

Credential Management Ansible

Studiengang: BSc in Informatik
Betreuer: Prof. Dr. Benjamin Fehrensen
Experte: Cyrill Brunschwiler

Im Bundesamt für Informatik und Telekommunikation (BIT) wird die Automatisierungsumgebung im Storage Team auf Ansible umgestellt. Im Rahmen der Arbeit wurden diese Umgebung sicherheitstechnisch anhand des NIST-Standards und des IT-Grundschutzes analysiert. Dabei wurde die Problemstellung ganzheitlich angegangen, beginnend mit der Identifikation und Akzeptanz von Risiken gemäss ISO 27001 Zertifizierung bis hin zur Umsetzung der Sicherheitslösungen und deren Bewertung.

Ziel

Ziel dieser Arbeit ist es, die neu aufgebaute Ansible Umgebung sicherheitstechnisch zu analysieren, Problematiken zu erkennen, einzuordnen und Lösungen umzusetzen. Die umgesetzten Lösungen werden kritisch hinterfragt und beurteilt mithilfe von dem NIST Standard und IT-Grundschutz, um die bestmöglichen Ergebnisse zu erzielen. Sicherheit soll gewährleistet werden, jedoch darf kein grosser Mehraufwand für das Storage Team entstehen und die ausgearbeiteten Lösungen müssen den Richtlinien und Gegebenheiten des BIT entsprechen.

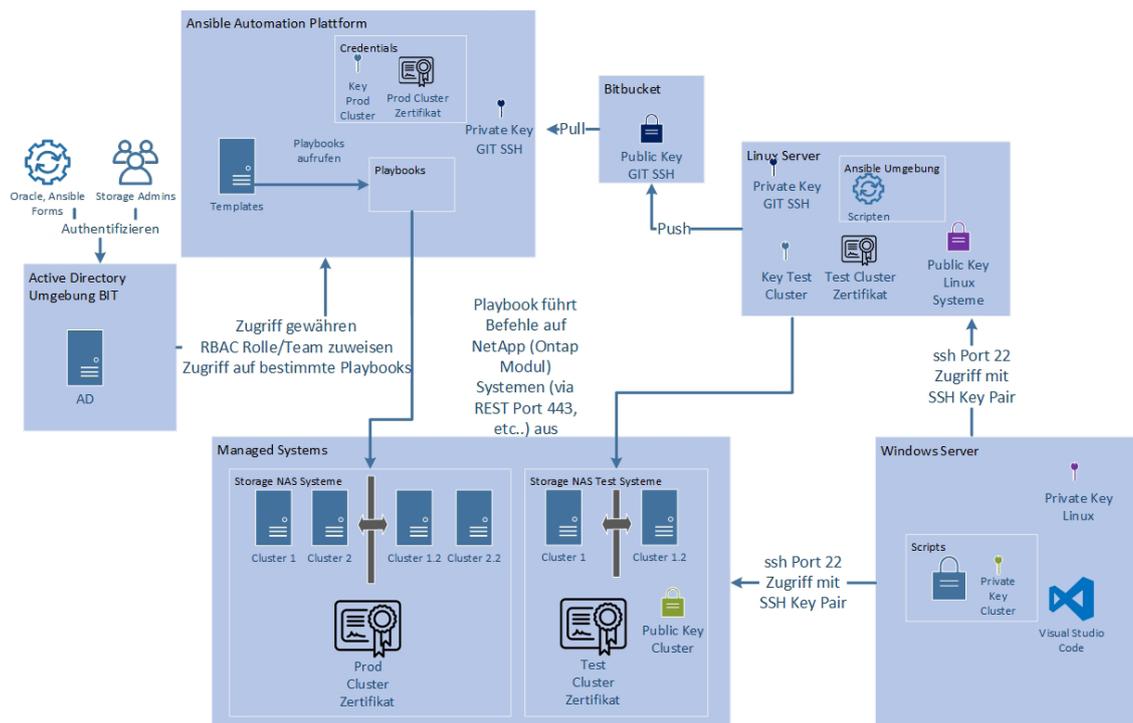
Umsetzung

Die initiale Analyse ergab, dass die Umgebung in drei Hauptthemen strukturiert werden kann. Jeder dieser Themenbereiche wurde durch spezifische Lösungsansätze adressiert. Das Hauptziel lag darin, von der

Verwendung von lokalen User/Passwort auf Passwortless oder Föderation umzusteigen. Ein grosser Gewinn wurde durch die Eliminierung lokaler Benutzerverwaltung und deren Integration in die AD-Benutzerverwaltung durch Föderation erzielt. Dies führt zu einer Zentralisierung der Zugriffslogs und einem integrierten Audit-Trail. In anderen Abschnitten, wo die Authentifizierung mittels Kerberos nicht möglich ist, konnte von der Verwendung von lokalen Usern auf SSL-Certificate-based Authentifizierung umgestiegen werden. Zudem wurden SSH Zugriffe mithilfe von SSH Key Pairs verbessert. All diese Änderungen konnten erfolgreich umgesetzt, anhand des NIST-Standards und IT-Grundschutzes analysiert sowie bewertet werden. Insgesamt konnte in allen Bereichen die Sicherheit erhöht und die Verwaltung der Umgebung erheblich vereinfacht werden.



Nathalie Aeby
IT Security



Übersicht der Umgebung nach Anpassungen