niyantrac

Infinite Control. Zero Chaos

Product User Guide

Document Version: 1

Table of Contents

Table of Contents

1 Introduction

Niyantrac is a centralized platform designed to version, visualize, and manage AWS CloudFront distributions, Route53 hosted zone configurations, and WAF Web ACLs. It simplifies the process of tracking changes, restoring previous states, and maintaining a complete configuration history—giving teams greater control and confidence over their edge, DNS, and web application firewall environments.

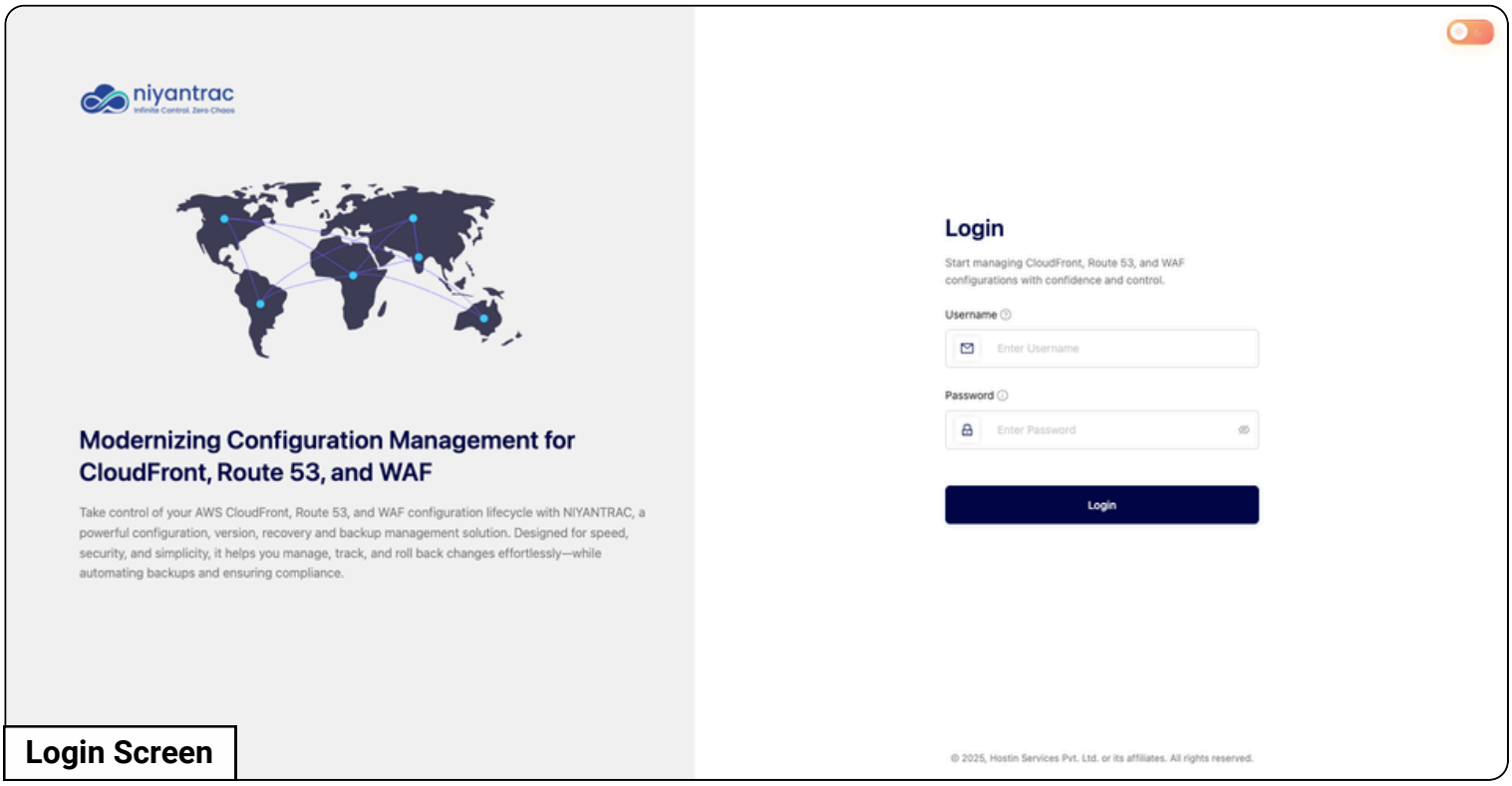
Key Capabilities:

- **Version History & Rollbacks:** Store every CloudFront distribution, Route53 hosted zone, and WAF Web ACL configuration change as a version. Roll back instantly or copy configurations across distributions, hosted zones, or Web ACLs.
- **Recovery & Cloning:** Recreate deleted CloudFront distributions, Route53 hosted zones, or WAF Web ACLs, or spin up new ones from any saved version.
- **Behavior, DNS & Security Configuration Management:** Manage CloudFront behaviors, origins, and error pages; update Route53 records, routing policies, and failover settings; and configure WAF rules, rule groups, managed rule group versions, and Web ACL settings directly.
- **AI-Powered Change Analysis** — Automatically analyze configuration differences between any two versions with AI-generated summaries, severity ratings, and security impact assessments. Connect your own self-hosted LLM or use AWS Bedrock — with full flexibility over your AI setup.
- **Tagging & Organization:** Add and manage tags to keep CloudFront, Route53, and WAF resources organized and easy to navigate.
- **Visual Insights:** View CloudFront metrics such as request volume, error rates, and data transfer; monitor WAF sampled requests and rule actions to understand performance and security trends.
- **Scheduled Backups:** Automate versioned backups for CloudFront, Route53, and WAF using cron-based scheduling.
- **Secure & Extensible:** Configure SSL settings, manage policy-based access control, and receive SMTP email alerts for important events across all services.
- **S3 Backup:** Back up all configuration versions securely to Amazon S3 for long-term durability.

Whether you're recovering from changes, replicating configurations, or managing multiple CloudFront distributions, Route53 hosted zones, or WAF Web ACLs at scale, Niyantrac gives you full control and confidence.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

The Niyantrac dashboard enables users to view, manage,and restore CloudFront distribution and Route 53 hosted Zones configurations efficiently with a modern and intuitive interface.



Login Screen

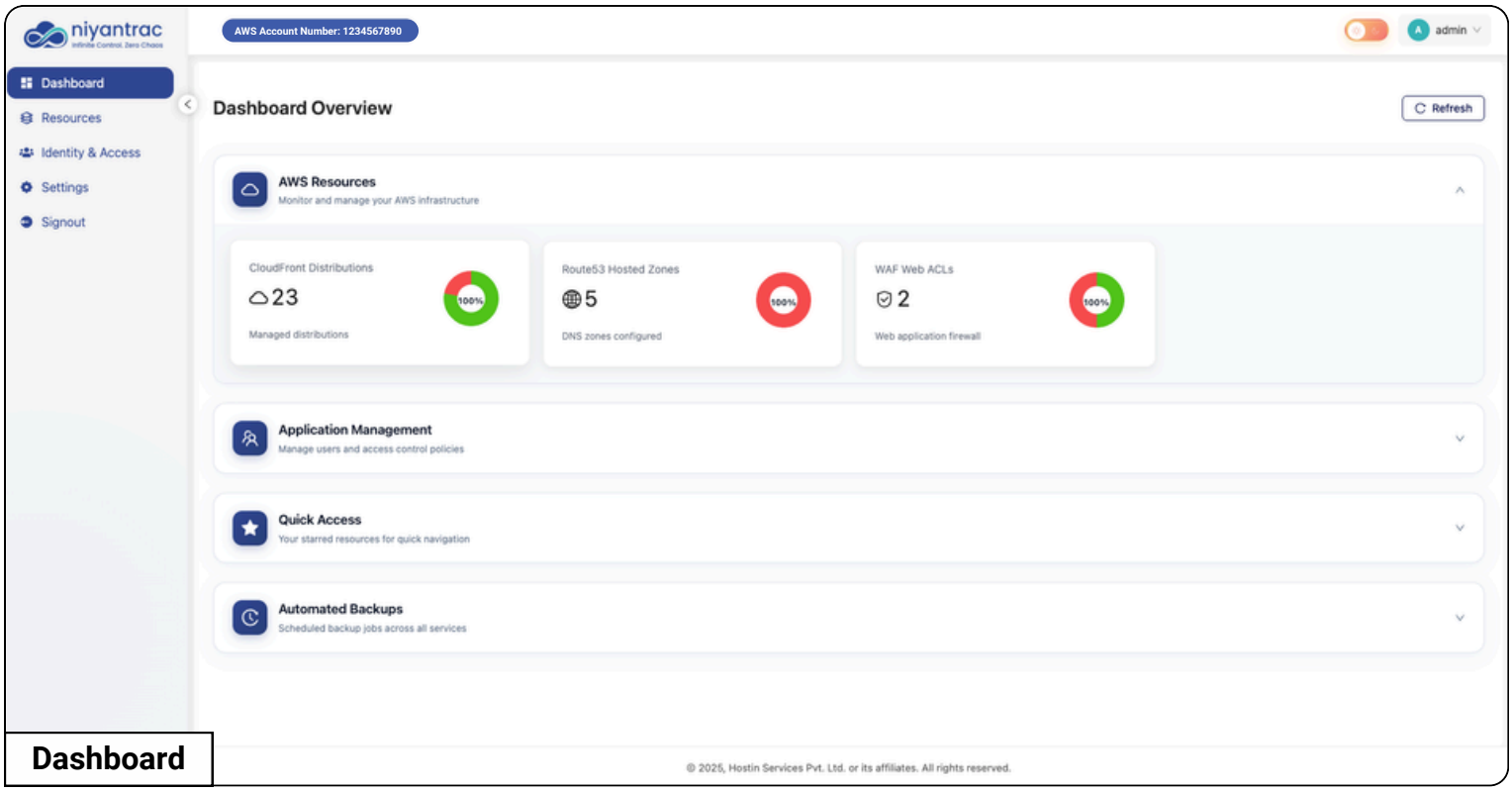
2. Application Layout

The application features a persistent sidebar offering the following primary navigation options:

- **Dashboard:-** It tracks AWS starred resources, user access, and backups to monitor system health and performance.
- **Resources:-** CloudFront Vault manages distributions, Route 53 Vault manages hosted zones efficiently and WAF Vault manages Web ACLs.
- **Identity & Access:-** The Identity & Access module enables granular control over user permissions through both
- user-based and policy-based access control (PBAC) mechanisms.
  Settings:- Schedule management, Email Notifications, SSL Configuration, Application backup, AI Management
  Signout:- Securely log out of the application.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

3. Niyantrac Dashboard



Dashboard

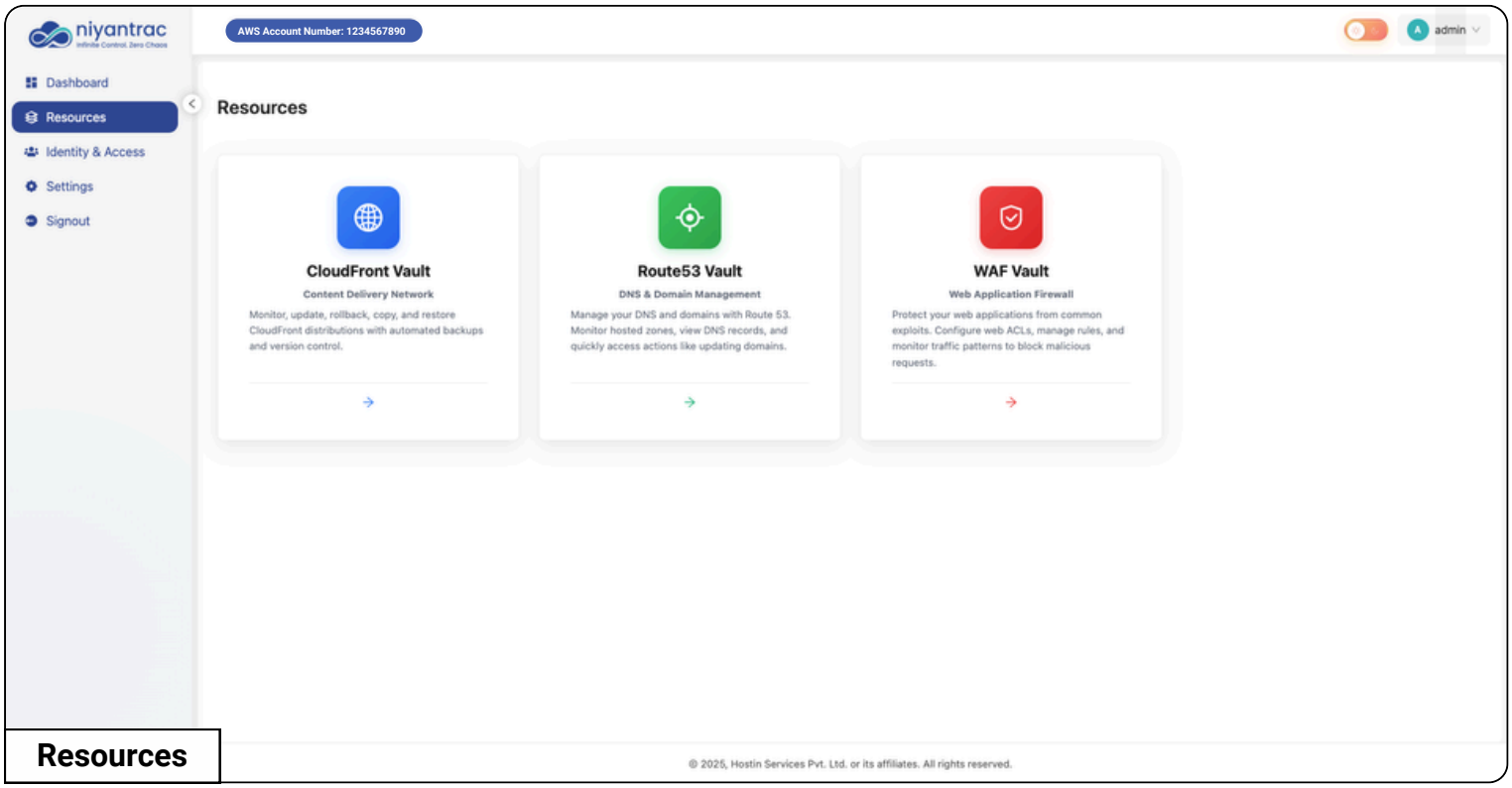
The Niyantrac dashboard provides a centralized interface for Overviewing your AWS infrastructure with comprehensive disaster recovery, versioning, and backup capabilities. The main dashboard is organized into four key sections:

- **AWS Resources:** Monitor and manage your AWS infrastructure, including CloudFront distributions, Route53 Hosted zones, and WAF ACLs.
- **Application Management:** Control user access and manage policy-based access control (PBAC) settings for team collaboration
- **Quick Access:** Navigate to your starred or frequently-used resources for faster workflow management
- **Automated Backups:** and manage automated backup jobs across all supported AWS services with version control and rollback capabilities

It tracks AWS starred resources, user access, and backups to monitor system health and performance.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

4. Resources



Resources

4.1 CloudFront Vault (Content Delivery Network)

- **Function:** This section provides tools for managing AWS CloudFront Distributions, which are the networks that cache and deliver website content (images, videos, etc.) globally.
- **Capabilities:** It enables Monitoring, Updating, Rollback, Copying, and Restoration of distributions.

4.2 Route 53 Vault (DNS & Domain Management)

- **Function:** This section provides tools for managing AWS Route 53 settings, which handle the Domain Name System (DNS).
- **Capabilities:** It allows users to monitor hosted zones, view DNS records, execute quick access actions for domain updates, and perform rollback and recreation when needed.

4.3 WAF Vault (Web Application Firewall)

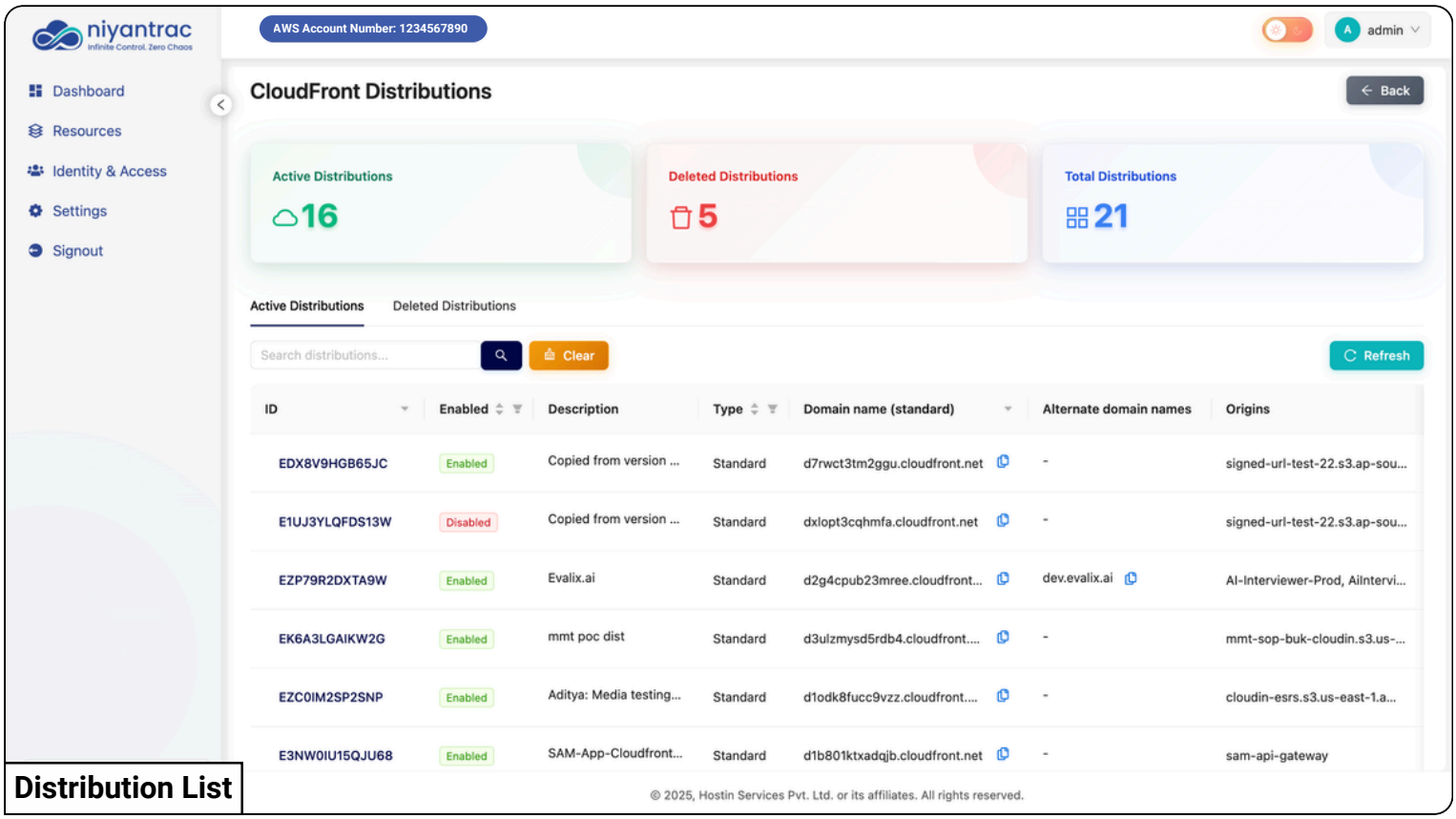
- **Function:** This section provides tools for managing AWS WAF configurations, which protect web applications by monitoring and filtering HTTP(S) traffic based on customizable security rules.
- **Capabilities:** It enables monitoring of Web ACLs and management of ACL configurations, versioning, rollback, and recreation.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

5. CloudFront Distributions

5.1 Accessing Distributions

- Click the **Distributions** menu from the sidebar.
- You'll see two tabs at the top:
  - **Active Distributions (default).**
  - **Deleted Distributions.**
- Below the tabs, the respective list of distributions is displayed.



Distribution List

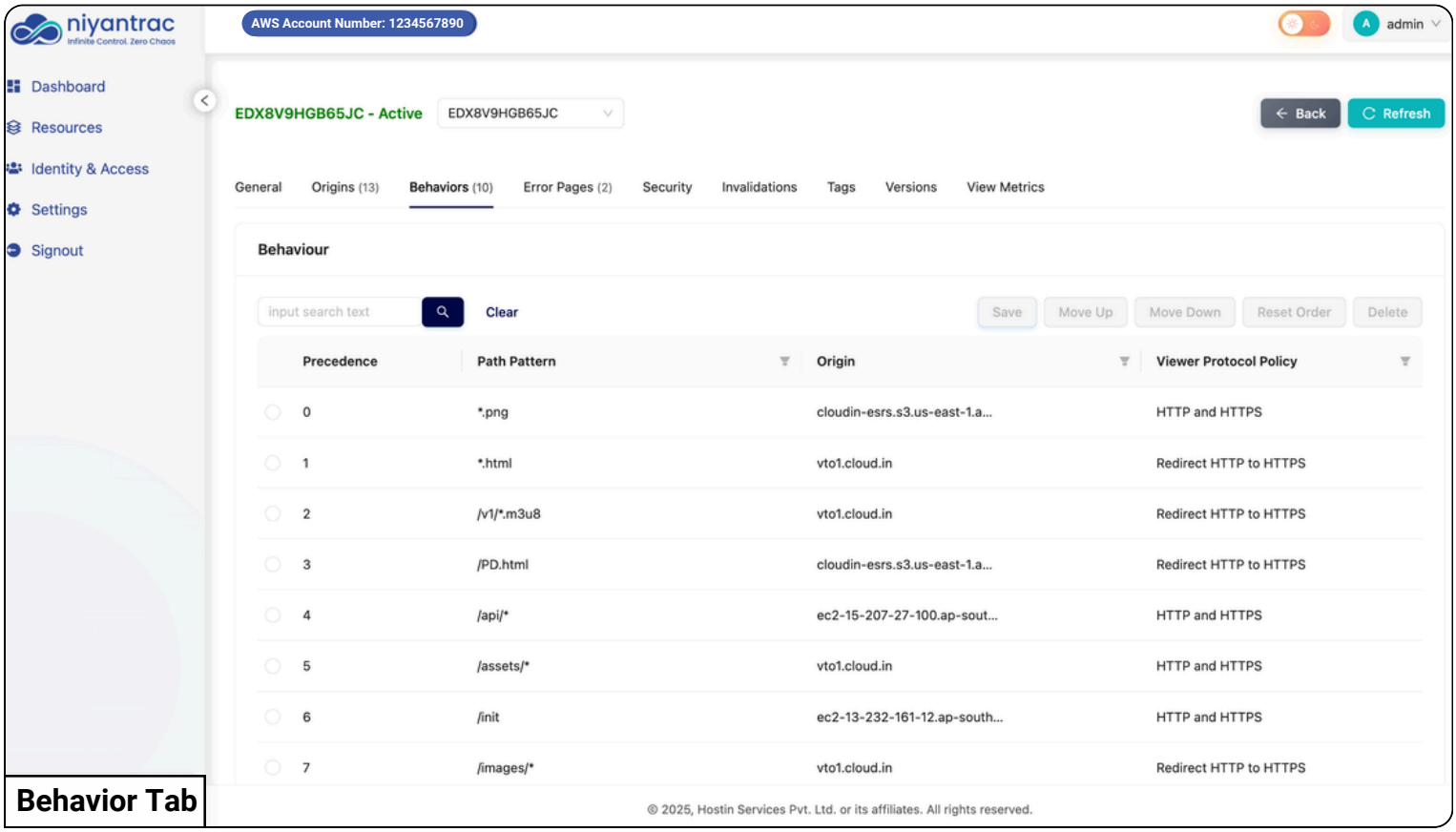
5.2 Distribution Details View:

Clicking on a Distribution ID opens a detailed view with several tabs, designed to resemble AWS CloudFront's distribution information layout. Tabs include:

- **General Info:** Basic configuration and metadata.
- **Origins:** Origin domain and path settings.
- **Behaviors:** Cache and request behavior configurations.
- **Error Pages:** Set a custom error page in CloudFront for specific error codes.
- **Security:** Control access by country using CloudFront geo-restrictions.
- **Invalidations:** History of cache invalidations.
- **Tags:** Use "Manage Tags" to organize your CloudFront setup with labels.
- **Versions:** Version history of distribution configuration.
- **View Metrics:** Shows your website's traffic, data flow, and error trends.
- **Schedule Backups:** A cron job auto-backs up CloudFront config changes regularly.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

5.3.1 Configuring CloudFront Behaviours



Behavior Tab

CloudFront Distribution Behaviors

Cache behaviors are routing rules that control how CloudFront processes requests for different content types within a single distribution. They allow you to configure multiple origins and apply different caching, security, and delivery policies based on URL path patterns.

Cache behaviors let you customize:

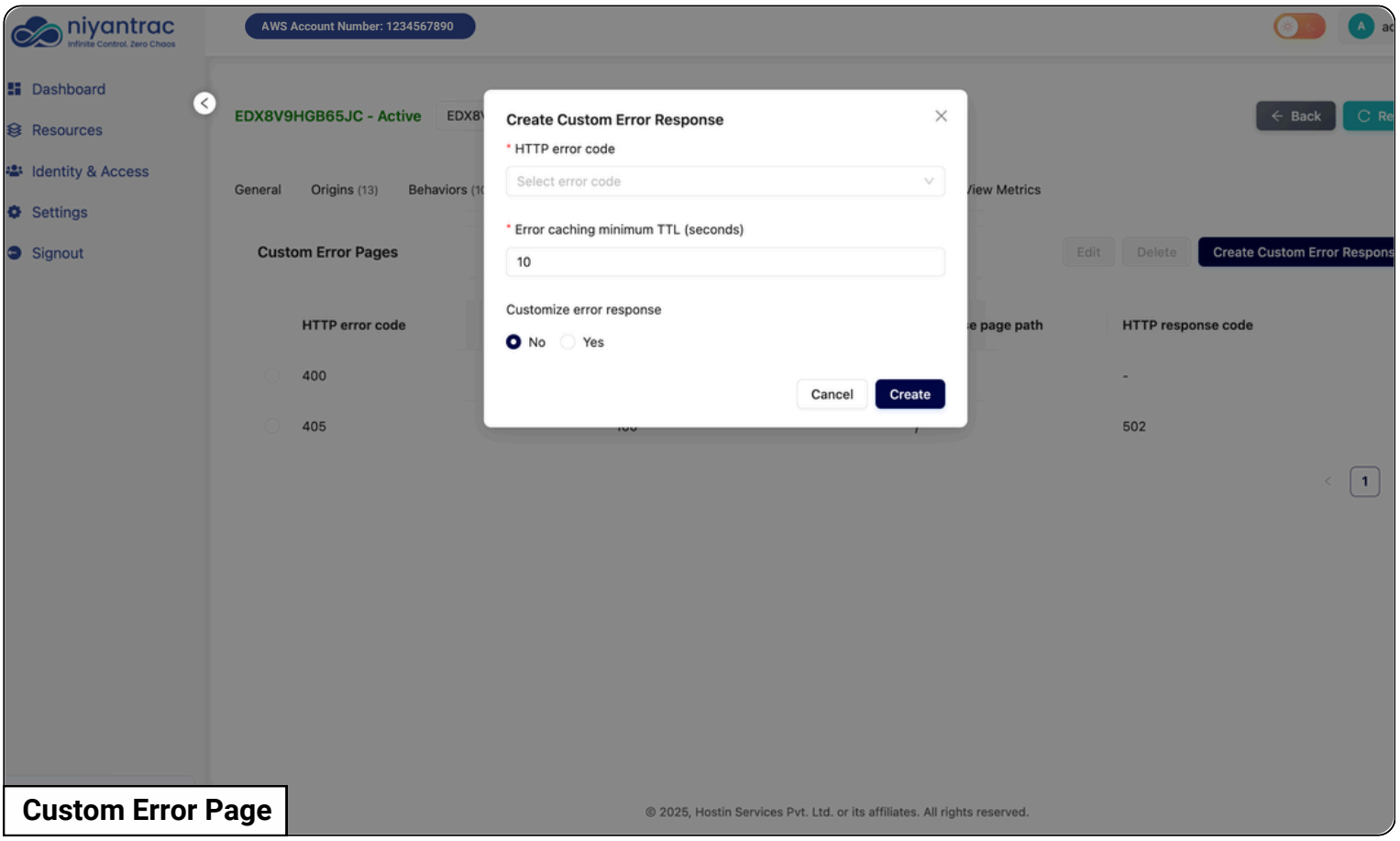
- Origin selection: Route different URL paths to separate origin servers (S3 buckets, load balancers, or custom HTTP servers)
- Caching policies: Set TTL values, cache key parameters, and compression preferences per content type
- Request handling: Configure query string forwarding, header passing, and HTTP methods allowed
- Security settings: Apply viewer protocol policies (HTTP/HTTPS), WAF rules, and origin access controls per path

- **Actions**

  You can change the order of these rules using the 'Move Up' and 'Move Down' buttons. Moving a behavior up means it will be checked earlier.

  Since the rules are checked from top to bottom based on "Precedence," being able to "Move Up" or "Move Down" a behavior allows you to change its priority. If a rule is more specific, you'll generally want it higher up so it's matched before a broader, more general rule.

5.3.2 Setting Up Custom Error Pages

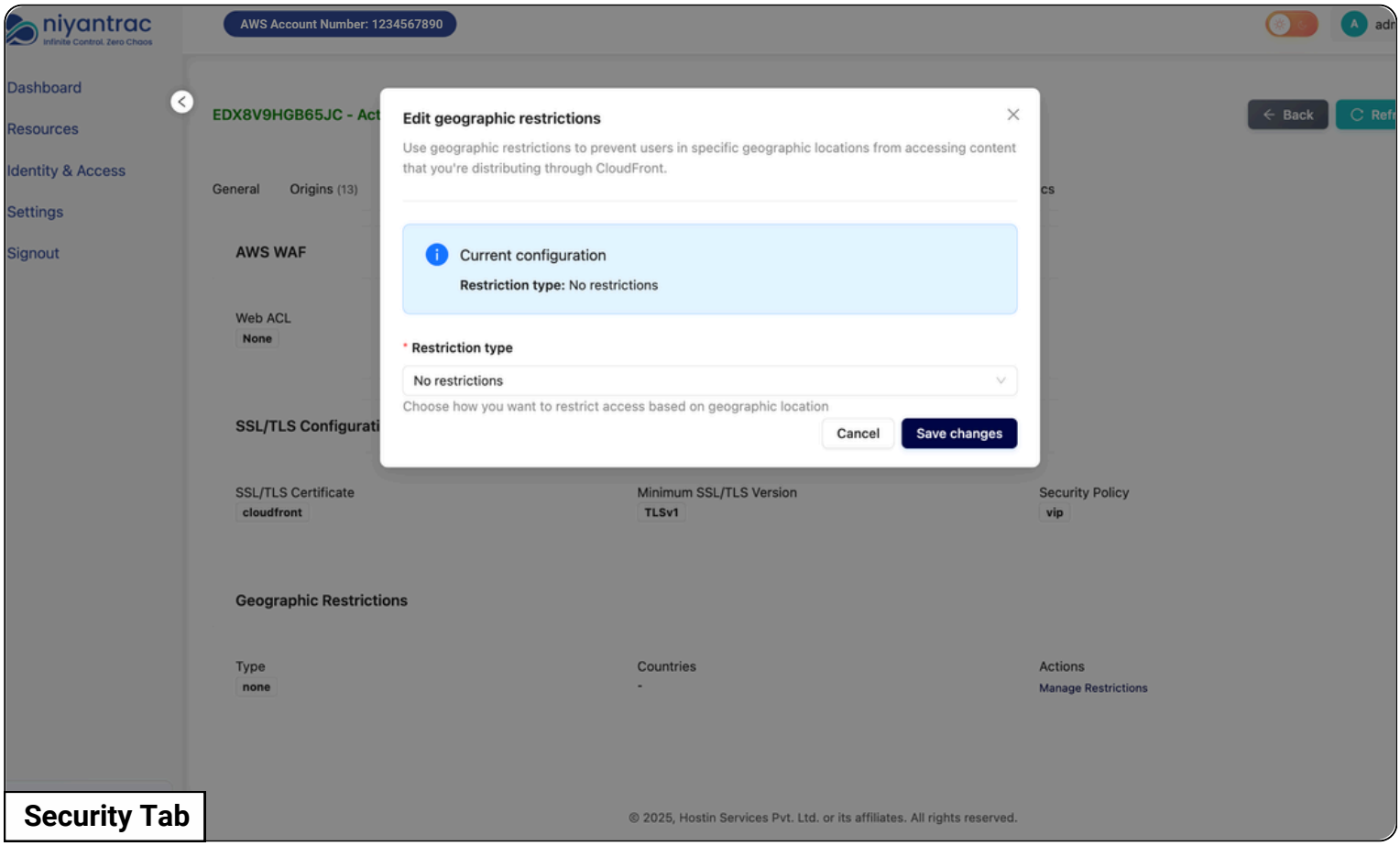


Custom Error Page

When a user tries to access content and your website has an issue (like a page not found or a server problem), CloudFront can show a custom error page you design.

- **Go to "Error Pages" tab: This section lets you see and manage existing custom error pages.**
- **Click "Create Custom Error Response":** This opens a window to set up a new custom error page.
- **Choose the HTTP Error Code:** You pick the **type of error** this custom page is for (e.g., "404" for "page not found" or "502" for a server issue).
- **Error Caching Minimum TTL (seconds):** This value determines the duration, in seconds, for which CloudFront caches an error response before reattempting to retrieve the correct content from the origin.
- **Enable Custom Response:** Select "Yes" to use **your own custom page**. If you pick "No," CloudFront shows its standard error message.
- **Provide Page Path:** If you chose "Yes," you'll enter the **exact web address** where your custom error page is stored (e.g., **/my-404-page.html**).
- **Set Response Code:** You decide **what error code CloudFront should send** back to the user's browser. It's usually the same as the original error (like sending a "404" response for a 404 error page).
- **Create:** Once everything's set, click "Create" to save your custom error page rule.

5.3.3 Geographic Restrictions Explained



Security Tab

This section lets you control who can access your website content based on their country.

a. Why Use Restrictions?

This is about blocking or allowing specific countries from accessing your content.

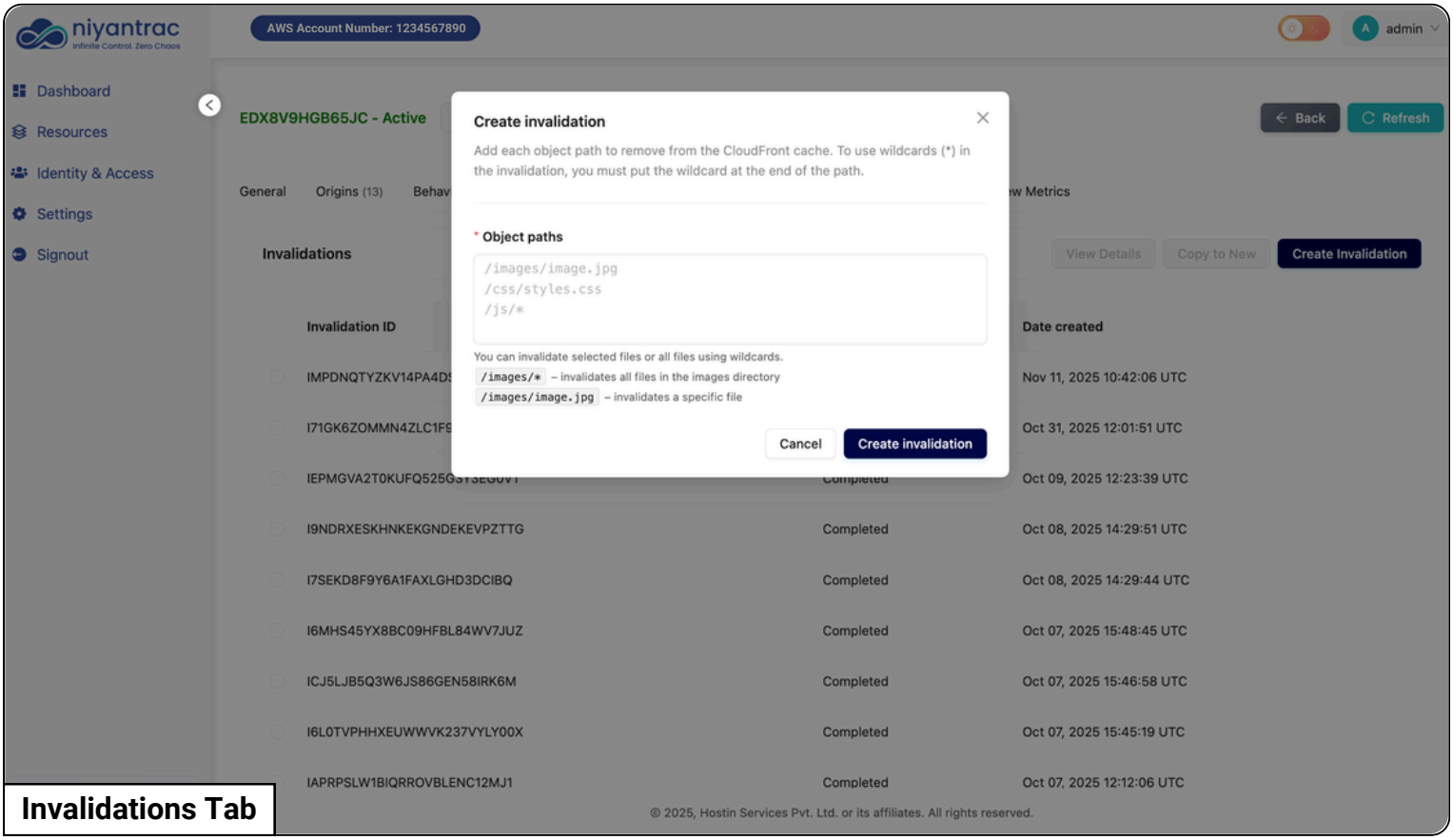
b. How to Set Up Restrictions

You choose how to control access to your content:

- **No restrictions:** Everyone can see it.
- **Allow list:** Only people from the countries you list can see your content.
- **Block list:** People from the countries you list cannot see your content.

After choosing, you simply add the specific countries to your list (for example, the United Arab Emirates, UAE). Once you're satisfied with your selections, click "Save changes" to activate your new rules.

5.3.4 Managing Cached Content with Invalidations



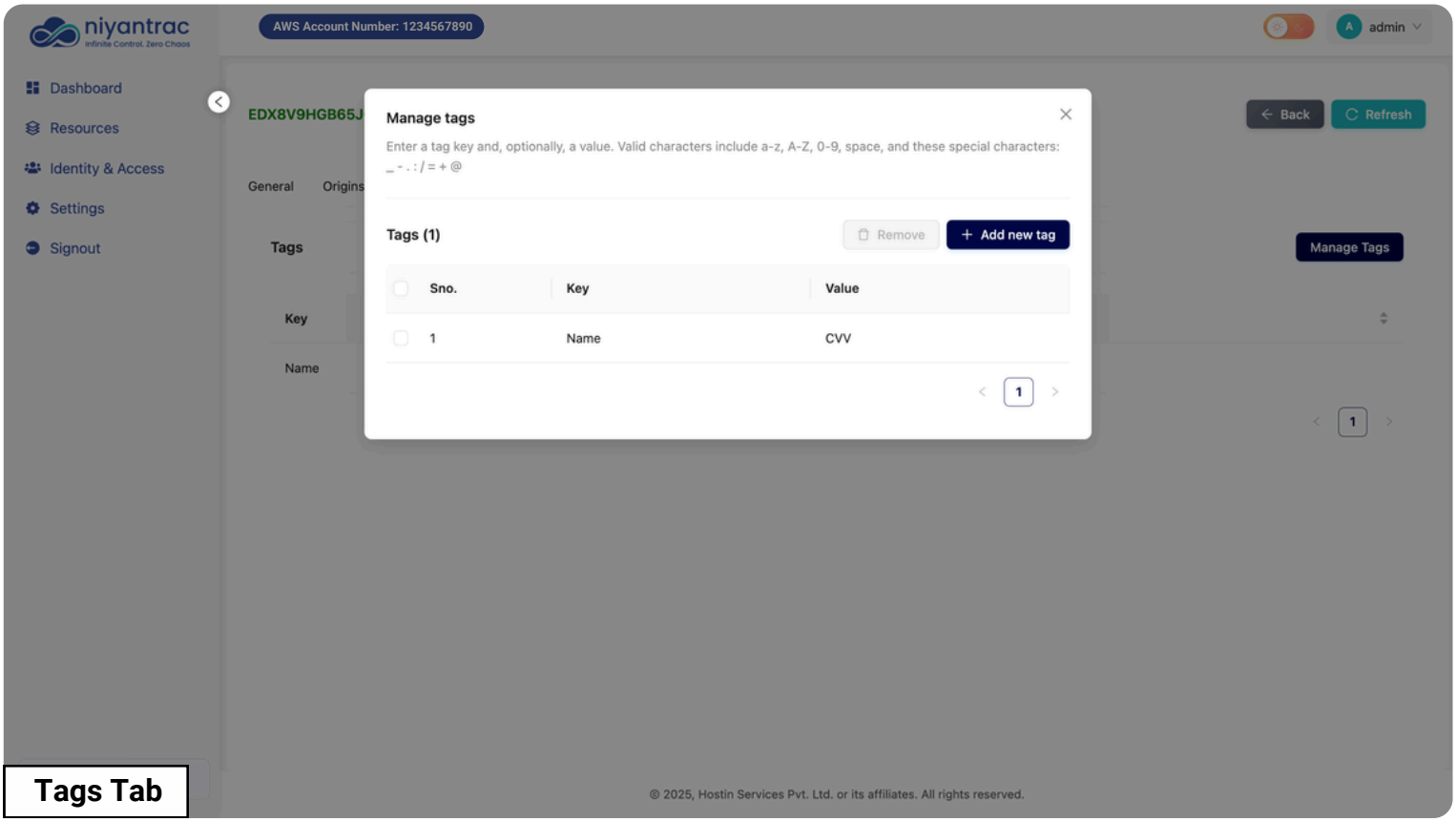
Invalidations Tab

This section enables you to instruct CloudFront to refresh cached content, ensuring that users receive the latest versions of your files. CloudFront stores copies of your website files in its cache for faster delivery; invalidations are used to force an update of these cached versions.

a. Initiating the Invalidation

- To execute the specified invalidation requests, click the "Create Invalidation" button located at the bottom of the dialogue box. This action transmits the command to CloudFront, instructing it to clear the designated cached content.
- The "Copy to new" button enables the creation of a new invalidation request, pre-populating the fields with the details of a previously selected invalidation for convenience.

5.3.5 Labelling Your CloudFront with Tags



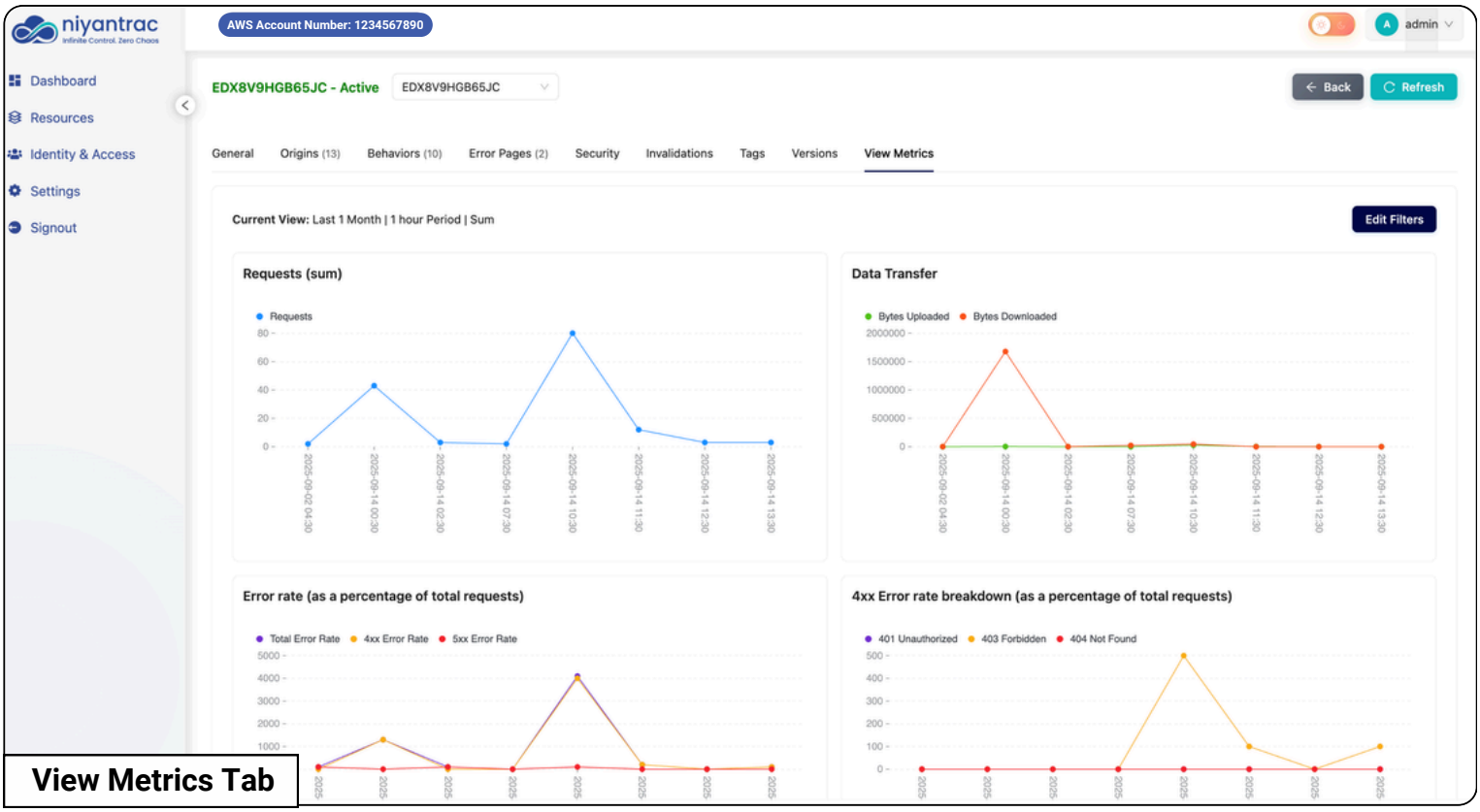
Tags Tab

a. The "Manage Tags" Window

- When you click the "Manage Tags" button, a modal window appears where you can add or change your labels.
- To add a new tag, just click the "+ Add new tag" button.
- You'll see any tags already on your CloudFront setup. For example, you might see "TagKey" as "TagValue", "Name" as "CVV"

In short: Tags are custom labels you use to organize and easily find your CloudFront setups, especially when you have many.

5.3.6 Understanding "View Metrics"



View Metrics Tab

This section shows you how busy your website is and if anything is going wrong.

a. The **"Requests" graph** simply counts **how many times people tried to access your website.** More requests mean more visitors.

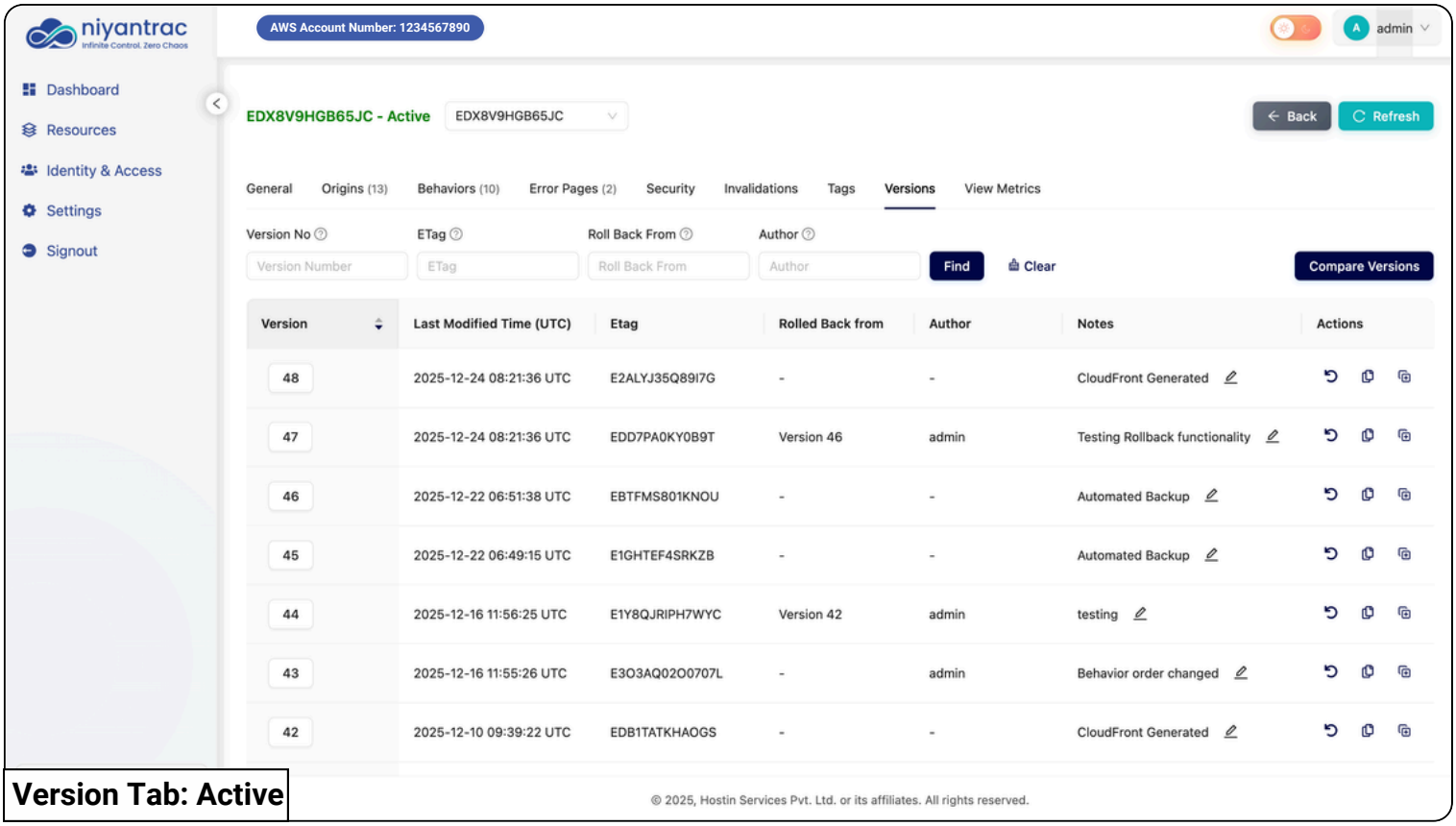
b. The **Data Transfer** graph shows how much information moved around, with the green line representing **Bytes Uploaded** and the red line representing **Bytes Downloaded.**

c. **Error Rates:** This graph indicates the frequency of issues encountered by users accessing your website.

- **Total Error Rate:** Represents the aggregate percentage of all errors.
- **4xx Error Rate:** Denotes client-side errors, typically caused by incorrect user requests (e.g., a "Page Not Found" error).
- **5xx Error Rate:** Signifies server-side errors, indicating an issue with the website's hosting infrastructure or application.

Basically, it's a quick way to see **your website's traffic and health at a glance.**

5.4 Working with Versions



Version Tab: Active

5.4.1 Versions Tab (For Active Distributions)

In the Versions tab of an active distribution:

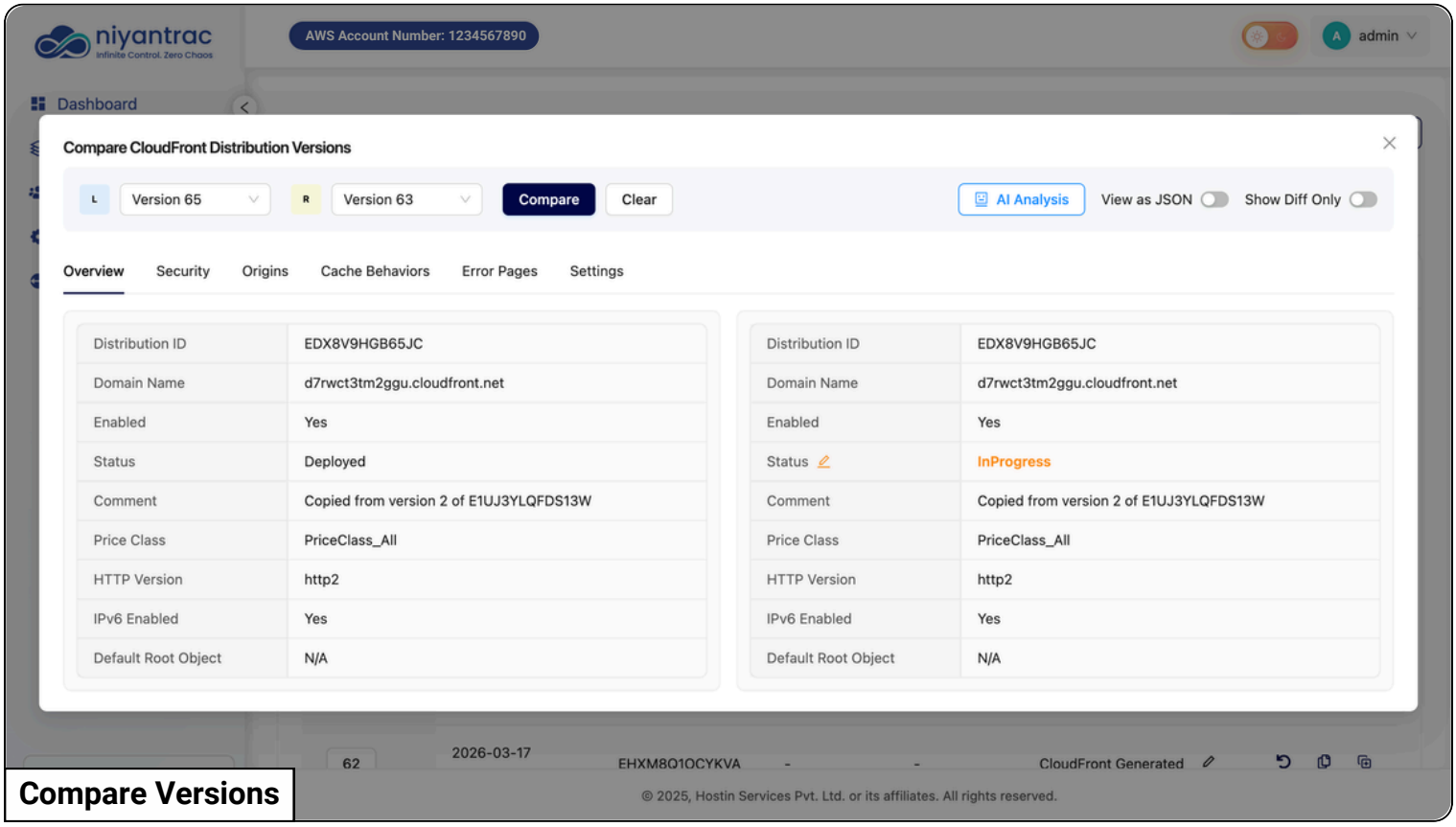
- You'll find a version table listing all saved configurations.
- For each version, the following actions are available:
- **Rollback:** Revert the distribution to this version.
- **Copy to Another Distribution:** Apply this version's config to another existing distribution.
- **Create New Distribution:** Launch a brand-new distribution using this version's config.

5.4.2 Versions Tab (For Deleted Distributions)

In the Deleted Distributions tab, selecting a Distribution ID and navigating to its Versions tab allows you to:

- Copy to Existing Distribution.
- Recreate Distribution using a selected version.

5.4.3 Compare Versions



Compare Versions

Comparing Distribution Versions

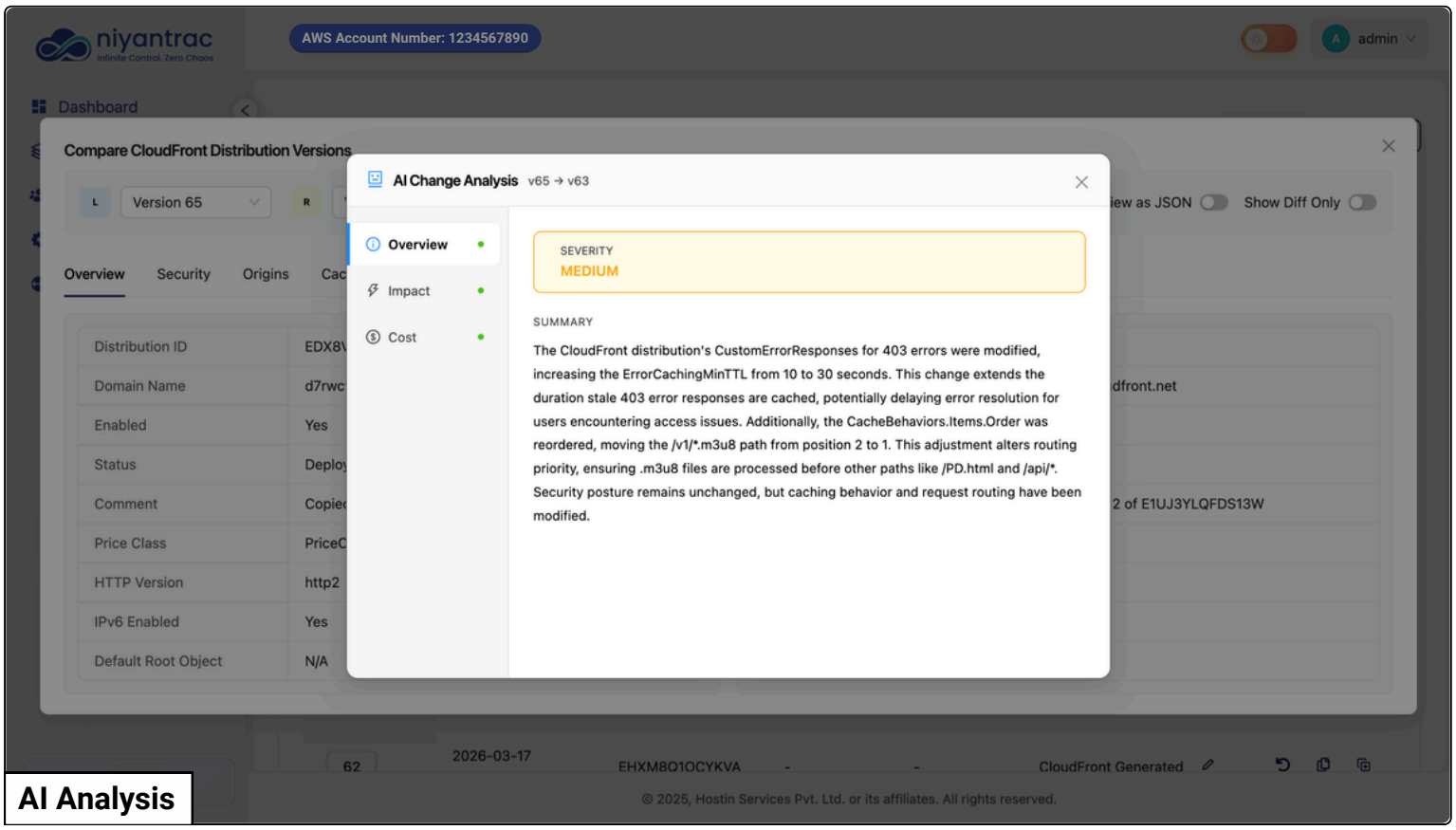
The version comparison tool allows you to view side-by-side differences between any two CloudFront distribution versions to understand changes before rollback or deployment decisions.

How to Compare Versions

- Select two versions from the dropdown menus (v1 and v2)
- Click Compare to display the configurations side-by-side
- Toggle Show only differences to filter out identical fields
- Use the tabs (Overview, Security, Origins, Cache Behaviors, Error Pages, Settings) to navigate different configuration sections

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

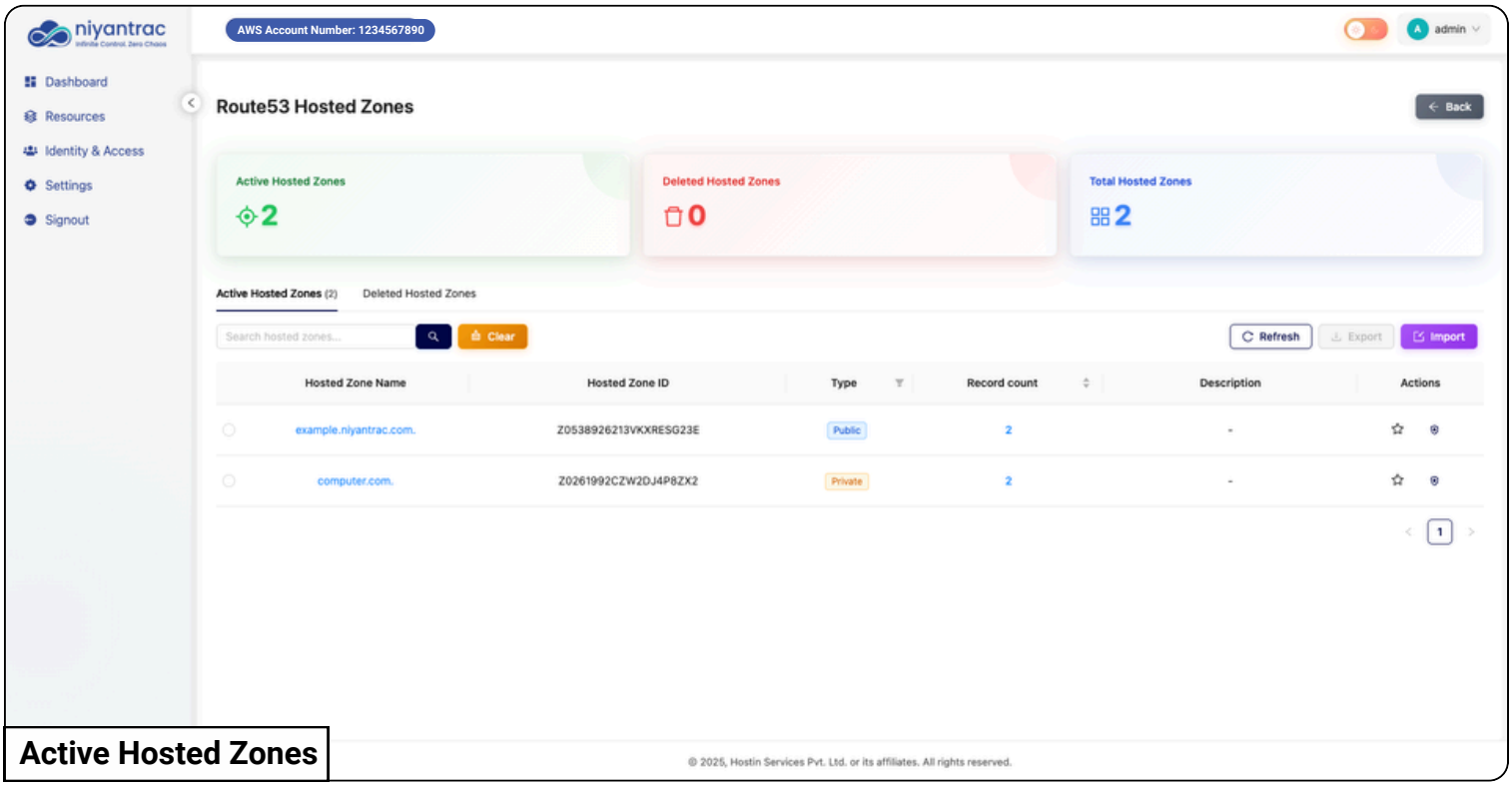
AI Change Analysis



AI Analysis

- Niyantrac's AI Change Analysis automatically reviews every configuration change across your CloudFront distributions, WAF Web ACLs, and Route53 records — and translates them into clear, human-readable summaries.
- Instead of manually diffing raw JSON configs, the AI highlights what changed, why it matters, and what risks it may introduce, all in seconds.
- The analysis is structured across three dimensions — Overview, Impact, and Cost — so you always know not just what changed, but how it affects your infrastructure and what it costs you.

6. Route 53 Hosted Zones



Active Hosted Zones

Zone Counts and Status

- **Total Managed Zones (4):** The system has records for 12 DNS configurations in total.
  - **Active Hosted Zones (2):** Only **two** DNS zones are currently active and being used
  - **Deleted Hosted Zones (2): Two** zones have been removed or archived.

Active Zone Details

The two active zones manage the domains example.niyantrac.com and computer.com.

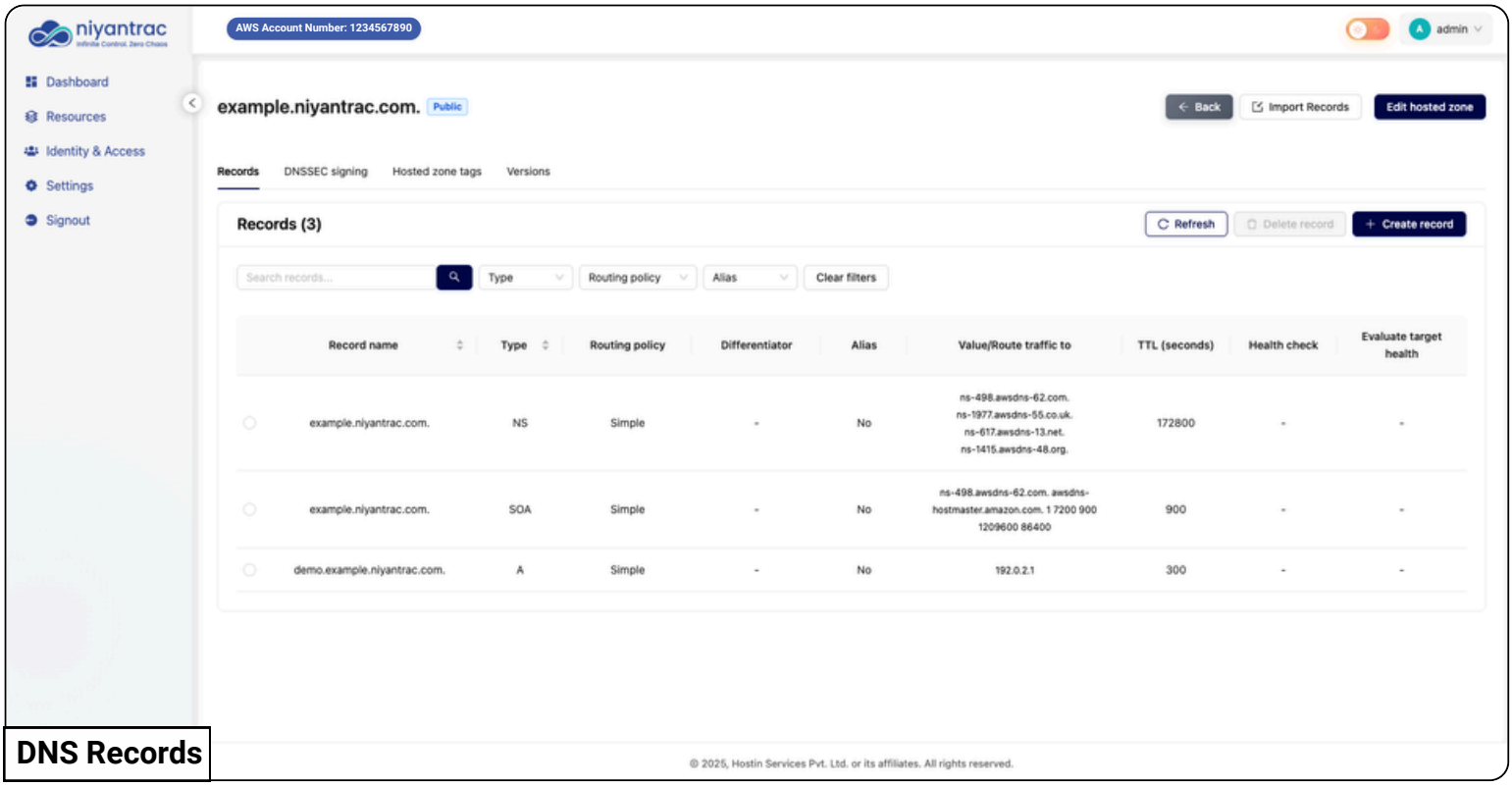
- **Public Type:** Both active zones are marked as Public. This is a critical technical point: it means the DNS records (the instructions on where to send traffic) are **visible to the entire internet** and are necessary for public-facing websites or services.
- **Unique Identifiers:** Each zone has a unique **Hosted Zone ID** (e.g., **Z0638...**), which is the internal AWS identifier used for API calls, billing, and system operations.
- **Record Count:** This indicates the **number of DNS resource records** (like A, CNAME, MX records) configured within the zone.

Management Features

The dashboard provides standard technical controls:

- **Refresh:** Used to update the displayed list with the latest status from the AWS service API.
- **Export:** Allows the user to download the list (likely in a bind or JSON format) for reporting or external management.
- **Import:** Suggests the ability to upload a configuration file (like a BIND or json zone file) to quickly create new hosted zones and records.

6.1. DNS Records



DNS Records

DNS Records Working Points

Core Required Records

These records are essential for any functioning DNS zone.

- **NS (Name Server):** This record lists the authoritative DNS servers (the servers that hold the master copy of the rules).

  It points to four servers ending in **awsdns-XX.org**. This confirms the domain is officially being managed by **Amazon Web Services (AWS) Route 53.**

  The **TTL (Time To Live)** is **172,800 seconds** (48 hours). This is a long duration, meaning internet resolvers will cache (remember) these server names for up to 48 hours before checking again.

- **SOA (Start of Authority):** This record holds administrative information about the zone, like the primary name server and the **hostmaster** (administrator's email address).

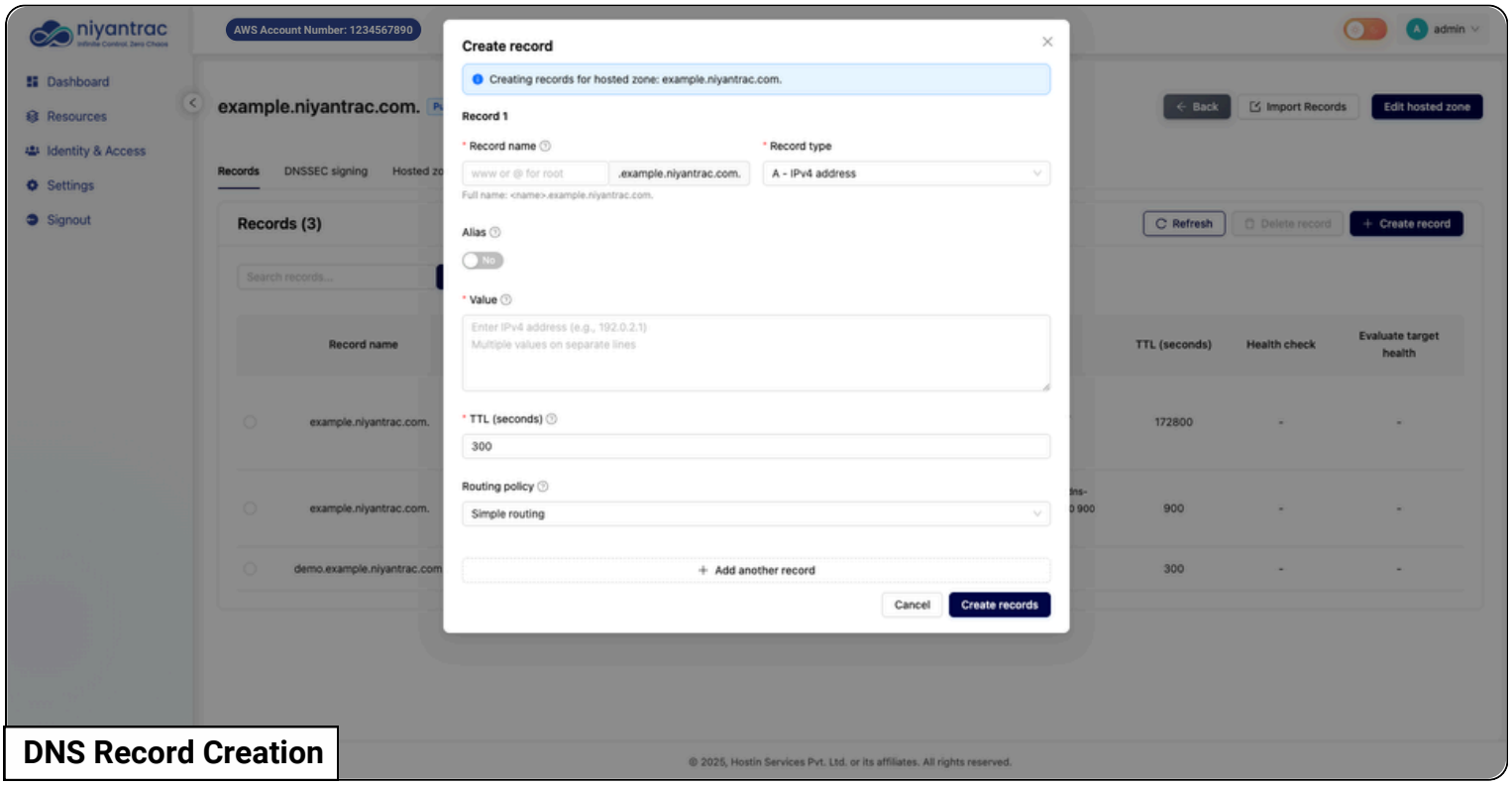
  The **TTL** is **900 seconds** (15 minutes), which is a short duration, allowing changes to other administrative details to propagate quickly.

Common Technical Settings

- **Routing Policy:** All displayed records use the **Simple** routing policy. This is the default and means there is one destination for the domain/sub-domain.
- **TTL (3600 seconds):** Most application records use a **Time To Live** of **3,600 seconds (1 hour)**.
- **Management Controls:** The user has technical controls to **Refresh, Delete record**, and **Create record,** allowing for real-time DNS configuration management.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

DNS Record Creation



DNS Record Creation

Record Definition

- **Hosted Zone:** The operation is targeted at the **example.niyantrac.com** DNS zone. This is the container for all the domain's rules.
- **Record Type (A - IPv4 address):** The user is creating an **A Record.**
  - **Technical Function:** An **A record** is the most fundamental DNS rule. It maps a human-readable domain name directly to a physical location on the internet, which is an **IPv4 address** (e.g., **192.0.2.1).**
- **Record Name:** The input field allows the user to specify a sub-domain (e.g., **www, blog, server1**).
- **Value (IPv4 Address):** This is the **destination IP address** where traffic for the specified Record Name will be sent. The field allows for multiple IPs, which can be used for basic load balancing or failover.

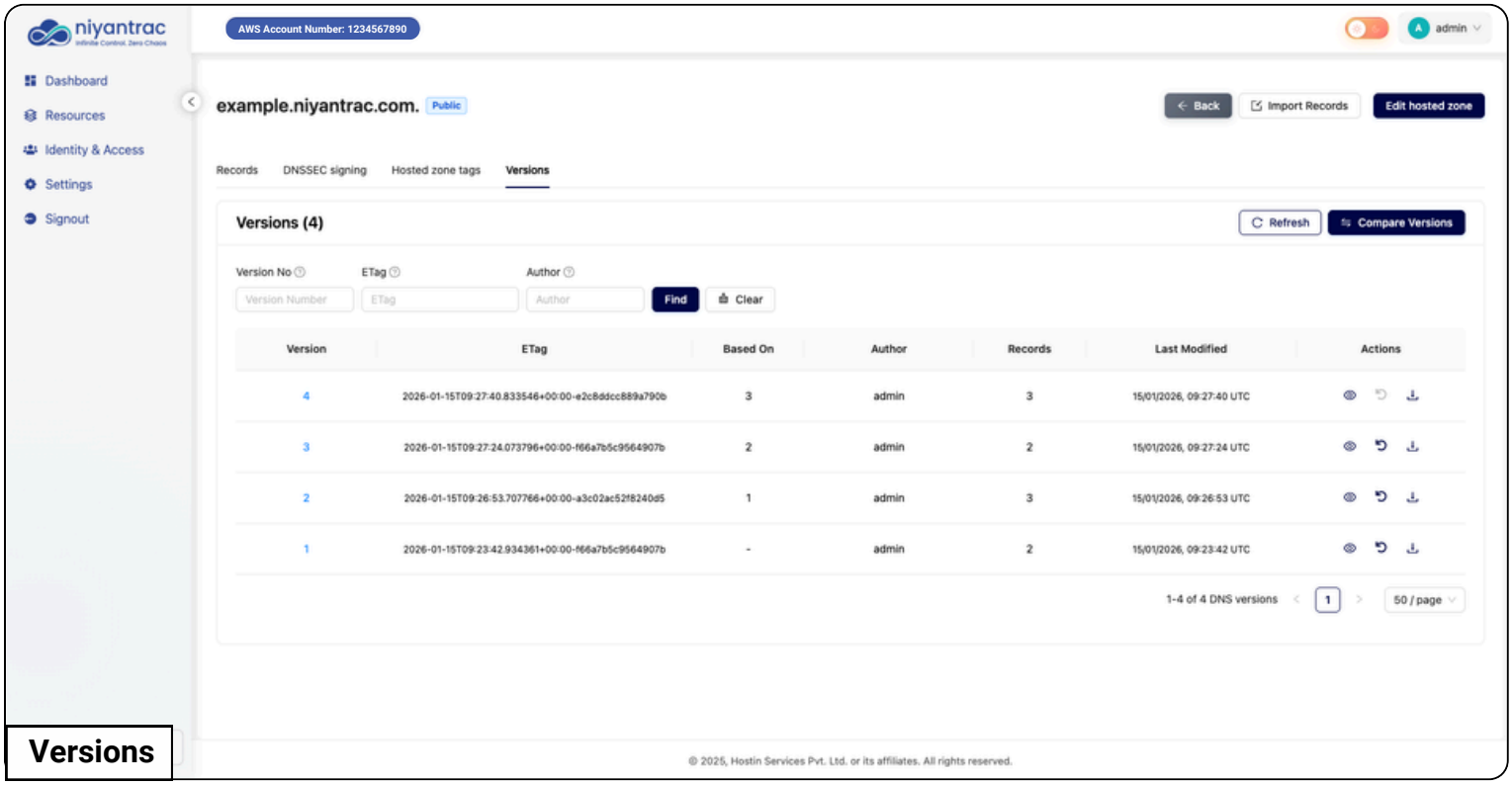
Caching and Routing

- **TTL (Time To Live): 300 seconds:**
  - **Technical Function:** This sets the amount of time (in seconds) that intermediate servers (like your Internet Service Provider's DNS server) should **cache** or remember this rule before asking Route 53 for an update.
- **Routing Policy: Simple routing:**
  - Technical Function: This is the default and most basic way to direct traffic. It means the record is configured to send all matching traffic to the specified **Value** (the IP address) without any complex checks or rules.

Optional Configuration

- **Alias:**
  - Technical Function: An Alias record is a Route 53 extension that lets you point a domain name to another AWS resource (like an S3 bucket or a CloudFront distribution) instead of a fixed IP address

6.2 Hosted Zone Versions



Version Tracking and Count

- **Total Versions (4):** The system has recorded **four distinct configurations** (or states) for the DNS records of **example.niyantrac.com**. This shows a history of changes, allowing administrators to track what the DNS looked like at different points in time.
- **Version Number:** The versions are numbered sequentially from **1 (oldest)** to **5 (current).**
- **Current State (Version 5):** The most recent version shows the zone currently has **8 DNS records.**

DNS Record Change Auditing

This feature automatically tracks and records every time the set of DNS rules (records) for the Hosted Zone is modified, providing a crucial technical audit trail.

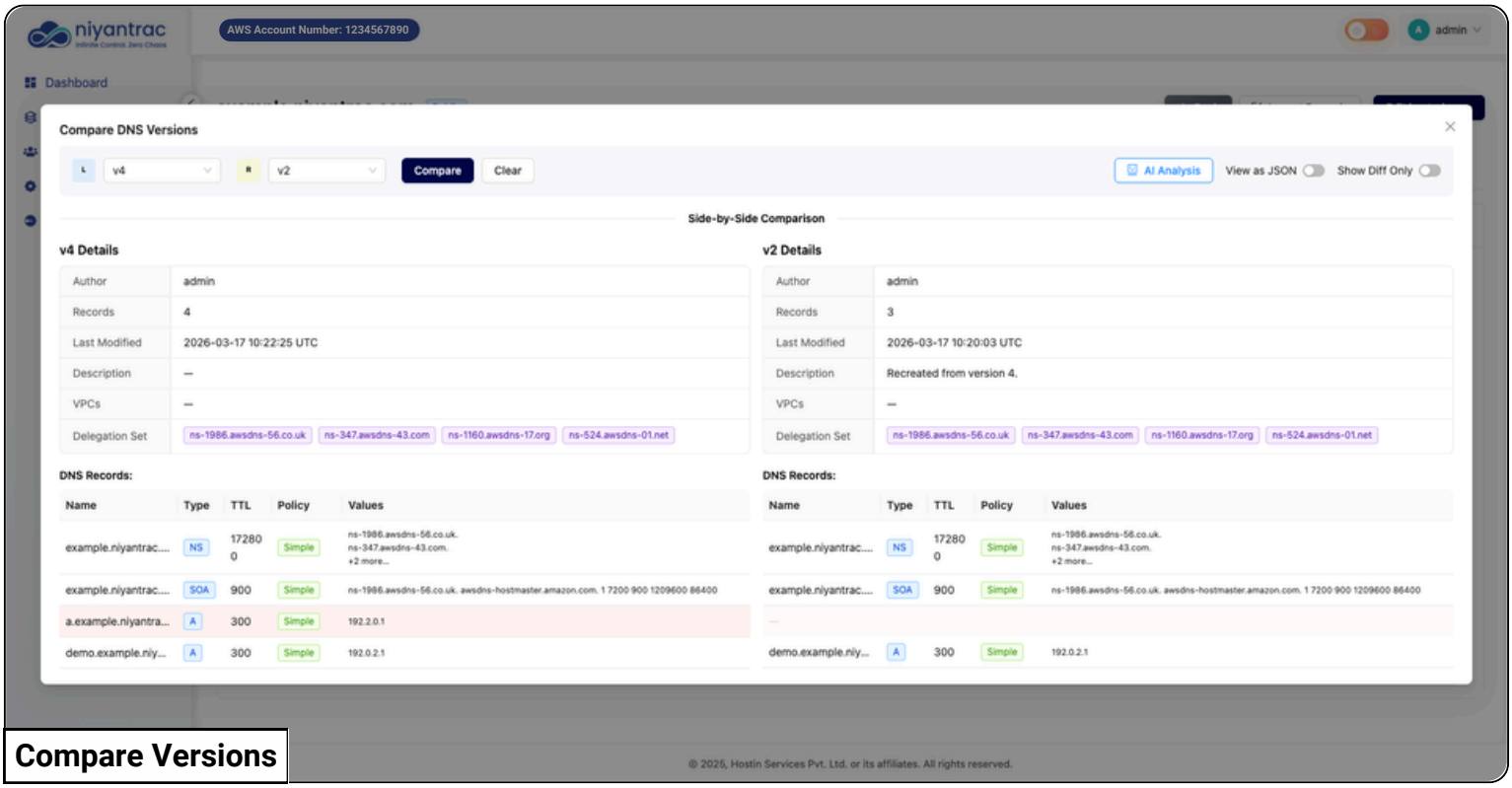
Management Capability

- **Rollback Capability:** Since the record count for each version is stored, this log facilitates **technical rollback**. An administrator can quickly identify a stable configuration (e.g., Version 4, which had 9 records) and use the system's "Compare Versions" or "Revert" features to **restore the DNS state** to that exact point in time.
- **Compare Versions:** The **"Compare Versions"** button is a key technical feature. It allows an administrator to quickly view the **exact line-by-line** differences between any two configurations (e.g., Version 4 and Version 5) to understand precisely what changed.
- **Export Version:** The download icon in the **Actions** column enables the **export of the specific version's configuration file**. This is used to create a **technical backup** of the DNS state or for **external analysis** or migration to another system.

This version history provides a powerful technical safety net for **auditing, and recovering** from configuration errors.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

Compare DNS Versions



Compare Versions

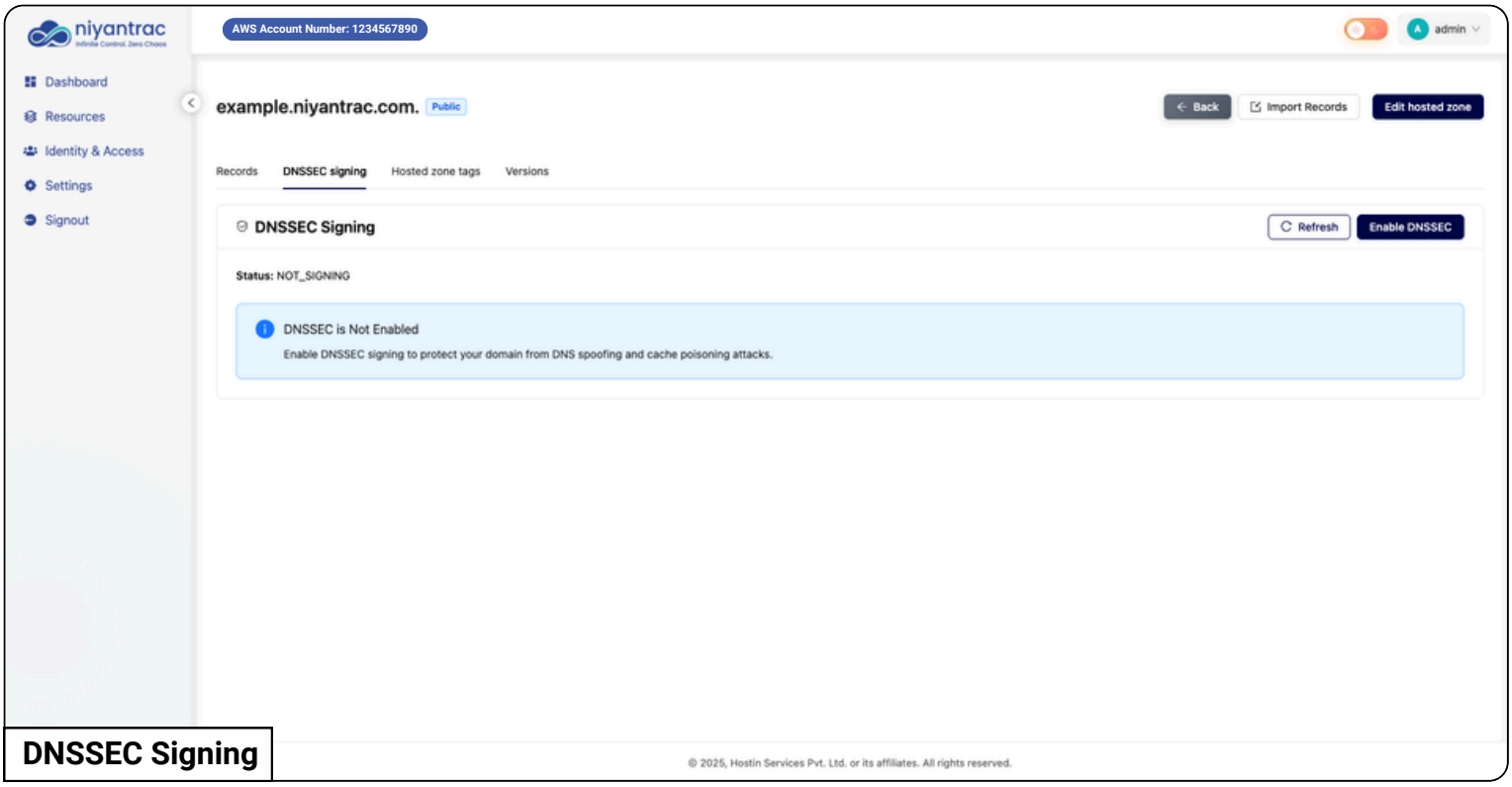
How to Compare Versions

- Select two versions from the dropdown menus (v1 and v2)
- Click Compare to display the configurations side-by-side
- Toggle Show only differences to filter out identical fields

AI Analysis

- Niyantrac's AI Change Analysis automatically reviews every configuration change across your Route53 records.
- translates them into clear, human-readable summaries.

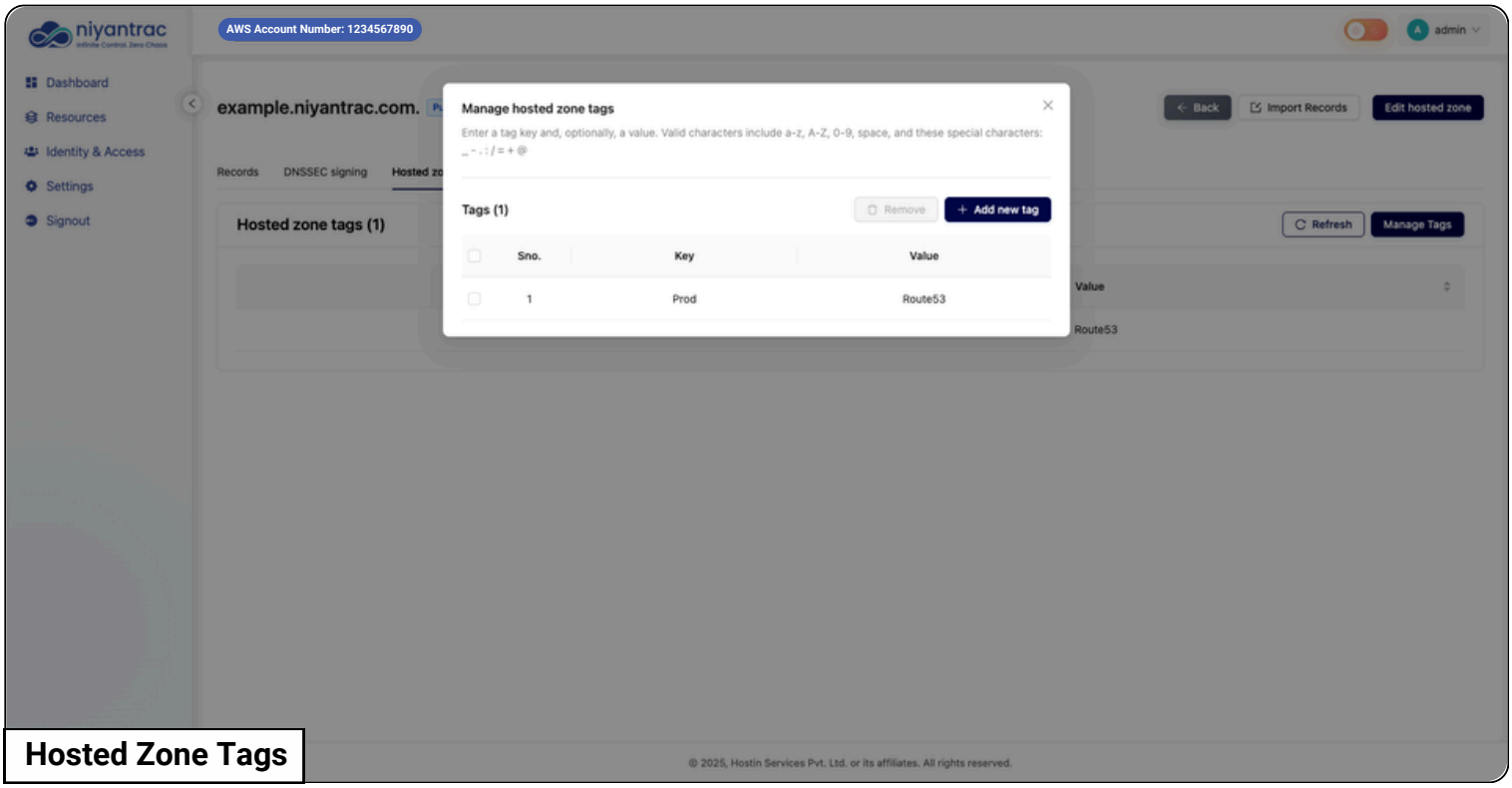
6.3 DNSSEC Signing



DNSSEC Signing

- **Feature Status:** The technical status is explicitly NOT_SIGNING, and the dashboard confirms DNSSEC is Not Enabled.
- **Current State:** The DNS records for example.niyantrac.com are not digitally signed, leaving the domain's resolution vulnerable to security exploits.
- **Security Risk:** The system warns the domain is currently unprotected against DNS spoofing and cache poisoning attacks.
  - DNS Spoofing allows an attacker to redirect users to a malicious site.
  - Cache Poisoning involves feeding fraudulent information to DNS resolvers.
- **Mitigation Action:** The presence of the "Enable DNSSEC" button provides the administrative action required to initiate the technical process of creating and configuring digital signatures (cryptographic keys) for the zone's records.
- **Purpose:** Enabling DNSSEC adds a layer of cryptographic integrity to the DNS records, ensuring that when a user requests the domain's IP address, the response is authentic and hasn't been tampered with.

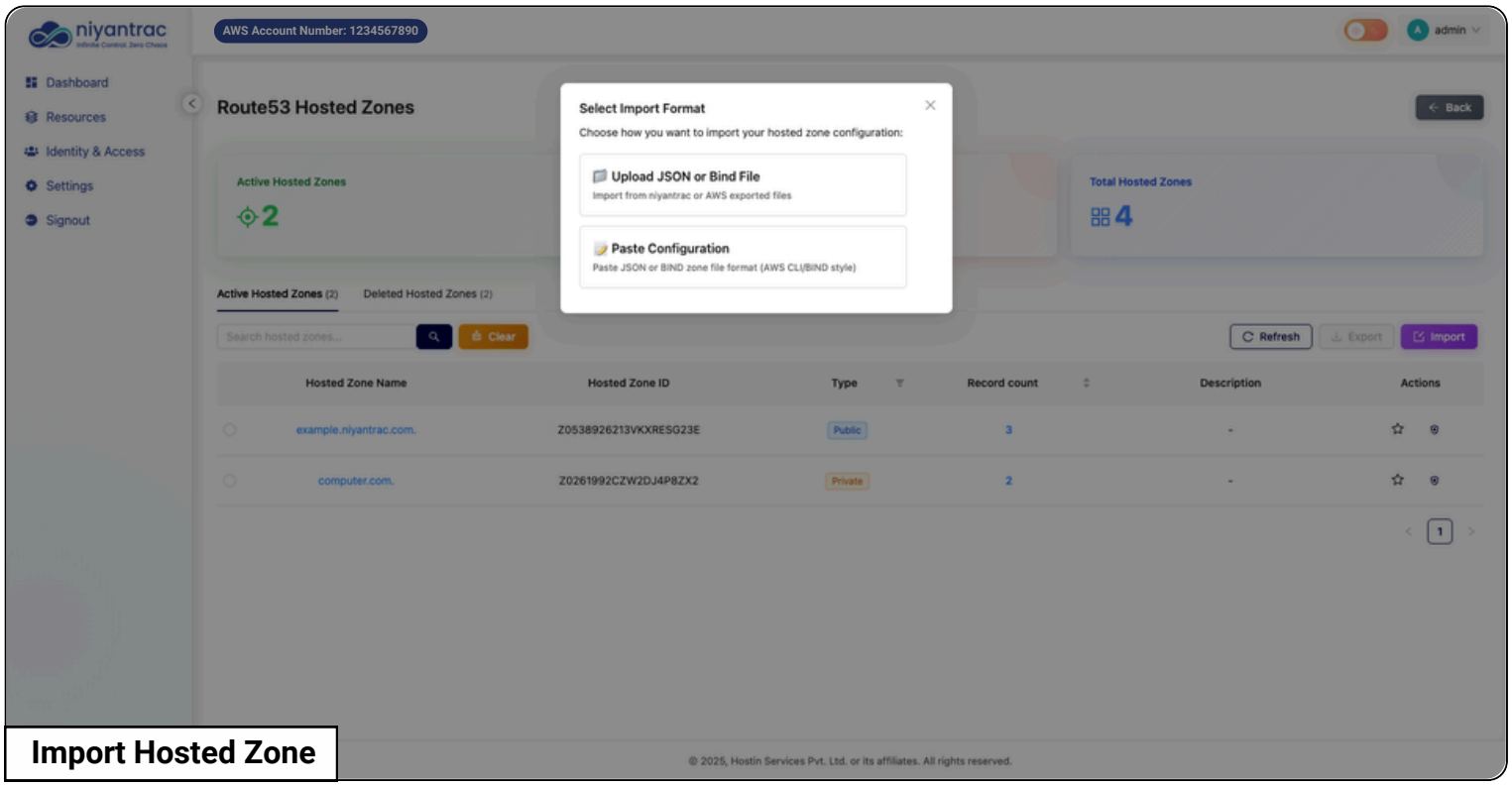
6.4 Hosted Zone Tags



Hosted Zone Tags

- **Tagging Functionality:** The purpose of this feature is to allow the administrator to attach metadata (tags) to the Route 53 resource.
- **Tag Count:** The section indicates 1 tag is currently defined (Hosted zone tags (1)), although the actual Key/Value data is not visible in the rows.
- **Structure:** Tags use a Key-Value pair structure (e.g., Environment: Production, Owner: Billing-Team), which are customizable, user-defined labels.

6.5 Import Hosted Zone

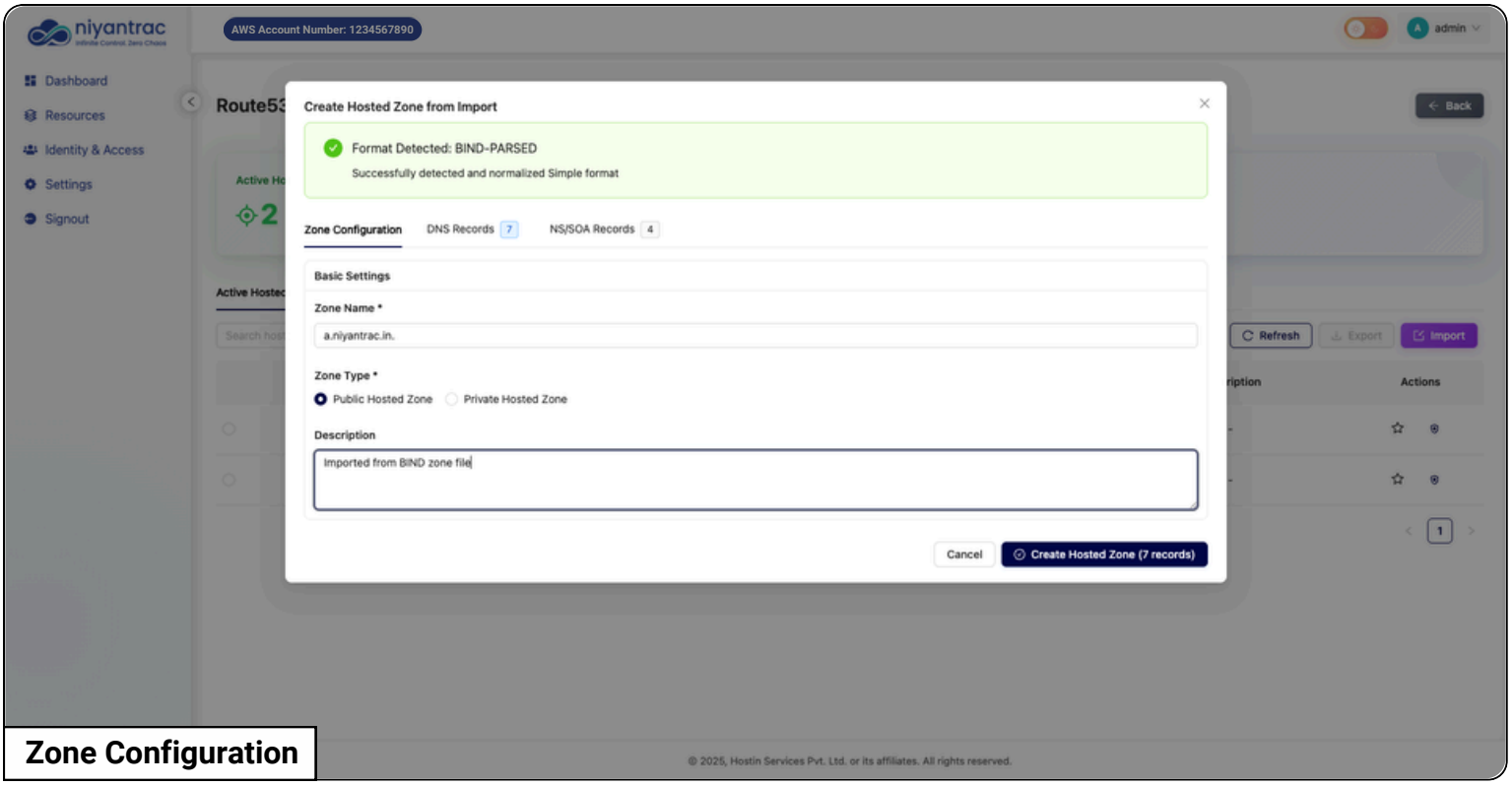


Import Hosted Zone

- **Goal:** To quickly create or update a Hosted Zone by loading a complete set of DNS records, bypassing manual entry.
- **Supported Formats:** The system accepts two primary configuration file formats:
  - **JSON (JavaScript Object Notation):** A structured, machine-readable format typically used for **AWS CLI/API operations** and exported files.
  - **BIND File (Zone File):** A plain-text, human-readable format that is the industry standard for DNS configurations, allowing imports from traditional DNS servers.
- **Import Methods:** Two technical methods are provided:
  - **File Upload:** Allows the user to select and transfer a complete JSON or BIND file from their local machine or a known vault/export location.
  - **Paste Configuration:** Allows the user to directly copy and paste the raw JSON or BIND text content into the interface for immediate processing.

UI Guide: Manage & Roll Back CloudFront Configurations

Create Hosted Zone from Import



Zone Configuration

Format Validation: The system has successfully detected and parsed the input as a BIND zone file (a standard DNS text format) and normalized it into a manageable format.

- **DNS Record Count:** The imported file contains a total of 7 DNS Records. This is the complete set of rules that
- will be loaded into the new zone.

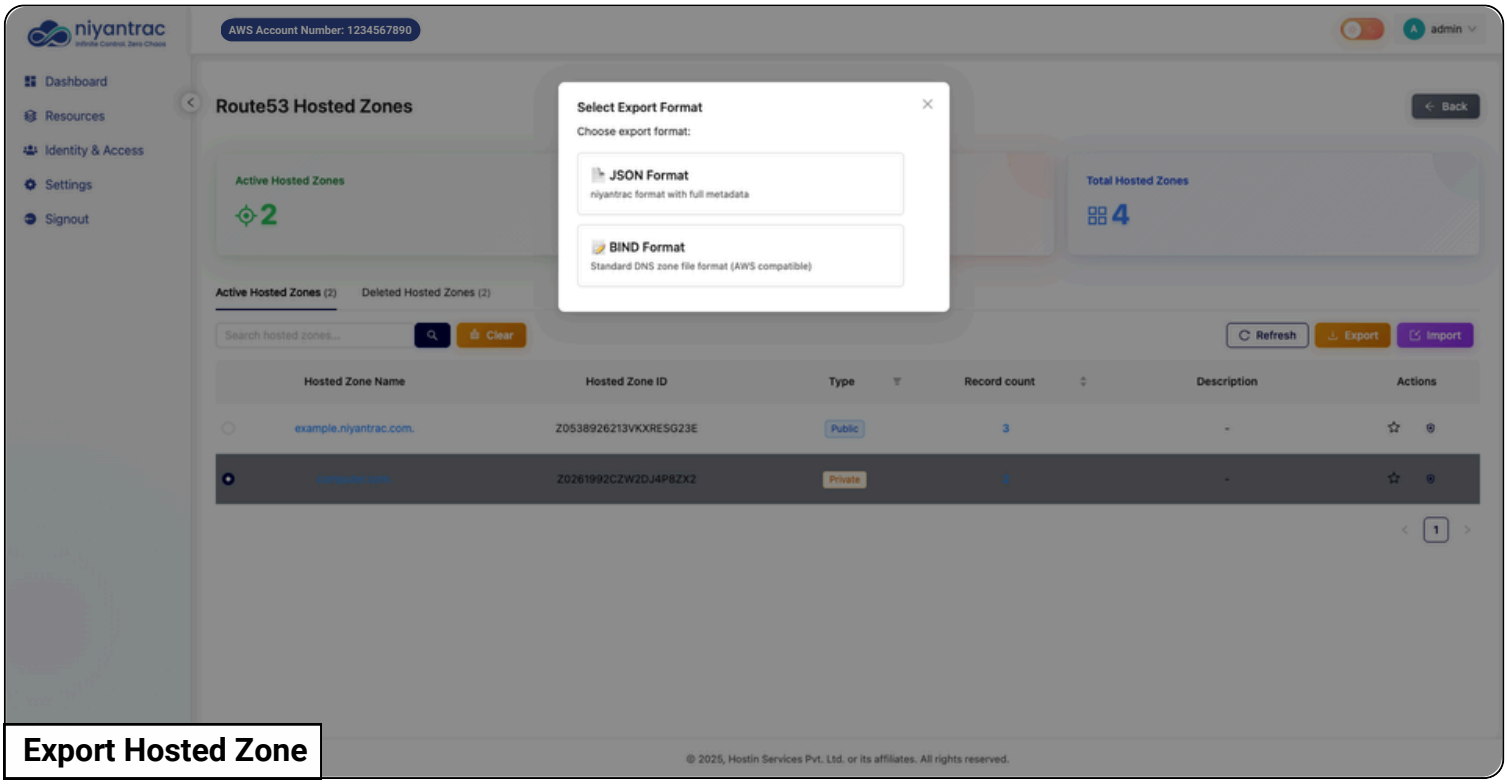
Required Records Check: Out of the 7 total records, 4 are NS/SOA Records. These are the fundamental records

- required for DNS authority and delegation, confirming the file is structurally valid.

Zone Naming: The new zone is assigned the Zone Name a.niyantrac.in based on the imported file content.

- **Zone Type Selection:** The configuration is set to create a Public Hosted Zone. This means the zone's DNS records will be publicly accessible and resolve traffic from the internet.
- **Required Records Check:** Out of the 7 total records, 4 are NS/SOA Records. These are the fundamental records required for DNS authority and delegation, confirming the file is structurally valid.
- **Description Tagging:** The zone is automatically labeled with the description "Imported from BIND zone file," providing immediate technical context about its origin.
- **Action:** The user is ready to execute the Create Hosted Zone (7 Records) action, which will provision the new DNS zone and activate all 7 records within the service.

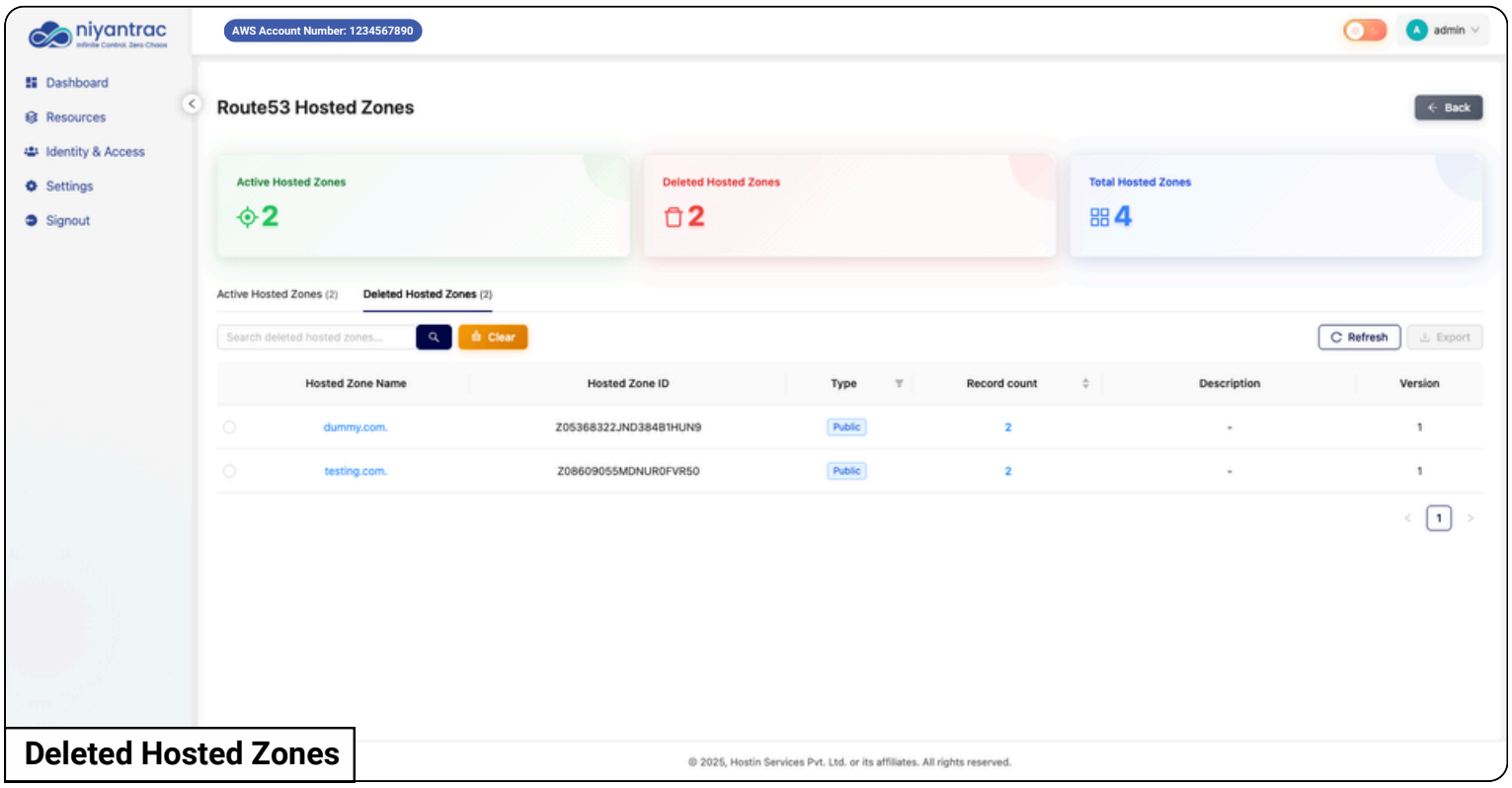
6.6 Export Hosted Zone



Export Hosted Zone

- **Goal:** To generate a complete copy of the DNS records and settings for external use.
- **Format Options:** The system offers two industry-standard technical formats:
  - **JSON Format:** Exports the configuration with full metadata. This highly structured format is ideal for API integration, scripting, and use with AWS tools (like the CLI) or the Niyantrac.
  - **BIND Format:** Exports the configuration as a standard DNS zone file. This plain-text format is essential for technical migration to non-AWS DNS servers or for traditional DNS archival and management.
- **Functionality:** Selecting either option triggers the serialization of the current DNS configuration into the chosen file format for download. This ensures data portability and disaster recovery capability for the zone.

6.7 Deleted Hosted Zones



Deleted Hosted Zones

Mixed Zone Types

The deleted zones were a mix of both Public and Private types:

- **Public (2 Zones):** These zones were previously used to direct **internet traffic** for publicly accessible services. Since they are deleted, those services are no longer reachable via these specific domain names.
- Private (0 Zones): These zones were previously used to direct traffic **only within a private, internal network** (like a VPC in AWS). Their deletion suggests internal services or development environments were shut down.

Domains and Usage

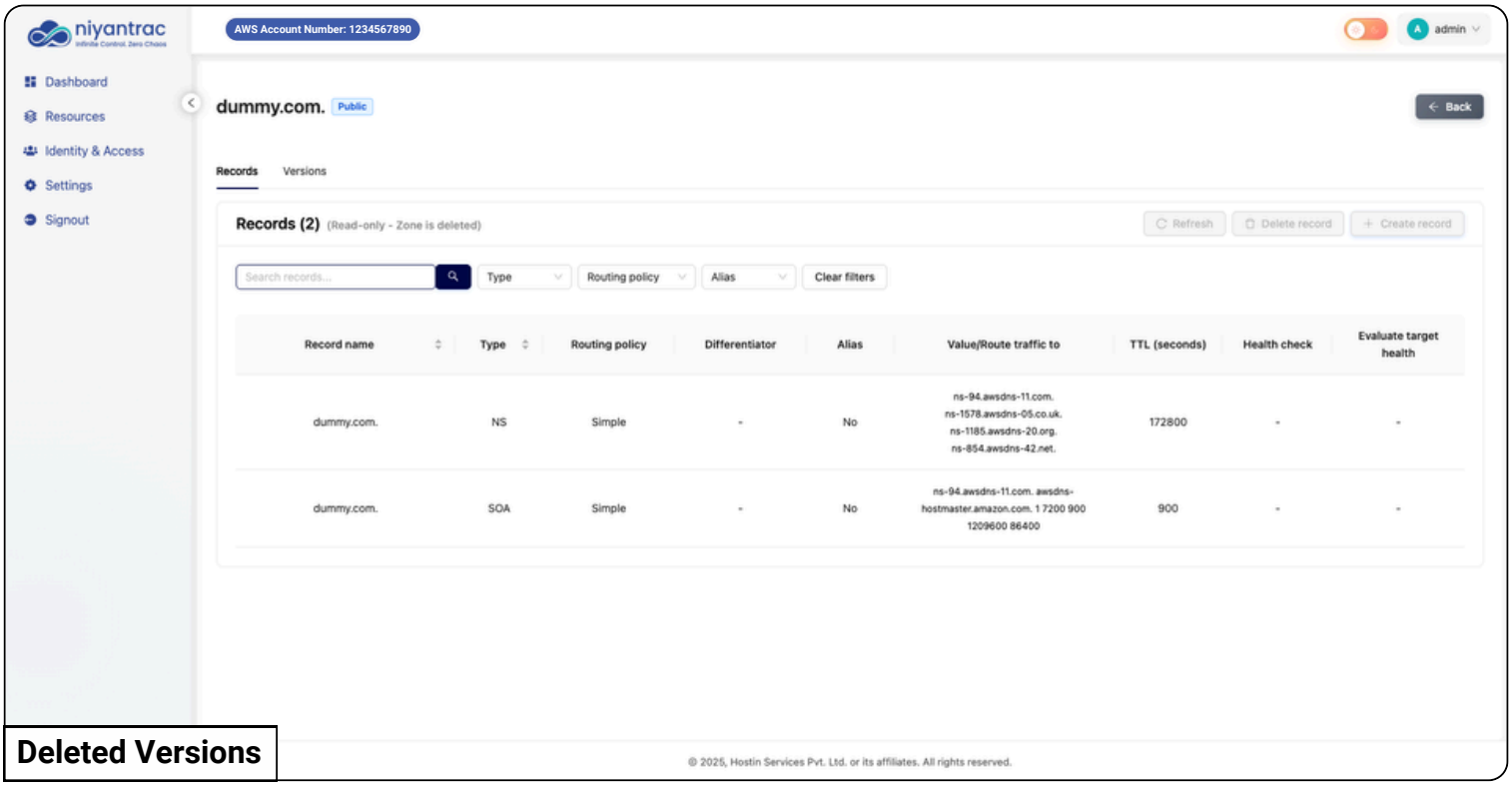
- **Record Counts:** The number of DNS rules (**Record Count**) in these deleted zones varied:

Technical History

- **Version Tracking:** The "**Version**" column is a key technical detail. It shows how many times the configuration for that specific Hosted Zone ID was modified before it was deleted.
    - The highest version is **6** , indicating that its DNS rules were modified six times over its lifespan. Other zones have versions 1, 2, or 3, suggesting less frequent changes.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

Deleted Hosted Zones details

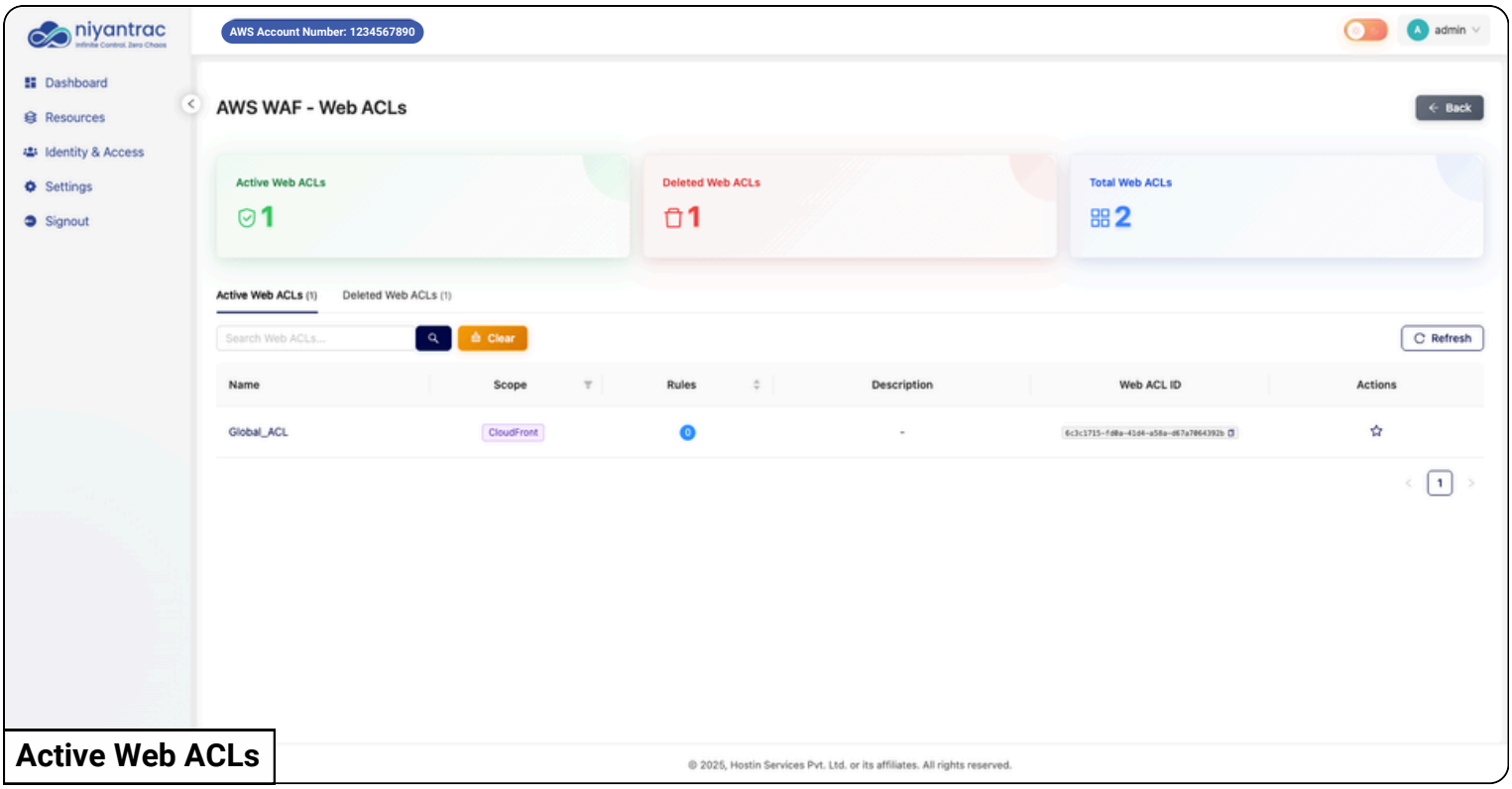


Deleted Versions

- **Version Count:** The zone has **two configuration snapshots (Versions 1 and 2)**, indicating it has been modified once since its initial creation.
- **Audit Trail:** Both changes were logged as being performed by the admin user, providing a clear access and action log.
- **Version Identifier (ETag):** Each version has a unique **ETag** (e.g., **2025-11-04T10...**), which is a technical fingerprint used to ensure the integrity of the configuration data.
- **Time Tracking:** The modifications occurred on the 4th of November, 2025, showing the time of the configuration changes (**19:45:22** and **19:48:59**).
- **Record Change Delta:** The key change between versions is the number of active DNS records:
  - **Version 1** started with **4 records.**
  - **Version 2** increased the count to **6 records**, meaning **two new records were added** to the zone's configuration in that update.
- **Management Control:** The **"Compare Versions"** button enables a technical diff operation to identify the exact two records that were added between V1 and V2. The Actions column (download/revert icons) allows for **data archival** and quick **rollback** to the previous, less-complex configuration **(V1)**.

7. WAF Vault

7.1 Web ACLs Management



Active Web ACLs

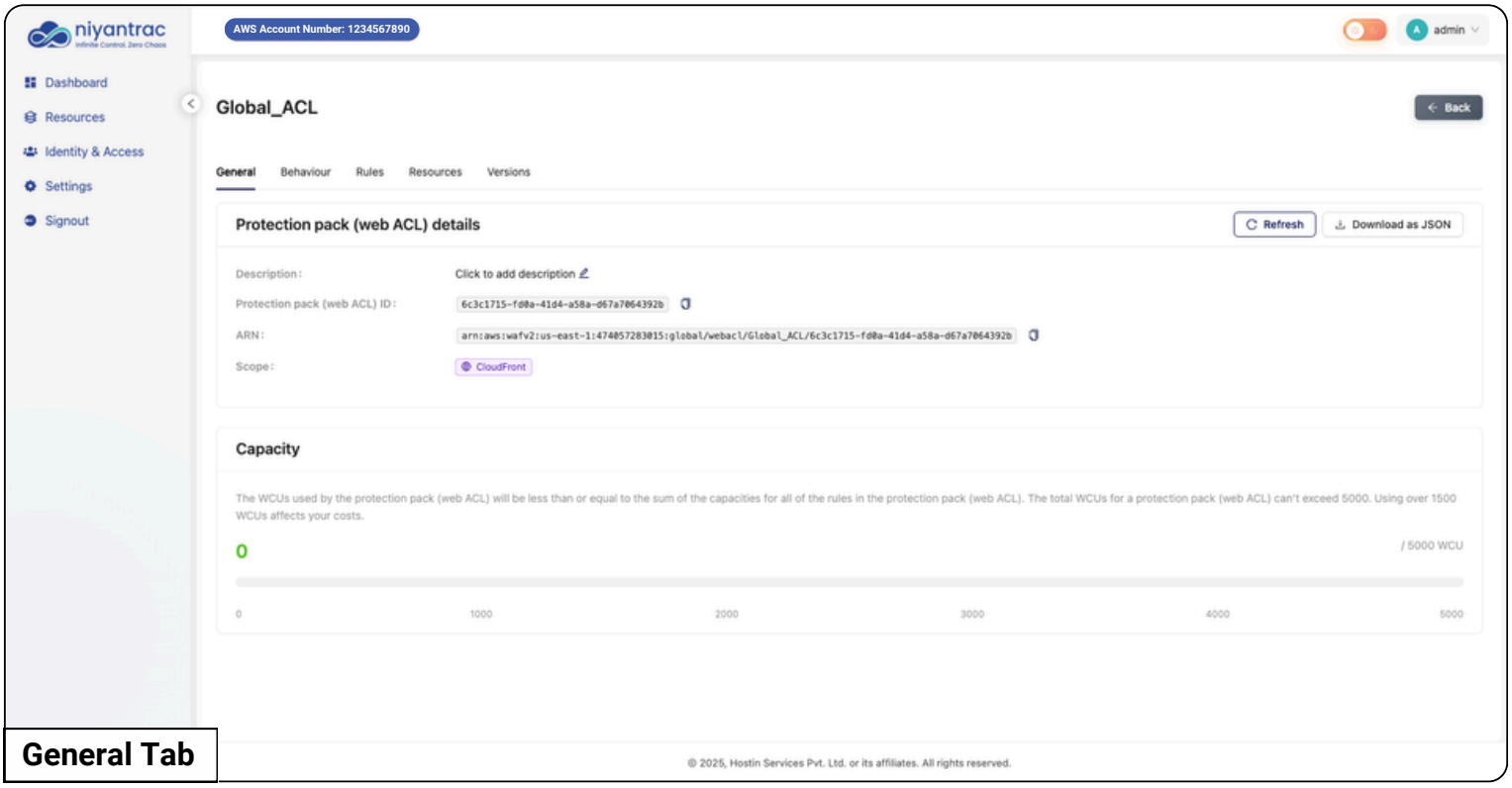
This interface displays the Web Access Control Lists (ACLs) management page for AWS WAF within the Niyantrac application. The page provides a comprehensive view of both active and deleted Web ACLs, allowing administrators to monitor and manage their web application firewall configurations.

Key Features

- Dual View Tabs: Toggle between Active Web ACLs (2) and Deleted Web ACLs (2) for tracking current and archived configurations
- Search and Filter: Quick search functionality with a clear button to locate specific Web ACLs efficiently
- ACL Details Table: Displays critical information including:
  - Name: Identifier for each Web ACL (e.g., Global_ACL, Regional_ACL)
  - Scope: Indicates whether the ACL is applied to CloudFront or Regional resources
  - Rules: Count of security rules configured within each Web ACL
  - Description: Custom notes about the Web ACL's purpose
  - Web ACL ID: Unique identifier for API and backup operations
- Actions Column: Star icon for quick access bookmarking and delete/archive functionality
- View Details Button: Access comprehensive configuration details and rule sets for each Web ACL

This interface enables version control and backup management for WAF configurations, supporting disaster recovery and rollback capabilities for your web application security rules.

7.2 Web ACL Details



General Tab

This page displays the comprehensive details for the "Global_ACL" Web Access Control List with a tabbed navigation interface for General, Behaviour, Rules, Resources, and Versions.

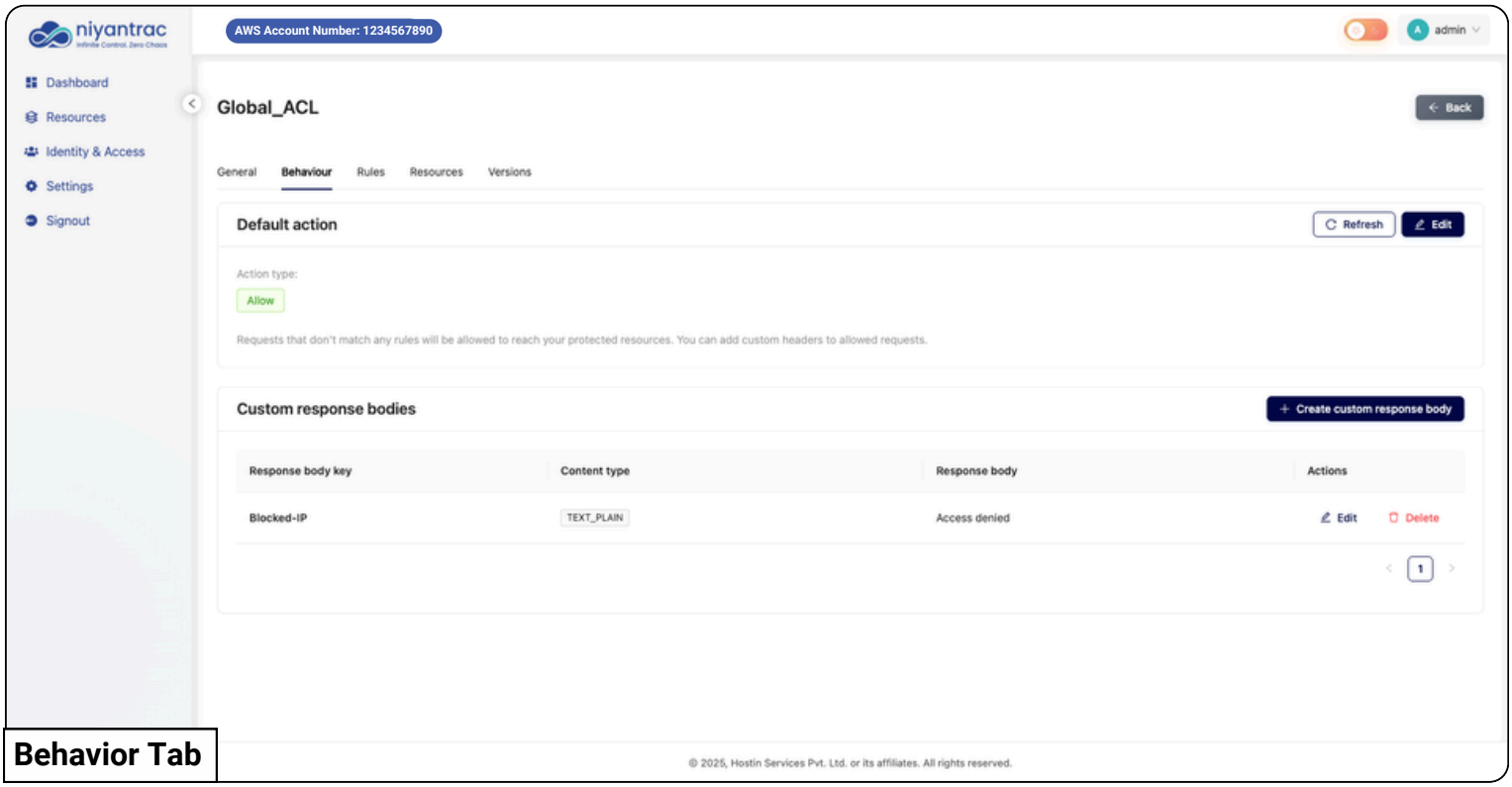
Protection Pack (Web ACL) Details

- The General tab presents core configuration information:
- Description: Editable field allowing administrators to add custom notes about the Web ACL's purpose and usage
- Protection Pack ID: Unique identifier (4d704074-bf64-4341-b402-72a0c4f8bd93) with copy functionality for API operations and backup references
- ARN: Full Amazon Resource Name for AWS API integration and cross-service linking
- Scope: Displays CloudFront designation, indicating this Web ACL applies to global CloudFront distributions
- Capacity Monitoring
- The interface includes a real-time capacity meter showing Web Capacity Units (WCUs) usage:
- Current Usage: 100 WCUs out of 5000 maximum capacity
- Visual Progress Bar: Green indicator showing low utilization (2% of total capacity)

Cost Information: Warning that exceeding 1500 WCUs affects pricing

This capacity tracking helps administrators monitor rule complexity and optimize costs while maintaining security coverage. The "Download as JSON" option enables configuration exports for backup and version control purposes.

7.3 Web ACL Behaviour Configuration



Behavior Tab

This page displays the behavior settings for the "Global_ACL" Web Access Control List, which control how the WAF responds to web requests.

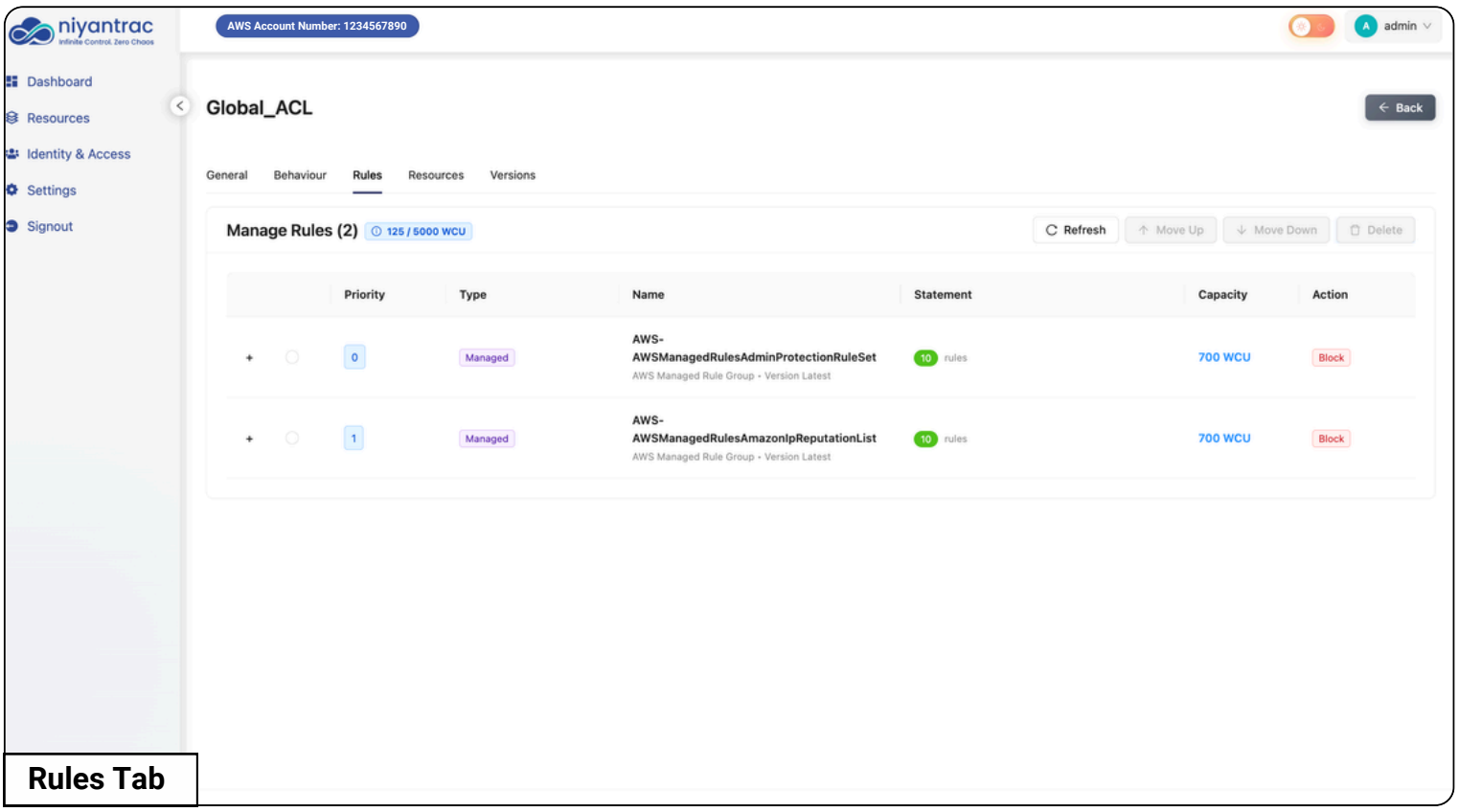
Default Action

- The default action configuration determines the Web ACL's behavior for requests that don't match any specific rules:
- Action Type: Set to "Allow", meaning requests that don't trigger any rules will be permitted to reach protected resources.
- Functionality: This fail-safe setting ensures legitimate traffic flows through when no blocking rules apply.
- Customization: Administrators can edit this setting using the Edit button to switch between Allow or Block as the default posture.

Custom Response Bodies

- This section manages predefined response messages sent to blocked users:
- Response Body Key: "blocked-ip-response" - identifier for the custom message template
- Content Type: TEXT_PLAIN format for simple, readable error messages
- Response Body: "Access denied" - the message displayed to users when their requests are blocked
- Management Options: Edit and Delete buttons allow modification or removal of custom responses

7.4 Web ACL Rules Management



Rules Tab

This page displays the security rules configured within the "Global_ACL" Web Access Control List, showing 2 rules consuming 101 out of 5000 Web Capacity Units (WCUs). Administrators can combine AWS-managed rule groups with custom rules to layer security, addressing both known threats and organization-specific requirements.

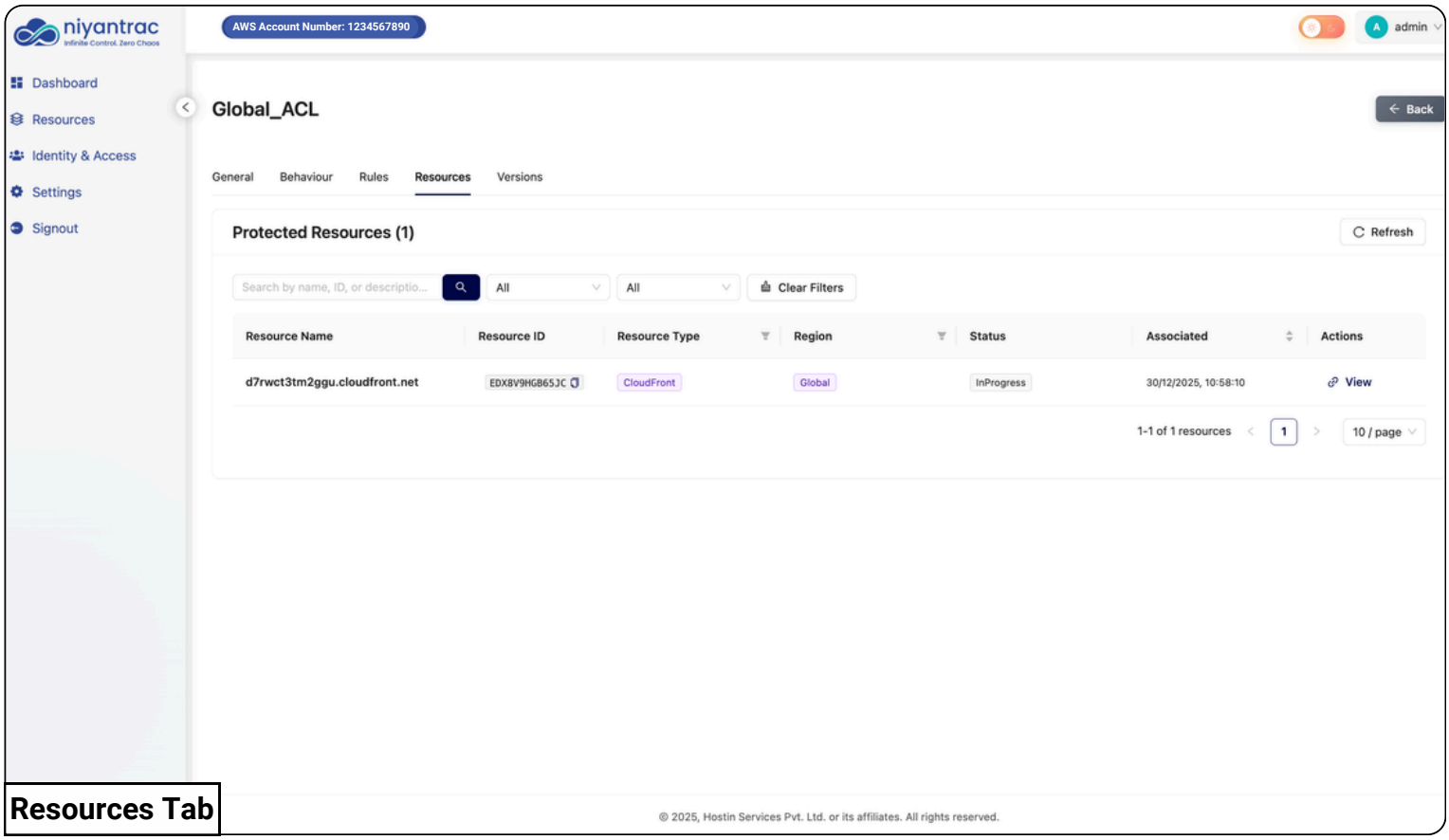
Management Features

- Rule Ordering: Priority numbers determine evaluation sequence, with lower numbers processed first to ensure important protections are evaluated before more specific rules.
- Expandable Rows: Plus icons allow viewing detailed rule configurations without cluttering the main interface.
- Toolbar Actions: Quickly refresh the rule set, move rules up or down to change their priority, and delete rules to respond rapidly to evolving security needs.
- Capacity Monitoring: Real-time WCU tracking ensures the Web ACL stays within AWS resource limits, preempting performance and cost issues as rules are added or updated.

Layered and Adaptable Protection

This rules interface empowers administrators to create multi-layered defenses using flexible, prioritized rule sets for web application security. AWS-managed rules, such as SQL injection and XSS protection, provide baseline threat mitigation while custom rules address application-specific conditions like country-based blocking, request rate limiting, or custom header validations. Administrators can rapidly tune, test, and update rules to respond to traffic trends, compliance mandates, or incident recovery—without downtime or manual reconfiguration

7.5 Protected Resources



Resources Tab

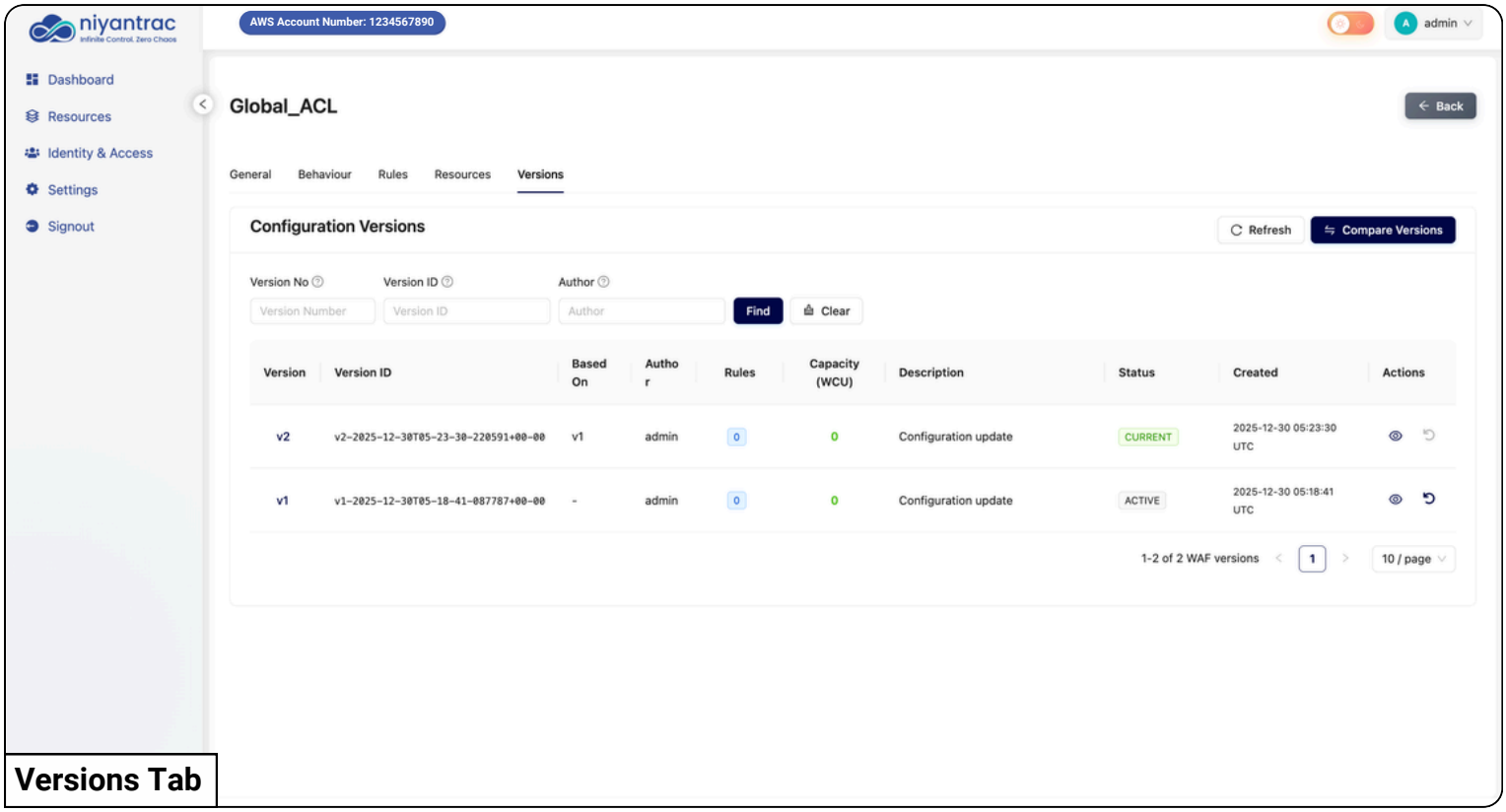
This page displays AWS resources currently protected by the "Global_ACL" Web Access Control List, showing 1 associated resource.

Protected Resources Table

- The table displays detailed information about each protected resource:
- Resource Name: d7rwct3tm2ggu.cloudfront.net - CloudFront distribution domain
- Resource ID: EDX89VHGB53JC (with copy functionality)
- Resource Type: CloudFront (purple badge) - indicates this Web ACL protects a CloudFront distribution
- Region: Global - reflects the worldwide scope of CloudFront and this Web ACL
- Status: Deployed (green badge) - confirms the Web ACL is actively protecting the resource
- Associated: 25/11/2025, 15:47:12 - timestamp showing when the Web ACL was linked to this resource
- Actions: View button for accessing detailed resource information

This interface allows administrators to track which CloudFront distributions or other AWS resources are protected by specific Web ACL security rules, ensuring proper coverage of their infrastructure.

7.6 Configuration Versions



Versions Tab

This page displays the complete version history for the "Global_ACL" Web Access Control List, with rollback capability as the core feature enabling instant restoration of previous configurations during security incidents or misconfigurations.

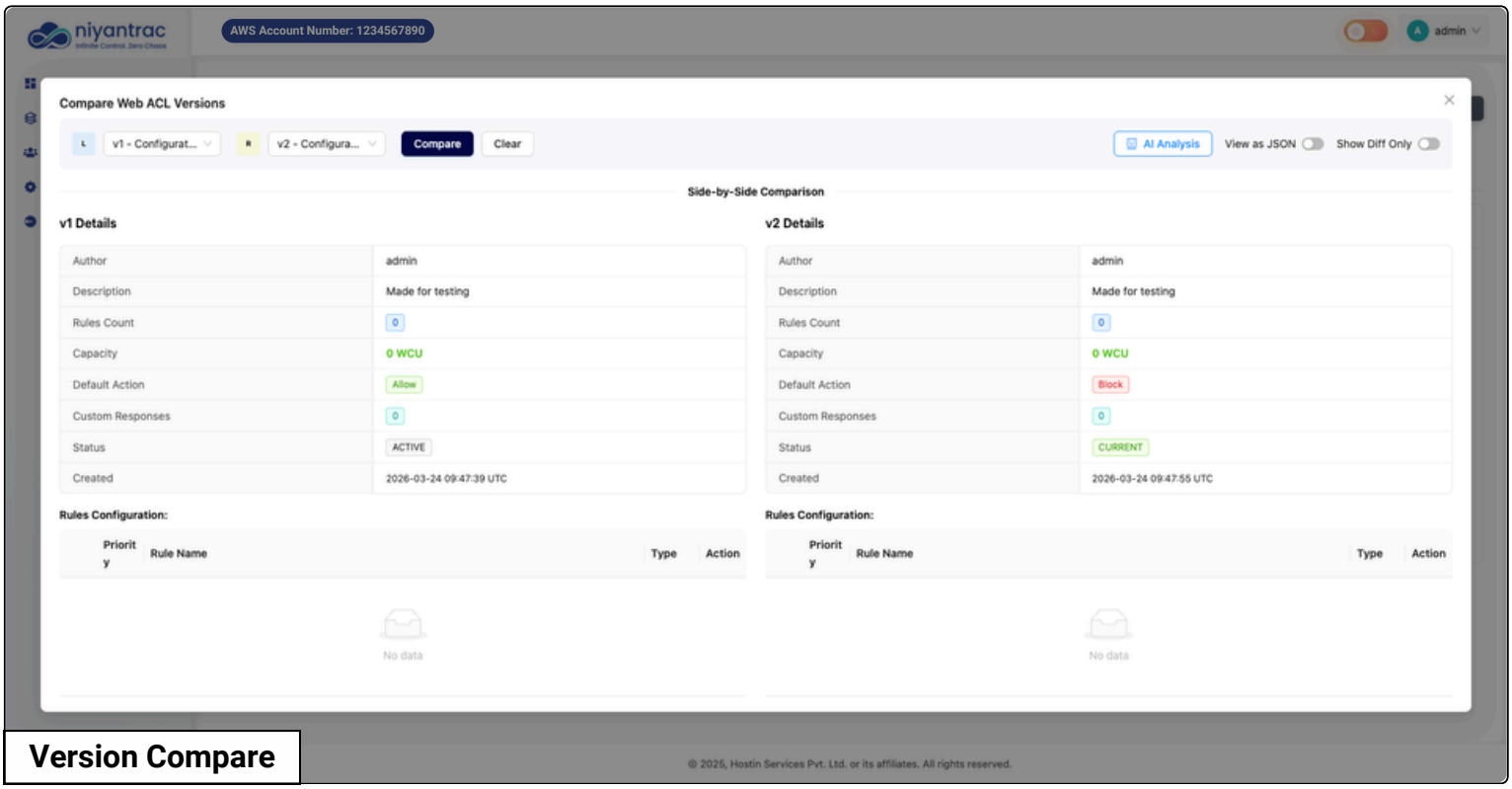
Version History Table

- The table maintains a comprehensive audit trail of all Web ACL configuration changes, tracking version details, rule counts, capacity usage, authors, and timestamps to support rapid disaster recovery decisions.
- Rollback and Management Features
- One-Click Rollback: The rollback icon in the Actions column enables administrators to instantly restore any previous Web ACL version, reverting security rules and settings to known-good configurations within minutes
- Compare Versions: Button to view differences between configurations, helping identify what changed before rolling back
- View Details: Eye icon to review complete configuration details of each version before restoration

This versioning system serves as a critical disaster recovery tool by maintaining complete configuration snapshots. When security misconfigurations occur, threat levels change, or rules cause unintended blocking, administrators can immediately roll back to a previous stable version without manually recreating rules.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

Compare Web ACL Versions



Version Compare

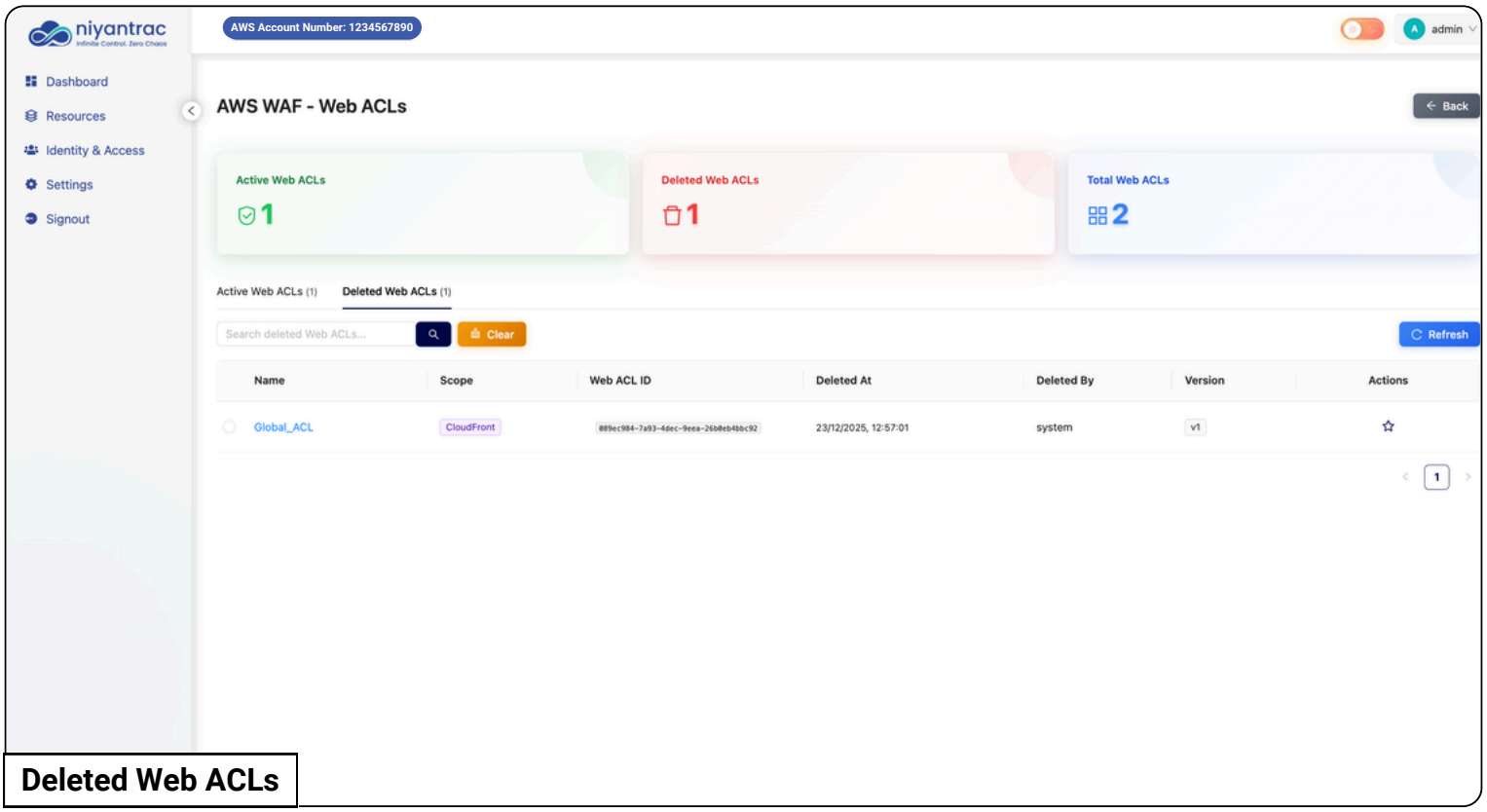
This comparison modal provides a side-by-side analysis of two Web ACL configuration versions, helping administrators understand changes before rollback decisions.

Key Differences Summary

- **A quick overview highlights primary changes:**
  - Rules Change: 1 added
  - Rules Modified: 0 rules
  - Capacity Change (WCU): 1 increase
  - Default Action: Unchanged
- **Side-by-Side Comparison**
  - The interface displays detailed configuration data in parallel columns showing:
  - General configuration (author, description, rules count, capacity, default action)
  - Rules configuration with priority levels and types
  - Version v1 has 1 rule (Priority 0: AWS-AWSManagedRulesAdminProtectionRuleSet)
  - Version v2 has 2 rules (adds Priority 1: Block-HU custom rule)
  - Status changes (ACTIVE → CURRENT) and timestamps
- **AI Change Analysis**
  - Niyantrac's AI Change Analysis gives you an instant, intelligent breakdown of what changed between any two versions of your CloudFront distribution, WAF Web ACL, or Route53 record.

This tool enables informed decisions by clearly showing what rules were added, removed, or modified between versions, supporting confident rollback operations when needed.

7.7 Deleted Web ACLs



Deleted Web ACLs

This view displays Web Access Control Lists that have been removed from active use, with recovery as the core feature enabling instant restoration of accidentally deleted security configurations.

Recovery and Disaster Protection

- The Recover button serves as the primary tool for restoring deleted Web ACLs back to active status, preventing data loss and minimizing downtime when configurations are accidentally removed. Administrators can quickly reinstate entire Web ACL configurations including all rules, capacity settings, and resource associations with a single click.

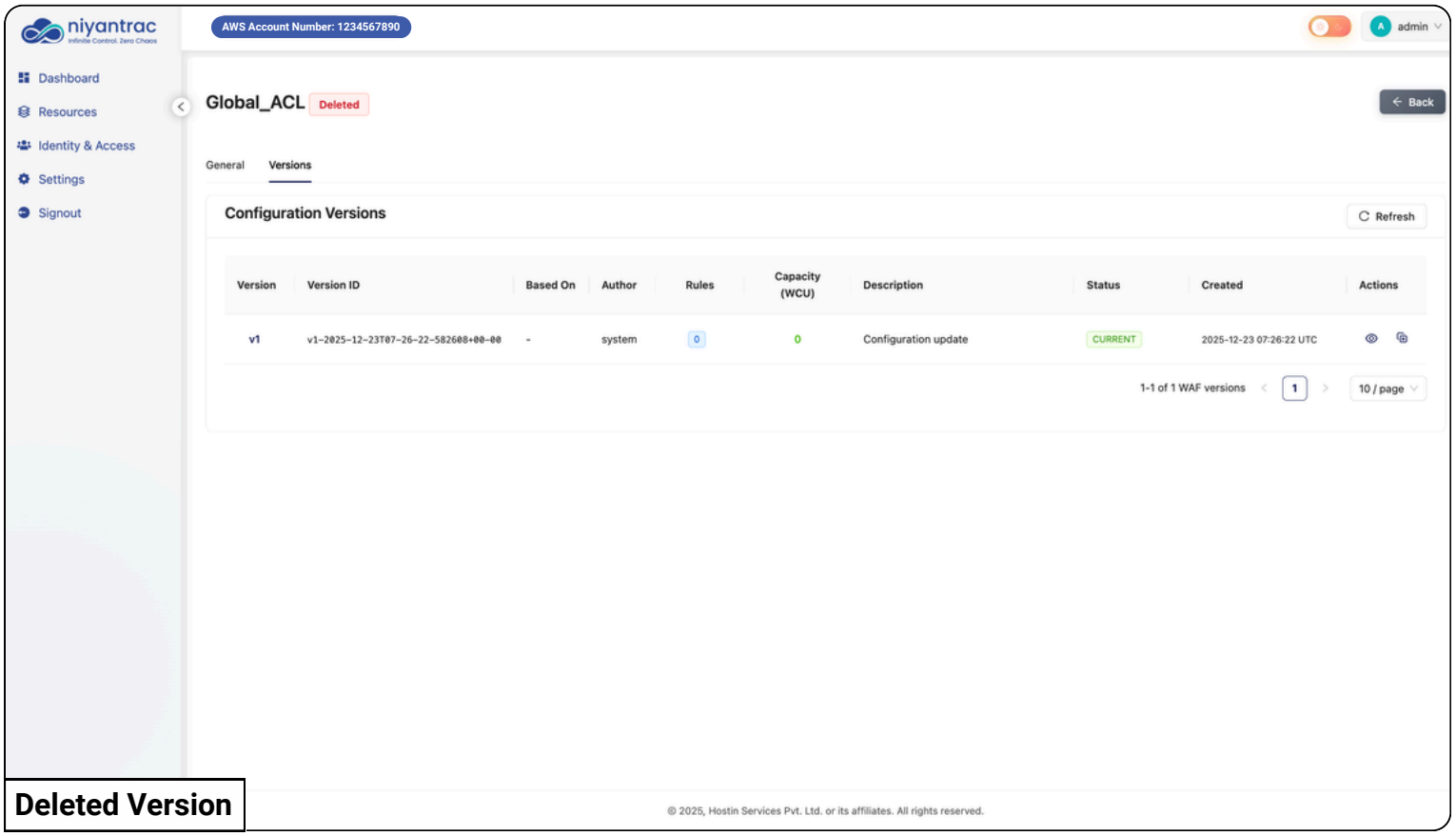
Deleted ACLs Table

- The interface shows 2 deleted Web ACLs with comprehensive tracking information:
- Scope: CloudFront designation
- Web ACL ID: Unique identifier for recovery operations
- Deleted At: Timestamp of deletion
- Deleted By: User or system that performed deletion

Version: Configuration snapshot preserved at time of deletion (v1, v9)

This archive serves as a safety net for disaster recovery, preserving complete Web ACL configurations with full metadata so administrators can restore accidentally deleted security policies without manual reconstruction.

7.8 Deleted Web ACL - Version History



Deleted Version

This page displays the configuration versions for deleted Web Access Control Lists, preserving complete version history for recovery operations.

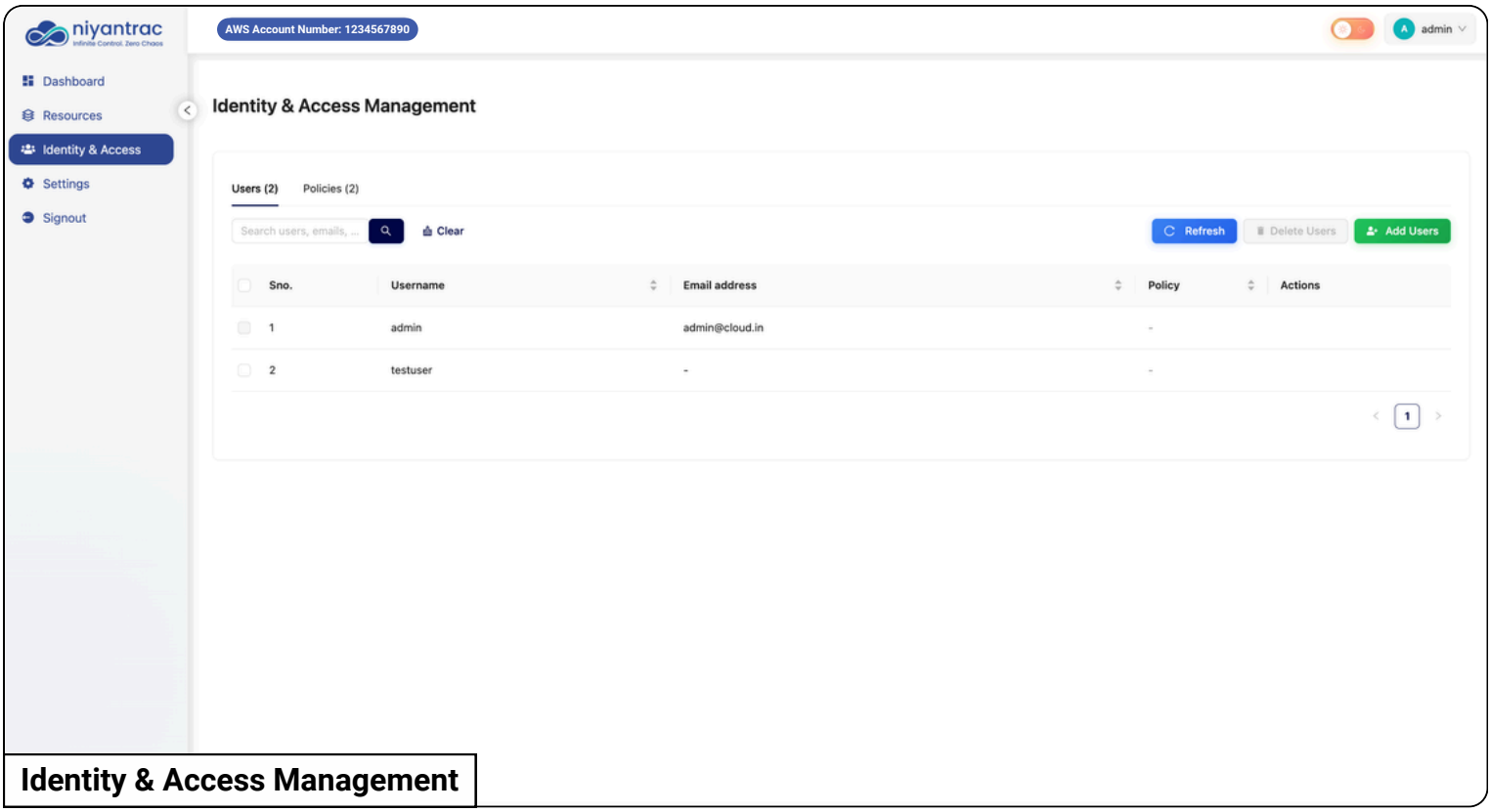
Version-Based Recovery

The copy icon in the Actions column enables granular recovery functionality. Administrators can select and recover from any specific version in the history, not just the most recent configuration. This allows you to:

- Choose which version to restore based on your recovery needs
- Recover from different points in time to address specific issues
- Clone any historical configuration to create a new Web ACL
- Compare versions before selecting the optimal recovery point

This version-wise recovery approach provides flexibility during disaster recovery scenarios, allowing administrators to restore the exact configuration needed rather than being limited to only the latest state.

8. Identity & Access Management



Identity & Access Management

8.1 User Management

This section lists all the individual users who have access to the system. Each user is identified by their:

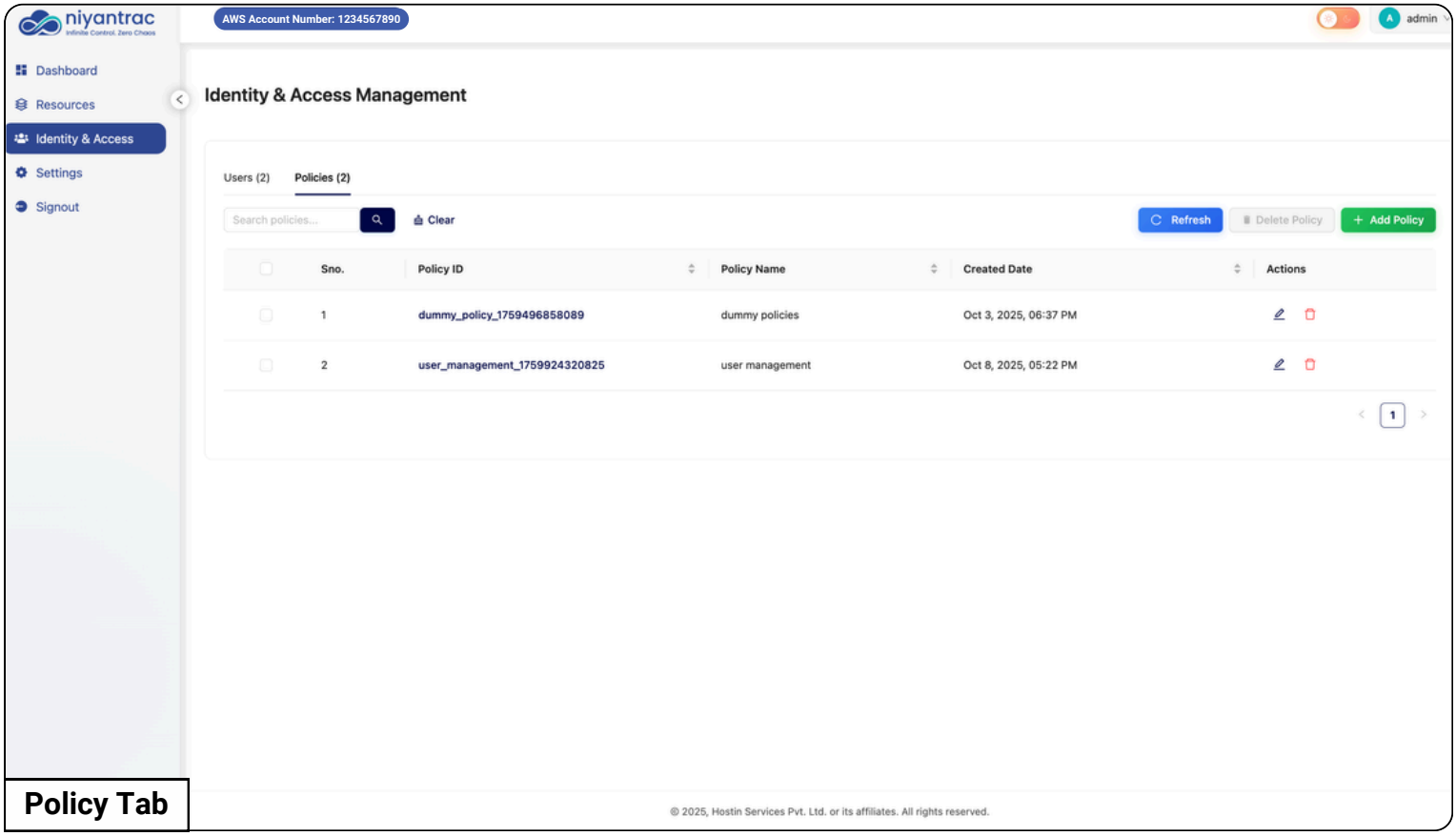
- **Username:** A unique name for logging in.
- **Email address:** The contact email associated with the account.
- **Policy:** A set of permissions that defines what the user is allowed to do.

Actions

These are the specific tasks a user can perform. The image displays two main actions for each user:

- **View:** This action allows you to see the details of a user's account, including their assigned policy. It's a read-only action.
- **Edit:** This action allows you to change a user's settings, such as their assigned policy or other profile information. It is used to update permissions.

8.2 Policy Management



Policy Tab

A policy is a rulebook for a user. It's not a single permission but a collection of them. Instead of giving each user individual permissions, you assign them a policy. For example, a "user_management" policy might allow someone to create and delete users, while a "distribution_management" policy might allow them to manage content delivery.

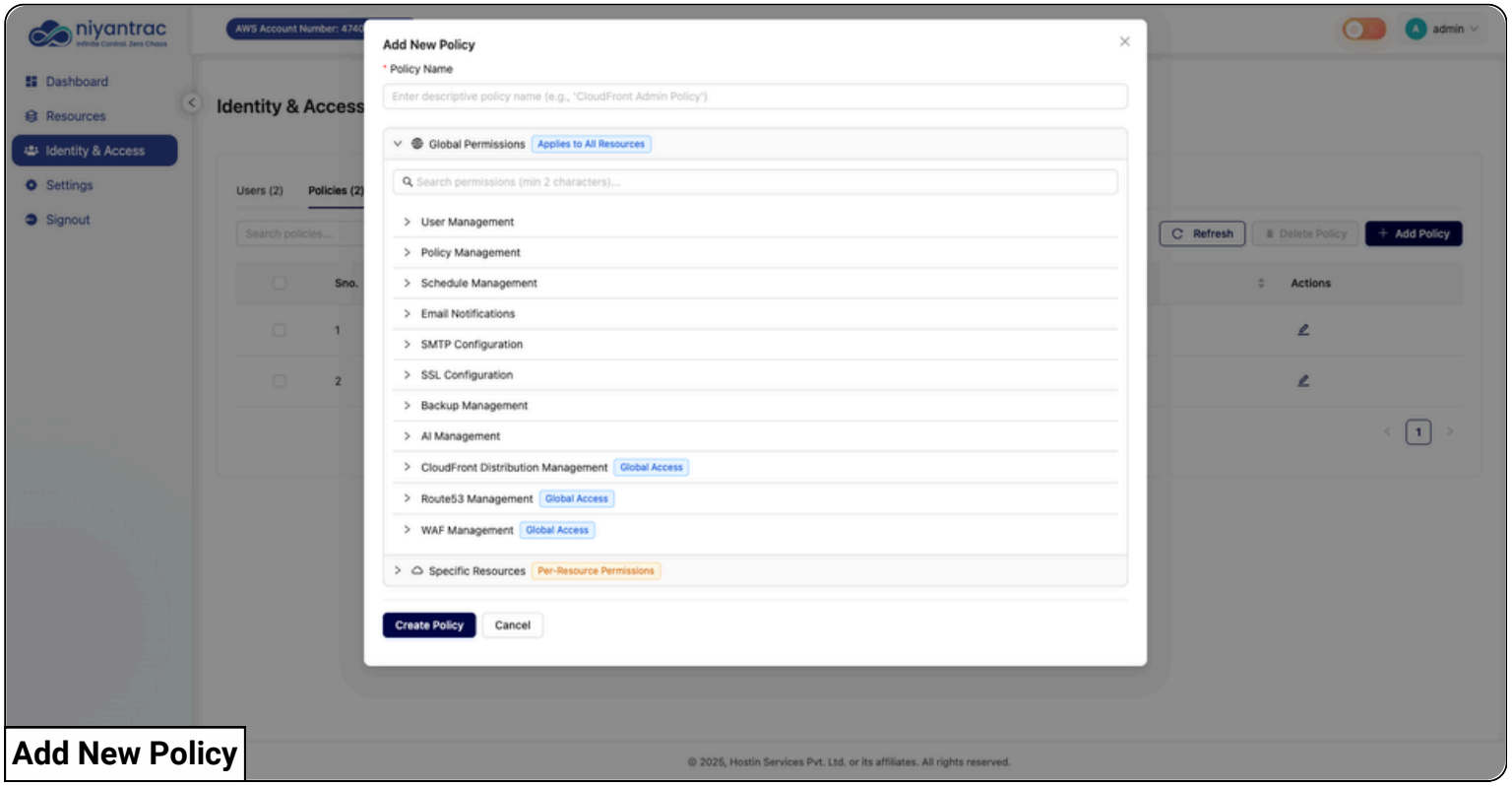
Policies are the core of access management. Each policy has a:

- **Policy ID:** A unique identifier, like a serial number, for the policy.
- **Policy Name:** A human-readable name, like "User management" or "Distribution management," that describes its purpose.
- **Created Date:** The date and time when the policy was first created.

Actions

Add Policy: Create a new policy to define access rules or permissions.
Edit Policy: Modify an existing policy to update its rules or settings.
Delete Policy: Permanently remove a policy from the system.

8.2.1 Add New Policy



Add New Policy

Permissions

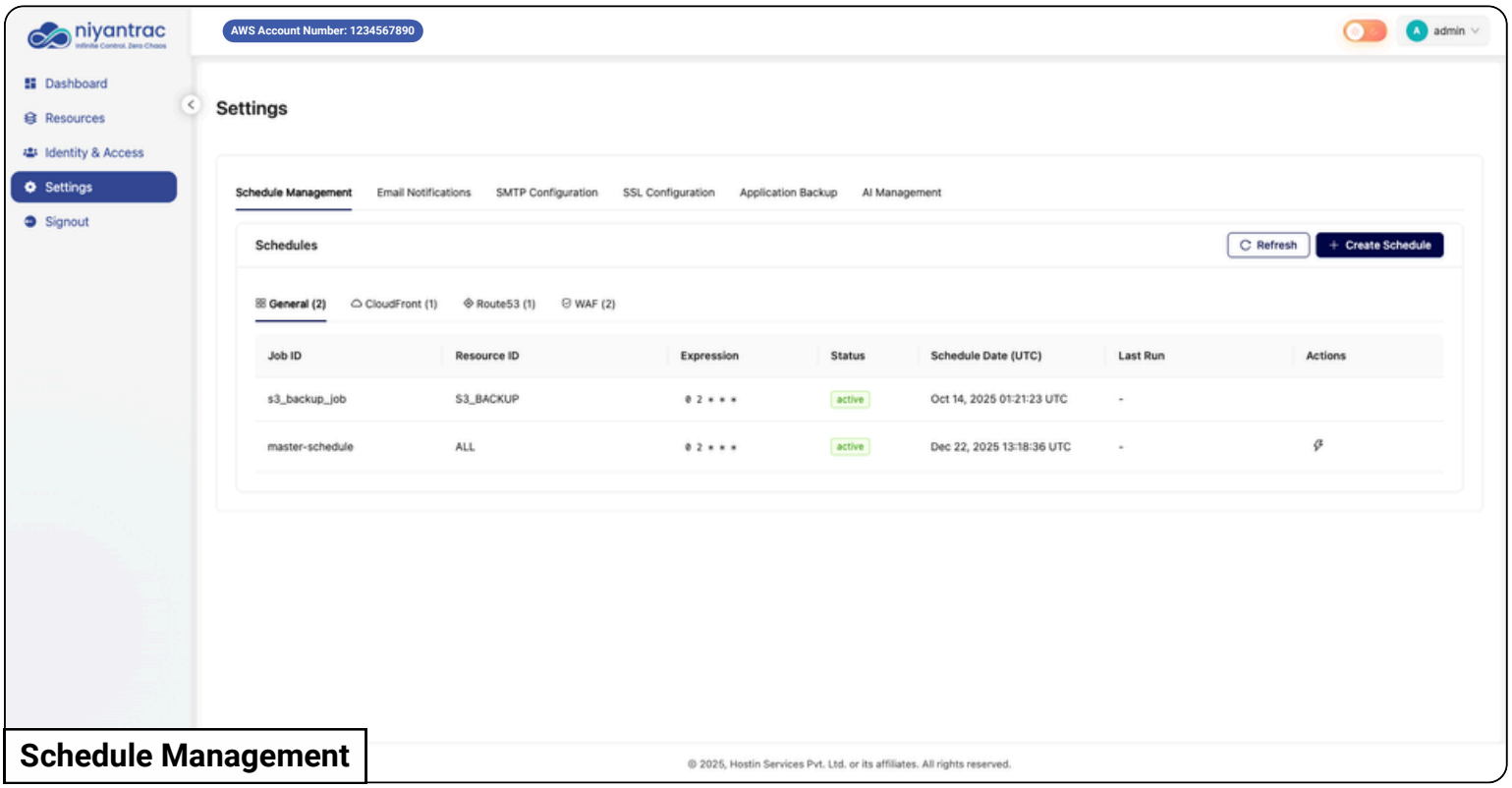
Global permissions and Cloud Distribution Management define the level of access and control a user has.

- **User Management:** This grants the ability to manage user accounts. A user with these permissions can view, add, edit, or remove other users. This is a critical permission set, often reserved for administrators.
- **Policy Management:** These permissions allow a user to view, create, delete, or edit policies. This is also a high-level permission set, as policies control the access of all users in the system.
- **Schedule Management:** This provides control over scheduled tasks, allowing a user to view, create, delete, or run schedules for updates or other maintenance.
- **Email Notifications:** This permission set allows a user to manage email alerts and settings, including the ability to view, set up, remove, or edit email configurations.
- **SMTP and SSL Configuration:** These permissions provide access to advanced server settings, allowing a user to view, set up, or remove settings for email (SMTP) and secure connections (SSL).
- **Backup Management:** These permission allows users to manage backup for the application.
- **AI Management:** Grants access to configure AI/LLM settings, manage model integrations, and use AI-powered change analysis and recommendations
- **CloudFront Distribution Management :** The primary focus is on configuring granular Global Access for all CloudFront Distributions.
- **Route 53 Permission Control:** The primary focus is on configuring granular Global Access for all Route 53 Hosted Zones.
- **WAF Management :** The primary focus is on configuring granular Global Access for all WAF ACLs.

9. Settings Tab

Within the Settings menu, the following key options are available:

9.1 Schedule Management



Schedule Management

- **Scheduling Mechanism (Expression):** The * * * * * in the Expression column indicates that the schedule is defined using a **cron-like syntax**. This allows for precise, repeatable timing (e.g., daily, hourly, or weekly).
- **Administrative Control:** The **Actions** column contains icons that allow for **editing** (changing the schedule/resource), **running the job immediately** (manual trigger), or **deleting** the schedule.

a. General Schedule

- **Configuration Change Detection:** Monitors CloudFront distributions, Route 53 hosted zones and records, and WAF
- web ACLs for any configuration modifications, tracking version history for audit and rollback purposes.
- Tracks deleted CloudFront distributions, Route 53 hosted zones, and WAF rules across all entries to prevent accidental data loss and enable recovery.
- **S3 Application Backup:** Automatically backs up Version Vault application data, configuration files, and metadata to S3 with versioning enabled for disaster recovery scenarios.

b. Distribution-Specific Schedules

This schedule monitors changes in a particular CloudFront distribution.

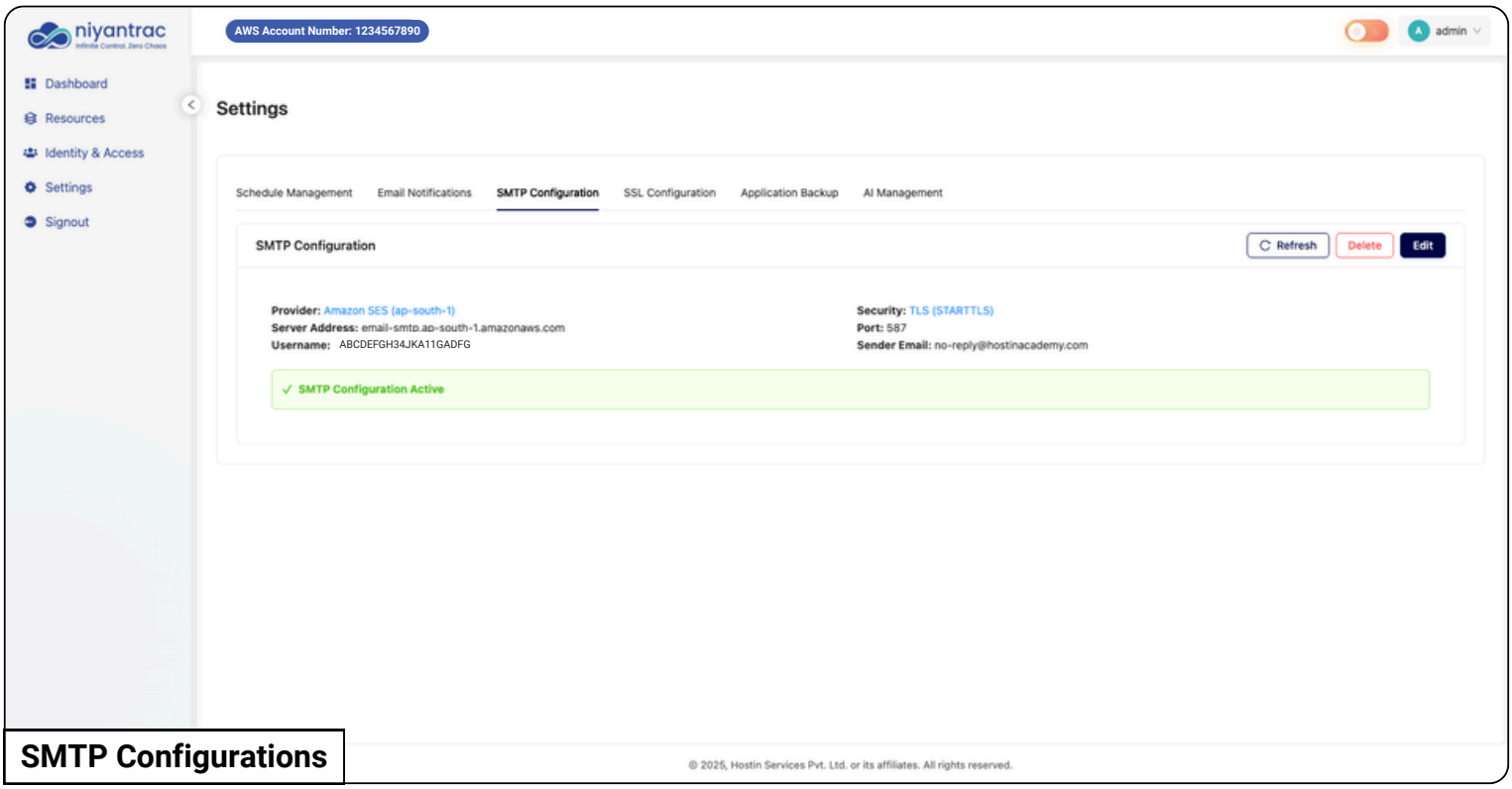
c. Route 53 Schedule Management

This schedule monitors changes in a particular Route53 Hosted Zone.

d. WAF Schedule Management

This schedule monitors changes in a particular Web ACL.

9.2 Email Notification and SMTP Configuration



SMTP Configurations

Step 1: SMTP Setup

- The admin adds the email server settings (SMTP).
- Once it's set, the system is ready to send emails.

Step 2: Notification Triggers

The system watches for important events like:

- Low disk space.
- User changes.
- Distribution updates.

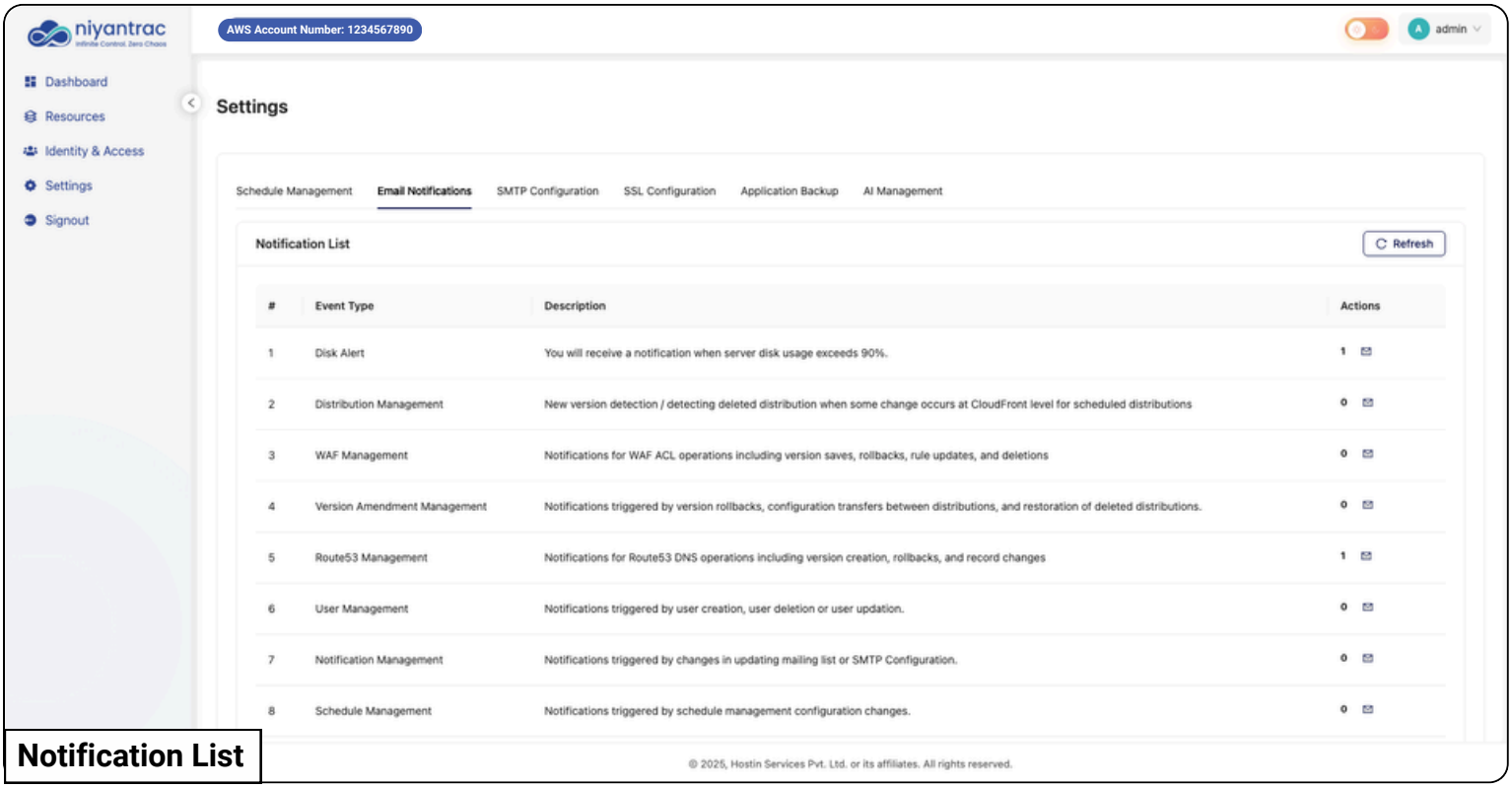
When something happens, the system prepares an email.

Step 3: Sending the Email

- The system sends the message using the SMTP server.
- The email goes out from the sender you set up to the right people.
- To manage recipients, the user clicks the mail icon in the Action tab, which opens the mailing list. modal. From there, they can add new emails or delete existing ones using the available options.

UI Guide: CloudFront, Route53 & WAF Versioning, Recovery & Management

Notification List



Notification List

Email Notifications

The Email Notifications panel provides centralized management of all system-generated alerts and event notifications for Version Vault. Configure which events trigger email notifications to stay informed about critical operations across CloudFront distributions, Route53 DNS management, WAF rules, and system health.

Available Notification Types

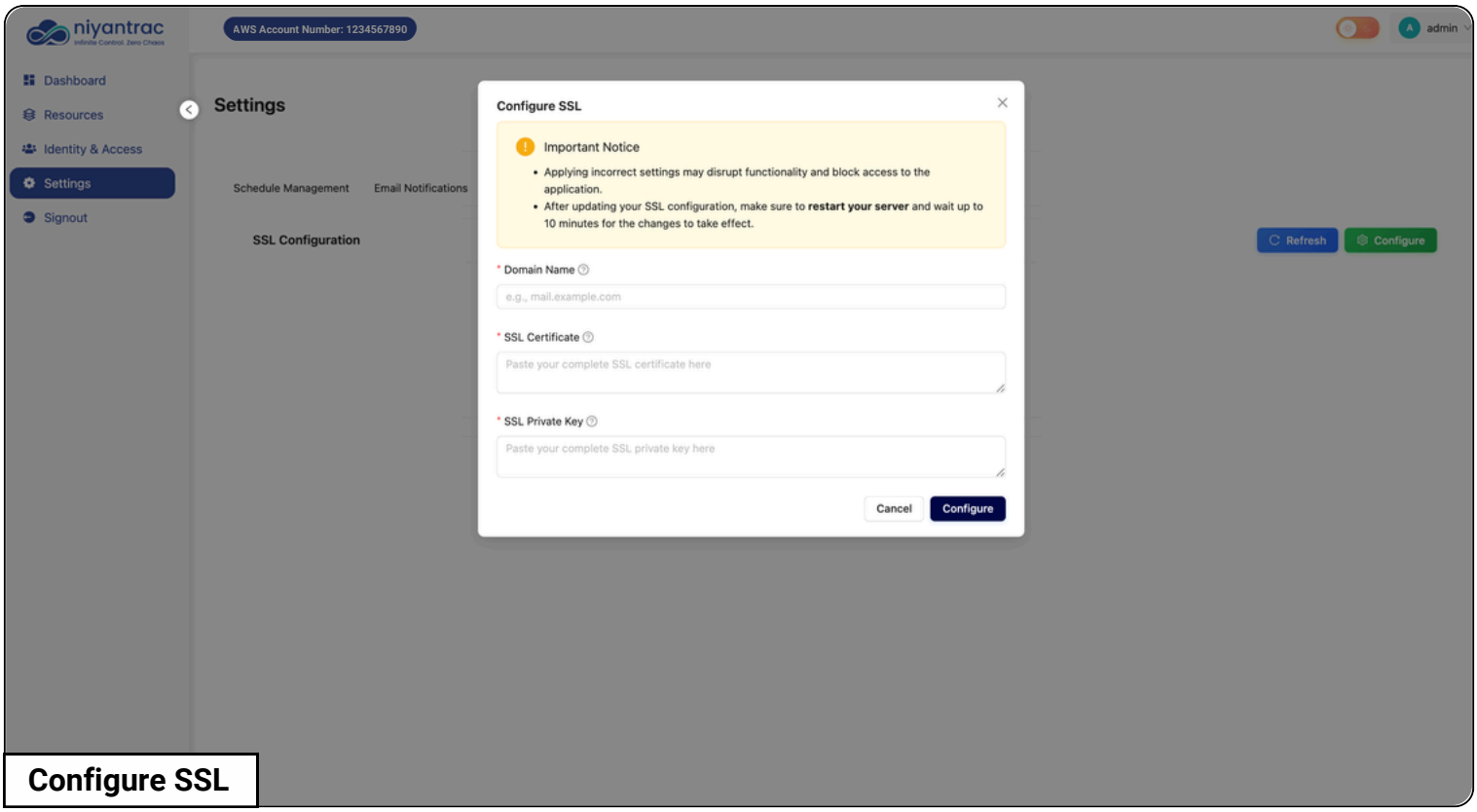
The notification list displays eight event categories:

- **Disk Alert**: Alerts when server disk usage exceeds 90% threshold to prevent storage issues
- **Distribution Management:** Notifies on CloudFront distribution version changes and deletion detection
- **WAF Management:** Alerts for WAF ACL operations including version saves, rollbacks, rule updates, and deletions
- **Version Amendment Management:** Notifications for version rollbacks, configuration transfers, and deleted distribution restorations
- **Route53 Management:** Alerts for DNS operations including version creation, rollbacks, and record changes
- **User Management:** Administrative notifications for user creation, deletion, or updates
- **Notification Management:** Meta-notifications triggered by mailing list or SMTP configuration changes
- **Schedule Management:** Alerts when backup or monitoring schedule configurations are modified

Each notification type can be individually enabled or disabled, with the counter column showing pending notification count for monitoring system activity.

9.3 SSL Configuration

SSL (Secure Sockets Layer) certificates are like a digital passport for your website. They make sure that the connection between your users and your CloudFront distribution is secure and private. This is important for protecting sensitive information and building trust.



Configure SSL

1. Domain Name

- This is the web address (like **yourwebsite.com** or **mail.example.com**) that your SSL certificate is for.
- Enter your domain name here.

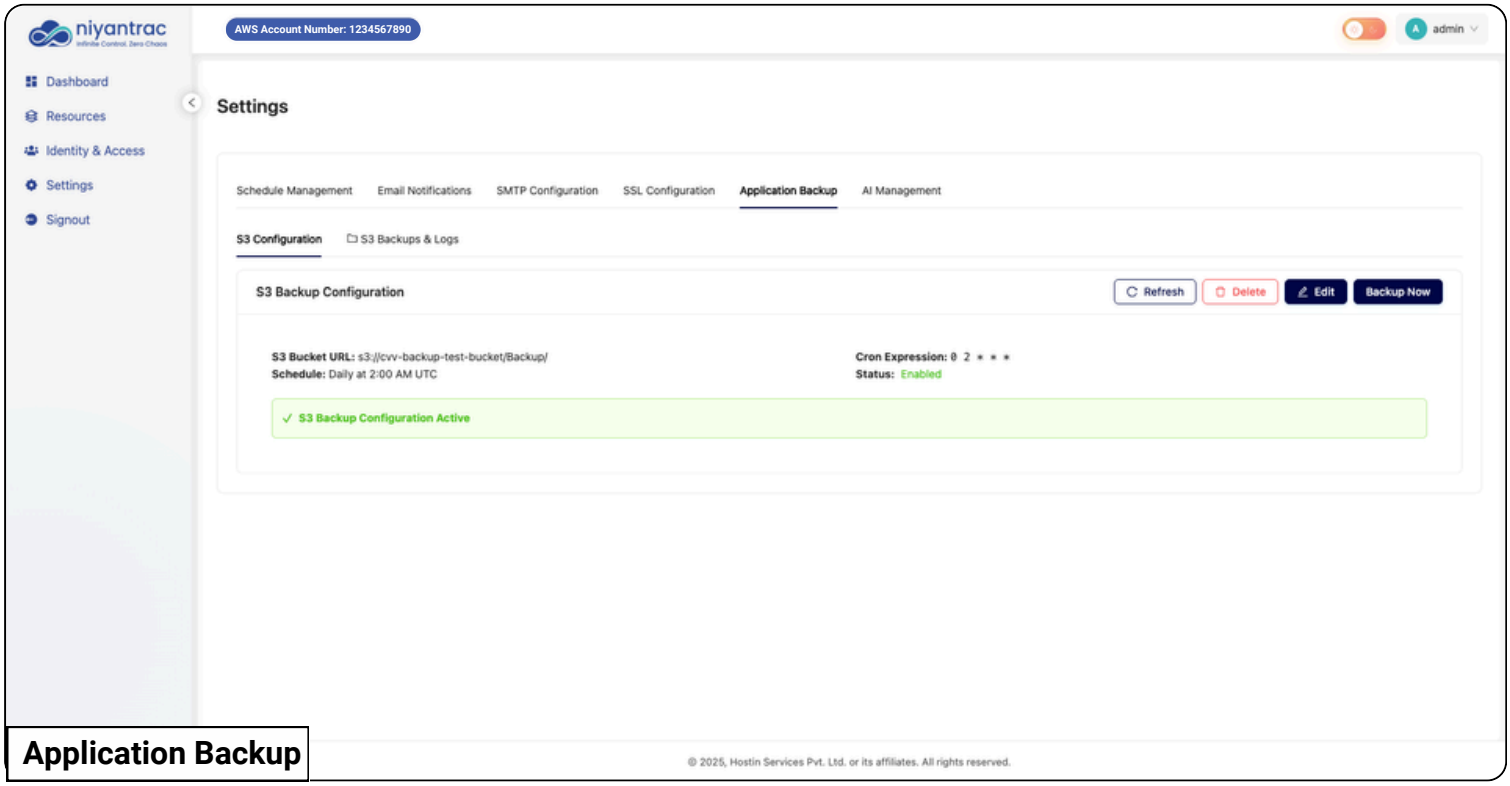
2. SSL Certificate

- This is the actual certificate code you received from your SSL provider (like Let's Encrypt, DigiCert, etc.).
- It's a long string of characters that typically starts with **-----BEGIN CERTIFICATE-----** and ends with **-----END CERTIFICATE-----**.
- Carefully copy and paste your complete SSL certificate into this box.

3. SSL Private Key

- Every SSL certificate has a matching private key. This key is crucial for decrypting the secure connection.
- It's another long string of characters, usually starting with **-----BEGIN PRIVATE KEY-----** or **-----BEGIN RSA PRIVATE KEY-----** and ending with **-----END PRIVATE KEY-----** or **-----END RSA PRIVATE KEY-----**.
- Carefully copy and paste your complete SSL private key into this box.
  Keep this private key very secure and do not share it with anyone!

9.4 Application Backup



Application Backup

S3 Bucket Configuration

- **S3 Bucket URL:** This is the unique web address for your S3 bucket, where the backed-up files are stored. The format is typically **s3://[bucket-name]/[folder-path]/**. The **s3://** part signifies that it's a path for an Amazon S3 resource.
- To configure S3 backups, the application needs permission to view and modify the bucket's access settings. Grant the actions **s3:GetBucketAcl** and **s3:PutBucketAcl** on the specific backup bucket ARN.
- **Cron Expression:** This is a standardized way to define a schedule for a task. It's a string of five fields representing a specific time for the backup to run automatically.
  - The five fields are **minute, hour, day of the month, month,** and **day of the week.**
  For example, a cron expression of **0 2 * * * means the backup will run at 2:00 AM every day. The** asterisks (*) are wildcards, meaning "every" or "any."
- **Schedule:** This indicates the frequency of the backup. The image shows a **Custom Schedule** which is defined by the cron expression. This gives you flexibility to set backups for any time and day you want.

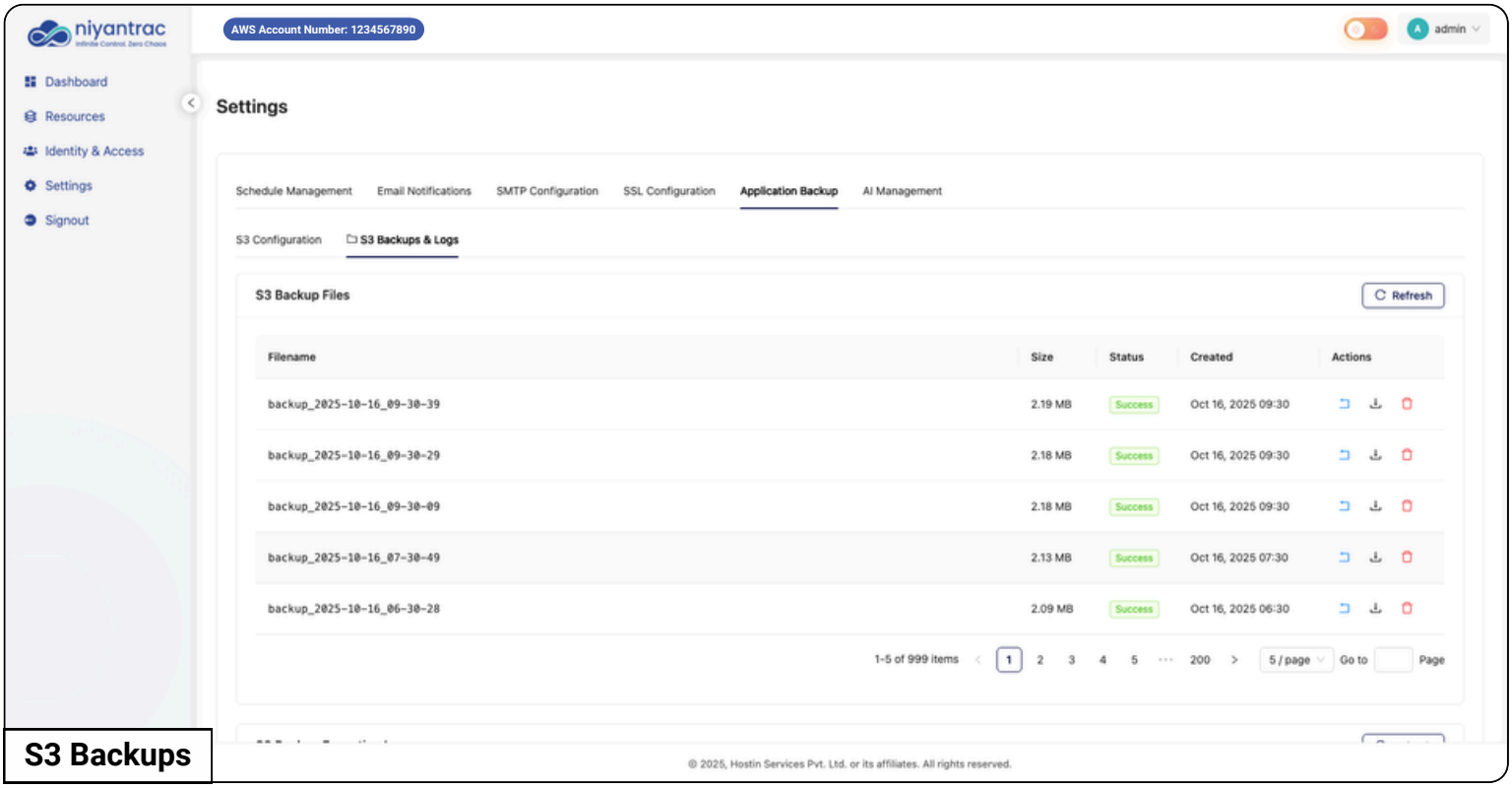
Backup Management Actions

Once the configuration is set up, you can perform several actions on it:

- **Delete:** This action permanently removes the backup configuration.
- **Edit:** This allows you to modify the configuration, such as changing the S3 bucket URL, the cron expression.
- **Backup Now:** This is a manual trigger that starts a backup immediately, regardless of the scheduled time.

9.4.1 Backup List

This is a table showing each backup that has been successfully created. For each backup, you can see the following details:



S3 Backups

The "S3 Backups & Logs" section gives you a view of all the completed application backups. It acts as a history log and a control center for your backed-up data.

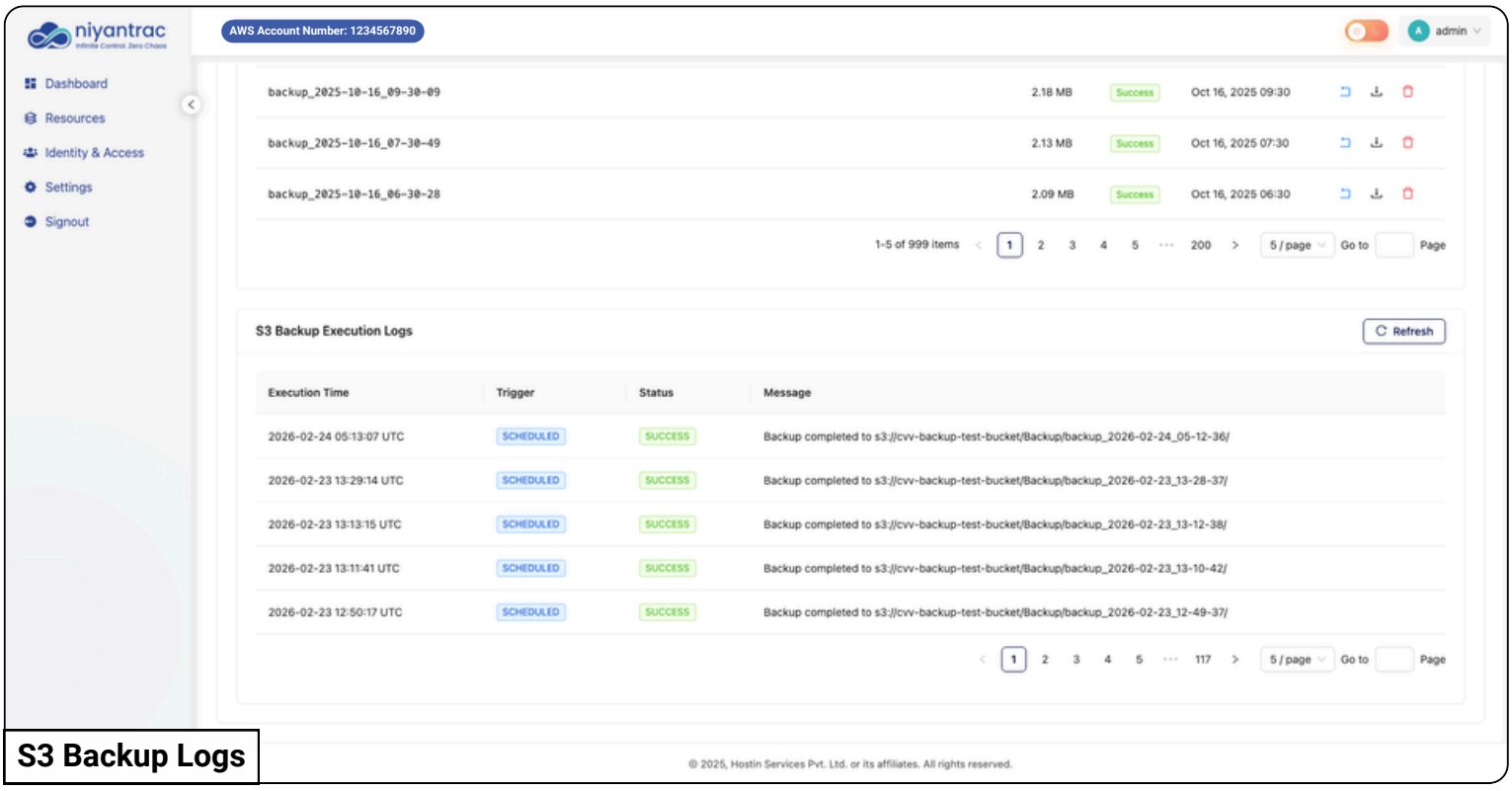
- **Filename:** A unique name for the backup file. It typically includes the date and time of the backup (e.g., **backup_2025-10-03_05-31-00**). This makes it easy to identify when a specific backup was created.
- **Size:** The file size of the backup, shown in megabytes (MB). This helps you monitor your storage usage.
- **Status:** Indicates whether the backup process was successful. A **"Success"** status means the backup was completed without any errors.

Actions

For each backup file listed, you have several actions you can take:

- **Download:** This action allows you to download the backup file to your local computer. This is essential for restoring your application data or moving it to another location.
- **Delete:** This action permanently removes the backup file from the S3 bucket. You can use this to clear out old or unneeded backups to free up storage space.
- **Restore:** This action is used to restore your application to the state of the selected backup. This is a critical function for disaster recovery or rolling back to a previous version of your application.

9.4.2 S3 Backups Execution Logs



S3 Backup Logs

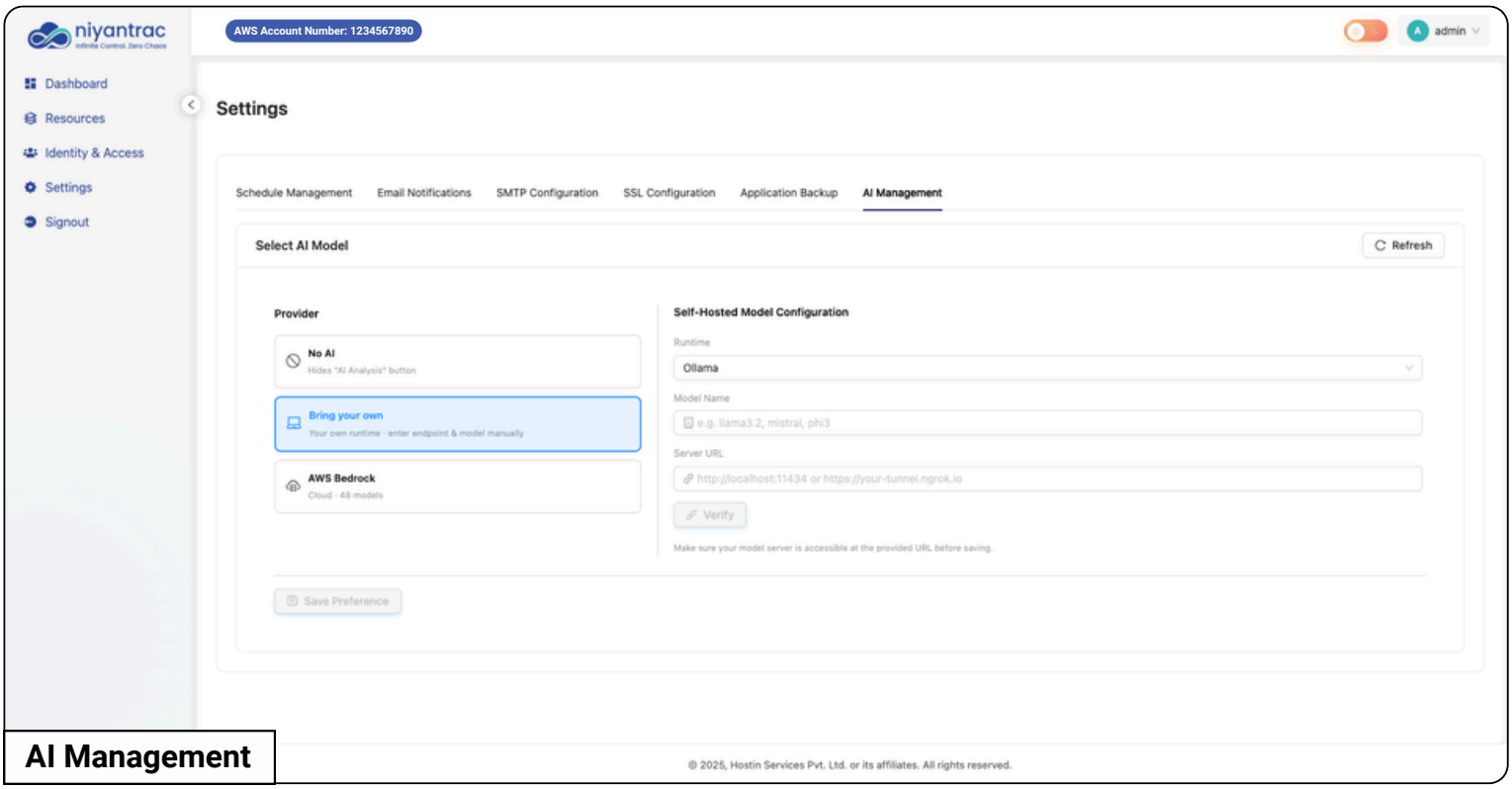
The **S3 Backup Execution Logs** provide a detailed history of all the backup tasks performed. This log is crucial for monitoring, troubleshooting, and verifying that your data is being backed up as expected.

Execution Details

This section provides a summary of each backup job, which includes:

- **Execution Time: The exact date and time the backup process started.**
- **Trigger:** How the backup was initiated. The image shows **"SCHEDULED"**, which means the backup was automatically started based on the cron expression you configured. A trigger could also be **"MANUAL"** if you clicked the **"Backup Now"** button.
- **Status:** The result of the backup job. A **"SUCCESS"** status indicates the backup process was completed without any issues. If there were any problems, the status would show a failure or error.
- **Message:** A brief description of the outcome of the backup job. For a successful backup, it will show the final path and filename where the backup file was stored in your S3 bucket.

9.5 AI Management



AI Management

Configure how Niyantrac uses AI to analyze configuration changes, generate summaries, and provide intelligent recommendations across your CloudFront, WAF, and Route53 resources.

- **No AI** — Disable AI features entirely. All core versioning, backup, and rollback functionality remains available without any AI-assisted analysis.
- **Bring Your Own** — Connect your own self-hosted or OpenAI-compatible LLM using your preferred runtime, model name, and server URL. Your data stays within your own infrastructure.
- **AWS Bedrock** — Use Amazon-managed foundation models via AWS Bedrock. No additional infrastructure required — runs securely within your existing AWS environment.

10 Conclusion

Niyantrac is a robust and intuitive tool designed to streamline the management of AWS CloudFront distributions, Route53 hosted zones, and WAF web ACLs. It provides full visibility and control over configuration changes, making tasks like rollback, monitoring, DNS updates, version management, and security policy management seamless.

With Niyantrac, you can:

- Instantly roll back to any previous version of a CloudFront distribution, Route53 hosted zone, or WAF web ACL to recover from misconfigurations.
- Copy any saved configuration to another distribution, hosted zone, or WAF ACL—or create a new resource based on an existing version for rapid deployment or testing.
- Compare two selected versions side-by-side to identify configuration changes, including detailed diff views for all supported resource types.
- Leverage AI-powered change analysis to automatically summarize configuration differences, assess severity, and get intelligent recommendations — using your own self-hosted LLM or AWS Bedrock.
- Schedule automated monitoring and backup tasks using flexible cron-based or master scheduling, supporting routine integrity and compliance checks.
- Receive real-time email alerts for critical events via configurable SMTP settings, including disk usage, deletions, config changes, and backup status.
- Secure your environment by managing and uploading custom SSL certificates for CloudFront and application access, ensuring encrypted communications.
- Ensure the integrity and availability of your data by securely backing up your application data in an S3 bucket.
- Manage user access and permissions with policy-based access.
- Manage granular user access and permissions through integrated policy-based or role-based access controls, supporting secure and auditable team collaboration.

We recommend reviewing version history regularly, keeping SMTP and SSL configurations up to date, and enforcing appropriate access control for all users.

Thank you for Trusting Niyantrac.

niyantrac
Infinite Control. Zero Chaos

For Support | support@niyantrac.com
For Enquiry | sales@niyantrac.com
Visit us | www.niyantrac.com