Adding Role Based Access Control onto a Unix Storage Platform

Steven Danneman
Isilon Systems, Division of EMC

September 20, 2011

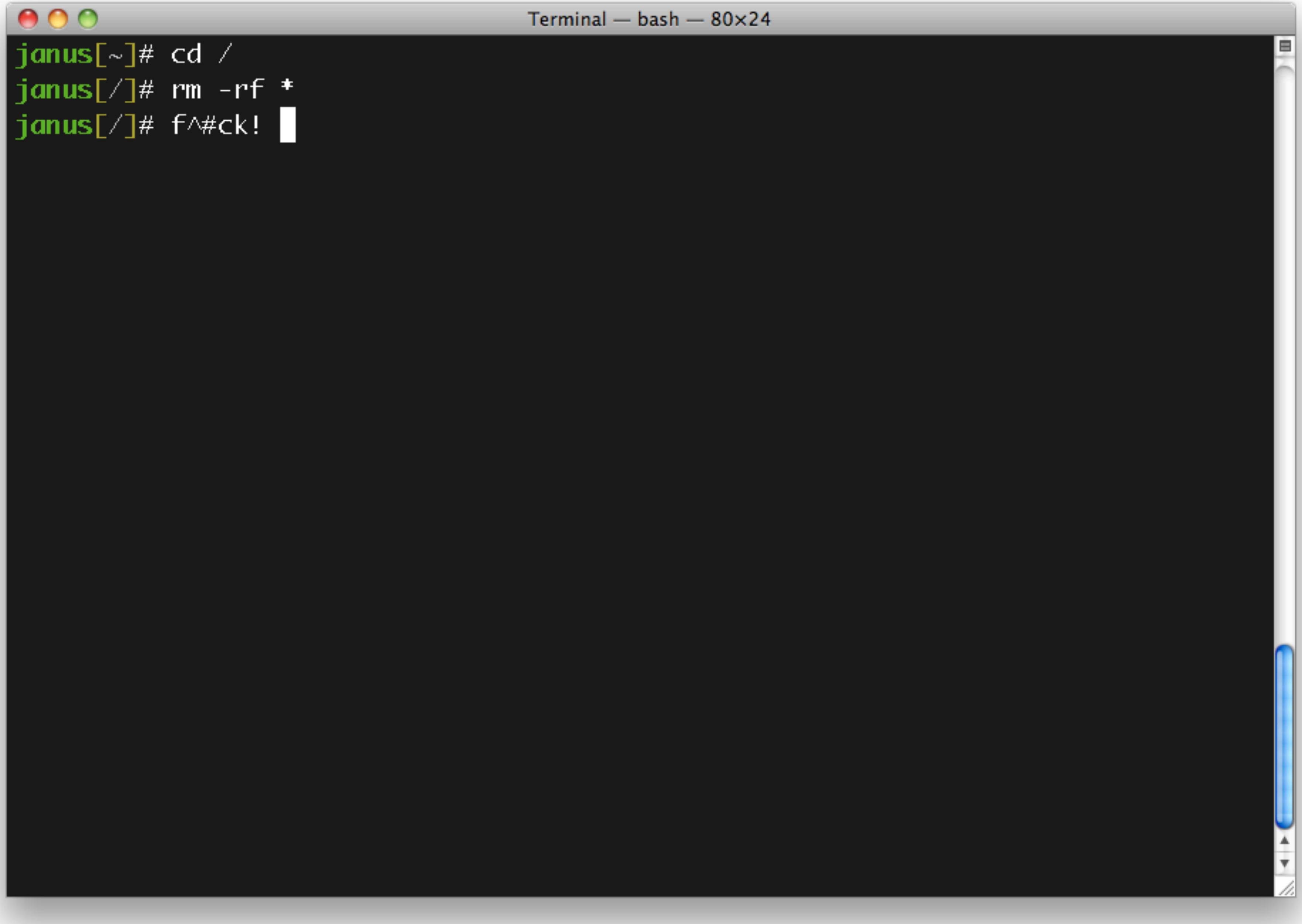
Scoping

- Discuss ideas prototyped on Isilon OneFS
  - FreeBSD based
- Storage Appliance
  - Not concerned w/ arbitrary binary execution
  - Controlled interfaces to the system
    - Data path
    - Config path

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Scoping

- Data path
  - Discretionary Access Control
    - Mode Bits
    - NTFS style ACLs
- Config path
  - *root* authentication



```
janus[~]# cd /
janus[/]# rm -rf *
janus[/]# f^#ck!
```

Problems with God-user Root

1. Has both data access and config access
   - In Unix everything is a file, including config
2. Administers all parts of the system
   - Hardware, file system, services
3. Administers all objects in the system
   - RWX on all files
   - RW all devices
   - Call all syscalls()

How do we Improve this Situation?

1. Separate file access from admin access
2. Partition system administration
   - ❐ Split up administrative tasks
   - ❐ Assign these tasks to different users
3. Delegate system administration
   - ❐ Split up the objects administered
   - ❐ Assign admin of these objects to different users

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Administrator Tasks

- Config tasks (CRUD):
  - Users, Groups
  - SMB shares, NFS exports, iSCSI LUNs
  - Quotas, Snapshots, WORM
- System tasks:
  - Shutdown
  - Backup
  - Replace drive

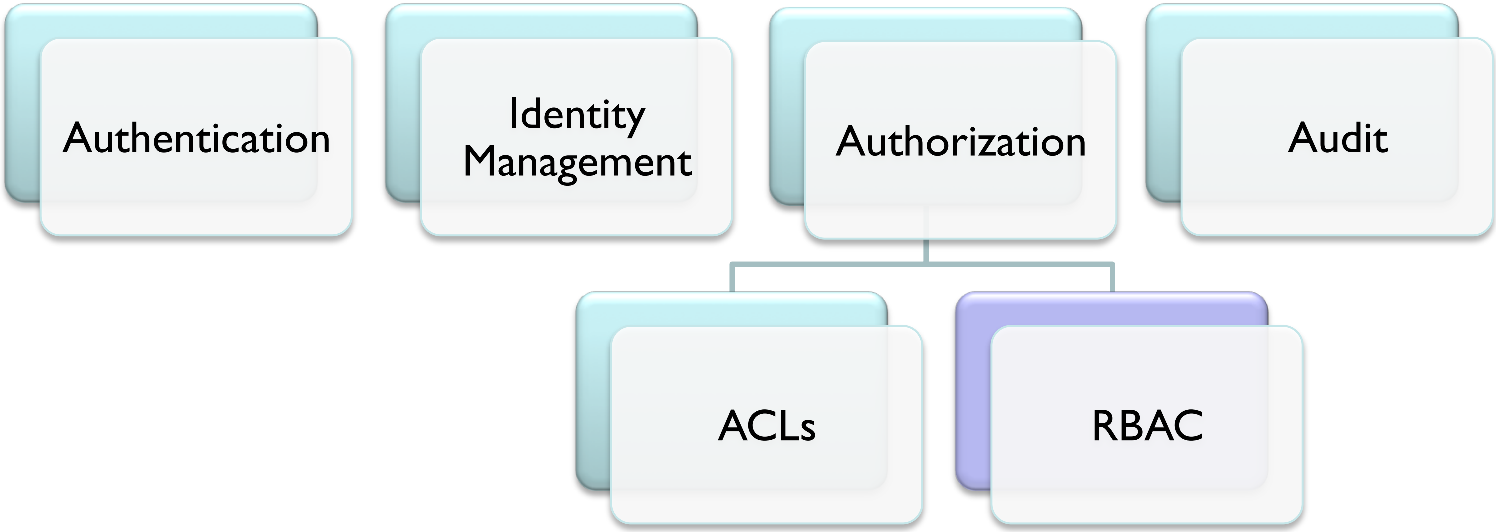
Data Access vs Config Access

- Give non-root users more privileges
  - Need to provide config access
- Solution 1: ACLs
  - Create different admin groups, assign within */etc*
  - Not easy to manage
  - Not granular enough
  - Can’t separate read vs write w/ only mode bits
- Solution 2: RBAC

2011 Storage Developer Conference. © EMC. All Rights Reserved.

What's RBAC?

Security Taxonomy



2011 Storage Developer Conference. © EMC. All Rights Reserved.

NIST RBAC Standard

1. A subject (user) may only complete an action if that subject has been made a member of a role.

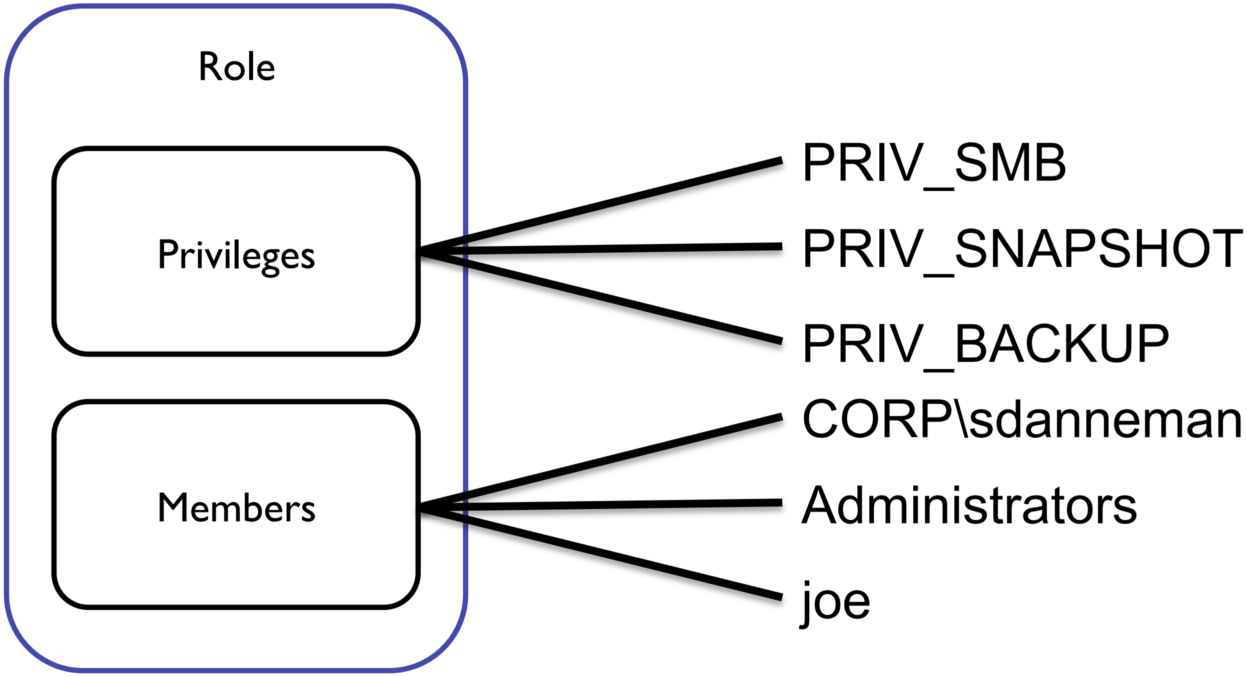
2. A subject's role membership must be assigned by an entity other than the subject.

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

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Roles

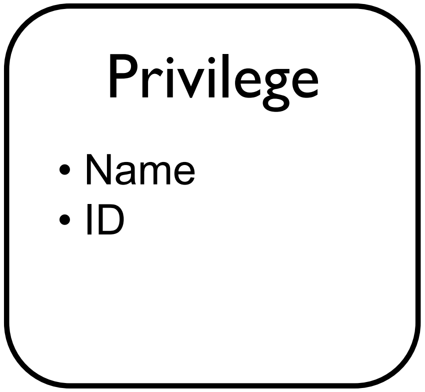

Role
Privileges
Members
PRIV_SMB
PRIV_SNAPSHOT
PRIV_BACKUP
CORP\sdanneman
Administrators
joe

Builtin Roles

- Security Admin
  - Users, Groups, Roles
- System Admin
  - Storage config
  - Hardware
- Audit Admin
  - Read-only access

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Privileges



Privilege

- Name
- ID

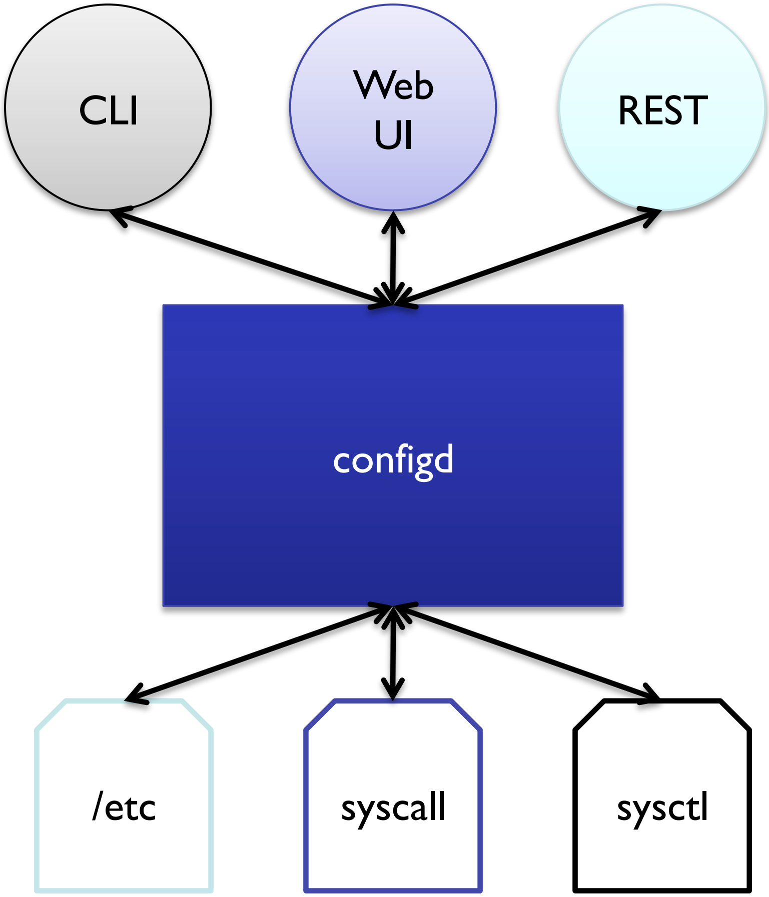
- Grants the right to take an action
  - But we don't have discrete config actions, yet…

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Configuration Service

- Define config changes as discrete actions
- Provide API for config changes
- Provides a trusted service for access checks
  - Access check same granularity as actions

Centralized Configuration



User Action Map – SMB

Action	CLI	WebUI	REST
List SMB config	isi smb config list	/SMB	/smb/config GET
Modify SMB config	isi smb config modify	/SMB	/smb/config PUT
List SMB shares	isi smb share list	/SMB	/smb/share GET
Create SMB share	isi smb share create	/SMB	/smb/share/<name> POST
Modify SMB share	isi smb share modify	/SMB	/smb/share/<name> PUT
Delete SMB share	isi smb share delete	/SMB	/smb/share/<name> DELETE

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Privileges

- Map to an action
  - Singular / Grouped
- Same actions available across all UIs
  - WebUI / CLI / REST

Privilege

- Name
- ID

2011 Storage Developer Conference. © EMC. All Rights Reserved.

User Action Map – SMB Singular

Action	CLI	REST	Privilege (PRIV_)
List SMB config	isi smb config list	/smb/config GET	SMB_CONF_LIST
Modify SMB config	isi smb config modify	/smb/config PUT	SMB_CONF_MODIFY
List SMB shares	isi smb share list	/smb/share GET	SMB_SHARE_LIST
Create SMB share	isi smb share create	/smb/share/<name> POST	SMB_SHARE_CREATE
Modify SMB share	isi smb share modify	/smb/share/<name> PUT	SMB_SHARE_MODIFY
Delete SMB share	isi smb share delete	/smb/share/<name> DELETE	SMB_SHARE_DELETE

2011 Storage Developer Conference. © EMC. All Rights Reserved.

User Action Map – SMB Grouped

Action	CLI	REST	Privilege (PRIV_)
List SMB config	isi smb config list	/smb/config GET	SMB_CONF_READ
Modify SMB config	isi smb config modify	/smb/config PUT	SMB_CONF_WRITE
List SMB shares	isi smb share list	/smb/share GET	SMB_SHARE_READ
Create SMB share	isi smb share create	/smb/share/<name> POST	SMB_SHARE_WRITE
Modify SMB share	isi smb share modify	/smb/share/<name> PUT	SMB_SHARE_WRITE
Delete SMB share	isi smb share delete	/smb/share/<name> DELETE	SMB_SHARE_WRITE

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Privileges - Grouped

- Prefer starting with grouped set
- Provides memorizable set of privileges
  - Grouped: ~40 privs
  - Singular: ~300 privs
- Grouped set can later be expanded to singular
  - Via privilege hierarchy

Role Database

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

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Logon

- Privileges retrieved from /etc/roles
- Stored in user credential
  - *setprivs()*
    - Union of all **privs** from all **roles**

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Credential

```
struct ucred {
  uid_t   cr_uid;       /* effective user id */
  uid_t   cr_ruid;      /* real user id */
  uid_t   cr_svuid;     /* saved user id */
  gid_t   cr_rgid;      /* real group id */
  gid_t   cr_svgid;     /* saved group id */
  gid_t   *cr_groups;   /* groups */
  int     cr_ngroups;   /* number of groups */
  int     *cr_privs;    /* privilege list */
  int     cr_nprivs;    /* num privileges */
}
```

2011 Storage Developer Conference. © EMC. All Rights Reserved.

Privilege Checking

- *priv_check(int priv)*
  - Userspace implementation
    - Called from configuration service
      - Trusted service
  - Kernel implementation
    - Called from all syscalls

Simple enough.

What else?

Unix Issues

- What happens to *root*?
- Logon user vs service/daemon user
  - Two sets of privileges
  - Two privilege systems
- 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

Future

- Delegated Administration
  - Currently action implies an object set
    - Define our own object sets
  - Accomplished with virtual machines
    - Can we do better?

Questions?

Contact: sdanneman@isilon.com

2011 Storage Developer Conference. © EMC. All Rights Reserved.