Windows Server 2012

Dynamic Access Control

Evan Anderson <EAnderson@wellbury.com>

Photo Credit: http://flickr.com/zeze57

My Background

- Messing around w/ computers since 1985
- Day job
  - Contract sysadmin since 2004
  - Subcontractor for IT security consulting firm
    - Internal / external network / app pentests
    - Architecture reviews
    - Red / blue team exercises

Why DAC?

- Overcome inflexible NT ACL model
  - Based on single boolean operation – OR
- Curtail group sprawl in AD
  - And security token bloat
- Make AD attributes usable for security
- Create centralized policy
- Give users access-denied remediation

DAC in a nutshell

- Users, client computers, and resources described by attributes
- Operators on attributes allow file servers to selectively grant permission
  - =, !=, >, <, <=, >=
  - Member_of, Not_member_of
  - Member_of_any, Not_member_of_any
  - Contains

Where is DAC applied

- File server access
  - Share permission
  - NTFS permission
  - DAC
- All permissions evaluated, effective permission based on amalgam

Components of DAC (1)

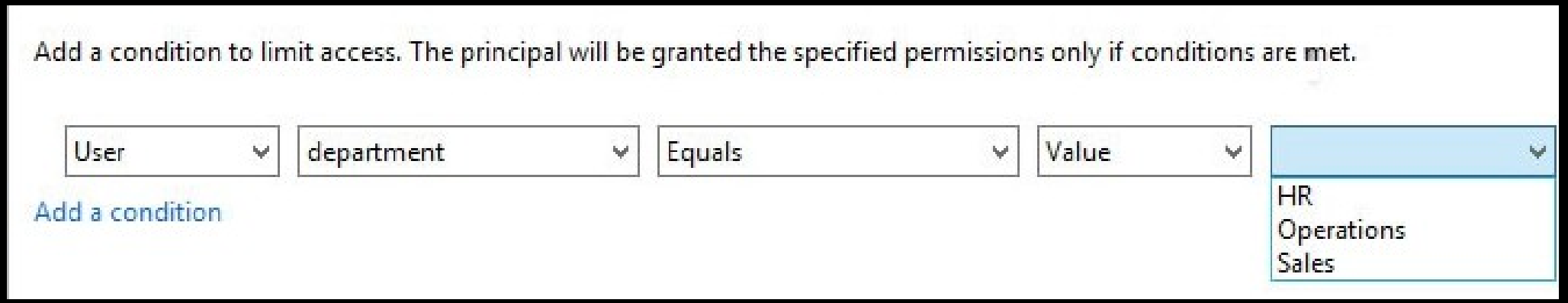
- Claims
  - AD attributes
  - Users
  - Devices
    - Windows 8+ clients only
  - Attribute types
    - Boolean, SID, integer, string, multi-valued integer and string

Components of DAC (2)

- Resource classifications
  - Stored as ADS in NTFS
    - ReFS not supported
  - Office document properties
    - O2K7+ file formats just ZIP files
    - Older files OLE compound documents

Components of DAC (3)

- Conditional expressions
  - For permission and for auditing
    - No deny permissions – allow only



Requirements

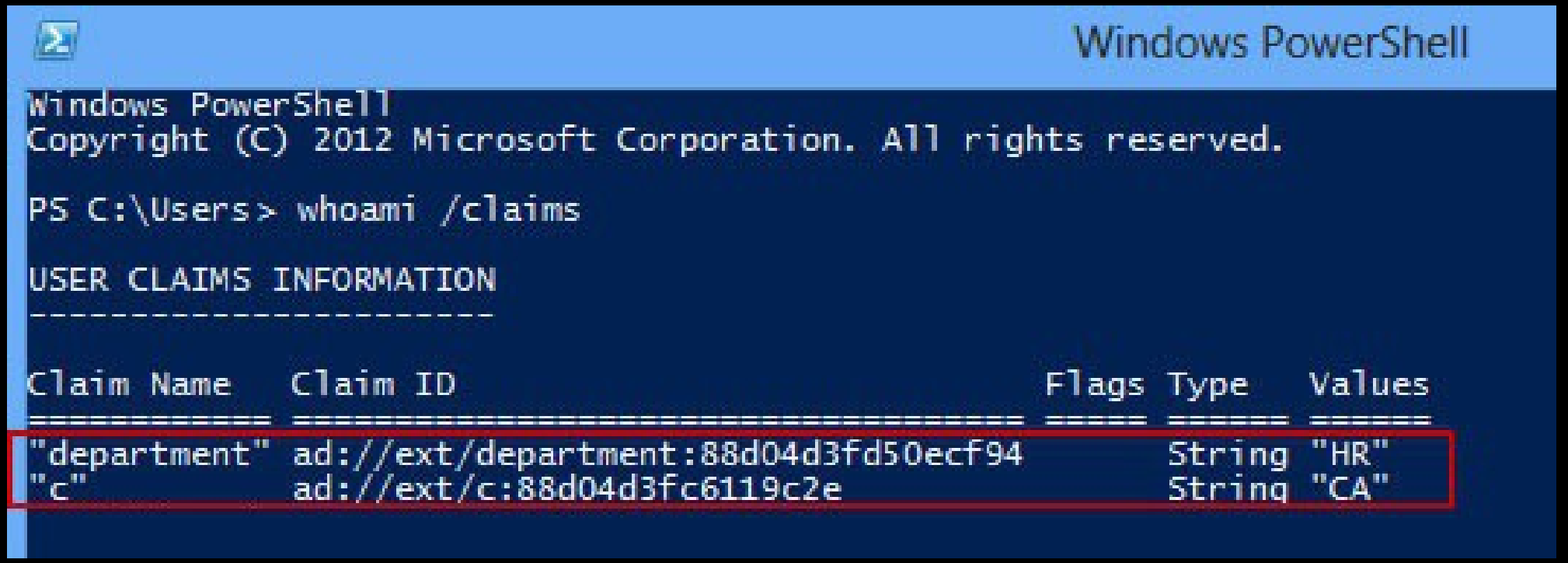
- Windows Server 2012 DCs
  - Doesn't need W2K12 domain-functional level
  - Need enough W2K12 DCs
- File servers
  - W2K12
- Clients
  - Windows 8 for device clients
  - User claims from any client OS

User / Device Claims

- Come from AD attributes
  - Subset of attributes to prevent token-bloat
  - Think about source of attributes
    - No validation of attributes in AD – import from authoritative, curated, controlled sources
    - You may be moving security boundaries in your organization
    - Delegation of control for attribute modification

Seeing claims in token

- On Windows 8: whoami /claims



Resource Classification

- Embedded (Office docs) or manually tagged
- File Classification Infrastructure
  - Much-improved in W2K12
    - W2K12 classifies in realtime, W2K8 scheduled task
    - W2K12 – GUI in Windows Explorer, W2K8 no GUI
    - W2K12 – Users can classify, W2K8 admins only
  - 3rd party classifiers
    - Content analysis products
  - Powershell-based classifiers

Central Access Policy

- Analogous to an NTFS DACL
  - Composed of Central Access Rules
- Stored in AD
  - CN=Claims Configuration,CN=Services,DC=Configuration,DC=domain,DC=tld
- Schema added in W2K12 ADPREP
- Published to file servers via Group Policy
  - Cached in registry on file servers

Central Access Policy

- Current and Proposed Permissions
  - What if ?
  - Events logged when effective permissions differ

Central Audit Policy

- Analogous to an NTFS SACL

Central Access Rules

- Analogous to an ACE in an ACL
  - Target resource attributes
  - Permissions
    - Conditionally applied based on user/device claims

Cross-forest DAC

- Claims transformation
  - Analogous to SID filtering
  - Similar to claims filtering in ADFS
- If edge DC in trusting forest is W2K8 R2 claims won't be returned
  - Sentinel SID functionality

Changes in Kerberos

- Armored TGS requests
  - Cannot have any W2K3 DCs in doman
- Compression to combat ticket/token bloat
  - MS says W2K12 tickets smaller than prior OS
- Compound authentication
  - Puts device claims into user ticket

Protocol differences

- Windows 8 clients vs. pre-Windows 8 clients
  - Win8 clients provide PAC containing claims to file server
  - Pre-Win8 – File server contacts DC to obtain claims on behalf of clients
- Device claims require Win8 clients
  - Compound authentication
- Kerberos armoring
  - RFC 6113 – Armoring or “FAST”
  - Prevent dictionary attacks against AS-REP

Problem DAC doesn't solve

- No way to tell where security groups have been used
- No ability to determine where DAC policies have been used centrally
  - Changing DAC rule may have “business impact”
  - Staging policy allows testing of new policies

Thanks, OISF!

Evan Anderson <EAnderson@wellbury.com>

Photo Credit: http://flickr.com/zeze57