

Adding Role Based Access Control onto a Unix Storage Platform

**Steven Danneman
Isilon Systems, Division of EMC**

August 30, 2011

- ❑ File access vs system access
 - ❑ Everything is a file, including config
- ❑ Partitioned system administration
- ❑ Delegated system administration

- ❑ Good, but not enough
 - ❑ Multiple UIs
 - ❑ CLI
 - ❑ Web
 - ❑ REST
 - ❑ Read-only tasks

1. A subject (user) may only complete an action if that subject has been made a member of a role.
2. A subject's role membership must be assigned by an entity other than the subject.
3. A subject may only complete an action if the action is authorized by the role that subject is a member of.

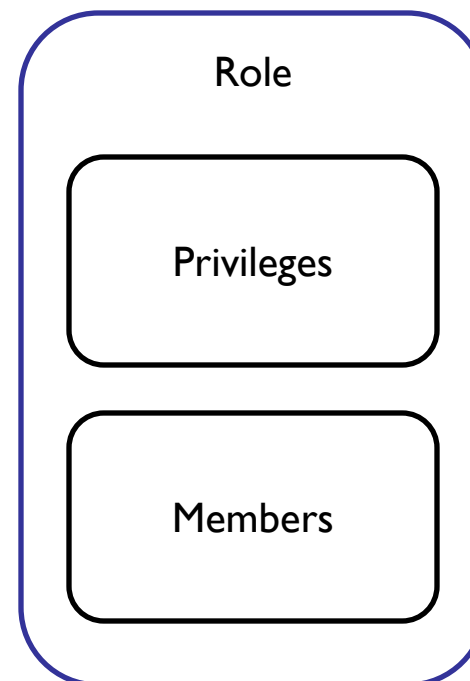
<http://csrc.nist.gov/groups/SNS/rbac/index.html>

RBAC vs ACLs

- ❑ Equivalent authorization systems
- ❑ RBAC definition is separate from assignment

	RBAC	ACLs
File Access		X
Configuration	X	X
System Tasks	X	

- ❑ Security Admin
- ❑ System Admin
- ❑ Audit Admin



- ❑ Singular / Grouped
- ❑ Mapped across all UIs
 - ❑ WebUI / CLI / REST
- ❑ Configuration
 - ❑ SMB, NFS, Snapshots, Quotas
- ❑ System Tasks
 - ❑ Shutdown

Privilege

- Name
- ID
- Attributes
 - Read-only

- ❑ /etc/roles
 - ❑ List privileges
 - ❑ List users / groups
 - ❑ From all auth providers
 - ❑ LDAP / NIS / AD
- ❑ /etc/role-privileges
- ❑ /etc/role-members

- Privileges stored in user credential
 - *setprivs()*
 - Union of all **privs** from all **roles**

- ❑ *priv_check(struct priv)*
 - ❑ userspace & kernel implementation
- ❑ syscalls
- ❑ Configuration
 - ❑ ACLs on FS
 - ❑ Need trusted service

- ❑ What happens to *root*?
 - ❑ Too difficult to administer a Unix system with no-*root*.
- ❑ Read-only access, Unix allows a lot
- ❑ Hierarchical systems
 - ❑ Sysctl, privilege per-MIB?

Open Questions

- ❑ Allow vs Deny privileges
 - ❑ Deny FS access
- ❑ Need for a Default/User role

- ❑ Auditing
- ❑ Subject Action Object
 - ❑ Accomplished with virtual machines, can we do better?
 - ❑ Prime directories
- ❑ Restricting logon user privs vs system daemon privs

Questions?

Contact: sdanneman@isilon.com