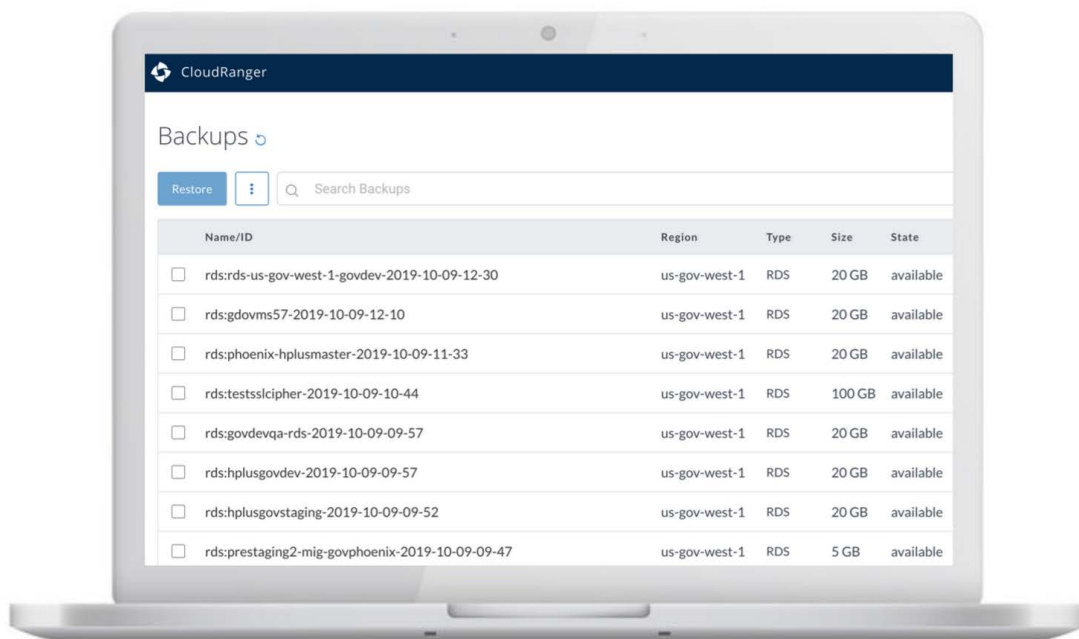




The AWS backup solution for GovCloud

Taking regular snapshots of your data is the logical first step for any robust data protection strategy for AWS GovCloud. However, the snapshot management capabilities of “AWS Backup” are not available in AWS GovCloud. You need a complete solution that keeps your AWS GovCloud data safe and easily recoverable from any scenario.



AWS GovCloud customers are facing a range of challenges with snapshot management above and beyond the basics, which require more sophisticated features such as the ones provided by **Druva Cloudranger**, including:



Backup and Recovery

- **No native solution** - Native-tools such as 'AWS Backup' do not provide AWS GovCloud support to create backups and restore backups or the functionality to create cross-region copies within AWS GovCloud (US-West) and AWS GovCloud (US-East).
- **Cross-region/Cross-account** - If you are hit by regional AWS GovCloud outages, or user error, you can restore from cross-account or cross-region storage copies within AWS GovCloud to minimize disruption
- **File-level search and recovery** - Retrieving individual files can be problematic using native tools, but there are times when critical files are needed quickly. Our file-level search and recovery solves for this



Amazon Machine Images (AMI)

- **AMI Based Policies** - Take full instance backups as Amazon Machine Images (AMIs) or Amazon EBS snapshots of individual Amazon EBS volumes
- **Restore AMIs** - If your restore objective is to create a new Amazon EC2 instance quickly to replace a failed Amazon EC2 instance, then creating an Amazon Machine Image (AMI) is the best option
- **AMI + EBS** - The process of creating an AMI will also create associated Amazon EBS snapshots. So, you can also restore a single Amazon EBS volume from the individual Amazon EBS snapshot



Centralized Global Management

- **Multi-tenancy** - Provides a single pane of glass to easily manage multiple AWS GovCloud accounts.
- **100% SaaS** - No software to be updated; utilizing IAM based access roles ensures a more secure AWS GovCloud environment
- **No IT overheads** - Lowers administration costs and ensures a more secure AWS GovCloud environment by reducing risk of user errors



Alerts and Reporting

- **Real-time alerts** - Whenever a job or backup policy fails, an alert is issued in real-time with a description of the failure via email, Slack or custom webhooks
- **Customize reporting** - Create customized reports for policies that can be exported to PDF or CSV



Governance and Compliance

- **Compliance SLAs** - Automatically configure data protection policies for newly created instances based on AWS tags
- **Agentless service** - Druva CloudRanger has no software or agents for users to manage or update; maintaining security integrity Access to your AWS account is controlled by role-based Identity and Access Management (IAM)
- **Serverless architecture** - Running entirely on AWS Serverless so no maintenance, patching etc. That's all handled by AWS. The underlying services are constantly up to date.

[Request a Demo](#) for a deeper look at why your organization should consider Druva CloudRanger for your AWS GovCloud data protection requirements.



Sales: +1 800-375-0160 | sales@druva.com

Americas: +1 888-248-4976

Japan: +81-3-6890-8667

Europe: +44 (0) 20-3750-9440

Singapore: +65 3158-4985

India: +91 (0) 20 6726-3300

Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital and Nexus Partners. Visit [Druva](#) and follow us [@druvainc](#).