Mandiant

SUDO COMMANDS EXPLAINED - ACTOR

When you install any Security Validation components using installable software, part of the install process is to add a Sudoers file that includes access information and aliases. When you enable sudoers during installation, this file is created and is located at `/etc/sudoers.d/` .

- Enabling sudoers is preferred. If you do not enable it, or if it is inadvertently modified, a copy is backed up in /opt/apps/verodin/node/settings/verodin_sudoers.
- The sudoers file is dynamically created. The comments in this version are to provide context and are not included in the actual file.

```
Cmnd_Alias VERODIN_REMOVE_ROUTES = /bin/rm /etc/sysconfig/network-scripts/route-*# Used for updating interface
s
Cmnd_Alias VERODIN_REMOVE_RULES = /bin/rm /etc/sysconfig/network-scripts/rule-*# Used for updating interfaces
Cmnd_Alias VERODIN_REMOVE_LOGS = /bin/rm /opt/apps//node/log/_*# Used to clear out our log data
Cmnd_Alias VERODIN_UPDATE_HOSTNAME = /bin/tee /etc/hostname# Used to control the hostname configuration
Cmnd_Alias VERODIN_UPDATE_IFCFGS = /bin/tee -a /etc/sysconfig/network-scripts/ifcfg-*# Used for updating interface
s
Cmnd_Alias VERODIN_IODINE_TUNNEL = /opt/apps//node/ext/iodine/bin/*# Needed to run the DNS tunnel actions
Cmnd_Alias VERODIN_HANS_TUNNEL = /opt/apps//node/ext/hans-master/hans# Needed to run the ICMP tunnel action
s
nodeone ALL=(ALL) NOPASSWD: VERODIN_HANS_TUNNEL, VERODIN_IODINE_TUNNEL, VERODIN_REMOVE_ROUTES, V
ERODIN_REMOVE_RULES,
VERODIN_UPDATE_HOSTNAME, VERODIN_UPDATE_IFCFGS, /bin/hostname, /usr/sbin/ifconfig, /usr/sbin/ifdown, /usr/sbi
n/ifup,
/usr/sbin/ip, /sbin/iptables, /sbin/iptables-restore, /bin/netstat, /user/bin/nmcli, /bin/pkill, /usr/sbin/route, /bin/sh,
/bin/printf, /bin/sed, /usr/sbin/shutdown, /bin/ssh-keygen, /usr/bin/sysctl, /bin/systemctl, /bin/rpm, /bin/chown,
/usr/sbin/ntpdate, /sbin/setcap
```

Sudoer Commands Explained

Category	Command	Functionality
Network Management	`/sbin/ifdown`	Used to bring down interfaces when making changes
Network Management	`/sbin/ifup`	Used to bring up interfaces when making changes
Network Management	`/sbin/ifconfig`	Used to turn off unused interfaces when running vsetnet
Network Management	`/bin/sed`	Update the nginx and ssh configurations when the IP address is changed
Network Management	`/sbin/route`	Used to add and delete network routes

Category	Command	Functionality
Network Management	`VERODIN_REMOVE_ROUTES = /bin/rm /etc/sysconfig/network-scripts/route-*`	Used to remove interface related files inside /etc/sysconfig/network-scripts
Network Management	`VERODIN_REMOVE_RULES = /bin/rm /etc/sysconfig/network-scripts/rule-*`	Used to delete interface related files inside /etc/sysconfig/network-scripts
Network Management	`VERODIN_UPDATE_IFCFGS = /bin/tee -a /etc/sysconfig/network-scripts/ifcfg-*`	Used in updating the network interface configurations
Network Management	`VERODIN_UPDATE_HOSTNAME = /bin/tee /etc/hostname`	Used to set the hostname on the system
Network Management	`/user/bin/nmcli`	Used to update network configuration on the system
Firewall Management	`/sbin/iptables`	Used to add and remove individual iptables rules for opening and closing ports as required when the Action is running.
Firewall Management	`/sbin/iptables-restore`	Used to restore the host firewall to a saved configuration from file.
Service Management	`/bin/systemctl`	Used to start, stop, and restart the services running as part of the Actor. Also used to reload services.
Service Management	`/sbin/shutdown`	Used to reboot the Actor after updates and by call from the Director.
Tunnel Actions	`/usr/bin/pkill`	Used to ensure specific processes associated with the SSH tunnel action is shut down
Tunnel Actions	`VERODIN_IODINE_TUNNEL = <prefix_path>/node/ext/iodine/bin/*`	Required to allow the DNS tunnel to bind to reserved port
	`VERODIN_HANS_TUNNEL = <prefix_path>/node/ext/hans-master/hans`	Required to allow the privileged binding for the ICMP tunnel

Category	Command	Functionality
Port Scan Action	`/sbin/sysctl`	Updating kernel parameters to ensure network traffic is passed properly during port scan actions.