Red Hat Summit

Connect

Windows Automation with Ansible

Christian Jung
EMEA Principal Specialist Solution Architect
jung@redhat.com

Kevin Blase
IT Specialist
kevin.blase@computacenter.com

Red Hat

Bio


```
---
- name: Christian Jung
  web: https://www.jung-christian.de
  Twitter: https://twitter.com/CJungCloud
  LinkedIn: https://www.linkedin.com/in/cjungcloud/
  eMail: jung@redhat.com
  facts:
    - nerd: everything Linux, Open Source, Software, ...
    - redhatter: since 2006
    - ansible: started 2016, full time since 2019
    - fun_fact: spent two years living in Malta
    - organizer: www.ansible-anwender.de
    - demo_project: www.ansible-labs.de
```


Red Hat

Bio

```
---
- name: Kevin Blase
  LinkedIn: https://www.linkedin.com/in/kevin-b-9078b9225
  eMail: kevin.blase@computacenter.com
  facts:
    - nerd: OpenShift, Ansible, Windows, …
    - it: since 2017
    - ansible: started 2019
    - fun_fact: knows how deers sound
    - hobbies: climbing and nature
```

Windows Automation

100+

Windows Modules

1,300+

Powershell DSC resources

Red Hat

What can I do using Ansible for Windows

Native Windows support uses PowerShell remoting to manage Windows in the same Ansible agentless way.

- Gather facts on Windows hosts
- Install and uninstall MSIs
- Enable and disable Windows Features
- Start, stop, and manage Windows services
- Create and manage local users and groups
- Manage and install Windows updates
- Fetch files from remote sites
- Push and execute any PowerShell scripts you write

Windows WinRM: Auth Methods

WinRM is a management protocol used by Windows to remotely communicate with another server. It is a SOAP-based protocol that communicates over HTTP/HTTPS.

Basic

Unencrypted

NTLM

Usually enabled by Default

Strong One Way Hash

Less Secure

Certificate

Most difficult to setup

Requires valid certs and CAs

Certificate is mapped to single account

CredSSP

Multi-hop Support

Delegates the credentials to remote machine
Uses TLS Tunnel and NTLM / Kerberos

Kerberos

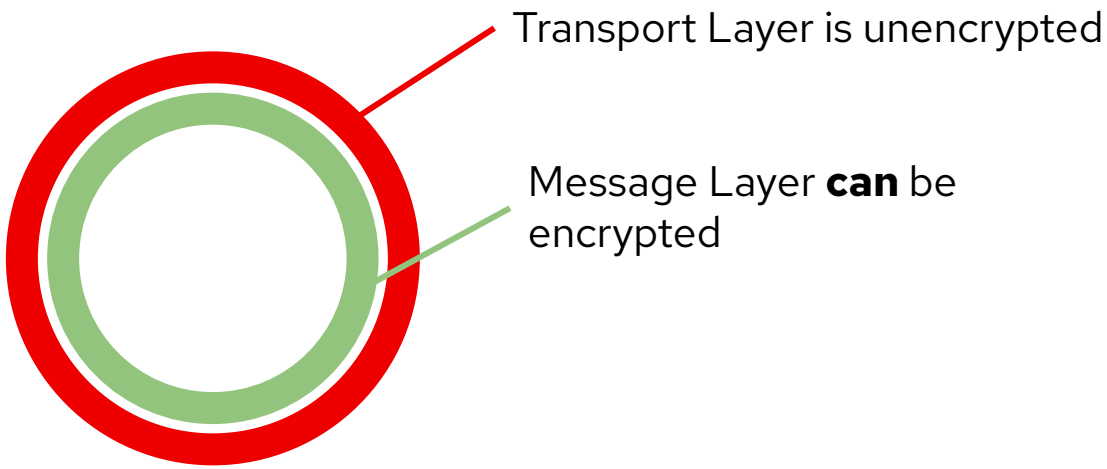
Must be on Domain

Uses a Kerberos Token to Authenticate
Multi-hop Support if using delegation

Windows WinRM: Transport

HTTP

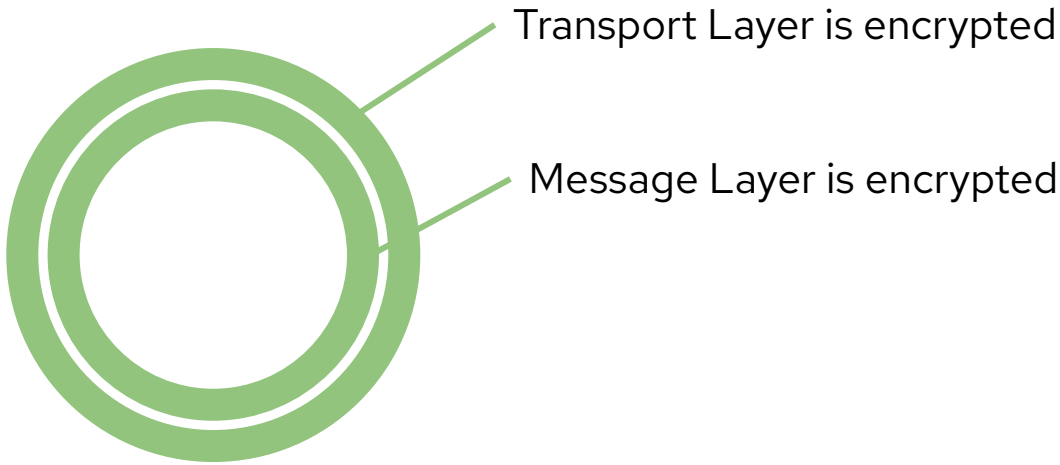
This is the default and most common implementation. Even though HTTP itself does not provide transport level encryption it can be used in junction with CredSSP or Kerberos which provide message level encryption. Typically works on TCP port 5985.



HTTPS

Used with self-signed (not recommended for production) or CA signed certificate. It provides additional layer of encryption.

Typically works on TCP port 5986.



Red Hat

Windows Basic: Software Installation

.MSI file

Installer package file (kind of like .rpm) Contains installation files, registry configuration, etc

Only one MSI can be installed at a time, hence the need for...

.EXE file

Windows Executable file Often used to orchestrate installation of .MSI files and related installation tasks

Disadvantage: Lack of idempotency

Chocolatey is a software packaging format that enables Linux-like software management and installation. Public repos exist, Artifactory and Sonatype nexus support private repos. Custom chocolatey content is not hard to produce.

Disadvantage: Doesn't support everything

Advantage: Simple, idempotent

Reuse Powershell scripts on Windows

Powershell Scripts can be reused with `ansible.windows.win_powershell`

Task in Playbook:

```
- name: Use a local Script
  ansible.windows.win_powershell:
    script: "{{ lookup('ansible.builtin.file', 'script.ps1') }}"
```

Output:

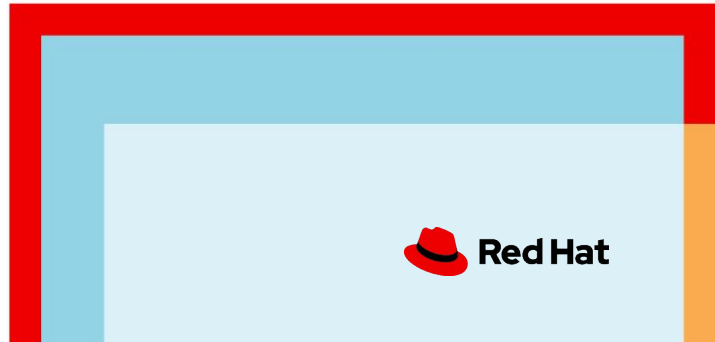
```
TASK [Use a local Script]
*************************************************************************
changed: [win-server]
```

- Easy first steps
- Ansible internal Variables can be implemented
  `$Ansible.Result, $Ansible.Changed, $Ansible.Failed, $Ansible.Diff`

- Checkmode Capabilities
- Idempotency and other Ansible features have to be implemented in the Script

DEMO

-



Action Items

- Self paced labs https://www.redhat.com/en/interactive-labs/ansible
- Windows Guide https://docs.ansible.com/ansible/latest/os_guide/windows_usage.html

Red Hat

Session 8: 17:15 - 17:45

Jetzt Session bewerten!

Einfach QR-Code scannen, Session wählen und bewerten.
Vielen Dank!

red.ht/rhsc-de-s8

Red Hat

Red Hat Summit

Connect

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat