الإسلامي

SECURITY الأمان

الفصل الأول

الأمان فى نيتوير3.1

المقدمة :

تحتاج لمعرفة عدة مظاهر للأمان فى نيتوير مثل تصميم الأمان وتيسيره وكيفية تحقيقها.

سنتمكن من دراسة : معالجة الأمان فى الشبكة والملفات - تجهيز الأمان للمستخدم والمجموعة ـ تحقيق أمان الشبكة والملفات ـ تحقيق الأمان للجهاز الرئيسى وشاشة المتابعة.

أولاً : معالجة الأمان فى الشبكة والملفات:

مستويات الأمان فى الشبكة كما يلى. .Login - Rights - Attributes - F.S :

انظر الرسم (٦-١-١)

Login (1) : يتحكم فى الوصول إلى الشبكة ، يتكون من اسم أو رقم تعريف المستخدم User ID يتبعه كلمة السر .

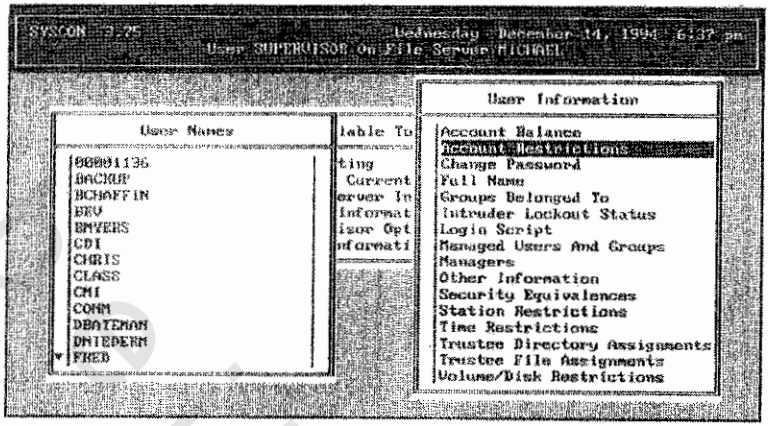
أول خطوة فى إجراءات الأمان هى : التحقق من كلمة السر ـــ مقارنة اسم وكلمة سر المستخدم ـ التحقق من محظورات المستخدم . ويتم ذلك فى معلومات الـ Bindary .

ملاحظة :

الـ Bindary عبارة عن قاعدة معلومات تحتوى ثلاثة معلومات Objects : مثل المستخدم والمجموعة ـ Properties خواص كل منهم مثل كلمة Data sets - قيم الخواص .

بعد التحقق من اسم وكلمة سر المستخدم يتم التحقق من المحظورات على المستخدم مثل الأيام والوقت المسموح له بالدخول على الشبكة خلالها . وعدد محطات العمل التى يمكن الدخول منها Intruder Detection . للتحكم فى عدد مرات

محاولة المستخدم الدخول الغير صحيح . تستخدم شاشة Syscon لذلك.



SYSCON's User Information menu.

انظر هذه الشاشة ☝

*محظورات الـــ : Account مثل هل لابد من كلمة سر للمستخدم – وأقصر طول للكلمة

ـــ هل يمكن له تغييرها وهل يغيرها دورياً ـــ وهل لحساب المستخدم تاريخ انتهاء – وهل يتم تحديد وصلاته بالشبكة.

*محظورات الـــ : Station يمكنك تحديد أى محطات الشبكة يمكن أن يدخل منهـــا المستخدم.

* محظورات الوقت : Time يمكنك تحديد أوقات الدخول خلال اليوم.

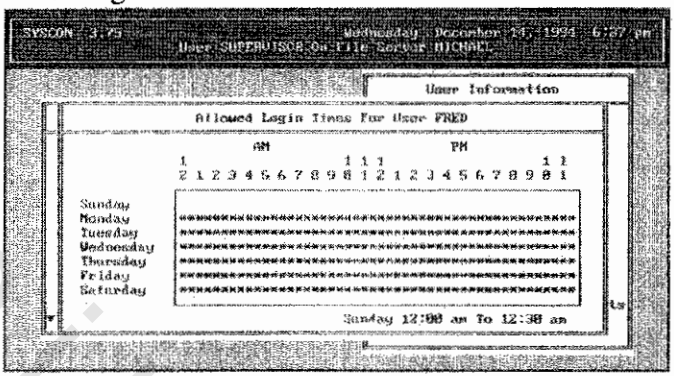
*محظورات الـــ : Volume Disk يمكنك تحديد المساحة المسموح بهـــا للمســـتخدم على اسطوانة الشبكة.

Rights (2) : لكى يستغل المستخدم موارد الشبكة بعد ما تم التـــأكد مـــن صحـــة دخوله، يجب أن تكون لديه حقوق Rights تم اعطاؤها له من مدير الشبكة . هـــذه الحقوق تعطى للمستخدم حسب تصنيفه . وأصنافه هى :

Supervisor - Sup. Equivalent - Workgroup Manager - Account Manager - Pconsole Operator - Fconsole Operator - User.

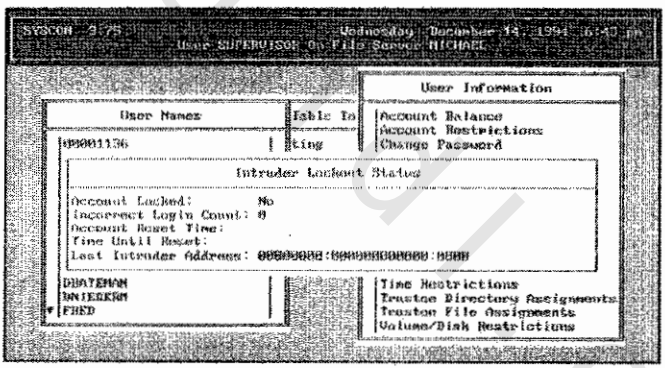
يمكنك تأمين نظام الملفات باستخدام :

Trustees - Directory and File Rights - Inheritance - Inheritance Rights Mask (IRM) - Effective Rights.



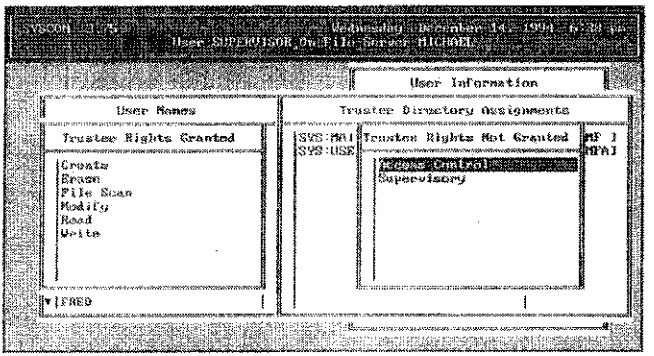
SYSCON utility display of Allowed Login Times For User FRED.

انظر هذه الشاشة



The Intruder Lockout Status for user FRED.

انظر هذه الشاشة



User FRED's Granted and Not Granted Trustee Rights.

انظر هذه الشاشات

الحقوق المعطاة للمستخدم تشمل ما يلى : التحكم فى الدخول (لتعديل الـــــ Trusteeو IRM لملف أو فهرس)

Create	إنشاء (لإنشاء ملفات أو فهارس)
Erase	مسح (لمسح ملفات أو فهارس)
File Scan	استعراض ملفات أو فهارس
Modify	تغيير ملف أو فهرس
Read	لفتح أو قراءة أو تشغيل ملف
Supervisory	هى الحقوق على الملفات والفهارس
Write	لفتح ملف والكتابة فيه

من خلال IRM يمكنك تحديد الحقوق أيضاً . وهى تتوفر لكل ملف عند إنشـــائه ومبدئياً تعطى كل الحقوق على الملف . ويمكنك تعديل IRM لاستخلاص أية حقوق لا تريد السماح بها على الملف أو الفهرس . لا يمكن للـــ IRM الاستخلاص مـــن الـــ Supervisory .

Attributes(3): باستخدام Flag يمكنك تخصيـــص صفـــات للملفـــات والفهـــارس Flagdir .

```
Z:\PUBLIC>flag /?
USAGE:  FLAG [path [ option | [+|-] attribute(s) ] [SUB]]

386 Attributes:
---------------
RO Read Only
RW Read Write
S  Sharable
H  Hidden
Sy System
T  Transactional
P  Purge
A  Archive Needed
RA Read Audit
WA Write Audit
CI Copy Inhibit
X  Execute only
DI Delete Inhibit
RI Rename Inhibit

All  All
N    Normal
SUB

Z:\PUBLIC>
```

FLAG Help screen displaying attributes.

انظر الشاشة

هذه الصفات هى :

- Hidden - Sharable - Read Write - Read only.
- Archive Needed - Purge - Transactional - System.
- Execute only - Copy Inhibit - Write Audit - Read Audit - Rename Inhibit - Delete Inhibit.

: File Server (4)

1ـ يجب وضع الجهاز الرئيسى فى مكان محظور كغرفة مغلقة من قائمة Monitor NLM

2ـ كلمة سر لرؤية الشاشة.

3ـ كلمة سر لامكانية مشاهدة الشاشة من بعد.

يطلب ذلك عند كتابة RCONSOLE وتشمل. REMOTE.NLM , RSPX. NLM

(5) Packet Signature: لتحديد تعريف الرزم بين الجهاز الرئيسى والعملاء لمنع المستخدم من جلب منفعة أكثر مما هو محدد له . ولها أربعة مستويات.

انظر الرسم (٦-١-٢)

ثانياً : المستخدم والمجموعة وتجهيزهم :

قبل أن يتمكن مستخدم من الدخول على الشبكة يجب أن يكون له حساب .

تجهيز حساب مستخدم يحتاج ثلاثة خطوات : إعداد الحساب ــ هل يحتاج كلمة سر ــ هل عليه محظورات .

لتسهيل إعداد مستخدم resU جهز مجموعة puorG لتنفيذ الحقوق والمحظورات عليهم .

* **User** : من Syscom اختار User Information ثم اضغط زر Insert وواصل العمل.

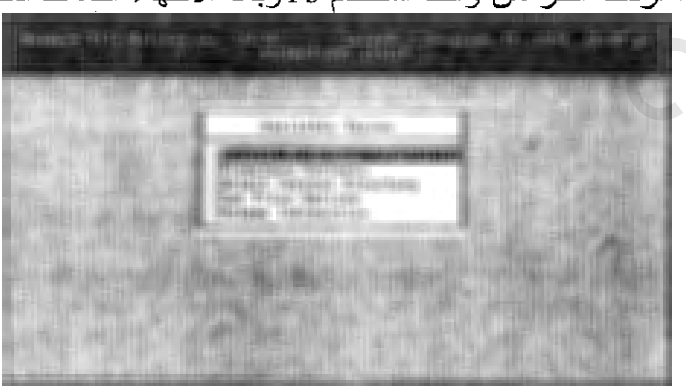
* **Group** : مثل User والفرق هو اختيار Group Information من قائمة. Syscon

ملاحظة :

يمكن تجهيز المستخدم والمجموعة بطريقة آلية من User DEF و Makeuser، وسوف ينفذ ذلك على كل مستخدم تنشئه.

ثالثاً : أمن الشبكة ونظام الملفات:

يستخدم لذلك امكانية Syscon و Filer من Syscon يمكن تجهيز مستخدم ومجموعة مستخدمين والأمان المتعلق بهم بالإضافة إلى مديرى مجموعات العمل Workgroup Manager، ومدير حسابات المستخدم والمجموعةAccount Manager أيضاً Console Operator والـ . Trustee من Filer يمكنك تحديد الـ Trustee باختيار من القائمة Current Directory Information ومنها اختار Trustee ثم Insert، وإذا أردت أكثر من واحد استخدم F5 وبعد الانتهاء اضغط أدخل.



FILER's Available Topics menu.

انظر الشاشة

لإعطائهم حقوق على هذا الفهرس Directory أو الملف File بالعودة إلى القائمة Available Topics واختار Current Directory Information اختار Trustee لاستقبال . Rights اضغط زر Insert لمشاهدة قائمة الحقوق واستخدام F5 لاختيار عدة حقوق ثم أدخل.

يمكنك أيضاً استخدام الأوامر التالية :

Rights - Tlist - Grant - Allow - Revoke - Remove.

ملاحظة :

استخدم Syscon لعمل محظورات مثل عدم السماح لمستخدم بالدخول على الشبكة والأوقات المسموح بها للدخول ــ ومن أى محطات العمل يمكن الدخول.

يتم عمل محظورت لمستخدم محدد من شاشة User Inform من: Syscon اخفى المستخدم User وبذلك لن يدخل على الشبكة ــ اظهره ــ جهز الحسابات Account لتحديد مدة صلاحية ــ أزل تاريخ انتهاء حظر.

رابعاً : أمان شاشة الجهاز الرئيسى :

وضعه فى مكان محظور ــ إنشاء كلمة سر للشاشة Aconsole or Rconsole . جهز أولاً Monitor NLM ثم. Lock

***الأوامر :**

Rights اكتب مكان Path باسم مسار ملفك المراد رؤية حقوقه.

Tlist لمشاهدة قائمة الـ Trustee لفهرس معين . اكتب اسم الملف أو الفهرس ثم User أو. Group

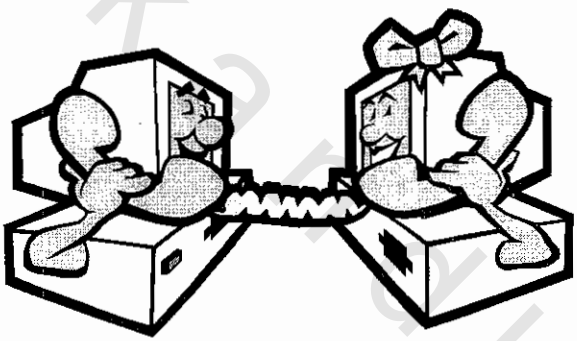
Grant لإعطاء Trustee Rights لفهرس معين أو ملف . اكتب مكان Rights الحقوق التى تريدها مفصولة بمسافات مثل R F واكتب المسار ثم المستخدم أو المجموعة.

Allow لتغيير IRM لفهرس معين أو ملف . اكتب المسار ثم الحقوق

التى تريد منعها.

Revoke لاستبعاد حقوق من مستخدم أو مجموعة . اكتب الحقوق ثـــم المسار ثم الاسم.

Remove لإزالة مستخدم أو مجموعة من قائمة Trustee لملف أو فهرس معين. اكتب الاسم والمسار ثم حدد الاختيارات. Options



الفصل الثانى

حماية شبكة نيتوير3.1x

المقـدمة :

أشياء معينة مثل كلمة السر وتعريف المستخدم للدخـــول و.Packet sign (NCP) وآخرين يساعدون فى حماية شبكتك من الدخول الغير مصرح به .

ليس الدخول الغير مصرح به هو المشكلة الوحيدة ولكن أيضاً انهيار التيار أو الاسطوانة الصلبة .

سوف نتمكن من دراسة : نيتوير تساعدك على تحقيق الحماية من كل ذلك يتوفيرها ثلاثة أشياء لسلامة البيانات ــ دراسة قدرة النظام على تحمل الأخطاء ــ دراسة خدمات إدارة التخزين ــ النسخة الاحتياطية.

أولاً : أخطاء النظام واحتمالها System Fault tolerance (SFT) :

SFT هو أحد طرق حماية البيانات فى شبكة نيتويـــر . وتوفـــر المـــيزات التالية:

Disk Monitoring - Disk Duplexing - Duplicate Fat's and Det's - Hot Fix - Read After Write Verification - TTS - UPS Monitoring.

انظر الرسم (٦-٢-١)

ثانياً : دراسة خدمات إدارة التخزين Storage Management Services :

إن مركزة الحفظ والوصول للبيانات يجلب معه احتماليـــة فقـــد البيانـــات لانهيار الاسطوانة الصلبة . توفر نيتوير امكانية Storage Management (SMS) Services وتسمح بحفظ واسترجاع البيانات . وهى مجموعة NLM وأهم مـــا فـــى هذه الامكانية هو تصميمها.

تمكنك SMS من النسخ الاحتياطى لملفات النظام باستخدام البرامج والمعدات الخاصة بالنسخ الاحتياطى المتوافقة مع SMS والتى تختارها أنت. ايضاً

NetWare's SFT Features

Feature	*Description*	*Purpose*
Disk Duplexing	NetWare duplicates data from the NetWare partition of one hard disk to that of another hard disk, using a different adapter, cable, and controller.	To protect data from hard disk failure.
Disk Mirroring	NetWare duplicates data from the NetWare partition of one hard disk to that of another hard disk, using the same adapter, cable, and controller.	To provide a second copy in case of hard disk failure.
Duplicate FATS and DETS	NetWare duplicates the *File Allocation Table* (FAT) and *Directory Entry Table* (DET) to different parts of the hard disk.	To ensure the OS always has access to these tables.
Hot fix	When a bad block is identified, hot fix redirects the data to another area on the hard disk.	To store data in a valid area of the hard disk.
Read-after-Write Verification	When data is stored in a block on the computer's hard disk, read-after-write verification checks that block of data to make certain it can be read. After several unsuccessful tries, it marks the hard disk block as bad and saves the data to another location.	To verify the readability of the data that it just wrote to disk.
TTS	Tracks database transactions to ensure either that all related database changes are saved to the database or that no changes are saved.	To protect the integrity of database files.
UPS	This software lets you control an *Uninterruptible Power Supply* (UPS) connected to your network server.	To protect your server from power outages/fluctuations.

انظر الجدول

تمكنك من النسخ الاحتياطى واسترجاع الملفات بصرف النظر عن نظام التشغيل الذى تستخدمه أنت . وهى تدعم دوس و OS/2 وماكنتوش ووندوز ويونكس.

نظام النسخ الاحتياطى فى نيتوير يسمى . Sbackup ولضمان سلامة البيانات يجب أن تجدول نسخها الاحتياطى سواء استخدمت نظام نيتوير Sbackup أو أى نظام خارجى.

إن نظامية النسخ الاحتياطى للشبكة هام . وتوصف نيتوير عدة تقنيات للنسخ الاحتياطى كما يلى :

Full Backup - Incremental Backup - Differential Backup.

ـ النسخ الاحتياطى الكامل :

ينسخ جميع الملفات الموجودة بالجهاز الرئيسى File server بما فيه الملفات التى تقوم بعملية النسخ الاحتياطى على الجهاز الرئيسى أو أى جهاز رئيسى آخر وبما فيها ملفات الـ System و . Bindary يسبب أن الـ) Modify Bit التى تبين ما إذا كان قد جرى تغيير على الملف منذ آخر نسخ احتياطى له) يحدث لها Reset للملف المعمول له نسخ احتياطى . يجب أن تعمل نسخ احتياطى كامل للشبكة نيتوير فور تجهيزها على الشبكة.

ـ النسخ الاحتياطى نوع Incremental or Differ :

يمكن اختيار النسخ الاحتياطى للآتي : فهارس محددة ـــ كل الملفات التى تغيرت منذ آخر نسخ احتياطى ـ الملفات ذات الامتداد المحدد.

ـ Incremental : لكل الملفات المنشأة أو المنسوخة على فهرس معين أو قد تعدلت منذ آخر نسخ احتياطى لها ـ ويحدث Clear للـ . Modify Bit

ـ Differential : لكل البيانات التى تغيرت منذ آخر نسخ احتياطى لها بصرف النظر عن أن الملفات المتغيرة قد نسخت احتياطياً بطريقة Incremental لأن الـ Modify Bit لم يحدث لها Clear ويسمح لك ذلك بعمل Incremental لاحقاً.

ثالثاً : النسخ الاحتياطى والاسترجاع للجهاز الرئيسى لنيتوير :

قبل استخدام Sbackup يجب أن تعرف شيئين فى نوفل . Target - Host :

- **Host :** هو الجهاز الرئيسى الذى يوجد عليه جهاز النسخ الاحتياطى.
- **Target :** هو الجهاز الرئيسى أو محطة العمل التى عليها الملفات التى يعمل لها نسخ احتياطى.

خطوات عمل النسخ الاحتياطى سواء من الجهاز الرئيسى أو العميل :

1ـ حمل TSA312.NLM على الجهاز الرئيسى. Target

2ـ حمل مشغل جهاز النسخ الاحتياطى على الـ. Host

3ـ حمل Sbackup على الـ. Host

4ـ أدخل اسم وكلمة سر المراقب. Supervisor

5ـ اختار جهاز النسخ من القائمة.

6ـ اختار الـ Target من القائمة لاختيار الجهاز الرئيسى أو محطة العمل التى عليها الملفات لعمل النسخ الاحتياطى لها.

7ـ أدخل اسم المستخدم وكلمة السر.

8ـ اختار قائمة Backup من القائمة الرئيسية .

The Backup Menu.

انظر الشاشة

9ـ اختار Select working dir وأدخل مسار الملفات.

10ـ املأ الحقول ثم اضغط. Esc

11ـ ثم Yes على . Proceed with Backup

12ـ اختار. Start Backup

13ـ بعد الانتهاء اضغط Enter لإعادة عرض قائمة الـ Backup ، ثم اضغط Esc للقائمة الرئيسية.

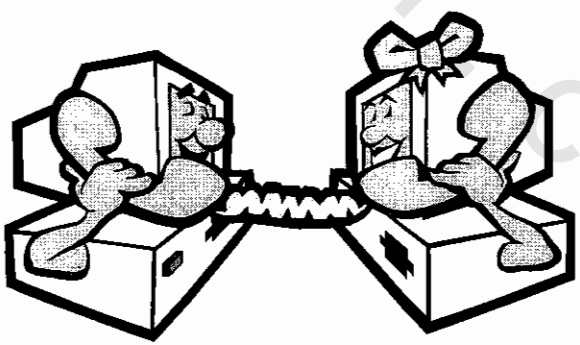
ملاحظة :

عميل على الدوس بدلاً من الجهاز الرئيسى يجب أن تحمل TSA - Dos.NLM وسوف يحمل آلياً كل من:

Streams.NLM , Smdr31X.NLM , TLI.NLM , SPXS.NLM or IPXS.NLM

بالإضافة لذلك يجب أن تحمل TSA_SMS.Com على محطة العمل التى عليها الملفات وذلك بتعديل ملف الحزمة لمحطة العميل Autoexec.Bat ثم أعد تشغيل العميل ثم أكمل خطوات لتحميل Sbackup على الجهاز الرئيسى.

يمكنك أيضاً عمل النسخ الاحتياطى على نظام OS/2 بتحميل TSAOS2.NLM على الجهاز الرئيسى



الفصل الثالث

دعم وحماية الجهاز الرئيسى لنتوير 3.1

Supporting & Protecting Netware 3.1x servers

المقدمة :

ليس هناك معنى فى مدى عمل الجهاز الرئيسى بكفاءة إذا ما صادفه فيروس أو تعرض الهارديسك للتحطم.

لذلك فبالاضافة لصيانة وتحسين أداء الشبكة فإنه يلزم أيضاً حمايتها . تأكد عند قيامك بحماية الشبكة من الفيروسات بأنه يمكنك استعادة ملفات الشبكة السابقة المعمول لها نسخة احتياطية.

سوف نتمكن من دراسة : الحماية من الفيروسات ـــ النسخ الاحتياطى والاسترجاع.

أولاً : تحقيق الحماية من الفيروسات:

انظر الرسم (٦-٣-١)

توجد عدة مصادر للفيروسات من خلال البرامج المنسوخة واللوحات الالكترونية BBS واسطوانات البيانات . وكلما زادت حقوقك على الشبكة كلما زادت فرصة الفيروسات فى التدمير . ولإن أغلب الفيروسات تكون وظيفتها مهاجمة الملفات التنفيذية فإن المستخدم الذى له حق تغيير علامة القراءة فقط (Read only) لملفات التنفيذية يمكنه تعريضها للهجوم. لتقليص حجم التدمير الذى يمكن إن يسببه الفيروس عند دخوله على الشبكة بسبب شئ ما فعلته ، استخدم Supervisor Login عند الضرورة . بالاضافة لذلك قلص عدد المستخدمين الذين لهم قوة المراقب أو مكافئه . يجب أيضاً تقليل عدد المستخدمين الذين لهم حقوق Rights المراقب . بالاضافة لتقليص عدد محطات العمل التى يمكن إن يدخل منها المستخدم المراقب .

كمثال : حدد دخول المراقب بمحطة عمل وأخرى للنسخ الاحتياطى . بعد ذلك لا أحد يستطيع الدخول على الجهاز الرئيسى كمراقب إلا إذا حأول أحدهم عمل ذلك من محطة عملك أو من محطة عمل تبادلية.

***مراقبة الوصول للشبكة وملفاتها يتحقق بكل أو أغلب ما يلى :**

1ـ تخويل جميع المستخدمين فقط حقوق قراءة Read والبحث عن الملفات File scan للفهارس العامة مثل. Public , Login

2ـ علم الملفات التنفيذية لنتوير وملفات التطبيقات بالقراءة فقط Read only أو نفذ علامات نتوير إذا كانت ملائمة.

3ـ تأكد من إن كل الاسطوانات المرنة محمية من الكتابة عليها.

4ـ حول محطات العمل لتكون بدون محرك اسطوانات Diskless إذا أمكن.

5ـ راقب استخدام الموديم.

*** تأكد من خلو جميع الاسطوانات المستخدمة على شبكتك من الفيروسات كما يلى :**

1ـ اشترى البرامج من المصنع والموزع المعتمد.

2ـ شغل برنامج مكتشف الفيروسات على أى برامج قبل تركيبها.

3ـ وفر برنامج مكتشف الفيروسات للمستخدمين وتأكد من استخدامهم له قبل استخدام الاسطوانات.

4ـ افحص أى اسطوانات يجلبها المستخدمون.

5ـ استخدم الاسطوانة المحمية ضد الكتابة عليها.

اثنين هامين من الإرشادات:

1ـ تدريب وتعليم المستخدمين الإجراءات المتبعة مع فيروسات الشبكة.

2ـ احتفظ بنسخة احتياطية من الملفات التى لم تصاب بالفيروسات.

استعد لاصابة الشبكة بالفيروس . كن على دراية بأنواع الفيروسات المختلفة حتى يمكنك التعرف على علاماتها . أيضاً درب نفسك على الإجراءات

التى يجب اتخاذها للقضاء عليها . لو وصل فيروس للشبكة ولم تستطيع إزالته ببرامج اكتشاف الفيروسات فأفضل حل هو استرجاع النسخ الاحتياطية التى لديك السابقة على تاريخ دخول الفيروس . وقد لا تستطيع تحديد متى دخل الفيروس للشبكة بالضبط . لو كنت محتفظاً بقياسات ملائمة للحماية على أية حال فقد تتمكن من تحديد من دخل بالتقريب.

لو شغلت مضاد الفيروسات وبذلت ما فى وسعك لازالتها من الشبكة ولكن لم تزل فإنك تستطيع اختيار الاسترجاع للنسخ الاحتياطية . توفر نتوير Sbackup لتتأكد من أنه لديك وظائف الشبكة للنسخ والاسترجاع الاحتياطى على الأقل . بالطبع لا تتمكن من الاسترجاع بـ Sbackup إلا إذا كنت عملتها به.

ثانياً : النسخ الاحتياطى والاسترجاع Backups and Restores :

انظر الرسم (٦-٣-٢)

تستخدم امكانية نتوير Sbackup لنسخ واسترجاع أجزاء متعددة من الشبكة . وهى توفر عدد (٨) Modules لنسخ واسترجاع الملفات الهامة على الشبكة . بعضها يتم تحميله على الجهاز المضيف) Host server الذى هو جهازك الرئيسى File server وملحق به جهاز النسخ الاحتياطى. Backup Tape)

كمثال Sbackup : يتضمن software device interface (SDI) Module لتمرير الأوأمر والمعلومات بين جهاز النسخ وامكانية النسخ . بعض هذه الـ Modules يتم تحميلها على الجهاز الرئيسى الهدف Target server التى تريد نسخ ملفاته ، وبعض الـ Modules يتم تحميلها على العميل الهدف Target Client والتى تريد نسخ اسطوانتها الصلبة .

***نسخ الـ Bindary للجهاز الرئيسى:**

بالرغم من أنه يمكنك نسخ كل الملفات والبيانات التى على شبكتك فإنه أحياناً فى غاية الأهمية نسخ واسترجاع ملفات الـ Bindary الخاصة بالجهاز الرئيسى خاصة بعد أول تركيب لنتوير أو بعمل العديد من تعديلات على Bindary أو بتشغيل Binfix لاصلاح الـ Bindary . ليس لك حاجة للنسخ الاحتياطى للـ

Bindary فى كل مرة تعمل نسخ احتياطى للشبكة طالما لم تعمل تغييرات متعلقة به.

لو أضفت أو أزلت مستخدمين ، أو غيرت حقوق مستخدم ، أو أديت بعض المهام الإدارية التى تؤثر على Bindary الجهاز الرئيسى فإنك يجب إن تعمل نسخ احتياطى للـ Bindary.

لعمل نسخ احتياطى للـ Bindary و Trustee Assignments باستخدام Sbackup أكمل الخطوات التالية :

1ـ اعمل مراجعة تمهيدية للجهاز الرئيسى و Sbackup تشمل ما يلى :

ـ تأكد من كفاية الذاكرة على الـ Host server . حمل Monitor.NLM وتأكد من إن الجهاز الرئيسى لديه (١) ميجا بايت من الذاكرة المتاحة.

ـ اعرف كلمات سر المستخدم الذى سوف يعمل النسخ الاحتياطى (المراقب أو مستخدم آخر له حقوق المراقب) ، وإذا كنت فى النسخ على العميل فلمحطة العمل بالمثل .

ـ تذكر أى مسار خاص تستخدمه لتخزين أو استرجاع ملفات الجلسة.

2ـ قم بإعداد جهاز النسخ (وصل الكهرباء وشغله وحمل الشريط الملائم وهكذا).

3ـ اكتب Load TSA 312 على الجهاز الرئيسى الهدف فيتم تحميل TSA لذلك فإن الـ Bindary يمكن نسخه احتياطياً.

ملاحظة :

لو تستخدم نتوير 3.11 استعمل TSA311.NLM ولو كإن ٣,١٢ استعمل الحالة . TSA312

4ـ حمل المشغلات Drivers الملائمة للجهاز الذى تستخدم على الجهاز المضيف.

ملاحظة :

ـ عدل ملف DIB12$DV.DAT فى مجلد sys:system للجهاز المضيف قبل اكمال الخطوة التالية.

ـ أزل أى سطور لمشغلات جهاز النسخ التى لا يستخدمها جهازك . قد يتعين

عليك إضافة اسم المشغل وإعدادات بطاقة التحكم لجهاز النسخ الخاص بك.

ـ علم ملف DIB12$DV.DAT بعلامة Normal ثم عدله بكتابة الأمر التالى :

Load Edit sys:system\DIBI\ DIB12$DV.DAT

ـ لو تستخدم المشغل Wang Tek DIBI-11 فعليك فقط تحميل . Sbackup.NLM

ـ لو تستخدم المشغل DIBI-11 DIBIDAI اكتب الأمر التالى:

Load AHAnnnn
Load TAPEDAI

ـ لو تستخدم المشغل DIBI-11 TAPEDC001 اكتب:

Load ADAPTEC

5ـ اكتب Load Sbackup.NLM على الجهاز المضيف.

6ـ أدخل اسم وكلمة سر المستخدم.

7ـ اختار اسم مشغل الجهاز Device Driver المناسب لجهاز النسخ الاحتياطى المستخدم

8ـ اختار الهدف للنسخ الاحتياطى.

9ـ اختار من القائمة الرئيسية قائمة Backup.

10ـ اختار Select working Directory من قائمة Backup وحدد الملفات.

11ـ فى نافذة Backup Options ومن حقل WHAT to Backup اختار نسخ الـ Bindery الجهاز الرئيسى لنتوير هو الافتراضى.

12ـ عبئ الحقول واعمل الاختيارات المطلوبة ثم اضغط زر . ESC

13ـ عند الاشارة إلى. Proceed with Backup

14ـ اختار Start Backup now وتابع بقية الخطوات مثل إدخال الشريط ، وهكذا.

عند اكتمال عملية النسخ الاحتياطى يمكنك عرض Error Log أو ضغط زر Esc للعودة للقائمة الرئيسية . بعد ذلك يمكنك الخروج من Sbackup واختار هدف آخر للنسخ الاحتياطى ، أو أعد استرجاع النسخة السابقة ، أو اختار النسخ الاحتياطى لعميل بالشبكة.

***النسخ الاحتياطى لشبكة العميل Network Client :**

يمكنك ذلك لعدة أسباب : أحسن الأسباب ـ خاصة مع العميل الذى يستخدم

الدوس ــ هو إن يكون العملاء منتج تشبيك الخاص بـــ Novell's Personal Netware . لو كذلك فإن المستخدمين الآخرين قد يصلوا إلى الاسطوانة الصلبة لهذا العميل مثل Sbackup فى نسخ الـ Bindery للجهاز الرئيسى عمل ذلك للعميل .

بعض المكونات المطلوبة لنسخ العميل تختلف عما يستخدم للجهاز الرئيسى .

جهز العميل لنتوير دوس للنسخ الاحتياطى بـ Sbackup.NLM كما يلى :

1ــ اكتب فى الجهاز المضيف . Load TSA-Dos بعض الـ NLM سوف تحمل تلقائياً منها Streams.NLM : الذى يوفر التقابل مع مشغل جهاز النسخ الاحتياطى للاتصال بأوامره مثل . Read , Write , Rewind , Eject :

TLI.NLM الذى يوفر التقابل بين Streams والبرنامج الطرفى للمستخدم .

SPXS.NLM أو IPXS.NLM الذى يوفر الوصول بين Streams والبروتوكول المتعلق به Sequenced Packet Exchange (SPX) : أو Internetwork Packet Exchange (IPX)

2ــ عدل ملف الحزمة Autoexec.bat للعميل لتحميل TSA-SMS.Com ثم أعد التشغيل . Reboot

ملاحظة :

عليك إجراء الخطوة رقم (٢) مرة واحدة على كل عميل الذى سوف تنسخ اسطوانته الصلبة . حينئذ كل مرة تشغل أى عميل فسوف يقوم ملف الحزمة بتحميل TSA-SMS.Com آلياً ويتم نسخ اسطوانته تلقائياً.

3ــ حمل Sbackup على الجهاز المضيف.

4ــ اختار العميل الهدف الذى تريد نسخه وتابع الارشادات.

5ــ عند انتهاء نسخ العميل أخرج من. Sbackup

ملاحظة :

لنسخ OS/2 اتبع نفس الخطوات باستبدال TSA-OS2.NLM ، واختار رمز OS2 بدلاً من. TSA-SMS.Com

الفصل الرابع

تجهيز وتأمين نظام ملفات الشبكة

فرق جوهرى بين نظم الملفات فى إصدارات نتوير يتعلق بكيفية عمل التجهيز والأمإن . فى نتوير 4 توجد اثنين من الامكانيات الرئيسية للتجهيز وهى: Netadmin , GUI فى بيئة الدوس.

سوف نتمكن من دراسة : تصميم وتخطيط وإنشاء نظام ملفات الشبكة ـــ تخطيط الأمإن ـــ تحقيق الأمإن.

أولاً : تصميم وتخطيط وإنشاء نظام ملفات الشبكة :

نتوير تستخدم المجلدات والفهارس Volumes & Directory لتنظيم الملفات والبيانات . أثناء تجهيز نظام نتوير على الجهاز الرئيسى File Server تنشأ مجلدات أساسية لبناء نظام الملفات . مجلد sys يحتوى على نظام التشغيل نتوير والملفات المصاحبة له . مجلدات أخرى يمكن إنشاؤها لعمل الآتى :

احتواء التطبيقات ـــ حفظ بيانات المستخدم ـــ التعامل مع نظم التشغيل المختلفة ـــ زيادة سماحية الخطأ ـــ بالاضافة لأى استخدامات منطقية أخرى .

يبدأ التخطيط بإنشاء أول مجلد لك ووضع نظام نتوير والفهارس المطلوبة فيه.

فهارس أخرى التى قد يضيفها مدير الشبكة لإنشاء بناء فهرسى كفء تشمل ما يلى :

*User Data : لوضع ملفات المستخدم فيه.

* Applications : لوضع التطبيقات فيها.

يمكن فصل ملفات البرامج (EXE , BAT , COM) مع فصل فهارس التطبيقات عن ملفات بيانات المستخدم فيسهل إضافة تطبيقات جديدة وتحديث الموجودة .

* Configuration : لحفظ ملفات التهيئة لتطبيقات الشبكة.

*DOS : لتسهيل الوصول لأوأمر دوس.

إذا أنشأت فهرس شبكة للدوس ضع أمر Comspec لكل محطة عمل لتشـير لدوس الشبكة لذلك تجد محطة العمل Command.com للإصدار الصحيح .

Shared Data : لجعل المجموعات للمستخدمين المشاركة فى الفهارس.

ثانياً : تخطيط أمإن نظام الملفات :

ـ المبادئ الأساسية التى يجب استيعابها لتحقيق أمإن الشبكة :

١ـ حقوق الفهرس والملف sthgiR.

٢ـ تحديد الـ eetsurT.

٣ـ ecnatirehnI.

٤ـ إعادة تحديد الحقوقRights .

5ـ IRF (Inherent Rights Filter) .

6ـ مكافئ الأمإنSecurity Equivalence .

7ـ الحقوق المؤثرة Effective Rights .

1ـ حقوق الفهرس والملف : للوصول للملف أو الفهرس يحتاج المستخدم حقـوق الوصول. Right of Access

كمثال : لو أردت قراءة ملف فإنك تحتاج حق القراءة . فى نتوير 4 يحتاج ReadRight .

NetWare 4 File and Directory Rights

Right	*Abbreviation*	*What You Can Do with This Right*
File Scan	F	See files and directories
Erase	E	Delete files and directories
Write	W	Open and modify a file
Supervisor	S	Everything all other rights enable you to do
Create	C	Make new files or directories
Read	R	Open and read or run files
Access Control	A	Change trustee assignments and IRF
Modify	M	Change attributes or name

☝ انظر الجدول

الطريقتين التاليتين Inheritance : و Parent Containers تؤمن فى الحقوق المعتمدة على مبدأ الأمان مثل تحديد الـــــ Trustee و Security Equivalance المؤمنة . وقد نوقشت من قبل.

آخر طريقتين فى القائمة Trustee [Public] وتحديد الحقـــوق الافـــتراضى سوف يتم مناقشتها .

: The [Public] Trustee–

إنه الأمين Trustee الوحيد وهو جزء من NDS عند إنشاء أول جهاز رئيسى لنتوير . 4 وهو يسمح بقراءة والبحث عن الملف Read , Scan عند طلبه من أى شئ موصل ــ (نتوير Dos Requester يكون محملاً ولكن المستخدم لـــم يدخـــل بعـــد للشبكة) – بالشبكة يعمل Trustee [Public] لشئ Object أو فهرس أو ملف.

ملاحظة :

تأمين حقوق Trustee [Public] يمكنك مـــن إعطـــاء جميـــع المســـتخدمين والأشياء حقوق Read , File Scan بدون الحاجة لسابق دخولهم على الشـــبكة ويتـــم تأمينها بطريقة افتراضية .

: Default Rights Assignment –

إذا أردت إنشاء فهرس لمستخدم حينما ينشأ شئ User Object فى NDS فإن User Object يتم إعطاؤه كل حقوق نظام الملفات مـــاعدا المراقـــبSupervisor

لفهرس المستخدم الخاص به .

بالاضافة لذلك فإن الأشياء Objects التالية تعطى حقوق المراقب فى نظـــام الملفات :

ـ أشياء لها حقوق NDS للمراقب للـ Server Object .

ـ شئ الخدمات المراقب للـ Bindery.

المستخدم الذى أنشأ شئ الـ NDS للجهاز الرئيسى يتم إعطاؤه أيضاً كـــل حقوق هذا الشئ شاملاً حق المراقب لنظام الملفات.

بصرف النظر عن الطريقة التى يحصل بهـــا شـــئ Role المســـتخدم أو المجموعة أو الشركة على حقوق نتوير لنظام الملفات ، الحقوق المحصلة عنـــد أى نقطة معطاة فى نظام الملفات تسمى Effective Rights الحقوق المؤثرة.

نظام ملفات نتوير يحسب الحقوق المؤثرة عند أى نقطة فى نظام الملفـــات ليحدد أى Access Object سوف يتم إعطاؤه.

لتأمين الشبكة فإن مدير الشبكة يجب إن يكون قادراً على تحقيق الحقـــوق المؤثرة لمستخدمين معينين.

لتحديد الحقوق المؤثرة يجب إن تعرف أولاً أى الحقوق تم تأمينها خـــلال الأشياء المختلفة . لإيجاد هذه المعلومة افحص تحديد الـ Trustee لشئ المســـتخدم نفسه . ثم انظر ما إذا كإن شئ المستخدم قد أعطى أى أمإن مكافئ أو هو جزء من مجموعة . أيضاً افحص الحقوق المحددة لشئ المستخدم Parent Container مثل أى Containerأعلى منه والذى منه يستطيع المستخدم Inherint الحقوق . هذا يعنى أنك تحتاج معرفة أى الحقوق تخص هذا الشئ وما إذا كانت هذه الحقوق مؤمنة بصفـــة خاصة للـ Container ومحددة تلقائياً By Default أو للـ . [Public] عندما تعـــرف أى الحقوق تم تأمينها لشئ المستخدم أو Inherinted اتبع مسار هذه الحقوق خـــلال الشجرة.

تذكر للأخذ فى حسبانك أى IRF الممكن ترشيحها خارج أى أو كل هذه الحقوق

ثالثاً : تحقيق نظام أمان الملفات:

ضع فى اعتبارك العاملين التاليين :

1ـ سريان الحقوق من أعلى لأسفل.

2ـ تخطيط تحديد الـ Trustee.

ضع الاعتبارات الآتية :

ـ صمم من التحديد المحدود للدخول Access إلى التحديد المتسع ومن قمة الشجرة إلى قاعها.

ـ اعطى كل Trustee الحقوق التى تحتاجها فقط عند كل مستوى.

ـ استخدم الميراث ecnatirehnI لتسهيل سريان الحقوق عند الحاجة واستخدمIRF لإزالة الحقوق عندما تكون حقوق معينة ليست ذات حاجة .

ـ ضع خطة الحقوق بادئاً من [Root] لتسرى لأسفل إلى الفهارس والفهارس الفرعية فالملفات.

ـ الحقوق الكبرى فقط عالية فى نظام الملفات عند الضرورة.

ـ خطط واصنع تحديد الحقوق للمجموعات أولاً ثم المستخدمين ثم مكافئ الأمان.

شئ آخر يؤخذ فى الاعتبار عند تخطيط أمان نظام الملفات وهو الصفات المعطاة Attributes للملفات والفهارس.

ملاحظة :

ـ الصفات (A/Archive,H/Hidden,R/Read only)والنظام system هى صفات الدوس

ـ الصفات (Copy Inhibit, Delete Inhibit , Rename Inhibit)هى صفات الماكنتوش

لتحقيق نظام أمان الشبكة استخدم أدوات إدارة الشبكة من نتوير .

الأداتين الرئيسيتين هما Netadmin , Netware Administrator Tool Utility. وتؤديان المهام التالية:

- منح وسحب وإعادة تعيين الحقوق.
- مشاهدة الحقوق المؤثرة . Effective Rights
- رؤية . IRF's
- إدارة صفات الملفات والفهارس.
- إدارة صفات. Trustee
- إدارة أشياء Object المجموعة والمستخدم .

File and Directory Attributes

Attribute	*Abbreviation*	*Apply To*
Archive Needed	A	Files
Can't Compress	Cc	Files
Compresses	Co	Files

☝ انظر الجدول

***منح وسحب وإعادة تعيين الحقوق :**

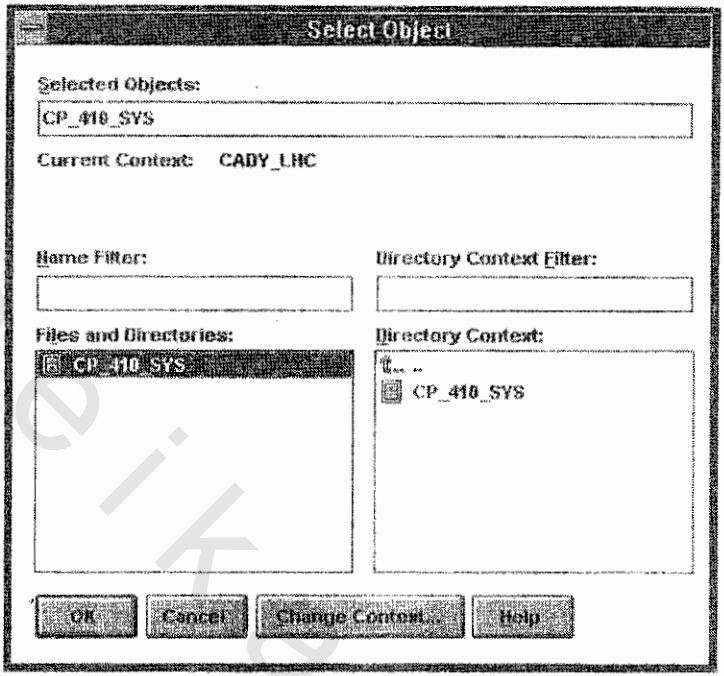
يمكنك استخدام كل من امكانيتى :

1ـ مدير نتوير .

2ـ Netadmin .

1ـ مدير نتوير Netware Administrater :

اختار الـ Object من نافذة مدير نتوير ثم اختار Rights to Files and Directories ثم اختار زر ADD وعندما تفتح نافذة Select Object اختار الملفات والفهارس التى تمنح الحقوق للشئ الخاص بها.



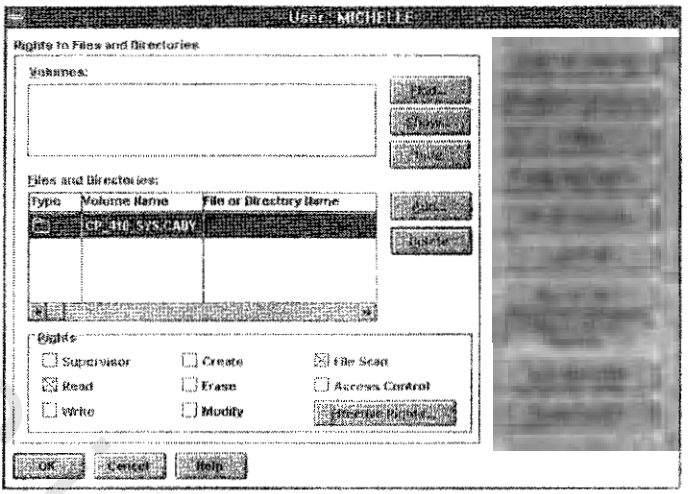
The Select Object window.

انظر هذه الشاشة

بعد منح الشئ الحقوق للملفات والفهارس فى مجلد ما Volume يمكن إعادة تخصيص (تعديل) أو مسح هذه الحقوق وذلك باختيار Rights to Files, Dir. من قائمة نافذة Netware Admin. ثم استخدم النافذة وعلم أو لاتعلم على الحقوق الممنوحة أو المسحوبة أو أزل المستخدم الممثل لـ Trustee باختيار زر Delete .

2- Netadmin :

من قائمة Class اختار Object ثم من شاشة المستخدم User name اختار View أو Edit لحقوق الملفات والفهارس . ثم اعطى اسم المجلد Volume Object والمسار البادئ لتحديد مكان الـ Object الممنوح له الحقوق . أيضاً اختار ما إذا كانت الحقوق سوف تمنح فقط للفهارس فى المسار المحدد أو للملفات فقط أو لكليهما وما إذا كانت الفهارس الفرعية ضمنها.



The Rights to Files and Directories window for user Michelle.

انظر هذه الشاشة ☝

اضغط F10 لعرض قائمة Trustee Rights . إذا لم توجد حقوق مخصصة لهذا الـ Object سوف تكون القائمة فارغة . لتخصيص (اضافة) حقوق اضغط زر Insert وحدد الفهرس الذى تضاف به الـ Trustee . الحقوق الافتراضية سوف تمنح . لتعديل هذه الحقوق اضغط Enter ثم أضف للقائمة الحقوق المتوفرة بضغط زر Insert ووضع علامة أو اختيار الحقوق الاضافية التى سوف تخصص.

***عرض الحقوق المؤثرة View Effective Rights :**

سواء كنت تشغل أى منهما يمكنك مشاهدة الحقوق المؤثرة بنفس طريقة منح وإعادة تخصيص وسحب الحقوق . الفرق الأساسى بالطبع أنك تشاهد الحقوق دون تعديلها

ملاحظة :

يمكنك استخدام الأمر Rights أيضاً لذلك الغرض.

***تجهيز IRF :**

تأكد أولاً من أنك تقف عند الموضع المطلوب فى نظام الملفات ثم استخدم أيٍ من الطريقتين السابقتين باستخدام : Netware Administrater

1ـ اختار الملف أو الفهرس .

2ـ اختار Details من قائمة Object.

3ـ اختار Trustee لهذا الملف أو للفهرس .

4ـ ضع أو (لا) تضع علامة أو اترك الخانة التالية لكل من الحقوق بدون تغيير والمذكورة فى جزء Inheritance Filter للـ Trustee الخاصة بهذا الملف أو الفهرس فى نافذتها .

ملاحظة :

لو الملف مطفأ (رمادى) فإن هذا الحق غير متاح . علامة (x) فى الخانة المقابلة للحق تبين إن الحق يمكن إن يكون . Inherited لمنع Inheritance لحق ما أزل العلامة .

باستخدام Netadmin لتجهيز : Volume Object IRF

1ـ من قائمة Object Class اختار . Volume Object

2ـ من قائمة Volume name الـ Actions اختار . View or Edit

3ـ من قائمة Trustee لهذا الملف اختار . Inherited Rights Filters

4ـ اضغط زر Insert لمشاهدة قائمة الخواص الممكن ترشيحها.

5ـ اختار الخواص المراد ترشيحها .

كمثال : اختار [Object Rights] من قائمة خواص الـ Object Rights لحصرها وسوف يتم سردها فى شاشة. Inherit.Rights Filters

6ـ اختار بند منها . قائمة من الحقوق المتاحة سوف تعرض (ليست عن طريق IRF).

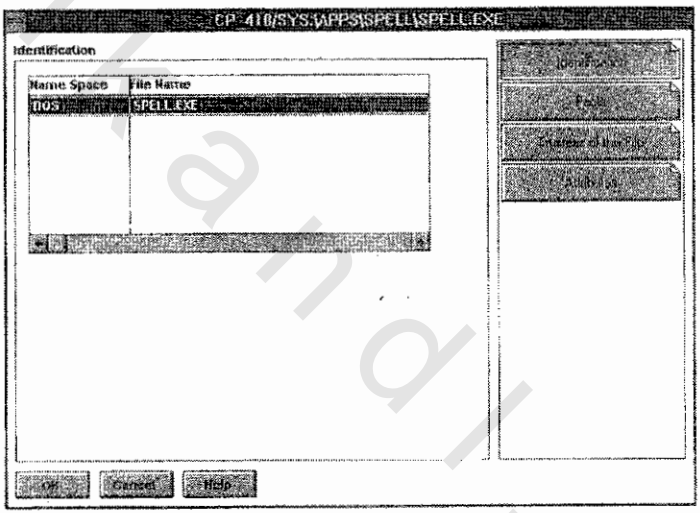
كمثال : اختار [Object Rights] سوف تفتح شاشة الحقوق المتاحة عارضة الـ [Object Rights] الغير مرئية حالياً بالـ IRF.

7ـ عدل الحقوق لكى تكون متاحة بضغط زر Insert لرؤية قائمة الحقوق التى

تختار منها الاضافة . أو امسح الحقوق من قائمة الحقوق الحالية الغير مرئية بالـــ IRF .

***إدارة صفات الملف والفهرس Attributes :**

استخدم امكانية Netware Administrator لإدارة صفات الملفات والفهارس . ولا يمكن استخدام امكانية Netadmin التى تعمل من محث الدوس ولكـــن يســتخدم Filer . باستخدام Net.Admin اختار أولاً المجلد Volume ثم قم بتوسيعه حتى تصل للفهرس أو الملف المطلوب إدارته ثم اختاره . عندما تفتح نافذة تعريفه اختـــار زر Attributes .



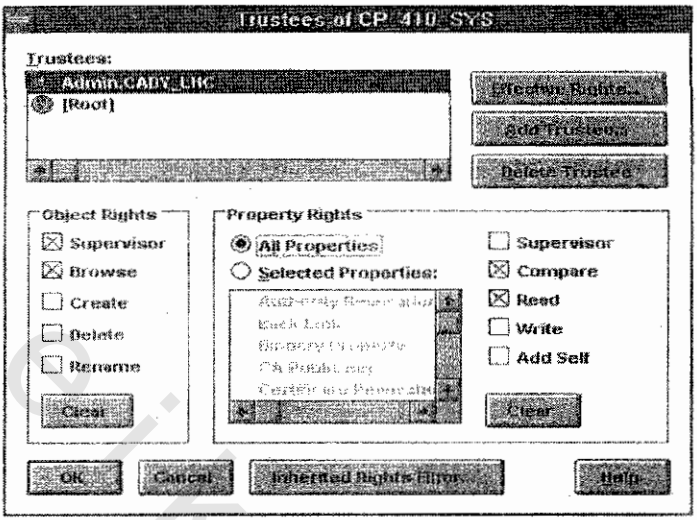
The Identification window.

انظر هذه الشاشة

ضع علامة أو (لا) تضع علامة على الصفة المطلوبة ثم Ok فتفتح النـــافذة السابقة

*** إدارة قائمة Trustee الملفات والفهارس :**

من Netware Admin اختار Object من القائمة . ثم اختار الـــ Trustee لهذا الشئ من القائمة المنسدلة . Objects من نافذة الـــ Trustee.



The Trustees window.

انظر هذه الشاشة

يمكنك استعراض الأشياء المضمنة حالياً . ومن أزرار هذه النافذة يمكنك تحقيق المهام التالية :

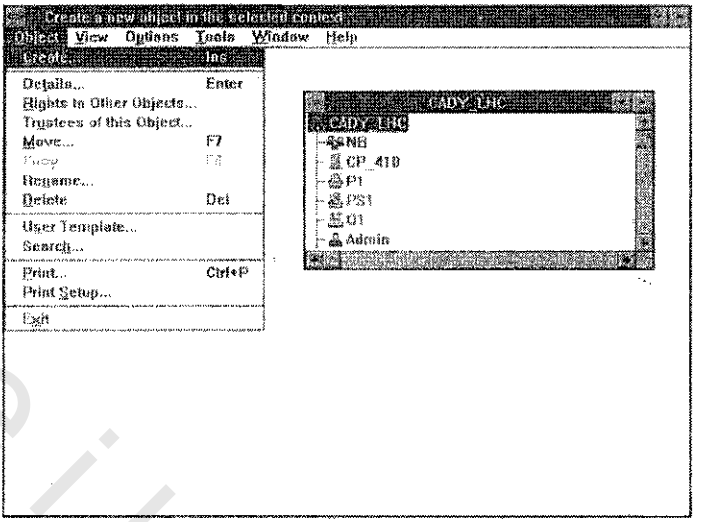
- إضافة أو مسح . Trustee
- تعديل Trustee لشئ والحقوق الخاصة به.
- استعراض. Trustee's Effective Rights
- تعديل. IRF

***إدارة المجموعة والمستخدم والأشياء الأخرى :**

قبل إدارة الشئ يجب إن يكون هذا الشئ موجوداً . إذا لم يكن موجوداً يمكن إنشاؤه باستخدام .Netware Administ أو . Netadmin

أ ـ باستخدام : .Netware Administ

اختار من النافذة الـ Container الذى سوف تضيف الـ Object إليه ثم من القائمة المنسدلة للـ Object اختار . Create



The NetWare Administrator window, with Object submenu open.

انظر هذه الشاشة

ب ــ باستخدام Netadmin :

اضغط زر Insert عند شاشة Class و Object واختار نوعه من شاشة Select an Object Calss ثم قدم المعلومات المطلوبة مثل الاسم ومحل البريد . يمكن إدارة الـ Objects الموجودة فى شجرة . NDR يمكن مسح أشياء بزر. Del يمكن أداء المهام التالية:

ــ استعراض أو تعديل صفات الأشياء.

ــ إعادة تسميتها.

ــ تحريكها .

ــ استعراض أو تعديل الحقوق الخاصة بالملفات والفهارس.

ــ استعراض أو تعديل الـ Trustee للشئ.

كل هذه المهام الإدارية تؤدى من قائمة Object-Name باختيار

Actions for Object ثم تقديم المعلومات المطلوبة.

بالاضافة لـــ .Netware Admin و Netadmin يمكنك استخدام Rights لمنـــح وسحب وعرض معلومات للحقوق من نقطة الدوس .

ملاحظة :

أمر Rights يستخدم للأسباب التالية :

ـــ استعراض الـــ . Rights/T : Trustee

ـــ مشاهدة الـــ. Rights : Effective Rights

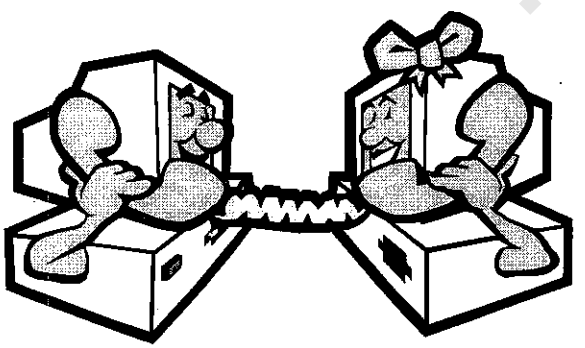
بالاضافة لذلك يمكنك استخدام أمر Ndir لمشاهدة معلومات عـــن الملفـــات والفهارس .

ملاحظة :

_يوجد اختيار إن للـــ Ndir : /Vol لمشاهدة معلومات عن المجلد.

/SPA لمشاهدة معلومات عن حجم التخزين المتاح

الاضافة لـــ Rights و Ndir يمكنك استخدام Filter لأداء مهام متنوعة عـــن الملفات والفهارس.



الفصل الخامس

تخصيص وصول المستخدم
CUSTOMIZING UESR ACCESS

إلى مدى معين فإن تجهيز محطة عمل مستخدم للوصول للشبكة يخصص وصول المستخدم للشبكة . فى الحقيقة على أية حال فإن عملية التجهيز تقوم بتخصيص وصول العميل CLIENT ACCESS أكثر من تخصيص وصول المستخدم. USER ACCESS توجد إختيارات أخرى لتخصيص وصول المستخدم. سوف تتمكن هنا من دراسة:

MENUES - LOGIN SCRIPT

أولاً : إنشاء جملة الدخول LOGIN SCRIPT :

توجد فى نتوير ٤ أربعة أنواع من جمل الدخول- CONTAINER DEFAULT - PROFILE - USER

مدير الشبكة يمكنه إنشاءها كلها ما عدا الـ DEFAULT LOGIN SCRIPT لافتراضية.

ملاحظة :

جملة الدخول الافتراضية عبارة عن جزء من ملف LOGIN . EXE ولا يمكن إنشاءها أو تغييرها بواسطة المستخدمين. وهى تعمل فقط إذا لم توجد جملة دخول مستخدم لمنعها من العمل عندما لا توجد جملة دخول مستخدم ضع أمر NO - DEFAULT فى جملة دخول نوع CONTAINER OR PROFILE.

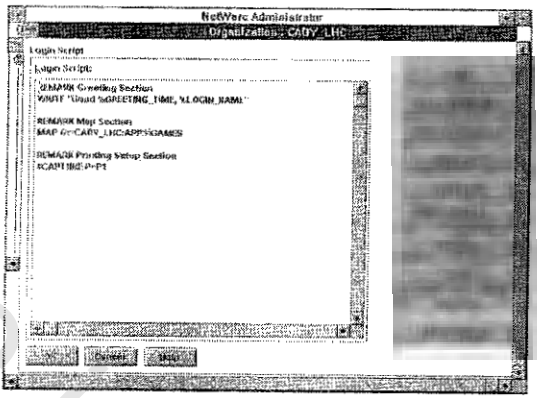
جملة الدخول نوع CONTAINER :

هى أول جملة تعمل عند دخول المستخدم لو وجدت فى USER'S PARENT CONTAINER. تستخدم أساساً لتكوين البيئة العامة للمستخدم وقد تحتوى على أوأمر لأداء المهام التالية:

- بناء تخصيص الشبكة العامة.

- توفير التفاعلات المصاحبة لدخول المستخدم والتى تخفى المستخدمين وحدهم (مثل عمل DRIVES MAPPING وتشغيل القوائم والتطبيقات) .

-إعداد الوصول لملفات وطابعات الشبكة المختلفة.



A sample container login script.

انظر هذه الشاشة

لإنشاء جملة دخول نوع CONTAINER اتبع ما يلى:

1- أدخل على الشبكة كمستخدم له حقوق المراقب SUPERVISOR ثم ابدأ إمكانية NETWARE ADMINIST.

2 - وسع شجرة NDS لعرض الـ CONTAINER حيث تريد إنشاء جملة دخول ثم اختاره

3-اختار DETAILS من قائمة OBJECTS

4 – اختار زر صفحة LOGIN SCRIPT.

5-اكتب أو أمر جملة الدخول.

6- اختار OK

جملة الدخول نوع PROFILE :

يتم تنفيذ هذه الجملة بعد جملة CONTAINER السابق شرحها لو وجـــدت. بالتالى فإنها تستخدم لتوفير نفس أنواع العمليات المشروطة التـــى توفرهـــا جملـــة دخول CONTAINER لمستخدميها (المستخدمين الذين أشياءهم توجد فـــى PARENTS آخر)

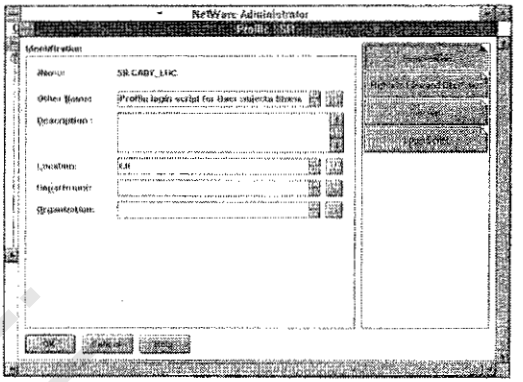
يمكن تجهيز هذا النوع كالمثال التالى:

- MAP NETWORK DRIVE

-ارسال رسائل

-توفير الوصول للطابعات

إن جملة دخول نوع PROFILE هى خاصية لشئPROFILE



The Profile object SR Identification page.

انظر هذه الشاشة

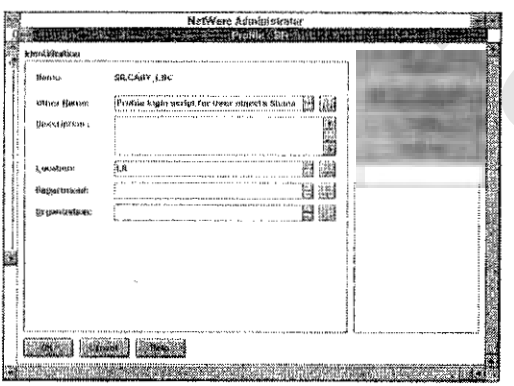
لإنشاء هذا النوع اتبع ما يلى-:

1- أدخل على الشبكة كمستخدم له حقوق المراقب SVPERVISOR ثم إبدأ إمكانيـــة NETWARE ADMINITRATOR

2- وسع شجرة NDS لعرض الـــ CONTAINER حيث تريد إنشاء جملة الدخول

3- اختار CREATE من قائمةOBJECT

4- اكتب اسم جملة دخول PROFILE ثم علم على DEFINE ثمCREATE



The Profile object SR Identification page.

انظر هذه الشاشة

5 -عند فتح صفحة التعريف اختار زر صفحة LOGIN SCRIPT

6- اكتب أوأمر جملة الدخول

7- اختار O.K

جملة الدخول نوع USER :

يجرى تشغيلها بعد جملة CON TAINER و) PROFILE لو مستعملة). لـــو جملة دخول المستخدم وجدت فإن جملة الدخول الـــ DEFAULT لا تشتغل. ولهـــذا فإن جملة دخول المستخدم يجب أن تحتوى على الأقل الـــ MAPPING الرئيســـى للنظام (لو هذا النظام غير متوفر فى واحد من الأنواع الأخرى لجمل الدخول). ما يلى هو استعمالات أخرى لجملة دخول المستخدم:

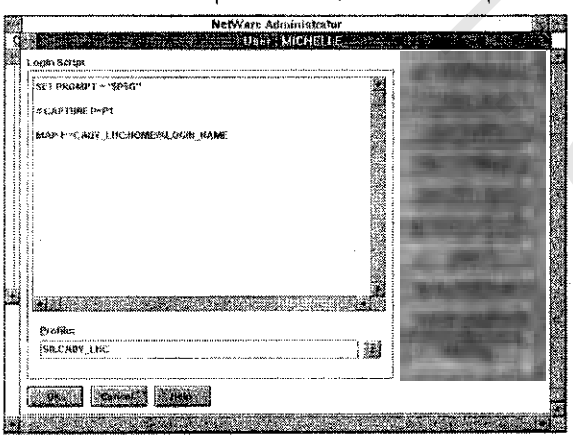
-تشغيل الأوامر المطبقة فقط على هذا المستخدم.

-إعداد التوصيل بالطابعات التى يصل إليها هذا المستخدم

-إرسال ملاحظات للمستخدم أو تذكيره فى أيام معينة من الأسبوع

-وقت دخول المستخدم على الشبكة بدء أى قوائم أو تطبيقـــات مســـتخدمة بهـــذا المستخدم.

إن جملة دخول المستخدم خاصية لشئ المستخدم



The User object MICHELLE login script page.

انظر هذه الشاشة

لإنشاء جملة دخول مستخدم اتبع ما يلى:

1- أدخل على الشبكة كمستخدم له حقوق المراقب SUPERVISOR ثم ابدأ NET.ADMIN.

2- وسع شجرة NDS لعرض شئ المستخدم لمن تريد إنشاء جملة دخول له ثم اختاره

3- اختار DETAILS من قائمة OBJECT

4- اختار زر صفحة جملة الدخول LOGIN SCRIPT

5- اكتب أو أمر جملة الدخول التى تريد وضعها فى جملة الدخول.

ملاحظة :

يمكنك أيضاً تحديد جملة دخول PROFILE لتشغيلها لهذا المستخدم عندما يدخل على الشبكة. اختار حقل PROFILE وأدخل الاسم الكامل لجملة الدخول. لو اخترت تشغيلها لهذا المستخدم فإنها تنفذ قبل جملة دخول المستخدم.

عندما تنشئ جملة دخول لأى نوع يجب أن تستخدم أوامر محددة فى النص المناسب. بالاضافة لذلك يجب إن تنفذ الخطوات التالية:

-أمر واحد فقط يمكن إدخاله فى السطر.

-السطور الفارغة يمكن إدخالها دون أن تؤثر على الجملة.

-عندما تستخدم متغيرات فى أمر ما يجب أن يسبقها العلامة المئوية%

ملاحظة :

المتغير هو جزء يخبر الكمبيوتر لإحلاله بالقيمة المكافئة له. كمثال المتغير LOGIN - NAME% يخبر الكمبيوتر أن يستخدم الاسم الفعلى لدخول المستخدم عوضاً عن هذا الجزء.

- يجب كتابة المتغيرات بالحروف الكبيرة.

NetWare 4.1 Login Script Commands

Command	*Description*	*Example*
#	Executes an external command	#CAPTURE P=P1
CLS	Clears the monitor	CLS
COMSPEC	Tells the PC where to find the COMMAND.COM file	COMSPEC=S3:COMMAND.COM
DISPLAY *file*	Prints a text file to the screen	DISPLAY AUTOEXEC.BAT
DRIVE	Specifies the default drive letter	DRIVE G
EXIT *file*	Ends the login script and runs a file	EXIT TODAY1.BAT
FIRE PHASERS	Causes the computer to beep	FIRE PHASERS 2 times
MAP	Sets a drive mapping or displays current settings	MAP G:=CADY_LHC:APPS
REMARK	Indicates that anything that follows is not to be run	REMARK This login script was last changed on 6/95
WRITE	Displays a message on the screen	WRITE "Remember your daily report!"

☝ انظر الجدول

ثانياً : إنشاء القوائم CREATING MENUS

عند دخول المستخدم على الشبكة يمكنك تبسيط وصوله للموارد بتوفير قائمة من بنود يختار من خلالها ما يريد . عامة إذا المستخدم دائماً يصل لإمكانية واحدة ونادراً ما يصل لأية موارد أخرى فإن القائمة تكون غير ضرورية. إذا كان على المستخدم إن يصل إلى ثلاثة برامج تطبيقات مختلفة كمثال فإن القائمة تصبح مفيدة جداً. لتمكين المستخدم من الوصول لقائمة يمكنك استخدام أمر EXIT فى جملة دخول المستخدم وتكتب بعد اسم القائمة. قبل أن يستطيع المستخدم الوصول للقائمة يجب أن يتم إنشاؤها . ولإنشاءها اكتب أوأمر القائمة فى ملف. استخدم أى معالج نصوص للدوس احفظه بنوع .SRC كمثال لو أردت إنشاء ملف قائمة لمجموعة من المستخدمين للوصول لتطبيقات مختلفة فى إدراة AB فقم بتسميته.AB . SRC

بعد إنشاء ملف المنبع SOURCE الاساسى قم بترجمته COMPILE فينتج ملف قائمة بنوع . DAT هذا الملف يمكن تشغيله بعد ذلك لوصول المستخدم لترجمة COMPILE ملف منبع SOURCE إستخدم أمر MENUMAKE متبوعاً بإسم ملف المنبع.SOURCE

كمثال لترجمة ملف AB . SRC اكتب MENUMAKE AB

إذا نجحت جهودك فإن النتيجة تكون ملف قائمة باسم MENUMAKE . DAT

ملاحظة :

إذا اخترت اسم نوع للملف غير SRC حدد اسم الملف باسم التمديد عندما تعمل ترجمة له.

إذا لم تنجح عملية الترجمة فربما تكون هناك أخطاء فى أوامر ملف المنبع للقائمة (الأوامر التى تحدد أشياء معينة مثل شكل القائمة وكيفية معالجة المعلومات وتنفيذ الأوامر). لإجراء الترجمة بنجاح يجب أن تصحح الأخطاء. لتصحيح الأخطاء تحتاج لفهم ليس الأوامر فقط لكن متطلبات الأوامر أيضاً.

ملف المنبع لقائمة نتوير يمكن أن تحتوى نوعين فقط من أوامر ملف جملة القائمة:

ORGANIZATIONAL - CONTROL

ORGANIZATIONAL : تحدد كيف تظهر القائمة على الشاشة. ما يلى هما أمرين لها

ITEM - MENU

CONTROL : يحدد أى الأوامر يتم تنفيذها وكيف تعالج المعلومات المتوفرة. توجد أربعة أوامر تحكم CONTROL أساسية إحداها له ثلاثة استخدامات تبادلية. ما يلى أربعة أوامر تحكم EXEC - LOAD - SHOW - GETX :

ملاحظة :

يجب كتابة أوامر ملف المنبع للقائمة بالحروف الكبيرة

بالاضافة للأوامر فإن ملف المنبع للقائمة يحتوى على اختيارات يمكن إستخدامها مع كل أمر كمثال عندما تستخدم أمر ITEM يمكنك أيضاً استخدام الإختيار المصاحب له . BATCH بذلك تتمكن من إزالة القوائم المقيمة فى ذاكرة محطة العمل وتحرير مساهمة حرة للبرامج والملفات الأخرى.

NetWare 4.1 Menu Commands and Options

Command	*Command Description and Format*	*Options and Descriptions*
MENU	Specifies start of each menu screen, along with number and name of menu **Format:** `MENU menu_number, menu_name`	No options available
ITEM	Defines menu options **Format:** `ITEM item_name {options}`	BATCH—removes menu from memory CHDIR—returns to default directory after a menu option is chosen PAUSE—displays "Press any key to continue" message and pauses until a key is pressed SHOW—displays name of a DOS command being run when one has been requested
EXEC	Runs a specified command **Format:** `EXEC {option}`	EXIT—closes menu and exits to the DOS prompt DOS—shells out to DOS requiring the user to type **EXIT** to return to the menu. LOGOUT—closes menu and logs user out of network, returning user to DOS prompt
LOAD	Runs another menu from within this menu, when the other menu was created as a separate menu file **Format:** `LOAD menu_name.DAT`	No options available
SHOW	Runs submenus created as part of this menu; can be used to display up to 255 submenus **Format:** `SHOW menu_number`	No options available
GET*X*	Prompts for user input. If *X* is replaced with the letter O, input is *optional*. If *X* is replaced with the letter R, input is *required* before additional processing can be done. If *X* is replaced with the letter P, input provided by the user is stored for later use. **Format:** `GETX instruction{prepend} length,prefill{append}`	No options available

☜ انظر الجدول

ملاحظة :

عند استخدام GETX فإن المستخدم يضغط F_{10} قبل استمرار العملية.

بالإضافة فإن الطرق الآتية تطبق لاستخدام GETX فى القوائم:

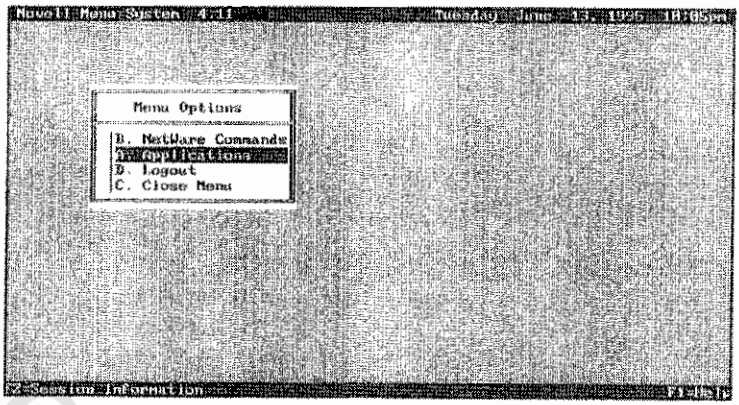
- GETX يجب إن يوضع بين أمر ITEM وأى EXEC أمر معه
- قد لا تستخدم أكثر من مائة أمر GETX لكل ITEM
- يمكنك توجيه المستخدم لألايتجأوب مع أكثر من ١٠ صناديق حوار أو يمكنك استخدام علامة (٨) لوضع كل توجيه فى صندوق الحوار الخاص به
- كل توجيه يجب أن يكون فى سطر منفصل فى ملف القائمة.

مثال لملف قائمة اسمها: TEST

```
NENU 01, MENU OPTIONS
ITEM ^ BNETWARE COMMANDS
SHOW 10
ITEM ^ AAPPLICATIONS
SHOW 2O
ITEM ^ DLOGOUT
EXEC LOGOUT
ITEM ^ CCLOSE MENU
EXEC EXIT
MENU 10 , NETWARE COMMANDS
ITEM NLIST
GETO CLASS NAME AND OPTION : { } 25 ,, { }
EXEC NLIST
ITEM DIR {PAUES}
GETO DRIVE LETTER : { } 25 ,, { }
EXEC NLIST
ITEM DIR {PAUSE}
GETO DRIVE LETTER :{ } 25,,{ }
EXEL DIR
MENV 20 , APPLICATIONS
ITEM WORD PROCESSOR
EXEC C:\WP\WP. EXE
ITEM SCREEN SHOTS
EXEC C:\COLLAGE\SNAP C:\BOOKS
```

بعد تشغيل إمكانية MENUMAKE لترجمة ملف المنبع SOURCE فإن ملف القائمة (المثال المذكور) TEST . DAT سوف ينشأ.

يستطيع المستخدم تشغيل هذه القائمة فيما بعد بكتابة NMENU متبوعاً بإسمها. كمثال NMENU TEST . DAT



Menu displayed from running the TEST.DAT file.

انظر هذه الشاشة ☝

ملاحظة :

يجب أن تكون للمستخدم حقوق READ و FILE SCAN علـــى الفهـــرس المحتوى على ملف القائمة وعلى حقوق READ , WRITE , FILE SCAN علـــى فهرس المستخدم.