Entra ID SSO Migration – Candidate Instructions

Repository Name & Link
lab-2025-10660 (solution branch sample)
GitHub URL: https://github.com/sparky948/lab-2025-10660/tree/feature/solution-sample

Overview

This assessment simulates real-world responsibilities for an Entra ID SSO Integration Engineer. You will work with SAML, claims mapping, Terraform automation, and legacy-to-modern migration patterns.

What You Will Deliver

1. Terraform configuration implementing a SAML app registration
2. JSON claims configuration
3. (Optional) Any diagrams or notes explaining your design choices
4. A brief written explanation for the troubleshooting scenario

Scenario Summary

You are migrating an application named 'Benefits-App' from a legacy SSO system to Microsoft Entra ID. The application uses SAML and requires specific claims, app roles, and manifest changes.

SAML Requirements

Identifier: urn:va:benefitsapp
Reply URL: https://benefits.va.gov/sso/saml/consume
NameID Format: Email address

Claim Requirements

Create three SAML claims:
- uid -> employeeId
- region -> extension_employeeRegion
- level -> extension_authLevel

App Role Requirements

Create an app role:
- display_name: BenefitsUser
- value: BenefitsUser
- allowed_member_types: ["User"]

Manifest Requirement

Use Graph API PATCH inside Terraform to set:
api.acceptMappedClaims = true

Troubleshooting Task

Explain how you would diagnose this SAML error:
AADSTS750052: The reply address does not match the reply addresses configured for the application.

Submission Instructions

Submit:
- Terraform files (*.tf)
- claims.json
- troubleshooting explanation

Do NOT submit any real credentials or secrets.
A fake token generator script is provided for local Terraform validation.