



Business Intelligence 101
Your Intelligent Source for Business Technology



WHITE PAPER

Copyright © 2003 NetPro Computing, Inc. All rights reserved.

This document introduces users to the Microsoft Windows Active Directory security monitor product, DirectoryLockdown, developed by NetPro Computing, Inc. All information contained herein is the property of NetPro Computing, Inc. and shall not be copied, photocopied, translated, or reduced to any electronic or machine-readable form, either in whole or in part, without prior written approval from NetPro Computing, Inc.

NetPro Computing, Inc. reserves the right to modify or revise all or part of this document, without notice, and/or change product features or specifications. NetPro Computing, Inc. shall not be responsible for any loss, cost, or damage, including consequential damage, caused by reliance on these materials.

NetPro Computing, NetPro, DirectoryLockdown, DirectoryInsight, DirectoryAnalyzer, DNSAnalyzer, DirectoryTroubleshooter, and the NetPro logo are either registered trademarks or trademarks of NetPro Computing, Inc. in the United States and/or other countries.

Microsoft, Active Directory, Windows NT, Windows 2000, and Windows Server 2003 are either registered trademarks or trademarks of Microsoft Corporation. Other brand and product names mentioned herein may be the trademarks of their respective companies.

*NetPro Computing, Inc. • 4747 N. 22nd Street, Suite 400 • Phoenix, AZ 85016 • USA
DL-WP-1103-300*

CONTENTS

Introduction	1
Classification of Threats	3
DirectoryLockdown Features & Benefits.....	4
How Can Active Directory Security be Compromised Maliciously?	5
What is DirectoryLockdown?	8
Exceptions For a Detected Intrusion	14
The DirectoryLockdown Recovery Utility.....	15
DirectoryLockdown in Action	16
Integration with Third Party Network Management Solutions.....	19
DirectoryLockdown System Requirements.....	20
NetPro's Secure Active Directory Lifecycle Suite	21
Summary and Contact Information	23
Glossary.....	24



INTRODUCTION

Delegation of administration is a key value proposition of Active Directory, the directory service at the heart of Microsoft's Windows 2000/2003 operating system. The ability to delegate administrative rights enables companies to design a directory infrastructure that spans multiple organizations, while still enabling an organization to meet specific requirements for structural and operational independence. However, delegation cannot be used to provide isolation between domains in the same forest.

As described in the Microsoft white paper "Design Considerations for Delegation of Administration in Active Directory,"¹ delegation of administrative rights within organizational structures does not limit administrator access to other critical structures or components of the forest. Specifically, Active Directory does not provide complete isolation from possible attacks by "rogue" administrators who maliciously breach the security or modify the behavior of a system.

The ability to change this information in the directory enables an attacker to:

- Change the default security descriptor of a domain, organizational unit (OU) or group, granting or denying access to subsequently created users or groups not under their control.
- Remove domain controllers and sites from the replication topology, causing widespread authentication and replication failures.
- Create a distributed denial-of-service (DDOS) attack by promoting DCs to Global Catalogs (GCs) or demoting GCs to DCs.

In addition to the threats posed by rogue administrators, companies that deploy Active Directory in a decentralized manner may also face an additional dilemma. In a decentralized administration model, domain administrators could operate in regional or remote offices, out of the direct control of the enterprise administrative group. For example, the IT department at a company's corporate headquarters in Boston may own the directory structure and manage it from an enterprise level, mandating policy, schema, and other configuration changes from their location on the East Coast. Likewise, an administrator hired to manage IT for the branch operation in Los Angeles can manage his own section of the directory, troubleshooting problems and pushing out necessary changes within the regional domain as required. Domain administrators located at remote sites and acting in a regional administrative role may, in certain circumstances, operate out of the full control of the enterprise administrator group. Therefore, unauthorized changes to the Configuration NC could occur from the regional IT groups, with or without malicious intent, putting the entire forest at risk.

¹ <http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/addeladm.asp>

For these reasons, the security implications of using forests, domains, or organizational units for delegation of authority must be carefully considered. Here's why:

An Active Directory forest is a highly distributed, replicated database system. Each Active Directory forest stores its enterprise configuration information in the Configuration Naming Context (NC). The Configuration NC contains information such as the site structure, replication topology and replication schedules, and is replicated on every DC in the forest. By altering the contents of the Configuration NC and allowing Active Directory to replicate the changes across the forest, an administrator can impact the operation of many servers or even, in a worst-case scenario, the entire enterprise.

As a result, companies may want to take steps to mitigate or limit the vulnerabilities that result from unauthorized modifications to the Configuration and Schema NCs in Active Directory. This white paper discusses NetPro's DirectoryLockdown, an Active Directory security monitoring solution that provides critical security against unauthorized changes to the Configuration and Schema NCs of Active Directory.

CLASSIFICATION OF THREATS

"Businesses must take steps to secure themselves against criminally intent insiders or resign themselves to suffering significant losses from insider crimes."

- Gartner Group 2003

There are several ways that a domain administrator can make unauthorized changes to Active Directory with or without malicious intent.

A rogue administrator might try to subvert Active Directory to either escalate his or her privilege level or to create a denial-of-service (DOS) attack. For the purposes of this white paper, we classify attacks as being either online or offline.

- An **online attack** (sometimes referred to as an "in-context" attack) involves subverting Active Directory while it is running on a DC.

DirectoryLockdown mitigates certain types of online attacks on DCs. Specifically, DirectoryLockdown can help prevent attacks that rely on modifications to the Configuration NC, including attacks that utilize a virus. There are certain online attacks that DirectoryLockdown does not mitigate, including attacks that depend on modifications to the Domain NC.

- **Offline attacks** (or "out-of-context" attacks) involve shutting down the DC and altering the contents of the disk system.

It is crucial to understand that, given physical access to a computer, a rogue administrator can **always** engineer an offline attack, regardless of any other software-based security mechanisms that may exist. Maintaining physical access control over your domain controllers is a requirement to ensuring the security of Active Directory. Absent that, all bets are off.

Although DirectoryLockdown can be subverted through an offline attack, DirectoryLockdown does provide a warning when a DC that is monitored by DirectoryLockdown is taken offline unexpectedly, warning the administrator of a potential attack.

DIRECTORYLOCKDOWN FEATURES & BENEFITS

Following is a brief list of the key features and benefits of NetPro's DirectoryLockdown:

DirectoryLockdown Features

- Monitors objects in the Configuration and Schema NCs on DCs 24x7
- Detects unauthorized changes to Configuration and Schema NCs on DCs
- Alerts network management when a modification to the Configuration or Schema NC occurs on a DC
- Helps to stop the replication to and from the DC where the intrusion occurred
- Prevents further changes of the Configuration and Schema replicas by quarantining the compromised DC
- Offers flexible response options: (1) Complete response and (2) Alert Only response
- Monitors and alerts on attempts to subvert the DirectoryLockdown system
- Monitors domain controllers and alerts when they are unexpectedly taken offline
- Alerts network management authorities of problems with the DirectoryLockdown Agent
- Includes a recovery utility to quickly restore a quarantined DC
- Features a MOM Management Pack and an HP OpenView for Windows SmartLink

DirectoryLockdown Benefits

- Reduces the security risks associated with domain administrators acting maliciously
- Reduces the security risks associated with domain administrators operating at remote or regional locations
- Alerts administrators to the possible corruption of Configuration and Schema NC information so that the corruption can be stopped in its tracks
- Helps network management maintain awareness and control of the Active Directory enterprise, despite the presence of rogue administrators and administration models that utilize regional management of Active Directory
- Gives administrators the power to choose variable levels of protection with flexible response options

HOW CAN ACTIVE DIRECTORY SECURITY BE COMPROMISED MALICIOUSLY?

As with any complex software system, there are several strategies an attacker might use to defeat the Windows 2000/2003 security system and gain unauthorized access to the directory. One such strategy is known as “Escalation of Privilege,” whereby an attacker attempts to assume the identity and privileges of an individual with greater access to the directory.

For instance, an attacker could assume the identity of a domain administrator by attempting to guess the administrator’s password. After successfully guessing the password and logging in as a domain administrator, the attacker could create a new administrator account for himself/herself, thereby gaining unfettered access to the directory.

How Can This Happen?

Each Active Directory forest has two NCs that contain critical structural information about the directory:

- **Enterprise Configuration NC** - contains information about the physical and logical structure of the entire directory, including the domain hierarchy and replication topology.
- **Enterprise Schema NC** - contains information about the types of objects and attributes allowed in the directory and their relationships.

Each DC in an Active Directory forest stores a complete read/write copy (or replica) of the Configuration and Schema NCs. To keep all copies synchronized, Active Directory replicates changes made to a replica on one DC to all other DCs in the forest.

Administrative Groups

In most enterprise deployments of Active Directory, administrators define a hierarchy of domains in a single forest. The root domain is the first domain installed in a forest and contains the following two unique security groups:

- **Enterprise Administrators** – by default, has complete access to the Enterprise Configuration NC.
- **Schema Administrators** – by default, has complete access to the Enterprise Schema NC.

Members of these groups can make enterprise-wide changes, such as adding domains, creating sites, or extending the enterprise schema. These two security groups do not exist in any other domains in the forest, but by default are granted the access rights in every domain.

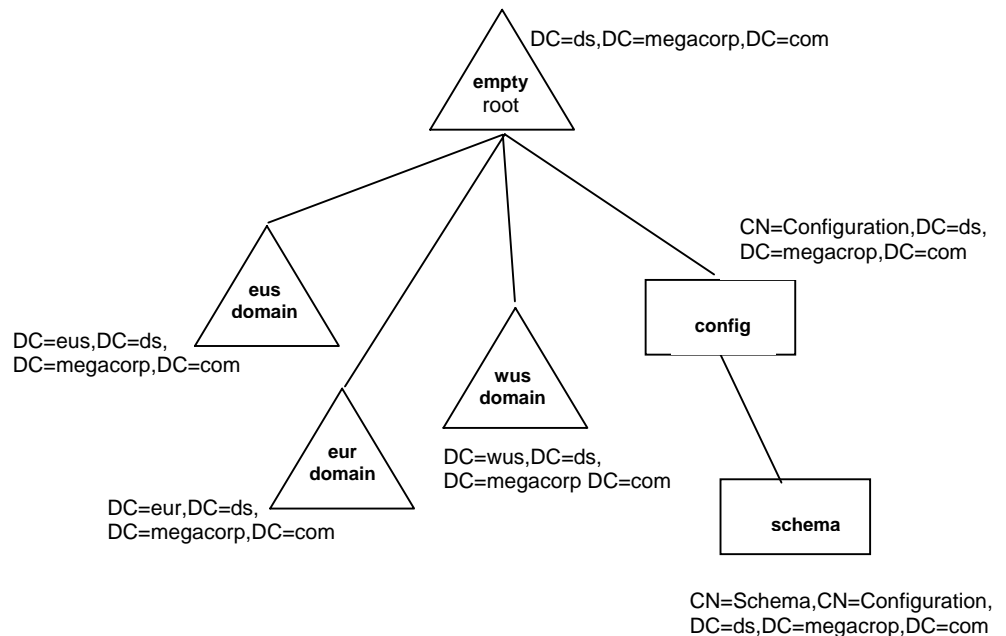


Figure 1. A Forest with Subordinate Domains

The third important administrative group is the Domain Administrators Group. This group's members typically have administrative access only to a specific domain. Members of the Domain Administrators Group can perform administrative tasks within the domain, such as creating groups and users. They also have administrative rights to the DCs in their domain, including the ability to log in to the DC interactively.

The LocalSystem Account

Each computer in Windows 2000 and Windows Server 2003 has a special system account referred to as "LocalSystem" or "the System account." This special account is normally used by system services running on the computer. By default, the System account has complete access to all the resources on the computer. Consequently, the System account on a DC has complete read/write access to the Active Directory replicas stored on the DC, including the Enterprise Configuration and Enterprise Schema replicas.

There are several mechanisms by which a domain administrator with physical access to a DC can login using LocalSystem credentials. With these privileges, a domain administrator can exercise complete read/write access to the replicas of the Configuration and Schema NCs on that DC, despite the fact that he/she is not a member of the Enterprise Administrators Group or the Schema Administrators Group. The result? Domain administrators can modify the contents of the Configuration and Schema NCs, thereby changing the configuration of Active Directory itself. And, because these NCs replicate forest-wide, a malicious domain

administrator is in the position to destroy an entire Active Directory deployment with only a limited level of access.

Without significant changes to Active Directory and the Windows 2000/2003 security architecture, Microsoft has determined that it is not possible to prevent domain administrators from modifying the Configuration and Schema NCs. However, NetPro has developed a different strategy for addressing this particular security risk. Using DirectoryLockdown, companies can mitigate the effects of this type of attack on Active Directory by quickly detecting unauthorized modifications to Configuration or Schema NC information and preventing their replication to other DCs in the forest.

WHAT IS DIRECTORYLOCKDOWN?

DirectoryLockdown is a security solution for Windows 2000/2003 that monitors the Configuration and Schema NCs of Active Directory DCs for unauthorized modifications. Once a DirectoryLockdown Agent is loaded and registered with a DirectoryLockdown Monitor, DirectoryLockdown monitors and detects modifications made to replicas of the Configuration and Schema NCs. When it detects an intrusion, DirectoryLockdown enables two types of responses. Alert Only Response immediately notifies the appropriate personnel of any intrusion via alert notifications, allowing users to choose how to proceed in protecting the enterprise. DirectoryLockdown's Complete Response goes a critical step further by preventing further damage to an enterprise by disabling replication to and from the compromised DC and quarantining the DC completely. To bring a quarantined DC back up, DirectoryLockdown also provides a special recovery utility that allows enterprise administrators to restore the DC.

Protects Against Detected and Inferred Intrusions

DirectoryLockdown provides safeguards for two types of intrusions. A "Detected Intrusion" is a situation where an unauthorized change occurs to replicas of the Configuration and Schema NCs. When a Detected Intrusion occurs, DirectoryLockdown responds with either the Alert Only Response or the Complete Response, depending upon the configuration selected by the administrator

An "Inferred Intrusion" is when the DirectoryLockdown agent becomes disabled, or the domain controller is shut down or disconnected from the network. In this case DirectoryLockdown sends alerts to the enterprise administrator that the domain controller may have been compromised.

DirectoryLockdown Architecture

DirectoryLockdown consists of three logical components:

- The **DirectoryLockdown Agent** is responsible for detecting any modification (add, delete, or modify) to any object in the Configuration or Schema NC on the DC on which it is installed. Two types of agents are available to accommodate users' requirements:
 - Alert Only Agent
 - Complete Response Agent
- The **DirectoryLockdown Monitor** communicates with and receives status from DirectoryLockdown Agents. In addition, the DirectoryLockdown Monitor solely determines whether or not a DirectoryLockdown Agent in its list is currently running, and sends notifications to the DirectoryLockdown Client if it is determined that an Agent module has been tampered with and is incapable of sending a status update.

- The **DirectoryLockdown Client** communicates with the DirectoryLockdown Monitor and displays the status for each DirectoryLockdown Agent. In addition, it provides the interface necessary for adding or removing a DirectoryLockdown Agent from a Monitor's Agent List, and/or stopping a DirectoryLockdown Agent with authorization.

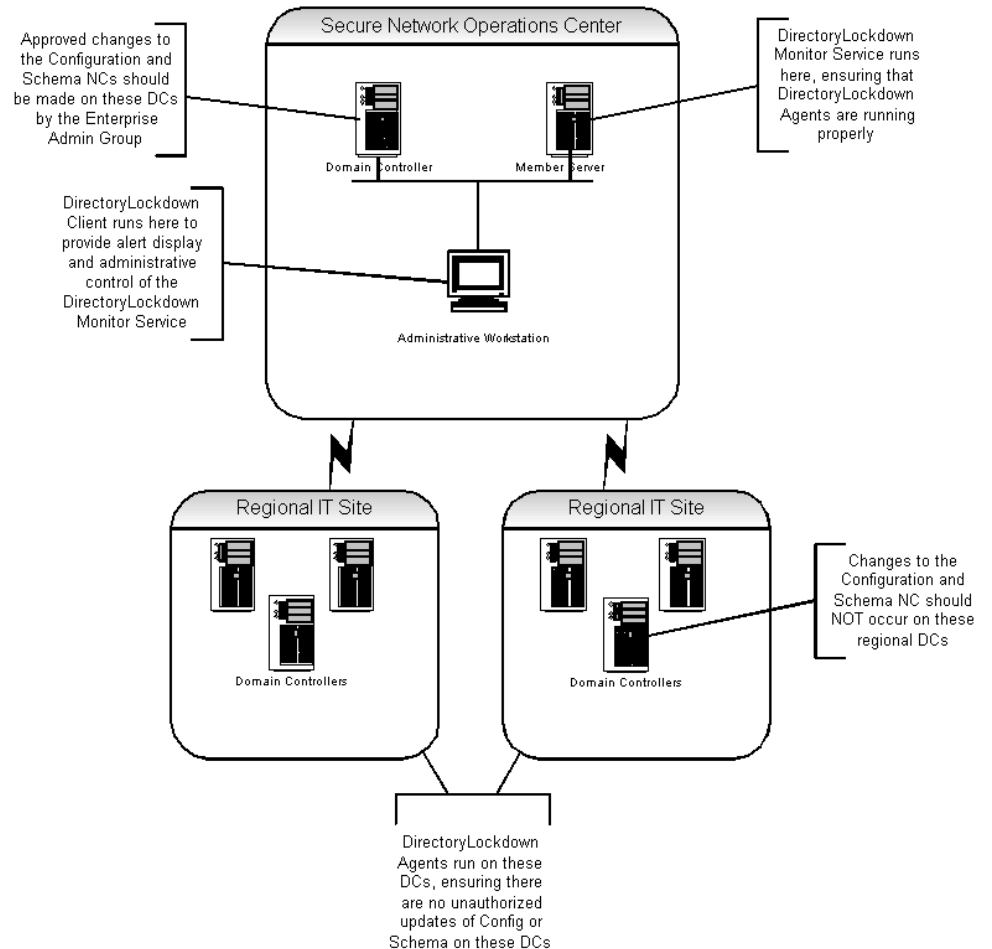


Figure 2. Directory Lockdown Deployment Model

The DirectoryLockdown Agent

Each DirectoryLockdown Agent runs as an NT service on Windows 2000 or Windows Server 2003 DCs. DirectoryLockdown agents can be installed on any domain controller running Windows 2000 Server, Windows 2000 Advanced Server with Service Pack 2 or later, or Windows Server 2003. DirectoryLockdown agents should be installed on all DCs that the Enterprise Administrators group wants monitored for changes.

The DirectoryLockdown Agent and Detected Intrusions

Upon a completed change (add, delete or modify) to the Configuration or Schema NC, the DirectoryLockdown Agent goes into Detected Intrusion-mode. There are two response options:

During an Alert Only Response, the DirectoryLockdown Agent immediately sends an alert to the DirectoryLockdown Monitor with the IP address of the DC and name of the modified object. If other notification methods are configured by the user (HP OVOW, MOM, event log, SMTP, SNMP), then alerts populate those consoles as well.

During a Complete Response, DirectoryLockdown first issues alerts in a manner similar to that of the Alert Only response, however the Agent goes further by:

- Recording the IP address and object name in the event log of the DC
- Disabling replication and all network adapters on the system in an attempt to stop the change from replicating out to the enterprise
- Replacing any login policies with a new and unique "DLRecover" account, so only a single trusted member may gain access to the DC (*Windows 2000 only*)
- Moving the compromised DC to a quarantined site Quarantines the compromised DC
- Removing members from the "Built-in Administrators" Group and changes the Domain Administrator's password to the recovery password (*Windows Server 2003 only*)
- Quarantining the DC. This is necessary to complete the security policy application of the newly created account.

These actions always occur in the event of a Detected Intrusion with a Complete Response Agent. However, the DirectoryLockdown Agent does not act upon updates and modifications that are generated by Active Directory's Knowledge Consistency Checker (KCC), NetPro's DirectoryAnalyzer, Microsoft Operations Manager (MOM), Microsoft's Licensing Server, Microsoft's Message Queuing Services (MSMQ), Terminal Services Licensing Server, or HP OpenView's Active Directory SPI.

NOTE: *If an attempt is made to access the Configuration or Schema NC container that is denied as a result of standard Active Directory security, no action is taken. An intrusion is only declared when a change is actually made to the Configuration or Schema NC container.*

The DirectoryLockdown Agent and Inferred Intrusions

The DirectoryLockdown Agent installs with an anti-tamper mechanism to prohibit its premature shutdown and/or modification. Any tampering with the DirectoryLockdown Agent service, including any attempt to stop the service or modify its registry entries, will generate a warning message to the DirectoryLockdown Monitor. The only exception to this occurs as a result of successfully stopping the service, in which case an Inferred Intrusion will be called from the DirectoryLockdown Monitor and an alert will be published to the DirectoryLockdown Client.

DirectoryLockdown Administrative Model

DirectoryLockdown requires the user to adopt certain changes to his or her administrative model. In particular, the user must implement an administrative policy that requires that no enterprise Active Directory configuration changes may be made on a domain controller running the DirectoryLockdown Agent.

The DirectoryLockdown Monitor

The DirectoryLockdown Monitor runs as an NT service on a Windows 2000 or Windows Server 2003 member server. It receives status updates from all DirectoryLockdown Agents in its Agent List. It collects this information for use by the DirectoryLockdown Client. Although it is possible to have more than one Monitor in an enterprise, any given domain controller with an Agent installed must not be added to more than one Monitor.

The DirectoryLockdown Monitor plays a key role by ensuring that the DirectoryLockdown Agents assigned to it are running properly and to generate alerts if any of the following conditions occur:

- A DirectoryLockdown Agent detects an intrusion.
- Connectivity to a DirectoryLockdown Agent is unexpectedly lost.
- An attempt is made to subvert the DirectoryLockdown Agent.

The DirectoryLockdown Monitor and Detected Intrusions

During a Detected Intrusion, the DirectoryLockdown Monitor receives the IP address and modified object information from the DirectoryLockdown Agent that detected the intrusion and reports that information directly to the DirectoryLockdown Client. In addition, the DirectoryLockdown Monitor does the following:

- Sends an SNMP trap (if configured) that an intrusion has occurred. This trap includes the IP address of the DC and the object affected (for detected intrusion only).
- Sends an SMTP message (if configured) that an intrusion has occurred. This message includes the IP address of the DC and the object affected (for detected intrusion only).

The DirectoryLockdown Monitor and an Inferred Intrusion

The DirectoryLockdown Monitor consistently checks to ensure that the DirectoryLockdown Agents assigned to it are up and running. If one of its Agents becomes unresponsive, the DirectoryLockdown Monitor will deem that the DirectoryLockdown Agent has been shut down without authorization and declares an Inferred Intrusion for that DC. If an Inferred Intrusion occurs, the DirectoryLockdown Monitor will:

- Alert the DirectoryLockdown Client
- Send an SNMP trap (if configured) that an intrusion has occurred.
- Send an SMTP message (if configured) that an intrusion has occurred.

NOTE: *A DirectoryLockdown Agent can be shut down from the DirectoryLockdown Client and DirectoryLockdown will not act in response to this type of authorized, DirectoryLockdown Agent shut down.*

The DirectoryLockdown Client

The DirectoryLockdown Client, as shown in Figure 3, runs as a Windows application on Windows XP, Windows 2000, or Windows Server 2003. An MDI Windows Application, the DirectoryLockdown Client allows multiple DirectoryLockdown Monitors to be viewed from a single DirectoryLockdown Client console. The DirectoryLockdown Client receives status from the DirectoryLockdown Monitor on all DirectoryLockdown Agents currently in its list using one of these two methods: by periodic updating from the DirectoryLockdown Monitor, and by active collection from the DirectoryLockdown Client itself. Active collection will be done when the user needs information about a specific DirectoryLockdown Agent.

The DirectoryLockdown Client provides a means by which the user can:

- Add or delete monitored DCs to the DirectoryLockdown Monitor's Agent List.
- Change configurable settings for both the DirectoryLockdown Monitor and each DirectoryLockdown Agent in the Monitor's Agent "watch" List. This includes recipients' lists for email (SMTP) notifications.
- Authoritatively shut down a DirectoryLockdown Agent service without generating an Inferred Intrusion from the DirectoryLockdown Monitor.

EXCEPTIONS FOR A DETECTED INTRUSION

There are standard services and applications that make necessary and unthreatening modifications to the Configuration container. Upon installation of DirectoryLockdown, these services and applications would normally trigger intrusions if installed on DCs protected by DirectoryLockdown.

There is a list of approved services and applications whose changes to the Configuration container (upon successful deployment) are allowed to proceed without intervention by DirectoryLockdown. The list of services approved for container modifications and services that do not trigger responses from DirectoryLockdown are as follows:

- Active Directory's Knowledge Consistency Checker (KCC)
- NetPro's DirectoryAnalyzer
- Microsoft's Operations Manager (MOM)
- Microsoft's Licensing Server
- Microsoft's Message Queuing Services (MSMQ)
- Terminal Services Licensing Server
- HP OpenView's Active Directory SPI

Strict care should be exercised, however, when installing any new service onto a DC while a DirectoryLockdown Complete Response Agent is running because its key role is to actively check, and respond to, container modifications. Therefore, it is recommended that the DirectoryLockdown Agent be stopped, through the DirectoryLockdown Client, prior to installing any such services to prevent any intervention by DirectoryLockdown. Once the service is successfully installed, the DirectoryLockdown Agent can be restarted.

THE DIRECTORYLOCKDOWN RECOVERY UTILITY

In order to quickly restore a downed DC, DirectoryLockdown comes with a special recovery utility tool. The utility re-enables all user accounts, at the discretion of the Enterprise Administrator. Once the process is complete, the utility deletes the DLRecover account, and all network adapters are re-enabled. When the DC is recovered and the DC's communications are re-enabled, replication will proceed normally.

IMPORTANT NOTE: *DirectoryLockdown does NOT undo any changes made to the downed DC during or after the detected intrusion, nor does it repair the Configuration container of any damage. The DirectoryLockdown Recovery utility should only be employed if it is determined that the changes that have been made were absolutely harmless. By "harmless" we mean that the enterprise would not be adversely affected when these changes replicate out or if the unauthorized changes were completely corrected.*

DIRECTORYLOCKDOWN IN ACTION

Acme, Inc. is a security-conscious company with several regional sites that has Active Directory fully deployed in its Windows 2000 network. Acme dictates that no containers be modified by anyone other than the Enterprise Administrator, who is located at Acme headquarters. In keeping with this policy, the DCs in every remote office are outfitted with DirectoryLockdown, and Domain Administrators are prohibited (denied permission through Active Directory) from making these changes. The Enterprise Administrator utilizes the DirectoryLockdown Client to manage the DirectoryLockdown deployment across all of Acme's remote sites.

Scenario 1 - A Detected Intrusion with a Complete Response Agent

A rogue administrator, "Paul" decides to execute an attack on Acme's network. He gains LocalSystem access to a DC that's running a DirectoryLockdown Complete Response Agent and alters the sites container and other items within the Configuration or Schema containers.

What Happens?

- Because he is running under LocalSystem, Paul now has full access to a replica of the Enterprise Configuration and Schema. His change will be made, circumventing the Active Directory security model.
- Once the change occurs, the DirectoryLockdown Client displays the "Detected Intrusion" information to the Enterprise Administrator immediately notifying him of the intrusion. In addition, DirectoryLockdown sends the intrusion information via SNMP trap and email notification to the Enterprise Administrator, ensuring instant notification of the issue.
- In the meantime, DirectoryLockdown disables all communications on the DC Paul utilized for the attack, helping to prevent the unauthorized change from replicating out to the rest of Active Directory and potentially affecting Acme's network in a negative way. The DC is then fitted with the new account, "DLRecover," and a password that only the Enterprise Administrator knows (created upon initial installation of the DirectoryLockdown Agent).
- The DC is then quarantined so no other modifications can be made to the machine. The offending DC is essentially 'Locked-down'.
- To restart the DC, the Enterprise Administrator logs onto the machine using the DLRecover username and password. This is the ONLY account that can log onto the DC.
- Once logged on, the Enterprise Administrator checks to see if the modifications that were made were harmful and he corrects the change. Once they've been corrected, he runs the DirectoryLockdown Recovery Utility and DirectoryLockdown restores the network adapters and brings the DC back online and running with Active Directory.

With DirectoryLockdown, Acme was able to pinpoint and stop the attack on the DC where the attack started. This, in turn, stopped the configuration changes from affecting Active Directory and the network. Without DirectoryLockdown, the rogue administrator's changes would have replicated to the forest and he would have

succeeded with in attacking Acme's network, potentially causing expensive damage and comprising the security of Acme's network resources.

Scenario 2 - A Detected Intrusion with an Alert Only Agent

In situation similar to the one outlined above, a rogue administrator, "Rich" decides to execute an attack on Acme's network. He gains LocalSystem access to a DC that's running a DirectoryLockdown Alert Only Agent and alters the sites container and other items within the Configuration or Schema containers.

What Happens?

- Once the change occurs, the DirectoryLockdown Client displays the "Detected Intrusion" information to the Enterprise Administrator, immediately notifying him of the intrusion. In addition, DirectoryLockdown sends the intrusion information via SNMP trap and email notification to the Enterprise Administrator, ensuring instant notification of the issue.
- At this point, the Enterprise Administrator can take further action in order to address the issue.

With DirectoryLockdown, the Acme Enterprise Administrator became immediately aware of a potential attack to the Active Directory environment. Without DirectoryLockdown, the Enterprise Administrator would have never known about the problem until it was too late.

Scenario 3 - An Inferred Intrusion

Foiled on his first attempt, Paul tries to disable DirectoryLockdown from the domain controller a week later. After several failed attempts to stop the DirectoryLockdown service manually on the DC, he thwarts the anti-tampering mechanism and succeeds, completely removing the DirectoryLockdown executables and entries in the registry. Then he reboots the domain controller.

What Happens?

- Once the DC is restarted and the communications layer is loaded, the DirectoryLockdown Monitor begins to ping the DC, aware that communication to the DirectoryLockdown Agent service has been interrupted.
- After a set number of pings, which are configurable in DirectoryLockdown, the DirectoryLockdown infers that an intrusion has occurred on the DC.
- DirectoryLockdown displays the "Inferred Intrusion" notification to the Enterprise Administrator's via the DirectoryLockdown Client and sends an SNMP trap and email notice to ensure instant notification of the issue.
- The Enterprise Administrator receives the Inferred Intrusion alerts and immediately acts on the issue.

DirectoryLockdown made Acme aware of the rogue administrator attack immediately. Without DirectoryLockdown, it is highly likely that Acme wouldn't have discovered the attack until after it succeeded in corrupting the directory as intended.

Scenario 4 - A Detected Intrusion (from an unauthorized change)

Bob, a Domain Administrator in Acme's Boston office, is unaware of Acme's policy that no containers be modified by anyone other than the Enterprise Administrator. He brings up his local DC "AD Sites and Services" application. Because of an administrative oversight, Bob is not among those prohibited from making these types of changes to Active Directory. He adds the site "New Haven" to the Configuration NC on the DC on which he is working.

What Happens?

- Because a change was made on the Configuration NC, DirectoryLockdown dispatches a "Detected Intrusion" and captures the IP address of the DC and the name of the offending object.
- The DirectoryLockdown Client displays the "Detected Intrusion" information to the Enterprise Administrator immediately notifying him of the intrusion. In addition, DirectoryLockdown sends the intrusion information via SNMP trap and email notification to the Enterprise Administrator, ensuring instant notification of the issue.
- In the meantime, DirectoryLockdown disables all communications on Bob's DC, helping to prevent Bob's unauthorized change from replicating out to the rest of Active Directory and potentially affecting Acme's network in a negative way.
- The DC is then fitted with the new account, "DLRecover," and a password that only the Enterprise Administrator knows (created upon initial installation of the DirectoryLockdown Agent).
- The DC is then quarantined so no other modifications can be made to the machine. The offending DC is essentially 'Locked-down'.
- To restart the DC, the Enterprise Administrator logs onto the machine using the DLRecover username and password. This is the ONLY account that can log onto the DC.
- Once logged on, the Enterprise Administrator checks to see if the modifications that were made were harmful and he corrects the change. Once it's been corrected, he runs the DirectoryLockdown Recovery Utility and DirectoryLockdown restores the network adapters and brings the DC back online and running with Active Directory.

DirectoryLockdown enabled Acme to stop the 'innocent mistake' from replicating throughout the directory and negatively impacting the network, saving network downtime and rebuild costs. Without DirectoryLockdown, Bob's change would have replicated to the rest of the forest, which could have prompted significant network issues and downtime.

INTEGRATION WITH THIRD PARTY NETWORK MANAGEMENT SOLUTIONS

DirectoryLockdown extends its Active Directory security monitoring capabilities to two of the leading network management consoles: Microsoft Operation Manager (MOM) and HP OpenView for Windows. By integrating DirectoryLockdown into a MOM or HP OpenView for Windows console, companies extend the built-in functionality of the framework by allowing network administrators to monitor the Configuration and Schema Naming Contexts (NCs) of Active Directory for unauthorized changes. For MOM, DirectoryLockdown delivers the functionality with a MOM Management Pack and for HP OpenView Operations for Windows, it occurs through certified SmartLink integration.

Administrators who take advantage of this vital functionality ensure critical added protection for the Configuration and Schema NC of Active Directory.

DIRECTORYLOCKDOWN SYSTEM REQUIREMENTS

DirectoryLockdown Agents

Both DirectoryLockdown Agents (Alert Only and Complete Response) run as an NT service on Windows 2000/2003 domain controllers. They can only be installed on a domain controller running Windows 2000 Server, Windows 2000 Advanced Server with Service Pack 2 or later, or Windows Server 2003. They will NOT operate on the same machine as a DirectoryLockdown Monitor component, or on the same machine as a DirectoryLockdown Client.

DirectoryLockdown Monitor

The DirectoryLockdown Monitor operates on a Windows 2000 or Windows Server 2003 member server. It can run on a domain controller, however this is not a recommended configuration and it will not operate on the same machine as a DirectoryLockdown Agent.

DirectoryLockdown Client

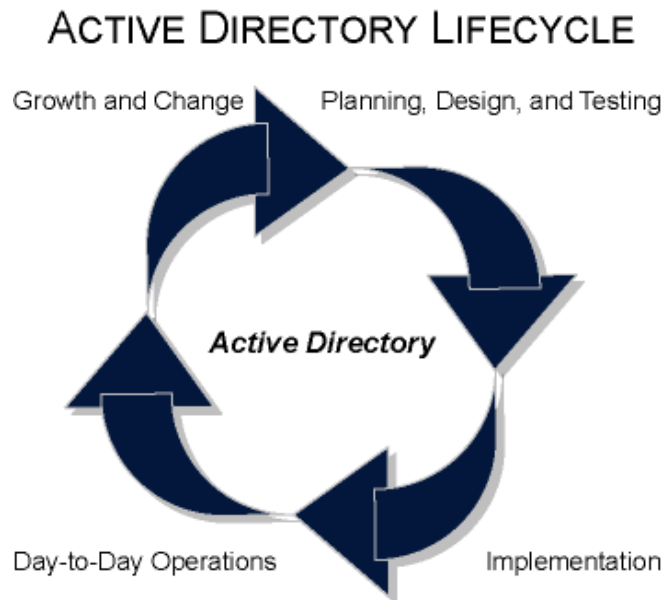
The DirectoryLockdown Client operates on machines running Windows XP, Windows 2000, or Windows Server 2003. It will run on either a member server or domain controller, but these are not recommended configurations. The DirectoryLockdown Client can run on the same machine that is running the DirectoryLockdown Monitor, but this is not a recommended configuration. And it will NOT run on the same machine as a DirectoryLockdown Agent.

NETPRO'S SECURE ACTIVE DIRECTORY LIFECYCLE SUITE

DirectoryLockdown anchors NetPro's Secure Active Directory Lifecycle Suite (ADLS). The Secure ADLS features five breakthrough solutions including: DirectoryLockdown, DirectoryInsight, DirectoryAnalyzer, DNSAnalyzer, and DirectoryTroubleshooter.

NetPro's Secure ADLS ensures the design, availability and performance of the directory and protects it from certain types of security breaches throughout the phases of the Active Directory lifecycle. Case in point: Active Directory issues and security breaches can strike at any phase of the directory lifecycle – from planning, design and testing to the growth and change phase. And, they have the potential to occur on a continuous basis as organizations evolve through different business circumstances, including mergers and acquisitions, downsizing, major system upgrades, etc.

The following diagram depicts the four phases of the directory lifecycle and the subsequent paragraphs further articulate the criticality of strategic directory management during these phases.



Proactive management and security throughout each phase of the Active Directory lifecycle is critical to ensuring total directory assurance and constant uptime for the services and applications that rely on the directory.

NetPro's Secure Active Directory Lifecycle Suite revolutionizes the management of Active Directory by simplifying its inherent complexities and enabling administrators of all levels to deliver on the promise of 24x7 availability and security for their internal users and customers. The solution set also saves organizations millions of dollars annually by ensuring productivity, slashing downtime, and freeing up expensive IT resources for other critical tasks.

The following table illustrates the technical benefits of these solutions throughout the directory lifecycle.

NetPro's Secure Active Directory Lifecycle Suite

<i>Strategic Function</i>	<i>Product</i>	<i>Benefits</i>	<i>Lifecycle Phases</i>
MANAGE CHANGE	DirectoryInsight	Track user population Smooth AD migration Simplify troubleshooting	Implementation; Operations; Growth and Change
MONITOR AND ALERT	DirectoryAnalyzer	Cut Mean Time to Repair Receive alerts earlier Diagnose issues faster	Planning; Implementation; Operations; Growth and Change
MONITOR AND ALERT ON DNS	DNSAnalyzer	Ensure 24x7 uptime Cut Mean Time to Repair Deliver detailed reports	Implementation; Operations; Growth and Change
TROUBLESHOOT AND DIAGNOSE	Directory Troubleshooter	Troubleshoot faster Increase uptime Gain directory knowledge	Implementation; Operations; Growth and Change
PROTECT	Directory Lockdown	Prevent attacks Control environment Protect IT assets	Planning; Implementation; Operations; Growth and Change

SUMMARY AND CONTACT INFORMATION

Through delegation of administration, Active Directory enables companies to design a directory infrastructure that spans multiple organizations, while still enabling an organization to meet specific requirements for structural and operational independence. However, since an Active Directory forest is a tightly coupled, distributed system, the breach of a single domain controller, with or without malicious intent, can impact many servers or even, in the worst case scenario, the entire network.

DirectoryLockdown mitigates the risks associated with unauthorized modifications to Active Directory's Configuration and Schema NCs and prevents far-reaching corruption of the Windows 2000/2003 system.

For the latest information on DirectoryLockdown, please visit www.netpro.com or contact NetPro at sales@netpro.com.

GLOSSARY

The following terms are important to Active Directory and DirectoryLockdown.

Authorized Change to the Configuration and Schema NCs	An approved change that is executed on a domain controller that is NOT running the DirectoryLockdown Agent by the Enterprise Administrators Group
Corrupted data	Any changes made to the Configuration or Schema NCs as the result of an intrusion on a DC with DirectoryLockdown running on it.
Detected Intrusion	An inappropriate modification to the Configuration or Schema NCs on a domain controller with DirectoryLockdown.
DirectoryLockdown Administrator Group	An administrative group where members have rights to use DirectoryLockdown to monitor DCs.
DirectoryLockdown Monitor	The component that is installed on a server to receive notifications from DirectoryLockdown Agents regarding any intrusions.
DirectoryLockdown Agent	The service that is installed on DCs to monitor for intrusions to the Configuration, Schema and Domain NCs. There are two types of agents: (1) Alert Only and (2) Complete Response.
Domain	A unit of replication and security boundary within Active Directory. Active Directory is made up of one or more domains.
Domain Administrators Group	An administrative group where members have rights to administer all functions within their specific domain.
Domain controller (DC)	A Windows 2000 or Windows Server 2003 server that contains a replica of a given Active Directory domain, as well as replicas of the Enterprise Configuration and Enterprise Schema NCs.
DLRecovery Utility	<p>A utility provided with DirectoryLockdown that will recover the DC in order to log onto the DC and re-enable communications.</p> <p>Important Note: This utility does NOT undo changes made by an intruder, nor does it repair any damage done to the Configuration container.</p> <p>DLRECOVERY.EXE should ONLY be used when it is deemed "safe" to replicate the changes out to the enterprise.</p>
Enterprise Administrators Group	A unique security group in the root domain of an Active Directory forest that has full access to the Enterprise Configuration NC.

Enterprise Configuration Naming Context (NC)	The NC, which identifies the domain controllers, replication topology and other, related information about the domain controllers within a specific implementation of Active Directory.
Enterprise Schema Naming Context (NC)	The NC, which defines the object class and attributes contained in Active Directory.
Forest	A collection of one or more directory trees organized as peers, sharing a common schema, configuration and global catalog.
Inferred Intrusion	A situation where a DirectoryLockdown Agent is shut down or affected in unauthorized manner.
Knowledge Consistency Checker (KCC)	A process that runs as part of the Active Directory service responsible for creating the Active Directory replication topology.
Quarantined Domain Controller OU	DirectoryLockdown moves the compromised DC to this Organizational Unit (OU) when an intrusion is detected. This OU is created when an intrusion is detected and deleted when the DLRecovery utility is run to restore the downed DC.
Quarantined Site	DirectoryLockdown moves the compromised DC to a new site named 'DLQuarantined' when an intrusion is detected. This site is created when an intrusion is detected and deleted when the DLRecovery utility is run to restore the downed DC.
Replication	The process by which changes to the directory, which can be stored on multiple domain controllers, are kept in synchronization with each other.
Schema Administrators Group	A unique security group in the root domain of an Active Directory forest that has full access to the Enterprise Schema NC.
Tree	A hierarchical structure of Active Directory domains that form a contiguous namespace.
Unauthorized Change to the Configuration and Schema NCs	An unapproved change that is executed, with or without malicious intent, on a domain controller that is running the DirectoryLockdown Agent



Business Intelligence 101
Your Intelligent Source for Business Technology

Corporate Headquarters

Livermore, CA. 94551

1(866) 55 - Bi101

sales@bi101.com

www.bi101.com