Samuel Hasert
769806

Setup und Deployment eines neuen Loghosts

Motivation

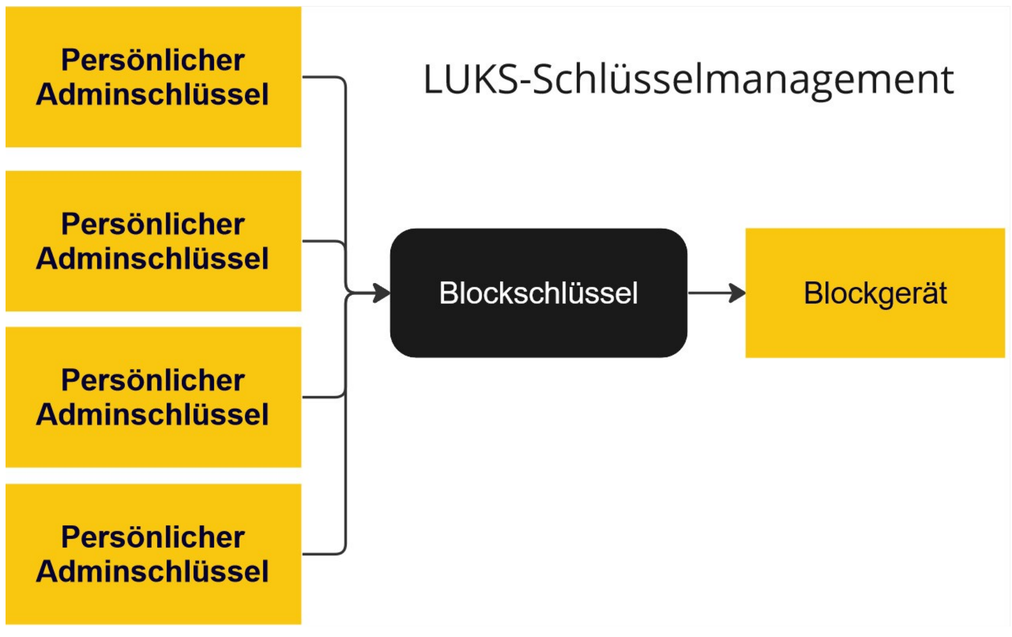
- Ein neuer Loghost wurde für die Abteilung CIT benötigt, aufgrund gestiegener Anforderungen an Datensicherheit, Performance und Loganalysefähigkeit.
- Rollebasierte Zugriffskontrolle wurde benötigt, um sicherzustellen, dass Administratoren nur auf die für sie freigegebenen Logs zugreifen können.
- Der bestehende Loghost sollte abgelöst werden.

Physische Datensicherheit:
Nach Ablauf der Lebensdauer einer Festplatte muss sie und die darauf enthaltenen Daten zerstört werden. Nun sollte die zu benutzenden Maschine verschlüsselt werden. Dadurch können Festplatten, welche ihre Lebensdauer durchlaufen haben ohne Sorgen wiederverwertet oder entsorgt werden.

Es sollen nach kompletter Umschaltung syslogs von etwa **1000** Linux-Maschinen, Switches und Routern verwaltet werden.

Chef

- Chef ist ein Konfigurationsmanagementsystem.
- Die GSI IT verwendet Chef zur Verwaltung der Linux-Server und -PCs.
- Lokale Agenten befragen periodisch einen zentralen Server nach ihrem gewünschten Zustand, führen ggf. Anpassungen aus und melden die Ergebnisse an den zentralen Server zurück.
- Änderungen werden nur vorgenommen, wenn Maschinen vom Soll-Zustand abweichen.
- Chef abstrahiert einen Großteil der Linuxinfrastruktur in Code.
- Chef stellt Cookbooks zur Verfügung, um systemübergreifende Funktionen bereitzustellen.
- Ein Cookbook enthält Rezepte, Attribute, benutzerdefinierte Ressourcen, Dateien und Vorlagen.
- Die Chef Infra-Sprache basiert auf Ruby und bietet umfassende Konfigurationsmöglichkeiten für Betriebssysteme.



Rsyslog

- Rsyslog ist eine Open-Source-Software für UNIX, welche Log-Nachrichten in IP-Netzwerken weiterleitet.
- Sie implementiert das Syslog-Protokoll und erweitert es um zahlreiche Filterfunktionen.
- Für das Projekt wurde der Empfang von Logs unverschlüsselt per UDP und TCP als auch verschlüsselt per TLS implementiert (RFC 5425).
- So können die unterschiedlichen Dienste (sowohl bei GSI als auch remote) je nach technischen Anforderungen und Fähigkeiten ihre Log-Nachrichten an den Loghost schicken.

```
'34-mattermost' => {
      templates: {
        'MattermostAll' =>
'/srv/rsyslog/services/mattermost/mattermost.log'
      },
      group: 'lx-web',
      actions: [
        "if $programname == 'mattermost' then ?
MattermostAll"
      ]
    },
```

```
luks_key '<name-of-device>' do
  passphrase '<passphrase>'
  [action :remove/:add]
  end
end
```

LUKS

- LUKS ist ein System zur Verschlüsselung von Speichermedien auf Linux-Computern.
- Es ermöglicht die Verschlüsselung beliebiger Inhalte, einschließlich Dateisystemen und Swap-Partitionen.
- Der veschlüsselte Header am Anfang eines verschlüsselten Volumens speichert bis zu 32 Zugangsschlüssel.
- Zusätzlich werden Verschlüsselungs-parameter wie Typ und Schlüsselgröße gespeichert.
- Ein selbstentwickeltes Cookbook wurde verwendet, um LUKS Schlüssel automatisiert anzulegen und zu entfernen.
- Das LUKS-Cookbook verwaltet individuelle Schlüssel für Administratoren, welche beim Verlassen des Teams invalidiert werden.

Als Open-Source auf Github veröffentlicht:
https://github.com/GSI-HPC/luks-chef-cookbook

h_da hochschule darmstadt informatik
member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY
GSI

Praxisprojekt 2
Informatik Dual
2024

Gruppe A