Open Enterprise Server: NetWare (v1) Consensus Baseline Security Settings

Version 1.0

Date: 2006-08-03

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 NetWare has long been a stalwart of networking technology. It is a robust and mature platform for deploying file and print services. Although historically NetWare has not been widely deployed as an application server platform, with the release of NetWare 6.5, Novell is offering a platform that contains not only their prior NetWare services, but now include many industry-standard software platforms such as Apache, Tomcat, MySQL, Perl, PHP, Java, and OpenSSH. Although, security on NetWare has in some cases been taken for granted, the integration of new open-source technologies adds software that has required relatively more frequent patching, and a better knowledge of the different services to properly configure for security.

Utilize this benchmark in combination with eDirectory benchmark

Please note that there is a separate, but integral, part of this benchmark that is the CIS benchmark for eDirectory. As NetWare uses eDirectory as the core part of its security infrastructure and for user and server configuration management, it is key that the eDirectory benchmark be utilized as part of the NetWare benchmark.

Intended Audience

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

It requires a basic understanding of NetWare 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/ or NetWare 6.5 Administration Utilities - http://www.novell.com/documentation/nw65/admin_ovw/data/altwi33.html)

- iManager: Go to this URI from a web browser: https://serverip/iManager.html or https://serverip/nps/iManager.html
- ConsoleOne for Windows: Download and install from Novell downloads or launch from the server at SYS:\public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe
- 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.
- iMonitor: Go to this URI from a web browser: https://serverip:8009/nds
- Novell Remote Manager (NRM):Go to this URI from a web browser: https://serverip:8009
- Remote Server Console (part of NRM): Go to this URI from a web browser: https://serverip:8009/ServerScreens
- eGuide Admin: Go to this URI from a web browser: https://serverip/eGuide/admin/index.html

Environment settings and editing AUTOEXEC.NCF and STARTUP.NCF

When changing environmental settings, this document typically requests that the configuration change be made to AUTOEXEC.NCF or STARTUP.NCF files. However, there are other places that environmental settings can be made. It is just that this method will override the other ways to configure these settings. See Setting Server Parameter Values at http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html

Editing the AUTOEXXEC.NCF and STARTUP.NCF files can be performed a number of ways. The easiest is probably to use the built-in editor on the console, as the STARTUP.NCF file is not typically available from standard NetWare server volumes. To do this, type "EDIT AUTOEXEC.NCF" OR "EDIT C:\NWSERVER\STARTUP.NCF" at the server console.

- AUTOEXEC.NCF is at SYS:\SYSTEM\AUTOEXEC.NCF
- STARTUP.NCF is at C:\NWSERVER\STARTUP.NCF

Another method is to use the file browser and edit capabilities in Novell Remote manager by utilizing the following URIs:

- AUTOEXEC.NCF - https://serverip:8009/SYS/SYSTEM/AUTOEXEC.NCF?LOCKEDIT=TRUE
- STARTUP.NCF - https://serverip:8009/_DOSDRV_/C/NWSERVER/STARTUP.NCF?EDIT

Changing file system trustee rights

You must use ConsoleOne, the Novell Client, or Novell Remote Manager (NRM) to set file system trustee rights at this time. To use NRM, navigate to Manage Server > Volumes. Naviate to the file or folder to change trustee rights on. Then click the info icon to the left of the name. Trustee rights can be edited from this screen.

Restarting services

- Tomcat 4:
    1. Enter "tc4stop" at the system console.
    2. Switch to the logger screen console and look for two lines that show "java: Class org.apache.catalina.startup.Bootstrap exited successfully".
    3. Enter "tomcat4" at the system console.
    4. Wait about five minutes or until the logger screen shows "INFO:JK2 ajp13 listening on /0.0.0.0:9010", or something similar.

- Restarting the server
    1. Enter "reset server" at the system console.

Other Notes

Open Enterprise Server vs. NetWare

Open Enterprise Server (OES) is the latest version of Novell's modern network services platform. On it, you can run Novell's service stack. There are two primary core components to OES, the operating system and eDirectory. With OES you can deploy services atop either the NetWare or SUSE Linux operating system. This guide covers OES version 1 with services deployed atop NetWare 6.5.

As of the release of NetWare 6.5 service pack 4, there is no significant software difference between NetWare 6.5 and OES-NetWare. Either software package contains the same kernel, patches, and services, or stated another way, those who deployed NetWare 6.5, not Open Enterprise Server, will get all of the benefits of OES-NetWare operating system and OES applications in the most recent service packs.

NetWare 6

Although this document is written for OES-NetWare v1 which includes NetWare 6.5, many of these steps also apply to NetWare 6. Be aware that Novell will be ending support for NetWare 6 on November 1, 2006, and at that time, no new security patches will be released. In the meantime, if eDirectory 8.7.x and iManager 2.x are loaded on the NetWare 6 server, many of the remedial steps of this document can be followed as written. If this updated software is not loaded, the steps taken to remediate the issues in iManager may be somewhat different, or may require using a different administration tool, such as ConsoleOne.

1 System

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 Disable unneeded services

Description:

Running services or leaving services installed that are not actively used on production systems is a security issue because it takes administrator effort to maintain these services and keep them secure. Also, many services, by default, are not securely configured. Security best-practices dictate that as few services as possible to provide the necessary services should be running, or even installed, to reduce vulnerabilities, maintenance, and system complexity.

Remediation: Remove any unused or unnecessary services. Most services can be removed from the Novell Install utility in the GUI.

Warning: Ensure that a service is unneeded prior to removing it.

1.3 Install the most recent support packs and security patches

Description:

NetWare 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 NetWare, eDirectory, and application software.

References:

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

Novell, Inc. "NetWare 6.5 Patches." Novell Website. Novell, Inc. <http://support.novell.com/filefinder/18197/>

1.4 Delete old eDirectory backup files

Description:

When migrating to modern eDirectory (8.x), it is possible to leave behind old migration files. These old eDirectory migration or backup files could be obtained by unauthorized personnel and used to crack old accounts and passwords.

Modern versions of eDirectory do not use these files, but they may be left from a prior upgrade to eDirectory. Modern versions of eDirectory have securely encrypted eDirectory backup files. This backup is now normally stored in SYS:\SYSTEM\DSR_DIB\00000000.$DU.

Remediation:

If any of the following files exist, they should be removed from the system.

```
SYS:\SYSTEM\BACKUP.DS
SYS:\SYSTEM\BACKUP.NDS
SYS:\SYSTEM\DSREPAIR.DIB
```

1.5 Do not use bindery contexts to emulate bindery services

Description:

NetWare can emulate the older bindery services using a service called "bindery emulation". However, utilizing this technology opens the server up to attacks based on this legacy access methods, and used to leave a "backdoor" account called Supervisor. Current releases appear to no longer support authentication using the Supervisor account.

Most software and systems no longer need this technology and it should be disabled.

Remediation:

Search for and comment out or remove any line in the SYS:\SYSTEM\AUTOEXEC.NCF file that starts with:

```
SET BINDERY CONTEXT
```

Also, put the following command into the AUTOEXEC.NCF file, and type the command into the system console to make it take effect immediately:

```
SET BINDERY CONTEXT=;
```

This will disable the bindery emulation.

Warning: It is possible that some legacy software or systems might be using bindery services. One example would be network-connected printers using bindery services to make themselves available to the server. In that case, they would need to be reconfigured. All modern printers (anything made in the past several years) support eDirectory (NDS is another name for eDirectory), direct IP printing, or IPP printing, which can be used by NetWare printing services.

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

1.6 Enable SECURE.NCF should be enabled

Description:

The SECURE.NCF file contains a number of security settings to improve security on the NetWare server. When this setting is on, the SYS:\SYSTEM\SECURE.NCF file will be executed during startup. Some of these settings are obsolete, such as IPX NetBIOS replication, but others are still relevant, such as peforming NCP packet checking.

SECURE.NCF, by default, enables the following settings (many are already the default settings if they have not been changed)- unloads DOS from memory, disables the debugger, allows loading NLMs from only the system path, disables unencrypted passwords from legacy clients and enables strict checking of NCP packets.

Remediation:

To enable SECURE.NCF at startup, do the following:

1. Go to NetWare Remote Manager.
2. Select Manage Server > Set Parameters in the navigation pane.
3. Click on Miscellaneous.
4. Click on the value, set to on, and press OK.

To enable the SECURE.NCF settings immediately, type the following command at the system console:

```
SECURE.NCF
```

Ignore any warnings that might be shown while it is loading.

Warning: Some of the (non-default) settings in SYS:\SYSTEM\SECURE.NCF could disable some functionality of the server. Check the SECURE.NCF file for any settings that are not compatible with your environment.

1.7 Ensure that the SSL certificates are functioning properly

Description:

NetWare has full PKI SSL (X.509) certificate capabilities including the ability to act as a certificate authority (CA) across an organization. These digital certificates must be working properly for SSL/TLS to function. Because SSL/TLS are used to secure many communications with NetWare, this is a critical part of security.

Novell refers to digital certificates in the directory as Key Material Objects or KMOs.

When servers are renamed or moved, their links to their server certificates or the root certificate can be broken. This would cause all SSL services to stop functioning on that server, which would impact web applications using HTTPS and even things like NetWare Remote Manager and iManager services that require SSL.

Remediation:

Use PKIDIAG to ensure that the digital certificates are working properly:

1. If you are running NetWare 6, you will need to download PKIDIAG from the Novell website and install it on the server. Also see the references.
2. Launch the PKIDIAG utility on the console by typing the command:

   ```
   LOAD PKIDIAG
   ```

3. If you wish PKIDIAG to fix the problems instead of just reporting on the problems, enter option 4.
4. Start the procedure by entering 0.
5. If all problems were not resolved, you may need to re-run the procedure.

The results of the diagnostics can be found in SYS:\ETC\CERTSERV\REPAIR.LOG

After the certificates are repaired, either all of the services can be restarted that rely on the certificates, or the server itself can be restarted.

Warning:

This procedure can effect the entire tree that the server is part of. Be aware that generating a new root certificate has the effect of rendering all server certificates invalid until they too can be regenerated.

Ensure that you are running the latest service pack or that you have downloaded the latest version of PKIDIAG prior to running it.

References:

Novell, Inc. "How to use PKIDIAG?." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10095905.htm>

Novell, Inc. "PKI Diag Utility 2." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/2967938.htm>

1.8 Isolate the server network from the user and network administrator network

Description:

Many of the attacks to hijack a session or utilize the man-in-the-middle attacks can only work if the targets are on the same network as the attacker.

Remediation:

Use physical network or VLAN boundaries to create separate networks for the servers, users, and network administrators, with routing (and preferrably firewalling and intrusion prevention) between them. This ensures that a user cannot hijack an administrator session, however, it does not protect one user from another on the same network without further measures.

Also, be aware that unless your secure network port and infrastructure are physically secured, unauthorized individuals can plug into the network and begin probing for resources. One way to mitigate this risk is to enable encrypted, signed packets. Also see rule "NCP Packet Signature" and "Novell Client NCP packet signature configuration".

Warning:

Be aware that you should never set multiple VLANs (VLAN trunk) on an interface that you do not physically control both ends on. VLAN security can be bypassed by a user with the tools and the knowledge of how to do so. Normally, these VLAN trunk links are infrastructure to infrastructure only, not infrastructure to workstation, but a misconfiguration would allow unauthorized access into secured networks. User workstation ports should never be configured to accept any VLANs except a single, default, untagged one.

1.9 Malware or antivirus protection

Description: Because there are no known NetWare viruses, a NetWare server that will not have any client computers directly connected to the server filesystem or through email clients is not a malware threat. However, if any Windows systems will be connecting to the server, it is possible for Windows viruses to be stored on the server and spread to other Windows systems connected to the server. NetWare servers that are email servers will also need malware protection.

Remediation:

Implement malware (antivirus) protection as needed from one of the companies in the Novell Partner Guide.

1. Set Choose product to NetWare
2. Set Product Category to Anti-Virus
3. Select a product, purchase and implement according to the vendor's installation guidelines.

Warning: Some anti-malware products lock files on the filesystem while scanning. Be careful to follow vendor suggestions for running this software on servers with active databases. This includes software such as MySQL, Pervasive, Oracle, ZENworks Inventory, and GroupWise. Normally, there will be certain filesystem folders and files that should be excluded from real-time malware scanning.

References:

Novell, Inc. "Partner Product Search." Partner Product Guide. Novell, Inc. <http://www.novell.com/partnerguide/search.html>

1.10 Enable CPU Hog Timeout

Description: In certain circumstances, a single process can absorb nearly all system processing resources. This setting helps ensure that such processes are controlled. This would provide some protection against an intentional or unintentional denial-of-service attack due to a runaway process.

Remediation:

CPU Hog Timeout should be set to 30 seconds or less.

Enter the following setting at the system console and put this line into the SYS:\SYSTEM\AUTOEXEC.NCF file. You can also change this setting in the NetWare Remote Manager.

```
SET CPU Hog Timeout Amount = 30 seconds
```

Warning:

If CPU Hog Timeout is set too low, legitimate processes could be terminated unexpectedly.

If this server is part of a cluster, this parameter will be set to the same as the watchdog heartbeat timeout, which is set to eight seconds by default.

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

Novell, Inc. "Why does the set parameter for the CPU hog timeout change when you change the tolerance and watchdog timeout in clustering?." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?10074377.htm>

1.11 cron utility

Description:

CRON.NLM is an implementation of the cron daemon originally from the UNIX world for NetWare. It is used to launch processes at specific times on the server. The CRON.NLM on NetWare is subject to many of the same security risks that cron has on UNIX/Linux. Primarily, you must ensure that the automated cron schedule, stored in SYS:\ETC\crontab, along with any scripts called by it, are readable and writable only by system administrators.

Remediation:

Use the following methods to ensure CRON.NLM security:

- Unload CRON.NLM and remove it from the SYS:\SYSTEM\AUTOEXEC.NCF file if you don't need it. It is not loaded by default, but some server-based applications may require it.
- Ensure that the SYS:\ETC\crontab file is available only to system administrators.

Warning: Some server-based, third-party applications may require cron to operate properly.

1.12 Uninterruptable Power Supply

Description:

Be certain to include a UPS or some other power protection system to protect the server in case of power failure.

Be sure that the UPS has the ability to cleanly shut down the server or keep the server running for a period of time to allow organizational personnel to do so themselves. (IE- This time may need to be hours if alerts are paged and personnel may not be on-site.)

Remediation: Set up power backup systems and software that can monitor the state of power so that systems can cleanly power themselves down, if necessary.

2 Applications

2.1 Default user web page should be set to a user service or disabled

Description:

The default NetWare user web page describes all of the services available on the server. It should be disabled unless you are going to use it to connect your users to user services, such as Virtual Office.

Remediation:

Perform the following steps to select an installed NetWare web service as a new default web page for Apache on port 80:

1. Go to the default server web page. (IE- http://serverip)
2. Click the login text in the upper-right corner of the window.
3. Authenticate as network administrator.
4. At the bottom of the default screen, there is a default page selection dialog.
5. Select the desired service as the default page and click Set Page.

Perform the following steps to select a "forbidden" or other custom default web page for Apache on port 80:

1. Go to Apache web manager.
    - (https://serverip:2200/apacheadmin - you may be running on a port other than 2200)
2. Authenticate as network administrator.
3. Click on View Configuration.
4. Change the setting from the default, "SYS:/APACHE2/htdocs" to some other default web directory, or an empty directory, if you don't want to activate the default web page.
5. Save and then select Save and Apply to make it active.
6. Clear your cache and reload the default web page. It should state "Access forbidden!" if the default document directory is blank. You can still go to the former welcome page, if you choose, by typing the IRL of http://serverip/welcome

2.2 iPrint should be configured to use SSL

Description: iPrint should be implemented using SSL authentication. Without SSL the printer traffic is unencrypted and printer communication cannot be secured.

Remediation:

To secure a printer, the printer's security level must be set. To set a printer's security level, do the following:

1. In Novell iManager 2.x, click iPrint / Manage Printer.
2. Browse to and select the printer you want to enable Access Control for.
3. Click Access Control / Security.
4. Select the level of security you want for the printer.
5. Click OK or Apply to save your changes.

References:

Novell, Inc. "NetWare 6.5 Secure Printing Using SSL." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/iprint/data/aaxguq6.html>

2.3 MySQL administrator account password should be set

Description: MySQL, if loaded, should have its administrator or root account password set. Otherwise, unauthorized users may be able to read and change the contents of all MySQL databases.

Remediation:

At the console, type:

```
mysqladmin -u root_user
```

Where the root_user is typically "root".

If this fails, you already have a password set, or the administator user has been renamed. You can type:

```
mysqladmin -u root_user -p
```

And then type in the password, if you wish to change the root password.

To change the password at the MySQL monitor console, type:

```
SET PASSWORD FOR root@localhost=PASSWORD('new_password');
```

Where new_password is the MySQL root password that you want to use. It should not be the same password as your eDirectory administrator account.

Type "exit" to leave the MySQL monitor console.

Warning: If you have applications that are built using the root password to authenticate to the MySQL database (this is not a good idea), you will need to update them to reflect the new root password.

References:

Novell, Inc. "Manually Starting MySQL and Setting the Root Password." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/web_mysql/data/aji5hd3.html#aji5hd3>

. "Securing MySQL: step-by-step." SecurityFocus. SecurityFocus. <http://www.securityfocus.com/infocus/1726>

2.4 MySQL administrator user should not be named "root"

Description: The MySQL administrator user should not be named "root". This will avoid dictionary attacks on the MySQL administrator user.

Remediation:

At the console, type-

```
mysqladmin -u root -p
```

Type in the root password.

To change the administrator or root account at the MySQL monitor console, type:

```
connect mysql;
update user set user="new_root_user" where user="root";
flush privileges;
```

Where new_root_user is the new name of your administrator account.

Type "exit" to leave the MySQL monitor console.

Warning: If you have applications that are built using the root account to authenticate to the MySQL database (this is not a good idea), you will need to update them to reflect the new root account.

References:

. "Securing MySQL: step-by-step." SecurityFocus. SecurityFocus. <http://www.securityfocus.com/infocus/1726>

2.5 Print servers should be secured with a password

Description: All print services should be provided through NDPS and iPrint to take advantage of modern security mechanisms, however, if old print servers are going to be in use, all print servers should be secured using a password, otherwise any unauthorized user could print to the printer.

Remediation:

From the NWAdmin GUI, perform the following for each Print Server Object:

1. Select the appropriate Print Server object,
2. Right click the mouse button and select "Details"
3. Select the "Change Password" button, and
4. Enter a complex password.

2.6 eGuide initial configuration should be completed

Description:

When installed, eGuide allows anyone to configure it without an administrator account. This allows a non-authorized user to configure eGuide and potentially configure their own account or any other account as the eGuide administrator account, and also to share their, potentially unrestricted, view of eDirectory through eGuide.

Also see the eGuide rules in this section regarding eGuide configuration.

Remediation:

Perform the initial configuration for eGuide to ensure it is configured correctly.

1. In a modern web browser, navigate to the eGuide URI: http://serverip/eGuide
2. Select the Quick Setup link.
3. Click Next.
4. Select the appropriate LDAP data source and click Next. Also see rule "eGuide should use SSL for remote LDAP connections".
5. Select the authentication proxy credentials and click Next. Be sure to select an account especially configured for this purpose. Also see rule "eGuide should use a secured proxy user for LDAP access".
6. Select the appropriate eGuide administrator accounts by searching for and selecting each one, then click Next.
7. Click Finished.

2.7 eGuide should use a secured proxy user for LDAP access

Description:

eGuide is a directory service which allows one to view all or a subset of the user accounts and many related attributes in eDirectory in a "white pages" directory format. By default, the application will display all user accounts. Although this can be useful, it can also be a security risk which would allow for information gathering of unauthorized individuals.

Remediation:

By using a proxy user for eGuide LDAP access, you can better restrict which information you provide in the eGuide white pages.

1. Go to the eGuide Administration page.
2. Authenticate to the eGuide Administration.
3. Navigate to Configuration > LDAP Data Sources
4. For each data source, select the edit link.
5. Ensure that an appropriate proxy user account is filled into the Proxy user name field and the Proxy password field contains the associated password.
6. Click save.
7. Repeat for each LDAP data source.

For more details about the eGuide LDAP proxy user, see the references.

References:

Novell, Inc. "LDAP Data Sources: Configuring LDAP Data Sources." Novell eGuide 2.1.2 Administrator Guide. 2005-04-15T00:00:00. Novell, Inc. <http://www.novell.com/documentation/eguide212/eguide/data/ammcida.html#brtjx0n>

2.8 eGuide reduce idle session timeout

Description: By default the eGuide idle session timeout is 60 minutes. By reducing the timeout to 15 minutes, it is less likely to be accessed by unauthorized users.

Remediation:

Reduce the length of the eGuide inactive session timeout to 15 minutes or less.

1. Edit the eguide.cfg file in the Tomcat eGuide configuration directory. Typically, this is located at SYS:\tomcat\4\webapps\eGuide\web-inf\config path.
2. Change the value of the Security.timeout setting to "Security.timeout=15" to drop sessions after that many minutes.
3. Restart Tomcat to make changes active.

References:

Novell, Inc. "Improving eGuide Performance: Reducing Session Time-Out." Novell eGuide 2.1.2 Administrator Guide. 2005-04-15T00:00:00. Novell, Inc. <http://www.novell.com/documentation/eguide212/eguide/data/bqtj2u7.html#bo8cftf>

2.9 eGuide should require authentication to access

Description: eGuide is a directory service which allows one to view all or a subset of the user accounts and many related attributes in eDirectory in a "white pages" directory format.

Remediation:

Ensure that all users must authenticate to access eGuide.

1. Go to the eGuide Administration page.
2. Authenticate to the eGuide Administration.

3. Navigate to Security > Restrictions
4. Ensure that force users to authenticate is checked.
5. Click save.

Warning:

Requiring authentication without using HTTPS is a security risk. Also see rule eGuide should require HTTPS to access.

References:

Novell, Inc. "Configuring eGuide Security Settings: Restrictions." Novell eGuide 2.1.2 Administrator Guide. 2005-04-15T00:00:00. Novell, Inc. <http://www.novell.com/documentation/eguide212/eguide/data/ad48882.html>

2.10 eGuide should require HTTPS protocol to access

Description: eGuide is a directory service which allows one to view all or a subset of the user accounts and many related attributes in eDirectory in a "white pages" directory format.

Remediation:

Ensure that all users must use the HTTPS protocol to access eGuide.

1. Edit the ./webapps/eGuide/WEB-INF/web.xml with a text editor.
2. Add the following lines immediately before the "</webapp>" tag.

```
<security-constraint>
<web-resource-collection>
<web-resource-name>SSL-requiring Area</web-resource-name>
<url-pattern>/servlet/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

3. Save and exit the editor.
4. Restart tomcat.

2.11 eGuide should use SSL for remote LDAP connections

Description: eGuide uses LDAP for its whitepages information source. Without SSL the LDAP protocol is unencrypted and insecure. This is important when an LDAP source is not on the same server as eGuide.

Remediation:

eGuide should utilize SSL for remote LDAP connections.

1. Go to the eGuide Administration page.
2. Authenticate to the eGuide Administration.
3. Navigate to Configuration > LDAP Data Sources
4. For each data source, select the edit link.
5. If the hose name refers to a remote host or IP address or a source that requires SSL, ensure that Enable SSL is checked. Also ensure that the appropriate port, usually 636, is selected.
6. Click save.
7. Repeat for each LDAP data source.

Warning:

Enabling SSL requires that the LDAP source support SSL. If it does not LDAP communications will cease to function. eDirectory typically supports SSL LDAP connections. Also see rule Disable unencrypted LDAP in the eDirectory benchmark.

References:

Novell, Inc. "LDAP Data Sources: Transport Layer Security." Novell eGuide 2.1.2 Administrator Guide. 2005-04-15T00:00:00. Novell, Inc. <http://www.novell.com/documentation/eguide212/eguide/data/ammcida.html#brtjx48>

2.12 iFolder should be set to use HTTPS as the passphrase form protocol

Description:

iFolder should have HTTPS set as the passphrase form protocol. This is the default setting. If this is set to HTTP, the iFolder passphrase will be transmitted in clear text across the network.

Remediation:

Enable HTTPS for iFolder authentication.

1. In iManager, navigate to File Access (NetStorage) > iFolder Storage Provider
2. Set Passphrase Form Protocol field to: HTTPS
3. The Secure Port field should typically be set to 443, unless you are running HTTPS on a different port.
4. Click Submit.

References:

Novell, Inc. "Understanding the NetStorage Configuration Settings: iFolder Storage Provider." NetWare 6.5 NetStorage Administration Guide. 2005-02-28T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/netstor/data/aji1610.html#bulrmad>

2.13 NetStorage connections should require encryption

Description:

NetStorage by default allows connections over HTTP. This basically sends the user name and password in clear text across the network connection.

Because the default mode of operation is to allow authentication with the user's eDirectory name and password, it is important that this connection should be encrypted.

Remediation:

To force NetStorage to use a secure connection. This must be done through the Apache configuration files. See the reference for more information.

Another option is to block all access to port 80 and require users to access using HTTPS over port 443, however, this can impact web applications that do not require authentication and do present a security risk running on port 80.

Warning: Editing the Apache configuration files as suggested in the reference will impact other services running on the same server from port 80.

References:

Novell, Inc. "Making NetStorage secure." Novell Cool Solutions. 2003-04-17T00:00:00. Novell, Inc. <http://www.novell.com/coolsolutions/qna/1104.html>

2.14 Remove Tomcat documentation

Description: If Tomcat is installed, it loads documentation that can be accessed by anyone.

Remediation:

It is considered a security best practice to remove information that can be accessed by unauthorized users to find out more about your environment. This documentation only serves a purpose in a development environment.

If this server is a production server, perform the following steps:

1. In a modern web browser, navigate to the Tomcat Manager URI: https://serverip/tomcat/htmlmanager/
2. Authenticate with the admin username and password.
3. Navigate to the Main HTMLManager page.
4. Find the line where Path is /tomcat-docs.
5. **Make certain you click in the right line, there is no confirmation and no undo.**
6. Click on the Remove link.
7. Repeat the process with the /tomcat/manager web application. This "application" is actually just documentation for the tomcat manager applications. **Be sure to remove the /tomcat/manager application, not the /tomcat/htmlmanager application.**
8. Close the browser.

2.15 QuickFinder should be disabled or secured

Description: QuickFinder is a search engine for web content stored on the server. It should either be disabled, or secured.

Remediation:

Perform the following steps:

1. In a web browser, go to the following URI: https://servername/qfsearch/admin
2. Navigate to Default Settings > Security
3. The settings should be configured as follows:
    - AdminServlet.properties > AdminServlet.RequireSSL = TRUE
    - AdminServlet.properties > AdminServlet.Authenticate = TRUE
    - Security.properties > Security.RequireHTTPS = TRUE

Also see the reference for other security best practices.

References:

Novell, Inc. "Security Considerations." QuickFinder Server Documentation. Novell, Inc. <http://www.novell.com/documentation/qfserver40/qfserver/data/bu0ossa.html#bu0ossa>

3 Auditing / Monitoring

3.1 Enable and use auditing services

Description:

NetWare 6.5 comes with Novell Audit (formerly Novell Nsure Audit). Novell Audit includes the capability to track events on your NetWare 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". (View the associated links for more information.)

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

Novell Nsure 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 the NetWare server and eDirectory tree.

References:

Novell, Inc. "Novell Nsure Audit 1.0.2 Administration Guide." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nsureaudit/nsureaudit/data/front.html>

Novell, Inc. "Nsure Audit 1.0.x Netware 6.x installation guide." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10091433.htm>

3.2 Enable console logging

Description:

NetWare includes many different logs to keep track of various types of events on the server.

System console logging stores everything that shows on the system console screen to a file that can be archived and searched.

The Logger Screen records all messages printed by NetWare applications (NLMs) that do not send output directly to their own screen. The contents of this screen can be saved to a file that can be archived and searched.

The following logs are available: Console log (covered here), Logger screen (covered here), System error log (SYS:\SYSTEM\SYS$LOG.ERR), Boot error log (SYS:\SYSTEM\BOOT$LOG.ERR), Abend log (SYS:\SYSTEM\ABEND.LOG), Health log (SYS:\SYSTEM\HEALTH.LOG), NetWare Remote Manager Log (SYS:\HTTPLOG.TXT). If utilizing traditional volumes (instead of NSS) you can also check the VOL$LOG.ERR file.

Also see other auditing rules for additional logs and reports.

Remediation:

Console Screen Logging

Edit the SYS:\SYSTEM\AUTOEXEC.NCF file.

The CONLOG.NLM is configured to load by default, you will have to remove any line that has "conlog" in it.

Add the following line to the AUTOEXEC.NCF:

```
LOAD CONLOG ARCHIVE=YES NEXT=03:00 ENTIRE=YES MAXIMUM=100
```

To make this setting effective immediately, type the following commands at the console:

```
UNLOAD CONLOG
LOAD CONLOG ARCHIVE=YES NEXT=03:00 ENTIRE=YES MAXIMUM=100
```

This will turn on console logging and will rotate the logs every morning at 3:00AM with a maximum of 100 days of logs. Older logs can be restored from backups.

Logs will be stored in sys:\etc\console.log. Prior logs will be renamed to console.000, console.001, and so forth.

Logger Screen Logging

First, the logger screen save path needs to be set. You can do this by issuing the following console command, and placing the command at the end of the SYS:\SYSTEM\AUTOEXEC.NCF file. (This example puts the log into a \LOGS directory on the DATA volume.)

```
LOGGERPATH = DATA:\LOGS
```

Then the Logger Screen contents can be saved to the target directory at any time by using the LOGGERSAVE console command.

Enter the following command at the console and put it at the end of the SYS:\SYSTEM\AUTOEXEC.NCF file to save the Logger Screen. (Putting this command in the AUTOEXEC.NCF effectively saves the startup output.)

```
LOGGERSAVE
```

To have this command execute daily or at other regular intervals, you can use either the NetWare Remote Manager scheduler or CRON to create a repeating job that runs the LOGGERSAVE command. Be aware that each time it is run, it will overwrite the former log.

Warning: Log files can fill your storage on the SYS volume causing issues for the server. Be certain to occasionally check the log files and archive and remove them as necessary.

3.3 Enable boot error log

Description:

This setting ensures that boot error messages will be logged. It is enabled by default, but should be ensured to continue to be enabled.

View this log in the SYS:\SYSTEM\BOOT$LOG.ERR file.

Remediation:

The following console command should be put into C:\NWSERVER\STARTUP.NCF. The setting will be active upon the next server restart.

```
SET Boot Error Log = ON
```

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

3.4 Rotate Log Files

Description:

By default, NetWare deletes old log files when they reach their maximum set size. Best practices dictate that these files are saved instead of deleted.

Remediation:

Enter the following setting at the system console and put this line into the SYS:\SYSTEM\AUTOEXEC.NCF file. You can also change these settings in NetWare Remote Manager at Manage Server > Set Parameters.

You can enable this by using the following commands:

1. SET Volume Log File State = 2
2. SET Server Log File State = 2
3. SET Volume TTS Log File State = 2
4. SET Boot Error Log File State = 2

Warning: Log files can fill your storage on the SYS volume causing issues for the server. Be certain to occasionally check the log files and archive and remove them as necessary.

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

3.5 Use system reports to create a configuration baseline and monitor changes

Description:

Having unauthorized applications or configurations on your NetWare server is a sure way to create security holes and availability problems.

Novell provides a report to track the configuration of server including all applications that are running.

Creating a baseline report and then tracking any changes improves security through configuration change control.

Remediation:

A quick user friendly way to view most of these logs and generate related reports is to use the Reports / Log Files toolbar button in Novell Remote Manager. To do this:

1. Authenticate to Novell Remote Manager. (https://serverip:8009)
2. Click Reports/Log Files button on toolbar across top of window.
3. Select the reports and log files you wish to view.

To view volume trustee reports:

1. Authenticate to Novell Remote Manager. (https://serverip:8009)
2. Navigate to Manage Server > Volumes.
3. Click the Volume Info Icon next to the volume to report on.
4. Select Volume Trustee Report link to generate the report.

Another option is to use command-line tools to pull configuration information and compare differences over time to ensure configuration change control, although how to do this in an automated fashion is beyond the scope of this document. The steps to perform this procedure manually are listed below.

The following command will generate a lengthy configuration report that is stored in the file SYS:\SYSTEM\CONFIG.TXT:

```
LOAD CONFIG /A
```

The following command will store all of the mounted volumes assigned trustee rights in the file SYS:\SYSTEM\TRUSTEES.TXT:

```
LOAD TRUSTEE.NLM /ET SAVE ALL SYS:\SYSTEM\TRUSTEES.TXT
```

The results of these reports can be archived and then future reports can be generated and compared against the earlier one to view what changes have occurred.

One free, command-line tool for comparing two text documents is DIFF. DIFF is part of the GNU diffutils package. It is available for Windows, Linux, NetWare, and many other platforms.

An example of using the diff command to find the differences between two configurations is illustrated below:

```
diff file1 file2 > results.txt
```

This launches diff, compares file1 to file2, and places the results into a file called results.txt.

Another option to view and compare the CONFIG.NLM reports is the aging, but still useful NetWare Config Reader utility. Also see the link in the references.

References:

Novell, Inc. "Generating, Viewing, and Sending Server Reports." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/remotemgr/data/br7xwcf.html#br7xy04>

Novell, Inc. "CONFIG.NLM for NetWare." Novell Knowledgebase. 2005-08-18T00:00:00. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?2972074.htm>

"Diffutils for Windows." GnuWin32 Project. <http://gnuwin32.sourceforge.net/packages/diffutils.htm>

"Diff for NetWare." Novell Forge (Unsupported). <http://forge.novell.com/modules/xfmod/project/?diff>

Novell, Inc. "NetWare Config Reader." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/2943247.htm>

3.6 Utilize security reports to monitor server

Description: This is not a configuration setting, but a security recommendation. You can review the Security report and Server settings reports.

Remediation:

To view the server security report:

1. Go to the NetWare Remote Manager (https://server:8009)
2. Click the Diagnose Server > Reports / Log Files in the navigation frame.
3. Click View Security Report or e-mail the report to your account to view and print it.

To view the server settings report:

1. Go to the NetWare Remote Manager (https://server:8009)
2. Click the Manage Server > Set Parameters link in the navigation frame.
3. In the Save Settings to a File on Volume Sys: field, accept the default filename (settings.txt) or enter a different filename.
4. Click the Save button to the right of the Save Settings to a File on Volume Sys: field.

5. Browse to the file on the server and print it.

References:

Novell, Inc. "Generating, Viewing, and Sending Server Reports." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/remotemgr/data/br7xwcf.html#br7xy05>

3.7 Disable "Audit Passwords"

Description: NetWare had a now-defunct "audit password" that could be used to enable special audit capabilities within the system. As this is no longer used, it should be disabled. If you are interested in auditing passwords (that is **not** what this setting does), consider Novell Audit, or other modern auditing products.

Remediation:

Enter the following setting at the system console and put this line into the SYS:\SYSTEM\AUTOEXEC.NCF file. You can also change this setting in the NetWare Remote Manager.

```
SET Allow Audit Passwords = OFF
```

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

4 Authentication

4.1 Disable unencrypted passwords

Description:

Do not allow unencrypted passwords to legacy clients. This is also included when enabling Secure Console. Also see rule "Secure console should be enabled."

Remediation:

Enter the following setting at the system console and put this line into the SYS:\SYSTEM\AUTOEXEC.NCF file. You can also change this setting in the NetWare Remote Manager.

```
SET ALLOW UNENCRYPTED PASSWORDS = OFF
```

Warning: Very old Novell client software or older non-Novell clients may not function with encrypted passwords.

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

4.2 Disallow Macintosh AFPTCP unencrypted passwords

Description:

NetWare can serve as a Macintosh server. It includes the option to send passwords across the network to help automatically update the Macintosh simple passwords. Unforuntately, these passwords can be captured by unauthorized persons, and used to compromise the account.

Instead, you should use either ConsoleOne or universal password services to manage your Macintosh user passwords. Also see the universal password services section in the eDirectory benchmark.

Remediation:

To ensure that unencrypted passwords are not allowed, look in the SYS:\SYSTEM\AUTOEXEC.NCF file for the following line:

```
LOAD AFPTCP CLEARTEXT
```

Replace it with the following to fix the flaw.

```
LOAD AFPTCP
```

To make the change happen immediately, type the following commands into the console:

```
UNLOAD AFPTCP
LOAD AFPTCP
```

Warning: This will disable the ability for end users to update their "simple passwords" from their eDirectory passwords, unless you implement eDirectory universal password services.

References:

Novell, Inc. "Administrator Tasks for Native File Access for Macintosh Services." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/native/data/ac1pdri.html>

4.3 Install an SSH login banner

Description:

Security best practices recommends placing a login banner on all services that support banners. SSH include the ability to enable a banner on nearly any platform that it is supported on, including NetWare.

The exact wording of the banner is beyond the scope of this document, but an example is shown below. Also see rule Enable a login banner in the login script in the eDirectory benchmark.

Remediation:

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. Create a text file containing your security banner text in the following file-sys:/etc/ssh/banner.txt.
3. Edit the SYS:ETC\ssh\sshd_config file to include the following line:

```
Banner sys:/etc/ssh/banner.txt
```

4.4 NetWare Remote Manager banner

Description:

Enable a banner for NetWare Remote Manager.

The exact wording of the banner is beyond the scope of this document, but an example is shown below. Also see rule Enable a login banner in the login script in the eDirectory benchmark.

Remediation:

To add a customized disclaimer or text screen:

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. Access the sys:\login\prtltxt.htm file.
3. Change the template text to a message of your choosing.
4. Rename the file to prtldisc.htm.

References:

Novell, Inc. "Setting Up a Customized Disclaimer or Text Screen." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc.
<http://www.novell.com/documentation/nw65/remotemgr/data/ajoqdn5.html>

4.5 Disable SAdmin and SDebug accounts

Description:

The SAdmin and SDebug accounts are emergency and debugging Novell Remote Manager accounts that do not exist in eDirectory. Essentially, these accounts are testing and emergency backdoor accounts that are disabled on default installations. These accounts should be disabled on production systems.

If the functionality from these accounts are required they should have strong (complex and very long) passwords applied to them to minimize the possibility of their being used to compromise the server. These accounts are not affected by intrusion detection, and should be changed on a regular basis.

The passwords used for each account have different properties than regular eDirectory passwords:

1. They are case-sensitive.
2. They can have maximum of 80 characters.

Remediation:

To disable the accounts, do the following:

1. Go to Novell Remote Manager and authenticate with an administrator account.
2. Click the configure icon in the toolbar across the top.
3. Click Disable Emergency account (SADMIN user) and clear password.
4. Click the configure icon in the toolbar across the top.
5. Click Disable Debug account (SDEBUG user) and clear password.

References:

Novell, Inc. "Controlling the Emergency Account." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/remotemgr/data/bqtzy2d.html#bqtyfn9>

Novell, Inc. "Controlling the Debug Account." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/remotemgr/data/bqtzy2d.html#bqtyi7k>

5 Console

5.1 Disable the NetWare GUI unless you are using it

Description:

The NetWare Graphical User Interface (GUI) is an implementation of X, otherwise known as X11. X11 has numerous vulnerabilities. Therefore it would be best to disable the loading of this service except while it is in use.

If you must allow it to continue running or plan to use the NetWare GUI intermittantly, be sure to set up a packet filter for TCP/UDP on port 6000. Also see the "Enable the server host firewall" rule for more details.

Remediation:

Remove the following line from the SYS:\SYSTEM\AUTOEXEC.NCF file:

```
STARTX
```

On the NetWare console, switch to the NetWare GUI using Ctrl-Esc, and typing in the number. Then exit the GUI from the Novell menu.

Warning: Some third-party java software may require the GUI to be loaded to function. Also, the GUI must be used when running the graphical Novell installation program or other NetWare GUI utilities such as ConsoleOne from the NetWare server console.

5.2 Lock Console with Scrsaver.nlm Screensaver

Description:

The console should be locked to block unauthorized access from local or remote users without the appropriate rights.

This command allows you to set a locking screensaver that will require an eDirectory login with appropriate rights to unlock the console.

Remediation:

The following console commands should be put into SYS:\SYSTEM\AUTOEXEC.NCF. Putting it near the top of the file decreases the chance that the AUTOEXEC.NCF could be aborted or bypassed on a restart. Then they should be typed into the console for immediate effect.

```
LOAD SCRSAVER
SCRSAVER ENABLE;ENABLE LOCK;DELAY=300;NO PASSWORD;ACTIVATE
```

The above commands load the screen saver, enables the screen saver, enables password-protected unlocking, sets the automatic screensaver lock delay to 300 seconds or 5 minutes, disables the requirement for a password only if directory services are disabled, and immediately activates the locked screen saver.

Warning:

Not using the "NO PASSWORD" option does increase security but may lead to a situation where the server is in the middle of the DSREPAIR job and locks directory services. If the screensaver auto-enables after the delay, you would have a locked console that could not be recovered from without switching off the server and resetting. (If the SECURE CONSOLE command is not used, the SCRSAVER.NLM lock can be bypassed by using the console debugger.)

Of course, by using the "NO PASSWORD" command, if an intruder is able to make directory services unavailable for any reason, they would be able to unlock the console without a password.

References:

Novell, Inc. "Using SCRSAVER to Lock the Server Console." NetWare 6.5 Server Operating System Documentation Administration Guide. 2005-04-01T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hpmfqfmr.html#hmcbcrx9>

5.3 RConAG6 and RConsoleJ should not be used for remote management

Description:

RConAG6 and RConsoleJ should not be used for remote console access on the server.

RConsoleJ does not support authentication from the directory, but requires a password to be placed into AUTOEXEC.NCF, LDRCONAG.NCF, or typed from the console at each startup. This means that every administrator who accesses the server will have to share the same password, so that there can be no user access tracking. This also makes changing passwords difficult on multiple servers and does not support eDirectory features such as Intruder Detection. Also, although the RConsoleJ password itself can be encrypted in the configuration files, the RConsoleJ protocol itself can be used insecurely if not properly configured. Also see Configure RConsoleJ for secure access only.

Other remote console methods, such as the NetWare Remote Manager web console and SSHv2 services can be used securely.

Remediation:

Remove any of the following lines from SYS:\SYSTEM\AUTOEXEC.NCF on the server:

```
RCONAG6.NLM
LOAD RCONAG6
LDRCONAG.NCF
LDRCONAG
```

Unload it from the server if it is loaded using the following command:

```
UNLOAD RCONAG6
```

If there are any modules which must be unloaded first, unload all of those modules, then unload RCONAG.

Remove the RCONAG6.NLM file from the SYS:\SYSTEM folder.

Warning: This will disable RConsoleJ remote console clients.

References:

Novell, Inc. "Remote Server Management." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sman_enu/data/hqcrag0y.html>

5.4 Configure RConsoleJ for secure access only

Description: RConsoleJ does not use eDirectory passwords and does not follow the intruder detection and lockout settings, so it should not be used at all, if possible. If it must be used, RConsoleJ can be configured to encrypt the remote console password in the script files that load it, and be configured to only allow secure, encrypted communications. Also see rule RConAG6 and RConsoleJ should not be used for remote management.

Remediation:

1. Be sure that RConsoleJ isn't already loaded by typing: UNLOAD RCONAG6
2. Type the following command: RCONAG6 ENCRYPT
3. Enter the desired remote password.
4. Enter '0' for the TCP port number for "Unsecure Connection".
5. Enter '0' for the SPX port number.
6. Press enter to accept the default 2036 port for TCP port number for "Secured Connection", or enter a preferred custom port number.
7. Press Y to write out the SYS:\SYSTEM\LDRCONAG.NCF file.
8. Exit the RCONAG6 configuration screen.
9. Type the following command: UNLOAD RCONAG6
10. Edit the SYS:\SYSTEM\LDRCONAG.NCF file. You can do this from the console by typing the following command: EDIT LDRCONAG.NCF
11. Replace each of the two zeros, separated by spaces near the end of the line with a "-1" (without the quotes) instead. This will disable insecure TCP communications and SPX connections.
12. Exit and save the file.
13. To load RConsoleJ securely, use the following command: LDRCONAG.NCF
14. Put the LDRCONAG.NCF command into your SYS:\SYSTEM\AUTOEXEC.NCF if you wish to have the remote console capability load at each startup.

5.5 REMOTE and RConsole should not be used for remote management

Description:

REMOTE.NLM, RConsole, and telnet should not be used for remote console access on the server.

REMOTE.NLM does not support authentication from the directory, but requires a password to be placed into AUTOEXEC.NCF or typed from the console at each startup. This makes changing passwords difficult on multiple servers and does not support eDirectory features such as Intruder Detection. Although the password can be encrypted in the configuration files, the RConsole protocol itself is not secure, and requires IPX to function.

Telnet can be used with REMOTE, but is also not secure as everything is sent in clear text across the network.

Other remote console methods, such as the NetWare Remote Manager web console or SSHv2 can be used securely.

Remediation:

Remove any of the following NLMs being loaded in from SYS:\SYSTEM\AUTOEXEC.NCF on the server:

```
RSPX.NLM
REMOTE.NLM
XCONSOLE.NLM
```

Unload it from the server if it is loaded using the following command:

```
UNLOAD REMOTE
```

If there are any modules which must be unloaded first, unload all of those modules, then unload REMOTE.

Remove the REMOTE.NLM file from the SYS:\SYSTEM folder.

Warning: This will disable RCONSOLE, XCONSOLE, and telnet server console access methods.

5.6 Secure console should be enabled

Description:

After you have provided physical security for your server, you can use the SECURE CONSOLE command to provide the following security features, while still allowing you to use the console:

- Prevent NetWare Loadable Module programs from being loaded from any directory other than sys:system or c:\nwserver. This means that no one can load an invasive NLM from a server's diskette drive or boot partition unless it is already in a search path.
- Prevent keyboard entry into the operating system debugger. This restricts the ability to alter the operating system.
- Prevent anyone from changing the date and time. Some security and accounting features depend on date and time for their enforcement.
- When you issue the SECURE CONSOLE command, the server must be taken down and rebooted to unsecure the console. Now that server parameter settings are persistent in

NetWare, you can shut down the server without losing the settings you made to optimize and tune your server.

- When you use SECURE CONSOLE with the NetWare Remote Manager or RCONSOLEJ, access is subject to the protections provided by SECURE CONSOLE.
- SECURE CONSOLE does not lock the server console. You can lock the console by using SCRSAVER. If the console is locked using the console-locking feature, an intruder can still access the console from a remote workstation; however, the intruder must still be authenticated to eDirectory through the SCRSAVER console lock.

Remediation:

The following console command should be put into SYS:\SYSTEM\AUTOEXEC.NCF. Putting it near the bottom of the file, to avoid conflicts with loading NLMs that are not in the SYS:\SYSTEM or C:\NWSERVER directories. After editing the AUTOEXEC.NCF file, the command should be typed into the console for immediate effect.

```
SECURE CONSOLE
```

This is usually automatically set if SECURE.NCF is enabled. Also see rule Enable SECURE.NCF should be enabled.

Warning:

Using SECURE CONSOLE makes it impossible to load drivers from places other than SYS:\SYSTEM and C:\NWSERVER.

If this is necessary, and this command is in the AUTOEXEC.NCF, restarting the server will not allow this because it will immediately go back into effect.

To disable this setting, the SECURE CONSOLE line in the AUTOEXEC.NCF would need to be removed or commented out (putting a # symbol at the beginning of the line) and the server restarted.

References:

Novell, Inc. "Securing the Server Console." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hpmfqfmr.html>

6 Privileges

Description: When testing trustee rights or privileges, using the "effective rights" option in ConsoleOne and iManager and selecting an average user account is a good way to view what rights the user has to the tested object.

6.1 Disable Guest accounts

Description:

Native File Access includes support for Guest authentication. Typically these guest accounts can be authenticated to without a password. These accounts are most commonly used with older (pre-Mac OS X) Macintosh clients.

Guest accounts (or any accounts without passwords) should typically be disabled unless there is a public, read-only file space.

Remediation:

Look in the SYS:\ETC\CTXS.CFG file for any configured search contexts for user objects in eDirectory.

In those eDirectory contexts, look for any user accounts with the name of "Guest" and remove them.

Warning: This will disable all Guest logins to the system. If your organization has a legitimate need for Guest access, make certain the access rights of the Guest account are restricted to files that you want to be publicly available. Also, Guest access should be read and filescan only, not write, modify, or any other privileges.

References:

Novell, Inc. "Administrator Tasks for Native File Access for Macintosh Services." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/native/data/ac1pdri.html#ac23dyz>

6.2 No write or supervisory access to root of SYS volume

Description:

No explicit write or supervisory trustee rights should be given to the SYS volume object or to the root directory of the volume. Server administrators will already have rights that are inherited through the server or organizational unit (OU) container.

Volume administrators should not typically be given access to SYS, because user data should only be stored on other volumes.

Remediation:

Ensure that only system administrators have rights to the SYS volume object.

In ConsoleOne:

1. Right-click on the SYS volume object and select properties, then the trustees tab.
2. By default, there should be no trustees assigned to this volume object. There may be additional volume or server administrator groups or organizational roles if these have been assigned.
3. To test to make sure regular users do not have elevated rights, you can click on the Effective Rights button.
4. Browse to and select a standard (non-admin) user and view what rights that user has to the file folder.
5. The rights should not exceed read and file scan.

6.3 No user rights to SYS:\SYSTEM folder

Description: Only server administrators should have rights to the SYS:\SYSTEM folder.

Remediation:

Ensure that only system administrators have rights to the SYS:\SYSTEM folder.

In ConsoleOne:

1. Right-click on the SYS:\SYSTEM folder and select properties, then the trustees tab.
2. By default, there should be no trustees assigned to this folder. There may be additional volume or server administrator groups or organizational roles if these have been assigned.
3. To test to make sure regular users do not have elevated rights, you can click on the Effective Rights button.
4. Browse to and select a standard (non-admin) user and view what rights that user has to the file folder.
5. The rights should not exceed read and file scan.

6.4 No user rights to DOSFAT_C volume

Description: Only server administrators should have rights to the DOSFAT_C volume. The DOSFAT_C volume is the boot volume and can only be seen if DOSFAT.NSS is loaded in memory.

Remediation:

Ensure that only system administrators have rights to the DOSFAT_C volume. You can do this by checking the trustee rights on the servername_DOSFAT_C object in ConsoleOne or iManager. You must have DOSFAT.NSS loaded to mount the DOSFAT_C volume.

If the servername_DOSFAT_C object does not exist in the same container as the server object and servername_SYS volume objects, you can check its trustee rights by doing one of the following:

- If you have a Windows XP client authenticated through the Novell Client, you can check the rights by doing:
    1. Browse to My Network Places > Novell Connections > eDirectory Tree > Containers-leading-to-server-container > Server > DOSFAT_C.
    2. Right-click on dosfat_c and select Trustee Rights.
    3. There should be no trustees in the Trustees list.
    4. If there are trustees listed here, they should be removed. Any users with supervisor rights to the server object will normally get rights to the DOSFAT_C volume.
- Otherwise, you can administer the trustee rights in ConsoleOne, assuming the DOSFAT_C volume object is in eDirectory. Note that trustee rights can be assigned independently of whether DOSFAT_C has a volume object in eDirectory, so you'll want to follow these steps to check.
    - If the DOSFAT_C isn't in eDirectory, perform the follwing:
        1. After loading DOSFAT.NSS on the server, go to iManager. (https://serverip:8009/nds)
        2. Click the Repair button from the toolbar across the top.
        3. Click Advanced.
        4. Uncheck all boxes except Repair Volume Objects.
        5. Click Start Repair.
    - If the object was in the eDirectory tree, or if you added it with the above procedures, follow these steps to look for and remove any trustee rights.
        1. Go to ConsoleOne. You should now see the servername_DOSFAT_C volume.
        2. Rlight-click on the DOSFAT_C volume and select Properties.
        3. Click the trustees tab and make sure no trustees are listed.
        4. If there are trustees listed here, they should be removed. Any server administrators will normally get rights to this volume.

If you loaded DOSFAT.NSS as part of this fix, make sure you unload it by using the following console command:

```
UNLOAD DOSFAT.NSS
```

Warning:

When you are finished testing the rights, if you loaded the DOSFAT.NSS module, unload it.

There are performance, security, and potentially stability issues to leaving DOSFAT.NSS loaded. Also see DOSFAT.NSS should be left unloaded.

6.5 DOSFAT.NSS should be disabled by default

Description: Running DOSFAT.NSS leaves the NetWare operating system boot partition available to remote access and creates a risk that files on the boot partition could be remotely tampered with.

Remediation:

1. Search the C:\NWSERVER\STARTUP.NCF and SYS:\SYSTEM\AUTOEXEC.NCF and ensure that DOSFAT.NSS is not being loaded from these files.
2. If a line is found that loads DOSFAT.NSS, delete it or comment it out.
3. At the console, type:

```
MODULES DOSFAT.NSS
```

4. If DOSFAT.NSS is loaded, unload it by typing:

```
UNLOAD DOSFAT.NSS
```

Warning:

Unloading DOSFAT.NSS will disable any DOS FAT-based volumes from being accessible on the server. It is not a Novell best practice to serve files from a DOS FAT partition.

6.6 No user rights to SYS:\ETC folder

Description: Only server administrators should have rights to the SYS:\ETC folder.

Remediation:

Ensure that only system administrators have rights to the SYS:\ETC folder.

In ConsoleOne:

1. Right-click on the SYS:\ETC folder and select properties, then the trustees tab.
2. By default, there should be no trustees assigned to this folder. There may be additional volume or server administrator groups or organizational roles if these have been assigned.
3. To test to make sure regular users do not have elevated rights, you can click on the Effective Rights button.
4. Browse to and select a standard (non-admin) user and view what rights that user has to the file folder.
5. The rights should not exceed read and file scan.

6.7 No excessive rights to SYS:\LOGIN folder

Description:

Users should not have elevated access rights for the SYS:\LOGIN folder. The access rights for the SYS:\LOGIN folder should either be assigned read and file scan (default rights), or none at all if your users do not need access to the folder to access client installation files and public NetWare management resources.

This folder is reserved as a place that non-authenticated users can read, not write, to server files.

Remediation:

Ensure that only system administrators have rights to the SYS:\LOGIN folder.

In ConsoleOne:

1. Right-click on the SYS:\LOGIN and select properties, then the trustees tab.

2. There should be only one trustee, which is typically the Public object. There may be additional sub-administrator groups or organizational roles if these have been assigned.
3. To test to make sure regular users do not have elevated rights, you can click on the Effective Rights button.
4. Browse to and select a standard (non-admin) user and view what rights that user has to the file folder.
5. The rights should not exceed read and file scan.

6.8 No excessive rights to SYS:\PUBLIC folder

Description:

Users should not have elevated access rights for the SYS:\PUBLIC folder. The access rights for the SYS:\PUBLIC folder should either be assigned read and file scan (default rights), or none at all if your users do not need access to the folder to access client installation files and public NetWare management resources.

Remediation:

In ConsoleOne:

1. Right-click on the SYS:\PUBLIC and select properties, then the trustees tab.
2. There should be only one trustee, which is typically the top organization in the tree that the server is in. There may be additional sub-administrator groups or organizational roles if these have been assigned.
3. To test to make sure regular users do not have elevated rights, you can click on the Effective Rights button.
4. Browse to and select a standard (non-admin) user and view what rights that user has to the file folder.
5. The rights should not exceed read and file scan. If they do, re-examine the rights at the folder level, at each of the parent folder levels, at the volume, at the server, and then at each organizational unit container until you reach the root looking for excessive privileges.

6.9 No user rights to system folders on SYS volume

Description:

Regular user objects should not normally have any trustee rights assigned to most default folders on the SYS volume, although there may be a few sub-folders under them that have trustee rights assigned. These folders are:

```
SYS:\adminsrv
SYS:\Apache2
SYS:\arkManager
SYS:\bin
SYS:\DELETED.SAV
SYS:\ETC
SYS:\exteNd
SYS:\iFolder
```

```
SYS:\JAVA
SYS:\libdata
SYS:\LICENSES
SYS:\MYSQL
SYS:\ndps
SYS:\NETBASIC
SYS:\NetStorage
SYS:\NI
SYS:\NSN
SYS:\perl
SYS:\php5
SYS:\PVSW
SYS:\qfsearch
SYS:\QUEUES
SYS:\README
SYS:\res
SYS:\RESEARCH
SYS:\SYSTEM
SYS:\tmp
SYS:\tomcat
SYS:\UCS
SYS:\usr
SYS:\var
SYS:\xtier
```

Remediation:

In ConsoleOne or iManager:

1. Examine the trustees of each folder object.
2. Ensure that user objects, groups, dynamic groups, organizational roles, or containers are not listed as trustees unless it is related to a network or volume administrator. Main administrators do not need this trustee assignment, because they typically have rights over the server object which normally grants rights to all volume objects.

6.10 Enable Check Equivalent to Me

Description: This setting ensures that a security equivalence was properly made before allowing authentication. This is important because without this, stealth security equivalents can be made that don't show on security reports.

Remediation:

The following console command should be put into SYS:\SYSTEM\AUTOEXEC.NCF. After editing the AUTOEXEC.NCF file, the command should be typed into the console for immediate effect.

```
SET Check Equivalent to Me = ON
```

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

6.11 Disable Change to Client Rights for Job Servers

Description:

Job servers are dedicated systems designed to handle a task and then return the completed task, such as a print server. This setting disables the ability of the job servers to assume the full rights of a client, which could be used by an attacker to create backdoor accounts with the privileges of others.

Remediation:

The following console command should be put into C:\NWSERVER\STARTUP.NCF. After editing the STARTUP.NCF file, the server has to be restarted to immediately enable the configuration change.

```
SET Allow Change to Client Rights = OFF
```

Warning: This can disable older print servers that log into the server (not modern IP printers), some backup software, or other non-Novell client applications or software which perform tasks on the server.

References:

Novell, Inc. "Setting Packet Signature for Job Servers." Server Operating System for NetWare Administration Guide for OES. 2005-01-14. Novell, Inc. <http://www.novell.com/documentation/oes/sos__enu/data/hc66y4qi.html#hxkr04cq>

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

7 Protocols

7.1 Disable SNMP (v1/2) as it is not a secure protocol

Description:

SNMP is a network management protocol. It allows someone to read information about the system, and, if enabled, make changes to a system.

SNMP, versions 1 and 2, is unencrypted on the network and so is an insecure protocol.

SNMP should be disabled if not used. Write SNMP access should always be disabled unless SNMPv3 is used. Unfortunately, SNMPv3 is not currently supported in NetWare 6.5.

Remediation:

Disable the SNMP protocol.

1. Go to Remote Manager.
2. Navigate to Manage Server > Configure TCPIP > Start TCP/IP Configuration.
3. Navigate to Manage Configuration > Configure SNMP Parameters.
4. For Monitor State and Control State, select No Community May Read.
5. For Trap State, select Do Not Send Traps.
6. Click Save.
7. Click Back.
8. Click Reinitialize Options > Reinitialize System to make the changes active.
9. Exit the TCP/IP Configuration winow.

Although the recommendation of this rule is to disable SNMP rather than risk its vulnerabilities, if the risks of disabling SNMP outweigh the risks of running it, the most secure way to do so is to put all SNMP into a VLAN isolated from users and then create network access controls in the routers that route between the isolated VLAN and other networks that block ingress or egress of all SNMP traffic to the secured VLAN, and to filter SNMP traffic on the server interfaces not on the secure VLAN.

Also see the rule Change SNMP community strings from default of 'public'.

Warning:

Disabling SNMP will cause network management consoles that might be using SNMP to announce that the server has gone down or is unavailable.

7.2 Change SNMP community strings from default of 'public'

Description:

If SNMP must be used, the default settings in Netware 6.x allow anyone to read SNMP management information from the server, although writes are blocked by default. This is still a security risk in that sensitive infrastructure information might be divulged. SNMPv2 is unencrypted on the network and so is an insecure protocol.

SNMP should be disabled if not used, or at a minimum the community string should be changed. Please note that it will be easy to read this changed community string from the network and compromise SNMP security. Write SNMP access should always be disabled unless SNMPv3 is used. Although the SNMPv3 protocol supports authentication and encryption, is not available as part of NetWare 6.5, although it is available on OES-Linux.

Remediation:

Change the read community string. Disable SNMP write capabilities.

1. Go to Novell Remote Manager.
2. Navigate to Manage Server > Configure TCPIP > Start TCP/IP Configuration > Manage Configuration > Configure SNMP Parameters.
3. Set Monitor State to Specified Community May Read
4. Enter the Monitor Community to a SNMP read password. This password should not be the same as any other administrative passwords, because SNMPv1/2 passwords are unencrypted across the network.
5. For Control State, select No Community May Read.
6. For Trap State, select Do Not Send Traps.
7. Click Save.
8. Click Back.
9. Click Reinitialize Options > Reinitialize System to make the changes active.
10. Exit the TCP/IP Configuration winow.

Although the recommendation of this security benchmark is to disable SNMP rather than risk its vulnerabilities, if the risks of disabling SNMP outweigh the risks of running it, the most secure way to do so is to put all SNMP traffic into a VLAN isolated from users and then create network access controls in the routers that route between the isolated VLAN and other networks that block ingress or egress of all SNMP traffic to the secured VLAN, and to filter SNMP traffic on the server interfaces not on the secure VLAN.

Also see the rule Disable SNMP (v1/2) as it is not a secure protocol.

Warning:

Changing SNMP community strings will require reconfiguring any management consoles that might use SNMP, or they will report that the server either has gone down or is unavailable.

7.3 Disable SSHv1

Description: By default NetWare 6.5 includes SSHv1. This protocol has been shown to be vulnerable to a number of security flaws and should be disabled in favor of SSHv2.

Remediation:

1. Edit the sys:\etc\ssh\sshd_config file.
2. Replace the line- "Protocol 2,1" with the line- "Protocol 2"
3. Save the file.
4. Type in the console command:

   ```
   sshd reload
   ```

   This will reload the configuration file, disabling SSHv1.

   You can also change this setting from NetWare Web Administration.

Warning: Obsolete versions of the SSH client, which do not support SSHv2 will not function. However, due to the security problems, these clients should be updated.

References:

CERT. "Incident Note IN-2001-12." CERT. CERT. <http://www.cert.org/incident_notes/IN-2001-12.html>

Novell, Inc. "Setting Up SSH on a Server." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/openssh/data/ajpc1oy.html>

7.4 Enable secure TCP/IP protocol configuration

Description: Ensure that the TCP/IP settings are configured in a way that improves resistence to attack. These settings improve the ability of the server to defend itself against network attacks and attempt to mitigate denial-of-service attacks. View the references for more information about each.

Remediation:

Add the following lines into the AUTOEXEC.NCF file: (these settings can also be set in NetWare Remote Manager)

```
SET Discard Oversized Ping Packets = On
SET Largest Ping Packet Size = 10240
SET Discard Oversized UDP Packets = On
SET Largest UDP Packet Size = 33792
SET TCP Diagnostic Services = Off
SET TCP Defend Land Attacks = On
SET Maximum Wait States = 1000
SET Maximum Pending TCP Connection Requests = 2000
SET Allow IP Address Duplicates = Off
SET TCP UDP Diagnostic Services = Off
SET SLP Close Idle TCP Connections Time = 30
```

Warning: Setting TCP Defend Land Attacks = On could cause a performance drop in heavily utilized servers.

References:

Novell, Inc. "Protection Against SYN and FIN Attacks." Novell AppNote. Novell, Inc. <http://developer.novell.com/research/appnotes/2002/april/01/a0204018.htm>

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

7.5 Enable NCP error checking

Description: The following steps will turn on various error checking abilities by the server to detect malformed or damaged packets.

Remediation:

The following console commands should be put into SYS:\SYSTEM\AUTOEXEC.NCF. After editing the AUTOEXEC.NCF file, the command should be typed into the console for immediate effect.

```
Set display NCP bad component warnings = ON
SET Reject NCP Packets with bad components = ON
SET Display NCP Bad Length Warnings = ON
SET Reject NCP Packets with bad lengths = ON
SET Enable UDP Checksums on NCP packets = 2
```

References:

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

7.6 NCP Packet Signature

Description:

For clients accessing a NetWare server utilizing the Novell client, the NCP Packet Signature prevents packet forgery by requiring the server and the client to sign each NCP packet. The packet signature changes with every packet.

Without NCP Packet Signature installed, a user could pose as a more privileged user and send a forged NCP request to a NetWare server. By forging the proper NCP request packet, an intruder could gain the Supervisor right to the Server object and access to all network resources.

NCP packets with incorrect signatures are discarded without breaking the client's connection with the server. However, an alert message about the invalid packet is sent to the error log, the affected client, and the server console. The alert message contains the login name and the station address of the affected client.

The packet signature levels are as follows:

```
0 - Do not do packet signature.
1 - Do packet signature only if requested by the other end.
```

```
2 - If the other end will allow packet signature, do it.
3 - Require packet signature or don't communicate.
```

To ensure that packet signatures are always used, the packet signature level should always be set to three (3) on both the NetWare server and the Novell Client on the workstation.

The default settings for both the client and server are level one (1), which will not use packet signing.

Also see "Novell Client NCP packet signature configuration".

Remediation:

The following console command should be put into C:\NWSERVER\STARTUP.NCF. The server will have to be restarted for the setting to take effect.

```
SET NCP Packet Signature Option = 3
```

Warning:

Enabling level 3 packet signature on the server or client without enabling it on the other could cause a situation where clients cannot communicate with the server, such as if the client is set to packet signature level 0, the clients are linux systems using ncpfs compiled without support for packet signing, or if the clients are very old.

Although not recommended, if you do not have complete control over all Novell clients but need to allow everyone to login, you may want to set the server to level two (2). This will require packet signatures if the client can support it (clients that are set to levels 1 to 3), but still allow non-signing clients to connect (level 0). However, this is a security risk as man-in-the-middle attacks could render any connection insecure and then compromise the session.

Enabling packet signatures on all NCP packets can create a heavier CPU load on older or very busy servers. If the server's primary use is a file server, then it likely is not utilizing most of its processor capabilities. However, if the server is already under a heavy processor load, this option may not be advisable unless the application that is causing the heavy load is moved to another server, or the server is upgraded to improve processing capabilities.

References:

Novell, Inc. "Using NCP Packet Signature." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hc66y4qi.html>

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

7.7 Enable the server host firewall

Description:

NetWare 6.5 includes a built-in firewall that will allow you to block external access to certain services running on the NetWare server. This firewall is pretty basic, but does do packet filtering

and stateful packet inspection. For a fully-featured commercial-grade firewall, you can purchase the BorderManager product from Novell for NetWare.

A default installation of NetWare 6.5 will all options enabled returned the following open ports (scanning ports 1-12,000)-

TCP Ports- 21 (ftp), 80 (http including user web services and iManager), 81 (NetWare Remote Manager - NRM), 83, 111 (rpcbind), 139 (netbios-ssn), 289, 389 (ldap), 427 (svrloc), 443 (https), 524 (ncp), 548 (afptcp), 631 (ipp), 636 (ldapssl), 731, 846, 847, 1061, 1063, 1234, 2049 (nfs), 2200 (iManager secure), 2211 (iManager unsecure), 2967, 3260, 3306 (mysql), 3351, 6000 (X11), 6901, 8008 (NRM), 8009 (NRM), 9009, 9010

UDP Ports- 111 (rpcbind), 123 (ntp), 137 (netbios-ns), 138 (netbios-datagram), 161 (snmp), 427 (svrloc), 524 (ncp), 902, 903, 904, 961, 1025, 1234, 2049 (nfs)

Best security practices dictates not installing services you don't need. If you do have services running that you don't need, they should be disabled or removed.

Remediation:

Enable the packet filter and block remote access to all services that should not be accessed across the network.

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 in the eDirectory benchmark.

To enable the packet filter host firewall. At the NetWare console:

1. Type INETCFG to get to the network configuration menu.
2. If it asks to transfer LAN driver, protocol, or remote access commands, say yes and restart the server. (Of course, only after making certain that no one is using the server.)
3. Do not use the fast configuration if asked.
4. Select the Protocols option.
5. Select the TCP/IP protocol. (The others are typically disabled or unconfigured.)
6. Go to the bottom of the menu where it has the Filter Support option.
7. Enable filter support.
8. Exit the menus and INETCFG, saving any changes.
9. Exit from the menu and from INETCFG, saving any changes.
10. Type in the following command to make the changes active- REINITIALIZE SYSTEM
11. Type FILTCFG at the console to go to the filter configuration menu.
12. Select Configure TCP/IP Filters.
13. Select Packet Forwarding Filters. (The name is a bit misleading as these filters work even if routing is disabled.)
14. Set the Status to Enabled.
15. Leave the action as "Deny Packets in Filter List". *Although it is more secure to set it to "Permit Packets in Filter List" and turn on only the ports you wish to allow, this is more likely to break an application if you are unfamiliar with the necessary ports on NetWare.*
16. Go to the Filters option and press Enter.

At this point, you can add filters to block certain services.

The following ports should always be blocked unless you know you have a special circumstance that requires it.

TCP 21 (insecure FTP), TCP 23 (insecure telnet), TCP 110 (insecure mail POP3), TCP/UDP 389 (insecure LDAP services), TCP 2034 (insecure RConsoleJ), TCP 3306 (remote MySQL access), TCP 6000 (remote X11 access)

To block a service, perform the following steps:

1. Press the Insert key to add a new filter.
2. Move to Packet Type and press Enter.
3. If the protocol/service you wish to block is in the list, you can select it. If not, follow the steps below.
4. Save the filter once done.
5. Repeat as necessary to allow all filters to be created.

While creating filters, you can create new TCP/IP packet types, by using the following steps:

1. At the Defined TCP/IP Packet Types screen, press Insert.
2. Type in a name of the protocol or service.
3. In the Protool field, press Insert and select TCP or UDP
4. Leave the Source Port <All>
5. Set the Destination Port to the number you wish to block (IE- 6000)
6. You can enable Stateful filtering if you are blocking a dynamic protocol, such as FTP.
7. Press Escape when done.
8. Press Enter to select your newly created packet type.

Once you are done making all your filters, you can exit out, saving any changes. The changes take effect immediately. Be sure to test all critical services from the server.

You can run a port scanner to see if your changes have taken effect. The free port scanner nmap in its default configuration shows the filtered ports as "filtered" instead of "open".

Warning: You must use care when disabling network services other than those listed that can always be blocked. Always be sure to do thorough testing after blocking any additional services with the firewall.

References:

Novell, Inc. "What are the default and common ports for NetWare 6?." Novell Knowledgebase. Novell, Inc. <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10071836.htm>

7.8 FTP should be disabled

Description:

FTP is an insecure protocol and should not typically be used. By default, NWFTP.NLM will accept user's account names and passwords across an unencrypted connection, rendering their other secure account access methods exposed.

NetWare 6.5 supports "secure FTP" or SFTP and is the preferred way to provide FTP services, if needed.

Although NetWare FTP does support TLS connections, most FTP clients do not support this and other standard, secure ways of file transfer are supported such as those listed above.

Remediation:

Disable FTP services on the server. Use NCP/IP (Novell Core Protocol over IP with the Novell Client) or SFTP (on NetWare 6.5) for secure file transfer to the NetWare server.

Type the following command at the system console:

```
UNLOAD NWFTPD
```

Also, remove any lines from the SYS:\SYSTEM\AUTOEXEC.NCF that start with the following:

```
NWFTPD
LOAD NWFTPD
```

Then perform the following steps:

1. Launch the Novell installer in the GUI.
2. Select Netware FTP Server from the list of installed products.
3. Click Remove.

If FTP services, and not SFTP services, are **required**, you can force the requirement of TLS or encrypted FTP authentication by making the following configuration changes. Be aware that any clients not configured to do so will transmit the username and password in the clear before being sent a message that encryption is required, and therefore disclose the account name and password before being told they cannot login.

1. Open and authenticate to iManager. (http://serverip/nps/iManager.html)
2. Navigate to File Protocols > FTP.
3. Select the Server.
4. Select the ftpserv.cfg file to configure.
5. Check the "Secure connections only" box.
6. Click Save.

Warning: Disabling FTP services will disallow all FTP client access to the server.

References:

Novell, Inc. "Configuring NetWare FTP Server." NetWare FTP Server Administration Guide for NetWare 6.5. 2005-02-08T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/ftp_enu/data/a2fbytp.html>

Novell, Inc. "Using the NetWare FTP Server from an FTP client." NetWare FTP Server Administration Guide for NetWare 6.5. 2005-02-08T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/ftp_enu/data/a3ep22p.html#al8n74e>

7.9 IPX, and other legacy network protocols, should be disabled if not used

Description:

Most of the security bypassing tools for NetWare are based on the older versions of NetWare and do not function with current technologies. Standardizing on the TCP/IP protocol will render those attacks impotent, and will fully utilize the current networking stack from Novell based on TCP/IP.

NCP over IP is secure with proper configuration, such as enabling mandatory packet signing.

Leaving unused protocols enabled also leaves other potential backdoors open to hackers familiar with the protocols and slows network performance by adding unnecessary traffic to the network.

Remediation:

To disable IPX (and any other protocols that aren't being actively used, such as AppleTalk), do this at the NetWare Console:

1. Type INETCFG to get to the network configuration menu.
2. If it asks to transfer LAN driver, protocol, or remote access commands, say yes and restart the server. (Of course, only after making certain that no one is using the server.)
3. Do not use the fast configuration if asked.
4. Go to the Protocols menu.
5. From this menu, you will be able to see the various protocols supported. Typically the only protocol that should be enabled is TCP/IP. If other protocols are enabled, select the protocol, and turn the protocol status (the top line) to Disabled. Exit and save the changes.
6. Perform this for each protocol you wish to disable. You can ignore protocols that say "Unconfigured" because they are not enabled.
7. Once done, exit out of INETCFG.
8. Type in the following console command to make the changes active:

```
REINITIALIZE SYSTEM
```

Warning: Some old workstations (especially DOS and Windows 3.x) as well as printers made before 1995 may use IPX to communicate with workstations. Old Apple systems (non-Mac OS X) may use AppleTalk to communicate. Both of these scenarios are very unlikely unless the NetWare 6.5 server replaced a NetWare 4.x or older server and all of the clients have not been updated or replaced since that time.

7.10 No external access to NCP protocol

Description:

No direct access should be allowed to NCP services outside of the organization or network domain.

In combination with unsecured eDirectory privileges, this port could be used to determine user accounts, services, and other information from the server.

Remediation: TCP port 524 on NetWare servers should be unavailable from public or unauthorized networks and should be blocked using network firewalls or router filters.

7.11 No external access to NetWare Remote Manager

Description:

If the server is available to public or unauthorized networks, access to the NetWare Remote Manager should be blocked at the perimeter through firewall or router access control lists.

Remediation: Block TCP port 81, 8008, and 8009 to the server at the perimeter through the use of router or firewall access control lists.

7.12 Require SSL for iManager

Description: iManager is a web-based management interface that replaces the older Java-based ConsoleOne and Win32-based NWAdmin tools. By default, iManager is enabled to be run over an SSL web connection.

Remediation:

Edit the following file:

```
SYS:TOMCAT\WEBAPPS\NPS\WEB-INF\PORTALSERVLET.PROPERTIES
```

Ensure that the System.DirectorySSL setting is equal to true.

```
System.DirectorySSL=true
```

7.13 Routing should be disabled unless the server has a need to route network traffic

Description: NetWare 6.x has full network routing capabilities. These should be disabled (and are off by default) unless they are needed for routing purposes.

Remediation:

To disable routing perform the following steps at the NetWare console:

1. Type INETCFG to get to the network configuration menu.
2. If it asks to transfer LAN driver, protocol, or remote access commands, say yes and restart the server. (Of course, only after making certain that no one is using the server.)
3. Do not use the fast configuration if asked.
4. Select the Protocols option.
5. Select the TCP/IP protocol. (The others are typically disabled or unconfigured.)
6. The following options should be disabled (if they are not, disable them)- IP Packet Forwarding, RIP, OSPF
7. Exit from the menu and from INETCFG, saving any changes.
8. Type in the following command to make the changes active:

```
REINITIALIZE SYSTEM
```

Warning: If the server is acting as a router on the network, it will need to have routing enabled. Examples of this are if there are multiple separate networks that are only connected through the server.

7.14 Disable UDDI services or use SSL with UDDI

Description:

UDDI services should be disabled, or if required, implement UDDI over SSL to ensure the security of the service.

Remediation: Please refer to the reference to enable SSL on UDDI.

References:

Novell, Inc. "Adding an SSL Provider." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/uddi/data/am6in4q.html>

8 Storage

8.1 All disk volumes should be NSS volumes

Description:

Although NetWare supports the legacy "traditional" volumes, all disk storage volumes should be NSS. NSS (Novell Storage Services) volumes are journaled. This means that if the disk were to suddenly become unavailable due to a power outage, storage volume disconnection, or other event, the data on the drive would be protected by replaying any pending transactions that were incomplete at the time of the loss of the connection. NSS volumes also resist corruption better than traditional volumes.

Although there were some problems intially with NSS volumes in certain circumstances under NetWare 5.x, these issues have been resolved in NetWare 6.x and with current service packs.

Remediation: All traditional volumes should be upgraded to NSS volumes.

Warning:

Ensure that you are running current service packs if deciding to use optional features related to NSS such as compression.

Novell does not recommend using compression on the SYS drive, or on drives that will be storing large, often modified files, such as databases.

References:

Novell, Inc. "Overview of NSS." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/nss_enu/data/hut0i3h5.html#hut0i3h5>

Novell, Inc. "Copying Data from Existing Traditional or NSS Volumes to NetWare 6.5 NSS Volumes." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/nss_enu/data/acijc1e.html#acijc1e>

8.2 iFolder data encryption should be enabled

Description: If iFolder is enabled on the server, ensure that a global client policy requires that all iFolders are created as encrypted. Otherwise, the data is transferred across the network without encryption due to the fact that iFolder network streams are unencrypted.

Remediation:

Enable mandatory encryption in the global client policy.

1. In iManager, navigate to iFolder Management > Launch iFolder Managmement
2. Authenticate to the iFolder Management console.

3. Navigate to Global Policies > Client Policies > Display > Client Policy Settings.
4. Ensure that On and Enforced is checked for Encryption.
5. Click Update for Client Policy.

Warning:

Enabling encryption only affects new and not existing iFolder accounts.

If encryption is enabled, and recover passphrase is not enabled, if the user loses their iFolder client passphrase, that user's files stored in iFolder will be irretrievably lost.

Enabling recover passphrase implies a trust relationship between the user and the administrator of the iFolder server, as the user's files would be accessible to the administrator.

References:

Novell, Inc. "Authentication and Encryption." Novell iFolder 2.1 Installation and Administration Guide. 2006-01-23T00:00:00. Novell, Inc.

Novell, Inc. "Configuring Global Client Policies." Novell iFolder 2.1 Installation and Administration Guide. 2006-01-23T00:00:00. Novell, Inc.

8.3 All print queues and iPrint/NDPS print spooling locations should be on a volume other than SYS

Description:

When using legacy print queues or iPrint/NDPS printers, they should not store their files on SYS. If SYS were to fill up due to print job activity, it would cause the server to cease to function. This could be exploited to perform a denial-of-service attack on the server.

By default, iPrint/NDPS print spooling is set to the same volume as the print manager database volume.

Remediation:

Move all print queue and iPrint/NDPS print spooling to volumes other than SYS.

1. In iManager, navigate to iPrint > Manage Printer.
2. Select a printer object.
3. Navigate to Configuration > Spooling.
4. Change the spooling location to a volume other than SYS.
5. If desired, you can limit the space allocated to spooling for the printer here.
6. Click Apply.
7. Repeat this process for all printers.

Moving legacy print queues is beyond the scope of this document. See the references for more information.

Warning: Be sure to use eDirectory management tools to move the directories. Just moving the directory to another volume using the file system will cause the print queues and iPrint/NDPS print spooling to cease to function.

References:

Novell, Inc. "iPrint Administration Guide for NetWare 6.5: Managing Printers." NetWare 6.5 Documentation. 2005-02-28T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/iprint/data/hx0rwd73.html#hizf9udg>

Novell, Inc. "Moving Novell's Legacy Print Services Between Volumes and Servers." Novell AppNote. 2001-09-01T00:00:00. Novell, Inc. <http://support.novell.com/techcenter/articles/ana20010902.html>

8.4 Data Protection

Description:

Data on all servers should be backed up to another location.

Remediation:

Be sure to have complete copies of all critical data stored in an off-site location to allow recovery in case of a disaster.

References:

Novell, Inc. "Software: Backup, Restore & Recovery." Novell Website. Novell, Inc. <http://www.novell.com/partnerguide/s100003.html>

8.5 Purge files immediately after deletion to ensure they are removed from the file system

Description: By default, if the purge immediately attribute is not enabled for the volume the operating system keeps an amount of deleted files available for recovery (salvage) until a specific storage condition has been reached. On traditional volumes, files are not purged until all of the free space on the volume has been used. In an NSS storage pool, the there are settings for a low and high "watermark" for purging files. By default, this setting in OES is 10%. This means that until the volume is 90% filled, deleted files do not even begin to be purged automatically, and are still available for recovery, whether the volumes are encrypted or not.

Remediation:

Unfortunately, Novell does not include the functionality in the operating system to automatically purge files that are older than a specified date.

What can be done is to adjust the high and low "watermarks". When the low watermark threshold is crossed, by default 10% of disk space being free, the purging will occur until the disk space equals the high watermark, which is by default 20% free disk space.

Depending on how full your volume is, and how often files are created and deleted, that might be months or even years. See the references for more information.

Although it is possible to use a cron job with an unsupported utility, TOOLBOX.NLM, to regularly purge files that are older than a particular number of days, this is unsupported by Novell.

Instead, you can enable immediate purge on the volume object, and all files which are deleted are purged immediately.

Be aware that it is still possible to recover the file until the disk space the file occupied is overwritten (called data shredding), or if the volume is encrypted. If you are interested in these options, check the references for more information.

To enable purge immediately on deleted files, put the following command into the C:\NWSERVER\STARTUP.NCF file. It will become active at the next server restart.

```
SET IMMEDIATE PURGE OF DELETED FILES=ON
```

Warning: By purging the files immediately, any deleted files will be very difficult to recover without a separate backup archive.

References:

Novell, Inc. "Salvaging and Purging Deleted Volumes, Directories, and Files." Novell Storage Services File System Administration Guide for OES. 2005-09-29. Novell, Inc. <http://www.novell.com/documentation/oes/nss_enu/data/bv6o5ay.html>

Novell, Inc. "TOOLBOX.NLM 2.17 for NetWare 4 - 6." Novell Cool Solutions. Novell, Inc. <http://www.novell.com/coolsolutions/tools/1490.html>

Novell, Inc. "Setting Server Parameter Values." NetWare 6.5 Documentation. 2003-12-19T00:00:00. Novell, Inc. <http://www.novell.com/documentation/nw65/sos__enu/data/hbv2js9h.html>

8.6 Enforce folder space restrictions

Description:

If you desire, you can set a maximum size restriction on folders. At the very least, this should be enforced for any user home directory folders, as well as any storage databases on the SYS volume so they cannot entirely fill the SYS volume.

It is preferrable to move all application storage to other volumes than SYS. Also see rule SYS volume reserved for NetWare system files.

Remediation:

In ConsoleOne:

1. Right-click on the folder to restrict and select Properties.
2. Click the Facts tab.

3. Check the Restrict size box.
4. Enter the desired maximum size of the folder.
5. Click OK.

From this point forward, if the contents of the folder (and sub-folders) exceed this restriction, any additional data being saved to the folder will return an "out of space" error.

Warning: This has to be done for each folder to apply the change to. For new folders, this will have to be done again.

8.7 Enforce user space quotas

Description: If you desire, you can restrict how much storage a user can utilize on a volume.

Remediation: See the references for information relating to implementation of user space quotas.

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.

References:

Novell, Inc. "Conserving Disk Space with Volume, Directory, or User Space Quotas." Novell Storage Services File System Administration Guide for OES. Novell, Inc. <http://www.novell.com/documentation/oes/nss_enu/data/bv3rpf1.html>

8.8 SYS volume reserved for NetWare system files

Description: Applications, user home directories, and other user data should not be stored on the SYS volume. The SYS volume should be reserved for NetWare system files only. Additional access rights to the SYS volume should not be granted to users. The SYS volume is where the operating system runs from and also the server will likely cease functioning if the SYS volume becomes full.

Remediation:

Place all applications, data, and user's home directories on other volumes than the SYS volume. Use Console One or iManager to remove any additional access privileges that users have been given to the SYS volume.

Although it is beyond the scope of this document, it is possible to move a series of folders and sub-folders while preserving their trustee rights by using the Server Consolidation Utility and NetWare Migration Wizard.

Warning: Moving some kinds of directories and files can break settings. For instance, if you move the user's home directories, be sure to reset the user's home directories in eDirectory to their new location and check the login scripts, so that mappings will continue to work and login scripts will continue to function.

References:

Novell, Inc. "Home or Username Directories." NetWare 6 Documentation. Novell, Inc. <http://www.novell.com/documentation/nw65/trad_enu/data/am8l8pi.html>

Novell, Inc. "Server Consolidation Utility and NetWare Migration Wizard." Novell Open Enterprise Server. Novell, Inc. <http://www.novell.com/products/openenterpriseserver/consolidationmigration.html>

8.9 The SYS:\MAIL folder should be removed

Description:

The SYS:\MAIL folder supports legacy MHS mail systems that are no longer supported or utilized. All users by default have create rights in this folder on the SYS volume.

Remediation: Remove the SYS:\MAIL folder along with all sub-folders, if any.

Warning: Old mail systems (pre-1990s) may use this directory. Some examples include any program that uses the MHS mail system, Pegasus Mail, or cc:Mail from Lotus. It is also possible that GroupWise has been misconfigured to store its messages in SYS:MAIL, so ensure you have a backup before removing, if mail services are running on the server.

9 Novell Client for Windows

Description:

This section covers not the NetWare server, but the Novell client often used to access an NCP server, such as OES NetWare, from a Windows workstation. When using the Novell client on Windows, it is important to also follow the security benchmark for the Windows platform in addition to this benchmark.

There are many ways to propigate Novell Client for Windows settings. The steps shown here are a simple, single client method. However, there are ways to ensure that all clients on the network are up to date and have the desired settings. Consult the referrences for more information.

9.1 Ensure the Novell Client is kept updated

Description:

If you are using the Novell client software on the workstations connecting to the NetWare server, ensure that the client software is kept current. One good method of accomplishing this is to use an automated installation through Automatic Client Upgrade or the Novell Client Update Agent.

Another option that is not covered here is to use a patch management system, such as Novell's ZENworks Patch Management.

Remediation:

Deploy the automatic client update (ACU) utility or comparable method of keeping the Novell client software current.

References:

Novell, Inc. "Novell Client for Windows." Novell Client Documentation. Novell, Inc. <http://www.novell.com/documentation/noclienu/>

Novell, Inc. "Understanding Automatic Client Update." Novell Client Documentation. Novell, Inc. <http://www.novell.com/documentation/noclienu/noclienu/data/bttizan.html#bu05uwy>

9.2 Novell Client should not display the last user that authenticated

Description:

By default, the Novell client will display the most recent user authenticated. This allows anyone at a physical workstation to find out which account was last used at that location. Not only does it make it easier to try to guess an account and password, but the information can be used to circumvent security measures on the physical system.

Remediation:

Remove the username from the client settings and keep it from saving it each time someone authenticates.

1. Go to Novell Client properties.
2. Go to the Location Profiles tab.
3. Click the default location profile and click properties.
4. Select the Login Service and Default Service Instance and click properties.
5. Delete all text in the field username.
6. Uncheck the box "save profile after successful login".
7. Click OK three times.

Warning:

Some users may not be used to typing in their account name and may have to be trained how to authenticate when their username is not already filled in for them.

9.3 Novell Client NCP packet signature configuration

Description:

The Novell Client has the ability to require packet signing in its communications with NCP servers.

Also see rule "NCP Packet Signature".

Remediation:

Although configuring the NCP packet signature level to two (2) would be more compatible, it also allows man-in-the-middle attacks to circumvent the protections afforded by packet signature.

To set the Windows client signature level for an individual workstation, change the parameter setting with the Advanced Settings tab of Novell Client Properties, as follows:

1. In the system tray, right-click N.
2. Click Novell Client Properties > Advanced Settings.
3. Set Signature Level to 3 from the scrollable list.
4. Click OK and restart the workstation to make the configuration change take effect.

You can also deploy the Novell client with this setting already configured. See the Novell Client documentation for details.

Warning: Setting the packet signature level to three (3) will require a signed connection to all servers. If there are any servers, including NCP-compatible NAS or similar appliances, which do not support packet signatures, no connection will be allowed.

9.4 Novell Client protocols

Description:

Many of the tools used to compromise a NetWare server utilize the legacy protocol IPX. Also, Novell no longer actively develops the IPX protocol, although it is still supported. Due to Novell's focus on IP as a modern protocol stack, it is likely that the IP protocol receives more attention and is therefore less prone to unresolved security issues than the IPX protocol services.

Also see rule IPX, and other legacy network protocols, should be disabled if not used.

Remediation:

Use IP to connect with Novell servers.

1. In the system tray, right-click N.
2. Click Novell Client Properties > Protocol Preferences.
3. Set Preferred Network Protocol to IP from the scrollable list.
4. Click OK and restart the workstation to make the configuration change take effect.

You can also deploy the Novell client with this setting already configured. See the Novell Client documentation for details.
