STATISTICS DENMARK

Statistisk sentralbyrå
Statistics Norway

Statistiska centralbyrån
Statistics Sweden

MZ:2005:20

Mission Report

from a short-term mission on Win03 and Migration

From the 28th of November until the 9th of December 2005

TA for the Scandinavian Support Program to Strengthen the Institutional Capacity of the National Statistics, Mozambique

Bo Guldager Clausen

Instituto Nacional de Estatística

Ref. no. 104.Moz.98

December 2005

Bo Guldager Clausen
Statistics Denmark
Sejrøgade 11
DK – 2100 Copenhagen O
Denmark
Tel.: +45 39 17 38 15
bgc@dst.dk

Table of Contents

1 Introduction 5

2 Activities during the mission 7

3 Conclusions and recommendations 8

3.1 Follow up on recommendations from January 2004 8

3.2 (New)Recommendations regarding Windows 2003 migration plan. 10

3.3 New recommendations regarding security 11

3.4 General recommendations. 12

Annex 1 Terms of reference for the mission 13

Annex 2 Persons met during the mission 15

Executive Summary

The mission follows the one in January 2004 about consolidation of network administration.

During the mission the plan for migrating the current Windows server environment from Windows NT 4.0 was further developed and tested. The migration did not take places because of missing licences from Microsoft.

Training in new features of Windows Server 2003 was provided throughout the mission. Hands on training in general security configuration was provided as well.

Security issues in general and particularly firewall configuration were subject to discussions.

The possibility for making restrictions on the use of the internet connection was tested and implemented. This was done as an experiment for freeing up internet bandwidth for INE relevant information.

1 Introduction

The mission was carried out 28 November – 8 December 2005.

The consultant would like to express his thanks to officials and individuals for their kind support and valuable information.

The migration from Windows NT to Windows Server 2003 has been in the pipeline for two years. Part of the network administration staff has been on Microsoft training in India. A migration plan and a test plan have been made and the physical servers have been bought. This means that INE is almost ready to do the migration. The last problem seems to be the financing of the Microsoft licenses. When this problem is solved the migration can take place.

The migration did not take place during the mission because of the missing licenses from Microsoft, but a series of tests were made on basis of copies of the existing environment and the evaluation version of Windows Server 2003.

INE has decided to do a migration from the old installation instead of doing an inbound upgrade. This is a rational plan because previous potential configuration mistakes will not be implemented in the new environment. A migration means to move one installation to another, and an inbound upgrade is an upgrade of the existing environment. If the migration contrary to expectation should fail then one can consider testing an inbound upgrade.

The documentation of the migration plan was carried out by Mr. Pedro Miambo and is written in Portuguese. The consultant is not able to check this documentation but the plan has been successfully tested in co-operation between Mr. Pedro Miambo and the consultant.

Discussion of security issues was carried out on this mission. The main goal for security is always to give the access that is needed and no more.

The firewall should only allow traffic that is needed. Source and destination addresses should as far as possible be based on hosts, and not on networks or “any”. The most important part is to block all traffic from the internet to the internal network.

The procedures for handling daily security management tasks should be well documented and known to all network administrators. Only use administrative rights when it is needed, and not for reading mails and browse the internet. Assign permissions to network objects such as files by use of group membership. Deployment of security updates from Microsoft should be carried out on a monthly basis by using Windows Server Update Service. Manage user accounts by using scripts to do the procedures involved for new users, users who moves inside INE and when users leave INE.

Disaster recovery plans for all servers must be written and tested. Part of these plans was made and tested during the mission. The backup tapes must be placed somewhere outside INE.

Physical security covers for example the access to the server room. The protection of this room has to be improved by a more secure door and key system.

INE has as limited bandwidth on the internet connection. This bandwidth ought not to be used for listening to internet radio or downloading music and videos. The limitations also gives problems concerning connecting the DPINEs in the provinces to INE in Maputo. Next year the national governmental network may solve some of these problems. INE in Maputo may get higher bandwidth and there is a possibility to get broad band to the province. Which of course does not eliminate the need to avoid heavy private use of the network.

The problem with financing software licenses will be a continuous problem in the future. For this reason considerations of using open source software may be a good plan. Many open source solutions are available on the internet and can be used for free. The network administration now has experience with Windows operating systems and this ought to be used for the immediate future, but the staff might start to test Linux operating systems and get experience with these solutions. Particularly for server solutions Linux can be an alternative to Windows. Open source software can also be implemented in Windows systems. As an example, the Open Office application can be an alternative to Microsoft Office. All users may not need an expensive Microsoft Office package, but can carry out the job by using Open Office.

The list of recommendations from the earlier mission in January 2004 was evaluated.

2 Activities during the mission

- Kick off meeting with Mr. Tomás Bernardo.
- Test migration from Windows NT 4.0 to Windows Server 2003 on constructed user accounts.
- Test of migration from Windows NT 4.0 to Windows Server 2003 on real user accounts and computers. The test was run on a copy of the existing Windows NT domain on basis of the documentation.
- Test of migration of printers and DHCP database from Windows NT 4.0 to Windows Server 2003.
- Restore of single and multiple user accounts from the Active Directory. The procedure was documented and tested.
- Restore of complete domain controller using the ASR method in Windows backup. The procedure was documented.
- A general server documentation template was developed. This template describes the server hardware, operating system and software configuration. This information is important in case of recovery.
- General discussion of security issues in the network environment.
- Introduction and hands on training in Windows Group Policy.
- Review of the firewall configuration. The network administration will get training in the currently used firewall by local consultants from Maputo.
- Upgrade of the Squid proxy server from version 2.3 to 2.5.
- The Squid Web Proxy was configured to reject internet radio. Configuration for blocking video and music based on file extensions was implemented. Blocking of specific site was also implemented and tested.
- A freeware (Open Source) tool was implemented to generate reports about the outgoing internet traffic through the Squid Web Proxy. The report is generated on Fridays at 12:00.
- Basic security check was done on the portal server. Check for security updates, firewall configuration and a simple port scanning from outside.
- During the mission the Exchange server had ad major break down. One day was used to solve the problem.

3 Conclusions and recommendations

3.1 Follow up on recommendations from January 2004

ID:	Description	Status and comments	
JAN-REC-01	Modernize old workstations	Almost all the workstations are now running Windows Xp or Windows 2000. The last 2 will be upgraded soon.	1
JAN-REC-02	Add more backup tapes	New tapes are still missing.	-1
JAN-REC-03	Only store INE relevant data at INE equipment	The content of the fileservers are unknown. When Windows Server 2003 R2 is implemented, it will be possible to control content by file extensions. The technique allows to ban music and video files etc., and the users will not be able to store this kind of files.	0
JAN-REC-04	Upgrade physical network	The physical network has been upgraded to switches. All hubs replaced with D-Link switches.	1
JAN-REC-05	Add knowledge about Microsoft Exchange	Mr. Pedro and Mr. Bruno have been on the official Microsoft courses in India.	1
JAN-REC-06	Centralize software installation	Not implemented. The user still have local administrator on their workstations. Only network administration staff should install software. It is also a security risk when the users have administrative rights on the workstations. Virus, worms and spyware have better conditions. When Windows Server 2003 is implemented, the use of group policy can install software on workstations.	-1
JAN-REC-07	Establish local network at Maputo Cidade as a pilot	Local network is implemented at Maputo Cidade with a wireless solution. The personal can access web mail at INE on the cable modem based internet connection.	1
JAN-REC-08	Analyze possible ISPs	The present ISP, TV Cabo, seems to be the most economic solution according to the INE staff. The other providers may have better solutions, but INE can not afford the prise of these solutions. Next year a governmental network infrastructure in part of Mozambique will be ready. INE can join the network at low cost. In a near future the first DPINE's can join the same network.	1, 0
JAN-REC-09	Add procedures for managing the user accounts.	Procedures for managing the user accounts when employees are hired, move from one part to another inside INI, or leave INE are not implemented. There should be procedures for these tasks. Human resources must provide the network administration	-1

		with this information. The technical procedures for managing user accounts should be automated by use of scripts or templates. A yearly check for consistency between the user account database and lists of employees from human resources is recommended.	
JAN-REC-10	Use personal normal and administrative accounts for daily work	Not implemented. The network administrators should have two accounts. One for daily work, and one for when administrative rights is needed. This can be implemented without any cost.	-1
JAN-REC-11	Implement password policy	Password length of 6 characters and retention period implemented. Complex password will not be implemented. Complex passwords are difficult to remember, and users might write the password one a little note on the screen.	1
JAN-REC-12	Log access to systems	In Windows Server 2003 logon and logoff attempts are logged in the system log. It is recommended to install a procedure for exporting the security log to file on a weekly or monthly basis.	0
JAN-REC-13	UPS capacity should be increased	A new UPS system has been implemented with capacity of 2 hours.	1
JAN-REC-14	Removable media should be disabled on workstations	The security policy first has to be approved by the president.	-1
JAN-REC-15	Store central files in a structured way	It is implemented. Will be refined when the migrating of the file servers to Windows Server 2003 take place.	1
JAN-REC-16	Update operation manual and prepare maintenance documentation for all systems.	Not implemented. Filling out information in the documentation template will give a good basis in a disaster recovery situation. The information should be updated regularly, printed and placed in a safe place. This can be the same place as the backup tapes. (And: Outside INE!!)	-1
JAN-REC-17	Store important data centrally	Policy implemented. The network administration presumes that most data is stored on the file servers. As long as the users have administrative rights on the workstations, they can store data locally.	0-1
JAN-REC-18	Sets of backup media should be stored offsite in order to facilitate recovery after a disaster	Not implemented. The best solution is to have an outside location, for example in a bank box. An alternative can be a fireproof box located at a lower floor inside INE.	-1
JAN-REC-19	Physical access to server room	Not implemented. It is recommended to find a solution as soon as possible. The ideal solution is to have a powerful door with a card reader based lock. Today 5 people have a key to the door.	-1

3.2 (New)Recommendations regarding Windows 2003 migration plan

DEC01	Windows Server R2	Microsoft is releasing the new version of Windows Server 2003 in December 2005. The version is called Windows Server 2003 R2 and is binary identical to Windows Server 2003 SP1, but there is many new functions INE can use. Particularly about storage management Microsoft has made many improvements. It is recommended that INE install this version of Windows.
DEC02	Update systems before migration	Implement any service packs and security updates to the Windows Server 2003 systems before start of the migration.
DEC03	Windows time service	Implement Windows time service. Logging on a Windows Active Directory is depending on Kerberos. The clock on the domain controllers must match the clock on the workstations within 5 minute otherwise the users can not log on the system. A domain controller can download the correct time from at time source on the internet, and the other servers and the client can get the correct time form this domain controller.
DEC04	2 DNS servers	Implement 2 DNS servers. Active directory is depending on the DNS service and the entire infrastructure will not be working properly if the DNS server is unavailable. For this reason there should be 2 DNS servers in the infrastructure. The DNS can be configured to forward DNS enquiries to an external DNS server on the internet. This will allow internal services to look-up IP addresses of external servers. This is useful for e.g. time service.
DEC05	2 DHCP servers	Implement 2 DHCP servers in the network infrastructure. The infrastructure can function for some days without at DHCP server, but new workstations will not be able to obtain an IP address. The DHCP service is part of the operating system, and for no extra cost, this service can be duplicated in the infrastructure. In case of disaster of one DHCP server, the other server can still maintain the service for the clients.
DEC06	2 WINS servers	Implement 2 WINS servers. Older applications may depend on the WINS service. For this reason it is recommended to install the WINS service in the network infrastructure. The WINS service should also be duplicated like the DHCP service.
DEC07	Front-end mail server in DMZ	Set up a front-end Webmail server in the

		DMZ zone. The employees at INE can read mail from a browser over the internet. To avoid direct access from the internet to the Exchange server it is recommended to implement a front end Webmail server. This server then forwards mail user request to the Exchange server on the internal network.
DEC08	Group policy	It is recommended to configure the windows environment and specially the security on the servers and workstation by use of group policy. When ever possible configure configuration changes by use of group policy.
DEC09	FSMO roles	Place all Flexible Single Master Operation (FSMO) roles on a domain controller with a tape device. Windows Server 2003 has 5 FSMO roles: Schema master, Domain naming master, PDC emulator, RID master and Infrastructure master. As a general rule, the infrastructure master should be located on a non global catalog server, but in a single domain forest it is not an issue. Both domain controllers should be global catalog servers.
DEC10		In a transitional period some servers will be in the new Windows Server 2003 domain and some servers will still be in the old Windows NT 4.0 domain. In this period permissions must be reflected to service users from both domains.

3.3 New recommendations regarding security

ID:	Description	Status and comments
DEC11	Deploy security updates.	Every second Tuesday Microsoft releases new security updates. Particularly the portal server but also internal servers and workstations ought to be patched on a regular basis. With use of Windows Server Update Server (WSUS) this process can be simplified. INE computers can contact a central WSUS server, instead of Microsoft. This will reduce the usage of the internet connection.
DEC12	Assign permissions using group nesting	It is recommended to assign file permissions using group nesting. Domain local group are assigned rights on objects. Every user should have a global user group account. This group can be added to the domain local group when permissions are needed.
DEC13	New physical firewalls	The production network is protected by an old firewall and the portal server is protected by a software firewall directly on the server.

		It is recommended to invest in new firewalls for better protection of the internal servers and the portal server. It is important to buy equipment that is well-known on the market, and well documented by the supplier. This may be at firewall/router from Watchguard, Cisco or some other well-known supplier.
DEC14	Only allow needed traffic through the firewall	The traffic that passes the firewall should only be allowed if it is necessary. If possible allow traffic to and from specific hosts. A recommended firewall configuration has been produced and sent to the INE network administration.
DEC15	Portal server connected to internal network	The portal server is of course connected to the internet, but there is also a connection directly to the internal network. If a hacker can manage to get control of the portal server, he will have access to the internal network. It is recommended to move the internal network connection to the DMZ LAN. The traffic from the internal network can be routed through the WatchGuard firewall.

3.4 General recommendations.

ID:	Description	Status and comments
DEC16	Only browse for INE relevant information on the internet.	It is recommended that only INE relevant information is downloaded from the internet. Internet radio, video, music etc. should be banned. This can be implemented by configuration changes on the Squid proxy server.
DEC17	Knowledge of Linux and open source	It is recommended to get basic knowledge of Linux for testing purpose. It is possible that part of the environment in the future can run on Linux. It will be advisable to get experience on this platform already now. Also look at open source software. There are many open source application that run on the Windows platform. For example the Open Office may be an alternative to Microsoft Office for some or even all users.

Annex 1 Terms of reference for the mission

TERMS OF REFERENCE

for a short-term mission
on

Migration from Window NT to Window 2003

November 28 - December 9, 2005

within the Scandinavian Assistance to Strengthen the Institutional Capacity of INE/Mozambique

Consultants: Bo Guldager
Counterparts: Anastácia Honwana, Salomão Muianga, Pedro Miambo, Bruno Couto de Abreu

D R A F T

Background

In 1999-2000 INE installed Windows NT server. This operating system is supported until 2003 and therefore INE needs to upgrade to a new operating system which, o current platform, means Windows 2003 Server. The initial planning took place in Jan 2004. In January 2005 two of the three involved technicians went to India for a mc training in the use of Windows 2003 Server. Due to the price of Windows 2003 Exchange Server software licenses the migration had to be postponed until INE ma major reallocation of funds, with the approval of the Steering Committee.

The migration will be carried out by INE technicians, rather than by LTAs on a short mission. However, an LTA knowledgeable of the platform can still add significant v by auditing the implemented solution in the areas of robustness, performance, security.

3.4.1.1.1 Objective

The general purpose of the activity is to ensure the reliability and security of the server environment.

The objective of the having an STA participate in the final stages of the migration is to dig into the experience of Statistics Denmark both regarding the new environment and ensure the quality of the implementation as well as of the documentation of the configuration (disaster recovery procedures and the like). Valuable input regarding the application of IT-policies and security policies at software level are also expected. Further, the LTA will give education on security issues related to Windows 2003, and in general. Finally,

general experience sharing between the STA and the DISI staff is considered very valuable.

3.4.1.1.2 Expected results

A well performing, secure, and well described server environment.

Activities

Server network upgraded from Windows NT to Windows 2003. This includes:

- Audition of server configuration
- Audition of the migration process itself
- Operation manuals
- Disaster recovery procedures
- Security auditing
- Training on security issues

Tasks to be done by INE to facilitate the mission

- Elaborate ToR for the mission
- Prepare and supply the consultant with necessary documents and information, such as mission reports, strategies, plans etc.
- Supply good working conditions for the consultant
- Supply hardware and software.

Consultant and Counterpart

Consultants: Bo Guldager
Counterparts: Anastácia Honwana, Salomão Muianga, Pedro Miambo, Bruno Couto de Abreu

Timing of the mission

Two weeks (November 28 - December 9, 2005).

Report

The consultant will prepare a short draft report to be discussed with the counterparts before leaving Maputo. The final version will be sent to INE within one week of the expert having returned to Denmark. The Counterpart then has to provide, also within one week, at least a summary in Portuguese (if the main report is in English – or else; vice versa) to be included in the final printed report. Statistics Denmark, as Lead Party, will print the final version within three weeks of the end of the mission. The structure of the report should be according to Danida format.

These Terms of Reference were prepared by

Day / / .....

Approved by/in the name of the President of INE

Day / / .....

Prepared by: Karsten Bormann, Advisors, Scanstat

Annex 2 Persons met during the mission

- Mr. Tomás Bernardo
- Ms. Anastásia Juda Honwana
- Mr. Salomão Muianga
- Mr. Pedro Miambo
- Mr. Bruno Couto de Abreu
- Mr. Lars Carlsson
- Mr. Karsten Bormann
- Mr. Jesper Ellemose