DMOOVE

AWS Landing Zone

Der Grundstein für sichere und skalierbare Cloud-Infrastrukturen

Yannick Tresch

DMoove Solutions GmbH

yannick.tresch@dmoove.com

Überblick

DMOOVE

Die DMoove

- Einleitung
- Was ist eine Landing Zone?
- Wozu eine Landing Zone?
- Komponenten einer Landing Zone
- Landing Zone bereitstellen
- Die Accounts einer Landing Zone

Einleitung

DMOOVE

DMoove

- Cloud Consulting
- Managed Services
  - DevOpsTools
  - Monitoring
- Kostenoptimierung on AWS
  - Up to 55% savings on EC2
- Partner: AWS, GitLab, Centreon, Microsoft

Was ist ein AWS Account?

DMOOVE

Account Modelle

Ein AWS-Account

100e von AWS-Accounts

1000e von AWS-Accounts

Wieso ein Account nicht genug ist

- Verschiedene Teams
- Isolation von Ressourcen
- Security & Compliance
- Berechnung von AWS-Consumption
- Geschäftsprozesse

Was ist eine Landing Zone?

Landing Zone

Eine Landing Zone ist eine Multi-Account AWS-Umgebung.

Sicher.

Skalierbar.

Gut strukturiert.

Wozu eine Landing Zone?

Schwierigkeiten ohne Landing Zone

- Unstrukturierte und unkoordinierte AWS-Konten und Ressourcen.
- Mangelnde Skalierbarkeit und effizientes Ressourcenmanagement.
- Schwierigkeiten bei der Implementierung konsistenter Sicherheitsrichtlinien.
- Erhöhtes Risiko von Sicherheitsverletzungen und Datenlecks.
- Eingeschränkte Transparenz und Kontrolle über AWS-Ressourcen.

Vorteile einer Landing Zone

- Strukturierte und koordinierte AWS-Konten und Ressourcen ermöglichen eine effiziente Verwaltung und Organisation von Workloads und Anwendungen.
- Durch vordefinierte Architekturmuster und Best Practices wird eine skalierbare Infrastruktur geschaffen, die mit dem Wachstum des Unternehmens mithalten kann.
- Die Landing Zone bietet eine zentrale Kontrolle und einheitliche Sicherheitsrichtlinien für alle AWS-Ressourcen, was die Sicherheit erhöht und Compliance-Anforderungen erfüllt.
- Automatisierte Bereitstellungsprozesse und Konfigurationsmanagement erleichtern die schnelle und reibungslose Implementierung von Workloads und Anwendungen.
- Durch die zentrale Überwachung und Transparenz über alle Ressourcen hinweg können Engpässe erkannt, Ressourcen optimiert und Kosten kontrolliert werden.

Komponenten einer Landing Zone

DMOOVE

Account Vending Machine

- Automatisiertes Erstellen von Konten für Benutzer
- Vereinfacht den Zugriff auf verschiedene Ressourcen
- Reduziert manuelle Einrichtungsprozesse
- Stellt sicher, dass Konten den erforderlichen Sicherheitsstandards entsprechen
- Ermöglicht effiziente Verwaltung von Benutzerzugriffen

Netzwerk-konnektivität

- Sichert eine sichere und zuverlässige Kommunikation zwischen Ressourcen
- Implementiert Netzwerkrichtlinien und Firewalls
- Stellt eine sichere Verbindung zu externen Netzwerken her
- Überwacht und sichert den Netzwerkverkehr
- Optimiert die Leistung und Skalierbarkeit der Infrastruktur

Sicherheits-überwachung und -steuerung

- Überwacht kontinuierlich potenzielle Sicherheitsbedrohungen
- Implementiert Sicherheitsrichtlinien und Zugriffskontrollen
- Identifiziert und reagiert auf Sicherheitsvorfälle
- Gewährleistet die Einhaltung von Compliance-Standards
- Verhindert unbefugten Zugriff auf Ressourcen

DMOOVE

Kosten-optimierung und Ressourcen-management

- Überwacht und analysiert den Ressourcenverbrauch
- Identifiziert ineffiziente Ressourcennutzung
- Optimiert Kosten und Ressourcenallokation
- Verwaltet und optimiert Lizenzen und Abonnements
- Bietet Transparenz und Kontrolle über die Infrastrukturkosten

Landing Zone bereitstellen

Arten von Landing Zones

Control Tower

Customized Landing Zone

DMOOVE

Control Tower

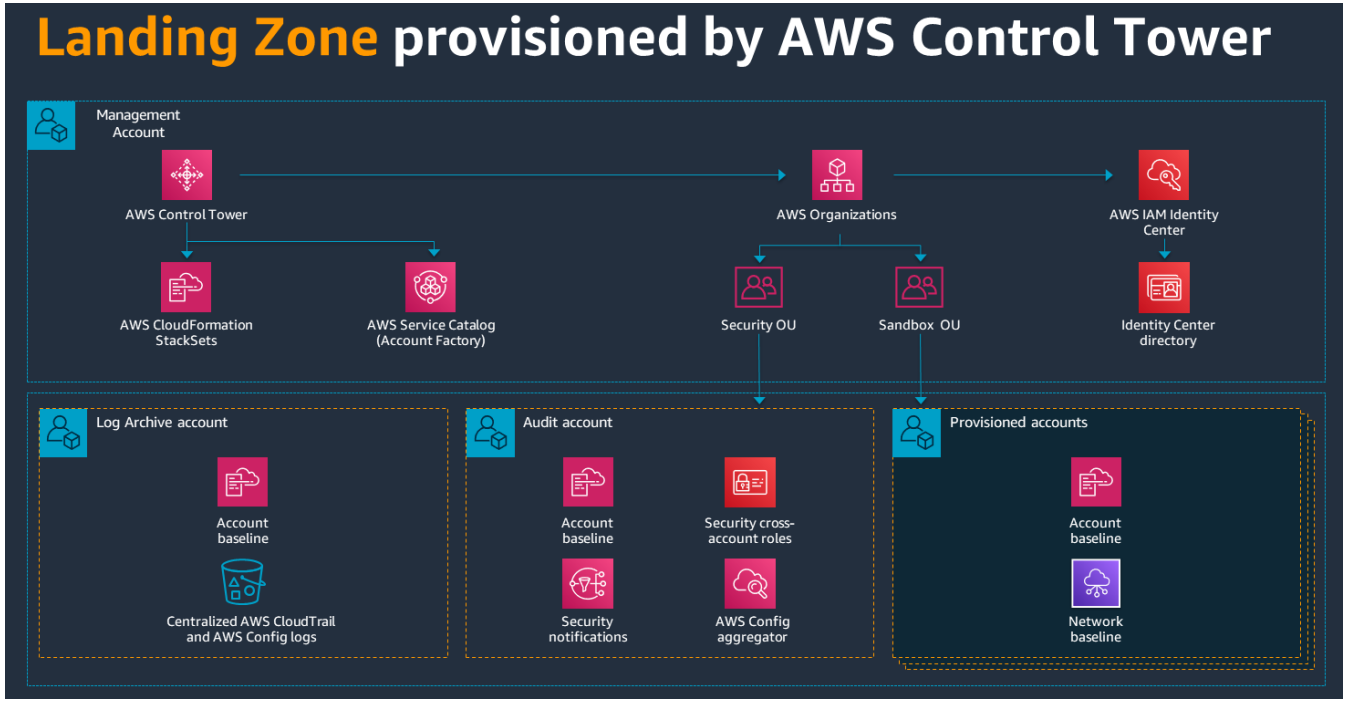
Vollständig verwalteter Service

AWS-bereitgestellte Guardrails und standardmäßig angewandte Compliance-Richtlinien

Zentrales Dashboard für Überwachung und Compliance-Status

Account Factory für die Bereitstellung neuer Konten

Control Tower



Customized Landing Zone

- Maßgeschneiderte Lösung für individuelle Anforderungen.
- Implementierung der Basisumgebung für umfassende Kontrolle.
- Flexibilität zur Anpassung aller Umgebungskomponenten.
- Notwendige Fachkenntnisse zur Verwaltung und Wartung erforderlich.
- Vollständige Kontrolle über Identitätsmanagement, Governance und Sicherheit.

Die Accounts einer Landing Zone

DMOOVE

Master Account

Der Master Account ist das zentrale Steuerungselement.

Er fungiert als oberstes Administrationskonto in der AWS-Organisation.

Er hat die höchsten Berechtigungen und Kontrollmöglichkeiten.

Über den Master Account werden alle anderen AWS-Konten verwaltet.

Er ermöglicht die Verwaltung von Abrechnung, Zugriffssteuerung und Ressourcenbereitstellung.

Log Archive

Es dient als zentraler Speicherort für Logdaten aller anderen AWS-Konten.

Das Log Archive ermöglicht eine zentrale Überwachung und Analyse von Loginformationen.

Es unterstützt die Einhaltung von Sicherheitsstandards und Auditing-Anforderungen.

Durch die zentrale Speicherung und Analyse können Bedrohungen und Anomalien schneller erkannt und behoben werden.

Network

Er ist verantwortlich für die Netzwerkinfrastruktur und -konfiguration.

Der Network Account ermöglicht eine zentrale Verwaltung von Netzwerkressourcen wie VPCs und Subnetze.

Er unterstützt die Implementierung von Sicherheitsrichtlinien und Netzwerkarchitekturen.

Durch die Trennung von Netzwerkressourcen in einem eigenen Account wird eine klare Abgrenzung und Kontrolle ermöglicht.

DMOOVE

Shared Services

Er stellt gemeinsam genutzte Dienste und Ressourcen für andere Konten bereit.

Der Shared Services Account bietet zentrale Funktionen wie Authentifizierung, Benutzerverwaltung oder Logging.

Er ermöglicht die standardisierte Bereitstellung und Verwaltung von Diensten für andere Konten.

Durch die Trennung von gemeinsam genutzten Diensten in einem eigenen Account wird eine klare Abgrenzung und Kontrolle ermöglicht.

Security Account

Er hat die Hauptverantwortung für Sicherheitsmaßnahmen und Compliance.

Der Security Account ermöglicht eine zentrale Überwachung und Durchsetzung von Sicherheitsrichtlinien.

Er beinhaltet Sicherheitsdienste wie Security Information and Event Management (SIEM) und Intrusion Detection Systems (IDS).

Durch die Trennung von Sicherheitsressourcen in einem eigenen Account wird eine klare Abgrenzung und Kontrolle ermöglicht.

Yannick Tresch
DMoove Solutions GmbH
yannick.tresch@dmoove.com