Novell eDirectory 8.7 Consensus Baseline Security Security Settings

Version 1.0

Date: 2006-05-26

http://www.cisecurity.org

Editor: David R. Bailey

Table of Contents

Terms Of Use Agreement

Background

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised

of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations (“**CIS Parties**”) harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS’s right, at our

expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://www.nsa.gov/ia).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

WE ACKNOWLEDGE THAT WE HAVE READ THESE AGREED TERMS OF USE IN THEIR ENTIRETY, UNDERSTAND THEM, AND WE AGREE TO BE BOUND BY THEM IN ALL RESPECTS.

Introduction

Novell's eDirectory is a cross-platform directory based off the Novell Directory Services (NDS) technology that was introduced in NetWare 4.0 during 1993 and over a decade later is still a leader in directory services and identity management. eDirectory trees can be partitioned into branches, distributed on servers across WAN or LAN links, and writable copies of the partition can be replicated in a loosely synchronized method across vast distances. It can be administered with a number of easy-to-use, yet powerful tools making enterprise directory services approachable for nearly anyone.

Currently, eDirectory is very popular for managing large numbers of identities for web-based applications (Yahoo! And CNN.com portals are two well-known examples), but it is also utilized in many other environments and for many other purposes, such as being the core infrastructure for security, administration, management, and replication of services are current available in NetWare as well as Open Enterprise Server (OES) on SLES.

Novell currently offers eDirectory on the Windows, Linux, Solaris, AIX, and HP/UX platforms as well as on NetWare. Through the separately purchased Novell Identity Manager, eDirectory can integrate with platforms and applications as diverse as IBM OS/400, Oracle, and Microsoft Exchange. As Novell moves to the Open Enterprise Server platform, eDirectory is increasingly being deployed on platforms other than NetWare.

The eDirectory benchmark was created for version 8.7.x and can be used with any platform on which it runs.

Utilize this benchmark in combination with OS benchmark

eDirectory runs atop an operating system (OS). The security of the base OS is directly tied to the security of eDirectory. Be sure to utilize the outstanding base OS benchmarks also available from CIS in combination with your eDirectory security efforts.

Intended audience

This benchmark is intended for anyone who is utilizing eDirectory and is responsible for the security of the system.

It requires a basic understanding of eDirectory as well as organizational authorization and the administrative rights to effect the changes required.

Administration utilities and methods

Administration utilities

What follows is a quick list of methods for accessing the various administration utilities. For more information, please refer to the appropriate documentation. (Novell Documentation - http://www.novell.com/documentation/)

- iManager: Go to this URI from a web browser: https://serverip/iManager.html or https://serverip/nps/iManager.html
- iMonitor: Go to this URI from a web browser: https://serverip:httpstack_port/nds - on a Linux server, httpstack_port is typically port 8030, on a Windows server, it is typically 8010, on a NetWare server, it is typically 8009.
- ConsoleOne for Windows: Download and install from Novell downloads.
- ConsoleOne for Linux: Download and install from Novell downloads.
- ConsoleOne for NetWare: Launch from GUI, "startx" at the server console, then launch from Novell menu.

Other notes

Earlier versions of eDirectory

Although this document is written for Novell eDirectory 8.7, many of these steps also apply to prior versions. Be aware that Novell ended support of all prior versions of eDirectory on November 1, 2004, and since then, no new security patches have been released. If you have iManager 2.x or later, many of the remedial steps of this document can be followed as written. If this software is not loaded, the steps taken to remediate the issues may be somewhat different.

Later versions of eDirectory

In addition, Novell has released eDirectory 8.8. eDirectory 8.8 was built off of the eDirectory 8.7 code base. Because of this, the information listed in this document would also apply to eDirectory 8.8. However, there are additive features to eDirectory 8.8 that can assist you in securing your environment. For more information about these features, you can refer to the Novell eDirectory 8.8's What's New document which is located at: http://www.novell.com/documentation/edir88/pdfdoc/edir88new/edir88new.pdf.

1 System Security

1.1 Make certain the server is physically secure

Description:

The server should be kept in a physically secure location where the keyboard, mouse, and ports cannot be accessed without authorization. If the server can be accessed physically, nearly all security precautions can be overridden in a relatively short period of time.

1.2 Install the most recent support packs and security patches

Description:

eDirectory requires current support packs and security patches to avoid known vulnerabilities.

Also see the patch listings in the references below. In the product patch list, be sure to look for the alert symbol next to any patches that fix security issues.

Remediation:

Install all current support packs and security patches for your current version of eDirectory, the server host operating system, and application software.

References:

Novell, Inc. "Patches: Security Alerts." Novell Website. Novell, Inc. <http://support.novell.com/filefinder/security/>

Novell, Inc. "Novell eDirectory Patches." Novell Website. Novell, Inc. <http://support.novell.com/filefinder/5069/>

1.3 Use a firewall to restrict access to network resources

Description:

Most operating systems cannot fully restrict access to all network services to extent necessary to fully secure all network-based services without utilizing a firewall either built into the host operating system, or utilizing third-party software.

It is a security best practice to utilize a firewall on the host operating system to restrict access to network resources available from the host system.

How to implement a firewall is specific to each operating system that eDirectory may be running on, so refer to the vendor information, or CIS benchmark, for that operating system for details on implementing a firewall.

It is a security best practice to ensure that administrative applications, such as iManager, should not be directly accessible from the Internet.A VPN can be used to connect to such services remotely. Also see rule Restrict access to web management applications.

Remediation:

Refer to the vendor information, or CIS benchmark, for that operating system for details on implementing a firewall.

2 Auditing / Monitoring

2.1 eDirectory Health Check reports should be run regularly

Description:

If eDirectory becomes unhealthy due to errors, recent changes may not be reflected across all servers in the tree.

According to Novell, eDirectory health checks involve the following:

1. Verifying directory services versions.
2. Time synchronization
3. Server-to-server synchronization
4. Replica synchronization
5. External references
6. Replica states
7. Schema synchronization

Remediation:

Run eDirectory Health checks regularly. To configure this:

1. Access iMonitor
2. In the toolbar icons, click the reports icon.
3. In the assistant frame, click the Report Config link.
4. Click Configure Report icon in the Server Information report line.
5. Check the Health sub-report box.
6. Schedule the report to run regularly, such as once a week or once a day.
7. Click Save Defaults to save your settings.
8. Click Schedule Report to schedule the report to run at the interval you specified.

In the Custom Reports and Scheduled Events you will see the report you scheduled. To run it now:

1. click the Run Report icon in the report line of the report you just scheduled.
2. Review the findings by clicking into each area of the report. Green icons are pass. Other icons indicate issues that need to be investigated.

For more information about resolving any issues found, read the references.

Warning: Only perform repairs when you need to perform them. Health checks and **not repairs** should be performed on a regular or scheduled basis. Directory services can be disrupted while running the automated repair.

References:

Novell, Inc. "Keeping eDirectory Healthy." Novell eDirectory 8.7 Administration Guide. Novell, Inc. <http://www.novell.com/documentation/edir87/edir87/data/a5ziqam.html>

Novell, Inc. "Checking eDirectory Health Using iMonitor." Novell eDirectory 8.7 Administration Guide. Novell, Inc. <http://www.novell.com/documentation/edir87/edir87/data/a5ziqam.html#a5zg0om>

Jim Henderson. "Using iMonitor to Perform eDirectory Health Checks." Novell Cool Solutions: Feature. Novell, Inc. <http://www.novell.com/coolsolutions/feature/15336.html>

Novell, Inc. "Troubleshooting Novell eDirectory." Novell eDirectory 8.7.3 Documentation. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/a2vw448.html>

Novell, Inc. "Repairing the Novell eDirectory Database." Novell eDirectory 8.7.3 Documentation. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/aese2hi.html>

2.2 eDirectory Reports

Description: There are several ways to monitor your environment and generate reports about it. iMonitor is a web-based tool for monitoring and diagnosing Novell eDirectory agents running on servers within an eDirectory tree. iMonitor provides an easy cross-platform method to access all the functionality of the console based utilities of DSRepair, DSTrace, DSDiag, and DSBrowse. iManager is a web-based administration tool and ConsoleOne is a java administration tool both of which allow administration and monitoring of eDirectory and many other related resources.

References:

Novell, Inc. "Novell iManager 2.6." Novell Documentation. Novell, Inc. <http://www.novell.com/documentation/imanager26/>

Novell, Inc. "Using the eMBox Logger." Novell eDirectory 8.7.3 Administration Guide. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/agayfpi.html>

Novell, Inc. "Using Novell iMonitor 2.1 - iMonitor Features." Novell eDirectory 8.7.3 Administration Guide. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/agwkqvb.html>

Novell, Inc. "Generating Reports in ConsoleOne." TechCenter Articles and Tips. 2003-03-01T00:00:00. Novell, Inc. <http://support.novell.com/techcenter/articles/ann20030301.html>

2.3 Enable auditing services

Description:

NetWare 6.5 and Open Enterprise Server comes with Novell Audit, formerly named Novell Nsure Audit. It can also be purchased separately. Novell Audit includes the capability to track events on your NetWare server, Windows server, Linux server, eDirectory, and can track events on other computers and network devices.

Auditing is critical to ensure that all events are consistent with the policies of the organization.

Remediation:

To implement Novell Audit on NetWare 6.5, view the NetWare 6.5 documentation chapter entitled "Novell Nsure Audit Administration Guide". Also the references for more information.

Specific instructions for how to implement auditing services are beyond the scope of this document.

Novell Audit can run on NetWare 5.1 and later, Windows 2000 and later, Solaris, or SUSE Enterprise or Red Hat Enterprise Linux. There are also 3rd-party solutions that allow in-depth auditing of events on an eDirectory tree.

References:

Novell, Inc. "Novell Nsure Audit 1.0.3 Administration Guide." Novell Nsure Audit 1.0.3 Administration Guide. 2005-10-18T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nsureaudit/nsureaudit/data/front.html>

Novell, Inc. "Generating Queries and Reports." Novell Nsure Audit 1.0.3 Administration Guide. 2005-10-18T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nsureaudit/nsureaudit/data/al0lgus.html>

3 Authentication

3.1 Administrator accounts should not be located in the same container as other users

Description: eDirectory administrator accounts should be placed in a different directory context or container than the other user accounts. This makes it more difficult to compromise the password or temporarily disable the administrator account through unauthorized access attempts.

Remediation:

In ConsoleOne or iManager 2.x:

1. Create a new container, if necessary, such as an organizational unit.
2. Move the administrator user object from the container where the users are located to a separate container.

Warning: If you have any automated processes that utilize the administrator account, this violates best practices, moving the administrator account can cause these process to stop working until they are reconfigured. (IE- data backup software.)

3.2 Administrator accounts should not be named common names

Description: eDirectory administrator accounts should not be named any common administrator account names. This makes it more difficult to find the account and attempt to brute-force attack the password or temporarily disable the administrator account through unauthorized access attempts.

Remediation:

Rename any administrator user objects to something other than "root", "admin", "administrator", or "supervisor". Note that user account authentication is not case sensitive.

Warning: If you have any automated processes that utilize the administrator account, this violates best practices, renaming the administrator account can cause these process to stop working until they are reconfigured. (IE- data backup software.)

3.3 All device-specific or node-specific accounts should be address limited

Description:

If you are using an eDirectory account to access services on a server using Novell Core Protocol (NCP), eDirectory has the ability to limit access to a user account based on the network address that is requesting access. If a user account isn't tied to a user, but a device or node with a fixed TCP/IP, not a dynamic one using DHCP, such as a printer or other non-user entity, that account should be restricted as to what network address can authenticate using it.

Remediation:

To set a network address restriction, perform the following steps:

1. Open ConsoleOne for Netware utility,
2. Select the User Object,
3. Select Network Address Restriction,
4. Select Add, and
5. Define the specific network and/or node from which the user may login

Warning: These address restrictions are only effective for NCP, and not for other services such as CIFS, HTTP, or LDAP.

References:

Novell, Inc. "User Restriction Limitations." Overview of OES Security Services. Novell, Inc. <http://www.novell.com/documentation/oes/implgde/data/secur-overview.html#bx7et49>

3.4 Configure an LDAP proxy user

Description:

By default LDAP uses the Public object to get its rights to return information from eDirectory. This is insecure as it also allows any non-authenticated user to read that same information from eDirectory. The secure way to offer LDAP connectivity is by using an LDAP proxy user.

Make certain that this proxy user does not have rights to sensitive portions of the tree, such as the administrator users containers, server containers, or SLP scope containers.

Remediation:

Perform the following steps in Novell iManager. These steps are for iManager 2.5:

1. Click the Roles and Tasks button in the icon toolbar at top.
2. Click eDirectory Administration > Create Object
3. Select User and click OK.
4. Create a proxy user (such as ldapproxy)
5. Use a descriptive Last name.
6. Leave the password blank and click OK.
7. Click eDirectory Administration > Modify Object
8. Browse to the proxy user object and click OK.
9. Select the Restrictions > Address Restrictions tab/menu.
10. Using the plus (+) button, add the IP addresses 127.0.0.1 and the IP address of all LDAP servers' local network interfaces.
11. Click OK.

12. Using Rights > Modify Trustees, assign the proxy user rights to specific containers you wish the proxy user to have access to. If the proxy user will only be reading and not changing values, it should not have more than Compare and Read attribute rights and Browse entry rights. Be sure that the user does not have rights to sensitive containers, such as the network administrators or SLP scope containers.
13. Click LDAP > LDAP Options/Overview > View LDAP Groups > the LDAP Group Object
14. In the Proxy User field, click the Browse button, browse to and select the proxy user
15. Make sure the checkbox is checked to require TLS for simple binds with password, then click OK.

References:

Novell, Inc. "Creating and Using LDAP Proxy Users." Novell eDirectory 8.7.3 Documentation. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/agtxhz5.html#agxk83p>

Novell, Inc. "What is an LDAP proxy user?." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062428.htm>

3.5 Disable LDAP anonymous binds

Description:

Allowing LDAP anonymous binds is somewhat adverse to security, especially so when public browse rights have not been revoked for the eDirectory tree. Also see rule Disable Directory Browsing. With eDirectory 8.7 with current patches, it is possible to completely disable all LDAP anonymous binds.

This can only be done on eDirectory version 8.7.0.3 or later.

Remediation:

For the steps to make this happen, see the Novell TID in the references.

Warning:

In some versions of eDirectory (8.7.3.7), there is a bug that can cause anonymous and non-anonymous binds to be denied with an error message indicating that anonymous bind is disabled. This has been fixed in later releases.

References:

Novell, Inc. "How to disable anonymous binds in LDAP." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10077872.htm>

3.6 Enable a Novell Client login banner in the login script

Description:

eDirectory supports enabling login banners in the login script. These banners impact the Novell Client only. There are other, perhaps better, ways to show a legal notice and require acknowledgement on a systems using the Novell client, but this method ensures that all Novell Client logins that have not disabled the login script results will see it.

The exact wording of the banner is beyond the scope of this document, but an example is shown below. Also see the references for a good source of security-related login banner information from the United States Department of Justice. Banners for organizations not under US jurisdiction will need to find alternate sources of information.

Remediation:

To create a login script banner within eDirectory for the Novell Client:

1. Create a text file containing your security login banner, such as the one shown here that has been approved by the United States Department of Justice.:

   ```
   This system is for the use of authorized users only. Individuals
   using this computer system without authority, or in excess of
   their authority, are subject to having all of their activities on
   this system monitored and recorded by system personnel. In the
   course of monitoring individuals improperly using this system, or
   in the course of system maintenance, the activities of authorized
   users may also be monitored. Anyone using this system expressly
   consents to such monitoring and is advised that if such
   monitoring reveals possible evidence of criminal activity, system
   personnel may provide the evidence of such monitoring to law
   enforcement officials.
   ```

2. Save the file into a place where all users have read access rights, such as the SYS:\PUBLIC folder on a NetWare server. For example, SYS:\PUBLIC\LOGINMSG.TXT
3. In iManager 2.x, select Roles and Tasks.
4. Select eDirectory Administration > Modify Object.
5. Select the container object where the user objects are located.
6. Select General > Login Script tab.
7. Enter a command, such as the one here to display the text from a banner file on your system: (this shows a file that was created with a text editor in SYS:\PUBLIC)

   ```
   DISPLAY SYS:\PUBLIC\LOGINMSG.TXT
   ```

8. Enter the command PAUSE to stop the login script display after the banner displays, so the user can more easily read it.
9. Save the changes.

References:

Novell, Inc. "Novell Login Scripts Guide." Novell Client Documentation. Novell, Inc. <http://www.novell.com/documentation/noclienu/login/data/front.html>

United States Department of Justice. "Appendix." Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. United States Department of Justice. <http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm>

3.7 Disable Simple Passwords

Description:

Simple passwords are a less-secure way to deal with the complexities of having multiple password hashes stored for different services in eDirectory.

In NetWare 6.5, Novell included the ability to synchronize all of the passwords assigned to a user object. This is called universal password. Without this feature, the user's simple password (for Native File Access Protocols, or NFAP) had to be set the same as their eDirectory (or NDS) password to remain synchronized. Even then, password controls, such as length and complexity could not be enforced on Simple Passwords.

Remediation: Utilize the universal password services and discontinue use of simple passwords. Also see rule Universal password services should be enabled.

References:

Novell, Inc. "Administrator Tasks for Native File Access for Windows Services." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/native/data/ac23vb4.html>

3.8 Universal password services should be enabled

Description:

Universal password is the modern framework for password policies and services on Novell eDirectory. It enforces uniform password policy across multiple authentication systems, such as Native File Access. Universal password services enables case sensitive passwords, support for extended or international characters, and advanced password policy enforcement, such as password complexity, all of which improve security.

Universal password requires eDirectory 8.7.3 or later.

Remediation:

Deploy universal password on your network as directed by the Universal Password deployment guide in the references.

Warning: Universal password can have undesired side effects when interoperating with older software, be sure to read the documentation prior to deployment.

References:

Novell, Inc. "Novell Password Management Administration Guide." Novell Password Management. 2005-10-13T00:00:00. Novell, Inc. <http://www.novell.com/documentation/password_management/pwm_administration/data/front.html>

3.9 Enable account access time restrictions

Description: If there are accounts that should definitely not be authenticating during times of the day, you can restrict the times that the accounts are active to increase security.

Remediation:

In ConsoleOne or iManager 2.x:

1. Select the user or users.
2. Edit the properties of the user(s).
3. Open the Restrictions > Time Restrictions tab.
4. Change the time restriction to the appropriate settings.
5. Save the changes.

Warning:

Be sure that the account isn't required to be accessed during off-hours (or hours where users should not be authenticated) in emergency purposes before implementing time restrictions. In companies that span time zones, be aware of the differences in time for the working hours at each location and how this setting will impact that.

This is a user-object setting. For new users, either these settings will have to be manually set, or you will have to create a user template object with the above settings, and then use the template to create all new users. Also see rule Create and use a user template object when creating users.

3.10 Enable Intruder Detection and Lockout

Description: In addition to setting strong password policies, eDirectory has the ability to disable certain accounts for a period of time if the number of invalid authetication attempts reaches a certain number. This is critical to stopping brute-force attempts at account and password discovery.

Remediation:

To enable intruder detection and lockout, use the following steps in ConsoleOne:

1. Open the properties of each container object that holds any user objects.
2. Select the General > Intruder Detection tab.
3. Enable Detect Intruders.
4. Set Incorrect login attempts to 15 or lower, depending on your policies.
5. Set Intruder attempt reset interval to 15 minutes or higher, depending on your policies.
6. Enable Lock account after detection.
7. Set lock account time to 15 minutes or higher, depending on your policies.
8. Click OK.

Warning: Be aware that if a user account name and sometimes context is learned, logging in multiple times with the wrong password can be used as a form of denial-of-service attack, in that the account authentication is disabled for a period of time. This is why it is important to rename the administrator accounts and keep user account names confidential. Also see rule

Administrator accounts should not be named common names, and Administrator accounts should not be located in the same container as other users.

3.11 Enable password policies

Description:

Because user account and password authentication is typically all that is used when authenticating users, it is critical to enforce password restrictions. Password restrictions are enforced in eDirectory by setting eDirectory attributes on the user objects.

Enabling universal password gives some additional security advantages including case-sensitive passwords. Also see rule Universal password capabilties should be enabled.

Current releases allow complex password policies to be deployed as part of an eDirectory system.

Another option to improve authentication security is to utilize third-party solutions to enable strong authentication using token or biometric authentication using Novell Modular Authentication Services which are included with eDirectory.

Remediation:

Using iManager, create the following configuration on the login policy object. (If you don't want it universally, you can enable it on the containers that hold user objects or on the user objects to be configured, although this is not recommended.

A prerequisite is that Universal Password services have been enabled. See rule Universal password services should be enabled.

1. Navigate to Passwords > Password Policies. If this isn't in iManager, read the documentation about deploying Universal Password and adding the password.
2. Locate your universal password policy and edit it, or create a new one with an appropriate name, such as base password policy.
3. When you get to step 2 - Select the Universal Password options, make certain Universal password and the advanced password rules are enabled. Click next.
4. At step 3 - Add rules to the Password Policy, enable the following settings by ensuring the fields have a white checkmark, or by entering the following values: Require a password, require unique passwords, set the number of days before password expires to 90 or less, limit the number of grace logins allowed to 15 or less, set the minimum number of characters in password to 8 characters or more, enable the allow numeric characters in password and allow special characters in the password. Click next.
5. Click next until you get to step 7 - assign the password policy.
6. Assign the password policy to the Login Policy object in the Security container at the top of the tree. This will make the policy universally active.
7. Click next, review the summary for errors and click finish.
8. If desired, you can create more restrictive policies for certain containers containing user objects, or for association with network administrator accounts.

Warning:

Universal password services can have undesired side effects when interoperating with older software, be sure to read the references in rule Universal password services should be enabled.

Users will have to change their passwords to non-repeating, long passwords on a regular basis (IE- monthly). If strong password policies are problematic in your environment, consider looking into multifactor authentication possibilities to increase security. (IE- biometric or token authentication)

References:

Novell, Inc. "Managing Passwords by Using Password Policies." Novell Password Management Administration Guide. 2005-10-13T00:00:00. Novell, Inc. <http://www.novell.com/documentation/password_management/pwm_administration/data/ampxjj0.html#ampxjj0>

3.12 Limit concurrent connections

Description: Unless you have a particular reason to allow it, user accounts should be limited in the number of times they can be authenticated to a tree to discourage account and password sharing, or leaving multiple workstations authenticated to eDirectory.

Remediation:

To restrict concurrent connections for users:

1. Open the Consoleone utility.
2. Select the user objects to restrict using the control or shift key select multiple objects.
3. Right-click one of the selected objects and select Properites of Multiple Objects.
4. Click the Restrictions > Login Restrictions tab.
5. Enable the Limit concurrent connections option.
6. Enter the number of maximum connections allowed for each user selected user account. Unless you have a specific reason otherwise, this should be set to 3.
7. Click OK to save the changes.

Warning:

This is a user-object setting. For new users, either these settings will have to be manually set, or you will have to create a user template object with the above settings, and then use the template to create all new users. Also see rule Create and use a user template object when creating users.

If you are using multiple protocols to connect to a server or connections are not cleanly logged out, multiple user connections may be needed to allow the user to reauthenticate without administrator assistance. If you have users that are experiencing problems logging in after logging out due to the client sessions not cleanly de-authenticating, first try using the recommended setting of three. If you experience further issues, try increasing the concurrent connections setting by one or two and test again.

3.13 Remove or disable inactive accounts

Description:

Inactive accounts are a security risk in that they can be exploited and used to compromise a network system. Any accounts that have not been active for 90 days or more should be deactivated.

Remediation:

There are many good third-party tools to run reports looking for inactive users, or you could use LDAP programming to easily locate them. To perform this task with existing Novell administration tools, we must use ConsoleOne on a Windows system.

Follow the steps on the referenced page to set up ConsoleOne reporting. Be sure to install reporting in the context where you want to manage the eDirectory objects, normally, at the top of the eDirectory tree.

The only change I noticed from the directions on the referenced web page, is that on Windows XP, you must use the navigation path, Control Panels > Administrative Tools > Data Sources (ODBC) to configure the ODBC DSN. Otherwise, you should be able to follow the directions exactly.

1. Follow the directions in the refererred to web page to configure ConsoleOne reports.
2. Browse to the NDS User Security Reports object in the tree, right-click on it, and select Generate Report.
3. Select the form, Users Not Logged In and click OK.
4. A list of all the users that have not logged in for 90 days or longer will be shown.

Make certain all of these accounts are disabled. If some of the accounts are already disabled, you may also want to run the Disabled User Accounts report and cross-reference the two to find only active accounts that have not been used.

References:

Novell, Inc. "Generating Reports in ConsoleOne." Novell AppNotes. 2003-03-01T00:00:00. Novell, Inc. <http://support.novell.com/techcenter/articles/ann20030301.html>

4 Management

4.1 Restrict access to web management applications

Description:

Individual ports can be blocked or restricted using the host firewall, see "Use a firewall to restrict access to network resources". However, the server running eDirectory allows web administration from standard web ports as well. If these standard ports are needed to host services, users will also have access to the web administration applications. They can then use the administration application login page to search for valid administrative accounts and passwords using repeated authentication attempts.

Remediation:

Access to web administration applications can be blocked using Apache's access restriction capabilities.

The Apache configuration file that allows access to the nps directory must be modified.

The following is an example list of files that will need changing based on the platform eDirectory is running atop. The file locations listed are just the defaults and may vary based on configuration changes. Check the root apache configuration files if the files are not located at these locations, and test the results to ensure that the changes made are working.

- Linux: /etc/opt/novell/iManager/nps-Apache.conf
- NetWare: SYS:\tomcat\4\conf\nps-Apache.conf
- Windows: C:\Program Files\Novell\Apache\conf\nps-Apache.conf

Perform the following steps to restrict access to iManager to one or more CIDR or IP range of addresses.

1. Edit the file with a text editor.
2. Find the Directory */webapps/nps section.
3. Change the "Allow from all" line to "Allow from XX.XX.XX.XX/YY" where XX.XX.XX.XX is the IP network address and /YY is the number of bits in the subnet mask. You can omit the /YY if you only want to allow a single host IP address.
4. Add additional hosts or CIDR ranges, each in its own "Allow from" line, if desired.
5. Find the Location /nps section.
6. Add the line "Order allow,deny" to the top of the section.
7. Change the "Allow from all" line to "Allow from XX.XX.XX.XX/YY" where XX.XX.XX.XX is the IP network address and /YY is the number of bits in the subnet mask. You can omit the /YY if you only want to allow a single host IP address.
8. Add additional hosts or CIDR ranges, each in its own "Allow from" line, if desired.
9. Save the changes.
10. Restart the Apache services to make the new settings take effect.

References:

The Apache Software Foundation. "Apache Module mod_access." Apache Version 2.0 Documentation. The Apache Software Foundation. <http://httpd.apache.org/docs/2.0/mod/mod_access.html>

4.2 Configure the iMonitor LockMask setting

Description: iMonitor contains the ability to block some requests until authentication has occurred. This protects the service from probes from unauthorized users or potential denial of service attacks. The LockMask setting does not override the eDirectory rights that must exist to use various management services.

Remediation:

Edit the SYS:\SYSTEM\NDSIMON.INI file on NetWare, /usr/share/ndsimon/ndsimon.conf on Linux, or the *install directory*\Novell\NDS\ndsimon.ini file in Windows.

1. Set the LockMask access level to 1 or higher to ensure eDirectory authentication.
2. Save and exit the file.

The following information explains the various LockMask levels from the Novell website:

Level 0: Require no authentication before iMonitor processes URLs. In this case, the eDirectory rights of the .[Public]. identity are applied to any request, and information displayed by iMonitor is restricted to the rights of the .[Public]. user. However, because no authentication is required to send URLs to iMonitor, iMonitor might be vulnerable to DoS attacks that are based on sending garbage in the URL.

Level 1: (Default) Before iMonitor processes URLs, require successful authentication as some eDirectory identity. In this case, the eDirectory rights of that identity are applied to any request and are, therefore, restricted by those rights. The same DoS vulnerability as level 0 exists, except the attack must be launched by someone who has actually authenticated to the server. Until a successful authentication occurs, the response to any iMonitor URL request is a login dialog box, so iMonitor should be impervious to attacks by unauthenticated users when it is configured in this state.

Level 2: Before iMonitor processes URLs, require successful authentication as an eDirectory identity that has supervisor equivalency on the server that iMonitor is authenticating to. The same DoS vulnerability as level 1 exists, except the attack must now be launched by someone who has actually authenticated as a supervisor of the server. Until a successful authentication occurs, the response to any iMonitor URL request is a login dialog box, so iMonitor should be impervious to attacks by unauthenticated users and non-supervisor authenticated users when it is configured in this state.

References:

Novell, Inc. "Ensuring Secure iMonitor Operations." Novell eDirectory 8.7.3 Documentation. Novell, Inc. <http://www.novell.com/documentation/edir87/edir87/data/a7gq3a8.html>

5 Privileges

5.1 Check for hidden objects in eDirectory

Description:

eDirectory contains a complex set of permissions including the ability to set "Inheritance Rights Filters" (IRF) that can be used to hide objects from even the Root administrator in the tree.

There are methods to find hidden objects within the tree to ensure that hidden, backdoor objects and accounts do not exist. Currently, this method requires a NetWare server somewhere in your eDirectory tree, because these tools are NetWare applications (NLMs).

Remediation:

If eDirectory is running on NetWare, you can run the Hidden Object Locator tool from Novell.

If there are any unauthorized hidden objects found, utilize tools such as EMADMIN to give you access to these objects, then investigate their trustee rights to track down any related eDirectory objects or filesystem files or folders.

Warning:

EMADMIN is a Novell-unsupported tool. Use at your own risk and only after making backups of critical information.

Preferably, load EMADMIN from a floppy, unless the "secure console" command is active. If you copy EMADMIN.NLM to the server filesystem, be sure to remove the file after using it, as it can be used to compromise security on eDirectory.

References:

Novell, Inc. "Using the Hidden Object Locator to find hidden objects." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10073403.htm>

Novell, Inc. "Emergency Admin." Novell Cool Solutions. Novell, Inc. <http://www.novell.com/coolsolutions/tools/1674.html>

5.2 Check your administrator users for unauthorized equivalence

Description: By setting a user to be an administrator equivalent, they are granted all rights that the administrator user is granted. This can be used by unauthorized users who have gained access to permanently grant administrator access to their account.

Remediation:

Perform the following steps in iManager 2.x:

1. Select eDirectory Administration > Modify Object
2. Browse to single or multiple network administrator user objects and click OK.
3. Click on the "Security Equal to Me" tab or menu.
4. Ensure that there are no accounts that are set as equal to your administrator accounts that are not authorized to be so.

5.3 Create and use a user template object when creating users

Description: When creating user accounts, make sure you have prepared a user template object when creating new user accounts to ensure the appropriate security-related configurations are done.

Remediation:

In ConsoleOne, select the location you wish to create the template object.

1. Create a new object, select Template, and click OK.
2. Name the template, select a user to base it on, if desired, check the define additional properties, and click OK.
3. Create the template according to the policies of your organization. Be sure to include the information from the "Enable password policies", "Limit concurrent connections", "Enforce volume space restrictions", and "Enable account access time restrictions". Select any other desired settings including group membership.
4. Click OK.

When creating new users, utilize this template to ensure that new user objects meet these setting requirements.

5.4 Disable Anonymous Directory Browsing

Description: Even without authenticating to eDirectory, users can attach to the directory and browse through the contexts and users by default. Security best-practices recommend only allowing authenticated users to see only the users and objects that they need access to.

Remediation:

Remove the [Public] object rights from the tree, and replace it with the tree root object [Root]. To do this, in ConsoleOne:

1. Right-click on the eDirectory tree [Root] object and select Properties.
2. Click Add Trustee
3. Browse to the top of the tree and add the top tree or root object as a trustee. Click OK.
4. Click on [All Attribute Rights], click Delete Property, and Yes.
5. The [Entry Rights] should be Browse with the Iinheritable option enabled.
6. Click OK.
7. Select the [Public] object.
8. Click Delete Trustee and Yes.
9. Click OK.

Warning: If no LDAP proxy user is configured, this disables contextless logins, LDAP anonymous binding browsing, and may interfere with the eGuide directory. Also see rule Configure an LDAP proxy user. These features being disabled may be desired in higher security environments.

References:

Novell, Inc. "Blank page is received when anonymous is used to search for users.." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10070486.htm>

5.5 Everyone group should not be used

Description: Privileges should be assigned by job function. Privileges should typically not be assigned through an "everyone" group, where all users are members of the group.

Remediation: Remove the "everyone" group and instead assign privileges based on organizational role, specific groups, or container objects.

5.6 Rights, especially Supervisor rights, should be assigned only where required

Description: It is easy, but violates a basic security principle, to assign more rights than what are necessary for a user to perform the work they are authorized to perform.

Remediation: Determine what rights are needed by each person that is performing work on your system, then ensure that the minimum rights are assigned to allow the user to perform their work.

5.7 Restrict access to the tree [Root] object

Description:

The [Root] object is the top object in any eDirectory tree. Unless the rights given at the [Root] are blocked from being inherited, any rights assigned here flow down throughout all parts of the tree.

Aside from the primary eDirectory administrator user object, other users, groups, organizational roles, or container objects should not have access to the [Root] object without a specific organizational need.

Remediation:

In ConsoleOne, perform the following steps:

1. Right-click on the tree object or [Root] object. In ConsoleOne, it is typically given the name of the tree.
2. Select Trustees of this Object.
3. Review the list of trustees for unauthorized objects.
4. Click on any object and click Assigned Rights to see what rights that object has for [Root].
5. Remove any unauthorized objects from the [Root] object and click OK.

Typical objects seen as trustees of [Root] are objects such as [Public] with only Browse Entry Rights, [Root] with only Browse Entry Rights, one or more administrator user, group, or organizational role objects with full rights including Supervisory rights, and Role Based Services objects with Supervisor Entry Rights.

Any unknown objects with Supervisory rights or with rights that exceed Browse Entry Rights, especially to the All Attributes Rights or Entry Rights are a concern and should immediately be investigated.

Warning: Removing a rights or trustee objects from the [Root] that are required to be there by some process may cause certain processes or authentications to fail. However, failing to secure the [Root] object properly exposes your entire tree to unauthorized access and modifications.

5.8 Examine top-level container for excessive privileges

Description: The top-level container(s) in an eDirectory tree should be examined for objects in the tree, such as users, groups, containers, organizational roles, with unauthorized access privileges.

Remediation:

Perform the following tasks:

1. Examine the trustee rights on the top-level Organization or other top-level containers, this includes all objects directly under the Root object.
2. Look for unauthorized objects, such as users, groups, containers, or organizational roles that have been given access to this container and usually all child containers and objects.

5.9 Restrict access to all NCP server objects

Description:

NCP Server objects are NetWare or Linux Novell Core Protocol servers, which are typically file servers with clients running the Novell Client software.

Ensure that all non-administrator users have no more than Browse, Compare, and Read rights.

Remediation:

Perform the following tasks:

1. Examine the trustee rights on the server object.
2. Look for unauthorized objects, such as users, groups, containers, or organizational roles that have been given access to this container and usually all child containers and objects.

Warning:

In eDirectory, having write [W] or supervisor [S] rights to the server object infers Supervisor rights to all NCP server volumes.

Ensure that only NCP server and volume administrators have write or supervisor rights to the server object.

References:

Novell, Inc. "Rights - DS Questions." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/2924799.htm>

5.10 Inherited rights filters should be used sparingly

Description:

Inherited rights filters (IRF) are used to block rights inheritance in the tree. This method of limiting access should be used sparingly, because it becomes difficult to determine where rights are being inherited.

Additive rights: directly assigning rights to all objects, versus subtractive rights: assigning rights at a higher level and then removing rights from specified lower levels, are normally less complex and easier to administer. You should only use IRFs in limited-scope cases where directly assigning all of the rights is more complex than using IRFs. Say for instance, that a parent container and all children but one should allow all users browse access, but that one child container should be hidden from all users.

Remediation:

Assign access only to organizational roles and groups directly to the objects and folders that that organizational role or group requires. Be aware that the default behavior for rights is to flow down and be inherited by all child containers and objects.

Use effective rights testing to ensure that proper rights are assigned to applicable objects.

Warning: Be cautious when using an IRF to block supervisor rights. Normally, you are required to directly assign another supervisor-rights object to the object that you are using an IRF to block supervisor rights to. Be aware although ConsoleOne and iManager usually warn you if you are removing the only object with supervisor rights to an object, but when using LDAP programmatically, you will get no such warning and may have to resort to assistance from Novell or other specialized utilities to resolve the issue.

5.11 Security Equivalence to user objects should not be used

Description: The use of security equivalence or "security equal to me" settings on a user object is an easy, but outmoded use of security privileges. It is a better practice to and easier to audit by assigning access privileges through organizational roles or groups.

Description: It is also easy for administrators who have set up the equivalence or other administrators unfamiliar with the user equivalence to delete the user object that the other users are equivalent to, thus wiping out the only record of all the privileges and forcing a backup restore or rebuilding all of the required privileges from scratch.

Remediation:

Create an organizational role or group object. Assign the rights to this object that you desire your security equivalent objects to have. Locate all objects using the security equivalence setting. Make the user object a member of the group or organizational role object. Remove the security equivalence.

To locate objects using security equivalence, perform the following steps in ConsoleOne. This can also be done using Novell iManager 2.x but with different steps.

1. In ConsoleOne, left-click on the container to search for user objects that are using security equivalence.
2. Select the menu Edit > Find.
3. Check the "Search subcontainers" checkbox.
4. Change the "Find type" to Advanced.
5. Set the "[Object Type]" equal to User.
6. Select the popup at the end of the line and select "Insert Row".
7. Set the first popup menu to "Security Equals".
8. Set the "Security Equals" equal to and enter the complete context of the administrator or other user object to test security equivalence to. (Don't use a leading period.)
9. Click Find.

Warning: You can ignore the NFAUUser object as this is a special object.

6 Protocols

6.1 Require TLS for all LDAP server operations

Description:

Even if the LDAP group requires TLS binds, in an attempted unsecured bind the information is still sent to the server before being denied, and could be captured.

Also see rule Ensure that LDAP group uses TLS.

Remediation:

To require TLS for all operations:

1. In Novell iManager 2.x, click the Roles and Tasks button Roles and Tasks button.
2. Click LDAP > LDAP Options/Overview > View LDAP Servers.
3. Click on the LDAP server object.
4. Click on the General > Connections tab/menu.
5. Check the Require TLS for all operations checkbox
6. Click OK to apply the changes.

6.2 Require TLS for simple binds with password for the LDAP proxy user

Description:

Ensure that the ldap proxy user requires TLS for simple binds with password.

If standard LDAP port 389 is disabled, this is not required.

Remediation:

Perform the following steps in Novell iManager. These steps are for iManager 2.5.

1. Click LDAP > LDAP Options/Overview > View LDAP Groups > the LDAP Group Object
2. In the authentication options, make sure the checkbox is checked to require TLS for simple binds with password, then click OK.

References:

Novell, Inc. "Creating and Using LDAP Proxy Users." Novell eDirectory 8.7.3 Documentation. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/agtxhz5.html#agxk83p>

Novell, Inc. "What is an LDAP proxy user?." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062428.htm>

6.3 Disable unencrypted LDAP

Description:

Even with TLS required for LDAP, normally on port 389, it is better to disable it and use SSL-tunnel encrypted LDAP, normally on port 636. This is because if an LDAP client is misconfigured, it will transmit clear-text authentication information to the LDAP server before being sent the error message that authenticiation requires TLS (STARTTLS). If this is not done, software watching network traffic would be able to gain unauthorized access to user names and passwords.

In a normal LDAP TLS session, a clear-text connection is established, then the STARTTLS command is issued, a secure encrypted connection is enabled, and finally the authentication takes place securely. The flaw occurs when a client is not configured to use STARTTLS. The user name and password is transmitted in the clear before the client software is notified that encryption or "confidentiality" is required.

This flaw does not exist with the SSL-tunnel encrypted LDAP, normally on port 636, because the SSL-encrypted tunnel session is established before authentication can occur.

Remediation:

Perform the following steps in Novell iManager. These steps are for iManager 2.5.

1. Click LDAP > LDAP Options/Overview > View LDAP Servers > the LDAP Server Object
2. In the Connections options, make sure the checkbox to "Enable Non-Encrypted Port" is unchecked, then click OK.

Warning:

The official IETF LDAPv3 standard specifies using LDAP, normally on port 389, with STARTTLS as the standard way of doing encrypted LDAP. However, it is insecure for the reasons cited in the description. SSL-tunnel encrypted LDAP, otherwise known as LDAPS, is a defacto, not IETF standard as is LDAPv3.

Disabling unencrypted-LDAP might require reconfiguring some software that uses LDAP on the server, so that it can communicate with the SSL-tunnel encrypted LDAP, normally on port 636, and some products may not support this form of the LDAP protocol.

References:

IETF LDAP (v3) Revision Working Group. "LDAP: Authentication Methods and Security Mechanisms." Internet Engineering Task Force (IETF). <http://www.ietf.org/internet-drafts/draft-ietf-ldapbis-authmeth-18.txt>

7 Storage

7.1 All tree partitions should be replicated across multiple servers

Description: With only a single server storing and serving an eDirectory replica, the loss of that server would mean the loss of the partition and potentially severe problems for the rest of the eDirectory tree.

Remediation: Ensure that all eDirectory partitions, there is at least one per tree: [root], are housed on at least three servers.

Warning: Too many replicas of an active partition can cause synchronization issues.

References:

Novell, Inc. "Replicas." Novell eDirectory 8.7.3 Administration Guide. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/fbaecheh.html>

7.2 Backup eDirectory files

Description:

Novell eDirectory is a complex database. One good way to ensure that it is being completely archived is by using the built-in backup and restore services in iManager.

The built-in eDirectory backup requires that you also perform a file-based backup. eDirectory is backed up to the server filesystem.

Remediation: The steps of exactly how to do a complete backup are beyond the scope of this checklist. Check the references for more information.

References:

Novell, Inc. "Backing Up and Restoring Novell eDirectory." Novell eDirectory 8.7.3 Administration Guide. Novell, Inc. <http://www.novell.com/documentation/edir873/edir873/data/a2n4mb6.html>
