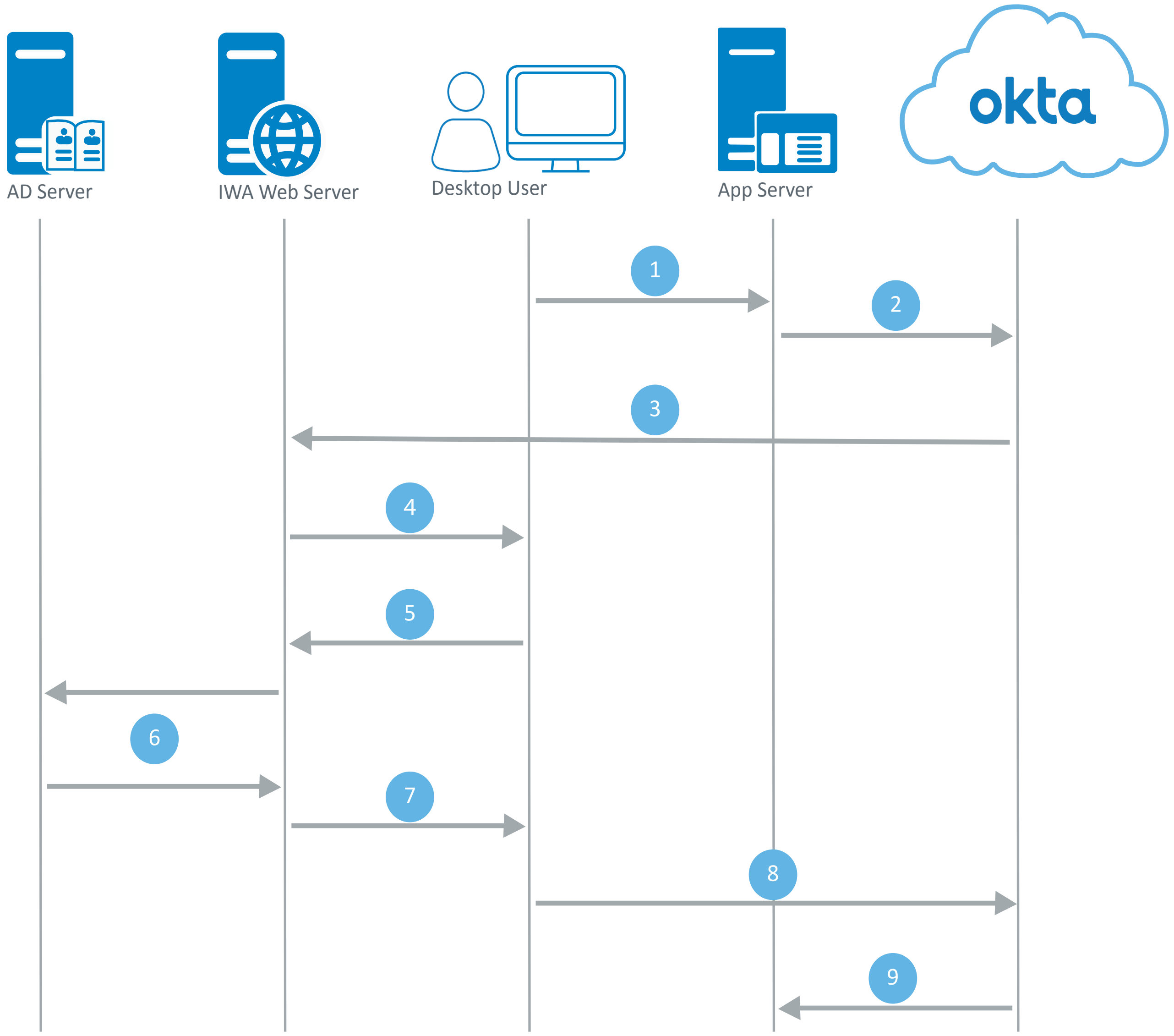

1. User tries to access an Okta-protected cloud app
2. App redirects the user to Okta for authentication
3. Okta redirects the user to the on-prem Okta IWA Web App via the browser
4. Okta IWA Web App challenges browser for authentication (WWW-Authenticate)
5. Browser sends NTLM/Kerberos credential for logged-on desktop user back to Okta IWA Web App
6. Okta IWA Web App validates NTLM/Kerberos credential and fetches the user profile from AD
7. Okta IWA Web App generates and digitally signs an SSO token and sends it to the browser
8. Browser returns the token to Okta via HTML form POST
9. Okta completes the app sign-in request and returns the user to the app with SSO token (e.g., SAML)