



ANSIBLE

# Ansible para SysAdmin

por

***Phillipe Costa***



127.0.0.1 | CHANGED | rc=0 >>  
Targets Micro\$oft Window\$



A problem has been detected and windows has been shut down to prevent damage to your computer.

## PFN\_LIST\_CORRUPT

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

## Technical information:

\*\*\* STOP: 0x0000004e (0x00000099, 0x00900009, 0x00000900, 0x00000900)



## Requisitos técnicos

- Sistemas Operacionais Windows:
  - Desktops: Windows 8.1+
  - Servidores: Windows Server 2012+
- PowerShell 3.0 ou superior.
- .NET Framework 4.0 ou superior.
- **WinRM** previamente configurado e habilitado.

Importante: Alguns módulos podem solicitar versões específicas de SO ou PowerShell. Consulte a documentação oficial de cada módulo para identificar os requisitos técnicos.

## Requisitos técnicos (Pontos importantes)

- Para Sistemas Operacionais Windows Server 2008 e/ou Windows 7, deve-se atualizar o .NET Framework e PowerShell. Para atualizar, basta executar o script disponível [aqui](#).
- Para Windows Server 2008, deve-se instalar SP2 (Service Pack). Já para Windows 7, deve-se instalar o SP1.

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Url = "https://raw.githubusercontent.com/jborean93/ansible-windows/master/scripts/Upgrade-PowerShell.ps1"
$file = "$env:temp\Upgrade-PowerShell.ps1"
$username = "Administrator"
$password = "Password"
```

```
(New-Object -TypeName System.Net.WebClient).DownloadFile($Url, $file)
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Force
```

```
&$file -Version 5.1 -Username $username -Password $password -Verbose
```

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

```
$reg_winlogon_path = "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon"
Set-ItemProperty -Path $reg_winlogon_path -Name AutoAdminLogon -Value 0
Remove-ItemProperty -Path $reg_winlogon_path -Name DefaultUserName -ErrorAction SilentlyContinue
Remove-ItemProperty -Path $reg_winlogon_path -Name DefaultPassword -ErrorAction SilentlyContinue
```

# WinRM

## Windows Remote Management



## WinRM

- WinRM é um protocolo de gerenciamento remoto utilizados em SO Micro\$oft Window\$ Server 2012+ e Windows 8.1+ (nativamente).
- O Ansible utiliza-se de um plugin do Python conhecido como **pywinrm** para se comunicar com seus targets Microsoft. Para realizar a instalação deste plugin, basta executar **pip3 install "pywinrm>=0.3.0"**.
- Por padrão, o WinRM permite conexões oriundas apenas de usuários administradores (locais/domínio).
  - Para ajustar os privilégios de conexões, execute o comando **configSDDL default** no PowerShell.



## WinRM

- O serviço por padrão é executado nas portas 5985 (HTTP) e/ou 5986 (HTTPS).
- Para validar se o serviço encontra-se em execução, basta utilizar `netstat -nop tcp` e/ou `winrm enumerate winrm/config/Listener` no PowerShell.
- No arquivo de inventário do Ansible, deve-se utilizar as variáveis abaixo (mínimo necessário) para definir o tipo de conexão:


- `ansible_winrm_scheme`: http | https
- `ansible_port`: 5985 | 5986
- `ansible_winrm_server_cert_validation`: ignore | validate



## WinRM

- Pontos importantes:
  - Por padrão, o WinRM apresenta falha quando executado sem a utilização de criptografia (TLS sobre HTTP = HTTPS).
  - Em um ambiente com domínio Microsoft, pode-se utilizar o **Active Directory Certificate Service** para emissão de certificados auto assinados.
  - Caso HTTPS não seja uma opção, o HTTP pode ser utilizado quando a autenticação for através dos protocolos NTLM, Kerberos e/ou CredSSP. Para isso, é necessário adicionar a variável **ansible\_winrm\_message\_encryption=always** nos targets do inventário.
  - Para criptografia das mensagens via HTTP, é necessário o plugin **pywinrm >= 0.3.0**.

```
ok: [localhost] => {  
    "output.stdout_info": [  
        'Obrigado e até a próxima aula'  
    ]  
}
```

A decorative network diagram at the bottom of the slide, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and white, set against a dark blue background.