get winrm config

winrm get winrm/config

gpo config

O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS) // add to GPO
Server=http://WEF.HTB.LOCAL:5985/wsman/SubscriptionManager/WEC,Refresh=60 // add to GPO (60 seconds)

on source computer: gpupdate /force

prereqs

start Windows Remote Management service on source computer
add builtin\network service account to "Event Log Readers" group on collector server

list subscriptions / export

C:\Windows\system32>wecutil es > subs.txt

check subscription status

C:\Windows\system32>wecutil gr "Account Currently Disabled"

Subscription: Account Currently Disabled
    RunTimeStatus: Active
    LastError: 0
    EventSources:
        LAPTOP12.HTB.LOCAL
            RunTimeStatus: Active
            LastError: 0
            LastHeartbeatTime: 2017-07-11T13:27:00.920

change pre-rendering setting in multiple subscriptions

for /F "tokens=*" %i in (subs.txt) DO wecutil ss "%i" /cf:Events

export subscriptions to xml

for /F "tokens=*" %i in (subs.txt) DO wecutil gs "%i" /f:xml >> "%i.xml"

import subscriptions from xml

wecutil cs "Event Log Service Shutdown.xml"
wecutil cs "Event Log was cleared.xml"

if get error "The locale specific resource for the desired message is not present", change subscriptions to Event format (won't do any hard running command even if they already are in this format)

1.

for /F "tokens=*" %i in (subs.txt) DO wecutil ss "%i" /cf:Events

2.

Under Windows Regional Settings, on the Formats tab, change the format to "English (United States)"

check subscriptions are being created on the source computer

Event Log: /Applications and Services Logs/Microsoft/Windows/Eventlog-ForwardingPlugin/Operational

troubleshooting WEF

collector server -> subscription name -> runtime status

gpupdate /force (force checkin, get subscriptions)

check Microsoft/Windows/Eventlog-ForwardingPlugin/Operational for errors