Protecting AD Domain Admins with Logon Restrictions and Windows Security Log

Sponsored by

solarwinds

Thanks to

- Made possible by

solarwinds

LOG & EVENT MANAGER

www.solarwinds.com

Preview of Key Points

- What are we trying to prevent?
- How we did it
- What you can't prevent – Detect!
  - SolarWinds Log and Event Manager

What are we trying to prevent?

- Prevent intruders from gaining privileged access to Active Directory
- Part of a larger goal: prevent intruder access to our most critical assets
  - Must protect all infrastructure components those assets rely on
    - Active Directory
    - VMWare infrastructure

Why is protecting privileged access to AD difficult?

- Separate end-user and domain admin accounts not sufficient if using same endpoint
- The mobile way we roll doesn't allow 2 different endpoints
  - One dedicated to administration
- Windows doesn't allow you to completely lock down which computers Domain Admins can logon from
  - Must monitor for Domain Admin logons from unauthorized systems
  - SolarWinds Log and Event Manager

How we did it

- Divided IT components into
  - Level 0 – infrastructure components that critical assets rely on
    - VMWare
      - vCenter
      - ESXi
    - Active Directory
  - Level 1 – other IT components
    - Member servers
    - Important but not critical applications
      - SharePoint
      - CRM

ULTIMATE WINDOWS SECURITY .COM

solarwinds

Admin accounts

- Create separate admin accounts for both levels
  - Randy
    - End-user account
    - Level0 – admin account
      - Domain admins and vCenter admin
    - Level1 – admin account
      - Member servers and applications
- Why the need to separate level 0 and 1?
  - You shouldn't be doing dangerous activities whiled logged on with either account
  - To prevent mal-agents that infect level 1 components from being able to jump to level 0 components
  - To prevent pass-the-hash attacks
    - Don't logon to the same system with accounts from 2 different levels
- 2 groups in AD
  - Level 0 Admins
    - Member of Enterprise Admins and vCenter Admins
  - Level 1 Admins
    - Use group policy Restricted Groups to make member of local Administrators group on non-critical servers
    - Add to various application admin groups/roles

ULTIMATE WINDOWS SECURITY .COM

solarwinds

Jump boxes

- Created 2 jump boxes
  - Jump0 - Used for privileged access to
    - AD and VMWare
  - Jump1 – Administering
    - All other IT components
    - Delegated AD tasks
      - Resetting passwords of users with non-critical access
    - Delegated VMWare tasks
      - Restarting VMs

Group policy objects

- Group policy objects
  - Mandatory Computer Policies
  - Default Domain Controller Policies
  - Level 0 Jump Box Policies
  - Level 1 Jump Box Policies

Group policy objects

- Mandatory Computer Policies
  - Linked to top level OU containing all computers except for
    - Jump boxes
    - Domain controllers
  - No override
  - User Rights Assignment
    - Deny logon locally: Level 0 Admins
    - Deny access this computer from network: Level 0 Admins
    - Deny logon through Remote Desktop Services: Level 0 Admins
    - Allow logon through Remote Desktop Services: Level 1 Admins
  - IP Security Policy
    - Restrict inbound RDP to Level 1 Jump Boxes

Group policy objects

- Default Domain Controller Policies
  - User Rights Assignment
    - Deny logon locally: Level 0 and 1 Admins
    - Deny logon through Remote Desktop Services: Level 1 Admins
  - IP Security Policy
    - Limit incoming Remote Desktop Connections to Level 0 JumpBoxes

Group policy objects

- Level 0 Jump Box Policies
  - User Rights Assignment
    - Allow logon through Remote Desktop Services
      - Level 0 Admins
    - Allow logon locally
      - Level 0 Admins
  - Windows firewall
    - Block all incoming except for remote desktop
  - IP Security Policy
    - Require security for outbound RDP to DCs and vCenter

ULTIMATE WINDOWS SECURITY .COM

solarwinds

Group policy objects

- Level 1 Jump Box Policies
  - User Rights Assignment
    - Allow logon through Remote Desktop Services
      - Level 1 Admins
    - Allow logon locally
      - Level 1 Admins
  - Windows firewall
    - Block all incoming except for remote desktop
  - IP Security Policy
    - Require security for outbound RDP to member servers

ULTIMATE WINDOWS SECURITY .COM

solarwinds

2 factor authentication

- Implemented 2-factor authentication on Jump Boxes
- Level 0 Admins can't logon to Jump Box without token/soft token

What we can't prevent

- Can't lock down the "Access this computer from network" logon right on domain controllers
  - Can't 2-factor either
- Network logons by Level 0 Admins to domain controllers from non-JumpBox
  - To administer AD with ADUC even on local DC itself
    - You need "Access this computer from network"
- What you can't prevent
  - Detect!

Detect

- Any logon attempt where user
  - Member of Level 0 Admins
  - Not coming from Jump0
- Any logon attempt where
  - Member of Level 0 Admins
  - Target computer not
    - Domain controller
    - Jump0

Try out SolarWinds

- Log and Event Manager
  - Virtual appliance
  - Download the VM
  - Boot it up
  - Connect to AD
  - Start collecting events
- Quick start
  - http://www.solarwinds.com/trials/lem/complete-virtual-appliance-deployment.aspx

More we could do

- Block/detect use of non-essential programs on jump boxes, level 0 components
- Block internet access to
  - Jump boxes
  - Domain controllers
  - vCenter
  - ESXi

ULTIMATE WINDOWS SECURITY .COM

solarwinds

Bottom line

- Isolate privileged accounts to clean systems
- Require 2FA for privileged accounts
- Detect and respond to violations
- Download LEM