
Reverse Proxy OS Configuration

v. 15.0.1-SNAPSHOT

User Guide

Table of Contents

Table of Contents	i
1. Introduction	1
2. Prerequisites	2
3. Usage	3
4. Changelog	4

1 Introduction

Various OS hardening configurations for reverse proxy host. OS configurations include:

- Kernel hardening aka sysctl configs
- IPTables rules
- Logrotate config - *Don't configure log rotation if reverseproxy is installed via installer as log rotation will be taken care of by the installer*

OS supported:

- CentOS 7

2 Prerequisites

- OS must be CentOS 7
- `logrotate` must be installed on the host. Install with `yum install logrotate -y` command.
- Uninstall or stop `firewalld` service on cent os
 - `sudo systemctl stop firewalld`
 - `sudo systemctl disable firewalld`
 - `sudo systemctl mask --now firewalld`
- `iptables` service must be installed. Install with below commands:
 - `sudo yum install iptables-services -y`
 - `sudo systemctl start iptables`
 - `sudo systemctl enable iptables`

3 Usage

Installer script is provided to automatically install all the configurations required. Various options can be provided to the script to control what all should be installed/configured.

```
USAGE: ./install_os_settings.sh [OPTIONAL_ARGS]
OPTIONAL_ARGS: -k -l -i -p <source-ip1> -p <source-ip2> ... -s <interface1> -s <int
-k: configure kernel hardening
-l: configure logrotate for given log directory
-i: configure iptables
-p: allowed source ip for ICMP ping messages. By default ICMP ping is blocked for a
-s: network interface name to allow SSH access to. By default ssh access is blocked
-r: disable rate limits for a source-ip on an interface. Provide value as INTERFACE

Example usage: ./install_os_settings.sh -k -l ~/reverse_proxy/proxy25.autobot.cvp/1
```

4 Changelog

v 12.6.2

- Initial release