Installazione e configurazione per Gestione remota Windows (WinRM)

Configurazione preliminare WinRM

Queste operazioni vanno effettuate sia sulle macchine client che server

Otteniamo le informazioni sui profili di connessione di rete attualmente in uso sul sistema e cambiamo il profilo di rete chiamato "Rete 2" impostando la categoria di rete su "Privata" :

```
Get-NetConnectionProfile
Set-NetConnectionProfile -Name "Rete 2" -NetworkCategory Private
```

```
PS C:\Windows\system32> Get-NetConnectionProfile


Name                     : Rete 2
InterfaceAlias           : Ethernet
InterfaceIndex           : 18
NetworkCategory          : Private
DomainAuthenticationKind : None
IPv4Connectivity         : Internet
IPv6Connectivity         : NoTraffic



PS C:\Windows\system32> Set-NetConnectionProfile -Name "Rete 2" -NetworkCategory Private
```

Avviamo il servizio WinRM

```
sc start winrm
```

Impostiamo la politica di esecuzione di PowerShell su "RemoteSigned", così da consentire l'esecuzione di script locali senza firma e di script scaricati solo se firmati digitalmente. L'opzione `-Force` applica la modifica senza richiedere conferma.

```
Set-ExecutionPolicy RemoteSigned -Force
```

Abilitiamo i breakpoint in PowerShell, forzando l'attivazione anche se ci sono già breakpoint esistenti o altre condizioni che potrebbero impedirlo.

```
Enable-PSBreakpoint -Force
```

Configuriamo il servizio Windows Remote Management (WinRM) applicando le impostazioni predefinite per abilitare la gestione remota con il seguente comando. L'opzione `-q` esegue il comando in modalità silenziosa, senza richiedere conferme da parte dell'utente.

```
winrm quickconfig -q
```

```
PS C:\Windows\system32> winrm quickconfig -q
Servizio Gestione remota Windows già in esecuzione in questo computer.
Gestione remota Windows già impostato per la gestione remota in questo computer.
```

Configurazione WinRM – Computer Server

Abilitiamo la comunicazione non criptata per le connessioni WinRM.

```
Set-Item -Path WSMan:\localhost\Service\AllowUnencrypted -Value $true
```

Abilita l'autenticazione di base per le connessioni WinRM, che invia credenziali in testo chiaro.

```
Set-Item -Path WSMan:\localhost\Service\Auth\Basic -Value $true
```

```
PS C:\Windows\system32> Set-Item -Path WSMan:\localhost\Service\AllowUnencrypted -Value $true

PS C:\Windows\system32> Set-Item -Path WSMan:\localhost\Service\Auth\Basic -Value $true
```

Nota: i comandi sopra potrebbero dare problemi di percorso, in tal caso possiamo verificare il percorso visualizzando l'albero delle variabili di Winrm con il comando

```
winrm get winrm/config
```

```
PS C:\Windows\system32> winrm get winrm/config
Config
    MaxEnvelopeSizekb = 500
    MaxTimeoutms = 60000
    MaxBatchItems = 32000
    MaxProviderRequests = 4294967295
    Client
        NetworkDelayms = 5000
        URLPrefix = wsman
        AllowUnencrypted = true
        Auth
            Basic = true
            Digest = true
            Kerberos = true
```

Creiamo un nuovo listener per il servizio Windows Remote Management che accetta connessioni su HTTP da qualsiasi indirizzo IP (`Address=*`). Questo listener consente la gestione remota del sistema tramite HTTP, senza crittografia.

```
winrm create winrm/config/Listener?Address=*+Transport=HTTP
```

Nella maggior parte dei casi il comando restituisce un errore in quanto il servizio crea di default il proprio listener HTTP, in tal caso ignoriamo l'errore e procediamo con il comando `winrm enumerate winrm/config/Listener` per avere l'enumerazione dei listener.

```
PS C:\Windows\system32> winrm create winrm/config/Listener?Address=*+Transport=HTTP
winrm : WSManFault
In riga:1 car:1
+ winrm create winrm/config/Listener?Address=*+Transport=HTTP
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (WSManFault:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

    Message
        ProviderFault
            WSManFault
                Message = Servizio WS-Management: impossibile eseguire l'operazione di configurazione. Esiste già un listener configurato con
Indirizzo=* e Trasporto=HTTP. È necessario eliminare il listener esistente prima di crearne uno con gli stessi valori di Indirizzo e Trasporto.
Numero errore:  -2144108493 0x80338033
Servizio WS-Management: impossibile creare la risorsa. Risorsa già esistente.
```

```
PS C:\Windows\system32> winrm enumerate winrm/config/Listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 169.254.4.249, 169.254.19.158, 169.254.108
.185, 192.168.56.1, ::1, fe80::22f:7d9a:37d1:145e%3, fe80::3f03:419c:bc
8528:7b01:9c9f%17, fe80::c240:ee9b:b492:f970%23, fe80::cbf9:4c75:5b68:c
```

Enumerazione del listener

Configurazione WinRM – Computer Client

Similmente alla configurazione del server, configuriamo il client WinRM per consentire la comunicazione non criptata ed abilitiamo l'autenticazione di base per il client WinRM.

```
Set-Item -Path WSMan:\localhost\Client\AllowUnencrypted -Value $true
Set-Item -Path WSMan:\localhost\Client\Auth\Basic -Value $true
```

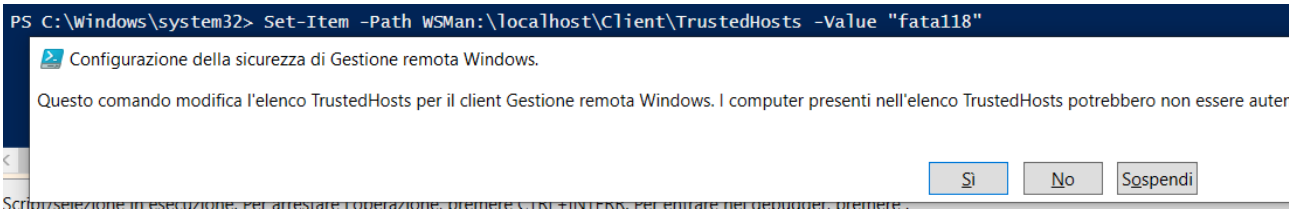
```
PS C:\Windows\system32> Set-Item -Path WSMan:\localhost\Client\AllowUnencrypted -Value $true
PS C:\Windows\system32> Set-Item -Path WSMan:\localhost\Client\Auth\Basic -Value $true
```

Nota: i comandi sopra potrebbero dare problemi di percorso, in tal caso possiamo verificare il percorso visualizzando l'albero delle variabili di Winrm con il comando

```
winrm get winrm/config
```

Aggiungiamo il server all'elenco degli host attendibili per il client WinRM sostituendo "nome_del_server" con il nome della macchina server

```
Set-Item -Path WSMan:\localhost\Client\TrustedHosts -Value "nome_del_server"
```



Possiamo verificare la lista degli host atendibili con il comando:

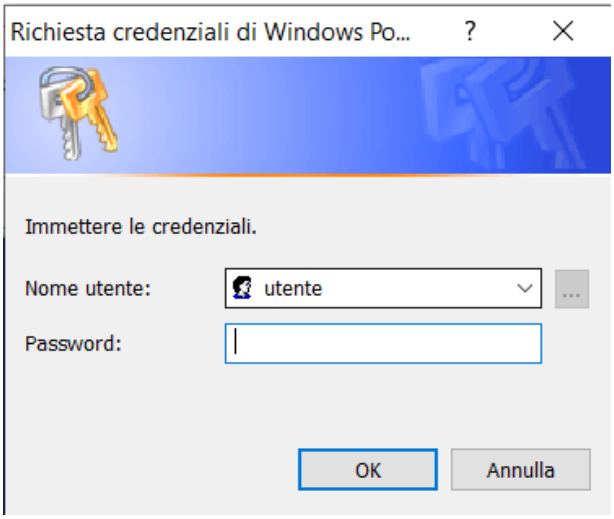
```
Get-Item -Path WSMan:\localhost\Client\TrustedHosts
```

```
PS C:\Windows\system32> Get-Item -Path WSMan:\localhost\Client\TrustedHosts

   WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Client

Type            Name                           SourceOfValue   Value
----            ----                           -------------   -----
System.String   TrustedHosts                                  fata118
```

Ora è tutto pronto per eseguire comandi sul computer remoto, utilizziamo il seguente comando inserendo il nome del computer remoto ed il nome utente. All'interno del parametro `-ScriptBlock` Inseriamo il comando da eseguire sul computer remoto.

```
    Invoke-Command -ComputerName "nome_server" -ScriptBlock { Get-Process } -Credential "nome_utente" -Authentication Basic
```

Si aprirà una finestra che ci chiederà le credenziali della macchina remota, inseriamole e clicchiamo OK




```
PS C:\Windows\system32> Invoke-Command -ComputerName "fata118" -ScriptBlock { Get-Process } -Credential "utente" -Authentication Basic

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName                                 PSComputerName
-------  ------    -----      -----     ------      --  -- -----------                                 --------------
    141       9     2556       8140       0,45    3484   0 AggregatorHost                             fata118
    410      24    10712      31552       0,11    5108   4 ApplicationFrameHost                       fata118
    373      22   500344      40256       0,53    6972   0 audiodg                                    fata118
    207      12     2836      11588       0,38    6800   4 AutoModeDetect                             fata118
    313      33    17808       2724       0,08   13544   4 backgroundTaskHost                         fata118
    255      17    12056      20404       0,14    2640   4 chrome                                     fata118
    224      15    13572      20204       0,19    3848   4 chrome                                     fata118
   1662      72    86132     175440      74,64    8168   4 chrome                                     fata118
    190      11     6664       8724       0,02    8576   4 chrome                                     fata118
   1303      33   150464     143480     123,28   10936   4 chrome                                     fata118
    379      26   115844     164988     134,61   12336   4 chrome                                     fata118
    397      45   385716     382360      68,84   12536   4 chrome                                     fata118
```