Managing Web Access using Role-Based Security

December 15, 2005

Brian Vladimiroff
IT Services
Pacific Northwest National Laboratory

Web Server Administration

- Maintaining Patch Levels
  - Stable/Secure Environment
- Maintaining Websites
  - Creation
  - Deletion
- Troubleshooting
  - Server Problems/Site Problems
- Configuring Website Access
  - Adding/Removing Users
  - Debugging User access issues
- Other Tasks

Modifying Website Access

- Workflow
  - Access is defined by the Owner
  - Requests are made to the Web Server Administrator
  - Web Server Administrator makes the change
  - Web Server Administrator notifies the Owner
- Problems
  - Requests are delayed
  - Mistakes can be made
  - Work is duplicated

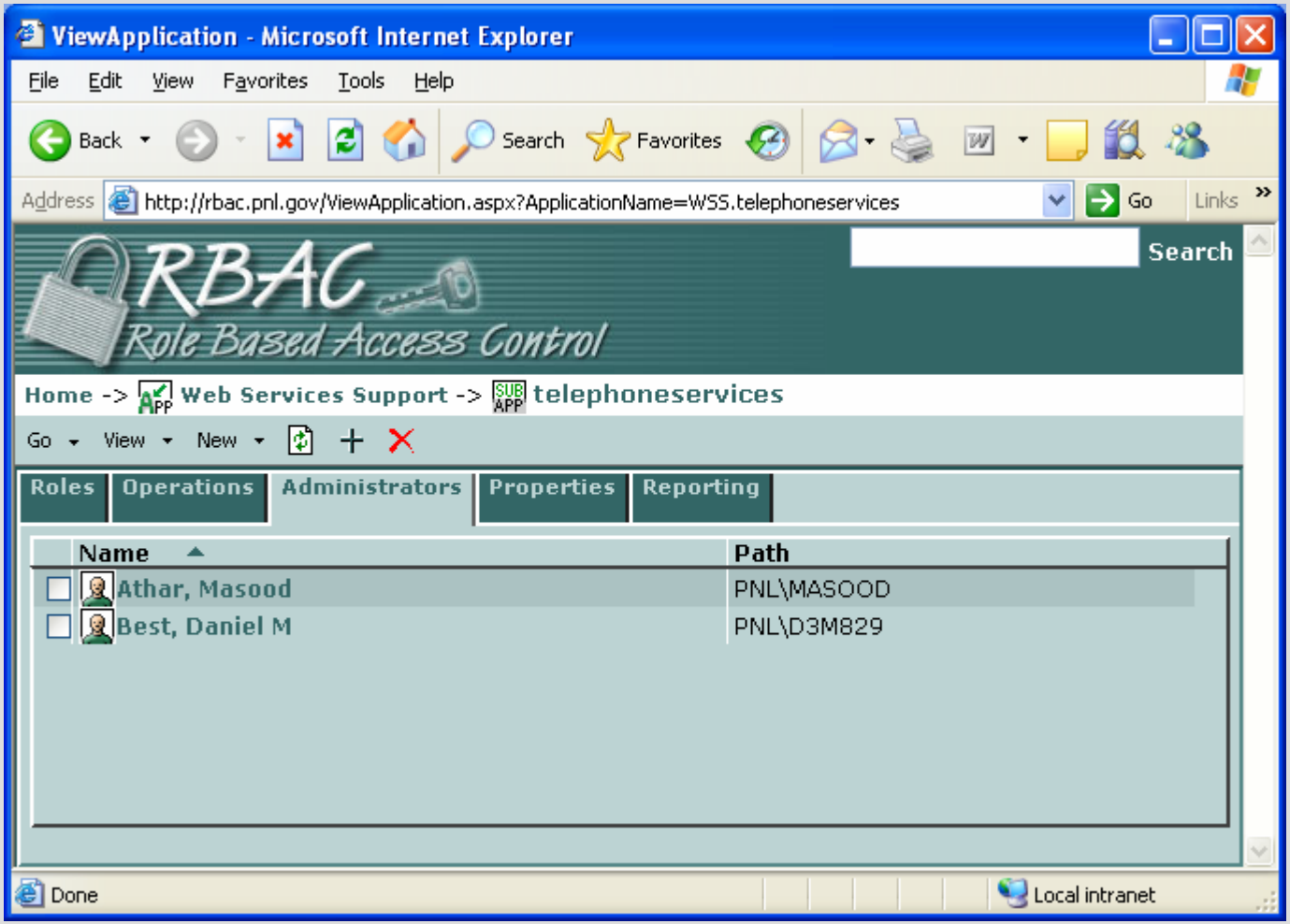
Key Concepts

- What is Role-Based Security?
  - Users with similar job functions are grouped together into roles
  - Access to resources is controlled using roles
  - Management of role membership is done by the owner of the role

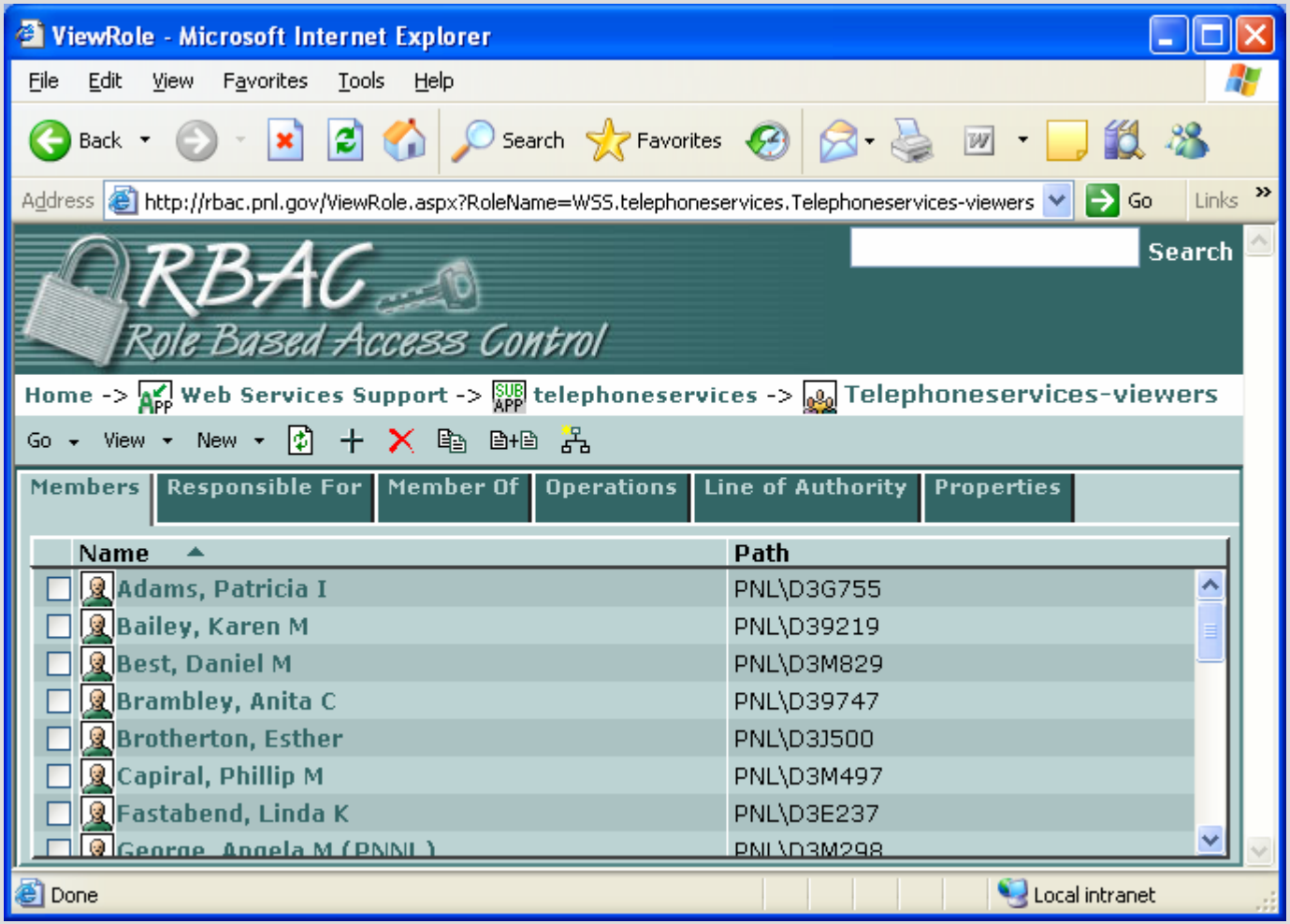
Practical Implementation

- Role Based Access Control (RBAC)
  - A Role Based Access Control system was implemented at the Pacific Northwest National Laboratory
  - Integrated with Microsoft Active Directory
  - Robust Application Programming Interface (API)
- RBAC Administration Website
  - Manage roles and role membership in a single interface
  - Gives control of access to owners

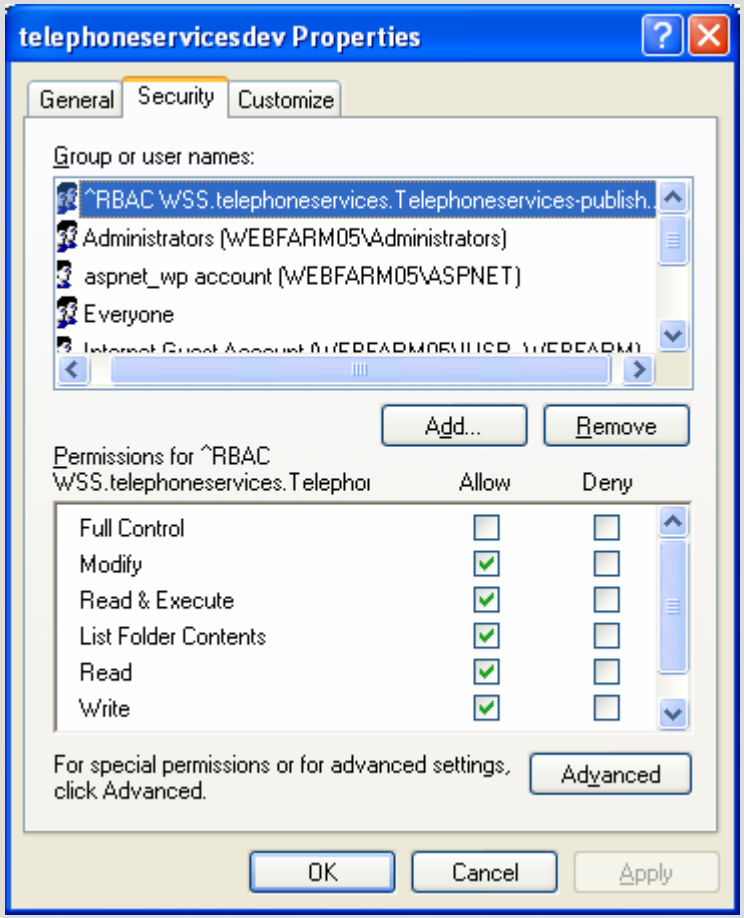
Example


ViewApplication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://rbac.pnl.gov/ViewApplication.aspx?ApplicationName=WSS.telephoneservices
Go Links
RBAC
Role Based Access Control
Search
Home -> Web Services Support -> telephoneservices
Go View New
Roles Operations Administrators Properties Reporting
Name Path
Athar, Masood PNL\MASOOD
Best, Daniel M PNL\D3M829
Done
Local intranet

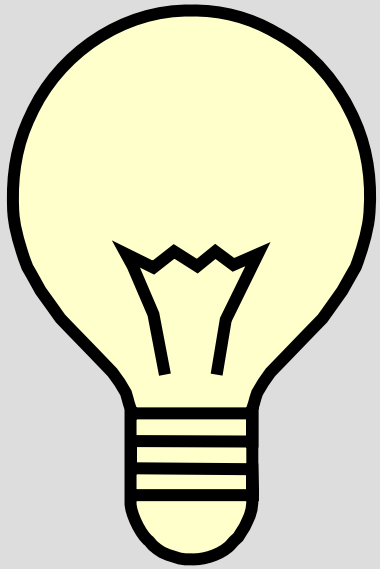
Example


ViewRole - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://rbac.pnl.gov/ViewRole.aspx?RoleName=WSS.telephoneservices.Telephoneservices-viewers
Go Links
RBAC
Role Based Access Control
Search
Home -> Web Services Support -> telephoneservices -> Telephoneservices-viewers
Go View New
Members Responsible For Member Of Operations Line of Authority Properties
Name Path
Adams, Patricia I PNL\D3G755
Bailey, Karen M PNL\D39219
Best, Daniel M PNL\D3M829
Brambley, Anita C PNL\D39747
Brotherton, Esther PNL\D3J500
Capiral, Phillip M PNL\D3M497
Fastabend, Linda K PNL\D3E237
George, Angela M (PNNL) PNL\D3M298
Done
Local intranet

Example


telephoneservicesdev Properties
General
Security
Customize
Group or user names:
^RBAC WSS.telephoneservices.Telephoneservices-publish..
Administrators (WEBFARM05\Administrators)
aspnet_wp account (WEBFARM05\ASPNET)
Everyone
Add...
Remove
Permissions for ^RBAC WSS.telephoneservices.Telephor
Allow
Deny
Full Control
Modify
Read & Execute
List Folder Contents
Read
Write
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

Other Uses of Role-Based Security

- File share access
- Dynamic website content
- Email distribution lists
- Delegation Management

Questions