Least Privilege Access

ACE-SECURITY

Least Privilege Access

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.

- Trust no one, not even internal services, resources, and actors
- User VPN
- RBAC
- Parameter security solutions not sufficient (lateral movement)

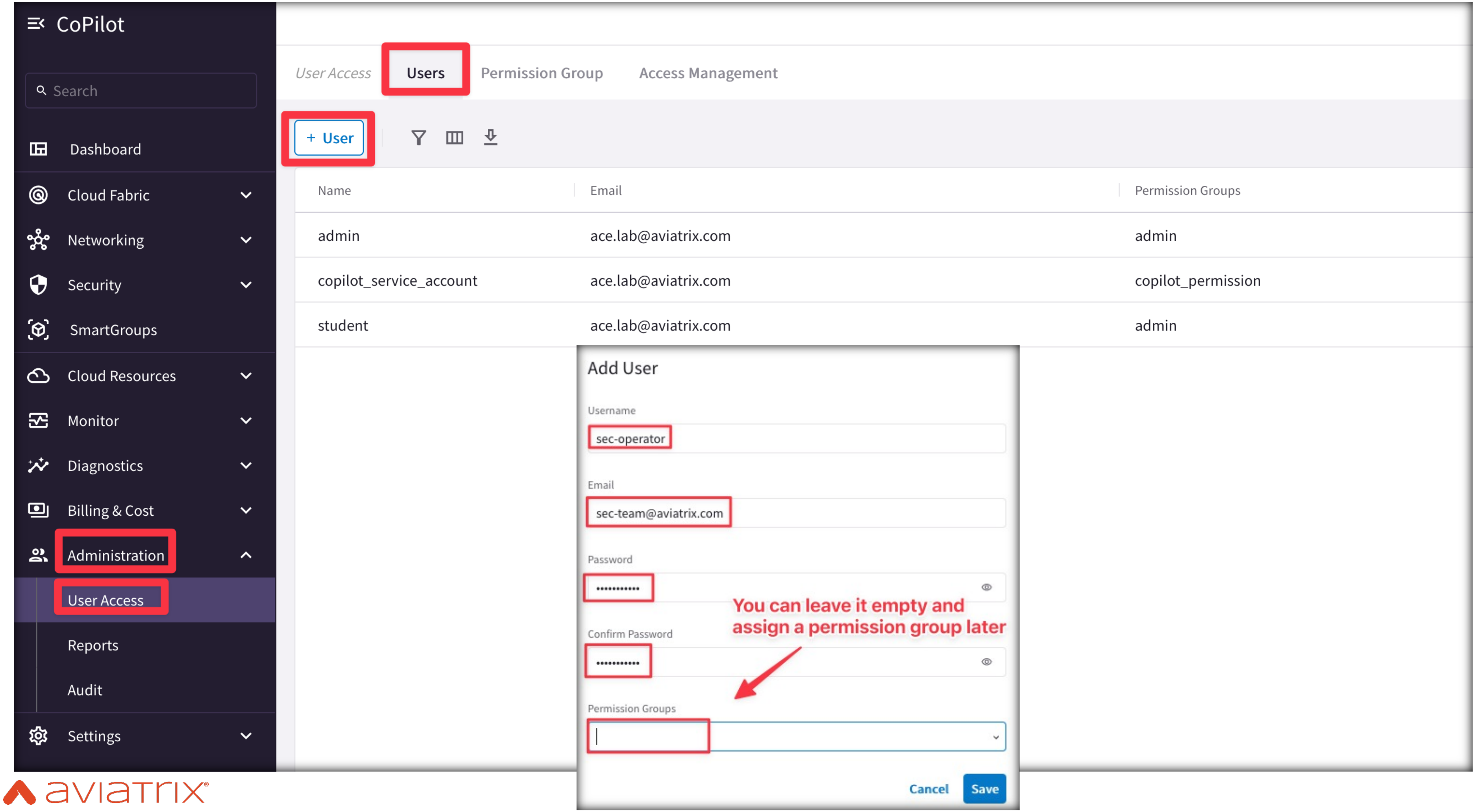
aviatrix

ACE

Aviatrix Certified Engineer

RBAC

User Access- CoPilot



Name	Email	Permission Groups
admin	ace.lab@aviatrix.com	admin
copilot_service_account	ace.lab@aviatrix.com	copilot_permission
student	ace.lab@aviatrix.com	admin

Add User

Username: sec-operator

Email: sec-team@aviatrix.com

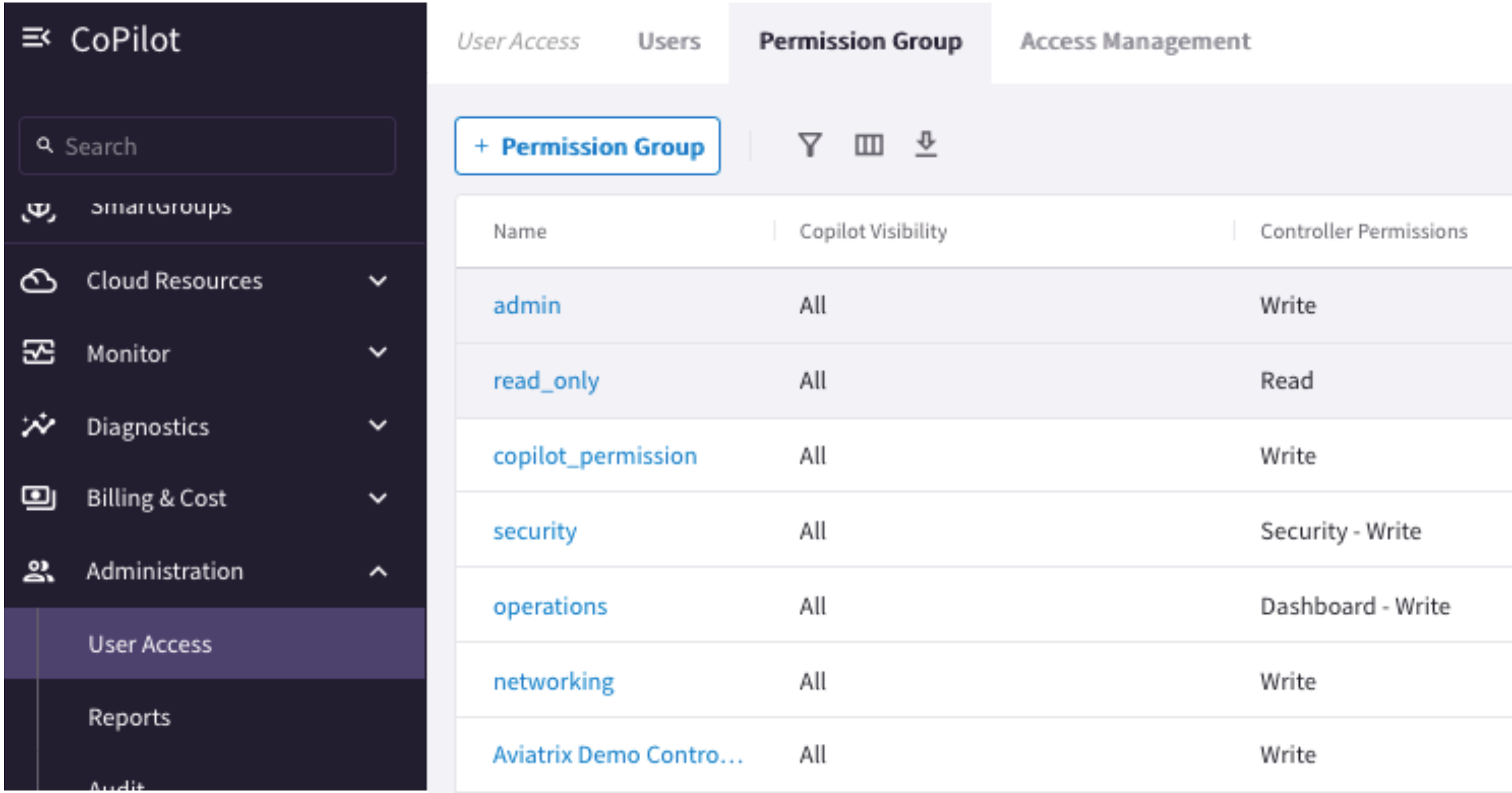
Password: •••••••••••

Confirm Password: •••••••••••

Permission Groups:

You can leave it empty and assign a permission group later

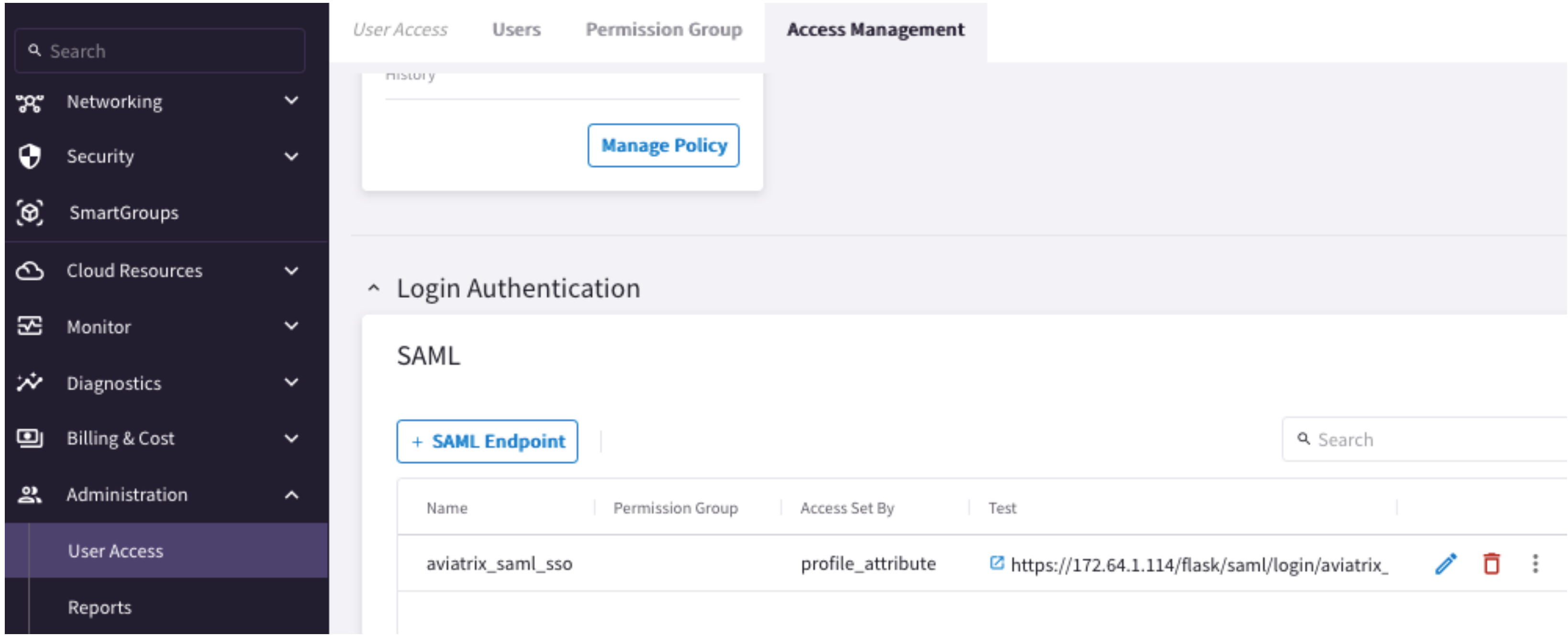
Aviatrix RBAC Control



Name	Copilot Visibility	Controller Permissions
admin	All	Write
read_only	All	Read
copilot_permission	All	Write
security	All	Security - Write
operations	All	Dashboard - Write
networking	All	Write
Aviatrix Demo Contro…	All	Write

Authentication

Users can be authenticated **Locally or** using **SAML IDP**



Name	Permission Group	Access Set By	Test
aviatrix_saml_sso		profile_attribute	https://172.64.1.114/flask/saml/login/aviatrix_

onelogin
okta
DUO
Azure Active Directory
Ping Identity
G Suite
AWS SSO
Centrify®

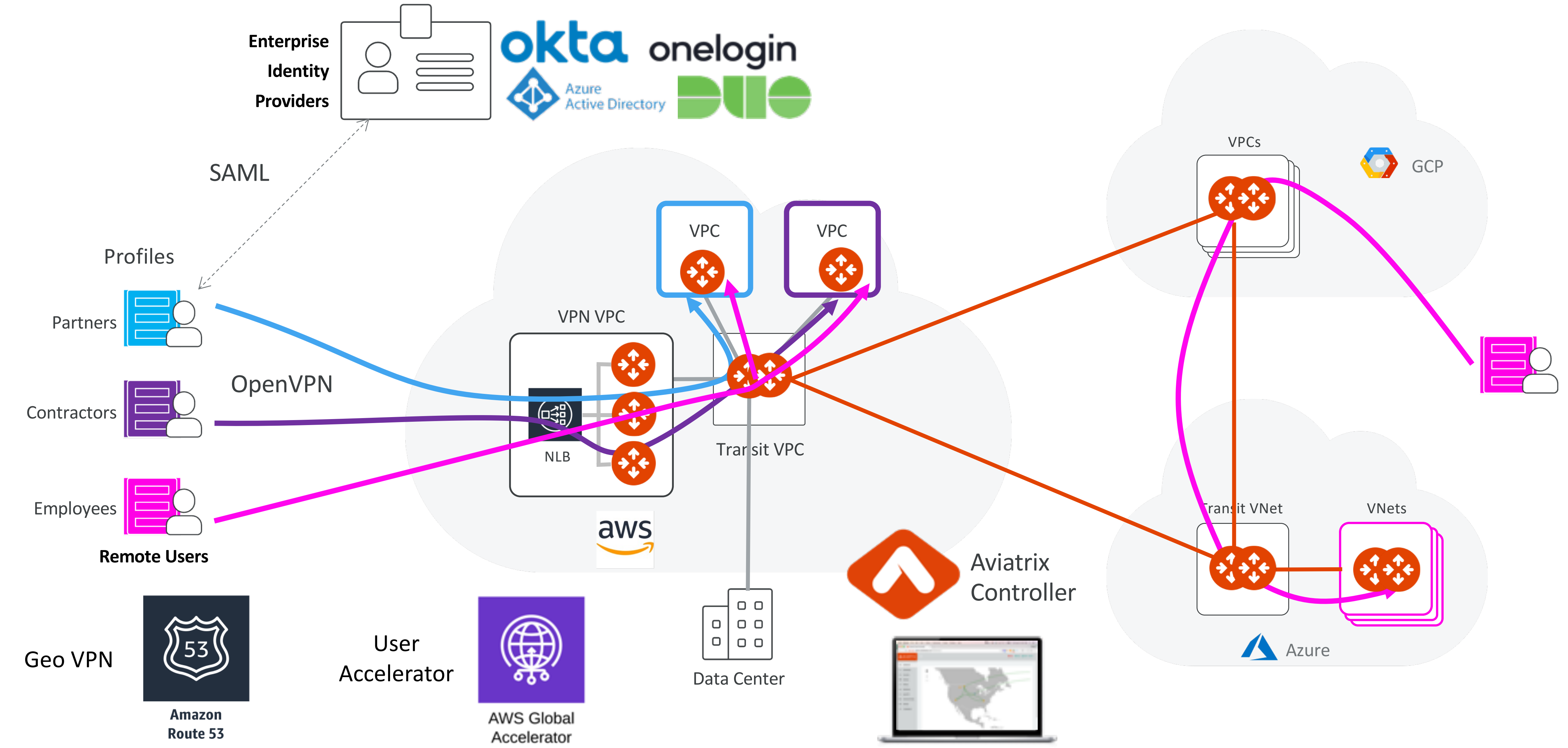
aviatrix

ACE

Aviatrix Certified Engineer

Aviatrix User VPN

Least Privilege Access for Developer – Aviatrix User VPN



Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com