

Scripting, Automation and Confidential Variables

Document Name :	Scripting, Automation and Confidential Variables
Version :	1.0
Version Date :	13/07/2022
Modified By :	Marc MARTINEZ
Creation Date :	13/07/2022
Created by :	Marc MARTINEZ
Approved by :	Marc MARTINEZ
Confidentiality Level :	INTERNAL

Modification History

	Date	Author	Commentary
1.0	13/07/2022	Marc MARTINEZ	Creation of the document

Introduction

This document will lay out suggestions the Security Team has to improve the Disponibility and the Confidentiality of the system.

We will mostly be talking about the tools ansible and crontab.

Content

Scripting

The Security Team suggests the use of ansible playbooks to create scripts for deployment and redeployment of some system as well as to automate the update process of some systems or reduce the down times of systems in case of incidents through automated responses.

Automation

Scripts that need to be run periodically can be set up using the tool crontab on unix systems.

This tool can be used to run scripts at a set hour, day, period depending on the configuration, it is a simple and robust automation system.

This tool can be used to run saving scripts and make sure the systems are kept up to date by running updates scripts every week or months.

Confidentiality

When using ansible playbooks to execute scripts on remote systems, some environments variables and/or passwords can be used. To prevent potential problems due to the transfer or storage of these important variables, the tool ansible vault can be used.

Ansible vault is an ansible tool that works by storing all of the important variables in a separate file that is encrypted. The file can only be opened and modified by using a passphrase.

This method does not leave the important variables in plain text in the ansible playbooks.

Tools suggested and required budget

- ansible (free)

- ansible vault (free)
- crontab (free)
- Three (3) days of man hours (2400 €)