Modifying Profiles

Novell® AppArmor on SUSE Linux ships with a preconfigured set of profiles for the most important applications. In addition to that, you can use AppArmor to create your own profiles for a set of applications defined in `/etc/apparmor/README.profiles`.

There are two ways of managing profiles. One is to use the graphical front-end provided by the YaST Novell AppArmor modules and the other is to use the command line tools provided by the AppArmor suite itself. Both methods basically work the same way.

Running unconfined as described in Section 4.1, “Choosing the Applications to Profile” (page 13) identifies a list of applications that may need a profile to run in a safe mode.

For each application, perform the following steps to create a profile:

1. As `root`, let AppArmor create a rough outline of the application's profile by running `genprof programname`

   or

   running *YaST → Novell AppArmor → Add Profile Wizard* and specifying the complete path of the application to profile.

   A basic profile is outlined and AppArmor is put into learning mode, which means that it logs any activity of the program you are executing but does not restrict it, yet.

2. Run the full range of the application's actions to let AppArmor get a very specific picture of its activities.

3. Let AppArmor analyze the log files generated in Step 2 (page 15). Do this either by running typing S in genprof

   or

   clicking *Scan system log for AppArmor events* in the *Add Profile Wizard* and follow the instructions given in the wizard until the profile is completed.

   AppArmor scans the logs it recorded during the application's run and asks you to set the access rights for each event that was logged. Either set them for each file or use globbing.

4. Once all access permissions are set, your profile is set to enforce mode mode. The profile is applied and AppArmor restricts the application according to the profile just created.

   If you started genprof against an application that had an existing profile that was in complain mode, this profile will remain in learning mode upon exit of this

learning cycle. For more information on changing the mode of a profile, refer to Section “Complain or Learning Mode” (Chapter 3, *Building Novell AppArmor Profiles*, ↑Novell AppArmor Powered by Immunix 1.2 Administration Guide) and Section “Enforce Mode” (Chapter 3, *Building Novell AppArmor Profiles*, ↑Novell AppArmor Powered by Immunix 1.2 Administration Guide).

Test your profile settings by performing every task you need with the application you just confined. Normally, the confined program runs smoothly and you do not notice AppArmor activities at all. However, if you notice certain misbehavior with your application, check the system logs and see if AppArmor is too closely constricting your application. Find the appropriate logs in `/var/log/messages` or run `dmesg`.

Any output resembling the following example hints at AppArmor too closely confining your application:

```
SubDomain: REJECTING w access to /var/run/nscd/socket (traceroute(2050) profile
/usr/sbin/traceroute active /usr/sbin/traceroute)
```

To adjust the profile, run the *Add Profile Wizard* again as described above and let it analyze the log messages relating this particular application. Determine the access rights or restrictions when prompted by YaST.

TIP: For More Information

For more information about profile building and modification, refer to Chapter *Building Novell AppArmor Profiles* (↑Novell AppArmor Powered by Immunix 1.2 Administration Guide).

4.3 Configuring Novell AppArmor Event Notification and Reports

Set up event notification in Novell® AppArmor so you can review security events. Event Notification is an Novell AppArmor feature that informs a specified e-mail recipient when systemic Novell AppArmor activity occurs under the chosen severity level. This feature is currently available via the YaST interface.

To set up event notification in YaST, proceed as follows:

1. Make sure that a mail server is running on your system to deliver the event notifications.

2. Log in as `root` and start YaST. Then select *Novell AppArmor → AppArmor Control Panel*).

3. In *Enable Security Event Notification* section, select *Configure*.

4. For each record type (*Terse*, *Summary*, and *Verbose*) set a report frequency, enter the e-mail address to receive the reports and determine the severity of events to log. If you want to include unknown events in the event reports, check *Include Unknown Severity Events*.

   NOTE

   Unless you are familiar with AppArmor's event categorization, choose to be notified about events for all security levels.

5. Leave this dialog with *OK → Finish* to apply your settings.

Configure Novell AppArmor reports. Using reports, you can read important Novell AppArmor security events reported in the log files without manually sifting through the cumbersome messages only useful to the logprof tool. You can decrease the size of the report by filtering by date range or program name.

To configure the AppArmor reports, proceed as follows:

1. Log in as `root` and start YaST. Select *Novell AppArmor → AppArmor Reports*.

2. Select the type of report you want to examine or configure from *Executive Security Summary*, *Applications Audit*, and *Security Incident Report*.

3. Edit the report generation frequency, e-mail address, export format, and the location of the reports by selecting *Edit* and providing the requested data.

4. To run a report of the selected type, click *Run Now*.

5. Browse through the archived reports of a given type by selecting *View Archive* and specifying the report type.

   or

Delete unneeded reports or add new ones.

TIP: For More Information

For more information about configuring event notification in Novell AppArmor, refer to Section “Setting Up Event Notification” (Chapter 4, *Managing Profiled Applications*, ↑Novell AppArmor Powered by Immunix 1.2 Administration Guide). More information about report configuration can be found in Section “Reports” (Chapter 4, *Managing Profiled Applications*, ↑Novell AppArmor Powered by Immunix 1.2 Administration Guide).

4.4 Updating Your Profiles

Software and system configurations change over time. As a result of that your profile setup for AppArmor might need some fine-tuning from time to time. AppArmor checks your system log for policy violations or other AppArmor events and lets you adjust your profile set accordingly. Any application behavior that is outside of any profile definition can also be addressed using the *Update Profile Wizard*.

To update your profile set, proceed as follows:

1. Log in as `root` and start YaST.
2. Start *Novell AppArmor → Update Profile Wizard*.
3. Adjust access or execute rights to any resource or for any executable that has been logged when prompted.
4. Leave YaST after you answered all questions. Your changes are applied to the respective profiles.

TIP: For More Information

For more information about updating your profiles from the system logs, refer to Section “Updating Profiles from Syslog Entries” (Chapter 3, *Building Novell AppArmor Profiles*, ↑Novell AppArmor Powered by Immunix 1.2 Administration Guide).