GitLab Backup

What to look for...

Backup ☐

- Automated and fully customized backups
- Widest GitLab data coverage (repos, metadata, LFS)
- GitLab and GitLab Self-managed versions supported
- Multiple backup plans/policies
- Policy-based advanced backup plans
- Backup on-demand

Restore & Disaster Recovery ☐

- Every-scenario-ready Disaster Recovery
- Mass restore of multiple repositories
- Restore Cloud to Self-managed and conversely
- Restore to device/on-premise
- Restore to the same GitLab account/organiation
- Restore to a new GitLab account/organiation
- Cross-over recovery different git service
- Point-in-time recovery
- Granular recovery of repos and metadata

Data migration and mobility ☐

- Migration between Self-managed & cloud deployments
- The same or new GitLab account
- To different git hosting provider

Security & Compliance ☐

- Your own AES 256 encryption key
- Separated customers cloud infrastructures
- AES encryption level of choice
- In flight and at rest encryption
- SSL transfer encryption
- Zero-knowledge encryption
- Data residency of choice (US, EU, AUS, custom)
- Compliance reports
- Ultra-secure authorization
- ISO27001/SOC 2 audited vendor

Authentication ☐

- OAuth App
- Account Credentials
- SAML integration
- SSO

Multi-storage support ☐

- Cloud storage integration
- On-premise storage integration
- Add unlimited no. of storage
- Unlimited cloud storage included

Backup performance ☐

- Full, incremental, differential backups
- Flexible scheduler and custom backup frequency
- Automatic repository sync
- Unlimited retention for compliance
- Enterprise backup-scalability
- Basic rotation scheme (daily backups)
- Grandfather-Father-Son rotation scheme
- Forever Incremental rotation scheme
- Data compression on source
- Backup replication based on plans
- Task balancing

Monitoring & Management ☐

- Central management console
- Data-driven dashboards
- Multiple admin accounts
- Access and privileges settings
- Customizable email and Slack notifications
- Advanced audit logs
- REST API automated operations
- Webhooks
- Daily reports for compliance purposes
- Unlimited accounts consolidation

Ransomware Protection ☐

- Immutable S3 storage
- Non-executable data in the copy
- Limited access to storage credentials
- Multi-storage system for 3-2-1 backup
- Encrypted backups

Cross-recovery between:

GitHub, GitLab, Bitbucket, Azure DevOps

SAML integration to look for:

Auth0, Azure AD, CyberArk, Google, Okta, OneLogin, custom

SSO support to look for:

Atlassian, Google, Microsoft, GitHub, GitLab

Storage compatybility to look for:

AWS Storage, Azure Blob Storage, Google Cloud Storage,Wasabi Cloud, Backblaze B2, S3 Compatible storages, NAS/local

Automated storage replication to:

AWS Storage, Azure Blob Storage, Google Cloud Storage,Wasabi Cloud, Backblaze B2, S3 Compatible storages, NAS/local

GitProtect.io
by Xopero ONE