PingFederate Federation Checklist

GCA Technology Services | gca.net

1. Federation Partner Inventory Critical 1-2 weeks Governance

Count every federation partner: SAML IdPs, SAML SPs, OIDC providers, OIDC relying parties, and WS-Federation partners. The number drives connector deployment, licensing, and partner onboarding workflo

2. Protocol Requirements Critical 1-2 weeks Governance

Map which federation protocols are required: SAML 2.0, OIDC, WS-Federation, and SCIM for provisioning. Protocol selection affects token format, attribute mapping complexity, and partner compatibility

3. Deployment Topology Critical 1-2 weeks Governance

Decide on deployment architecture: standalone, clustered (active-active or active-passive), geo-distributed, or hybrid with PingOne. The topology affects latency, failover behavior, and operational co

4. Compliance & Data Residency Critical 2-4 hours Governance

Identify which compliance frameworks and data residency requirements govern your federation: GDPR data transfer rules, SOC 2, FedRAMP, or industry-specific regulations. Federation involves cross-borde

5. High Availability & Clustering Critical 1-2 weeks Security

Design the HA cluster: replicated nodes, session affinity, database clustering (if using external session store), and failover testing. PingFederate clustering requires careful configuration of the re

6. Attribute Mapping & Transformation Standard 1-2 weeks Security

Design attribute mapping between identity sources and federation partners: SAML attribute statements, OIDC claims, custom attribute sources, and attribute transformation rules. Each partner may requir

7. Partner Onboarding Workflow Standard 1-2 weeks Operations

Standardize how new federation partners are onboarded: metadata exchange process, certificate management, attribute contract negotiation, and testing procedures. Ad-hoc onboarding creates security and

8. Certificate & Key Management Standard 1-2 weeks Security

Plan certificate lifecycle management: signing certificates, encryption certificates, partner certificate rotation, and automated renewal. Certificate expiration is the #1 cause of federation outages.

9. Migration from Existing IdP Standard 1-2 weeks Operations

Plan migration from existing identity providers (ADFS, Shibboleth, legacy IdPs): metadata export, partner notification, parallel run period, and cutover strategy. Federation migration affects every co

10. Monitoring & Alerting Standard 1-2 weeks Operations

Configure PingFederate audit logging, health monitoring, and SIEM integration. Monitor authentication latency, error rates, certificate expiration, and partner connectivity status.

11. Disaster Recovery Testing Standard 1-2 weeks Security

Test DR procedures: node failure, database failure, data center failover, and certificate compromise scenarios. Federation DR testing must include partner-side validation to confirm failover works end

12. Operational Handoff Standard 1-2 weeks Operations

Decide who operates PingFederate after go-live: internal team, GCA managed services, or hybrid. PingFederate requires ongoing partner management, certificate rotation, monitoring, and platform upgrade

Schedule a consultation: gca.net/book-a-consultation