



PowerShell Remoting - Installing and Troubleshooting in a Multiplatform Environment

OpenSSH

Anthony E. Nocentino and Richard Siddaway



Anthony E. Nocentino

Consultant and Trainer

Founder and President of Centino Systems

Specialize in system architecture and performance

Microsoft MVP - Data Platform - 2017-2018

Linux Foundation Certified Engineer

Microsoft Certified Professional

email: aen@centinosystems.com

Twitter: [@nocentino](https://twitter.com/nocentino)

Blog: www.centinosystems.com/blog

Pluralsight Author: www.pluralsight.com





Agenda

- Installing OpenSSH on Windows and Linux
- Authenticating Users
- Setting Up PowerShell Remoting on Windows and Linux
- Troubleshooting OpenSSH



Installing OpenSSH on Windows and Linux

Yea, seriously...OpenSSH on Windows!



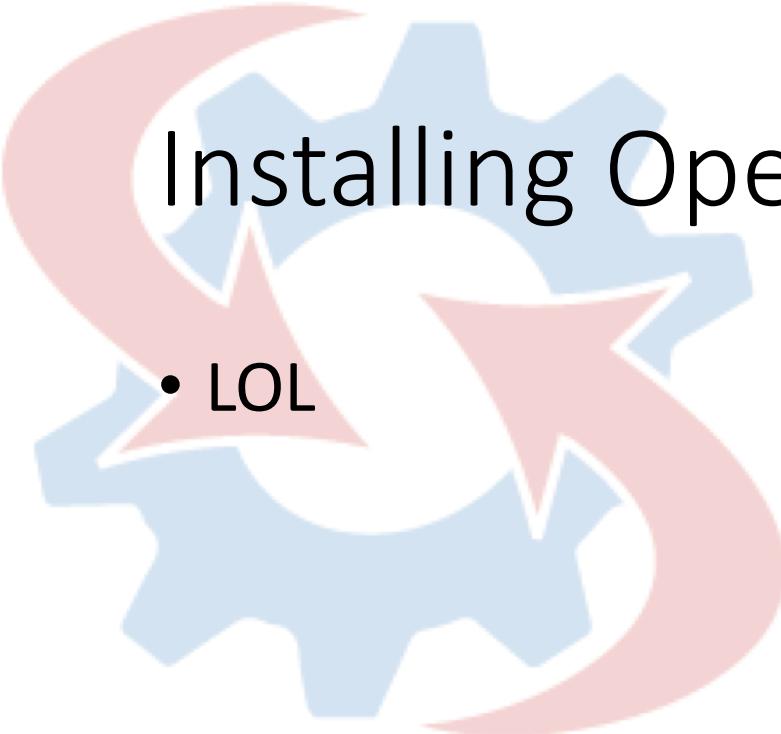
Key OpenSSH Functionality

- Secure client to server communication
- Remote command execution
- Secure file copy
- Tunneling of arbitrary TCP Services (firewall evasion)
- Ensures remote system is who it says it is
- Message Integrity



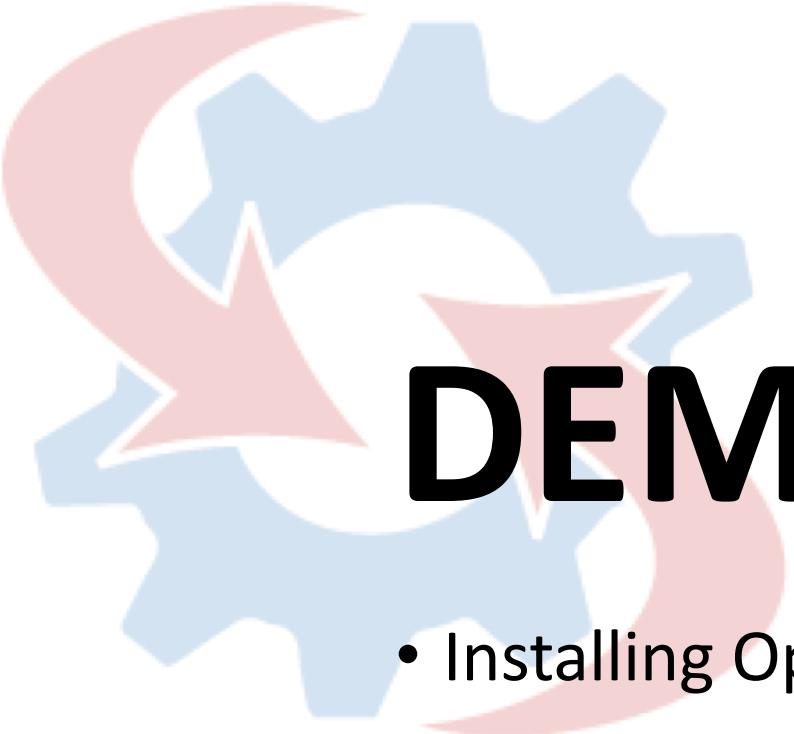
Installing OpenSSH on Windows

- PowerShell team managed GitHub project
 - <https://github.com/PowerShell/Win32-OpenSSH/wiki/Install-Win32-OpenSSH>
 - Gonna get your hands dirty
- Windows Feature
 - Fall Creators Update and Windows Server 1709
 - <https://blogs.msdn.microsoft.com/powershell/2017/12/15/using-the-openssh-beta-in-windows-10-fall-creators-update-and-windows-server-1709/>
 - Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
 - Has a utilities module to help with some permissions issues with StrictModes
- Windows Services for Linux
- Windows Server 2019...



Installing OpenSSH on Linux

- LOL



DEMO

- Installing OpenSSH on Windows Server 2016
- DC1 – Domain Controller
- CENTOS-W1 – Linux management workstation
- CENTOS-S1 – Linux server
- WINDOWS-S1 – Windows server



Authentication Methods

Getting your users on your servers!



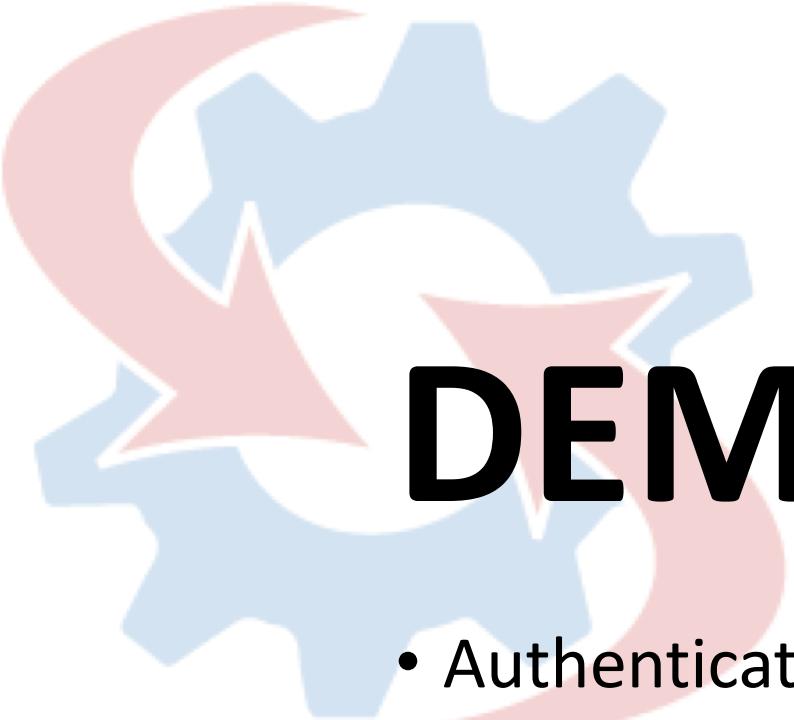
Authentication Methods

- GSSAPI – Kerberos
- Host based - based on which client
- Public key – based on a per user key pair
- Challenge response – two factor
- Password – p4ssword?
- Processed in this order at login



Authenticating Users

- Local user account databases
 - On Windows
 - On Linux
- Active Directory Authentication
 - Can be used on Windows and Linux
 - LDAP – User lookup
 - Kerberos – user and host authentication
 - System Security Services Daemon (SSSD) – brokers the deal for auth & user lookup
- **aen@lab.centinosystems.com@centos-s1**



DEMO

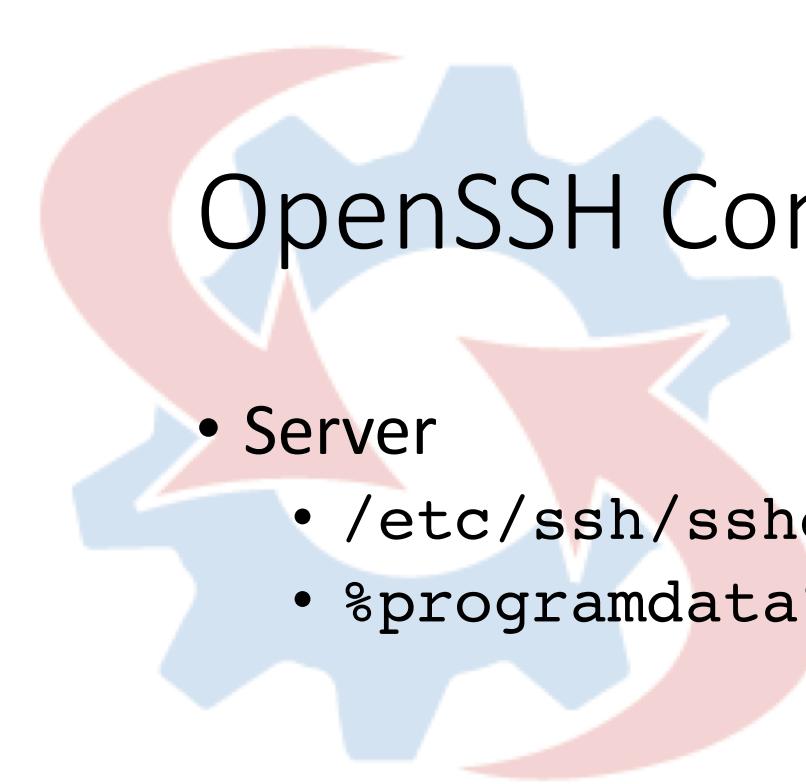
- Authenticating users with user keys
- Configuring user authentication via Active Directory
- Combining AD and key based authentication



Setting Up PowerShell Remoting on Windows and Linux

I can do what???



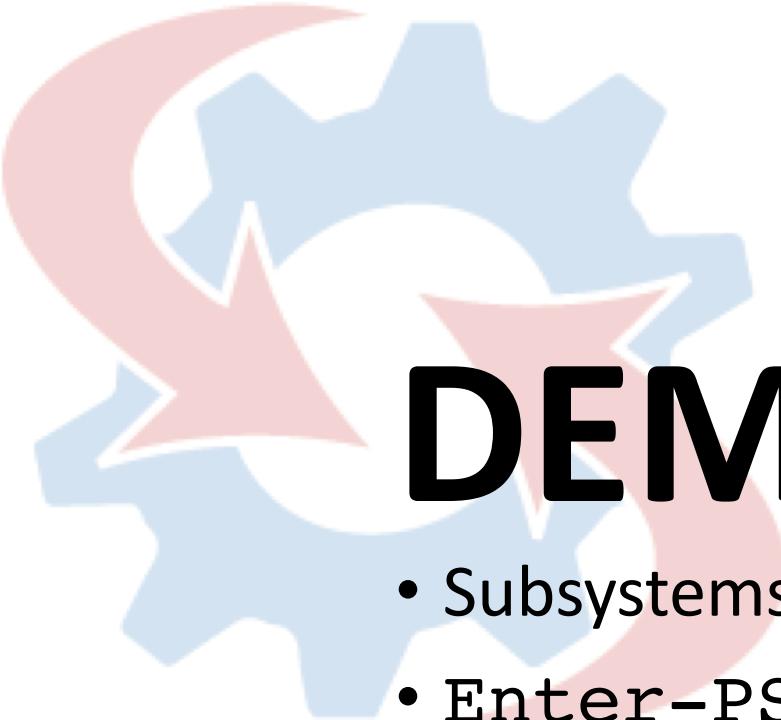


OpenSSH Configuration

- Server
 - `/etc/ssh/sshd_config`
 - `%programdata%/ssh/sshd_config`

PowerShell Core and Subsystems

- PowerShell Core
 - Subsystem `powershell c:/program files/powershell/6.1.0-preview.1/pwsh.exe -sshs -NoLogo -NoProfile`
- PowerShell as a subsystem
 - `C:\Program Files\PowerShell\6.1.0-preview.1\pwsh.exe` (whoa...slashes)
 - `/usr/local/bin/pwsh`
 - `/bin/pwsh`



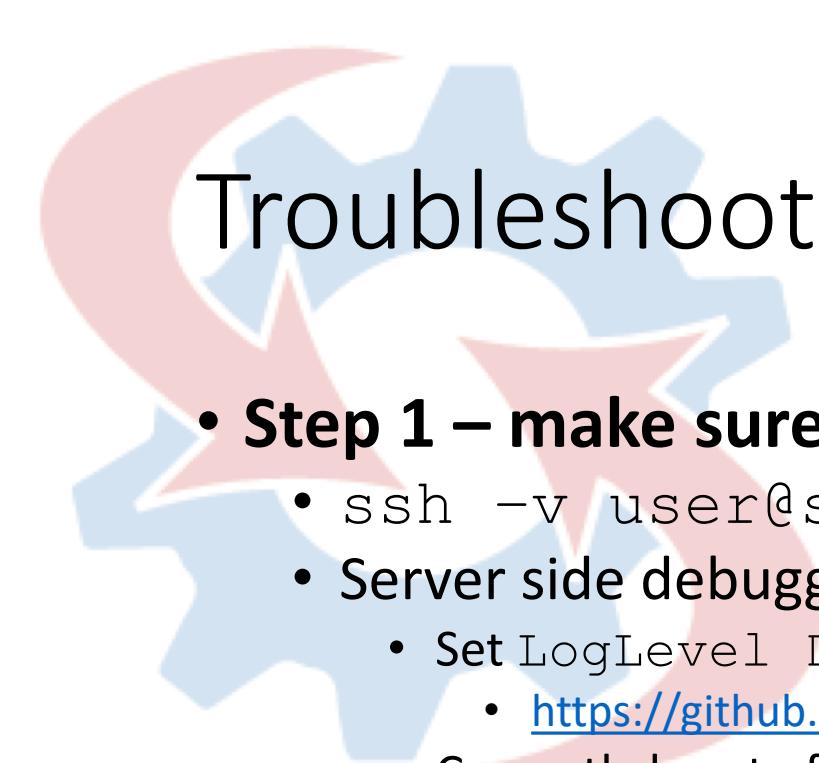
DEMO

- Subsystems
- Enter-PSSession
 - Key based authentication
 - Active Directory authentication



Troubleshooting OpenSSH

Why doesn't this &*%^E)@#! work??!!?



Troubleshooting

- **Step 1 – make sure SSH works!**
 - ssh -v user@servername
 - Server side debugging on Windows hosts
 - Set LogLevel DEBUG3 in sshd_config
 - <https://github.com/PowerShell/Win32-OpenSSH/wiki/Troubleshooting-Steps>
 - Currently logs to files. Logs to ETW in 7.6.1.0
 - <https://github.com/PowerShell/Win32-OpenSSH/wiki/Logging-Facilities>
- Host key mismatch
- Permissions on authorized_keys because of StrictModes
- No Subsystem Configured
 - PowerShell client will yell at you when you try it...

More data?

- Come see me in room 403!
- Email: aen@centinosystems.com
- Twitter: [@nocentino](https://twitter.com/nocentino)
- Blog: www.centinosystems.com/blog
- LFCE: Network and Host Security
 - OpenSSH
 - Copying files, remote command execution and tunneling TCP
- Understanding and Using Essential Tools for Enterprise Linux 7
 - Installation, command execution, bash basics, file system and permissions

THANK YOU!

Please use the event app or Sched.com to submit a session rating!

