Ubuntu Desktop in Azure als zukünftiger Entwicklerarbeitsplatz

Studiengang: BSc in Informatik
Vertiefung: Digital Business Systems
Betreuer: Prof. Hansjürg Wenger
Experte: Dr. phil. nat. Igor Metz (Glue AG)

Die Schweizerische Post braucht für externe Entwickler schnell verfügbare, sichere und einheitliche Arbeitsplätze. Eine zentral verwaltete Ubuntu-Desktop-Umgebung in Azure bietet dafür eine ideale Basis: modern, gut automatisierbar und nah an produktiven Linux-Servern.

Einleitung

In der Schweizerischen Post verursachen Windows-VMs für externe Entwickler durch manuelle Prozesse und unnötige Lizenzen hohe Kosten und lange Wartezeiten. Es fehlt eine automatisierte, kostengünstige Linux-Alternative.

Technische Umsetzung

Die Lösung setzt konsequent auf etablierte Cloud-Werkzeuge. Die Infrastruktur in Azure wird mit Terraform automatisiert bereitgestellt. Ubuntu 24.04 LTS dient als Basis für die Entwickler-Desktops und wird mit Ansible gehärtet und vor konfiguriert. Für die zentrale Authentifizierung kommt Microsoft Entra ID zum Einsatz, während der Authentifizierungsdienst authd auf den VMs die Anmeldung gegen Entra ID integriert. Der Remote-Zugriff erfolgt über Azure Bastion und RDP, sodass die Desktops ohne öffentliche IP-Adressen betrieben werden können.

Zugriffs- und Netzwerkflüsse

Benutzer verbinden sich über ein CLI mit Azure Bastion, das einen HTTPS-Tunnel aufbaut und darüber RDP-Sitzungen zu den Ubuntu-Desktops vermittelt. Admins greifen getrennt davon per Ansible SSH auf die VMs zu. AppArmor, CIS-Benchmarks und ein restriktives Snap-basierendes Softwaremodell begrenzen die Angriffsfläche zusätzlich.

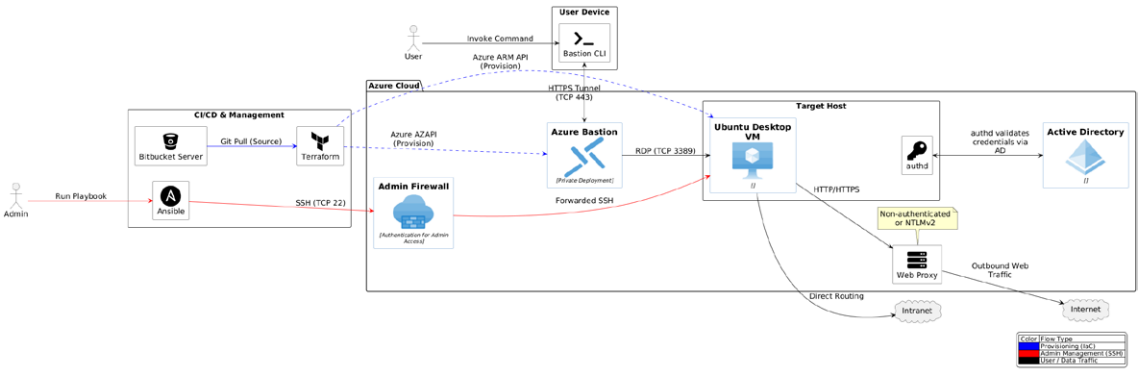
Integration in die Systemlandschaft der Post und Nutzen

Die VDI-Lösung fügt sich in die bestehende Infrastruktur der Schweizerischen Post ein, indem sie Bitbucket als zentrales Git-Repository, Terraform und Ansible für Workflows und die vorhandenen Proxy-Dienste nutzt. Neue Entwicklerarbeitsplätze lassen sich damit reproduzierbar ausrollen und über Playbooks warten. Für die Post entsteht ein mehrfacher Nutzen: standardisierte, Linux-nahe Entwicklungsumgebungen für externe Entwickler, reduzierte Betriebs- und Onboarding-Aufwände durch Automatisierung sowie eine klar kontrollierte, compliance-konforme Zugriffskette von der Identität über das Netzwerk bis zum einzelnen Desktop.

Ausblick

Künftig soll die VDI-Architektur so erweitert werden, dass der Zugriff kontrolliert auch von außen möglich ist, ohne das Sicherheitsniveau zu senken. Zudem wird die Konfigurations- und Update-Automatisierung von lokalen Playbooks auf einen zentral betriebenen Ansible Tower ausgelagert, um Wartung und Betrieb der Umgebung einfacher und besser skalierbar zu machen.

Silvio Davide Geismar
silvio.geismar@hotmail.com



Aufbau der Infrastruktur und Zugriffsfluss auf die Entwicklermaschinen