SCDRM

Security, configuration, disaster-recovery manager

What is it?

Just a bunch of bash scripts and Ansible playbooks stacking known software into ‘Ansible local agent’ with disaster recovery capabilities. It stacks AIDE, Git, and tlog into a secure configuration change process.

Tested on RHEL(7/8/9) and Debian/Ubuntu.

Targeted audience?

Linux people! Enterprise environments as well as SMBs.

Anyone ever wanting Ansible local agent for Linux.

Anyone looking for a Linux DR manager.

Anyone in need of a strict change process for their Linux infrastructure.

Why would I use it?

To enforce a more secure change process.

To extend Ansible behavior with local agent.

To protect your systems from human made error/disaster.

How to use it?

Get the project and install it:

- Github - https://github.com/klovric/scdrm
- Ansible Galaxy - https://galaxy.ansible.com/klovric/scdrm

Discover what you need, adapt and run in active protection mode.

Programmed function will allow ease of use.

Ask yourself these

1. If someone accidentally removed *‘/etc/passwd’* from your entire Linux infrastructure, how long would it take You to recover? What would the damage be?

2. If you found yourself alone in a room with a military grade secured OFFLINE computer, what would be biggest and most likely security/disaster impact vector or risk?

3. Newly joined junior system admin accidentally removed default route from you systems. Can you fix this fast? Is it fast enough?

4. While working with globally dispersed team, you find yourselves stepping over each other’s toes. How can you force only one person to be able to make configuration changes at a time?

5. Senior admin did a configuration change last minute before logging off and going onto vacation, off grid. This change was not tested properly and causes significant problems to production. Can you revert fast enough what he did?

6. While playing around with Ansible, your coworker accidentally rewritten ‘/bin/bash’ on 100+ production VMs. Can you fix this fast enough?

7. Junior sysadmin is writing a new playbook for checking stuff. He does a typo and the end results are that SSH daemon and network service are stopped on hundreds of production machines. How do you recover from this?

8. Co-worker had made some trouble using parted. You can see that from the shell history, however you don’t see what exactly he typed in. Do you log the stdout and stderr to see what exactly your administrators did?