zmanda

Amanda Enterprise **Whitepaper**

Top considerations for implementing secure backup and recovery

A best practice whitepaper
by Zmanda

In the last few years there have been many headlines about high-profile incidents of lost or stolen backup tapes. Despite increasing attention to security, backup procedures are often neglected in overall security policies. The main reason for that discrepancy is that, historically, backup and security have had almost opposite goals. Security procedures often require strong access control to user's data. Backup software, however, is optimized to simplify recovery, sometimes to a different platform or different location and often by someone other than the original owner of the data.

Using the example of the most popular open source backup and recovery software, Amanda Enterprise, we will review best practices for ensuring security of backup data. Specifically, we will review the following aspects of backup security:

- Authentication of users and backup clients to the backup server.
- Role based access control lists for all backup and recovery operations.
- Data encryption options for both transmission and storage.
- Flexibility in choosing encryption and authentication algorithms, for example, aespipe or gpg.
- Backup of remote clients to a centralized location behind firewalls.
- Backup and recovery of clients running Security-Enhanced Linux (SELinux).
- Using best practices to write secure software

Are your systems really contacting the correct backup server?

Most data centers rely on network-based backup. In order to do this securely, there must be a trust relationship established between the backup client (the machine being backed up) and the backup server (the machine doing the backup). Without a verifiable way to establish this trust relationship various "man-in-the-middle" attacks can occur.

One possible vulnerability is the case where backup software allows the backup client to specify that any backup server may initiate a backup. Unlike Amanda Enterprise, some popular closed-source backup tools ship with this setting as a default. Unless you are aware of this vulnerability and change the default setting, anyone with a laptop or desktop computer can install the trial version of the backup package and initiate backup of any backup client in your organization. These backups could then easily be directed to the disk of a rogue backup server.

A similar concern exists in the opposite direction. Is your backup server providing data for recovery to the appropriate system? Or is someone forcing a system to masquerade as a backup client?

A much better approach is requiring that backup software uses strong authentication of both the backup client and the backup server. Of course the method of authentication should also be open to scrutiny. A good choice would be a key-based mechanism, similar to the one offered by the open source tool openssh (http://www.openssh.com).

Can your backup data be compromised when it travels the network or if your backup tape "falls off the truck"?

It does no good if your client and server authenticate each other, only to find out that someone has intercepted the backup data. This is especially important if your backup data travels over an unsecured network, such as over the Internet from a regional office to headquarters.

Over the past few years there have been well-publicized events where companies lose track of their backup tapes. Often these involve the loss of sensitive financial information. In one such incident in 2005, a well-known time-share company lost backup tapes with sensitive financial information for 260,000 of its customers. Obviously the potential damage to the customers was huge, as well as the damage to the time-share company and its reputation.

Your backup software should provide flexibility to encrypt data in transit before it is sent on a wire, or at rest when data is written to the backup media. It should use freely-available, verifiable methods of encryption. You should also have the option to use different encryption methods and take advantage of new developments and encryption algorithms.

There are hardware-based solutions. Both Network Appliance's Decru division, and Neoscale offer hardware appliances that intercept writes to backup media (tape) and encrypt it on the fly. This has the advantage of speed, but comes at a high infrastructure cost.

Amanda Enterprise has the ability to encrypt the data either on the client, prior to transmission to the backup server, or on the backup server itself. Both client- and server-side encryption can use any encryption program that reads from standard input and writes to standard output. This includes the aespipe command, which supports a variety of AES encryption routines. Another commonly used tool with

Amanda Enterprise encryption program is gpg.

Of course, without good key management the data cannot be recovered. Amanda Enterprise does not provide a key management solution on its own but rather works with any key management solution mandated by your IT policy.

The openness and flexibility of encryption options allows Amanda Enterprise to fit well into security policies and processes of most IT environments including organizations with strict security requirements.

Who has control over your backups and recoveries?

These days there are a variety of people that must participate in configuring and using backup and recovery software. In larger enterprises it is not unusual for help desk staff to approach dozens of individuals. Often these personnel need to be given some authority over data recovery operations.

It is wise to choose a backup program that lets you delegate authority to individuals, as long as it provides a fine level of granularity. If your backup and recovery system does not have a fine level of granularity then you are exposed to the possibility of recovery abuses. Most backup and recovery packages have the concept of administrators. These administrators often have global privileges and can recover anyone's data. This might include highly sensitive data, such as payroll or financial records.

Amanda Enterprise takes a better approach. It lets you create roles for each operator, limiting what data they have access to. This lets you segregate sensitive data to ensure that only those with an absolute need to recover the data have the ability to do so.

Can you backup through a firewall?

Today's data center environments often include the use of firewalls even internally to protect corporate computers from attack. Your backup server will almost invariably be behind your corporate firewall. The question arises - how do you backup those computers on the other side of a firewall?

One solution is to deploy a second backup server on the appropriate side of the firewall. However, this is not always feasible or desirable. This increases security concerns, rather than reducing them. A better solution is for your backup client and server software to use well-defined (but changeable) ports to communicate. You can then configure your firewall to allow traffic from known IP addresses through the firewall to allow backup and restore traffic through.

A consideration about this approach is the number of ports the backup software requires. Your backup software should not use too many ports, since it is difficult enough to get one or two ports opened up in your firewall. Some commercially available closed-source backup products use dozens of ports per backup server.

Amanda has the ability to use a few administrator-defined ports for the backup server and client to communicate with. This ability makes it well-suited to backup through a firewall.

Support for Security Enhanced Operating Systems such as SE Linux

Security-Enhanced Linux (SELinux) is a Linux variant that implements a variety of security policies, including U.S. Department of Defense style mandatory access controls, through the use of Linux Security Modules (LSM) in the Linux kernel. Since Red Hat introduced SELinux with its Enterprise offerings, SELinux is now widely used in government, military and often commercial environments. Today there is no closed source backup vendor that supports SELinux. Amanda Enterprise, however, works with SELinux policies very well.

Is your backup software written with security in mind?

Backup software has configuration files that store passwords and access control rights not just for file servers but also for application and database servers. Make sure these configuration files are readable only by authorized users.

Everyone who uses a closed-source software product can only guess what is inside of it. Since the vendor does not make the code available for inspection it is very difficult to tell if the software is totally secure, or if there are "back doors" coded into the software such as infamous back door discovered in Microsoft IIS servers in 2000.

The United States Computer Emergency Readiness Team (US-CERT) issues the vulnerability alerts for commercial backup software all the time. For example, the Vulnerability Note VU#744137 alerts that in Symantec Veritas NetBackup software the catalog daemon contains a stack-based buffer overflow that could allow a remote attacker to execute arbitrary code on a NetBackup master server.

Open source, on the other hand, is almost impervious to this kind of problem. There is a built-in mechanism of peer review of the code that virtually insures that nothing that is unnecessary is included. No self-respecting open-source developer would risk his reputation and career by putting a back door into an

open source product. Even if such a back door were included, it would mostly likely be quickly found and removed.

Additionally, open source software can be easily inspected for both quality and security. There are both commercial and freely available open source tools for analyzing software code for security vulnerabilities. Some of these are:

- Rough Auditing Tool for Security (RATS)
- ITS4 by Cigital
- Flawfinder by David A. Wheeler

These tools are freely available, and able to scan a variety of programming languages. Bogosec (http://bogosec.sourceforge.net/index.html) is a wrapper around these tools, and can predict security concerns in software. However, without available source code for backup software, these tools are useless.

When it comes to information security these are very real concerns for any backup package. When selecting a backup package you have to make sure there are no known security flaws in the software. Amanda, the leading open source backup package, has been tested with a variety of tools and by several organizations. For example, Coverity (http://scan.coverity.com), a collaborative effort between Stanford University and the open source community, tested Amanda code quality. When bugs were discovered the Amanda community quickly corrected them and reduced the count to zero. This compares to an average defect rate of 20 to 30 bugs per 1000 lines of code for commercial software, according to Carnegie Mellon University's CyLab Sustainable Computing Consortium.

Backup Security Checklist

	Yes	No
Is there a strong authentication of backup server and backup clients?		
Is there encryption on a client for securing data in transit?		
Is there encryption on a backup server for securing data on a backup media, e.g. tape?		
Can you choose between different encryption methods and take advantage of new encryption algorithms?		
Is there role-based access control for administration, backup and recovery?		
Can you open just a few ports (ideally only one port) for backup through a firewall?		
Is there support for SELinux?		
Did you verify security of backup software configuration files that store passwords for file-, database- and application servers?		
Did you verify that US-CERT has no alerts about your backup software?		
Are there independent reports about quality and security of code for your backup software?		

Conclusion

Since your backup is a copy of your most valuable digital assets, backup security is a critical consideration. Implementing truly secure yet financially viable backup policies requires a thorough understanding of the associated trade-offs. However, any organization can find a reasonable compromise to establish secure backup policies that it can afford. The important thing to remember is that backup security is not a project, but a process that requires constant monitoring and improvement.

Now that you understand these concepts, we invite you to try Amanda Enterprise. Contact zsales@zmanda.com to request a demo.