

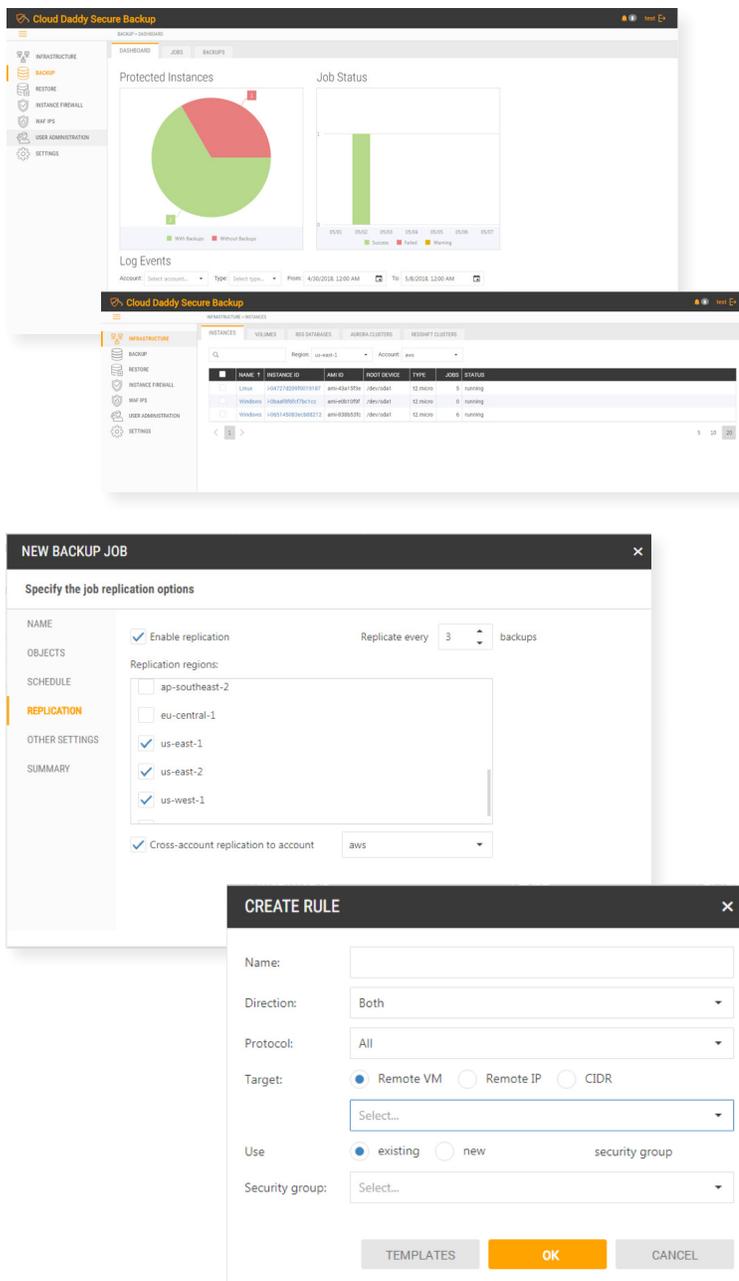
Cloud Daddy Secure Backup

The world's most secure data protection solution for AWS



Product Overview

Gone are the days of thinking about backup, security and infrastructure management as three separate areas of responsibility within IT. In today's elastic cloud world, agility combined with security is required. The combination of backup, security, and infrastructure management therefore go hand-in-hand, creating a new paradigm. And because these considerations are so critical, they form the three pillars of Cloud Daddy Secure Backup. It's the only solution in the world that joins backup and disaster recovery, advanced security, and infrastructure management into one solution for Amazon Web Services (AWS).



Data Protection

BACKUP, RESTORE, DISASTER RECOVERY

Cloud Daddy Secure Backup is a cloud-native, secure backup solution explicitly built for AWS. It utilizes native Amazon APIs and implements Amazon's own best practices to deliver rock solid data protection for AWS. Rather than reinventing the wheel, Cloud Daddy Secure Backup extends rock-solid constructs already available in AWS.

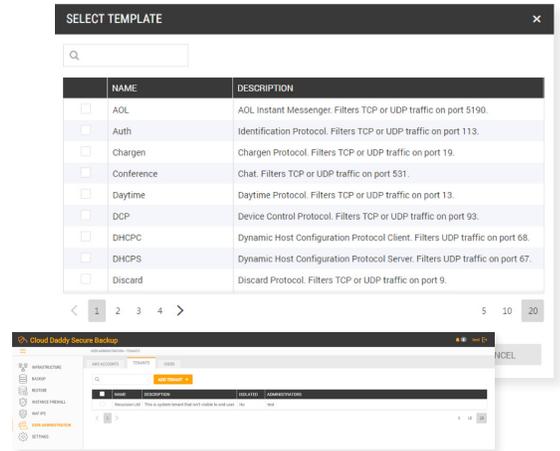
- **Comprehensive backup.** Cloud Daddy Secure Backup can protect Amazon EC2 instances, EBS volumes, RDS and Aurora databases, and Redshift clusters.
- **Restore on your terms.** Restore and replicate across multiple AWS regions and accounts for geographical diversity.
- **Recover what you need, and only what you need.** Cloud Daddy's file-level recovery provides the flexibility and granularity to restore exactly what you need and nothing more.
- **Run backups and snapshots on your schedule.** Schedules are flexible allowing you to set up periodic backup jobs with any conceivable schedule, or run a job at a specific time. You can schedule snapshots with frequencies ranging from minutes to months, and retained by the number of recovery points and the age of snapshots you determine.



Advanced Security

In today's digital world, your data, intellectual property and business-critical infrastructure are at constant risk and vulnerable to cyber-attack. Shouldn't your backup and disaster recovery solution incorporate security by design to protect your organization's last defense and ability to recover from not only a natural disaster but cyber-attack? Cloud Daddy provides additional cybersecurity countermeasures to safeguard your AWS workloads with superior data protection.

- Get a firm grasp on your firewalls.** See everything in one place. Cloud Daddy provides an elegant interface for managing firewall rules applied to AWS instances, as well as for management of AWS Web Application Firewall (WAF). Rule templates are supplied to speed up the process of adding and customizing new rules and applying them to instances for added protection.
- Quickly mitigate shifting attack vectors.** The interface makes it simple to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns.
- Feed your other security tools.** Cloud Daddy gives you the ability to generate firewall logs for selected instances over a period of time. Logs can be exported to CSV or syslog format to perform security analytics using third-party SIEM and UEBA tools.
- Stay ahead of threats with advanced AI.** By harnessing the power of artificial intelligence and machine learning, Cloud Daddy Secure Backup can trigger actions in response to anomalies, protecting your backup and disaster recovery with an added layer of prevention against cyber-attacks. (Coming in Release 2.0)



Infrastructure Management

Enterprise environments are increasingly complex, and virtual infrastructure changes constantly. Cloud Daddy provides the visibility and control of your AWS infrastructure's backup and disaster recovery at scale, with a single point of management designed to simplify data protection. Cloud Daddy Secure Backup marries infrastructure management with disaster recovery and advanced security.

- Single pane of glass.** Manage all of your AWS infrastructure (AWS Instances, EBS Volumes, RDS and Aurora databases, and RedShift Clusters) from a single view.
- Built for scale.** Cloud Daddy's multitenant model serves corporate clients of any size, ranging from SMB to very large multi-tenant distributed enterprises, public sector, and managed service providers. The tenancy model has support for IAM roles and credentials for secure cross-account access.
- Maximum flexibility with IAM.** Cloud Daddy makes it easy to configure role-based access to your multi-account AWS infrastructure using the built-in constructs of tenants, roles, and users. AWS accounts can be distributed among tenants, while users of each tenant have limited role-based access to the objects within the tenants in which they reside.

KEY USE CASES

Unified AWS Backup: Perform backups of AWS infrastructure including EC2 Instances, EBS Volumes, RDS and Aurora Databases, and Redshift Clusters.

File-Level Restore Capability: Perform a restore of a specific file within a volume or full restore of an instance within AWS infrastructure from a snapshot.

Replication Across Regions: Perform replication of one or more AWS resources to a different AWS region anywhere in the world.

Secure Data with Instance Firewalls: Configure instance firewall for specific EC2 instances as an additional cybersecurity countermeasure.

