Beyond File Permissions: Controlling User Actions

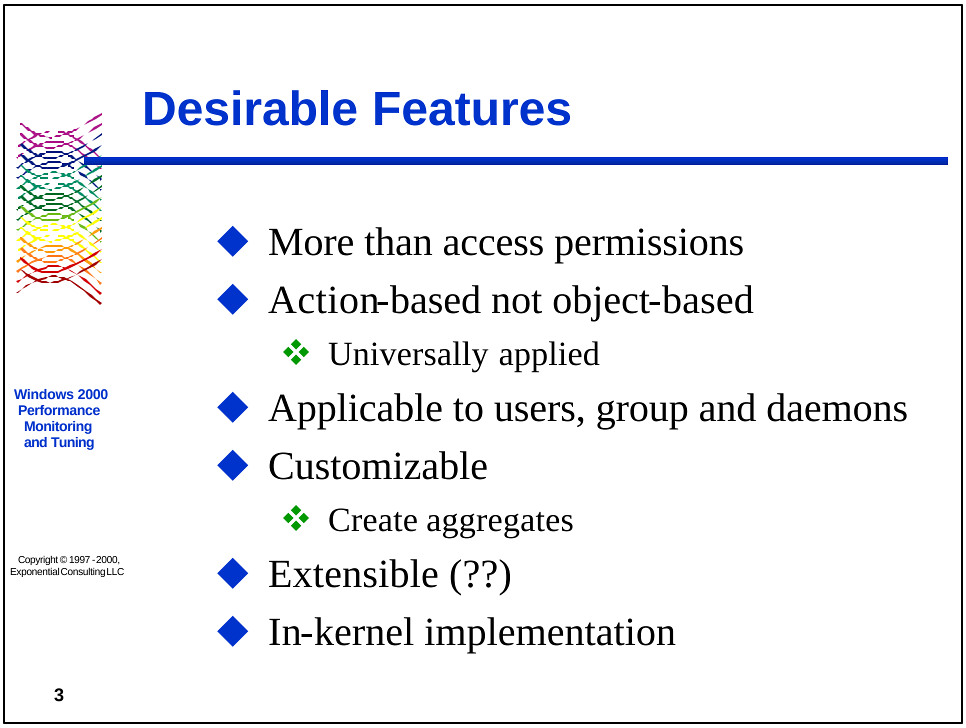
Æleen Frisch
aefrisch@lorentzian.com
www.aeleen.com

e**^{x}ponential Consulting, LLC**
North Haven, Connecticut, USA

“New” Approach?

- W(indows) NT--

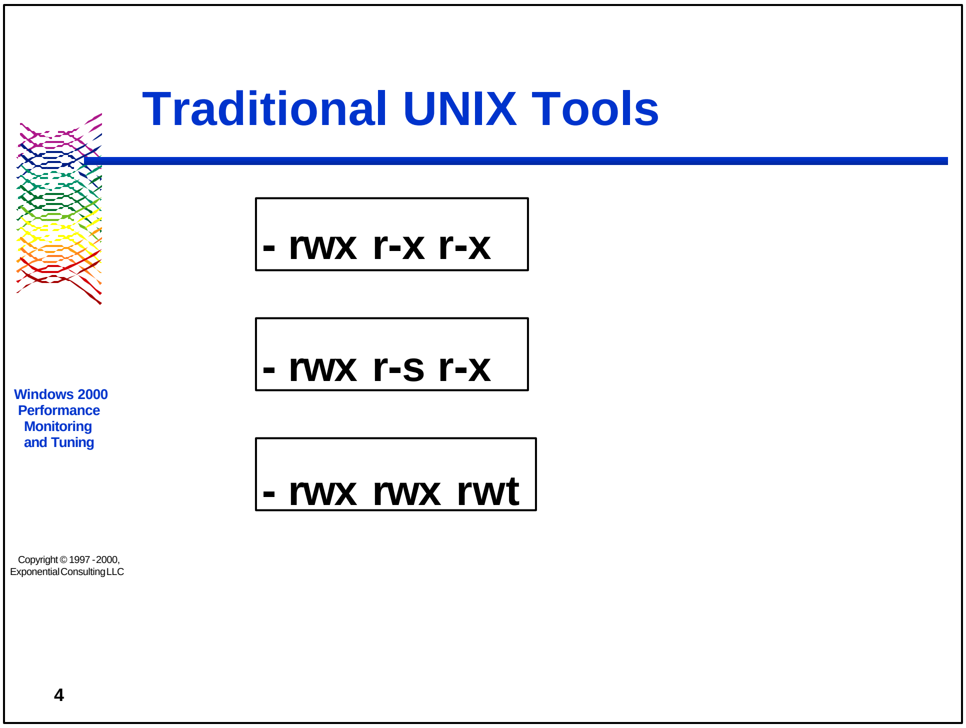
Windows 2000
Performance
Monitoring
and Tuning



Desirable Features

- More than access permissions
- Action-based not object-based
  - Universally applied
- Applicable to users, group and daemons
- Customizable
  - Create aggregates
- Extensible (??)
- In-kernel implementation

Windows 2000
Performance
Monitoring
and Tuning



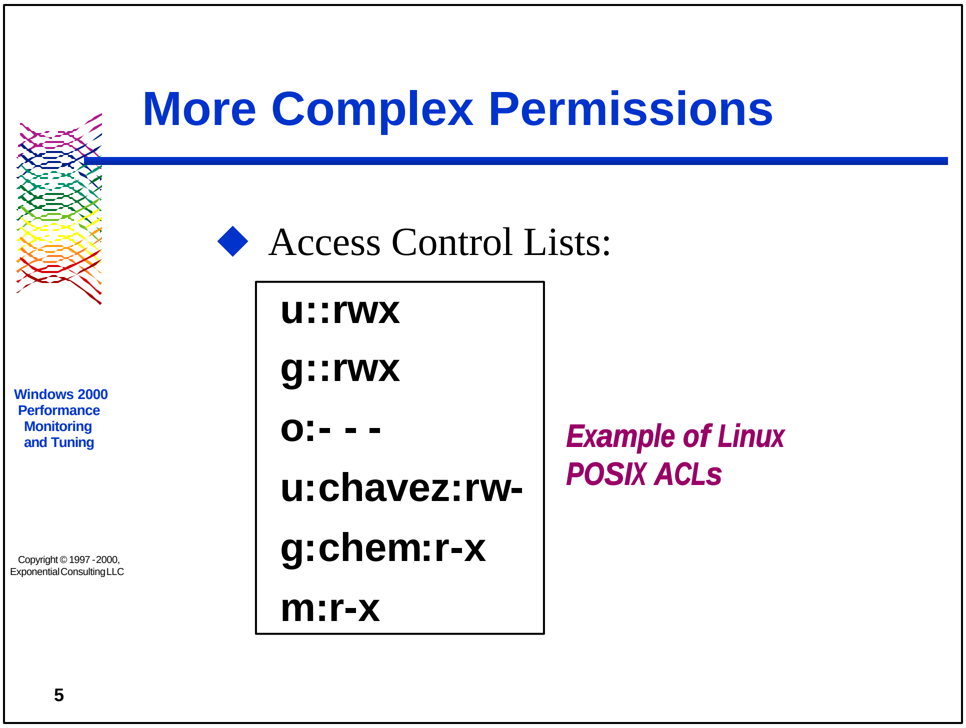
Traditional UNIX Tools

```
- rwx r-x r-x
```

```
- rwx r-s r-x
```

```
- rwx rwx rwt
```

Windows 2000
Performance
Monitoring
and Tuning



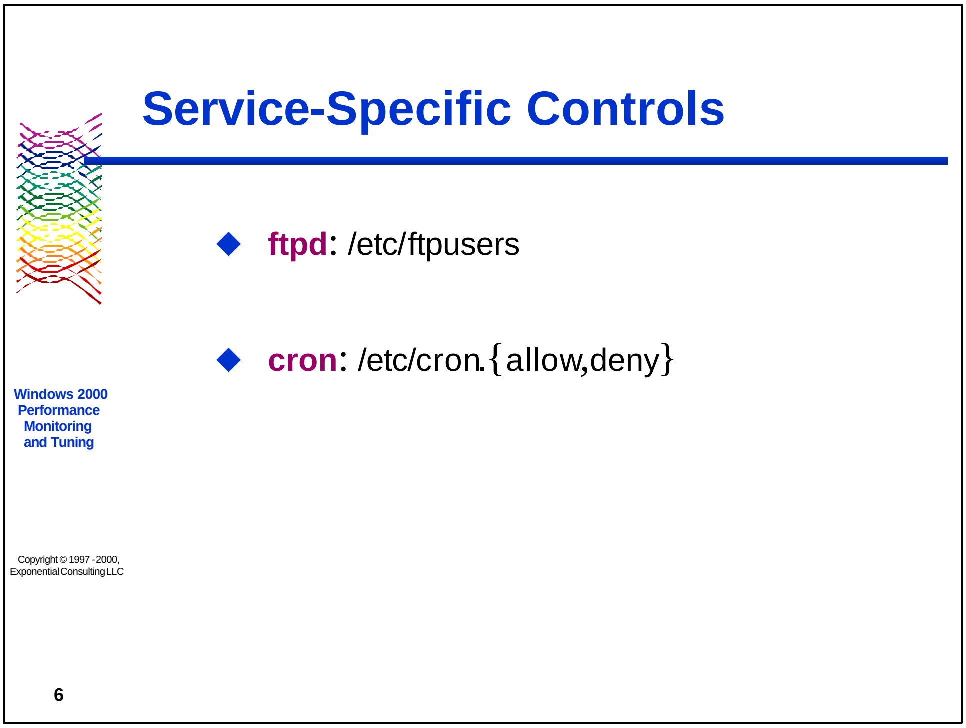
More Complex Permissions

- Access Control Lists:

```
u::rwx
g::rwx
o:- - -
u:chavez:rw-
g:chem:r-x
m:r-x
```

Example of Linux POSIX ACLs

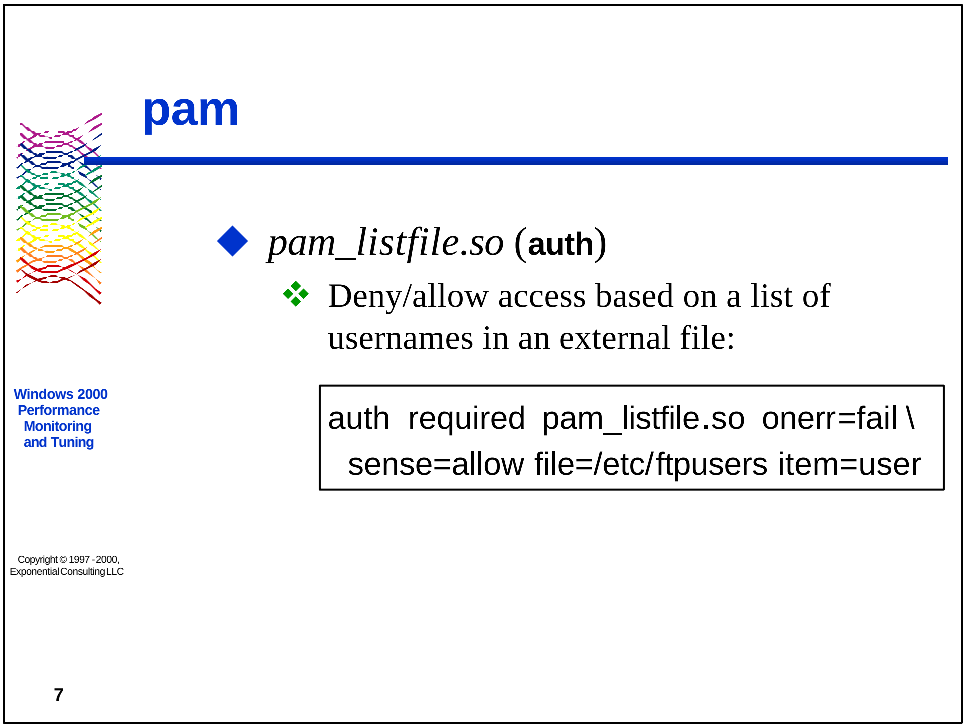
Windows 2000
Performance
Monitoring
and Tuning



Service-Specific Controls

- **ftpd**: /etc/ftpusers
- **cron**: /etc/cron.{allow,deny}

Windows 2000
Performance
Monitoring
and Tuning



pam

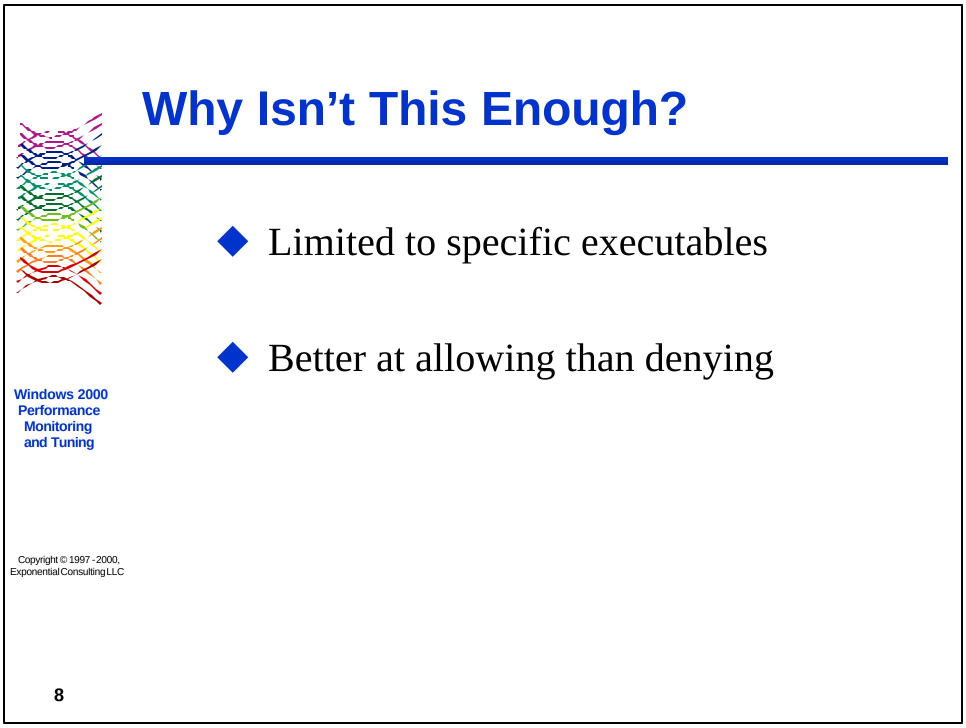
- *pam_listfile.so* (**auth**)
  - Deny/allow access based on a list of usernames in an external file:

```
auth  required  pam_listfile.so  onerr=fail \
  sense=allow file=/etc/ftpusers item=user
```

Windows 2000
Performance
Monitoring
and Tuning

Copyright © 1997 -2000,
Exponential Consulting LLC

7



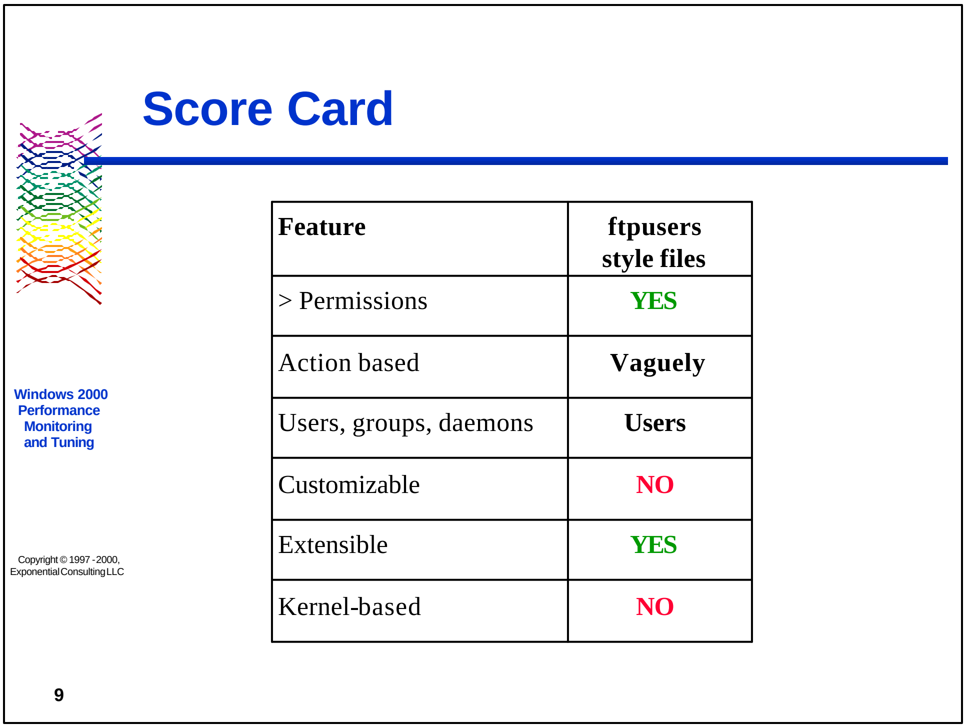
Why Isn’t This Enough?

- Limited to specific executables
- Better at allowing than denying

Windows 2000
Performance
Monitoring
and Tuning

Copyright © 1997 -2000,
Exponential Consulting LLC

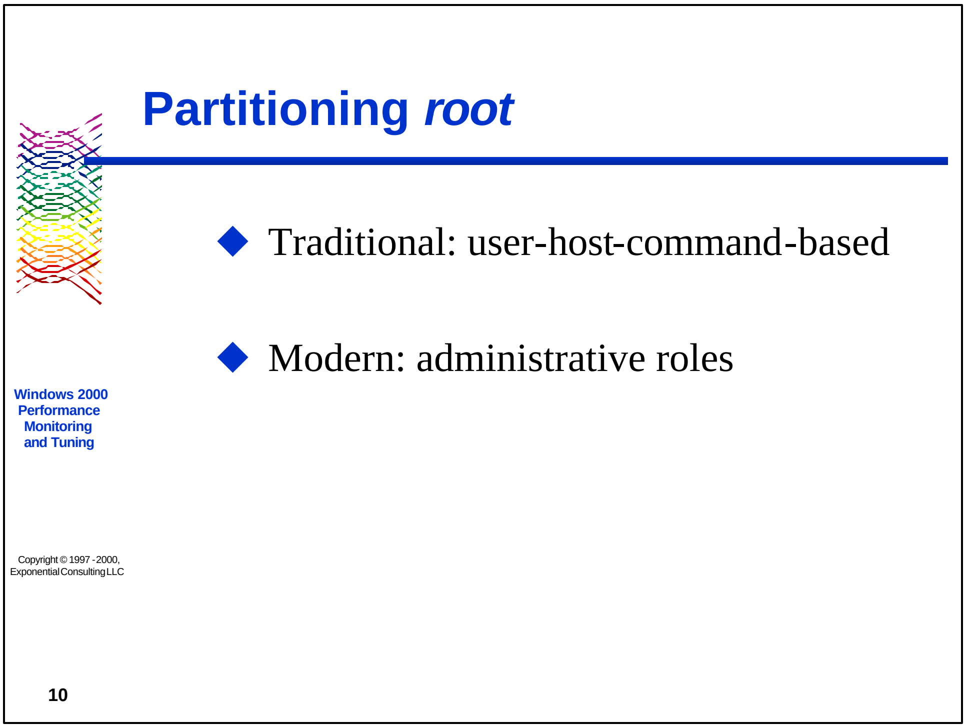
8



Score Card

Feature	ftpusers style files
> Permissions	**YES**
Action based	**Vaguely**
Users, groups, daemons	**Users**
Customizable	**NO**
Extensible	**YES**
Kernel-based	**NO**

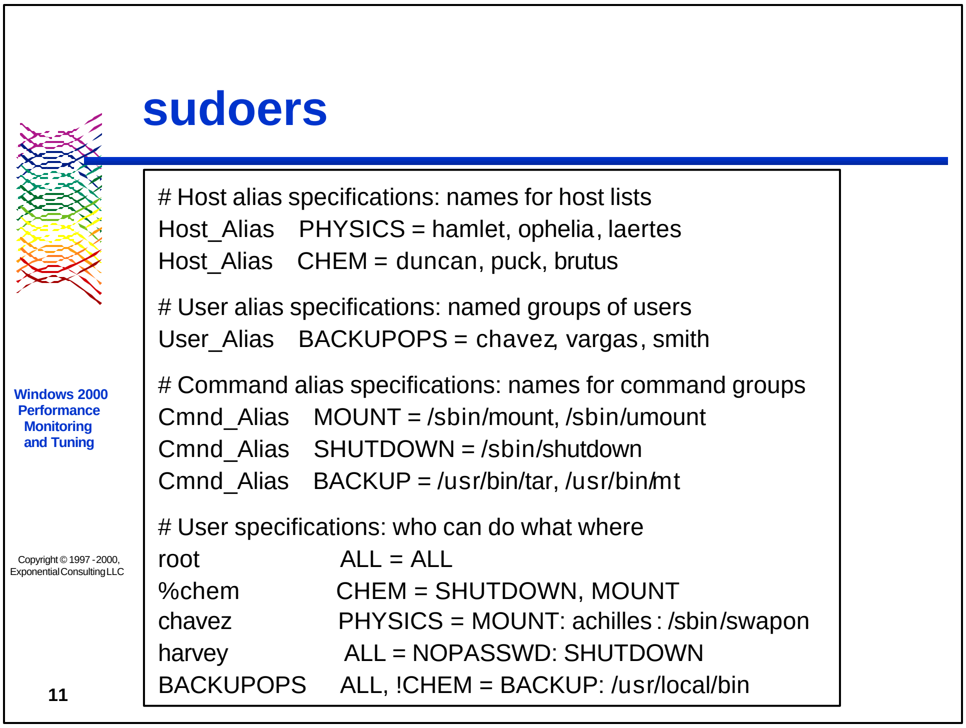
Windows 2000
Performance
Monitoring
and Tuning



Partitioning *root*

- Traditional: user-host-command-based
- Modern: administrative roles

Windows 2000
Performance
Monitoring
and Tuning

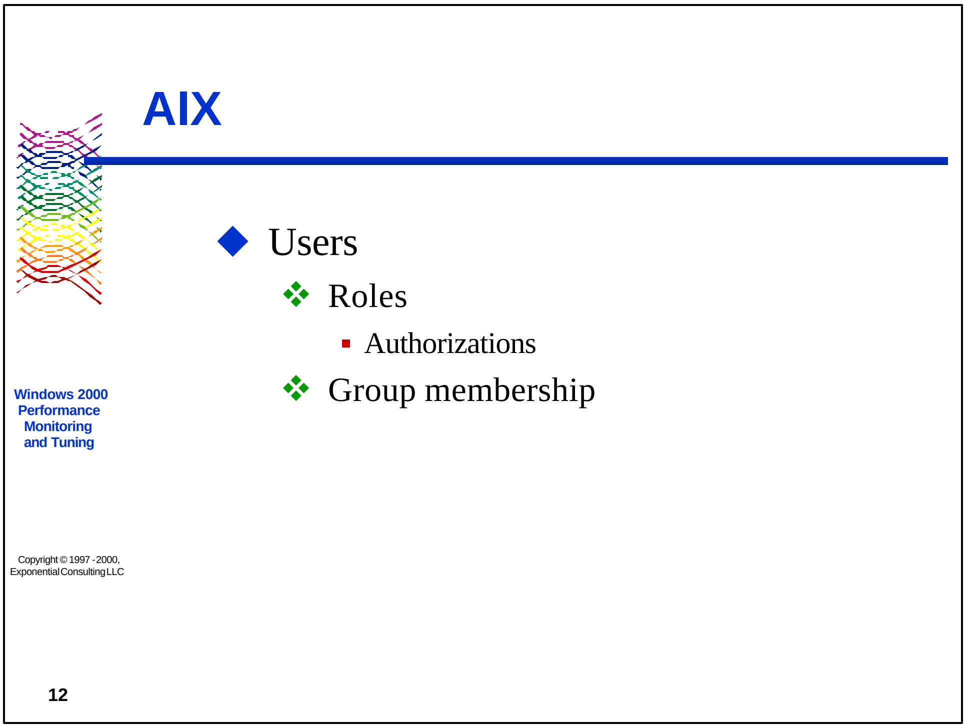


sudoers

```
# Host alias specifications: names for host lists
Host_Alias    PHYSICS = hamlet, ophelia, laertes
Host_Alias    CHEM = duncan, puck, brutus

# User alias specifications: named groups of users
User_Alias    BACKUPOPS = chavez, vargas, smith

# Command alias specifications: names for command groups
Cmnd_Alias    MOUNT = /sbin/mount, /sbin/umount
Cmnd_Alias    SHUTDOWN = /sbin/shutdown
Cmnd_Alias    BACKUP = /usr/bin/tar, /usr/bin/mt

# User specifications: who can do what where
root              ALL = ALL
%chem             CHEM = SHUTDOWN, MOUNT
chavez            PHYSICS = MOUNT: achilles : /sbin/swapon
harvey            ALL = NOPASSWD: SHUTDOWN
BACKUPOPS         ALL, !CHEM = BACKUP: /usr/local/bin
```

Windows 2000 Performance Monitoring and Tuning

11

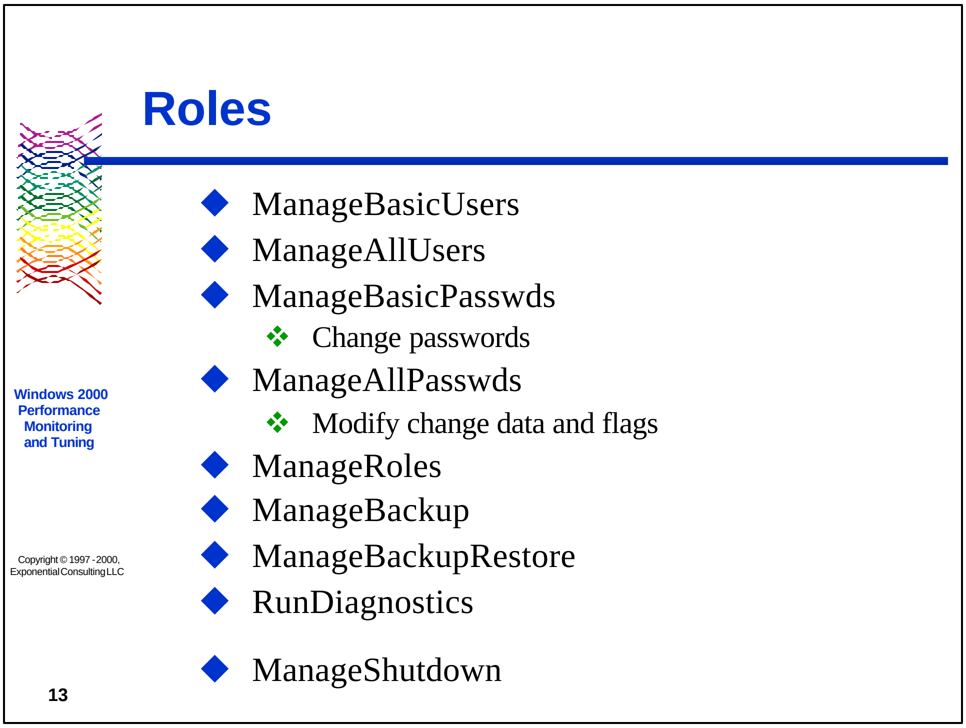


AIX

- Users
  - Roles
    - Authorizations
  - Group membership

Windows 2000 Performance Monitoring and Tuning

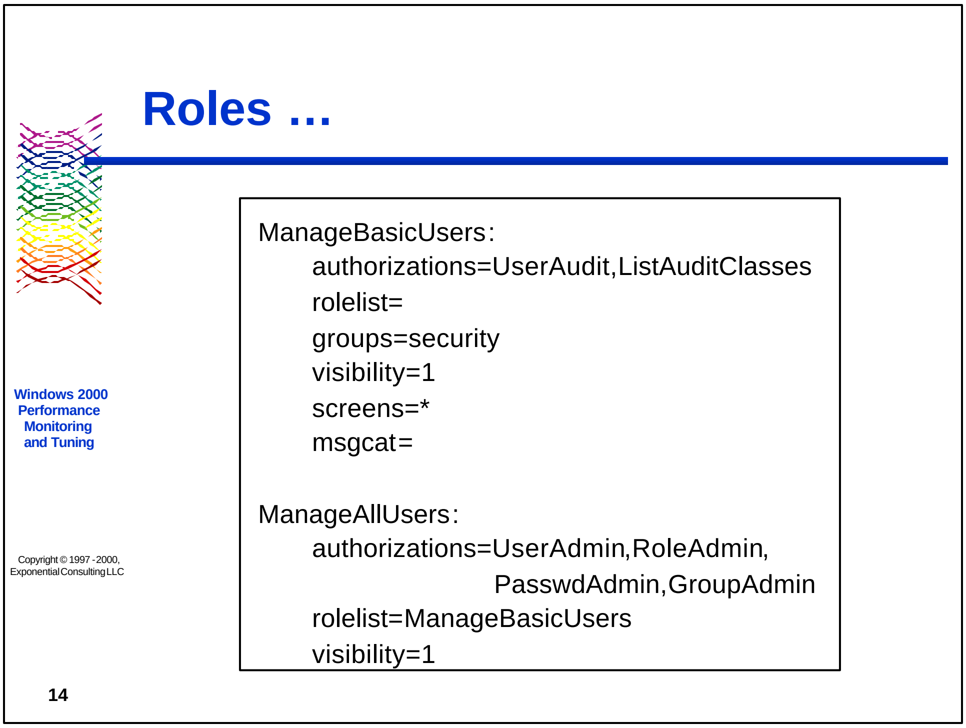
12



Roles

- ManageBasicUsers
- ManageAllUsers
- ManageBasicPasswds
  - Change passwords
- ManageAllPasswds
  - Modify change data and flags
- ManageRoles
- ManageBackup
- ManageBackupRestore
- RunDiagnostics
- ManageShutdown

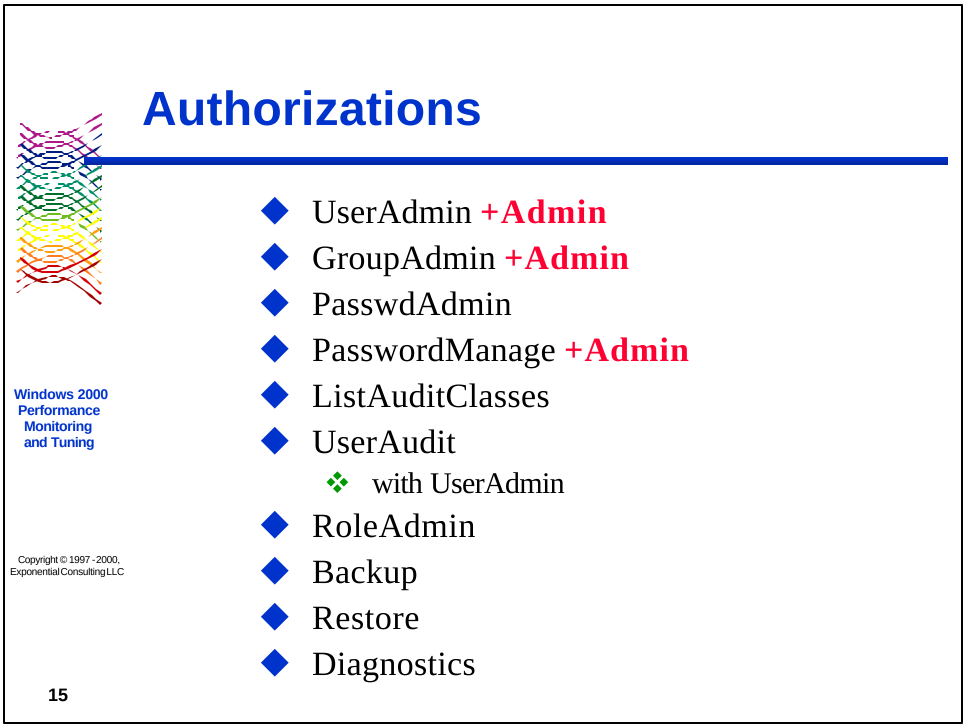
Windows 2000
Performance
Monitoring
and Tuning



Roles …

```
ManageBasicUsers:
      authorizations=UserAudit,ListAuditClasses
      rolelist=
      groups=security
      visibility=1
      screens=*
      msgcat=

ManageAllUsers:
      authorizations=UserAdmin,RoleAdmin,
                          PasswdAdmin,GroupAdmin
      rolelist=ManageBasicUsers
      visibility=1
```

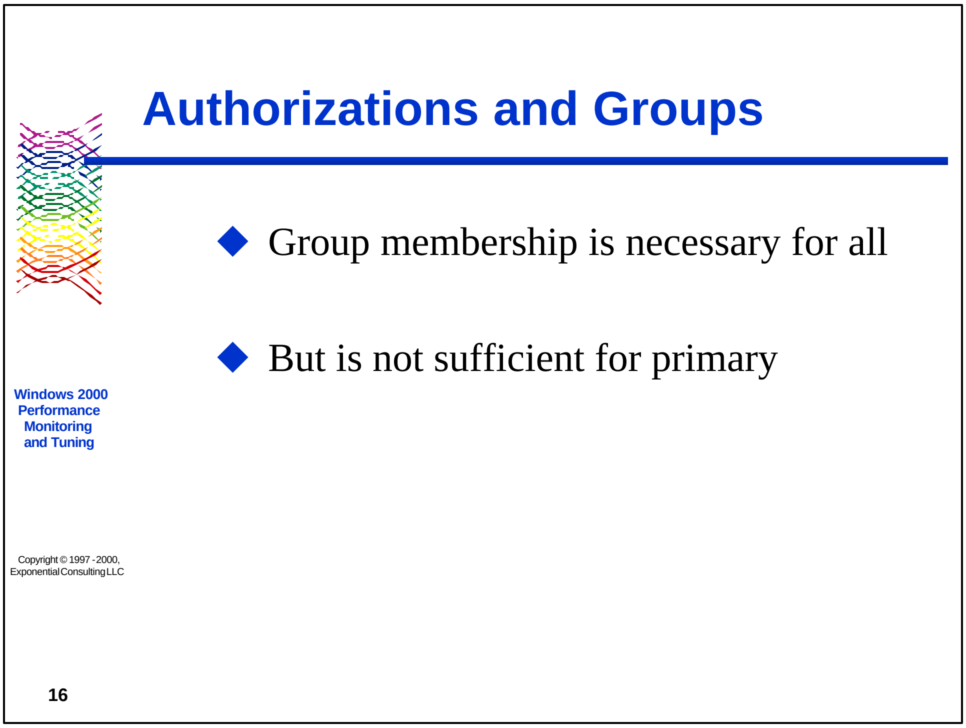
Windows 2000
Performance
Monitoring
and Tuning



Authorizations

- UserAdmin **+Admin**
- GroupAdmin **+Admin**
- PasswdAdmin
- PasswordManage **+Admin**
- ListAuditClasses
- UserAudit
  - with UserAdmin
- RoleAdmin
- Backup
- Restore
- Diagnostics

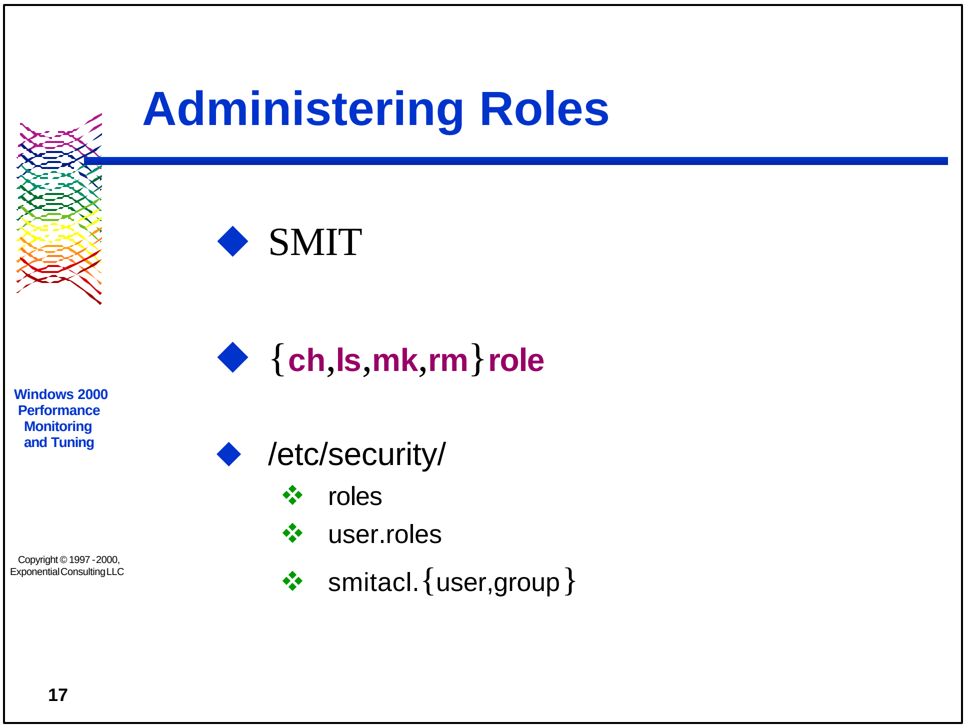
Windows 2000 Performance Monitoring and Tuning



Authorizations and Groups

- Group membership is necessary for all
- But is not sufficient for primary

Windows 2000 Performance Monitoring and Tuning

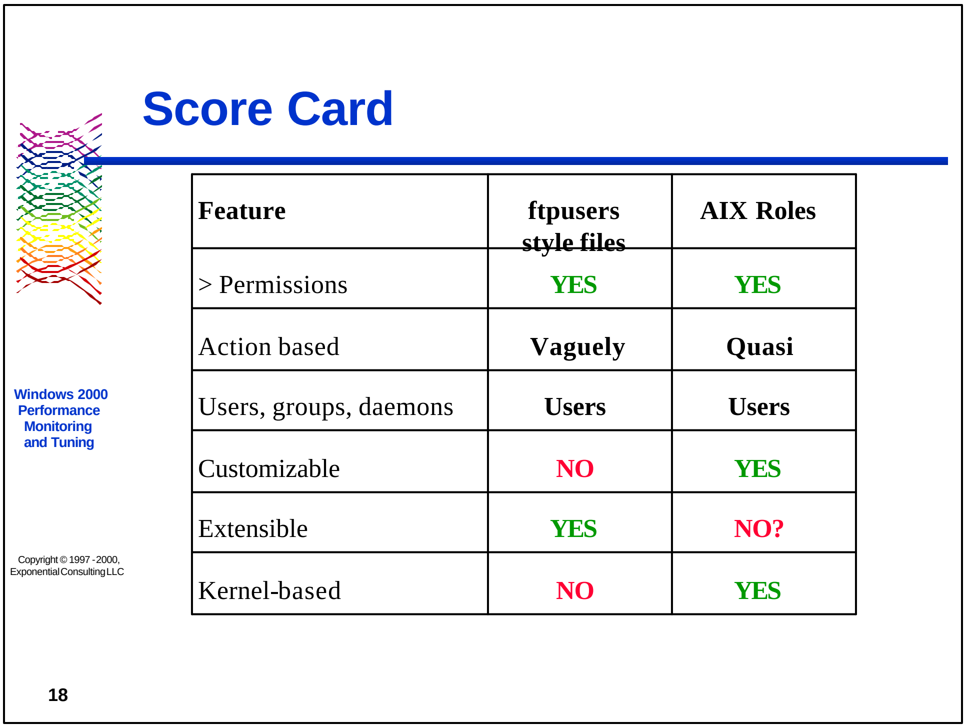


Administering Roles

- SMIT
- {ch,ls,mk,rm}role
- /etc/security/
  - roles
  - user.roles
  - smitacl.{user,group}

Windows 2000
Performance
Monitoring
and Tuning

17

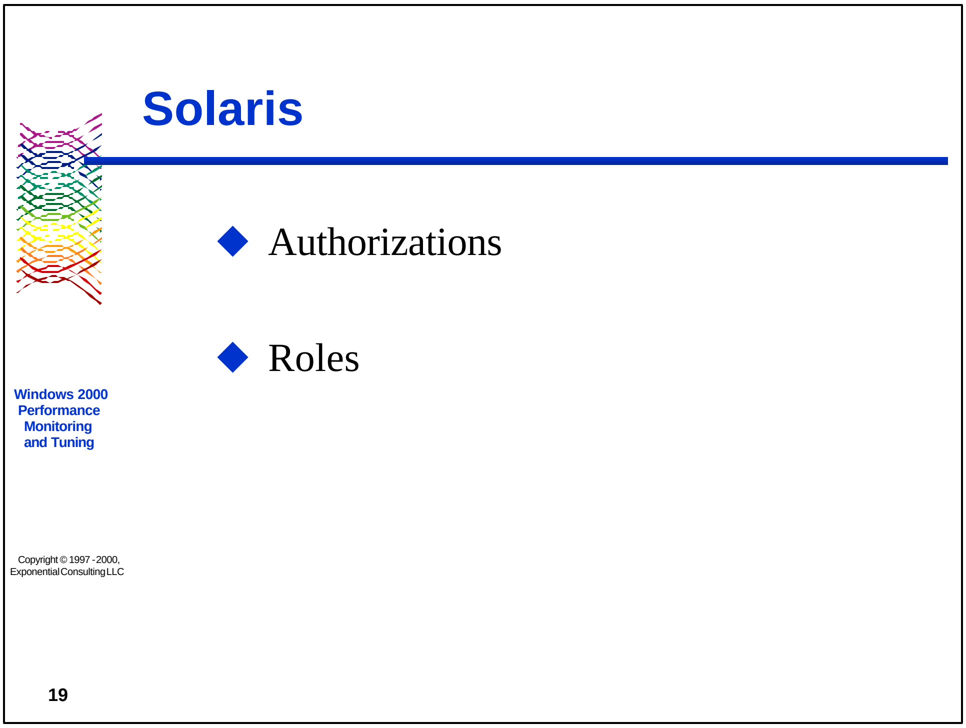


Score Card

Feature	ftpusers style files	AIX Roles
> Permissions	YES	YES
Action based	Vaguely	Quasi
Users, groups, daemons	Users	Users
Customizable	NO	YES
Extensible	YES	NO?
Kernel-based	NO	YES

Windows 2000
Performance
Monitoring
and Tuning

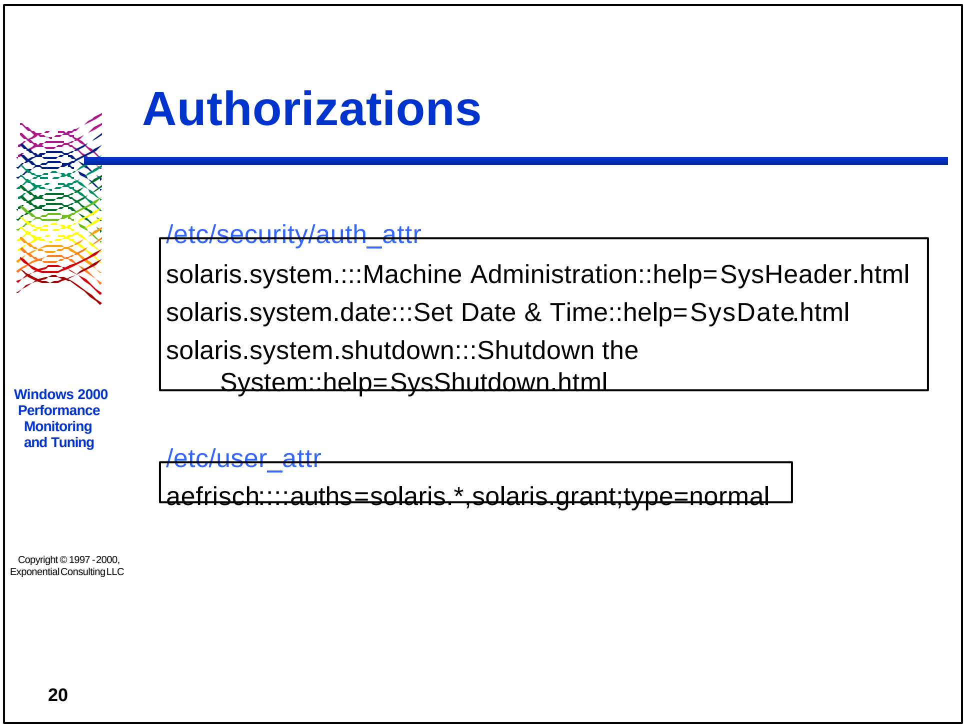
18



Solaris

- Authorizations
- Roles

Windows 2000
Performance
Monitoring
and Tuning



Authorizations

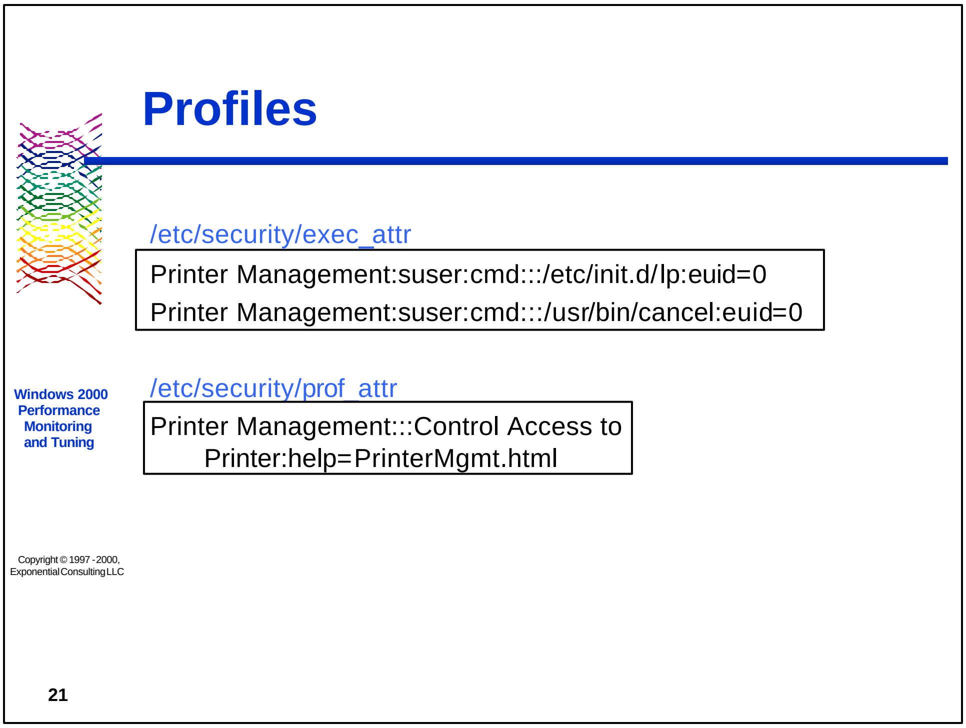
/etc/security/auth_attr

```
solaris.system.:::Machine Administration::help=SysHeader.html
solaris.system.date:::Set Date & Time::help=SysDate.html
solaris.system.shutdown:::Shutdown the
        System::help=SysShutdown.html
```

/etc/user_attr

```
aefrisch::::auths=solaris.*,solaris.grant;type=normal
```

Windows 2000
Performance
Monitoring
and Tuning



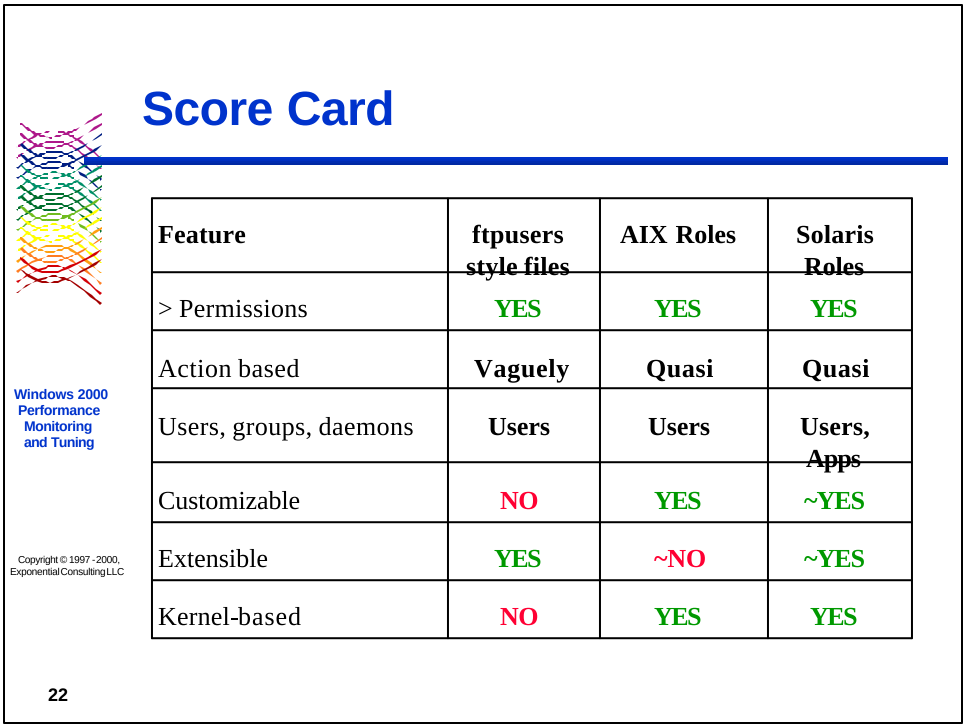
Profiles

/etc/security/exec_attr

```
Printer Management:suser:cmd:::/etc/init.d/lp:euid=0
Printer Management:suser:cmd:::/usr/bin/cancel:euid=0
```

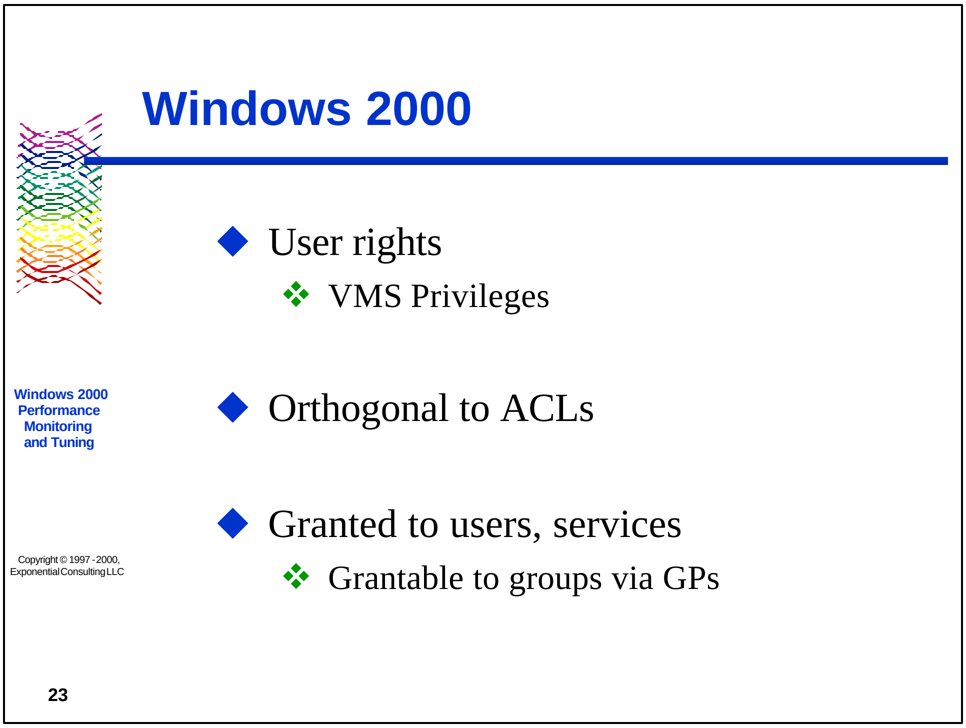
/etc/security/prof_attr

```
Printer Management:::Control Access to
    Printer:help=PrinterMgmt.html
```



Score Card

Feature	ftpusers style files	AIX Roles	Solaris Roles
> Permissions	YES	YES	YES
Action based	Vaguely	Quasi	Quasi
Users, groups, daemons	Users	Users	Users, Apps
Customizable	NO	YES	~YES
Extensible	YES	~NO	~YES
Kernel-based	NO	YES	YES



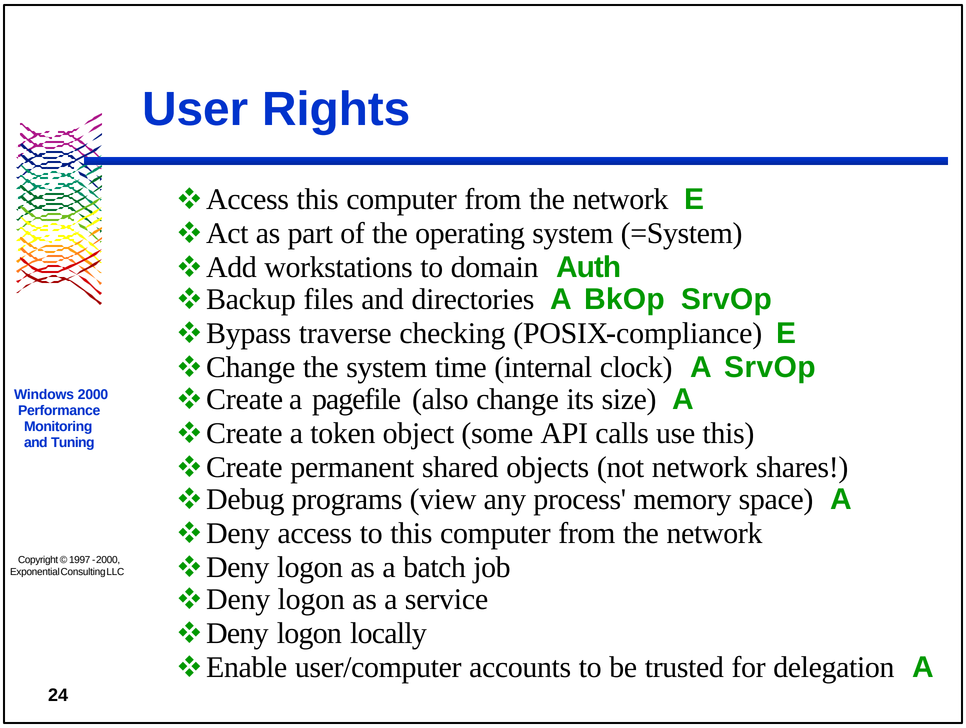
Windows 2000
Performance
Monitoring
and Tuning

Copyright © 1997 - 2000,
Exponential Consulting LLC

Windows 2000

- User rights
  - VMS Privileges
- Orthogonal to ACLs
- Granted to users, services
  - Grantable to groups via GPs

23



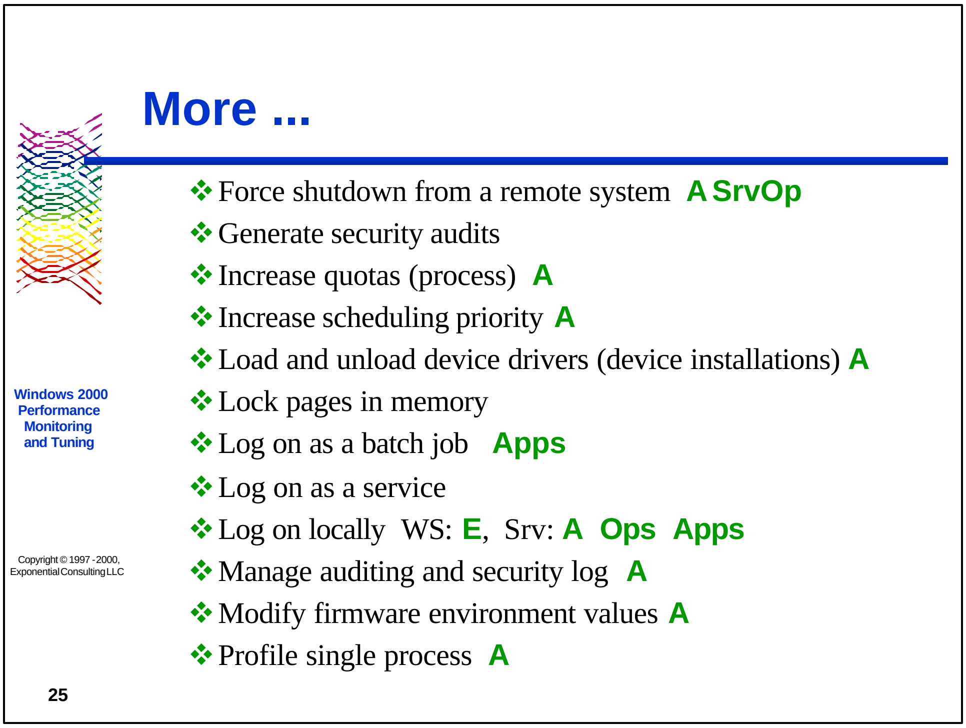
Windows 2000
Performance
Monitoring
and Tuning

Copyright © 1997 - 2000,
Exponential Consulting LLC

User Rights

- Access this computer from the network **E**
- Act as part of the operating system (=System)
- Add workstations to domain **Auth**
- Backup files and directories **A BkOp SrvOp**
- Bypass traverse checking (POSIX-compliance) **E**
- Change the system time (internal clock) **A SrvOp**
- Create a pagefile (also change its size) **A**
- Create a token object (some API calls use this)
- Create permanent shared objects (not network shares!)
- Debug programs (view any process' memory space) **A**
- Deny access to this computer from the network
- Deny logon as a batch job
- Deny logon as a service
- Deny logon locally
- Enable user/computer accounts to be trusted for delegation **A**

24

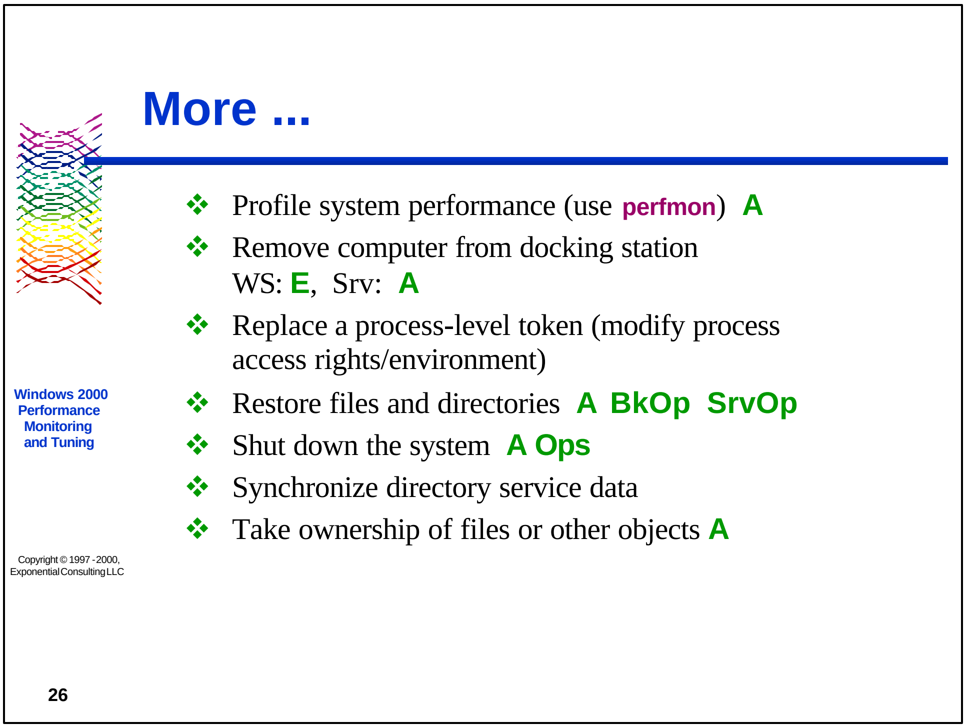


More ...

- Force shutdown from a remote system **A SrvOp**
- Generate security audits
- Increase quotas (process) **A**
- Increase scheduling priority **A**
- Load and unload device drivers (device installations) **A**
- Lock pages in memory
- Log on as a batch job **Apps**
- Log on as a service
- Log on locally WS: **E**, Srv: **A Ops Apps**
- Manage auditing and security log **A**
- Modify firmware environment values **A**
- Profile single process **A**

Windows 2000
Performance
Monitoring
and Tuning

25

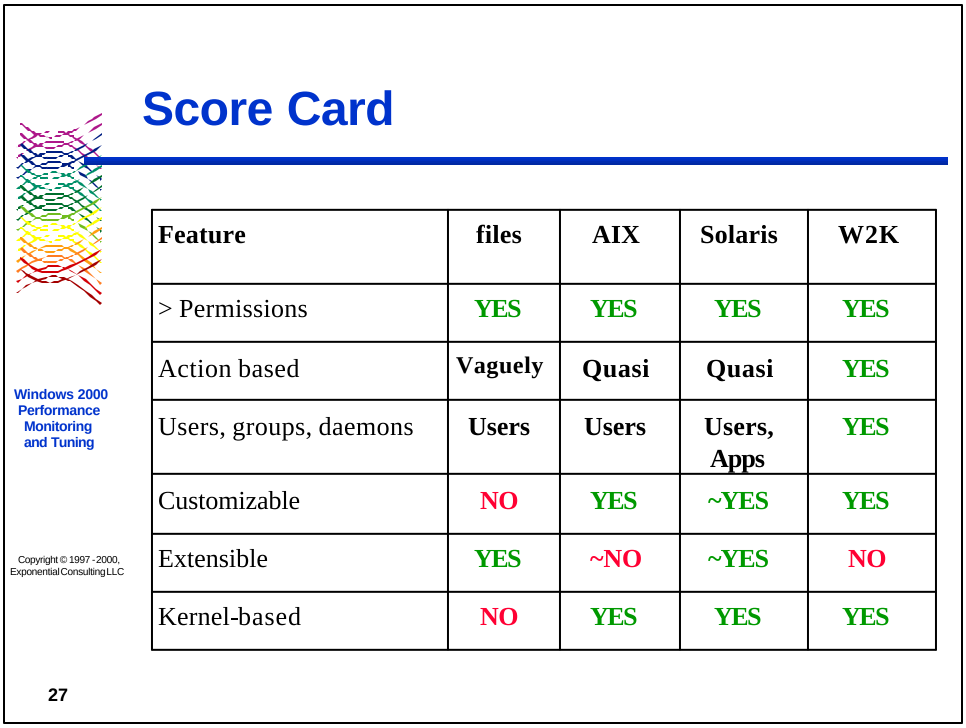


More ...

- Profile system performance (use **perfmon**) **A**
- Remove computer from docking station
  WS: **E**, Srv: **A**
- Replace a process-level token (modify process access rights/environment)
- Restore files and directories **A BkOp SrvOp**
- Shut down the system **A Ops**
- Synchronize directory service data
- Take ownership of files or other objects **A**

Windows 2000
Performance
Monitoring
and Tuning

26

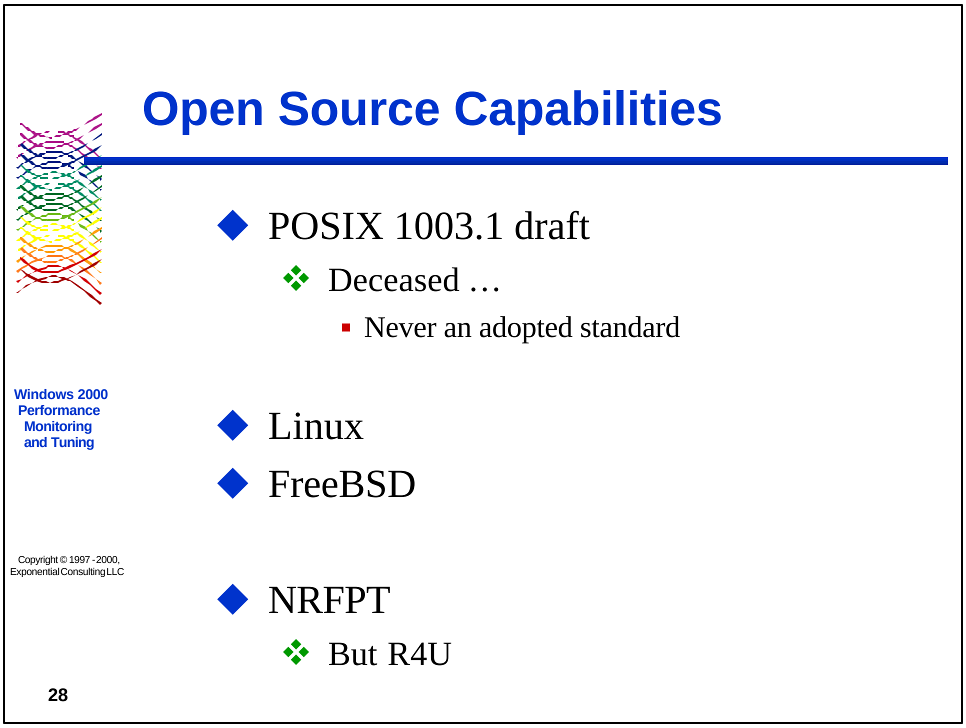


Score Card

Feature	files	AIX	Solaris	W2K
> Permissions	YES	YES	YES	YES
Action based	Vaguely	Quasi	Quasi	YES
Users, groups, daemons	Users	Users	Users, Apps	YES
Customizable	NO	YES	~YES	YES
Extensible	YES	~NO	~YES	NO
Kernel-based	NO	YES	YES	YES

Windows 2000 Performance Monitoring and Tuning

27

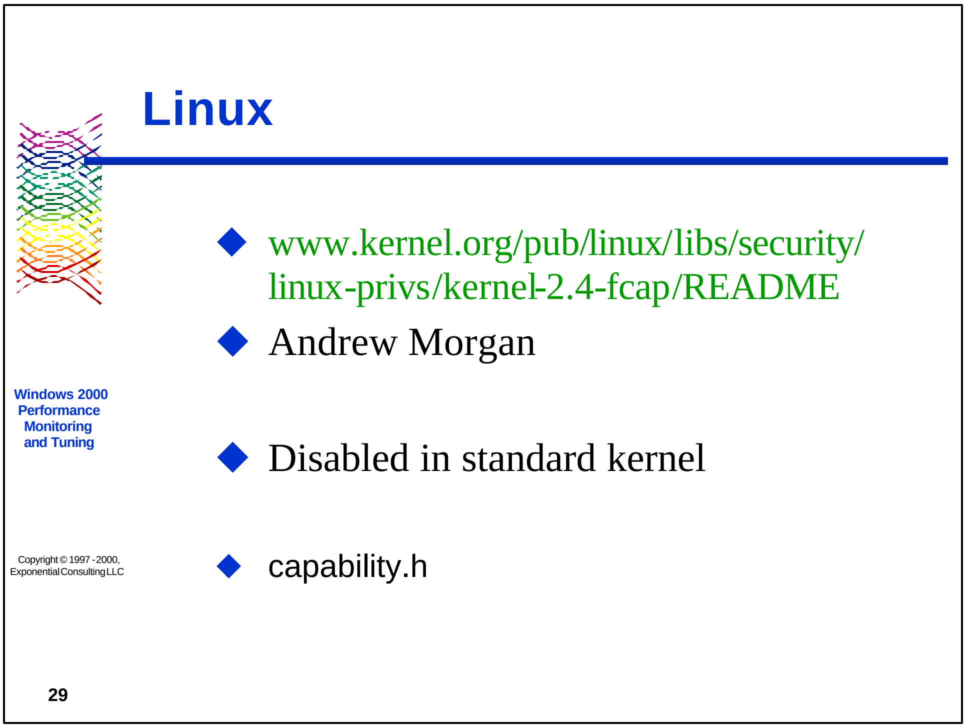


Open Source Capabilities

- POSIX 1003.1 draft
  - Deceased …
    - Never an adopted standard
- Linux
- FreeBSD
- NRFPT
  - But R4U

Windows 2000 Performance Monitoring and Tuning

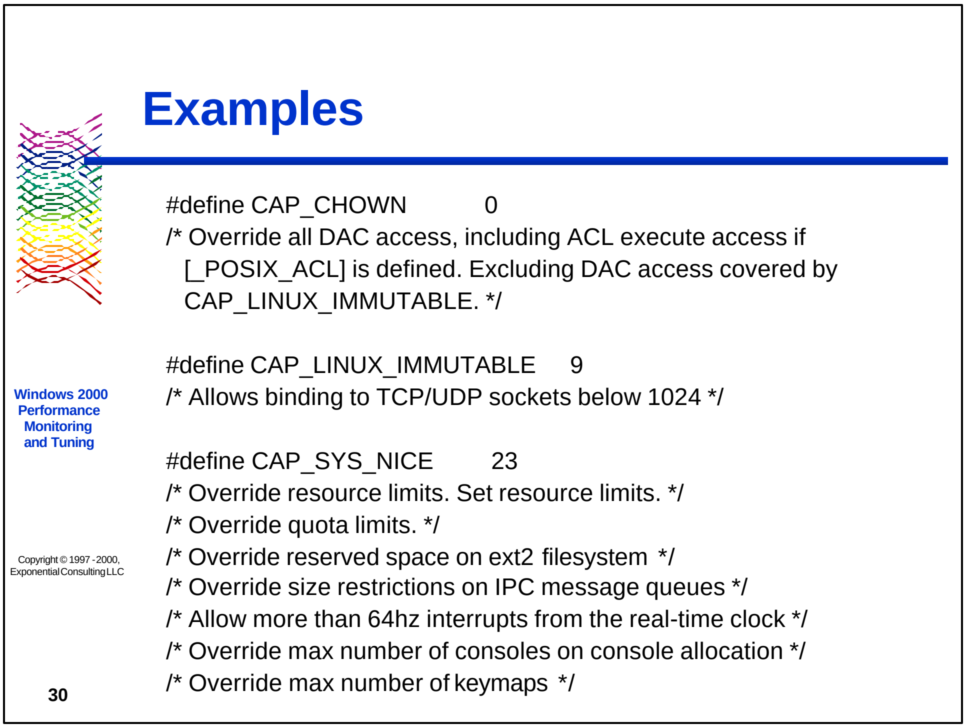
28



Linux

- www.kernel.org/pub/linux/libs/security/linux-privs/kernel-2.4-fcap/README
- Andrew Morgan
- Disabled in standard kernel
- capability.h

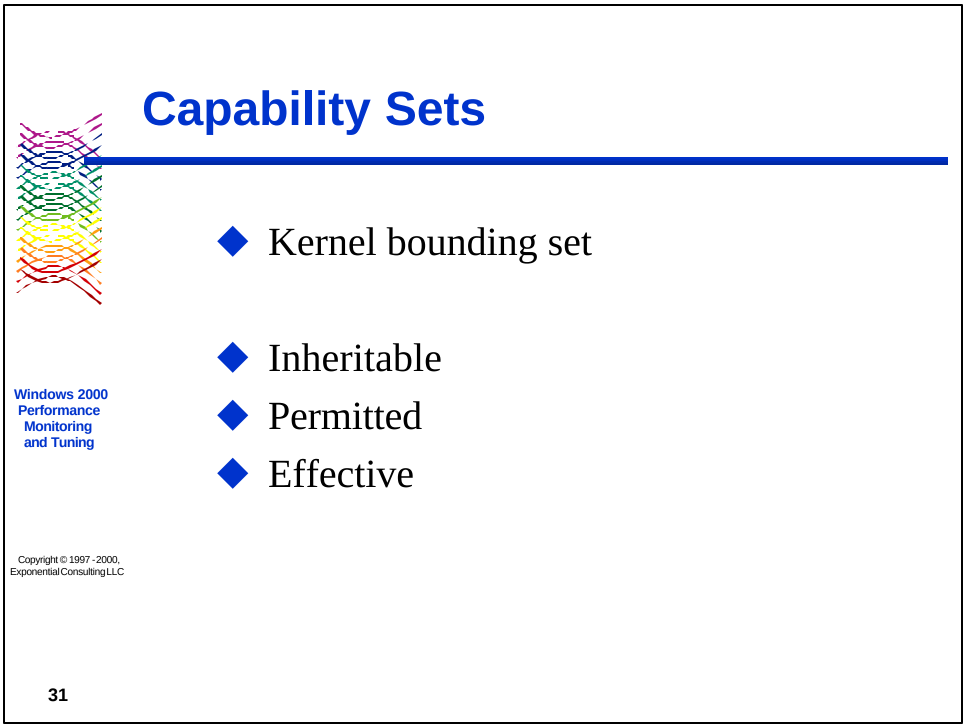
Windows 2000
Performance
Monitoring
and Tuning



Examples

```
#define CAP_CHOWN           0
/* Override all DAC access, including ACL execute access if
   [_POSIX_ACL] is defined. Excluding DAC access covered by
   CAP_LINUX_IMMUTABLE. */

#define CAP_LINUX_IMMUTABLE     9
/* Allows binding to TCP/UDP sockets below 1024 */

#define CAP_SYS_NICE        23
/* Override resource limits. Set resource limits. */
/* Override quota limits. */
/* Override reserved space on ext2 filesystem */
/* Override size restrictions on IPC message queues */
/* Allow more than 64hz interrupts from the real-time clock */
/* Override max number of consoles on console allocation */
/* Override max number of keymaps */
```

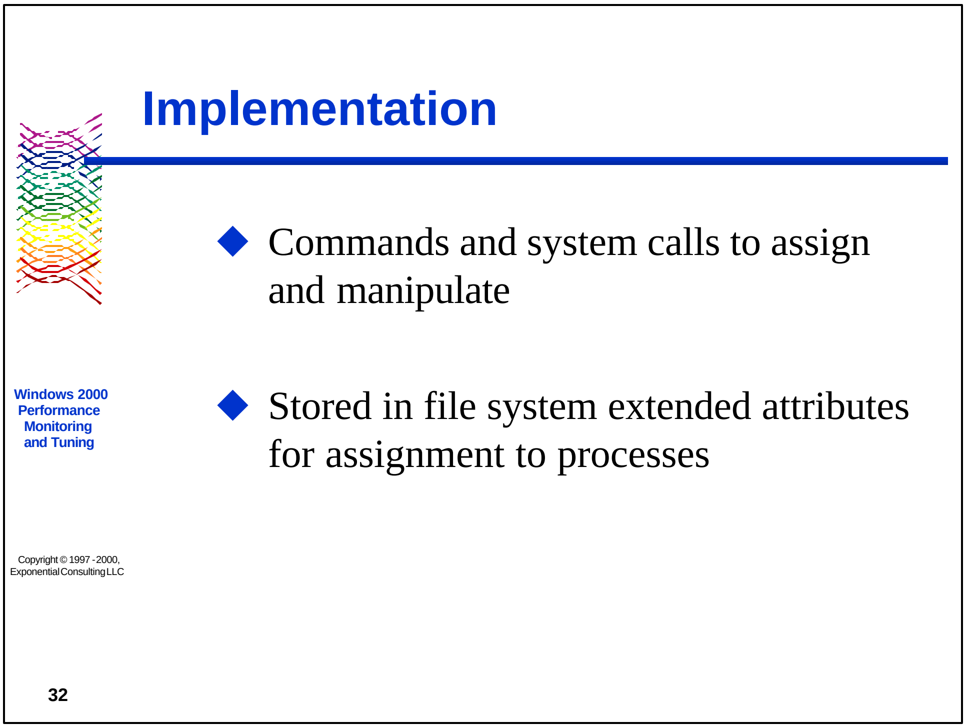
Windows 2000
Performance
Monitoring
and Tuning



Capability Sets

- Kernel bounding set
- Inheritable
- Permitted
- Effective

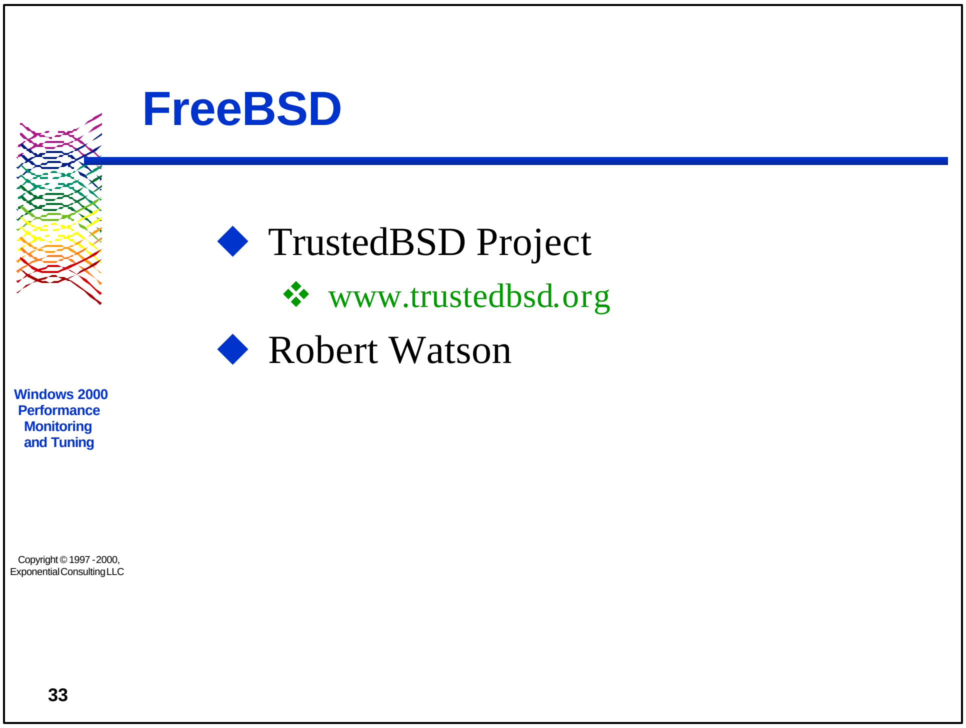
Windows 2000
Performance
Monitoring
and Tuning



Implementation

- Commands and system calls to assign and manipulate
- Stored in file system extended attributes for assignment to processes

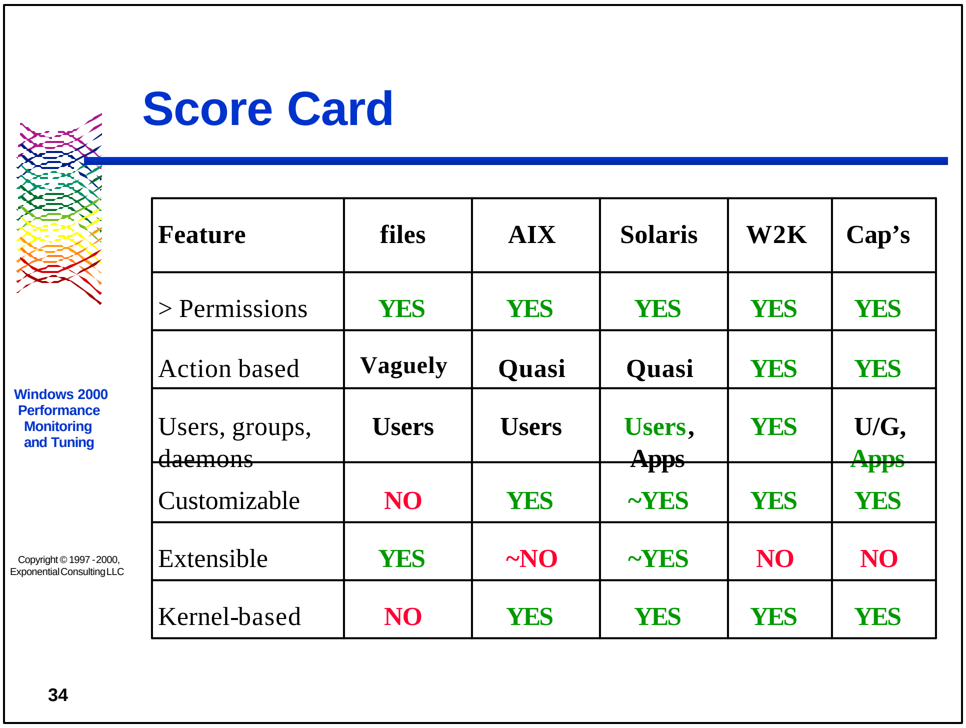
Windows 2000
Performance
Monitoring
and Tuning



FreeBSD

- TrustedBSD Project
  - www.trustedbsd.org
- Robert Watson

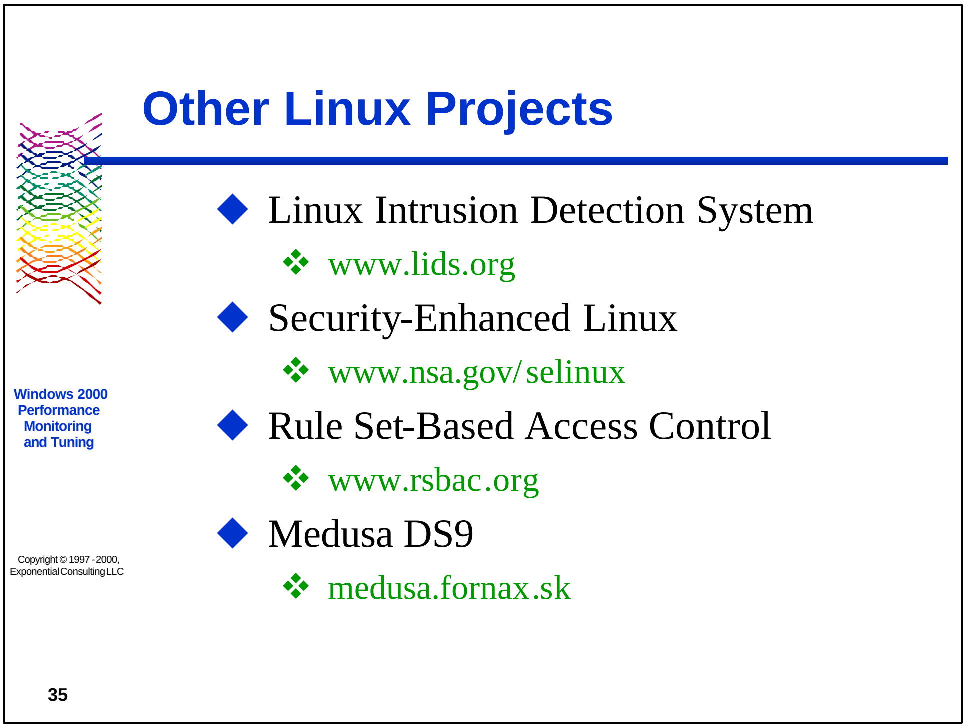
Windows 2000
Performance
Monitoring
and Tuning



Score Card

Feature	**files**	**AIX**	**Solaris**	**W2K**	**Cap's**
> Permissions	**YES**	**YES**	**YES**	**YES**	**YES**
Action based	**Vaguely**	**Quasi**	**Quasi**	**YES**	**YES**
Users, groups, daemons	**Users**	**Users**	**Users, Apps**	**YES**	**U/G, Apps**
Customizable	**NO**	**YES**	**~YES**	**YES**	**YES**
Extensible	**YES**	**~NO**	**~YES**	**NO**	**NO**
Kernel-based	**NO**	**YES**	**YES**	**YES**	**YES**

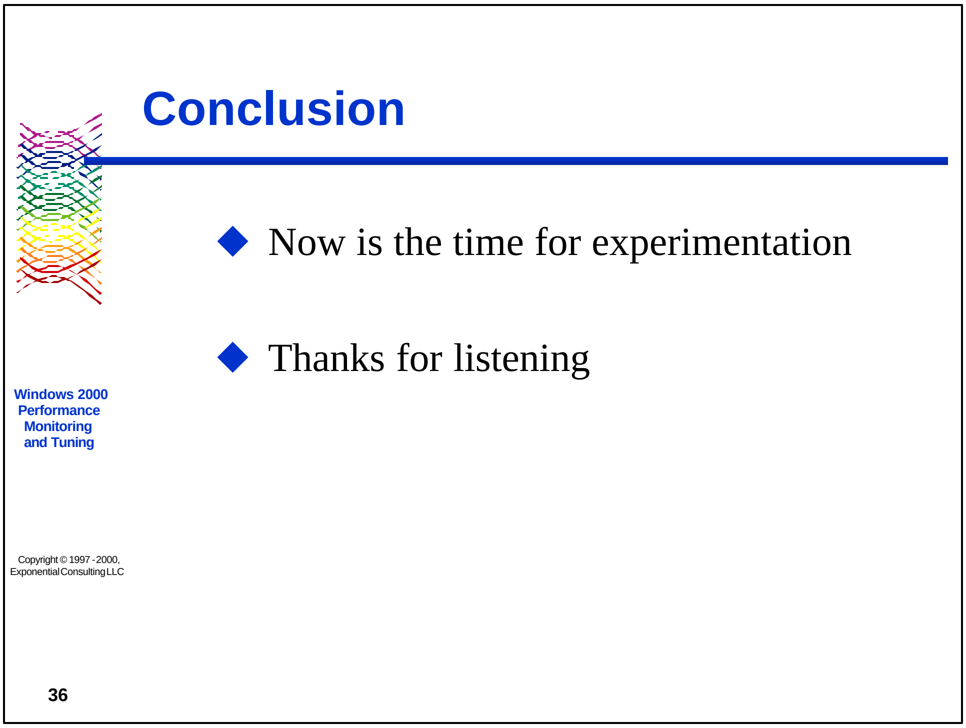
Windows 2000
Performance
Monitoring
and Tuning



Other Linux Projects

- Linux Intrusion Detection System
  - www.lids.org
- Security-Enhanced Linux
  - www.nsa.gov/selinux
- Rule Set-Based Access Control
  - www.rsbac.org
- Medusa DS9
  - medusa.fornax.sk

Windows 2000
Performance
Monitoring
and Tuning



Conclusion

- Now is the time for experimentation
- Thanks for listening

Windows 2000
Performance
Monitoring
and Tuning