

PHYLAX CYBER / PORTFOLIO CASE STUDY

Hybrid Identity and Access Management: AWS Active Directory + Okta

A practical identity lifecycle lab

Self-managed Microsoft Active Directory on AWS EC2, connected to Okta Identity Engine for directory imports, delegated authentication, email verification, SAML federation and group-based application access.

Outcome	Evidence from the lab
Provision and authenticate	John Doe imported from AD and signed into Okta using AD credentials.
Authorize and revoke	Okta-Users controlled application access; removing membership removed the application tile after import.
Deactivate and restore	Disabling AD deactivated the Okta identity. Reactivation required import confirmation with auto-activation, then group membership restoration.
Federate	RSA demo service accepted the restored SAML login.

Engineering focus

Least-privilege remote management, directory sourcing, separation of authentication from authorization, and repeatable joiner / mover / leaver validation.

Publication edition | 9 October 2026

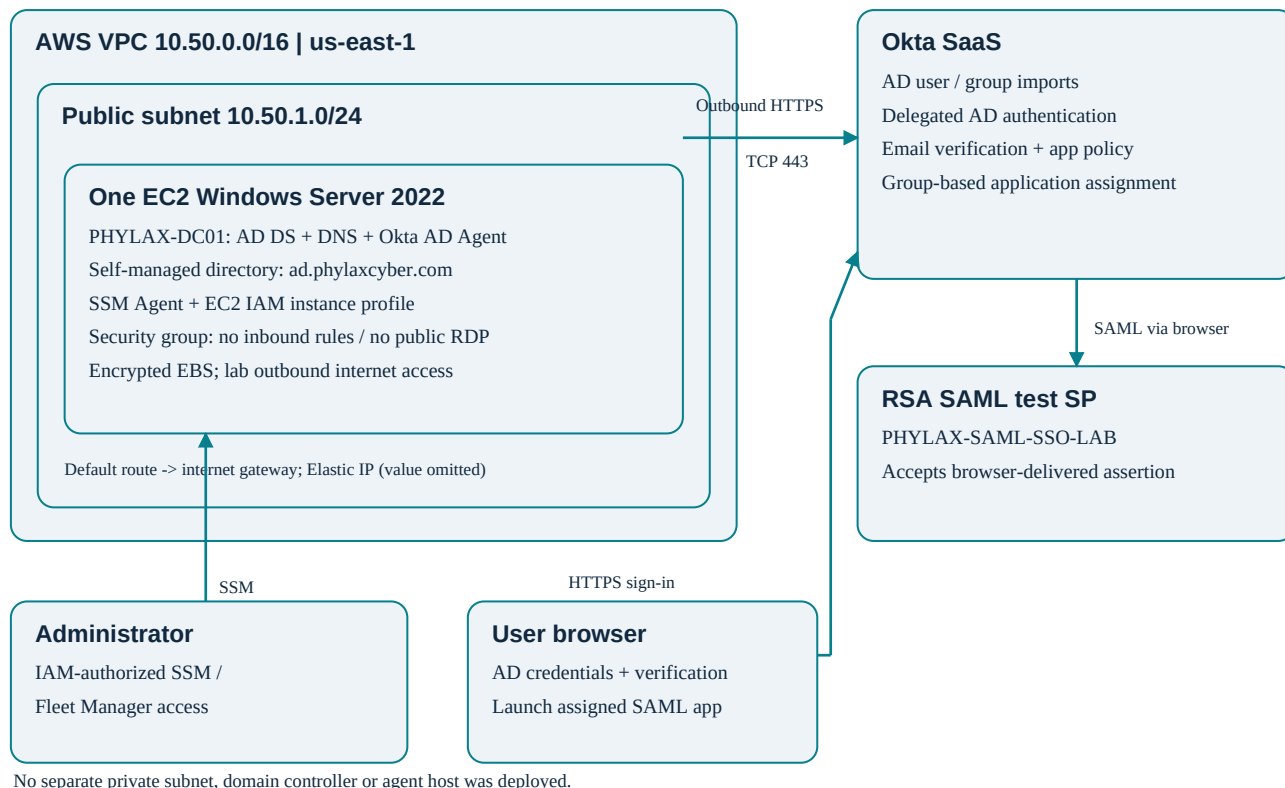
Prepared for Phylax Cyber. This is a single-server learning environment, not a production reference deployment. Commands are sanitized reproduction steps checked against vendor documentation; they were not executed again during preparation.

Evidence labels throughout: **SCREENSHOT** = directly visible in retrieved images; **LAB RECORD** = reported in the original conversation; **OPTIONAL** = recommended extension, not demonstrated.

01 / ARCHITECTURE

Actual lab topology and trust boundaries

PHYLAX CYBER | ACTUAL SINGLE-SERVER LAB



Directory and authentication: the co-located AD Agent opens outbound HTTPS to Okta. Users, attributes and groups import from AD; delegated password validation uses AD through this agent connection. Okta applies the configured authentication policy.

Federation: an assigned user signs into Okta and launches the RSA test application. The browser delivers the SAML assertion to the service provider; group membership controls the application assignment.

Administration: Systems Manager and Fleet Manager provide IAM-authorized access. The instance reaches AWS services over outbound connectivity; no public inbound TCP 3389 rule was used.

Lab boundary: this was one Windows server in one public subnet. Private subnets, redundant DCs and separate agent hosts are production recommendations, not deployed lab components. Public addresses and tenant identifiers are omitted.

02 / BUILD AWS

VPC, EC2 and secure administration

Resource	Lab configuration (LAB RECORD)
Network	PHYLAX-IAM-VPC: 10.50.0.0/16; PHYLAX-PUBLIC-SUBNET: 10.50.1.0/24; us-east-1.
Routing	Internet gateway attached; subnet route table has local route and 0.0.0.0/0 to gateway. Elastic IP associated during connectivity troubleshooting.
Compute	Windows Server 2022 Base; PHYLAX-DC01. t3.large was selected in the build guidance; final instance size is not independently visible in retrieved evidence.
Address	Actual primary private IP: 10.50.1.103. The earlier proposed 10.50.1.10 was not the deployed address.
Storage	50 GiB gp3; 3,000 IOPS; encrypted with aws/ebs; delete on termination enabled, as reported in launch review.
Access	IAM-SG: zero inbound rules; lab outbound rule allowed all traffic. PHYLAX-EC2-SSM-Role trusted EC2 and used AmazonSSMManagedInstanceCore.

Implementation sequence

1. Create the VPC and subnet. Attach the internet gateway, add the default route and explicitly associate the subnet route table.
2. Launch Windows with encrypted storage and the SSM instance profile. Remove the launch wizard's public RDP rule.
3. Ensure the SSM Agent is running and can reach AWS endpoints over HTTPS. Confirm the node is Online before continuing.
4. Open Session Manager, verify the session's actual Windows identity and administrative privileges, then use Fleet Manager Remote Desktop for GUI setup.

```

whoami
whoami /groups
Get-Service AmazonSSMAgent
Test-NetConnection ssm.us-east-1.amazonaws.com -Port 443

```

The lab encountered an SSM HTTPS timeout. Route table, NACL, security group egress and Elastic IP association were checked before the node came online. An internet gateway route alone does not give a private-only instance outbound internet access. [1, 2]

03 / INSTALL AD DS

Create the domain and validate DNS

Run in an elevated Windows PowerShell session. Install AD DS and its management tools; rename the host before promotion. Reconnect after each restart. [3]

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Rename-Computer -NewName "PHYLAX-DC01" -Restart
```

Use a private DSRM password through a functioning secure input method. Promotion creates a new forest and restarts Windows; do not repeat it on an existing domain controller. [3]

```
$DSRMPassword = Read-Host "New DSRM password" -AsSecureString
Install-ADDSForest -DomainName "ad.phylaxyber.com" `
  -DomainNetbiosName "PHYLAX" -InstallDNS `
  -SafeModeAdministratorPassword $DSRMPassword
```

Post-restart validation

```
Get-ADDomain | Select-Object DNSRoot, NetBIOSName
Get-ADForest | Select-Object RootDomain
Get-DnsClientServerAddress -AddressFamily IPv4
Resolve-DnsName "ad.phylaxyber.com" -Type A -Server 127.0.0.1
Resolve-DnsName "_ldap._tcp.dc._msdcs.ad.phylaxyber.com" `
  -Type SRV -Server 127.0.0.1
dcdiag /test:DNS
```

LAB RECORD: DNSRoot and forest were ad.phylaxyber.com, NetBIOS was PHYLAX, local DNS was 127.0.0.1, and the domain resolved to 10.50.1.103. Connectivity and DNS checks were reported as passing. The SRV query above is an additional recommended check, not captured in the lab.

AWS supplies the primary private address through DHCP; the lab retained it on the primary network interface. Keep the DC DNS client pointed at AD DNS and verify forwarder resolution to external services. Domain-joined clients need AD DNS, not only AmazonProvidedDNS. Do not publish the DC address or AD DNS service in public DNS.

Troubleshooting lesson

DSRM complexity failures coincided with a captured input length of one character. Hidden input through Fleet Manager was suspected; promotion later succeeded. Do not reproduce the plaintext workaround from the original chat. Use a secure input path and rotate exposed credentials; rotation completion was not evidenced.

04 / DIRECTORY OBJECTS

Organize users and access groups

Create dedicated OUs so directory import scope excludes unrelated identities. The test identity John Doe / jdoe is a synthetic lab user. The group is a Global Security group. [4]

```
$base = "DC=ad,DC=phylaxcyber,DC=com"
New-ADOrganizationalUnit -Name "PHYLAX-Users" -Path $base
New-ADOrganizationalUnit -Name "PHYLAX-Groups" -Path $base
New-ADUser -Name "John Doe" -GivenName "John" -Surname "Doe" `
  -SamAccountName "jdoe" `
  -UserPrincipalName "jdoe@ad.phylaxcyber.com" `
  -Path "OU=PHYLAX-Users,$base" -Enabled $false
Set-ADAccountPassword -Identity "jdoe" -Reset `
  -NewPassword (Read-Host "New lab user password" -AsSecureString)
Enable-ADAccount -Identity "jdoe"
New-ADGroup -Name "Okta-Users" -SamAccountName "Okta-Users" `
  -GroupScope Global -GroupCategory Security `
  -Path "OU=PHYLAX-Groups,$base"
Add-ADGroupMember -Identity "Okta-Users" -Members "jdoe"
```

Confirm the source objects

```
Get-ADOrganizationalUnit -Filter * |
  Where-Object Name -like "PHYLAX-*" | Select-Object Name
Get-ADUser jdoe -Properties mail |
  Select-Object Name, Enabled, UserPrincipalName, mail
Get-ADGroup "Okta-Users" |
  Select-Object Name, GroupScope, GroupCategory
Get-ADGroupMember "Okta-Users" | Select-Object Name
```

LAB RECORD: both OUs were created, jdoe was enabled after password setup, and John Doe appeared in Okta-Users. The user was initially disabled, which prevented treating object creation alone as successful onboarding.

These are one-time creation commands for a fresh lab, not an idempotent deployment script. Use secure password prompts only where input is reliable; never put a literal password in commands, screenshots or public documentation.

05 / CONNECT OKTA

AD Agent, scoped imports and attributes

- 1. In Okta Admin Console, open Directory > Directory Integrations and add Active Directory.
- 2. Download the agent on the Windows server from the admin console. Verify the installer's signature. The lab record names agent version 3.23.0; use a currently supported release for a rebuild.
- 3. Install on PHYLAX-DC01, select the domain and configure the agent service account with the permissions required for the chosen features.
- 4. Register with an authorized Okta administrator and confirm the agent is connected. Keep credentials and registration material private.
- 5. Scope user imports to PHYLAX-Users and group imports to the lab OUs. Select UPN as the Okta username format.
- 6. Run the initial Full Import, review matching, select John Doe, then Confirm Assignments with auto-activation enabled. [5, 6]

Attribute / object	Purpose and evidence
userPrincipalName	Login identity: jdoe@ad.phylaxcyber.com. LAB RECORD.
givenName / sn / displayName	Name fields for the test identity; review mappings in Profile Editor.
mail	Reachable mailbox for email verification; changed in AD and reported updated in Okta. Personal address omitted.
objectGUID / DN / sAMAccountName	Directory identification and linking. Actual GUIDs and SIDs are excluded from publication.
Optional imported attributes	displayName, employeeID, employeeType, manager and mobile were discussed in profile selection. No governance or ABAC behavior was demonstrated.
Okta-Users	AD-sourced group membership grants the SAML app assignment.

Retain required base schema fields. Review AD-to-Okta mappings and profile-source precedence before confirming imports. A warning about unmapped attributes for provisioning *to AD* appeared in the record; this case study does not claim that reverse provisioning was configured.

LAB RECORD: agent registration completed; John Doe became Active and AD-sourced in Okta. Service account privileges and final attribute values are not independently audited by the retrieved screenshots.

06 / AUTHENTICATE

Delegated authentication and email verification

1. Open the AD integration's Provisioning > Integration settings. Enable delegated authentication and save.
2. Use Test Delegated Authentication with the test user's UPN and private AD password.
3. Start a fresh private browser session and sign into the Okta tenant with the same identity.
4. Complete the email authenticator prompt according to the test policy. [5, 7]

LAB RECORD: the admin test reported authentication successful. The subsequent browser login reached an email verification prompt. The original UPN was not a provisioned mailbox, so the test could not initially receive email.

Correct the mailbox attribute at its source

```
$mailbox = Read-Host "Reachable lab mailbox address"
Set-ADUser -Identity "jdoe" -EmailAddress $mailbox
Get-ADUser jdoe -Properties mail |
    Select-Object Name, UserPrincipalName, mail
```

Run an Incremental Import where available and verify the changed email on the Okta profile. Keep the UPN unchanged. Retry sign-in, send the email verification message and complete the challenge. Do not publish an OTP, magic link or mailbox address.

LAB RECORD: the email update synchronized, verification completed and the user signed in. The exact authentication policy and System Log event payloads were not retrieved; no claim is made about assurance level or every future login requiring a challenge.

Security boundary

Email verification was used for the lab. Email codes and links are not phishing-resistant. A production rollout should use appropriate phishing-resistant authenticators and protect enrollment and recovery paths. Mailbox ownership, UPN and SAML NameID serve different purposes. [7, 8]

An AD password-change test and Okta password-reset/writeback settings were discussed, but a completed reset or writeback result was not captured. Password migration, password sync, SSPR and Desktop SSO are outside the demonstrated scope.

07 / FEDERATE AND AUTHORIZE

RSA SAML application and group-based RBAC

- 1. Open Applications > Applications > Browse App Catalog and locate RSA SAML Test Service Provider.
- 2. Add the integration and label it PHYLAX-SAML-SSO-LAB. Keep the user-facing icon visible.
- 3. Use the integration's supported SAML configuration. For a custom SP, obtain actual ACS URL, Entity ID and trust settings from its current metadata; do not invent endpoints.
- 4. In Assignments, choose Assign to Groups and assign Okta-Users. Avoid a direct user assignment that could bypass the revocation test.
- 5. Sign in as the test user in a fresh browser session and launch the tile. [9, 10]

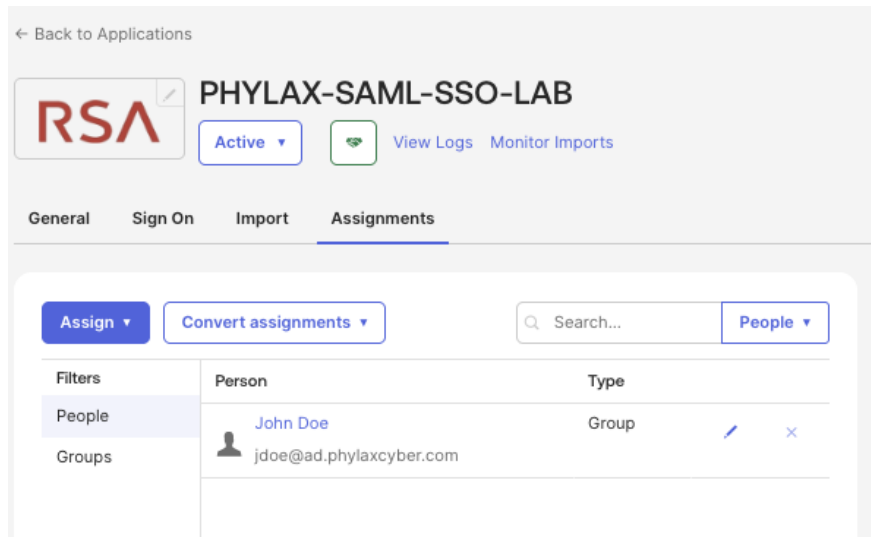


Figure 1. SCREENSHOT: the restored application assignment is Type = Group, not a direct individual grant.

LAB RECORD: initial SAML login succeeded. **SCREENSHOT:** the final restoration login shows successful federation and NameID jdoe@ad.phylaxcyber.com (Figure 6).

The earlier custom application attempt was replaced by the RSA catalog integration after the initially suggested test site was unavailable. The final tested application is PHYLAX-SAML-SSO-LAB. Exact ACS, audience, signing-certificate and SAML attribute settings are not exposed in retrieved screenshots; no synthetic configuration values are presented as tested.

RBAC here means a group represents application entitlement. It is not an AWS IAM role federation test and does not show provisioning a user account into a production application.

08 / REVOKE AND DEACTIVATE

Separate entitlement removal from account status

Test A | Remove group-based access

```
Remove-ADGroupMember "Okta-Users" -Members "jdoe"
Get-ADGroupMember "Okta-Users" | Select-Object Name
```

Confirm removal when prompted. Run the directory import, verify the group is empty and check the dashboard in a fresh browser session. **LAB RECORD:** group count reached zero and the user remained Active.

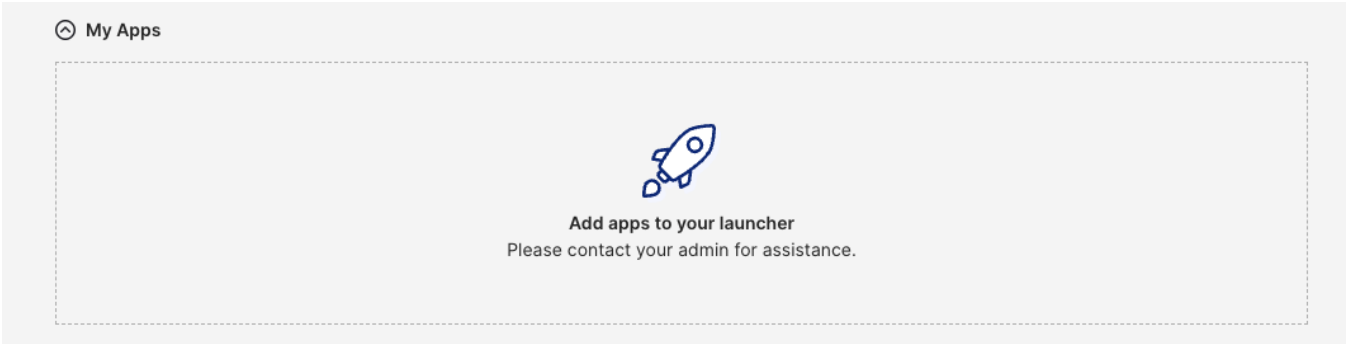


Figure 2. SCREENSHOT: the test user's app launcher is empty after membership removal and import. Tenant chrome was cropped out.

Test B | Disable the directory account

```
Disable-ADAccount -Identity "jdoe"
Get-ADUser jdoe | Select-Object Name, Enabled
```

Run the import and check the Okta status. AD profile sourcing and lifecycle settings must allow deactivation. **LAB RECORD:** the AD account was disabled. [6]

Person & username	Primary email	Status
John Doe jdoe@ad.phylaxcyber.com		Deactivated

Figure 3. SCREENSHOT: John Doe is Deactivated in Okta. Mailbox pixels were removed; unrelated identities were cropped out.

Application unassignment and account deactivation are distinct operations. These tests show the resulting dashboard and identity status after import; no synchronization latency was measured. Existing service-provider sessions were not tested or proven terminated.

09 / REACTIVATE

Resolve inactive import state before restoring access

```
Enable-ADAccount -Identity "jdoe"  
Get-ADUser jdoe | Select-Object Name, Enabled
```

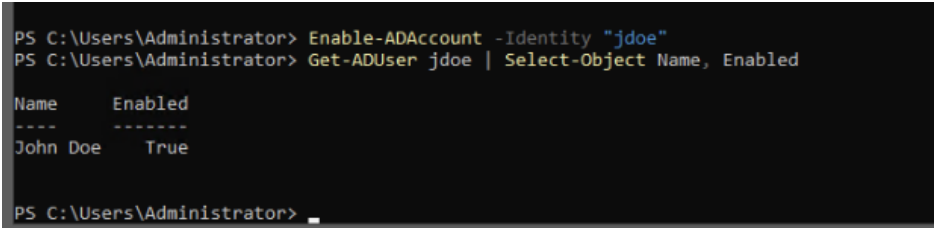


Figure 4. SCREENSHOT: the AD account is enabled again (True).

Run the AD import. The first confirmation attempt failed because the matching Okta identity was still INACTIVE. The confirmation dialog had auto-activation unchecked.

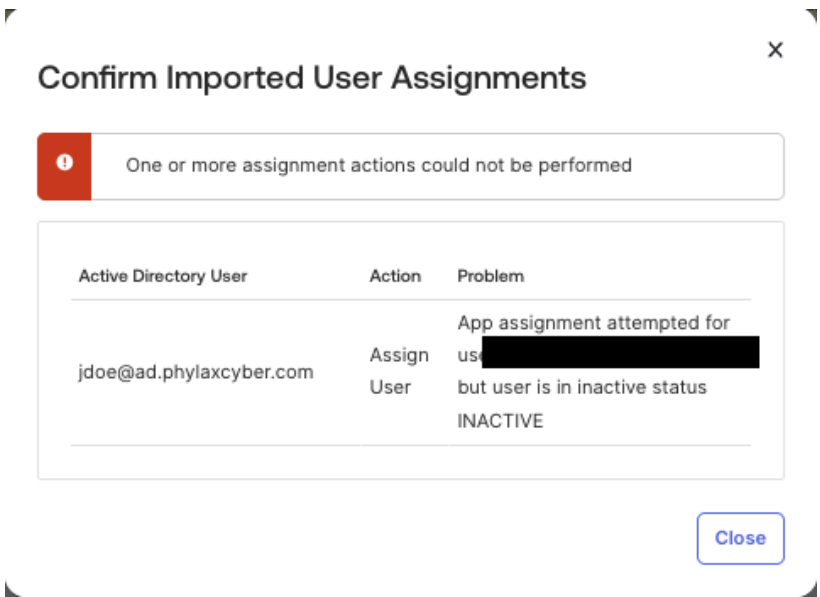


Figure 5. SCREENSHOT: import assignment failed for the inactive identity. The internal Okta user identifier was removed from image pixels.

Select the pending imported user and retry Confirm Assignments with **Auto-activate users after confirmation** enabled. The user then reported successful re-entry. Review lifecycle sourcing settings and matching before applying this to production. [6]

The captured error and unchecked setting explain why enabling AD alone was insufficient in this run. Reactivation required an administrator-confirmed import step; it was not demonstrated as fully unattended end-to-end reactivation.

10 / RESTORE

Group membership restores the SAML journey

```
Add-ADGroupMember "Okta-Users" -Members "jdoe"  
Get-ADGroupMember "Okta-Users" | Select-Object Name
```

After identity reactivation, restore membership in AD and run another import. Confirm both the group membership and group-derived application assignment. Sign in with a fresh browser session and launch the application.

Group name	People	Applications
 Okta-Users No description	1	1

SCREENSHOT: Okta-Users shows one person and one application after restoration.

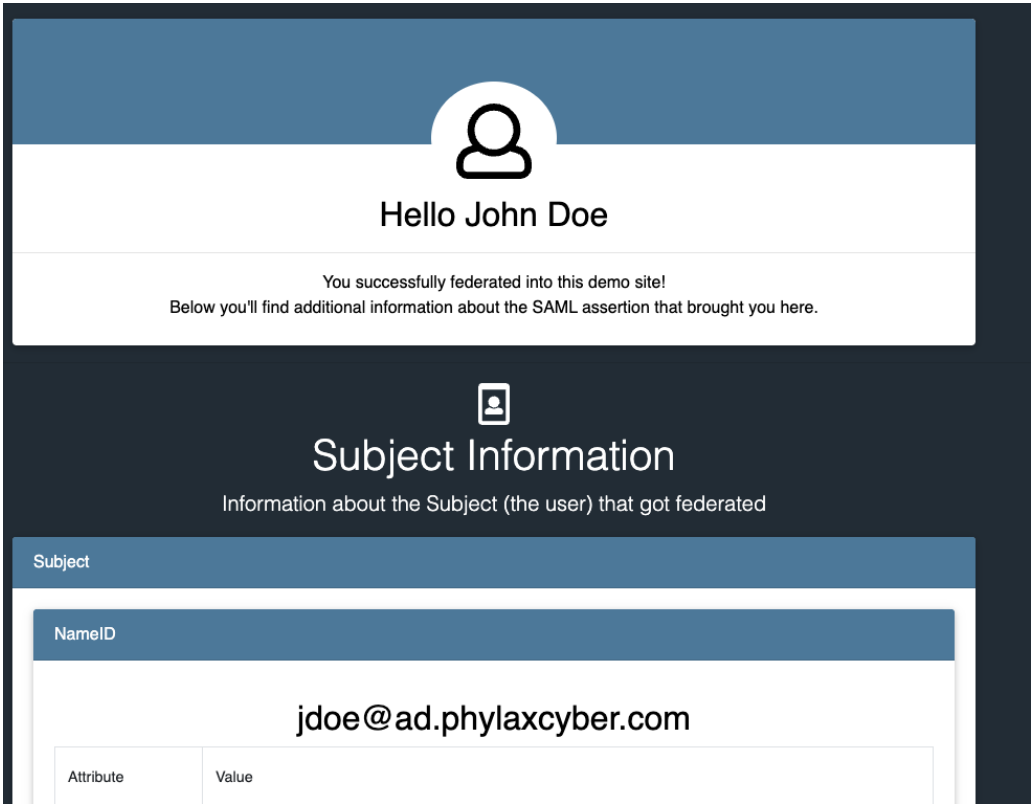


Figure 6. SCREENSHOT: the RSA demo service confirms successful federation after restoration; NameID is the synthetic lab UPN.

The application reappeared on the dashboard and the assignment remained group-based. Together, the final screenshots support successful entitlement restoration and SAML login following the confirmed reactivation and membership import.

11 / VALIDATION LEDGER

What the evidence supports

Test	Result / evidence strength
AD DS + DNS	Reported working domain and passing DNS tests. LAB RECORD; earlier images not retrievable in this export.
Agent + user imports	Reported registered agent, confirmed import and Active AD-sourced user. LAB RECORD.
Attributes + authentication	Reported mail update, successful delegated authentication, email verification and browser sign-in. LAB RECORD.
SAML + initial RBAC	Initial federation and group grant reported. Final group assignment visible in Figure 1.
Group removal	Zero-member group reported; empty launcher directly visible in Figure 2.
AD disable / Okta deactivate	Disable reported; Deactivated status directly visible in Figure 3.
Reactivation	AD Enabled=True visible in Figure 4; inactive import error visible in Figure 5; corrected confirmation and successful login reported.
Restoration	One-member group and group assignment visible; successful federation directly visible in Figure 6.
Not demonstrated	SSPR/writeback, password migration, Desktop SSO, behavior detection, ABAC, HA, production SP session termination, automated import timing.

Reproducibility and publication handling

The original conversation was reviewed across 123 turns. Ten final-stage screenshots were available to retrieve; six numbered evidence figures and one group-count crop are included. Earlier setup screenshots were referenced in the conversation but their image files were not returned. Diagram and command blocks are explanatory material, not recreated screenshots.

Screenshots were cropped to the relevant evidence and saved as fresh raster files. Personal email addresses and the internal user ID were removed with opaque pixel masks before embedding. No raw source screenshots, plaintext passwords, activation codes, public IPs, AWS resource IDs, tenant URLs, GUIDs or SIDs are included. The lab domain and synthetic user UPN are retained intentionally for technical clarity.

12 / OPERATIONAL LIMITS

Security, costs and cleanup

Production improvements | OPTIONAL, not tested

Move DCs to private subnets and deploy redundant domain controllers across failure domains. Use separate domain-joined agent hosts and follow Okta's availability guidance. Provide controlled outbound access for Okta and the required AWS endpoints. Add only necessary internal AD traffic for clients; do not expose LDAP, DNS or RDP publicly. Restrict administrator SSM permissions and adopt phishing-resistant authentication. [1, 5, 8]

The lab allowed broad egress and permissive NACLs. Zero inbound security group rules reduced exposure but did not create a complete production security architecture. A stopped or failed single DC/agent interrupts imports and delegated authentication. Review the special risks of SSM administrative access on a domain controller. Port-forwarded sessions do not support payload logging; retain API/session metadata and Windows audit events. [1, 2]

Cost model | no measured lab invoice available

Budget for Windows EC2 runtime, provisioned EBS capacity, retained snapshots, public IPv4 allocation, applicable data transfer and Okta licensing. T3 Unlimited surplus CPU credits may add charges. Credits offset eligible charges only until their balance or expiration is reached. Confirm Windows t3.large and gp3 rates in us-east-1 before a rebuild. [11, 12]

Public IPv4 list price is \$0.005 per address-hour: one retained address for 730 hours is \$3.65 before taxes, credits or other resources. An allocated Elastic IP can continue costing money while the instance is stopped. Stopping reduces compute charges but retains EBS billing. A private-subnet redesign can add endpoint or NAT costs. [11]

Cleanup sequence | recommended, completion not evidenced

1. Rotate all credentials exposed during troubleshooting, including the test user, administrator, DSRM and agent service account; update the service configuration and validate connectivity.
2. Preserve only sanitized evidence. Remove demo entitlements and identities when no longer needed. Verify independent Okta administrator access before retiring AD authentication.
3. Stop EC2 between lab sessions if continued testing is needed. Expect imports and delegated login to be unavailable.
4. For final teardown, retire the AD integration safely, uninstall/unregister the agent and terminate the lab instance after reviewing backups.
5. Confirm EBS deletion behavior, delete unneeded retained volumes/snapshots, release the Elastic IP and remove unused lab network and IAM resources. Check Billing/Cost Explorer for residual costs.

13 / REFERENCES

Vendor documentation and source notes

Documentation checked during preparation on 9 October 2026. Sources verify supported procedures and caveats; they do not independently attest to the lab outcomes. Commands containing secure prompts replace unsafe plaintext examples from the source conversation.

[1] [AWS: Securely extend and access AD domain controllers](#)

[2] [AWS: Start a Systems Manager session](#)

[3] [Microsoft: Install AD DS on Windows Server](#)

[4] [Microsoft: ActiveDirectory PowerShell module](#)

[5] [Okta: Manage your Active Directory integration](#)

[6] [Okta: Make Active Directory the profile source](#)

[7] [Okta: Configure the email authenticator](#)

[8] [Okta: Phishing resistance success factors](#)

[9] [Okta: SAML field reference](#)

[10] [Okta: Workforce Identity trial walkthrough \(RSA demo\)](#)

[11] [AWS: Amazon VPC pricing](#)

[12] [AWS: EC2 and EBS pricing](#)

Primary project source: Build AWS Active Directory Integration, user-supplied ChatGPT conversation. Reported results were cross-checked for chronology and limited to what the record supports. Original sensitive transcript content is not bundled with this public PDF.