

DirectoryLockdown™

Active Directory Security Monitoring and Intrusion Detection

Replication is the core process driving Active Directory's distributed architecture. It ensures that critical information stored in the directory replicates throughout the system, making it readily available to those who need it, where and when they need it.

With all the benefits achieved through replication, however, come some real risks. Active Directory administrators have the potential to subvert the system to gain access to critical Configuration and Schema naming contexts (NCs). Once they gain that access, the administrators can then make changes to the NCs and use replication to transmit those changes. So, in cases when an Active Directory administrator decides to maliciously attack the system or makes an infrastructure change by accident, replication can become the vector of his attack.

Ensuring the security of Active Directory and the information and resources it contains requires steadfast auditing and protection. Enter NetPro's DirectoryLockdown, the only solution available to help protect the directory from "rogue administrators" who assume the rights of highly trusted enterprise administrators in an attempt to subvert the system.

Flexible levels of protection.

DirectoryLockdown is the only security solution designed to mitigate certain types of Active Directory intrusions. DirectoryLockdown stands alone in its ability to detect the corruption of the enterprise-wide configuration information stored in Active Directory by monitoring the Configuration naming context 24x7. When DirectoryLockdown detects an intrusion, it offers two types of responses. Alert-Only Response will immediately notify the appropriate personnel of the intrusion via alert notifications, giving users the choice of how to proceed in protecting the

networking environment. For an extra level of automated protection, DirectoryLockdown's Complete Response will go a critical step further by preventing further damage to an enterprise by disabling replication to and from the compromised DC and shutting the DC down completely. With DirectoryLockdown's flexible response options, you get to choose the level of protection that's right for your environment.

Take back the keys with DirectoryLockdown.

Changes to the Configuration and Schema NCs have the potential to create denial of service problems, serious reliability and service access issues, and security breaches that make the entire network vulnerable to attack. In the worst-case scenario, changes to the Configuration or Schema NCs may also take down the entire network.

What exactly happens? When systems are unprotected by DirectoryLockdown, local Active Directory administrators have the power to alter the directory's replication topology, thereby altering replication schedules. Rogue administrators may also promote and demote global catalogs in an effort to overload the system, or set security on the containers so that users are denied access. In addition, rogue administrators could delete configuration settings to stop replication from occurring at all. In each case, the results can be crippling and may require dramatic recovery efforts. At best, recovering from an attack will require extensive troubleshooting by a well-trained directory engineer. At worst, recovery may require the restoration of every domain controller in the enterprise from a backup copy. Or, when backups are unavailable, a complete rebuild of the DCs from scratch may be the only option. The same results may occur in cases of administrator error or viruses.



*For more information about DirectoryLockdown,
visit www.netpro.com/products/directorylockdown
Or call today 800.998.5090.*

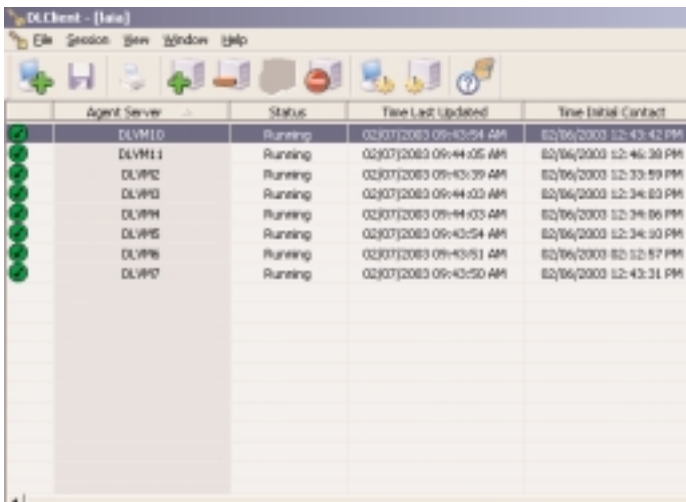
Raise the bar on intruders.

To avoid these consequences, the best line of defense is an ounce of prevention. While DirectoryLockdown does not stop intruders from compromising remote DCs, it significantly diminishes the potential damage of the attack by monitoring for changes and localizing those changes when they occur. And, with DirectoryLockdown, you're not only protecting your environment, you're also gaining unprecedented peace of mind because, at the first sign of trouble, you receive an alert and replication stops. Further, DirectoryLockdown's recovery tool ensures that recovery of the downed DC is fast, efficient and painless.

As one industry analyst put it: "When you have the keys to Active Directory, you have the keys to the kingdom." For companies with strict security requirements – including banks, insurance companies, military installations, and government agencies – this is a challenging concern. And, DirectoryLockdown is the only solution available today to address the issue. While it does not solve the entire problem, DirectoryLockdown provides a breakthrough solution for raising the bar on rogue administrators and devastating administrative errors, greatly enhancing the security of remote domain controllers. When combined with a well-conceived change control policy and strict security strategies, DirectoryLockdown is a vital tool for limiting exposure to the potentially devastating effects of rogue attack.

"When you have the keys to Active Directory, you have the keys to the kingdom."

*-- Al Gillen, Research Director
IDC*



Agent Server	Status	Time Last Updated	Time Initial Contact
DLVME0	Running	02/07/2003 09:43:54 AM	02/06/2003 12:43:42 PM
DLVME1	Running	02/07/2003 09:44:05 AM	02/06/2003 12:46:30 PM
DLVPE2	Running	02/07/2003 09:43:39 AM	02/06/2003 12:33:59 PM
DLVPE3	Running	02/07/2003 09:44:03 AM	02/06/2003 12:34:03 PM
DLVPE4	Running	02/07/2003 09:44:03 AM	02/06/2003 12:34:06 PM
DLVPE5	Running	02/07/2003 09:43:54 AM	02/06/2003 12:34:30 PM
DLVPE6	Running	02/07/2003 09:43:51 AM	02/06/2003 02:52:57 PM
DLVPE7	Running	02/07/2003 09:43:50 AM	02/06/2003 12:43:31 PM

DirectoryLockdown mitigates certain types of attacks on Active Directory by rogue administrators by monitoring the Configuration and Schema NC's 24x7.

NetPro . . . the experts behind DirectoryLockdown.

With a strategic combination of software solutions, conferences, and web resources, NetPro is revolutionizing the way companies manage their directories and driving the availability and performance of networks everywhere. NetPro delivers the only comprehensive suite of solutions designed to manage network

DirectoryLockdown at a glance...

- Monitors objects in the Configuration and Schema naming contexts on DCs 24x7
- Detects unauthorized changes to Configuration and Schema NCs on DCs
- Offers flexible response options: (1) Complete Response or (2) Alert-Only Response
- Alerts network management when a modification to the Configuration or Schema NC occurs on a DC
- Stops the replication to and from the DC where the intrusion occurred
- Prevents further changes of the Configuration and Schema replicas by shutting down the compromised DC
- Monitors and alerts on attempts to subvert the DirectoryLockdown system
- Includes recovery tool for fast and efficient DC recovery
- Features a MOM Management Pack and an HP OpenView Operations for Windows SmartLink

directory services for 24x7 availability throughout the directory lifecycle. Proactive directory management gives administrators the power to drive down costs, minimize downtime, and maximize income and resources. NetPro's partners include Microsoft Corp., Hewlett-Packard, and Novell Inc., and its customer list features such respected companies as DaimlerChrysler, Wells Fargo, Bank One, and General Motors. DirectoryLockdown is just one of the many software solutions that demonstrate our commitment to keeping the world's directories working. With support from Microsoft®, NetPro has added a five-product suite offering, the Secure Active Directory Lifecycle Suite, to its family of world-class directory management software.

For more information about DirectoryLockdown, visit our web site at www.netpro.com/products/directorylockdown. To order DirectoryLockdown today, call your nearest NetPro Authorized Reseller or NetPro directly at 800.998.5090, Fax 602.346.3610. Outside the U.S. call +31 36 540 5959. Email requests to: info@netpro.com.



4747 North 22nd Street, Suite 400 Phoenix, Arizona 85016

NetPro® and NetPro Computing® are registered trademarks of NetPro Computing, Inc. DirectoryLockdown™ and the NetPro logos are trademarks of NetPro Computing, Inc. Microsoft®, Windows® 2000 Server and Active Directory™ are either registered trademarks or trademarks of Microsoft Corporation. 111403