close window

IBM Systems magazine

e-Newsletter Exclusive

Print

New AIX v7 Features Enhance System Security

August 2011 | by Jaqui Lynch

With AIX v6.1, IBM introduced several new security features, including enhancements to role-based access control (RBAC), Encrypted File System (EFS), Trusted AIX and AIX Security Expert. It also added the Secure by Default installation option, Trusted Execution and the filesystem access tool for set-user ID (SUID).

In AIX v7, IBM has again focused on enhancing these security options with features like domain-based RBAC, enhanced encryption for EFS, Internet protocol security (IPSec) and Trusted Execution, as well as other updates for Common Criteria CAPP/EAL4+ security certification. Let's take a closer look at updates to AIX Security Expert, RBAC and Secure by Default installation.

AIX Security Expert

First introduced at AIX v5.3 tl05, AIX Security Expert was significantly enhanced in AIX v6 and v7. It consists of policy-based rules that can be implemented on your system simply by setting the level to one of the default options—low, medium, high or Sarbanes Oxley (SOX). The SOX option was added in AIX v6 and provides password policy enforcement, violation and security activity reports, firewall architecture and malicious software prevention. For example, SOX requires turning on auditing, and it disables all direct root userid logins. It also turns on IPSec and enables filter rules that prevent port scans.

It's important to note that medium, high or SOX security disables many network-level functions and other applications, so this should be tested thoroughly, first. For instance, setting the level to "high" disables rlogin, FTP and telnet. Therefore, OpenSSH should be configured and tested prior to using this setting.

AIX Security Expert controls more than 300 settings from one interface with templates provided as a starting point, which can then be customized. Once levels are set, it's possible to build an XML file of the policies that can be used for future consistency checking. This file can also be exported to other systems, so they can be set the same, or the settings can be loaded into Lightweight Directory Access Protocol (LDAP) for propagation across systems.

Role-Based Access Control

In AIX v6 the major change to access control was the implementation of enhanced RBAC. It allows administrators to grant authorization for management of specific resources to users other than root, or to assign specific management privileges with programs, reducing the need to run those programs under the root user or via setuid. The idea is to delegate routine administrative tasks to nonroot users and thus to reduce the number of root users required to manage systems.

Additionally, enhanced RBAC is required for the implementation of workload partitions (WPARs) and is now the default when the system is installed. The new RBAC allows specific roles to be allocated, and replaces and enhances many of the functions provided by tools such as sudo. It is now possible to set and control privileges for processes, files and devices. At login time, no role is assigned so the user has no real privileges by default. Instead, the swrole command is used to switch into the correct role so that the user can then perform the privileged commands they need to do. This allows you to have multiple administrators and to provide tiered security levels, based on the functions a user needs to perform. Additionally, since everyone uses their own account and no one logs on as root, you can provide a full accounting of who did what and when; something required by auditors.

RBAC has three key elements—authorizations, roles and privileges. Authorizations are used to grant access to commands or functions that one needs to perform. There are a several predefined system authorizations that start with AIX at the top level. If you've been using RBAC in earlier releases, the authorizations will need to be migrated to the new format. Roles are assigned to a user and act as a container for a set of authorizations. Privileges are used to grant the power to a process to perform certain privileged operations. When users issue a swrole, they receive the authorizations and privileges assigned to that role, and they receive the necessary access. Once they switch out of that role, the authorizations and privileges are removed.

While it is possible to have all the RBAC information stored in an LDAP database the default files are in /etc/security and are called privfiles, privdevs, authorizations, privcmds and roles. Keep in mind, the system expects the files, etc., that privileges are being set for already exist. Additionally, privileges are now granted by the kernel so it's important to update the kernel security table once changes are made. This is done using the setkst command. Useful commands to research are: lsrole ALL, lssecattr, swrole, ls -ltra, and swrole.

Within AIX v7, RBAC is enhanced to provide domain support. This enables you to restrict administrative access to a specific set of similar resources, such as a subset of the available network adapters. This can be used to restrict administrator access to only the resources associated with a particular LPAR. Domains can be used to control access to volume groups, filesystems, files and devices. Domains were introduced in AIX v7 and are now available in AIX 6 Technology Level 6.

Secure by Default (SBD)

SBD is an installation option that ensures the system is only installed with a minimum group of filesets (about 100). This ensures that when the system comes up, it has good security. Most of the network filesets are not installed, so they must be installed individually once you determine which are needed. The intent is to have the absolute minimum filesets needed to run AIX, thus minimizing security risks. This security approach allows you to get nothing until you explicitly add it. In this case, it means that additional filesets will need to be explicitly added later in order to provide functionality beyond a fairly minimal system. SBD works best when used in combination with AIX Security Expert to tightly control the security configuration of each system.

More Secure, Less Effort

These three AIX v7 enhancements—when combined with a layered security plan that includes network security, firewalls and SSH—enables a high level of security. The AIX Security Expert can ensure consistent implementation of security options across all systems with minimal administrative effort.

Resources

1. AIX Strength to Strength Brochure
2. AIX v7 Data Sheet
3. AIX v7 Security Expert
4. AIX v7 Information Center—General Security
5. AIX v6 Advanced Security Features