NEXTLABS®

CloudAz Policy Controller

Zero Trust Policy Platform

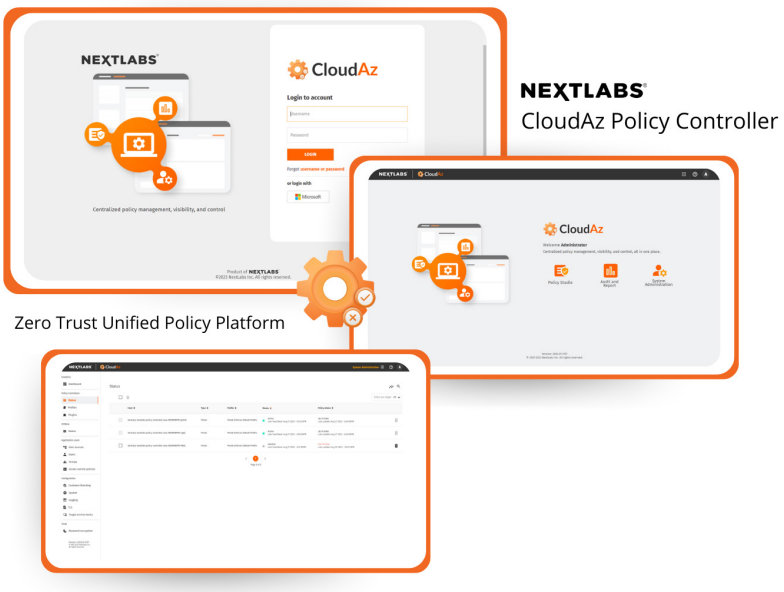
THE SITUATION

In today's increasingly digital and globalized business environment, the needs of enterprise access entitlements and data security demand a policy-driven approach to automate and secure access to diverse applications, data stores, systems, and topologies. These applications run on servers, desktops, laptops, mobile devices – both online, offline, and on the Internet as software services. Custom built authorization and entitlement solutions only provide static and role-based policy evaluation for specific applications and no longer meet cybersecurity requirements. A Zero Trust Policy Engine allows organizations to adapt to the ever-changing needs of today's business requirement by providing the flexibility to make changes to access rights and data security needs on the fly via policy without complex customization and manual procedures.

THE SOLUTION

NextLabs' CloudAz Policy Controller is the Zero Trust Policy Engine (Policy Decision Point) of CloudAz. It allows organizations to adapt to the ever-changing needs of today's business landscape by providing the flexibility to implement least privilege access policy, externalize authorization, and enforce data security controls with ability to make changes on the fly.

The CloudAz's Policy Controller uses real-time contextual information to evaluate conditions in policy set to make authorization decision. These conditions are based on user, environment, and resource characteristics ("attributes"), which are evaluated in real-time to grant permission and authorize what a user or subject can perform on applications, APIs / microservices, business transactions, and data. This Policy Engine accounts for changes in user status or changes in the resource. For instance, if an employee moves to a different department within the company, no new policy needs to be created since policies are evaluated against the latest set of attributes without the need for manual intervention or changing the policy.



KEY BENEFITS

- **Highly Scalable Real-Time Policy Evaluation** - Supports thousands of applications in a hybrid and multi-cloud environment through the use of APIs, SDKs, and OOTB enforcers that allow for seamless integration with applications developed with most technologies and programming languages.
- **Persistent policy vault built on a High Availability architecture** - Provides flexibility to support large scale deployment and uptime requirement while allowing offline policy evaluation, especially useful for disrupted, disconnected, intermittent and low-bandwidth (DDIL) environments.
- **Centralized Logging –** User activity and data access across applications and services are logged in a centralized audit repository, allowing administrators and auditors to analyze risky behavior and detect anomalies through reports and automated monitoring facilities.
- **Automated Policy Deployment and Policy Testing –** The CloudAz Policy Controller works with the CloudAz Policy Distribution and Policy Testing capabilities to deploy policy seamlessly and automate test plan creation to validate policies. The test plan library can then be re-used across deployments. Optimized policy bundles are automatically distributed to each Policy Decision Point to streamline policy evaluation and improve performance.
- **Hybrid and Multi Cloud Environments** - Support policies to enforce access and protect applications across enterprise on private or public clouds. Policies can be leveraged across public clouds, on-premises deployments, and hybrid environments for consistent enforcement.
- **Internet Scale** - Distributes and runs across multiple data centers for performance, scalability, and high availability. NextLabs' CloudAz Policy Controller scales to meet the most complex requirements in critical internet scale applications.

KEY CAPABILITIES

Comprehensive and Robust API - The CloudAz Policy Controller can be integrated with applications written in any programming language in minutes to hours using our standards-based REST APIs and SDK. The CloudAz Policy Controller accepts JSON Web Tokens (JWTs) and SAML tokens as subjects in authorization requests, simplifying the integration. A Permission API allows querying the user permissions for resources and applications. In addition to CloudAz's native policies, the CloudAz Policy Controller can consume XACML and REGO policies, ensuring seamless policy enforcement for organizations with existing XACML and REGO policies.

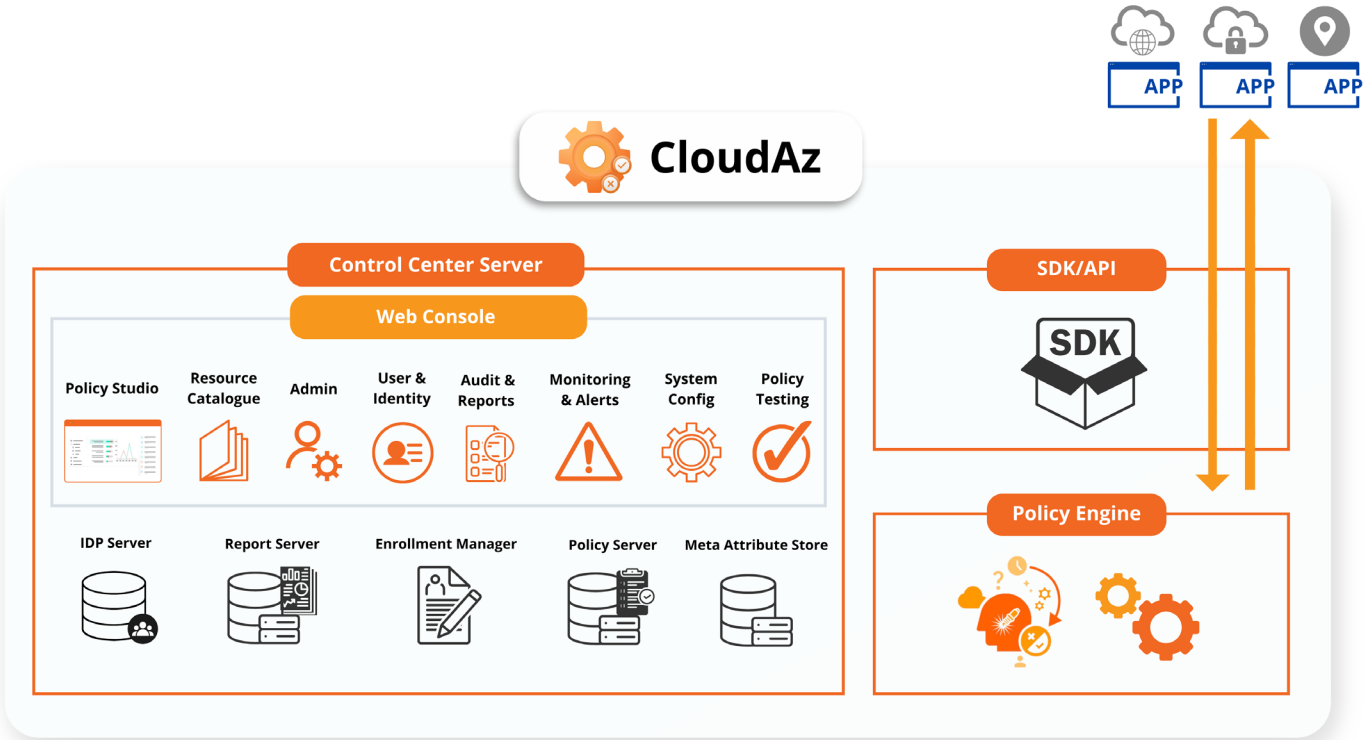
Real-Time Policy Evaluation and Offline Support - Policies are evaluated and dynamically enforced in real-time. Policy evaluation is optimized as policies are pre-compiled for each CloudAz Policy Controller rather than attempting to evaluate XML rules in real-time. The result is very low-latency policy decisions with no perceptible performance degradation to end users. NextLabs' CloudAz Policy Controller can work in tandem with policy enforcement points (PEP) so that policy decisions can be made locally, without the need for costly server lookups. This approach speeds up policy evaluation and allows the CloudAz Policy Controller to be used on disconnected devices.

Dynamic Attribute-Based Access Control (ABAC) - The use of attribute-based access control (ABAC) policies allows the CloudAz Policy Controller to grant permissions to ensure only authorized users can access data under the specific guidelines set by the policies. The Dynamic Attribute Provider framework allows integration with any attribute sources to retrieve attributes dynamically at the time of data access request.

Enterprise Scalability - Distributing the policy decisions to multiple engines provides the scalability to meet the requirements of large-scale enterprise deployments. The management and configuration of all CloudAz Policy Controllers is centralized, allowing for flexibility and speed when making changes.

KEY FEATURES

Feature	Detail
Policy Decision Point	Using patented technology, NextLabs' CloudAz Policy Controller is able to deliver real-time policy decisions to critical business applications. The CloudAz Policy Controller is available on servers, clients, and as a cloud service, enabling it to work with on-premises, desktop, and cloud applications. Using smart deployment, the CloudAz Policy Controller provides the fastest policy evaluation available with >90% of authorization checks evaluated in <2 milliseconds.
Comprehensive Apis	The CloudAz Policy Controller software development kit (SDK) provides APIs for common programming languages to make it easy to integrate with a variety of applications, including Java, C#, C++, and REST-based web services.
Extensible for Increased Flexibility	The CloudAz Policy Controller is easily extended to address complex authorization requirements. Integration with external Policy Information Points (PIPs), custom policy functions, and custom obligations are all supported. Expanded CloudAz Policy Controller plugin management allows fully automated integration of dynamic attribute retrieval from any source.
Architecture Extensibility	The CloudAz Policy Controller architecture is extensible to consume access control policy languages other than CloudAz's native ACPL 4GL policy language. CloudAz provides end to end workflows for customers to use their existing XACML and REGO policies for policy enforcement.
Permission Api	The CloudAz Policy Controller's permission API can be used to provide a list of user permissions simplifying compliance reviews. For example, for a given user and resource, the Permission API can return all permissions that the user is entitled to on a particular protected resource.
Central Management	Distributed CloudAz Policy Controllers are centrally managed from CloudAz. Administrators can centrally register, configure, monitor status, and deploy policy. Policy activity logs are transferred to CloudAz, ensuring real-time reporting of audit data. Dashboards are provided for Policy Administrators to monitor the policy enforcement activities.
Security Services	Each CloudAz Policy Controller authenticates bi-directionally with CloudAz using digital certificates and SSL. Deployed policies are authenticated via digital signatures and secured using encryption.
Optimized Policy Deployment	Policies are deployed to CloudAz Policy Controller using an optimized deployment technology, which creates highly optimized policy bundles for each CloudAz Policy Controller. Optimized deployment ensures that each CloudAz Policy Controller has the minimum set of relevant policies, and even pre-evaluates components of the policy in advance in order to speed up policy evaluation.
Dynamic Attribute Provider Plugins And Central Deployment	A dynamic attribute provider framework enables CloudAz Policy Controller to use subject and resource attribute provider plugins to perform a runtime look up of attributes at the time of a data access request. CloudAz's Plugin Management tool automates deployment of attribute provider plugins and dependencies across multiple CloudAz Policy Controllers.
Support For JWT And SAML Tokens	The CloudAz Policy Controller can consume JSON web tokens and SAML tokens as a subject in an authorization request, simplifying the integration with applications. The CloudAz Policy Controller validates the token and uses the user claims in the token to make authorization decisions.
Obligation Manager	The CloudAz Policy Controller allows customers to integrate with third-party applications by adding custom actions, called obligations, which are invoked based on policy evaluation. Obligations can be used to automate tasks; workflows based on policy events or inject a security filter in SQL query to restrict the data being selected.
Logging and Notification Services	Policies can be used to trigger logging or email notification actions. The Policy Controller provides out-of-the-box obligations for logging events to a central report server and sending email notifications in response to policy events.



SUPPORTED PLATFORMS

CloudAz Policy Controller Deployment Model

CloudAz Policy Controller can be deployed as a standalone cloud authorization service or in a hybrid model where applications and policy enforcement points can be either in the cloud or on-premises.

CloudAz Policy Controller On-Premises System Requirements

Policy Controller Type	Supported Platform(s)
Windows Policy Controller	Microsoft Windows Server 2016, 2019, and 2022 Microsoft Windows Desktop 7, 10, 11

Server Policy Controller	**Operating systems**
	• Microsoft Windows Server® 2016, 2019, and 2022
	• Microsoft Windows® Desktop 7, 10, 11
	• Red Hat® Enterprise Linux® (RHEL) 7.9
	• Oracle Linux 7.9 and 8.6
	• SUSE Linux 15 SP3 LE on PowerPC
	• SUSE Linux Enterprise Server 12 SP5 and 15 SP3
	
	Application servers
	• On Microsoft Windows:
	  • Apache Tomcat® 9.0.70 with OpenJDK 11.0.15_10
	• On Red Hat Enterprise Linux:
	  • Apache Tomcat® 9.0.70 with OpenJDK 11.0.15_10
	  • JBoss® Enterprise Application Platform (JBoss EAP) 7.0 and 7.2
	• On Oracle Linux:
	  • Apache Tomcat® 9.0.70 with OpenJDK 11.0.15_10
	  • JBoss® Enterprise Application Platform (JBoss EAP) 7.0 and 7.2
	• On SUSE Linux:
	  • Apache Tomcat® 9.0.70 with OpenJDK 11.0.15_10
	  • JBoss® Enterprise Application Platform (JBoss EAP) 7.0 and 7.2

Cloud Deployment

CloudAz Policy Controller's containerized architecture supports both Kubernetes-based and non-Kubernetes based cloud platforms to allow for seamless deployment of CloudAz Policy Controller OCI-compliant containers to cloud platforms. The CloudAz Policy Controller microservice can be deployed, upgraded, and scaled independently. Using CloudAz's cloud-native Policy Controller, organizations can take full advantage of cloud infrastructure, orchestration, data services and application run time.

Private, Hybrid, and Multi-Cloud System Requirements

CloudAz Policy Controller provides private, hybrid and multi-cloud deployment support by leveraging Docker and Kubernetes.

Supported Cloud Platforms

- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)
- Azure VMs
- Azure Kubernetes Service (AKS)
- Google Compute Engine
- Google Kubernetes Engine (GKE)

Supported multi-cluster container orchestration platforms

- Rancher
- OpenShift

CLOUD DEPLOYMENT SYSTEM SPECIFICATIONS

Service Provider	Specifications
AWS ECS	ECS Cluster, EC2 Worker Nodes, EFS, Auto-Scaling Group, Load Balancer, Route 53, ACM, Cloud Map, ECR
AWS EKS	EKS Cluster, EC2 Worker Nodes, EFS, Auto-Scaling group, Ingress Controller, Load Balancer, Route 53, ECR
AWS EC2 instance	Windows installer, Linux Chef Installer, Kubernetes, Auto-Scaling Group, Load Balancer, Route 53, ACM, ECR
Azure AKS	AKS Cluster, Azure Storage Account, Ingress Controller, Load Balancer, Azure DNS, Azure Container Registries
Azure Virtual Machines	Windows installer, Linux Chef Installer, Kubernetes, Virtual Machine Scale Sets, Load Balancer, DNS Zones, Container Registries
Google GKE	GKE Cluster, Instance Groups, Filestore, Ingress Controller, Load Balancer, Cloud DNS, GCR
Google Compute Engine VM instances	Windows installer, Linux Chef Installer, Kubernetes, Instance Groups, Load Balancing, Cloud DNS, Container Registry
OpenShift	OpenShift Cluster, Worker Nodes, Network File Share Storage, OpenShift Route, Certificates, Load Balancer, DNS Records, Container Registry
Rancher (Kubernetes management platform)	RKE Cluster, AWS EKS, Azure AKS, Google GKE

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS®