10 Things I Hate About You: Manage Windows like Linux with Ansible

Matt Davis
Senior Principal Software Engineer, Ansible Core
I LOVE WINDOWS
Who am I?
10 Things I Hate About You

In Theatres Wednesday, March 31
WinRM (HTTP-based remote shell protocol)
Non-interactive logon
Different connection plugin
What about Microsoft OpenSSH?
DEMO: WinRM Connectivity
Powershell

- Unlike Python, "just there" on modern Windows
- We can use .NET
- Powershell 3+, Windows 7/Server 2008+
  - Experimental PSCore/6/7 support
- Access to the DSC universe via win_dsc
- `win_psmodule`: # install xDNSServer DSC module on target
  name: xDnsServer
- `win_dsc`: # create DNS zone
  resource_name: xDnsServerPrimaryZone
  name: createdbyansible.com
- `win_dsc`: # create DNS record
  resource_name: xDnsRecord
  name: test
  zone: createdbyansible.com
  target: 1.2.3.4
  type: ARecord
App Install/Maintenance

- win_chocolatey!
- win_package if you must
- `shell: c:\temp\setup.exe /quiet /dostuff`
DEMO: win_chocolatey module
Reboots, oh the reboots...

- `win_reboot` action makes managed reboots trivial
- `wait_for_connection` is just the second half
Windows Update

- Basic, synchronous updates
- Uses configured source (Windows Update/WSUS)
- Transparent SYSTEM + auto reboot
- win_updates:
  category_names: CriticalUpdates
  reboot: yes
  blacklist:
  - KB4056892
Modules for managing websites, webapps, apppools, virtual dirs, etc.
IIS

- win_iis_website:
  name: Default Web Site
  physical_path: C:\Inetpub\WWWRoot

- win_iis_webapp:
  site: Default Web Site
  name: OrchardCMS
  physical_path: C:\Inetpub\WWWRoot\Orchard
- Manage individual key/value (win_regedit)
- Manage idempotent bulk import (win_regmerge)
Registry

- \texttt{win\_regedit}:
  \begin{itemize}
  \item path: HKLM\Software\Microsoft\Windows
  \item name: SomeValueName
  \item value: 0x12345
  \end{itemize}

- \texttt{win\_regmerge}:
  \begin{itemize}
  \item path: ComplexRegData.reg
  \end{itemize}
Services

- `win_service` looks/acts like Linux service module
- Provides fine control over complex service behavior config in Windows SCM (who/what/when/how)
Services

# ensure IIS is running
- win_service:
  name: W3Svc
  state: running

# ensure firewall service is stopped/disabled
- win_service:
  name: MpsSvc
  state: stopped
  start_mode: disabled
Windows' way of doing enterprise identity
- Makes auth complex
- Ansible can do "throwaway" domains easily
- Promote/depromote DCs
- Joining/leaving domain is simple
- Manage basic domain objects
Domains

# create a domain
- win_domain:
  dns_domain_name: mydomain.local
  safe_mode_password: ItsASecret

# add a domain user
- win_domain_user:
  name: somebody
  upn: somebody@mydomain.local
  groups:
    - Domain Admins
DEMO: Domain Join/Unjoin
ACLs

- More granular than Linux permissions
- SDDL?!
- More like SELinux ACLs
ACLs

0:BAG:S-1-5-21-328427983-2845905853-4261175022-513D:AI
(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICID;LC;;;BU)(A;CIID;DC;;;BU)(A;OICIIIOID;GA;;;CO)
ACLS

- win_owner:
  path: C:\Program Files\SomeApp
  user: Administrator
  recurse: true

- win_acl:
  path: C:\Temp
  user: Users
  rights: ReadAndExecute,Write,Delete
  inherit: ContainerInherit,ObjectInherit
Wrapup
Questions?
#ANSIBLEFEST2019

THANK YOU

youtube.com/AnsibleAutomation
facebook.com/ansibleautomation
linkedin.com/company/Red-Hat
twitter.com/ansible