



Pega Cloud

4 March 2024

CONTENTS

Learning about Pega Cloud	6
Pega Cloud 3 overview.	15
Pega Cloud 3 on Google Cloud Platform overview.	18
Connectivity for Pega Cloud.	19
Pega Cloud High Availability.	21
Monitoring your Pega Cloud services environments.	30
Pega Cloud services delivery.	35
Understanding Pega Cloud services subscription provisioning.	36
Pega Cloud services support and help resources.	43
Enabling Pega GenAI in Pega Cloud.	43
Pega Cloud FAQs.	47
Getting started	49
Defining your support contact roles.	49
Accessing Pega Cloud.	50
Networking details for your Pega Cloud environments.	56
Requesting a custom domain name for applications hosted in Pega Cloud.	59
Developing your application.	65
Preparing your Customer Decision Hub application.	67
Securing your application running in Pega Cloud.	69
Tracking your Pega project in Agile Studio.	69
Moving your application using Deployment Manager.	71
Establishing a prescriptive Route to Live.	74
Best practices for RTL deployment.	76
Route to Live FAQ.	81
Pega-provided support.	84
Exploring My Pega Cloud portal.	85
Configuring your portal preferences.	87
Review My Pega Cloud portal self-service tile functionality.	88
Using Predictive Diagnostic Cloud.	90

How Pega maintains your Pega Cloud service	93
What's new.....	93
Pega Cloud 3 enhancements.....	94
Pega Cloud 2 enhancements.....	106
How Pega keeps your Pega Cloud service current.....	110
Process to update to Pega Cloud 3.....	113
Viewing the Pega Cloud 3 update process in My Pega Cloud.....	119
Client Pre-Update Actions and Approval.....	124
Deployment Manager during the update to Pega Cloud 3.....	132
Pega Cloud connectivity options	135
Change of support for connectivity options.....	138
Environment connectivity overview.....	140
Pega Cloud Secure Connect: your access to Pega Cloud.....	146
Public connectivity using AWS Direct Connect public virtual interface.....	148
Public connectivity using Cloud Exchange.....	150
Control public peering access to Pega Cloud with Border Gateway Protocol	153
Google Peering.....	169
Private connectivity using AWS PrivateLink.....	171
Connect enterprise resources to Pega Cloud with AWS PrivateLink.....	176
Private connectivity using GCP Private Service Connect.....	189
Configuring private access to Pega Cloud services (legacy options).....	195
AWS Transit Gateway.....	202
VPC peering.....	206
Virtual Private Network service.....	208
AWS Direct Connect Private Virtual Interface (VIF).....	215
Administering your Pega Cloud service	219
Setting up Pega Cloud account users.....	220
Setting up your Pega Cloud environments.....	220
Viewing maintenance activity for your Pega Cloud environments.....	226
Rescheduling Maintenance through My Pega Cloud.....	227
Entering a Support Request in My Support Portal for Pega Cloud.....	230
Initiating software updates in Pega Cloud.....	231

Messages and actions for your Pega Cloud environments.....	239
Troubleshooting using Pega log files in Pega Cloud.....	241
Using Pega Cloud status.....	242
Working with your Pega Cloud service	248
Data management services.....	249
Managing your cloud data storage effectively.....	250
Database backup and restore.....	255
Pega Platform database tools.....	257
Database archiving, purging, and data retention.....	262
Business Intelligence Exchange for Pega Cloud applications.....	262
Understanding and obtaining Pega log files.....	263
Downloading log files for troubleshooting.....	268
Streaming Pega logs to an external Amazon S3 bucket.....	274
Streaming Pega logs to Splunk.....	283
Integrating Pega applications with external systems.....	287
Connecting to REST and SOAP services.....	293
Configuring enterprise messaging using JMS.....	296
Configuring enterprise messaging using IBM MQ.....	297
File management options.....	299
Using Pega Cloud File storage.....	299
Secure Data Transfer service.....	309
Authenticating your system with the Secure Data Transfer service.....	313
Using the Secure Data Transfer service.....	318
Using Pega Cloud SFTP service.....	325
Pega Cloud SFTP service FAQ.....	330
Environment restarts.....	334
Immediate restarts.....	338
Schedule a restart.....	341
Edit or withdraw a restart.....	343
Managing hibernated environments.....	347
Change Management process.....	354
Client-configured Pega Cloud changes.....	361

Cloud Change approval process.	363
Security data and protection	374
Data-at-rest encryption.	375
Data-in-transit encryption.	375
Vulnerability testing policy for applications on Pega Cloud.	377
Vulnerability testing process for applications on Pega Cloud.	382
Considerations when Pega decommissions a Pega Cloud environment.	386
Anti-virus on Pega Cloud.	389

Learning about Pega Cloud

Pega Cloud® subscription offers a state-of-the-art, flexible and scalable cloud services. Using Pega Cloud® helps you reduce time to market, improve planning and cost efficiency, and ensure enterprise-grade security for your business.



Pega Cloud® services overview

The Pega Cloud subscription provides a fully managed cloud service platform running Pega Infinity™ and Pega Strategic Business Applications as-a-Service. Pega owns and manages Pega Cloud services, and provides clients with global and regional support models for 24x7 operations, security and monitoring to support the most demanding

enterprise applications. Pega has devoted years of significant engineering to provide a complete ecosystem to run clients' mission-critical Pega workloads.

A list of our services includes:

- Operational system support and monitoring
- Fault tolerant environments with multi-layer redundancy and backups
- Fully scalable environments not constrained by server resource limits
- Secure and hardened environments built with
 - Host-Based FW & IDS
 - Anti-Virus & Anti-Malware
 - File Integrity Monitoring
 - Data Management Services
 - Resiliency & Backup services built in
 - Management of Operating System
 - Network and Firewall configurations
 - Encryption of Data-At-Rest and Data-In-Transit

Pega Cloud is backed by a Production Availability SLA and a security/compliance strategy to support the strictest security postures that your business requires.

Pega Cloud assumes the responsibility for preparing and hosting comprehensive compliance audits, offering a service that has been independently audited and attested by many industries' most demanding compliance requirements. Go to the [Pega Trust Center](#) to learn details.

Pega's Multi-Cloud Strategy

Pega provides our Pega Cloud capabilities through a multi-cloud strategy, supporting Google Cloud Platform (GCP) and Amazon Web Services (AWS). Pega's Multi-Cloud solutions promote innovation, increase strategic alignment with our clients, expand our reach, and improve upon the already strong compliance and data sovereignty position of Pega Cloud. Pega solutions on Pega Cloud are now available on both the [Google](#)

Cloud Marketplace and AWS Marketplace, to support better strategic alignment with our clients' existing investments.

Multi-cloud is a huge leap forward for Pega clients, where the power of Pega Cloud is delivered in more places, and is more closely aligned with client's data, machine learning, and AI investments. Pega Cloud, Pega's as-a-service offering, delivers the most scalable, reliable, and secure cloud services to run your application workloads using Pega Infinity™.

Pega's multi-cloud strategy provides our clients with the following benefits:

- **Market reach:** By building a multi-cloud strategy, Pega offers our capabilities to our clients in different regions, with better proximity to the markets they serve today, or want to serve tomorrow.
- **Diligent delivery:** When deploying to multiple cloud providers, it is vital to be extremely strict about architecture, deployments, and monitoring, to mitigate operator error and ensure operations at scale. Pega designs, architects, deploys, and runs its services using a single set of tools, orchestration capabilities, and much more. This unrelenting diligence, grounded by the Pega-powered Global Operations Center, drives operational effectiveness and efficiency.
- **Innovation:** This multi-cloud strategy enables Pega to deliver more collaborative innovations for and with our partners. Pega customers gravitate to best-of-breed capabilities made available in the market from the largest hyperscalers, such as those that excel in big data, AI and ML solutions. Bringing Pega Cloud closer to capabilities our clients use every day, drives strong alignment.
- **Strategic Alignment:** Companies execute against a broad set of strategies when it comes to their cloud journeys, where the fit and purpose of a set of solutions may drive significant investment and thus closer alignment with one hyperscaler vs another. Understanding this reality, drives our multi-cloud journey for Pega Cloud, where customers can leverage existing investments to bring Pega solutions to the forefront of their digital transformation.

- **Compliance:** Our multi-cloud strategy enables customers of Pega Cloud to better meet the myriad of different regulatory requirements such as data sovereignty and data privacy in different regions, by providing more regions, in more places.

Deployment Region availability

Pega Cloud running on Google Cloud Platform is offered in selected deployment regions. For details on which Pega solutions are available in which regions, see [Deployment regions for Pega Cloud](#).

Time to Value

Why Pega Cloud services?

With Pega Cloud services, Pegasystems provides cloud services for hosting, managing and monitoring a Pega application. During onboarding, Pega provisions each client with cloud services which provide isolated Pega environments for development, testing, and fault-tolerant production services. Pega Cloud environments are encrypted with a minimum 256-bit encryption of all data-at-rest to ensure clients have complete confidence in their information security.

Pega Cloud provides the appropriate amount of computing resources and storage to support your licensed business metrics while committing to a Production availability SLA (Service Level Agreement) of 99.95%. Pega Cloud has been proven to deliver a 20,000 concurrent user application with sub-second screen response times for a major bank, and processes over a million claims transactions in under 45 minutes for a major insurer. Pega Cloud is architected to ensure your business does not need to worry about the platform or infrastructure and can feel confident in an enterprise class “Pega-as-a-Service” solution.

Our clients elect to use the Pega Cloud services for several reasons:

1. Faster time to market: Pega provisions production environments scaled to support the entire business solution with the reliability to ensure your applications are available 24x7. Pega Cloud environments are available and

operational in days, as opposed to weeks or months with traditional infrastructure approaches.

2. Lower TCO: In this cost-conscious economy, Pega provides our clients with a flat, predictable, monthly operational expense that is all-inclusive of equipment, software and personnel – so that clients can immediately tie the business case and ROI for the solution to business metrics, and avoid a large capital expense.
3. Enterprise-grade security and scalability: Pega routinely meets and exceeds clients' own internal security, performance and reliability needs.
4. Keeping your Pega solution current to allow you to continuously innovate.

Today's market conditions demand speed and agility from all businesses. We provide your Pega Cloud services environments shortly after you sign on and get you started on your Pega journey. For details on our Subscription Packages and environments, see [Understanding Pega Cloud services subscription provisioning](#).

Pega Cloud services provides each client with access to Pega Global Client Support (GCS) premium-level service for assistance with:

- Problems encountered during application development
- Issues encountered during standard use or testing
- Environmental issues, including performance and configuration problems with the product
- Upgrade or migration problems
- Other software use or operation errors

For more information, see [Pega Cloud services support and help resources](#).

Services Ready When You Are

Pega Cloud services provides a fully managed service, deploying, managing and monitoring our client's Pega application in isolated Pega environments for development, testing, and fault-tolerant production services. Pega also provides additional optional deployment services, including:

- Integration: We recognize our clients won't run Pega apps as an "island" but rather as part of an integrated collection of systems that automate and streamline their internal operations. With that in mind, Pega Cloud services includes support for numerous integration capabilities that can be licensed by the client. For details, see [Integrating Pega applications with external systems](#).
- Agile Studio: The Pega agile project management system enables your application development teams and your stakeholders to execute your projects using the industry best practice Scrum methodology. Agile Studio integrates with Dev Studio (in the Pega Platform™) for traceability between your developer environment and your project management system. As part of implementing your Pega applications, Pega strongly recommends that you use Agile Studio to track your projects' status.
- Deployment Manager: In order to make it easier for your DevOps engineers to migrate application changes from your Dev/Test system through Staging to Production, Pega can provide the Deployment Manager. Deployment Manager is a simple, ready-to-use application that offers built-in DevOps capabilities to users. It leverages Pega case-management technology to manage an automated orchestration engine, enabling you to efficiently build and run your CICD pipelines.

Security and Privacy

Pega supports some of the largest clients with the most complex business needs in the world. Pega Cloud services always keeps security central and top-of-mind when working with these clients. We provide isolated cloud services for each client, with full data encryption, and third-party attested/certified cloud services.

Pega and the client are jointly responsible for security in Pega Cloud services:

- The client is responsible for the security of, and access to, the client Application at the application level. For more information, see the Client privacy and security responsibilities section of [Client Data Rights and Responsibilities for Pega Cloud](#).

- Pegasystems is responsible for the security of the client Application and environments at the infrastructure level. See the [Security standards for Pega Cloud](#).

Pega Cloud services offers a robust set of networking and security controls that enable clients to leverage the power of Pega Platform and strategic applications as a cloud-delivered service. Your services are isolated from other clients, and include sandbox and production environments. Pega supports isolated and secure networking, and you can schedule work without affecting other clients.

Pega keeps pace with emerging and established international and local compliance standards and regulations; we maintain extensive compliance certifications and attestations, plus third-party assessments. Visit our [Trust Center](#) for details on our Compliance Certifications and Attestations.

Recognizing that our clients have different needs as they relate to connectivity, Pega provides several connectivity options for clients to connect to their Pega Cloud services. These options take into account the fact that many Pega clients now consume cloud services from other providers as well; hence, the options we provide rely on proven, enterprise-grade connectivity mechanisms that are common in the industry. For more information about private connections to Pega Cloud services, see [Pega Cloud connectivity options](#).

High Availability

Business today demands underlying systems be up and available to support nearly constant work. We provide a highly available, fault-tolerant and resilient architecture that includes a 99.95% availability SLA for your Pega solutions. For details, see [Service Level Agreement for Pega Cloud](#).

Pega Cloud services subscription includes deployment into one AWS Region. Clients select the region into which they want their Pega Cloud services to be deployed, either to meet legal locational requirements or to be located closer to their users. Pega Cloud services provisions client sandbox and production environments into the selected

region, with service components deployed across availability zones for resiliency and scale.

Pega Cloud is currently available to be deployed into numerous AWS regions; for the latest list of available regions, see [Deployment regions for Pega Cloud](#).

Pegasystems is committed to preventive safeguarding of the Pega Cloud network and high availability of Pega Cloud client environments. Pega Cloud Operations maintains a disaster recovery plan that is used by incident responders in the event of a multiple-client Severity-1 incident (as defined in the plan), and which prepares the team to rapidly respond and efficiently recover service to affected Pega Cloud clients. For more information, see [Disaster Recovery for Pega Cloud](#).

Pega Cloud Production Services provide various levels of backup and redundancy for client data, to provide full recovery of environments in the event of service disruption or failure. For more information, see [Data backup, data restoration, and data recovery for Pega Cloud](#).

Platform Transparency

To deliver a highly-available service, the Pega Cloud operations team monitors the health of Pega Cloud environments with 24x365 support from strategically located Pega Cloud operations centers. The team, a collection of Pega application experts, database administrators, and service reliability engineers, delivers Pega-specific expertise to manage your Pega Cloud services environments. See the Infrastructure Monitoring section of [Monitoring your Pega Cloud services environments](#).

The Pega Cloud operations team leverages industry-leading monitoring tools, including [Pega Diagnostic Center](#), to translate infrastructure and application activity into real-time dashboards. Pega Cloud services monitoring tools gather data at each level of the client's environment. For details, see the Monitoring architecture section of [Monitoring your Pega Cloud services environments](#).

You can access your logs in different ways. See [Understanding and obtaining Pega log files](#).

Pega Cloud services provides add-on Pega Platform log streaming. By integrating an existing Splunk logging service with Pega Cloud services, you can customize your Pega Platform application monitoring and more efficiently manage your Pega Platform logs. Log streaming gives you continual access to the Pega Platform logs in any of your Pega Cloud environments. For more information, see [Streaming Pega logs to an external Amazon S3 bucket](#) and [Streaming Pega logs to Splunk](#).

Pega is constantly delivering new capabilities in our products and services with continuous updates. Pega Cloud makes it easy for you to stay current, allowing you to maximize your investment and continuously innovate. See [How Pega keeps your Pega Cloud service current](#).

We actively support clients who run as few as dozens and as many as tens of thousands of users, many of whom have grown and scaled up with us over time. To provide this scalability, Pega Cloud offers services beyond those included in standard subscriptions. These additional options include:

- Production Mirror Sandbox
- Business Operations Environment (specific to clients who subscribe to the Strategy Optimizer bundle as part of the Customer Decision Hub solution)
- Cloud Data Storage
- Cloud File Storage
- Decision Data Storage (specific to clients who subscribe to Pega Decisioning services)
- Private connectivity

For more information on our additional services, see [Understanding Pega Cloud services subscription provisioning](#).

- **[Pega Cloud 3: The next generation of Pega Cloud services](#)**
- **[Pega Cloud 3 on Google Cloud Platform overview](#)**

- [Connectivity for Pega Cloud](#)
- [Pega Cloud High Availability](#)
- [Monitoring your Pega Cloud services environments](#)
- [Pega Cloud services delivery](#)
- [Understanding Pega Cloud services subscription provisioning](#)
- [Pega Cloud services support and help resources](#)
- [Enabling Pega GenAI in Pega Cloud](#)
- [Pega Cloud FAQs](#)

Pega Cloud 3: The next generation of Pega Cloud services

Pega Cloud® announces the general availability of its latest release, Pega Cloud 3. This new architecture delivers the most scalable, reliable, and secure Pega Cloud services to run your application workloads using Pega Infinity™. By adopting Pega Cloud 3, existing clients already running Intelligent Automation, 1:1 Customer Engagement, Customer Service, Sales Automation, and Client Onboarding solutions will experience the superior technological advancements upon which Pega builds Pega Cloud 3.

Pega Cloud 3 benefits

The Pega Cloud 3 provides a microservices architecture and uses container orchestration capabilities provided by Kubernetes. Clients running applications on this release will continue to receive the same mission-critical resiliency and security standards, while experiencing the following key benefits:

Improved Scalability

Pega Cloud's services auto-scale to meet your application demand, even beyond peak usage. Pega Cloud 3 scales dynamically, even if you have a sudden, unforeseen load increase.

Improved self-healing and fault-tolerant services

Pega Cloud 3 takes advantage of the self-healing capabilities of Kubernetes-based architecture to autonomously recover and restore services. This means that the Pega Cloud 3 recovers faster than ever, while maintaining high-availability and performance for your application workloads.

Blazing fast maintenance

Highly available environment restarts using Pega Cloud 3 allows Pega to quickly apply maintenance updates and patches across Pega Cloud.

Independent microservice updates

The microservices-based Pega Cloud 3 architecture allows for targeted, independent, and continuous service updates. This means that the latest Pega Cloud features and fixes become available to clients quickly.

Evolution of Pega Cloud services

Pega Cloud 3 is the third generation of Pega Cloud services released in the last decade. Pega is committed to continuously evolving its architecture standards, based on the latest industry technologies and practices. Pega has years of experience managing client workloads running on cloud technologies, and has mastered the management of Pega Cloud on public cloud platforms using its own automation tool suite, known as the Global Operations Center.

Coming soon on Pega Cloud 3

By adopting Pega Cloud 3, you unlock access to these planned, premium add-on services, including:

- Pega Deployment Manager support for application deployments across multiple regions.
- Multi-Region Disaster Recovery, which is a step beyond our existing support for multiple availability zones.
- Multi-cloud support allows you to run your workloads on AWS or GCP architectures.
- Self-service data management from the My Pega Cloud portal.
- Support for any new public cloud regions.

What Pega Cloud 3 means for clients

New clients or new projects for existing clients get Pega Cloud 3 by default. Pega will work with current clients to perform a one-time major update to Pega Cloud 3. After this major update, Pega Cloud will continue to conduct all maintenance processes as outlined in [Pega Cloud maintenance and types of system updates](#). Pega will strive to minimize downtime for this one-time update and complete any required connectivity reconfiguration with you before scheduling the update.

The Pega Cloud 3 update experience

Pega uses a standardized update process that provides the new Pega Cloud 3 infrastructure for your current Pega applications. Your update experience includes:

- No changes required to your applications.
- Connectivity reconfiguration. Pega will work with you to perform connectivity reconfiguration, if required. Clients might have to validate the integration endpoints that use the new connectivity configurations.
- Minimal downtime, given this is a major update. Pega will work with you to schedule the update.

Ready for action?

Pega will work with you to plan your Pega Cloud 3 updates beginning in the second half of 2023. To learn more about the update process, see [Process to update to Pega Cloud 3](#).

Pega Cloud 3 on Google Cloud Platform overview

As part of Pega's multicloud strategy, Pega Cloud® is available on Google Cloud Platform (GCP) and Amazon Web Services (AWS). This overview describes the functionality available on GCP.

What Pega Cloud 3 on Google Cloud means for clients

Clients can select Google Cloud for new projects that use Pega Cloud 3. Pega Cloud conducts all maintenance processes as outlined in [Pega Cloud maintenance and types of system updates](#).

Deployment Region availability

Pega Cloud 3 on Google Cloud is available in selected GCP deployment regions. For details, see [Deployment regions for Pega Cloud](#).

Feature support

The Pega Cloud 3 architecture, which is a fully hosted and managed as-a-service offering, delivers the most scalable, reliable, and secure Pega Cloud services to run your application workloads using Pega Infinity™.

Pega Cloud 3 on Google Cloud supports the following features:

- Connectivity that uses Private Service Connect. For more information, see [Private connectivity using GCP Private Service Connect](#).

- The use of Google Peering to establish a public peering connection with the Google network. For more information, see [Google Peering](#).
- A Secure Data Transfer Service that is API-based with which you can securely exchange files between your enterprise and your Pega Platform applications running in Pega Cloud. For more information, see [Secure Data Transfer service](#).

In the future, Pega plans to add support for Log streaming to Google projects for clients that use Pega Cloud 3 running on Google Cloud.

The following add-on services are available for purchase for subscriptions that use a GCP Pega Cloud Deployment Region. (Note that although these services are available for subscriptions in GCP regions, they run only on AWS resources):

- Pega Workforce Intelligence™
- Pega Digital Messaging
- Pega Co-Browse™
- Legacy Web Chat (formerly Pega Chat)
- Pega Voice AI

For details, see the appropriate section of [Deployment regions for Pega Cloud](#).

Connectivity for Pega Cloud

To support you in building a seamlessly integrated application environment that encompasses in-house or third-party solutions, Pega Cloud offers four connectivity options, including access over the public Internet.



Note: This content applies only to Pega Cloud environments.

Pega Cloud is a public as-a-Service solution. We recognize that clients will typically run Pega as part of an integrated estate of solutions that often span other third-party and homegrown applications. For most clients, these solutions will include both cloud and premise-based deployments. Whatever your specific case, your Pega Cloud solution

must be factored against the collective whole of your enterprise applications and services.

To simplify connectivity and provide broad accessibility, Pega supports 4 options for access to and from Pega and between client-managed or third-party SaaS providers. These options are common in the industry today, and significantly reduce configuration complexity when compared to legacy alternatives which operated more as an extension of a client's in-house network. They also provide high reliability and robust security, and include support for system-to-system integration across a broad set of interfaces.

For clients who wish it, Pega permits access over the public Internet, the ubiquitous, default approach for connecting to cloud services providers like Pega. In addition to public Internet, we support a set of additional connectivity methods, referred to as Pega Cloud Connect options, that are common in the industry.

Supported Pega Cloud Secure Connect options include:

- Cloud Exchange: a high-performance, reliable, and cost-effective solution that provides simplicity and ease of access to cloud services providers like Pega that bypasses the Internet. When we talk about cloud exchanges, we mean solutions like Equinix Fabric, Megaport MCR, PacketFabric, and many more that enable organizations to connect their existing data centers, public resources, etc. to many of the largest CSP's and as-a-service providers
- Direct Connect (Public Virtual Interface - VIF): Direct Connect is a service available from Amazon that makes it easy to establish a dedicated network connection from your premises and connected networks to the Pega Cloud, bypassing the Internet
- AWS PrivateLink: as more workloads move to the cloud, Pega Cloud needs to make sure its services can reliably and easily connect to other AWS workloads, in a "cloud-to-cloud" integration. PrivateLink provides a cost-effective and reliable solution to connect Pega Cloud services to an existing customer-managed AWS VPC

For details about Pega Cloud Secure Connect, see [Pega Cloud Secure Connect: your access to Pega Cloud](#).

Pega Cloud High Availability

Pega designs, architects, and deploys its Pega Cloud® Environments in a deployment region with significant fault tolerance and survivability.

Each Environment can endure many of the most common, and even some of the most uncommon, failure scenarios, including but not limited to failure of:

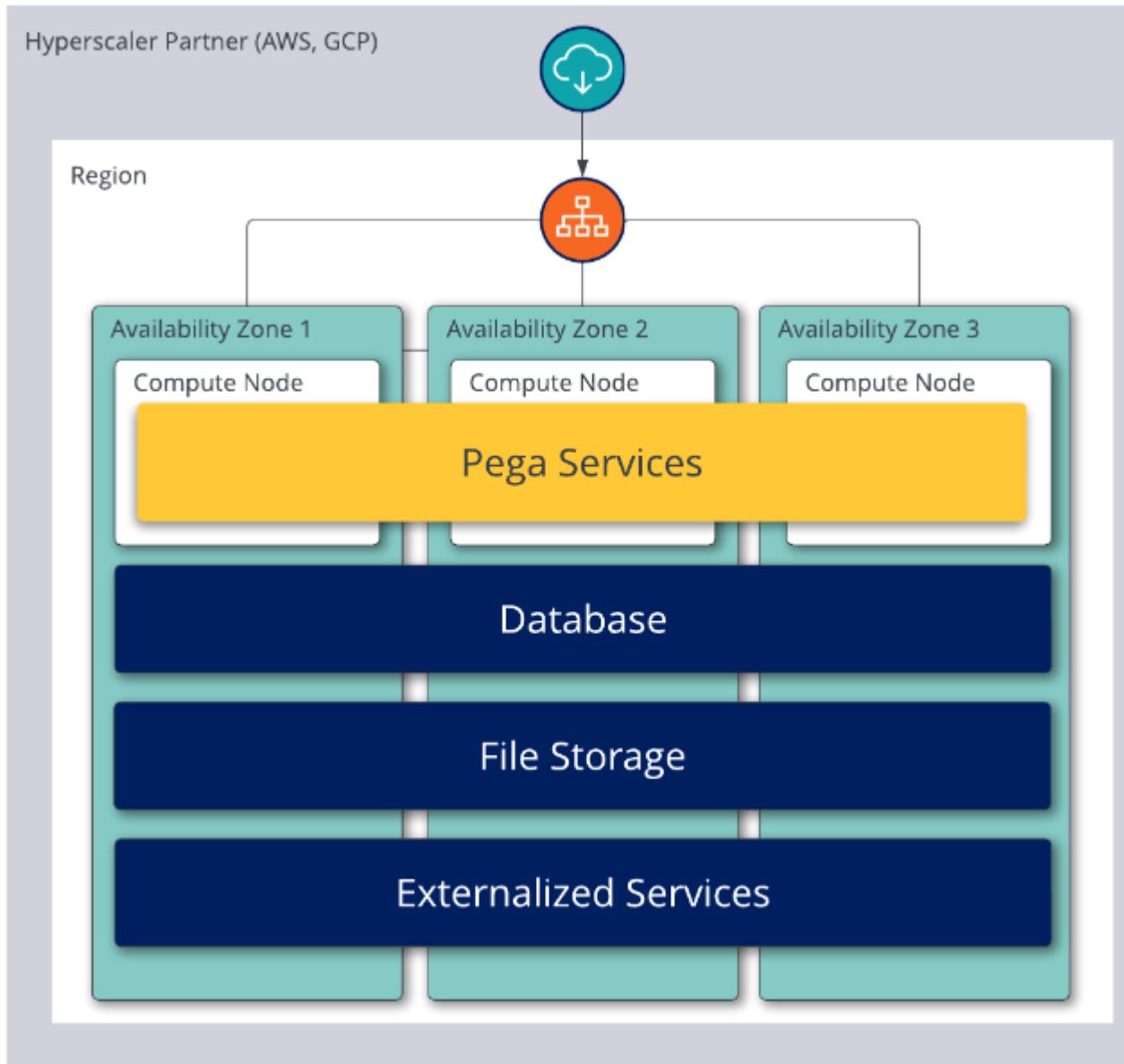
- Any single compute instance.
- A database instance or database node cluster.
- An entire Zone caused by flood, fire, or other such catastrophic event.
- Power, cooling, or other such services to a Zone.
- Load balancing resources.
- An underlying storage device within a Zone.
- A database cluster or database pair.
- Any Pega software tier or service.

Pega deploys its resources with a high availability architecture that incorporates industry-leading best practices from our hyperscaler partners and decades of Pega know-how. Our design choices around physical infrastructure, networking and routing, data and data stores, container orchestration, and Pega Infinity help us achieve the [Pega Cloud Service Level Agreement](#) and our [Data backup, data-restoration, and data durability Recovery Point and Time Objectives \(RPO/RTO\)](#).

Physical Infrastructure

Hyperscalers like AWS and GCP provide Zones which are a critical element of our high availability. Zones are highly reliable, discrete deployment areas designed to minimize risk of correlated failures from physical infrastructure outages like loss of power or cooling failures.

Pega Cloud leverages three Zones within a region for each Environment, and components are deployed to at least two of the three, depending on the high availability model of the Pega tier. We designed this highly resilient architecture with our clients' mission-critical workloads in mind. Pega Cloud Environments can survive the loss of a single Zone without suffering an outage, as the service will continue operation in another Zone without human intervention. Once our IaaS (Infrastructure as a Service) providers have restored the Zone, the Pega Cloud service will reincorporate the Zone and return to full resiliency.



Network and Routing

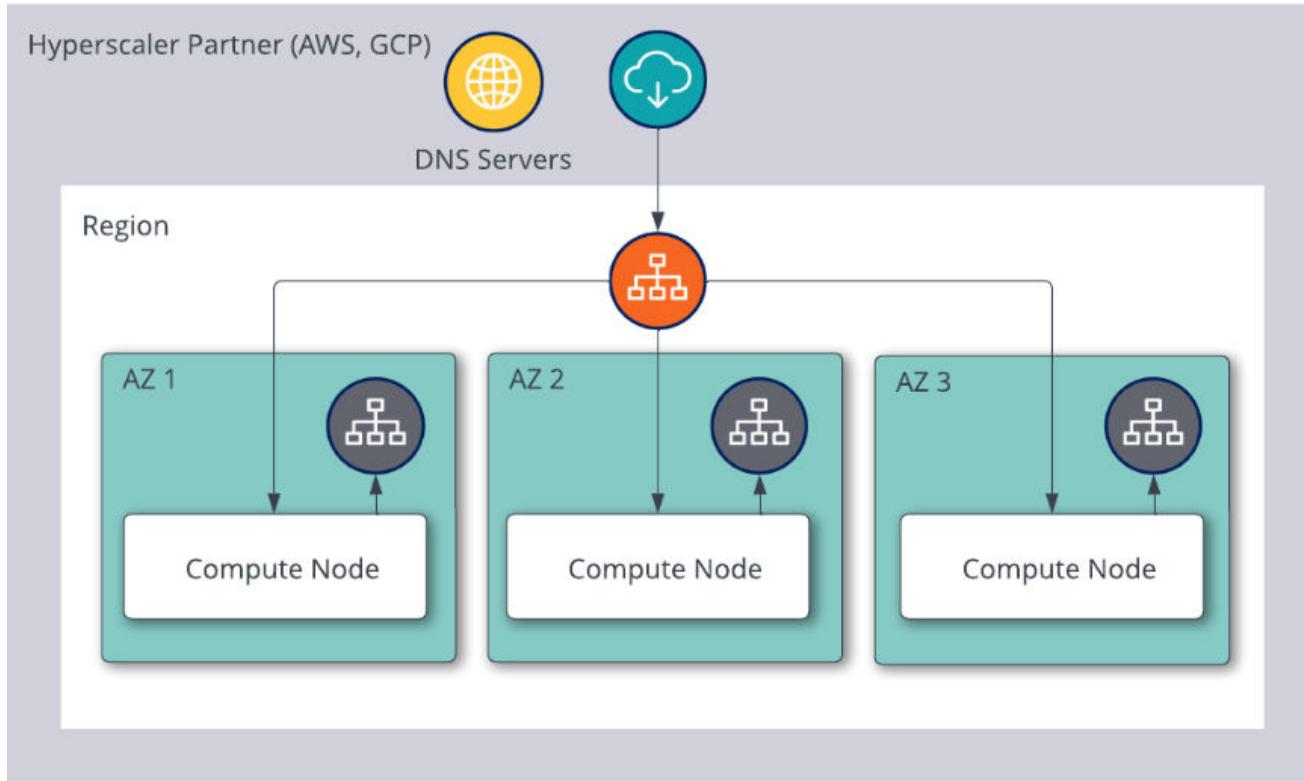
At the initial interface point of all client and system traffic originating to or from Pega Cloud, also known as the Network Edge, Pega Cloud leverages cloud native services to provide near limitless scalability, intelligent routing, and fault tolerance.

The Domain Name System (DNS) Pega Cloud leverages is highly available, and to maintain high availability, the service relies on a global anycast network of DNS servers.

around the world. Pega Cloud DNS leverages anycast, wherein many DNS hosts advertise the same IP Address. If one host fails, it stops advertising and is automatically removed from processing new requests, which helps Pega Cloud deliver optimal performance and survivability.

Public connectivity for broad access is provided through a diverse range of reliable global service providers who reliably deliver internet transport with no single points of failure. Clients leveraging connectivity through [Pega Cloud Secure Connect](#) are supported by highly available software networking. Pega Cloud Secure Connect is powered by some of the largest interconnect providers in the world who can efficiently fulfill a wide range of connectivity path requests on demand.

The highly available, infinitely scalable Pega Cloud load balancing tier routes inbound traffic to available Pegaservices. The tier also provides robust failure detection and recovery mechanisms to mitigate disruption to end users and continuously route requests to healthy services. NAT gateways provide secure access to external resources and highly available, scalable exit points for outbound traffic. These infinitely scalable NAT gateways are deployed by our hyperscaler partners across Zones for increased resiliency.



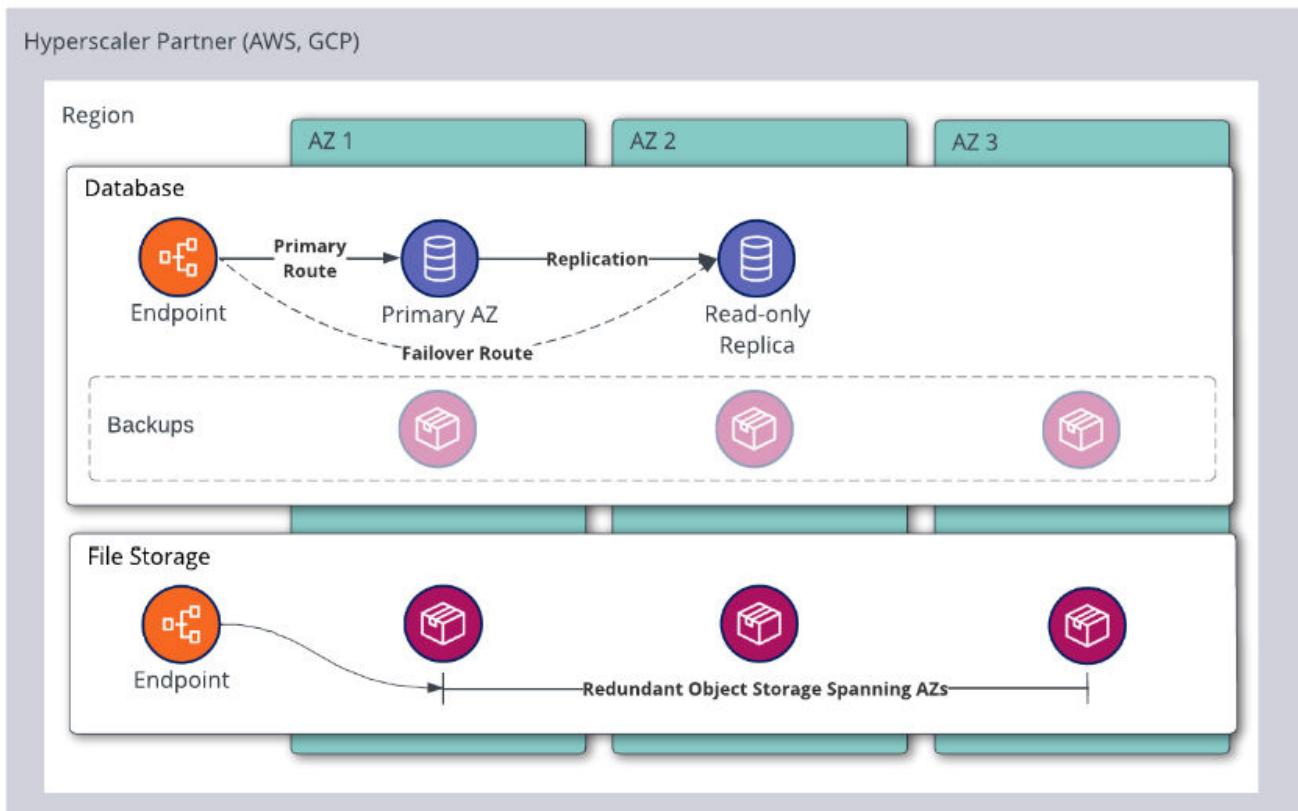
Data and Data Stores

Protecting and ensuring the durability and availability of data is critical for Pega and its clients. To achieve our world-class availability, durability, and restoration, Pega relies on state-of-the-art capabilities from the three data storage technologies we leverage.

- **Cloud Data Storage:** Pega Cloud relies on replication services that protect data by deploying a real-time standby database in a different Zone and replicating the data synchronously between the primary and the standby. Synchronous replication means that for a transaction to be viewed as successfully committed by Pega, it must be written to both the primary and standby databases. As a result, committed transactions are durably written to multiple Zones, which heavily mitigates the potential for data loss.
- **Decision Data Storage:** Database technologies operate in a clustered architecture spanning multiple Zones. A defined replication factor guarantees that multiple

copies of data exist across nodes within the cluster. This protects the service from a node or Zone failure, mitigating any impact on the durability of data.

- **Cloud File Storage:** This is commonly used for storing attachments, flat files, images, and other similar content types and provides significant durability and availability using multiple Zones. It uses industry standard concepts like erasure-coding that allow our IaaS partners to use data and code “chunks” to reconstruct an object in the event of infrastructure failure.



For more information, see [Understanding Pega Cloud services subscription provisioning](#).

Container Orchestration

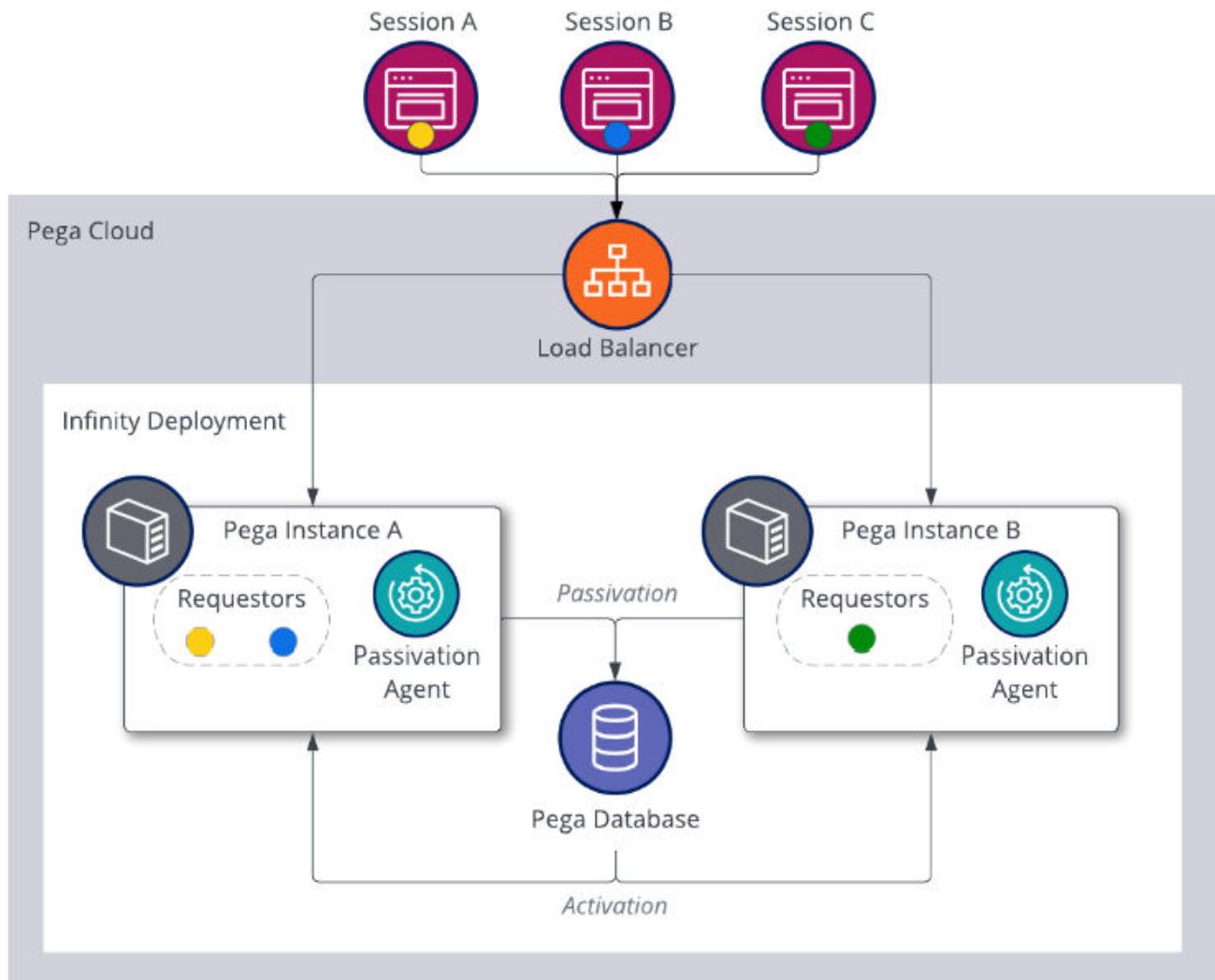
Pega Cloud leverages capabilities inherent in the Kubernetes container orchestration platform, in conjunction with hyperscaler capabilities, to seamlessly recover instances and [Kubernetes Pods](#) without user intervention.

Pega Cloud compute infrastructure is configured to restore failed resources and always keep the necessary number of instances required to meet our capacity planning requirements. The Pods that power Pega applications have native recovery capabilities: they can detect node failures, evict resources that are operating on failed nodes, and schedule resources on available nodes. This ensures the core building blocks powering Pega solutions are highly survivable.

Pega Infinity

Pega software is designed with high availability to deliver the optimal client experience. All Pega tiers are deployed without single points of failure, so new requests and work can continue to be accepted when common failures occur. Pega deployments running on Pega Cloud can seamlessly recover from resource or system failures and browser crashes. Because Pega Infinity periodically saves work in progress, it can restore a UI state to the last persisted state after a crash or failure, a process known as passivation.

Passivation is used as part of the Pega Cloud update and maintenance process. To ensure zero or near-zero downtime, Pega quiesces active resources which use passivation to cleanly take a Pega Platform node out of service for maintenance or other activities. Active users are migrated to an active node when a quiescing node is no longer available.

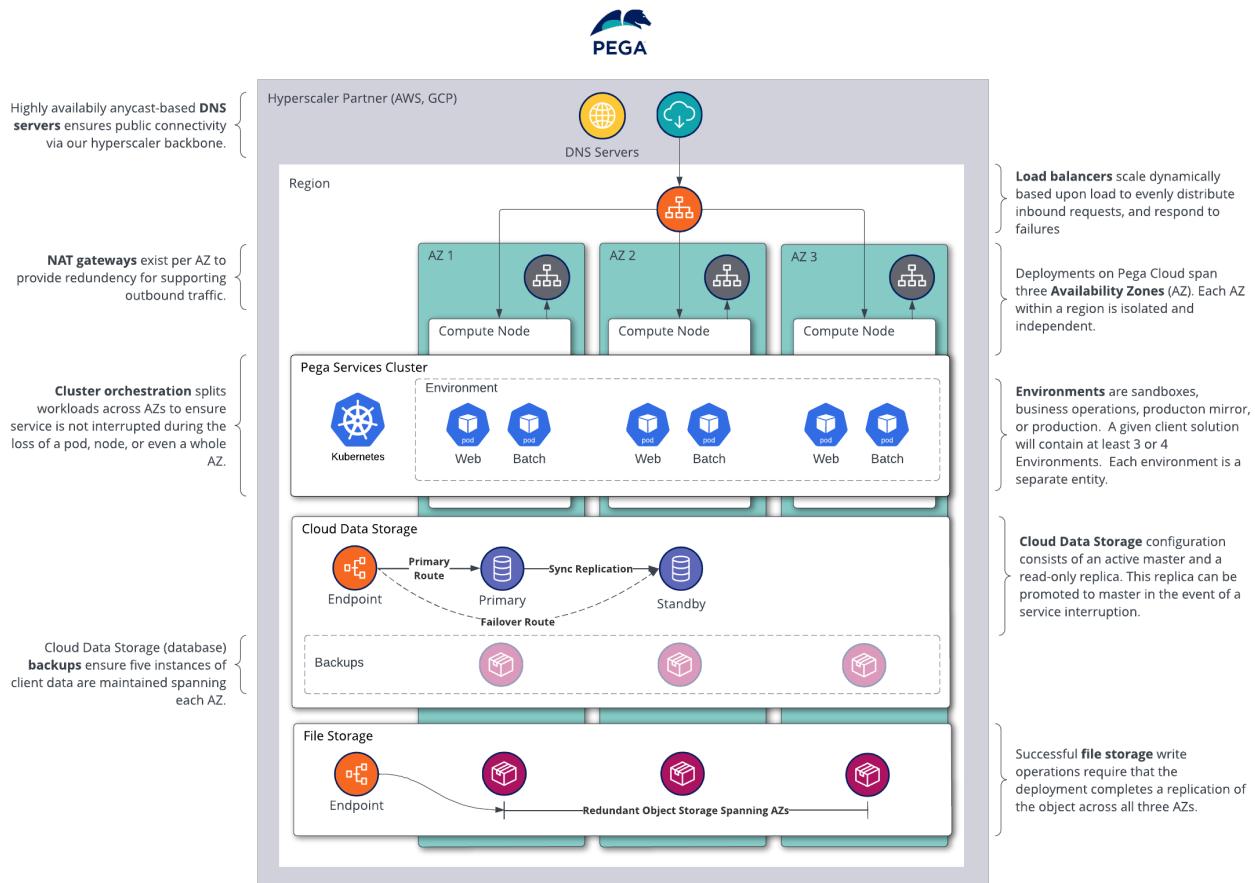


Putting it all Together

Pega Cloud is designed for fault tolerance from the ground up. In this article, you learned how:

- Multiple Zones provide robust survivability at the core, compute, and database infrastructure levels.
- The network edge, including name resolution services, provides infinite scalability, intelligent routing, and survivability.

- All Pega Cloud data stores, including object-based data stores, relational databases, and NoSQL databases, leverage state-of-the-art replication strategies and deployment topologies to ensure high availability and data durability.
- Container orchestration technology scales out, manages, and recovers Pega compute nodes to ensure client Environments can meet demanding scale and availability requirements.
- Pega service tiers are deployed without single points of failure, so new requests/work can continue to be accepted if failures occur. They can also recover session context and resume sessions in the event of crashes or browser failures.



Monitoring your Pega Cloud services environments

Pega jointly shares the responsibility of maintaining service reliability with our clients.

This is different than on-premises, or even infrastructure-as-a-service, where clients bear most of the burden of maintaining uptime and service reliability.

 **Note:** This content applies only to Pega Cloud® environments.

To deliver a service that is highly available, the Pega Cloud operations team monitors the health of Pega Cloud services environments with 24x7x365 support from strategically located Pega Cloud operations centers.

The teams are a collection of Pega application experts, database administrators, operations engineers, and security engineers who continually deliver Pega-specific expertise to help clients manage their applications running in Pega Cloud.

To maintain service reliability and uptime, our teams respond to automatically-generated alerts which, if ignored, can potentially cause degradation or disruption in Pega Cloud client applications.

Our monitoring process has the following primary areas of observations:

- Monitoring the infrastructure resources
- Monitoring the applications

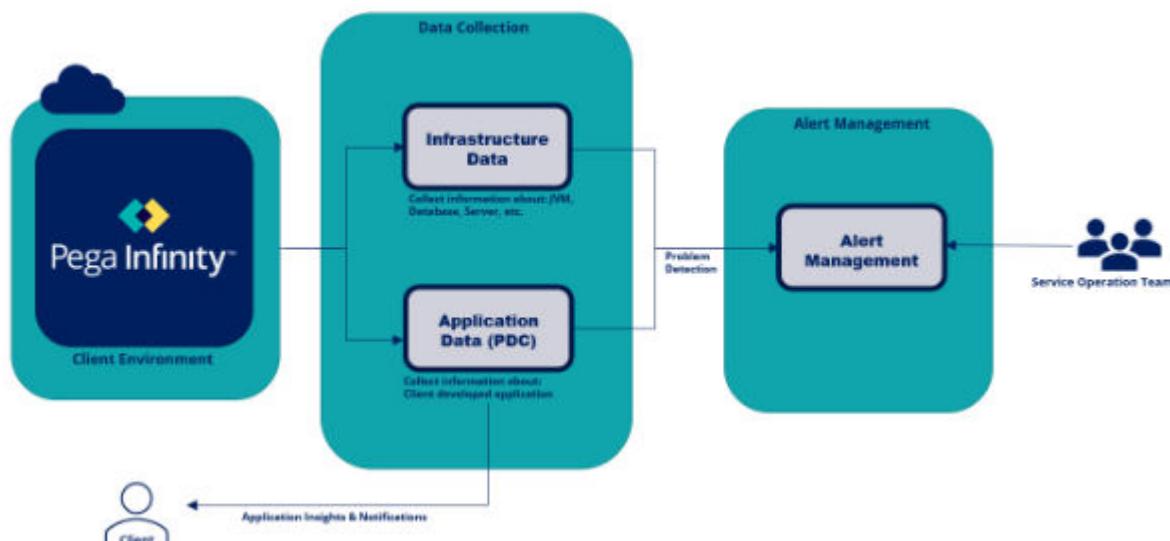
Monitoring tools and process in Pega Cloud services

The Pega Cloud operations team leverages industry-leading monitoring tools to translate infrastructure and application activity into real-time insights.

Pega Cloud services monitoring tools gather data at each level of the client's environment, such as:

- Network connectivity
- Databases
- Application servers
- The Pega Platform Layer
- Client-configured applications

Our Monitoring tools transform the raw infrastructure and application data into useful models. Data models are then translated into real-time service impact maps, that are designed to capture Key Performance Indicators (KPIs) of the health of Pega Cloud services environments. This enables the Pega Cloud operations team to maintain system availability and overall health.



The Service Operations Team data model

The Pega Cloud operations team continuously monitors all client environments for infrastructure component issues and failures, system performance degradation, and resource utilization issues. Both Pega Cloud clients and the Pega Cloud operations team share the joint responsibility of monitoring application health using Pega Predictive Diagnostic Cloud (PDC). For the PDC documentation set, see [Pega Diagnostic Center](#).

Monitoring FAQs

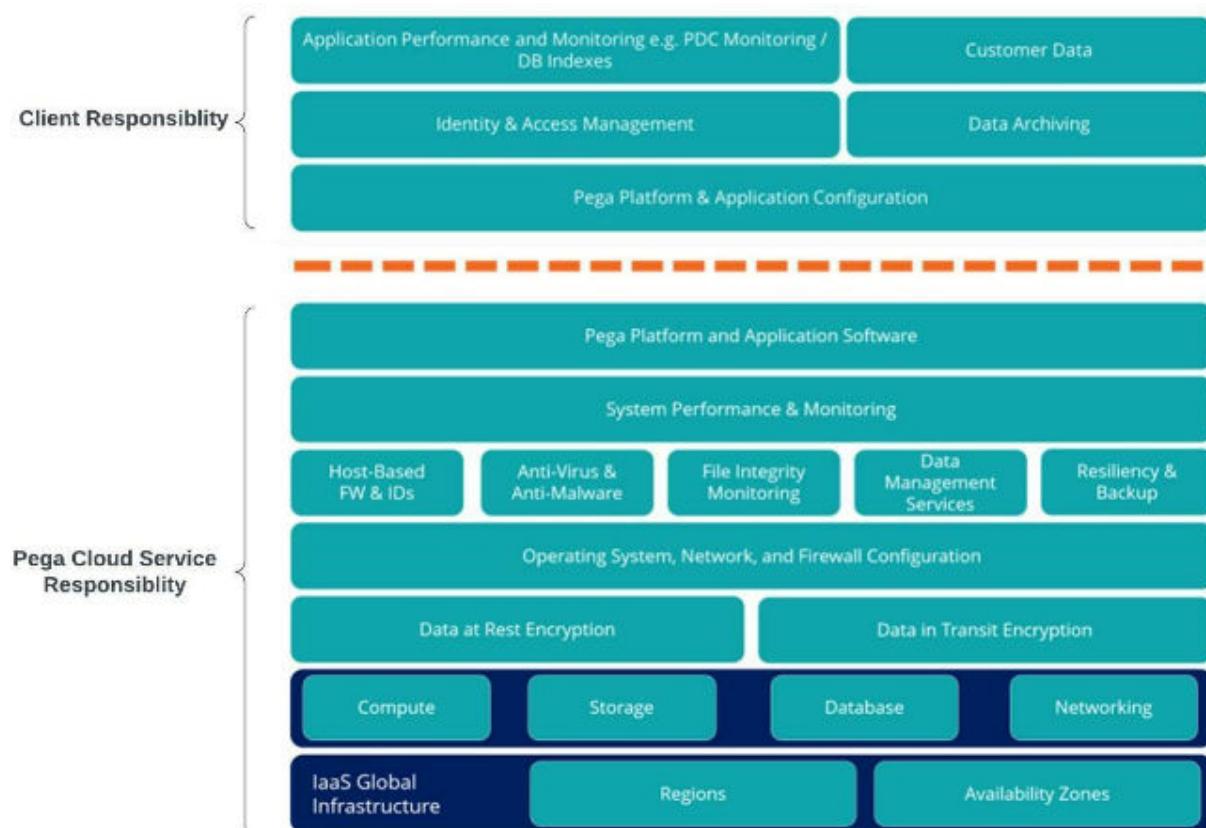
Find the most frequently asked questions about monitoring and its functionalities.

1. What are different ways to access/stream log files, track application performance, and manage PDC notifications?
 - Downloading log files for troubleshooting
 - Streaming Pega logs to an external Amazon S3 bucket
 - Streaming Pega logs to Splunk

- Using Predictive Diagnostic Cloud
- Subscribing to Pega Diagnostic Center notifications by using a REST API

2. What is the shared responsibility model of Pega Cloud?

One of the core design principles of Pega Cloud is that clients maintain control over certain functions and features jointly with the Pega Cloud team. When deploying application with an “as-a-service” provider, a shared responsibility model is the cornerstone to success. While our clients perform the tasks related to Pega applications above the dotted line, Pega performs the application-specific tasks below the dotted line. Refer to the below image:



For more details about the shared responsibility model, you can review [Pega Academy content: The Responsibility Model](#).

3. In a shared responsibility, who is responsible for ensuring underlying system utilization remains within target thresholds?

Pega fully owns the responsibility for the system level utilization of resources.

4. Can clients access the infrastructure data of their applications running in Pega Cloud?

No, Pega owns and manages Pega Cloud services and offers a 24x7x365 regional support model to clients. Additionally, Pega offers security and monitoring solutions to support the most demanding Pega enterprise applications. Pega has devoted years of significant engineering to provide a complete application ecosystem to run the clients' most mission critical Pega workloads.

5. Who will manage the infrastructure stability of a client's applications running in Pega Cloud?

The Pega Cloud operations team monitors the health of Pega Cloud services environments with our 24x7x365 support model. The team, which is a collection of Pega application experts, database administrators, and cloud operations engineers, strive to deliver Pega-specific expertise to manage your Pega Cloud services environments.

6. At what threshold infrastructure metrics is been monitored?

The Pega Cloud operations team considers multiple contexts to decide the threshold at different client and fleet environments to maintain stability in client environments. These thresholds continue to change depending on the continuous analysis and new discoveries.

7. What areas are not covered in Pega Cloud infrastructure monitoring?

- Application behavior
- Hotfix installation

For more information about Pega Diagnostic Center, see [The Pega Diagnostic Center FAQ](#).

Pega Cloud services delivery

Pega Cloud® infrastructure is fully managed by Pega. Thanks to that, you receive a secure environment for your applications without the need to manage the infrastructure stack on your own.



Note: This content applies only to Pega Cloud environments.

Pega Cloud services offers Pega Platform™ “as-a-service”, which enables our clients to focus on developing their applications. This relieves your team from the burden of managing components of your infrastructure stack. As part of your subscription agreement, Pega is responsible for provisioning, upgrading, and maintaining the reliability of your Pega Cloud infrastructure. Pega has developed a proprietary control plane to operate Pega software in the cloud, which Pega maintains, updates, and extends as part of the service. The architecture of Pega Cloud services – and how Pega operates this service – is the Intellectual Property (IP) of Pega.

The security of Pega Platform and the Pega Cloud services infrastructure is a top priority at Pega. Our technical experts are here to resolve issues that clients have in their Pega Cloud services environment. As such, unless it is relevant to the client’s responsibilities for their environment, Pega Cloud services support teams typically do not share specifics of the Pega Cloud services infrastructure, such as screenshots of capacity or usage, infrastructure logs, firewall or security configurations, and details about the general architecture of Pega Cloud services. The release of this information puts the security of Pega Cloud services environments at risk.

To help you better understand your Pega Cloud services subscription agreement, Pega provides the following examples of information which Cloud Services support teams can share with clients:

- Which aspects of your Pega application are impacting your cloud environment.
- Recommended next steps you can take to help remediate issues in your cloud environment.
- What actions Pega Cloud services support teams have taken to remediate risks or potential risks.
- How you can leverage [Pega Predictive Diagnostic Cloud](#) (PDC) to diagnose your application's health.
- Self-service capabilities available to you from the My Pega Cloud portal. For details, see [Administering your Pega Cloud service](#).
- Reports and metrics on your system's availability.
- Your cloud environment's Deployment Region.
- General information about Pega Cloud services capabilities such as [Pega Cloud connectivity options](#), [Pega Cloud Security and data protection](#), and how Pega works with your organization in [Monitoring your Pega Cloud services environments](#).

By following this approach, Pega ensures we provide clients with secure and reliable cloud environments. For more information on security responsibilities in Pega Cloud services, refer to the Security standards and Client security responsibilities sections of the [Pega Cloud subscription documentation](#).

Understanding Pega Cloud services subscription provisioning

To best match your business needs, Pega offers a range of subscription options that vary in terms of available environments and storage capacity, and can be adjusted as needed with the help of the Pega team.



Note: This content applies only to Pega Cloud environments.

During the sales cycle, the Pega Cloud® services team works with you to determine the appropriate business metrics that reflect your business needs. Pega Cloud services

uses this information to optimize the configurations of your environments in areas such as data management, security, system availability, network integrations, and data backup.

Pega recommends a development environment to start, followed by introducing staging and production environments as you integrate your Pega application into a DevOps environment. The main differences between these types of environments are shown:

Environment	Cloud Instance	Description
Development	Standard Sandbox	Development, testing and User Acceptance Testing
Staging	Large Sandbox	<p>Pre-production, staging, user acceptance testing, and/or limited performance testing.</p> <div style="background-color: #e0f2ff; padding: 10px; border-left: 2px solid #337ab7; margin-left: 20px;"> Note: This Sandbox is not intended for load testing. For full-scale performance testing, contact your Pega representative about a Production Mirror sandbox. </div>
Production	Production	A scaled environment that supports the production

Environment	Cloud Instance	Description
		deployment of Pega Platform™, applications, and transactional use cases

Subscription Provisioning

Following the signing of your initial subscription agreement, the Pega Cloud services team provisions your environments based on your contracted entitlements. The Pega Cloud services team configures each component of your environment using a fault-tolerant architecture which includes your virtually isolated network, subnets, database, application servers, Pega Platform™, and any other subscribed Pega applications. As soon as your environments are provisioned, you receive a New System Release email which outlines the software which the Pega Cloud services team installed. For more information, see [Accessing Pega Cloud](#).

Subscription Packages

Pega Cloud Standard Production Services Subscription Package

The Standard Production Services subscription package provides entitlements for Pega Cloud services. The standard subscription package includes:

- Client cloud services in a single geographic region.
- One production environment, which offers isolation of core processing and data, that is designed and built to support the licensed Pega Platform, applications, business metrics, and services as described in the client's contract.
- One Standard Sandbox (see definition in Environments)
- One Large Sandbox (see definition in Environments)
- 500 GB of Cloud File Storage (allocated per customer account – shared across all environments)
- 100 GB of Cloud Data Storage

Pega Cloud Standard Dev/Test Subscription Package

The Standard Dev/Test subscription package supports additional development and testing needs for Pega Cloud. Features of this subscription package include:

- Client cloud services in a single geographic region.
- Two Standard Sandboxes or, by request, one Large Sandbox instead of two standard sandboxes.



Note: Software licenses are not included with this package.

Additional Pega Cloud Storage Capacity Options

Pega Cloud services includes a base amount of storage, based on subscription commitment. Clients who require additional capacity can add storage, as follows:

Cloud Data Storage

An integrated database that the Pega application manages, into which it stores its business/process data and rules data. For Pega Marketing and/or Pega Customer Decision Hub applications, this is the storage location for Interaction History and the Pega Customer Movie. Expanded storage capacity can be added as needed (additional fees apply).

Cloud File Storage

An additional data repository managed by the Pega application, into which it stores files associated with features such as archive/purge, large attachment handling and file transfer services. Expanded storage capacity can be added as needed (additional fees apply).

Decision Data Storage

An additional datastore which is managed by the Pega application, into which the Pega Marketing and/or Pega Customer Decision Hub applications store recoding decisions that are leveraged through the Adaptive Decision Manager (ADM) module.

(included for clients purchasing Pega applications using Pega Customer Decision Hub)

Additional Pega Cloud services

Services beyond those included in standard subscriptions, which can be quoted separately. These additional options include:

- Private Connectivity
- Ensuring encryption of data in transit (within the client environment)
- Secure File Transfer (SFTP) (no additional fee required)
- In-region client support
- Specific industry compliance (example: FedRAMP)

Environments

Standard Sandbox

The Pega Cloud services Standard Sandbox (often called a “development” or “Dev/Test” environment) is designed to support clients who need easy access to an environment for development, functional and unit testing, and user acceptance testing. This environment is scaled to support your current licensed Pega products, with:

- Up to 15 regular developers, testers, or users
- Includes 50 GB Cloud Datastorage
- Does not include Cloud File storage

This service is not recommended to be used for live data and production services, or to support performance testing at load.

Large Sandbox

The Pega Cloud services Large Sandbox (often called a “Staging” environment) supports preproduction, staging, and testing. Clients can use this sandbox to

support the needs of larger development teams. This fixed-size environment supports your current licensed Pega products, with:

- Up to 45 regular developers and testers
- Includes 100 GB Cloud Data storage
- Does not include Cloud File storage

This service is not recommended to be used for live data and production services, or to support performance testing at load.

Production Mirror Sandbox

Clients with additional security or compliance requirements for their production environments may consider subscribing to the provisioning of a Production Mirror sandbox service (for an additional fee). This service provides an architectural replica of your scaled production environment and can be used for production staging, scale benchmark testing, and load performance testing. Data sets are not automatically synchronized between the production mirror sandbox and production environments, but service includes support for one data refresh per month, which is facilitated by [creating a ticket in My Support Portal](#).

Business Operations Environment

This environment is only relevant for Pega Customer Decision Hub clients who subscribe to the Strategy Optimizer bundle.

The Business Operations environment allows you to simulate the offers that your decisioning engine would suggest, so that you can test our Pega Customer Decision Hub (previously called Pega Marketing) and the decisioning recommendations you've configured. The Business Operations Environment uses the most recent 20% of your history to simulate offers.

The Business Operations Environment is an environment that allows business users and Next-Best-Actionspecialists to design and test various artifacts that are intended to eventually move into production for execution. This is not a performance test environment. Rather, it is an environment where you can

design, build and test various Next-Best-Action changes based on business needs to add, adjust and tune items such as offers, treatments, engagement policies, channel configurations and so forth. It allows you to understand the impact of proposed changes before pushing into Production.

The Business Operations Environment supports the functional simulation testing of Pega Customer Decision Hub (CDH)-based decisioning applications in the form of a batch decisioning process in an 8-hour window. It is scaled to support processing through 20% of the most recently engaged client records, their associated interaction history and supporting analytical models. Data refresh is orchestrated by Deployment Manager up to a maximum of once per day from the Production Environment, as limited by the licensed batch/bulk decisioning capacity defined in the order schedule for the associated Production Environment.

This environment is not required for CDH, but is recommended as a best practice for clients that leverage CDH, to effectively and efficiently design, build, and test strategies. All development work and business-as-usual changes should be done outside of the Production Environment. For more information, see [1:1 Strategy Optimizer Bundle](#).

The Business Operations Environment is available as part of the Strategy Optimizer bundle, which is an optional purchase. See your order schedule to determine whether your organization has subscribed to the Strategy Optimizer bundle; if you wish to add it, please contact your Pega or Pega-Partner account representative.

For more information, see [1:1 Strategy Optimizer Bundle](#).

Production Environment

The Pega Cloud services Production Environment is a scaled environment that supports the production deployment of licensed Pega Platform, applications, and licensed entitlements. This environment:

- Allows for business continuity, scalability based on the licensed business metrics, and a defined storage limit set in the Order Schedule.
- Is deployed across multiple availability zones with database backup and replication services and is backed by a 99.95% Availability Service-Level Agreement (SLA).

Pega Cloud services support and help resources

Leverage the full potential of your Pega Cloud® subscription by using the knowledge resources and support services provided by Pega alongside your main service.



Note: This content applies only to Pega Cloud environments.

The Pega Global Client Support (GCS) team is dedicated to keeping your Pega products, including Pega Cloud services, up and running effectively. For information about GCS and the support the team provides, see [How to Get Support](#) and [Support@Pega Client Handbook](#).

In addition, you can refer to the following resources for information about using Pega products, including Pega Cloud services:

- The [Pega Support Center](#) offers a search function for specific support topics about Pega Platform™, Pega Cloud, and other Pega products.
- [Pega Academy](#) offers courses that are designed and developed by Pega-certified experts to provide design and implementation best practices for Pegasystems products.

Enabling Pega GenAI in Pega Cloud

Pega GenAI™ capabilities are available exclusively for Pega Cloud® clients with active subscriptions. Clients can leverage Pega GenAI for enhancing their application

development experience, as well as developing application scenarios for proof of concepts to model and experimenting with how Pega GenAI can improve business processes and client interactions.

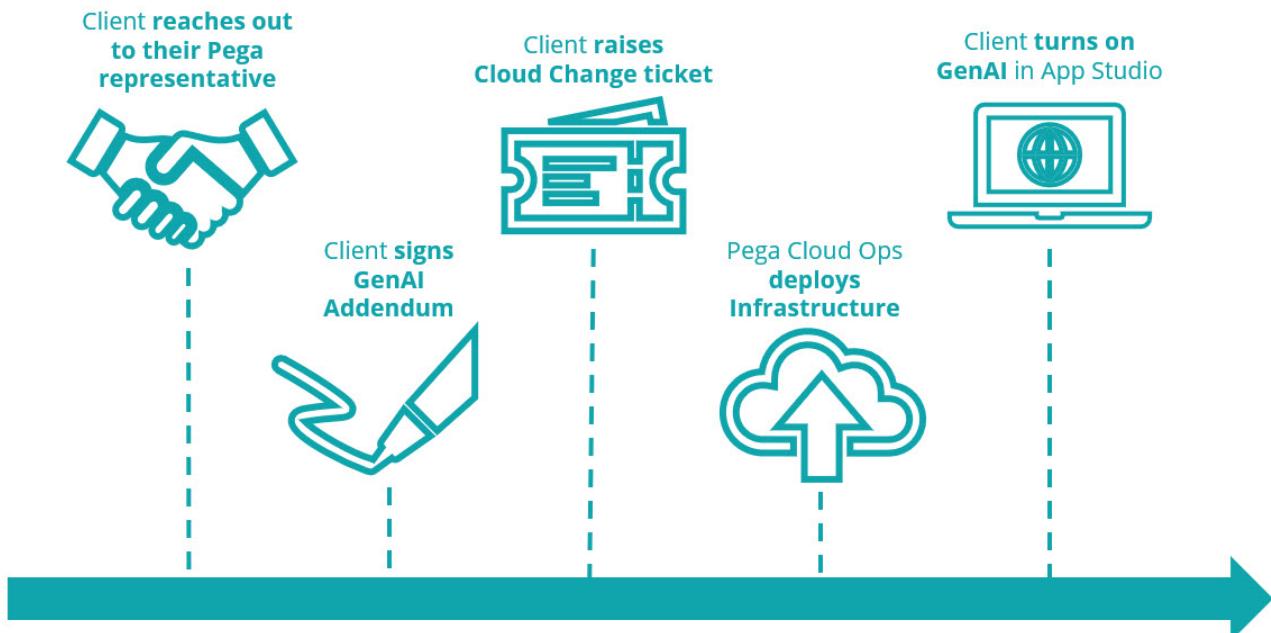
For more information on Pega GenAI capabilities, see [What's new in generative AI](#).

If you are a Pega Cloud client and you would like to add Pega GenAI capabilities to your subscription, reach out to your Pega account representative. Pega will work with you to validate that your Pega Cloud service meets the prerequisites for Pega GenAI.

After validation of your Pega Cloud service, your representative will work with you to incorporate Pega GenAI capabilities into the terms of your subscription.

Enabling Pega GenAI in Pega Cloud

Below is an overview of the process to enable Pega GenAI in Pega Cloud.



Creating the Cloud Change request



Remember: Clients sign the GenAI Addendum before creating the Cloud Change request to enable Pega GenAI in their Pega Cloud environments.

After you have signed the GenAI Addendum:

1. Confirm you have the Cloud Specialist role in My Support Portal, which provides you the privilege to create Cloud Change requests. To learn more, see the [Cloud Change approval process](#).
2. Create a Cloud Change request in [My Support Portal](#). To learn more, see [How to request a Cloud change in My Support Portal \(MSP\)](#).
3. Choose the Pega Cloud environment(s) to enable Pega GenAI.
4. Select the **Activate Pega GenAI** task.

Add new task

Task *	Responsible team
Gen	Select

New or Additional Deployments

Activate Pega GenAI	Standard	Singular
---------------------	----------	----------

Description
--
[Hide task description](#)

Task details

[Cancel](#) [Submit](#)

[Continue](#)

After you submit the Cloud Change request, the Pega Cloud operations team deploys Pega GenAI in your selected Pega Cloud environment(s) and notifies you about the successful deployment in the Cloud Change ticket.

Enabling Generative AI in App Studio

After you are notified that Pega GenAI has been deployed in your Pega Cloud environment(s), you connect your application to generative AI in App Studio. To learn more, see [Connecting to the generative AI provider in Pega Cloud](#).

Pega Cloud FAQs

Consider these Frequently Asked Questions (FAQ) to become familiar with common inquiries about Pega Cloud®.

What is the auto-scaling methodology of Pega Cloud?

The auto-scaling methodology is Pega intellectual property. Consequently, we do not disclose it. As a fully managed service, the operations team monitors the performance of each Pega Cloud environment. If any performance challenges are noted, the team manages scaling your infrastructure in a targeted fashion to ensure continued performance and availability.

The auto-scaling strategy is based on a pragmatic approach focused on optimizing your stack--applications, database, and network. The methodology is a continuous improvement process that ensures we provide the resources to meet your application needs.

Does Pega Cloud support customer-provided application monitoring?

As a fully managed service, the operations team leverages a suite of monitoring tools to ensure your applications can meet peak performance requirements. Each subscription includes [Pega Predictive Diagnostic Cloud](#), which provides detailed insight into your application performance. To ensure a consistent and optimized Pega Cloud environment, the use of other monitoring applications is unsupported by Pega.

Can Pega Cloud customers access the database of their application?

Pega Cloud does not support direct access to your application database to avoid negative downstream impacts. For example, changes to the database can prevent successful deployment of future Pega Platform™ releases and patch releases and the adoption of the latest features.

Where can I find the latest information on software upgrades and patches and infrastructure updates for my Pega Cloud environments?

Pega maintains the latest details for software upgrades and patches and infrastructure updates to Pega Cloud environments in the article, [Pega Cloud maintenance and types of system updates](#).

What details are available in customer-facing release notes on the Pega Cloud page?

Release notes for Pega Cloud are organized and published on a quarterly basis. This schedule is based on continuous cadence of releases. The release notes detail enhancements made to Pega Cloud throughout the current quarter that impact customers. New Pega Platform features and enhancements supported by Pega Cloud services are documented in Pega Platform release notes, so they are not included in the Pega Cloud services release notes.

Can I modify the production level for my Pega Cloud environment?

During the provisioning for any Pega Cloud environment, Pega Cloud does not support changing the default production-level that Pega Cloud sets. For additional details, see [Specifying the production level](#).

Getting started with Pega Cloud

Now that you've received your new Pega Cloud® environment(s), you are ready to run and manage your Pega applications. Pega Cloud has already provisioned your virtual spaces and environments (Dev/test, Staging, or Production) and installed all of your required software as outlined in your agreement.

While your software is ready for your use, there are required set up steps that only you can complete, such as entering in your user information. Use the information here as a path to complete the various set up steps required or recommended after your organization signs a Pega Cloud contract.

- [Defining your support contact roles](#)
- [Accessing Pega Cloud](#)
- [Developing your application](#)
- [Exploring My Pega Cloud portal](#)
- [Using Predictive Diagnostic Cloud](#)

Defining your support contact roles

As part of the sales process, you define your Pega Cloud® support contact roles at your company. The contacts with these roles work with Pega Global Client Support (GCS) for issues with your Pega Cloud. If you still need to define the roles or need to change them, use the following information.



Note: These contacts must remain current in order for Pega to know whom to contact for important Pega Cloud issues.

For information about what each role grants, see [Understanding Support user roles](#).

Your organization must designate these contacts as part of your adherence to Pega Cloud Security best practices. Only the authorized contacts are allowed to approve changes to your cloud environment or receive alerts and other information.

Each of your organizational contacts must have already created an account for themselves on Pega Community before they can be designated as a contact. If you have licensed one or more Pega Cloud services environments, determine which people are going to become contacts, and verify that they have each created their own account on the Pega Community.

Accessing Pega Cloud

When your Pega Cloud® environment is ready, you receive one or more *New System Release Notification* emails with information about your system. These emails provide you with the details needed to gain access, such as the different types of build environments, where they're located, and the credentials you use. Use this information to help you gain access to Pega Cloud.

Depending on whether environments such as dev-test and production are provisioned on the same day, you might receive separate emails as the environments become ready.

- Note:** Clients who need to request a custom domain name that conforms to
- ⓘ your enterprise standards should review the article, [Requesting a custom domain name for applications hosted in Pega Cloud](#).

Emails include details about the installed software and access. However, to provide appropriate security, you will receive a separate email from Pega Sharefile. This email includes instructions on how to download credentials in a secure manner.

Important: After you receive your credentials and log in for the first time, update your password immediately as a security measure. Choose a password that conforms to your site security standards and policies. To secure your environment, review and implement the best security practices as outlined in [Security Checklist when deploying on Pega Cloud](#). If you require a password reset or have questions about account access and user or role changes in your account, refer to [My Support Portal Frequently Asked Questions](#).

Pega Cloud Services URLs

Note: The example urls in this article use the "pega.net" domain, which is applicable for Pega Cloud 3. Pega Cloud 2 urls use "pegacloud.net" instead of "pega.net". You can view your own urls in [My Pega Cloud](#).

The URL designation for each system follows a standard assignment. For example:

```
https://<company designation>-<project designation>-<system/server designation>.pega.net/prweb
```

<*Company designation*> is the short name for your company. For example, ABC Company has the designation *abc*.

The <*Project designation*> is the project where your company will use this application. ABC Bank might have a credit card, or *ccard* project.

System/server designation specifies the system or server that is being accessed. Some standard examples include the following environments:

Environment	Description
prod1	Production environment
dt1	Development/test environment

Environment	Description
stg1	Staging environment
agilestudio	Agile Studio environment
pdc2	Pega Predictive Diagnostic Cloud environment

If your system includes the Secure File Transfer Protocol (SFTP) Service, you also receive URLs for that service. For more information about SFTP, see [Using Pega Cloud SFTP service](#).

Example Production Environment email information

Example Email

An example email for “ABC Company” is shown below, with URLs that contain the company designation of “abc”:

For example:

Your Pega Cloud services subscription provides access to the following software:

- Pega Infinity™/ <version number>
- Pega BIX
- Pega CRM
- Pega Field Service

Access Details

- Pre-production / Staging [Large Sandbox]
 - Application: <https://abc-stg1.pega.net/prweb>
 - SFTP Service: abc-stg1-sftp.pega.net
- Production [Production Environment]
 - Application: <https://abc-prod1.pega.net/prweb>
 - SFTP Service: abc-prod1-sftp.pega.net

Access Credentials

You will shortly receive an email from Pega Sharefile with instructions to download your credentials in a secure manner. If you do not receive an email within the next hour, message CloudSystemRelease@pega.com.

Pega Cloud Services Utilities:

Predictive Diagnostic Cloud:

```
https://pdc2.pegacloud.com/prweb/PRServlet/  
abcdefghijklmnopqrstuvwxyz6HdERvrbPVd-JAoQUkyNZ1xXcqdqFw%5B%5B*/!  
STANDARD
```

Pega Cloud comes integrated with [Pega Predictive Diagnostic Cloud](#) (PDC), which continually evaluates various areas of your system to ensure stability and identify the most valuable improvement opportunities. For more information about access PDC in your Pega Cloud, see [Using Predictive Diagnostic Cloud](#).

Deployment Manager: <https://dmas-abc.pegacloud.com>

Deployment Manager is available as a service free of charge; it is used to jumpstart the DevOps automation journey. Deployment Manager has pre-configured templates that automate CICD workflows, including branch merges, application packages, artifact management, quality gates, and deployment. Use your Pega Community credentials to access Deployment Manager. See [Getting started with Deployment Manager](#) on Pega Cloud to understand the guided steps to create your first pipeline.

Agile Studio: <https://abc-agilestudio.pegacloud.net/prweb>

Agile Studio is another optional environment available free of charge, which enables your application development teams and your stakeholders to execute your projects using the industry best practice Scrum methodology. If you would

like this optional environment provisioned, you can request it by selecting [Create a ticket in My Support Portal](#).

Credential Information

Credentials are provided in a series of text files, and are sent separately from the *Welcome* email information for the greatest security. The following are examples for ABC company, with their credit card project, ccard.

For example:

Dev/Test Environment file:

Application URL: `https://abc-ccard-dt1.pega.net/prweb`

Username: `administrator@pega.com` password:

`*****`

For example:

Staging environment file:

Application URL: `https://abc-ccard-stg1.pega.net/prweb`

Username: `administrator@pega.com` password: `*****`

For example:

Production environment file:

Application URL: `https://abc-ccard-prod1.pega.net/prweb`

Username: administrator@pega.com password: ****

❖ **For example:**

Pega Marketing environment file:

Application URL: https://abc-ccard-dt1.pega.net/prweb

Username: administrator@pega.com Password: ****

Decision Hub URL: https://abc-ccard-dt1-decisionhub.pega.net/prweb

SFTP Hostname: abc-ccard-dt1-sftp.pega.net

ⓘ **Note:** The Decision Hub URL sends you to the landing page for your Customer Decision Hub.

❖ **For example:**

Agile Studio environment file:

Application URL: https://abc-ccard-agilestudio.pega.net/prweb

Username: administrator@pega.com password: ****

AgileStudio Username: AgileStudioSysAdmin password: ****

≡ **For example:**

Pega PDC environment file:

```
PDC Tenants PDC Access URL: https://pdc2.pegacloud.com/prweb/  
PRServlet/abcdefghijklmnoprpqkEeSbUxnzFXDJa3vf8FY%5B*/!  
STANDARD
```

```
SOAP URL: https://pdc2.pegacloud.com/prweb/PRSOAPServlet/  
abcdefghijklmnoprpqkEeSbUxnzFXDJa3vf8FY%255B*/SOAP/PegaAES/  
Events
```

```
Operator: DiagnosticCloudManager Password: *****
```

```
Operator: DiagnosticCloudUser Password: *****
```

≡ **For example:**

If you require a password reset or have questions about account access and user or role changes in your account, refer to [My Support Portal Frequently Asked Questions](#).

- [Networking details for your Pega Cloud environments](#)
- [Requesting a custom domain name for applications hosted in Pega Cloud](#)

Networking details for your Pega Cloud environments

Pega Cloud® maintains a robust set of networking and security controls that enables you to take advantage of the power of Pega Platform™, strategic applications, and third-party integrations provided as a cloud-delivered service.

Pega provisions development, staging, and production environments for each client hosted in an AWS region for public, private, and hybrid connectivity.

Connecting to Pega Cloud

You have access to your applications and integration services in Pega Cloud through a secure Internet connection using IPV4. Pega Cloud does not support IPv6 network connections. Pega Cloud supports the following network connectivity methods:

Internet only

This option supports secure Internet access for all user traffic, such as hosted applications and Dev Studio, as well as integration services traffic.

Private connection only

For private network connectivity, several private access services for connection traffic are available.

Internet plus private connection

This option includes secure Internet access for all user traffic, as described above, as well as the option to have private access services to your private network for all inbound traffic.

Accessing Pega Cloud

For each client Pega Cloud supports a series of Pega application computing resources. You can connect to each application with a public IP address and a private IP address. During the client onboarding delivery process, Pega allows inbound traffic (client to Pega Cloud) by default and can restrict inbound traffic based on your application needs. Pega allows all outbound traffic (Pega Cloud to client).

Pega Cloud offers a secure, flexible, and scalable way to integrate with your enterprise network, including connections that originate from a pool of three static source IP

addresses to connect to your enterprise network. All system instances in Pega Cloud share from this pool of static source IP addresses.

Pega chose to support specific connectivity options to provide the best experience on Pega Cloud. Our choice of options are grounded in the principles of Zero Trust Architectures and enforce separation between networks. Following this methodology offers maximum flexibility for Pega Cloud and clients. For example:

- Integrations, such as adding additional third-party services, become much easier to manage, identify and monitor.
- Network isolation insulates all parties from Enterprise network variations, such as scaling your enterprise network.

Combining our connectivity options with application-level encryption, authentication and authorization provides you with a highly secure architecture.

For more information about adding public connections to an allow list and configuring private access to and from Pega Cloud, see [Configuring public access between your Pega Cloud environment](#) and [Configuring private access to your Pega Cloud environment](#).

DNS resolution

Pega does not resolve network connectivity to Pega Cloud using IP addresses. Instead, Pega Cloud relies on the DNS (Domain Name System) server for the enterprise network of each client for communication between Pega Cloud and the public Internet. During onboarding, Pega requires you to share your DNS name resolution protocol so that Pega can configure Pega Cloud connectivity to use your DNS server. As long as the DNS server in your enterprise environment provides name resolution, your network traffic can access your Pega applications.

Pega Cloud assigns each client a single public domain for public Internet access for your Pega Cloud services during initial provisioning. In addition, Pega maintains a private host zone for internal communications.

For clients using a public domain, Pega uses the naming convention:

<clientname.pegacloud.io>.

If you only want remote access to your private servers or private services through Pega Cloud, Pega uses the naming convention: <clientID.internal>.

Pega also provides the option for you to use a customized domain, for example:

<AcmeBank.mortgage.com>. To request a custom domain, see [Requesting a custom domain name for applications hosted in Pega Cloud](#).

Pega also supports the ability to forward traffic to domains, IP addresses, or host zones that you have specified in your DNS server resolver rules that depend on the type of connection to Pega Cloud:

- For inbound connections, Pega can resolve domains to a private host zone on your Pega Cloud environment.
- For outbound connections, Pega can specify domains and IP addresses that you want to forward to match a specific resolver rule. For example, if you connect to a domain that contains multiple resolver rules (acmebank.mortgage.com , mortgage.com), Pega can forward the query to the domain with the most specific match (acmebank.mortgage.com).

If you want Pega Cloud to resolve to private host zones only, or if you want to add additional forwarding rules to your resolution requirements, you can make a request that states your DNS resolution requirements with your regional Pega support representative by using the [Create a ticket](#) button in [My Support Portal](#). Pega Cloud provides the details required to resolve DNS according to your specification.

Requesting a custom domain name for applications hosted in Pega Cloud

For your applications that are hosted in your Pega Cloud®, a client can use a custom domain name that conforms to your enterprise standards.

By using a custom domain name, users of your Pega Cloud services-hosted applications see domain names that are familiar to them. For example, if a client already registered a domain (for example, www.CustomerSite.com), you can now host your Pega applications on CreditCard.CustomerSite.com instead of CreditCard-prod1.pega.net.

The certificates that are generated by this process are protected and managed by Amazon Web Services (AWS) Certificate Manager (ACM). ACM simplifies the certificate request and renewal process as well as secures each certificate's private key using AWS Key Management Service (KMS).

A client's private key can never be exported or exposed which ensures a secure process.

Certificate validation requirements

Every certificate must be validated. The following two methods are available:

- DNS Validation
- Email Validation

Pega Cloud recommends every client utilize the DNS validation method. If a client does not have the ability to add a new record to your Domain Zone file, email validation is required.

Pega Cloud selects one of the two methods during the certificate request process based on your preference.

DNS validation

Pega Cloud selects DNS validation during the certificate request process. This method requires that the client has the ability to update their Domain Zone file with a CNAME record that references the certificate request. ACM uses this CNAME record to validate the certificate.

As long as the CNAME record remains intact, certificate renewal occurs automatically, eliminating the potential of the certificate expiring.

Email validation

Pega Cloud selects email validation during the certificate request process. ACM sends a validation email to a maximum of eight contacts described in this section. You must have access to one or more of these emails in order to validate the certificate. A client who prefers email validation must agree to following the terms of certification renewal, including the need to re-validate the certificate within 825 days. For more information, see the AWS document [How Domain Validation Works](#).

ACM sends email to the three contact addresses listed in the WHOIS directory and an optional five common system addresses for each domain that you specify. This means ACM sends up to eight email messages to registered and common contacts for every domain name and subject alternative name that you include in your request as shown below.

- Registered Contacts:
 - Domain registrant
 - Technical contact
 - Administrative contact
- Common Contacts:
 - administrator@your_domain_name
 - hostmaster@your_domain_name
 - postmaster@your_domain_name
 - webmaster@your_domain_name
 - admin@your_domain_name

Note: If your organization has turned on contact address privacy protection for your domain, email validation will fail. You must either disable privacy protection for your domain or use DNS validation in place of email validation.

- ⓘ For details, see the articles:

- Domain privacy ([wikipedia link](#))

- Enabling or disabling privacy protection for contact information for a domain

Outline and details of the certificate validation

Certificate validation requires that Pegasystems, Inc and clients coordinate their efforts throughout the process as described below.

1. The client makes a request by selecting [Create a ticket](#) in [My Support Portal](#). For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#). Clients must provide the following information in the support ticket:
 - Your custom domain name (for example, CreditCard.CustomerSite.com).

Note: Pega Cloud recommends the use of Fully Qualified Domain Names (FQDN) and does not recommend the use of wildcard domains.

- Each environment for which a client wants to generate a certificate requires listing the Pega URL. For example, if you wanted certificates for both your prod1 and stage environments, you must provide both the pega URLs and your requested certificate | domain for each. Your ticket must include the following details:

Note: The example urls in this article use the "pega.net" domain, which is applicable for Pega Cloud 3. Pega Cloud 2 urls use "pegacloud.net" instead of "pega.net". You can view your own urls in [My Pega Cloud](#).

- Production environment details:
 - Pega URL: <https://CreditCard-prod1.pega.net/prweb>
 - Requested Certificate | Domain: CreditCard.CustomerSite.com
- Staging environment details:

- Pega URL: <https://CreditCard-stg1.pega.net/prweb>
- Requested Certificate | Domain: CreditCard.CustomerSite-stg.com
- Your preferred certificate validation method, DNS or Email.
- Your deadline for completing this request.



Important: A client ticket cannot be processed without including a preferred validation method; when a client does not provide a preferred method, Pega Cloud contacts the client to confirm the certificate validation method before proceeding.

2. Pega Cloud operations processes the client ticket and generates a certificate request in ACM using the preferred validation method stated in the request:
 - For DNS Validations, Pega Cloud operations generates a DNS CNAME, attaches the record to your ticket, and then instructs the client on how to add the record to their domain zone file.
 - For Email Validations, ACM will send up to 8 emails to contacts listed in the domain registration. The client must respond to one of the emails within 72 hours.

After ACM validates the certificate request, either by looking up the new CNAME record or by you responding to the validation email, ACM generates the public certificate and private key. Pega Cloud operations then apply the public certificate and private key to the load balancers in your Pega Cloud environments.
3. Pega Cloud operations associates each validated SSL/TLS certificate with the appropriate environment. Pega Cloud operations leaves in place the Pega Cloud certificate so your previous URL (example, <https://CreditCard-prod1.pega.net/prweb>) continues to work without service interruption.
4. To resolve the new custom domain name, the client must add a CNAME record that points your custom domain name to the Pega Cloud services domain name. For example:

CreditCard.CustomerSite.com CNAME CreditCard-prod1.pega.net.

After your custom domain name is set up, you can still resolve the original URL of your system, such as <https://CreditCard-prod1.pega.net/prweb>. With your customer domain certificate and the Pega Cloud certificate in place, both URLs terminate SSL without any errors.

Certificate revocation

Clients can request the revocation of an ACM certificate that it has in service for one or more of their environments. It is important to note that the revocation process removes the certificate from their environment. If a new certificate is not applied for the custom domain, the custom URL no longer works.

The certificate revocation process requires that Pegasystems, Inc and clients coordinate their efforts throughout the process shown below.

1. The client files a ticket using the [Create a ticket](#) button the [My Support Portal](#) and provides the following information in the ticket:
 - New Certificate FQDN (only if the old certificate is to be replaced)
 - Certificate Common Name (FQDN) to be revoked.
 - Customer URL
2. Pega Cloud processes the client ticket to revoke the certificate which includes the following steps:
 - a. If a new certificate is to be applied, a new certificate request will be processed. Refer to requesting a new custom URL above.



CAUTION: If Pega Cloud does not apply a new certificate before the old certificate is revoked, the client site using the custom URL can no longer be accessed by your customers.

- b. Pega Cloud will remove the certificate to be revoked from all services to which it is applied.

- c. Pega Cloud will delete the certificate from ACM.
- d. Pega Cloud will notify the client using the ticket that process has been completed.

For immediate questions or additional information, call the contact listed in [Pega Support Contact Information](#) for your region.

Developing your application

As a Pega Cloud® services client, you do not need to worry about installing, patching, or updating Pega software. Pega Cloud services does it for you. After you receive your credentials and can log in, review the appropriate Pega application implementation guides in order to develop your applications, including any client-managed, post-installation steps that your application might require.

Pega Cloud services provisions your environment with your Pega software. You then must complete required implementation steps to customize the application for your business. Pega provides implementation guides that provide the detailed steps you must follow to complete your application development. Use the implementation guides for the applications that you have licensed. Review the [All Products](#), click on the link for each of your products, and then click the specific, required, application implementation guide.

Depending on which application you choose for your Pega Cloud services installation, you might need different implementation guides to complete your application development. For example, for Pega Customer Service™ for Healthcare, you must review the following guides:

- *CRM Implementation Guide*
- *Healthcare Foundation Implementation Guide*
- *Customer Service for Health Care Implementation Guide*

For Pega Customer Decision Hub versions 8.7 and later, see [Customer Decision Hub Implementation](#). For Pega Customer Decision Hub versions 8.6 and earlier, start with [Preparing your Customer Decision Hub application](#).

Certificate management practices for developing applications to run in Pega Cloud

Pega Cloud secures inbound interfaces in AWS deployment regions using Amazon ACM root Certificate Authorities (CAs). Modern operating systems and browsers use the Amazon Trust Services CAs by default; if you use an older software or your application is using a custom trust store or certificate store, you must add Amazon Trust Services CAs to ensure seamless connectivity to Pega Cloud.

Due to the dynamic nature of certificates used in Pega Cloud, Pega recommends that source systems and your applications that interact with Pega Cloud environments do not use certificate pinning. This policy aligns with Amazon and Google best practices.

Pega recommends that source systems and your applications that interact with Pega Cloud environments adopt the use of a common alternative to certificate pinning known as Certificate Transparency (CT). For details, see [How CT fits into the wider Web PKI ecosystem](#).

If your application uses certificate pinning to leaf or intermediate certificates, please update your application to pin to all Amazon root certificates or adopt CT practices by April 10, 2023. By doing this, you can avoid any service issues that can occur during an automated certificate renewal by Pega or AWS. This request aligns with the [AWS certificate manager best practices for certificate pinning](#); to review the latest certificates in use, review the Root CA Certificate Information section of [Amazon trust services Certification Authorities repository](#).

- [Preparing your Customer Decision Hub application](#)
- [Securing your application running in Pega Cloud](#)
- [Tracking your Pega project in Agile Studio](#)

- **Moving your application using Deployment Manager**
- **Establishing a prescriptive Route to Live**
- **Pega-provided support**

Preparing your Customer Decision Hub application

Note:

Follow these instructions when implementing Pega Customer Decision Hub™ (previously called Pega Marketing™) version 8.6 or earlier in your Pega Cloud® services environment.



If you are implementing Pega Customer Decision Hub version 8.7 or later, skip this procedure and follow the instructions in [Customer Decision Hub Implementation](#).

Before you create the Pega Customer Decision Hub implementation application in your Pega Cloud services Development environment, create a system architect operator with the privilege to run the First-time Setup Process.

Customer Decision Hub is a decision management-based solution for one-to-one customer engagement, which analyzes customer data in real-time and recommends next-best-action decisions for managing your customer interactions.

1. Log in to your Pega Cloud services Development environment as the `administrator@pega.com` operator.



Note: If you have not yet changed the default password, Pega Platform prompts you to change it.

2. In the header of Dev Studio, click **Create > Organization > Operator ID**.
3. In the **Operator ID** short description field, enter a description of the operator's role, for example, **System Architect**.
4. In the **Operator ID** field, enter a name for the operator, for example, **SystemArchitect**.
5. In the upper-right corner of the new record, click **Create and open**.
6. On the **Profile** tab, in the **Application Access** section, in the **Access Group** field, enter the appropriate access group:
 - For Pega Customer Decision Hub, enter **CDHTemplate:CDHInstall**.
 - For Pega Marketing, enter **MKTTemplate:MarketInstall**.



Note: Ensure that the default access group radio button is selected.

7. Click the **Work** tab.
8. In the **Routing** section, click **Update**.
9. In the **Update Organization Unit** dialog box, perform the following actions:
 - a. In the **Organization** field, enter the name of your organization.
 - b. In the **Division** and **Unit** fields, enter the names of the division and unit to which the system architect operator belongs.
10. Click **Submit**.
11. On the operator ID record, click the **Security** tab.
12. On the **Security** tab, select the **Allow rule check out** checkbox.
13. Click **Update password**, enter the new password, and then click **Submit**.
14. In the upper-right corner of the operator ID record, click **Save**.
15. In the lower-left corner, click the user icon, and then select **Log off** to log out of Dev Studio.

What to do next:

Create your Pega Customer Decision Hub implementation application.

1. Log in to your Development environment as the system architect operator that you created above.
2. Follow the steps of the First-time Setup Process wizard.



Note: If you did not designate your Organization in the previous task, Pega Platform prompts you to enter it.

3. After you create your implementation application, review [Customer Decision Hub Implementation](#) for any additional implementation steps that you need to take to complete the development of your application for your business needs.

Securing your application running in Pega Cloud

Secure your application by creating the organization and user structures to limit access to your application. Configure groups and roles and create operator IDs for users who can perform tasks by using your application, based on their access, group, and role.

For more information about security at the infrastructure level of Pega Cloud®, see [Security and data protection](#).

See [Security Checklist when deploying on Pega Cloud](#), which summarizes the different features that you use to configure user access and secure your application.

Tracking your Pega project in Agile Studio

As you develop your application, track your Pega projects using Pega Agile Studio.

Agile Studio helps you implement an iterative and adaptable approach that delivers results in significant innovative and competitive business benefits, including:

- Managing changing priorities
- Expediting time-to-market

- Increasing productivity
- Enhancing software quality

Your application teams and your stakeholders can use Agile Studio to complete projects using the best practice methodology. Agile Studio integrates with Dev Studio in Pega Platform for traceability between your developer environment and your project management system. For more information about how Agile Studio can help you, see [Agile goes mainstream](#).

Agile Studio is one of the Pega-provided tools included in Pega Cloud®.

By using Agile Studio, your clients can focus on the following core pillars of effective project management:

- **Planning** their software development and product needs over their software release lifecycles.
- **Managing** their teams, backlogs, and technical debt to ensure that they deliver their releases effectively.
- **Completing** planned work by enabling their teams to complete their assigned release-driven work so they can track their work using the same tool in which they plan work.

Logging into Agile Studio

Pega Cloud clients can login to Agile Studio using your credential file which supports two separate logins:

Application URL: <https://abc-ccard-agilestudio.pegacloud.net/prweb>

AgileStudio Username: AgileStudioSysAdmin password: *****

Username: administrator@pega.com password: *****

Use your SysAdmin login username and password for implementation tasks, as described in the [Pega Agile Studio Implementation Guide](#). This Guide provides system administrators with detailed instructions about how to perform post-installation setup and configuration tasks that should be completed before users begin working in the Agile Studio application.

Perform the connection setup tasks in your development system; you must repeat the setup process in each development system where you are planning to track and monitor project work. In the [Setting up a connection to a development system](#), you will use the `administrator@pega.com` login username and password.

The [Pega Agile Studio 8.7 User Guide](#) helps you become familiar with commonly used features that support creating and managing Scrum projects in your organization.

Moving your application using Deployment Manager

To integrate your application with a DevOps pipeline, use Deployment Manager to help you promote changes to your Pega Platform™ application across your various Pega Cloud® services environments.

Do not make these types of changes to your applications in a production or live environment that your customers are using. Instead, create and then test your changes in a development environment. A standard Pega Cloud installation typically includes the following environments:

- Development and Testing environment (*dev/test*)
- Staging environment for user testing
- Production environment

After you complete your change validation testing in your DevTest and Staging environments, use your pipeline to push the changes into your production environment.

Deployment Manager

Simplify DevOps tasks in your Pega Cloud environments by using Deployment Manager. It is a simple, ready-to-use Pega application that offers you built-in DevOps features. It uses the Pegasystems case management technology to manage an automated orchestration engine, enabling you to efficiently build and run your CICD pipelines. For an overview of using Deployment Manager for Pega Cloud services, [Deployment Manager overview](#).

You might have a robust DevOps program already established in your company. You also might use tools, such as Jenkins or Bamboo. You can use those products with Deployment Manager. In addition, you can use Deployment Manager to run deployments of your application updates or other changes with a single click, without the need for third-party automation services, such as Jenkins or Bamboo. As part of near-zero downtime upgrades, fully automated pipelines help significantly reduce the lead time to deliver value to end users.

If your subscription includes Deployment Manager, your *welcome* email contains the URL for your Deployment Manager *orchestration* environment and your administrator credentials to access your *devops* environment. Follow the instructions in [Getting started with Deployment Manager](#).

Note: For a prescriptive, Pega-recommended approach for managing your

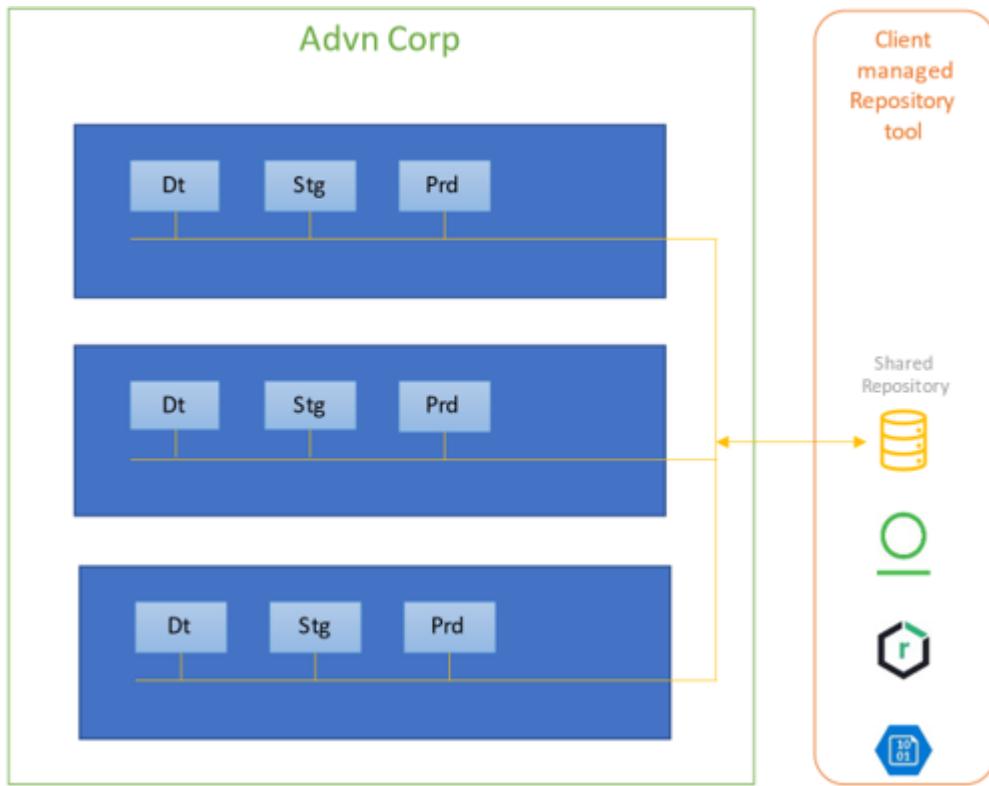
- ⓘ Pega application releases using Deployment Manager pipelines, see [The prescriptive application release Life Cycle](#).

Note: For an overview of the requirement for establishing prescriptive Routes

- ⓘ to Live (RTL) for your Pega applications deployed in Pega Cloud, see [Establishing a prescriptive Route to Live](#).

Deploy Pega Platform applications across Virtual Private Cloud or regions

You can use Deployment Manager to deploy Pega Platform applications across Virtual Private Cloud (VPC) or regions by configuring a shared repository that you own, as shown in the following figure:



Example of how an organization can share Pega Platform applications across VPC or regions

When using a shared repository, use the following best practices:

- Select a Pega-supported repository that your organization shares across regions. If you have a repository solution that is not Pega supported, you can adopt it for your Pega application by creating a custom repository. For more information, see [Creating a custom repository](#).

- Test the connectivity from each environment across region or VPC.

Establishing a prescriptive Route to Live

Learn how to either introduce or reinforce the requirement for establishing prescriptive Routes to Live (RTL) for your Pega applications that are deployed in Pega Cloud® services. RTLs are efficient, easily upgradable, and allow for continuous improvement.

Create RTLs from an environmental view to help you ensure that you use your Pega Cloud assets effectively, which lowers costs and improves delivery results. You can also find answers to the most common questions and concerns about how to align your software development life cycle (SDLC) with recommended best practices for development, as well as about the existing demarcation points with which you can separate several RTLs.

For more information on how best to make use of Pega Platform™ and Deployment Manager together, see [The prescriptive application release Life Cycle](#).

Introduction to Route to Live

An RTL is an industry-standard DevOps pipeline with which you can continuously evolve your work across multiple environments running an application in various stages of development. In practice, an RTL helps you to deliver work rapidly, iterate code more frequently, and verify that the choices you make to establish your solution life cycle meet business needs and deliver high-quality results. Pega recommends organizing delivery of application enhancements around the concept of RTLs that include a packaged set of services that align to the functions and stages used to deploy new applications and continuously improve existing ones.

The most common stages of an application life cycle are listed below, but not all elements of the life cycle are used consistently:

Development

The technical configuration of a Pega application using Dev, App Studio, or Prediction Studio to build integrations, create case workflows, control adaptive models, or to continuously improve existing solutions.

Quality assurance

The testing stage of a Pega application, validating and testing scenarios, integrations, and unit testing.

Integration testing

End-to-end testing of a Pega solution that can be composed of many sub-systems. The main objective of integration testing is to ensure that all dependencies are functioning properly.

User acceptance testing

A test stage focused on ensuring that actual users of the software can handle day-to-day tasks under real-world scenarios according to a defined specification.

Training

Users of the systems can be made aware of changes to the solution that impact usability before they impact productivity.

Performance Testing

A testing stage that validates that the end-to-end solution can support the full workload, without undue delays.

Productive (Production)

When a solution is live and servicing production users and workloads.

Business Operations (specific to Pega Customer Decision Hub deployments)

An Pega-required environment in CDH pipelines which Pega provides to support functional simulation testing against your most recent engagements, their activity history, and their analytical model.

Service Definition

The functional elements of the service life cycle defined above are performed within the following environment types, as defined by Pega Cloud:

Standard sandbox

A general-purpose sandbox that supports development, functional and unit testing, user acceptance testing, and pre-production staging.

Large sandbox

A general-purpose sandbox that supports development, functional and unit testing, training, user acceptance testing, and pre-production staging.

Production mirror environment

An environment that is scaled to support application performance testing up to the volume of the Production Environment service.

Production environment

The Pega Cloud production environment is a scaled production deployment of licensed Pega Platform and applications.

Business operations environment

The business operations environment supports functional simulation testing of decisioning applications, in batches, in contractually defined windows.

- [Best practices for RTL deployment](#)
- [Route to Live FAQ](#)

Best practices for RTL deployment

Learn about best practices when implementing some of the most common and recommended RTLs for the core Pega Cloud® services product offerings.

The figures in this topic are labelled with the following definitions:

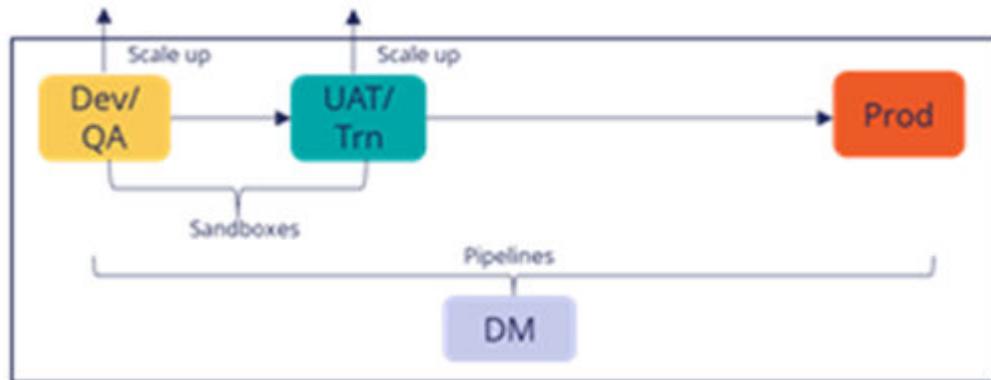
- Dev = Development
- QA = Quality Assurance
- UAT = User Acceptance Testing
- Trn = Training
- PM = Production Mirror (performance testing)
- Prod = Production
- DM = Deployment Manager

General best practices

- A single Pega Customer Service application RTL can support multiple applications and versions, and you can create an application release life cycle to supports this.

For more information on how best to make use of Pega Platform and Deployment Manager together, see [The prescriptive application release Life Cycle](#).

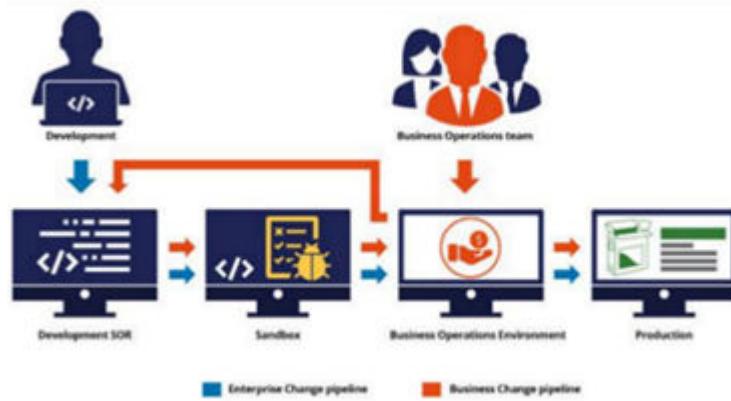
- A production environment within your RTL must always have an accompanying staging environment. This means that for a given RTL, as shown in the following example, there must always exist a staging stage environment (UAT/Trn).



Staged environments within an RTL pipeline include a staging environment

- Application(s) that are deployed in your staging environment must match the application(s) that are deployed in production. Pega Cloud services infrastructure and software updates rely on the staging environment to be representative of production to ensure that the Pega Cloud update validation process works correctly. Deviations from this will invalidate Pega Cloud validation testing.
- When you use Pega solutions for multiple separate business applications, such as Pega Customer Service™ application and Pega Customer Decision Hub™, Pega recommends having a distinct RTL for each application where you apply Pega technology.
- All applications deployed within the same RTL share the same Pega-managed update and change management process.

- All applications deployed within the same RTL will have the same Pega Cloud maintenance windows and patch policy.
- Reusability of application components is strongly recommended by Pega. As a rule of thumb, when applications share common components, they should exist within the same RTL. This is because including shared assets and dependencies can be difficult if applications do not share the same RTL.
- A single Pega Customer Service application must be developed within a single development environment and cannot be spread across multiple development environments. Pega Cloud services supports accommodating large developer communities within a single development environment.
- A Pega Customer Decision Hub can have two entry points for development. A development environment for technical changes that involves the development system of record (SOR), and a business operations environment (BOE) for business operator changes.
- All changes within a Pega Customer Decision Hub application must be merged within a common development environment as shown in the following example:



Merging changes within a common environment

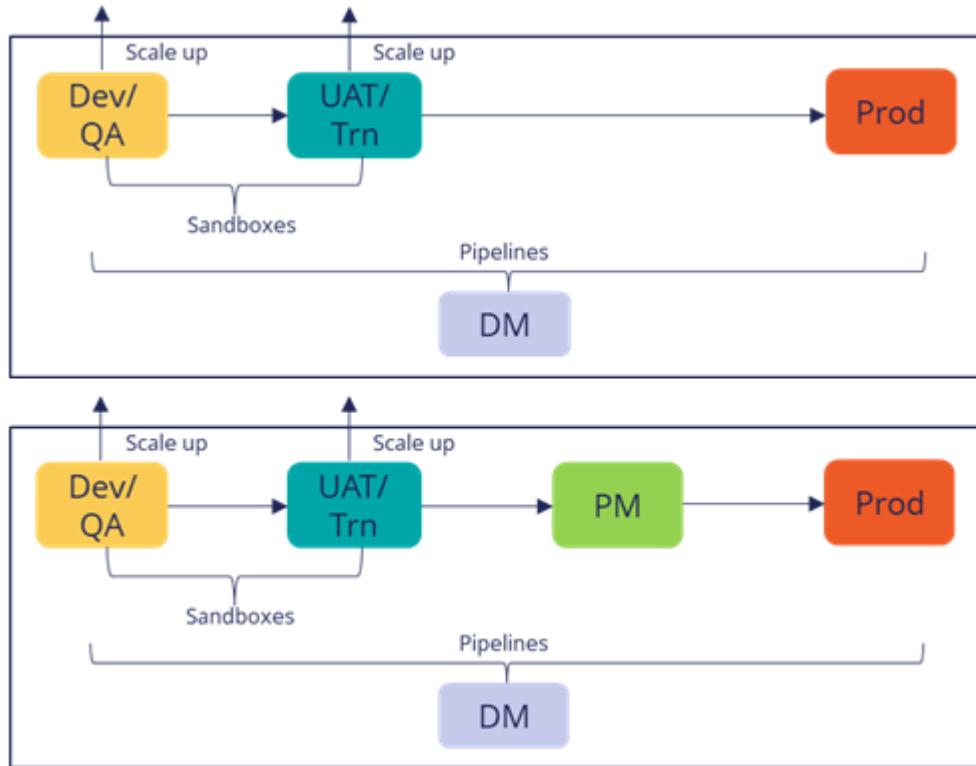
- Deployment Manager is the only recommended approach for deploying and managing the development life cycle of solutions deployed on Pega Cloud.
- A single RTL will store all data that is created from, or stored when executing the application, within the region(s) where it is deployed.

- Pega Customer Decision Hub RTLs can only contain one application.
- Pega Customer Decision Hub use cases that span lines of business, but operate against the same customer base, should be done within a single RTL. This ensures that it is able to view all data elements of the customer engagement.
- Decisioning use cases where the lines of business do not overlap, and have very different customers, should operate within different RTLs. For example, a business-to-business application versus a business-to-consumer application.

RTLs for Pega Customer Service application and Pega Platform, Pega Robotic Automation, and Pega Workforce Intelligence

A typical Pega Customer Service application or Pega Platform, Pega Robotic Automation, and Pega Workforce Intelligence RTL has functional roles like UAT and Training that can share an environment, resources can be scaled to support additional demands, and deployment orchestration that is managed exclusively by Deployment Manager (DM).

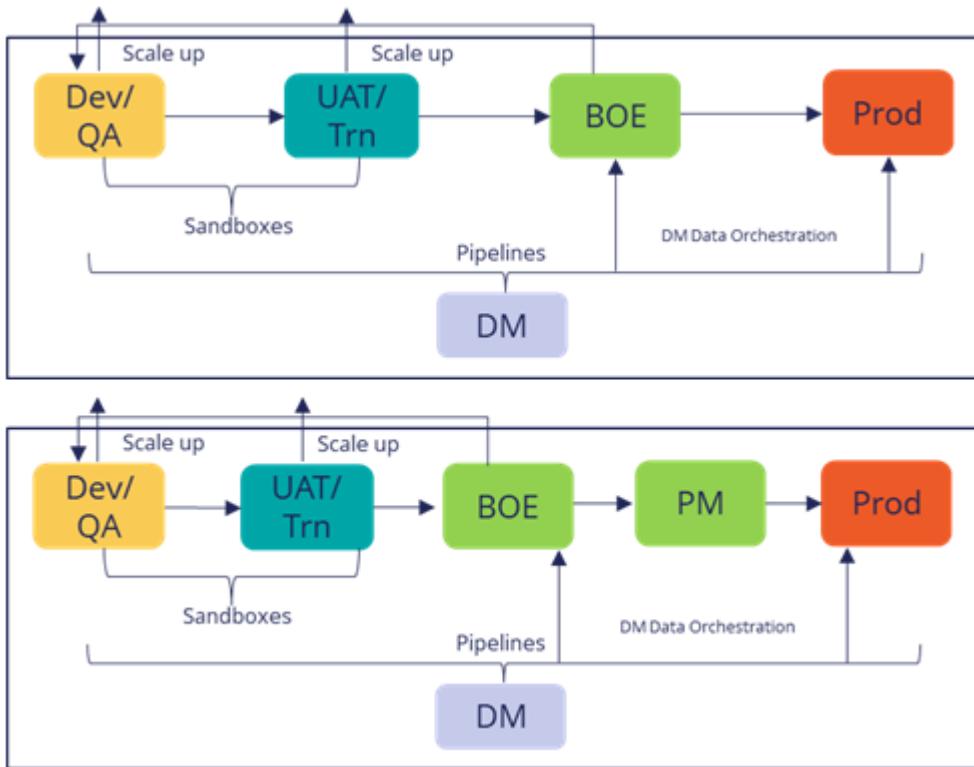
The primary difference between the Pega Customer Service application or Pega Platform, Pega Robotic Automation, and Pega Workforce Intelligence RTL is that the Pega Customer Service application RTL includes a PM environment, which you use for scaled performance testing, as shown in the following figure:



Pega Platform, Pega Robotic Automation, and Pega Workforce Intelligence and Pega Customer Service *RTL*

RTLs for Pega Customer Decision Hub

A typical 1:1 Customer Engagement or Pega Customer Decision Hub RTL will look like one of the following figures. While the Pega Customer Decision Hub RTL is very similar to the RTLS mentioned previously, it includes a specific Business Operation Environment (BOE) type that is only used by Pega Customer Decision Hub solutions and is used for certain personas to commit changes.



Pega Customer Decision Hub *RTL*

Route to Live FAQ

Review the following frequently asked questions to learn more about Route to Live for Pega Cloud services:

When does Pega recommend that all Pega Platform™, Pega Robotic Process Automation™, Pega Workforce Intelligence™, Pega Customer Service™, and Pega Sales Automation applications reside within a single RTL?

Based on the best practices illustrated previously, if you answer yes to the following statements then your applications are recommended to follow a single RTL:

- Data does not need to reside in multiple different regions because of data sovereignty or other regulatory or compliance requirements.

- The lines of business that these applications service can operate under a single update timeline and policy.
- Decisioning applications span multiple lines of business but interact with the same customer base.
- The lines of business that these applications service can operate under a single patch and maintenance timeline and policy.
- These applications share common application layers and frameworks.
- These applications do not have a similar mission critical profile; those applications living in a single RTL should not all be 24x7, high volume, mission critical workloads.

When does Pega recommend that Pega Platform, Pega Robotic Automation, Pega Workforce Intelligence, or Pega Customer Service applications be deployed in separate RTLs?

Pega can provide guidance based on best practices defined previously. If you answer yes to the following statements, then your applications are recommended to follow the separate RTL process:

- Applications servicing a global user base, impacted by data sovereignty or other regulatory and compliance requirements that require that data cannot be moved from the data subjects' region into a single region of operation.
- The lines of business that these applications service cannot adhere to a single update timeline and policy because it would create unmanageable prioritization and coordination among disparate teams.
- The lines of business that these applications service cannot operate under a single patch and maintenance timeline and policy because it would create unmanageable prioritization and coordination among disparate teams.
- These applications have a similar mission critical profile: the workloads are similarly operated, such as when usage is 24x7, there is high volume of processing, and it is a mission critical application.

When does Pega recommend that Pega Customer Decision Hub™ applications be deployed in separate RTLs?

1:1 CE solutions that target a materially different customer base, for example B2B vs B2C. Or more specifically when the benefit of operating off a single data set and evaluating across different lines of business for the same customer base provides no benefit.

When does Pega recommend Pega Customer Decision Hub applications be deployed in a common Route to Live?

All applications target a similar customer base. Critical to this thought process is, if there is benefit to your strategies to have a centralized brain evaluating all interactions, you should deploy with a single RTL.

Does Pega recommend including Pega Customer Decision Hub and Pega Customer Service application or Pega Platform, Pega Robotic Automation, and Pega Workforce Intelligence in the same RTL?

No, Pega recommends that these exist in isolated RTLs.

When Pega performs updates, will all applications within a single RTL be updated in the same workflow?

Yes

When Pega performs maintenance, such as patches or infrastructure updates, will all applications within a single RTL receive these changes in the same workflow?

Yes

Can a single community of developers working on the same application span multiple development sandboxes?

No. Pega does not recommend or support application development spanning multiple environments due to synchronization requirements.

Do I have to ensure that my “staging” sandbox contains an identical set of applications to those running in production?

Yes. The update process and testing strategies rely on a staging environment that matches production.

Can a single RTL support multiple intelligent automation applications and versions?

Yes! And in fact, it is common place. The prescriptive RTL content provides details on the ways to achieve this with native Pega capabilities.

How many applications can I create in a single Pega Customer Decision Hub?

One.

I do performance testing on every major release. What do I need so I can accomplish this?

Pega provides an RTL with a production mirror (PM) environment. PM environments are scaled to support production level volume testing.

Pega-provided support

The Pega Global Client Support (GCS) team provides support for both Pega Cloud® and your Pega applications. GCS keeps your Pega Cloud environments running effectively.

For information about GCS and the services provided, see [How to Get Support](#).

In addition, see the following resources for information about using Pegasystems and Pega Cloud products:

- See [Learning about Pega Cloud services](#) to learn about Pega Cloud features and functionality, including how-to information.
- You can find answers to specific questions that you might have about Pega Platform™, Pega Cloud, and other products. For details, see [Pega Support Center](#).
- [Pega Academy](#) offers courses to provide best practices for Pegasystems products.

My Pega Cloud

You can manage Pega Cloud environments from the [My Support Portal](#). For example:

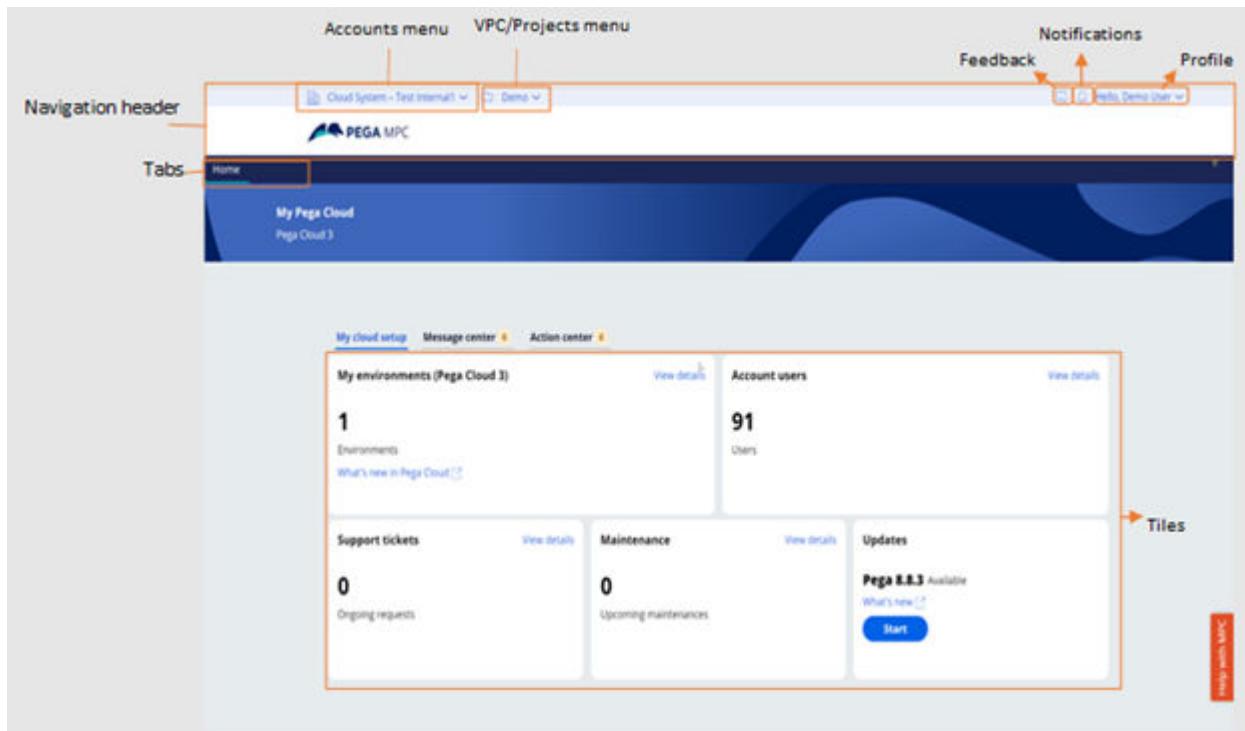
- Restart your dev/test and staging environments
- Stream or download log files
- View high-level details about the environment
- Perform required actions during an update journey

For more information about these tasks, see [Administering your Pega Cloud service](#).

Exploring My Pega Cloud portal

Familiarize yourself with the My Pega Cloud portal home page and its layout to get yourself started working in the portal.

After you log into [My Pega Cloud portal](#), the home page screen offers self-service features to help you work with the portal. The following figure shows the main features of the home page:



My Pega Cloud portal home page layout

Item	Gives you access to:
Navigation header bar	<ul style="list-style-type: none"> Your accounts and environments. You can choose a combination of an Account and a Project/VPC*. The Home page changes to reflect your selections. You can then access the tiles there, as well as the other non-environment specific options. Quick Menu with access options for the various areas of the portal, such as: <ul style="list-style-type: none"> Feedback Notifications User Profile and log off
Portal locations tab bar	Access to that area of the portal.

Item	Gives you access to:
My cloud setup	Shows tiles that provide information on different functional areas of the selected Account and Project/VPC.
Actions & Messages banner	Access to the Actions & Messages Centers, where you perform required actions for self-service and upgrades.
Feedback & Notifications	Give feedback about your portal experience or view notifications.
Help with MPC	Links to the MPC FAQ page. This button is visible on all screens.
Profile	Provides options to view user profile, modify default Account or Project/VPC, adjust time zone, and log off.
Tiles	At-a-glance information and access to manage the functional areas of your environment.

To continue learning about My Pega Cloud, read the documentation in the [Administering your Pega Cloud service](#) section.

*Projects are applicable to Pega Cloud 3. VPCs are applicable to Pega Cloud 2.

- [Configuring your portal preferences](#)
- [Review My Pega Cloud portal self-service tile functionality](#)

Configuring your portal preferences

When you first log in to the My Pega Cloud portal, you select the cloud account details that you want to associate with your portal experience. Your selections define the default preferences for your portal home screen and determine what you see each time you log on.

The portal settings you can specify include:

- Your account containing the Projects or virtual private clouds (VPCs) that you want to manage.

- Projects/VPCs containing the environments you want to manage.

To update your default preferences, select the User profile icon, select Profile, and then click Edit in the **Account Preferences** section. Update the following preferences:

- Set the Default Account and Project/VPC using the pull-downs to choose which values you want as your default.
- Set your timezone that applies to all dates and times in the My Pega Cloud portal.

Review My Pega Cloud portal self-service tile functionality

In your My Pega Cloud portal, you can access the most common self-service tasks through the home page. The header there provides you with self-service options and the tiles provide at-a-glance information, as well as access to manage those functional areas of your environment.

Prerequisites

Before you can use the portal, you must have completed the prerequisites in [Administering your Pega Cloud service](#).

Navigating the My Pega Cloud portal tiles

Use the functional tiles to navigate to the self-services task you want to perform by clicking **View details** in the tile.

Item	Description
My cloud setup tile	<ul style="list-style-type: none"> • Access all your Pega Cloud services environments. • Download a Pega Cloud log bundle. <p>For more information, see Downloading log files for troubleshooting.</p>

Item	Description
	<ul style="list-style-type: none"> Restart all of the tiers or just a specific tier. <p>For more information, Environment restarts.</p> <ul style="list-style-type: none"> Wake up your hibernated environment. <p>For more information, see Managing hibernated environments.</p> <ul style="list-style-type: none"> Monitor your environment in PDC. <p>For more information, see Monitoring your application using Pega Predictive Diagnostic Cloud.</p> <ul style="list-style-type: none"> View the activity logs for self-service actions on your Pega Cloud environments.
Account users tile	View users in of all your environments, their cloud-specific roles, and their email addresses that have been granted access by using My Pega Cloud portal .
Support requests tile	<p>View the support requests that are submitted for this account, and make additional support requests.</p> <p>For the latest documentation about making requests, see Requesting support services.</p>
Maintenance tile	<p>View upcoming and completed maintenance activities for your environments.</p> <p>My Pega Cloud maintenance activities include the following standard and emergency maintenance types:</p> <ul style="list-style-type: none"> Patches Hotfixes

Item	Description
	<ul style="list-style-type: none"> • Database updates • Pega Infinity™ updates
Updates tile	Complete requested actions for your Pega software update process.

Navigating to other self-service functions

Click the icons in the Home page navigation header to display these other functions.

Item	Description
Action and Message Centers	View messages about actions on your environments that were performed or are to be performed by you or the system.
Feedback and Notifications	Give feedback about your portal experience or view notifications about actions you've taken on your environment.

Using Predictive Diagnostic Cloud

Your My Pega Cloud portal provides you with the option to use Pega Predictive Diagnostic Cloud (PDC), a performance management service that can support your management and development teams. PDC can help you monitor your Pega application performance and notify you when system health issues occur, so you can address issues quickly.

PDC monitors your system stability, throughput, and responsiveness. When you use PDC for monitoring, your Pega applications send data to it. PDC collects the data and presents it in a way that helps you identify performance issues and decide how to improve your system.

For the PDC documentation set, see [Pega Diagnostic Center](#).

Accessing your instance of Pega Predictive Diagnostic Cloud

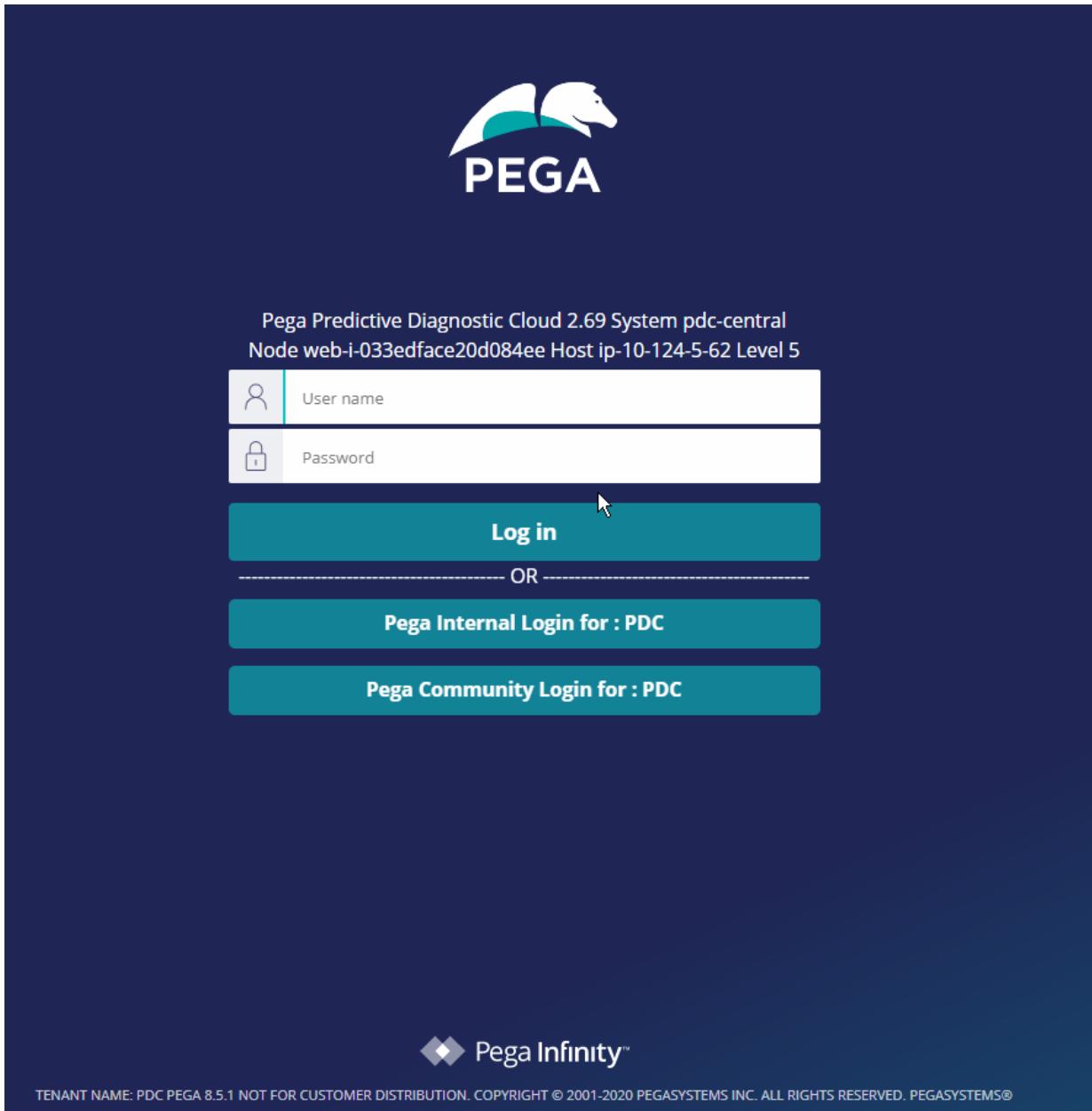
When you use Pega Predictive Diagnostic Cloud (PDC) for monitoring, you have visibility into the health and performance of your Pega applications.

PDC is not just a tool for clients. Pega Cloud® also uses PDC to monitor stability, throughput, and responsiveness for all our client environments, and to help Pega Cloud clients diagnose any reported issues.

Pega Cloud environment provisioning automatically connects your environments to PDC, so you can log on, immediately explore the tool, and set up your notifications.

Pega Cloud clients can access the PDC interface for any environment which your credentials provide access from the My Pega Cloud portal.

1. Log in to your [My Pega Cloud](#) portal.
2. In the **My cloud setup** tile, click View Details.
3. In the **Environments** section, click the environment name.
4. In the Environment Details tab, click Monitor on PDC.
5. On the PDC login view for the environment, enter your credentials.



How Pega maintains your Pega Cloud service

Pega Cloud ensures that you have access to the latest features and capabilities of Pega Platform™ and your Pega applications by performing periodic system maintenance on your Pega Cloud environments. Use the information linked to below to learn more.

- [What's new in Pega Cloud](#)
- [How Pega keeps your Pega Cloud service current](#)
- [Process to update to Pega Cloud 3](#)

What's new in Pega Cloud

Learn about the latest security updates, new features, performance improvements, and supportability enhancements delivered in the latest Pega Cloud® infrastructure updates.

For more information, see Pega Cloud maintenance and types of system updates.

- Review the latest important security updates that Pega automatically applies to Pega Cloud. For more information, see [Security Bulletins](#).
- Review the latest Pega Platform™ and CRM patches. For more information, see [Pega Platform Resolved Issues](#) and [Patches for Pega software](#).
- Maximize your Pega software investment by using the newest Pega Platform version. For more information, see [What's New in Pega Platform](#).

Review the significant, client-oriented enhancements in the Pega Cloud infrastructure update that is applicable to your infrastructure deployment version:

- [Pega Cloud 3 enhancements](#)

- Pega Cloud 2 enhancements

Pega Cloud 3 enhancements

Review the Pega Cloud® 3 continuous infrastructure updates that include critical security fixes and the following significant, client-oriented enhancements.

Q4 2023 enhancements

Pega Cloud New Region Announcement

Pega Cloud 3 is now available in four new regions.

- AWS: Jakarta, Indonesia (ap-southeast-3)
- AWS: Zurich, Switzerland (eu-central-2)
- AWS: Seoul, South Korea (ap-northeast-2)
- GCP: Netherlands

For more information on Pega Cloud deployment regions, see [Deployment regions for Pega Cloud](#).

Update from Cloud 2 to Cloud 3

During the [update to Pega Cloud 3](#), My Pega Cloud will display the audit history of update approval and responses provided for the network configurations questionnaire for Major Infrastructure Update. Clients will be able to export their DNS records to an excel file to prevent errors in copy and paste operations.

The screenshot shows a 'Network config...' section under 'Home'. It displays a message about network configurations approved for a major infrastructure update, a note about adding Pega IP addresses to the allow-list, and a confirmation message about adding Pega provided IPs to the allow-list. Below this, there is a table titled 'Please confirm that you have completed the certificate validation process for any environments with custom domain names'. The table has columns for Domain name, Record name, Record type, Record value, and Status. It shows two entries for an environment named 'selfservice-dev': one CNAME record with value '_a7704b8c' and status 'ISSUED', and another CNAME record with value '_7adc1176' and status 'ISSUED'. A note at the bottom states 'We have created the DNS record on our side'.

Logging Enhancements

Clients can request log type exclusion in [Streaming Pega logs](#) to an external Amazon S3 bucket, thus reducing their data storage and transit costs.

Deployment Manager Enhancements

Added support for cross-region deployments for their Pega applications with Deployment Manager v6.3 on Pega Cloud 3.

Users can define the Applications and components that are reusable; each reusable application will have its own CD pipeline that will validate and certify builds. Only the certified versions (production-ready) will be available to other RTLs in the same or different region.

The screenshot shows the 'Shared applications' section of the Pega Cloud interface. At the top, there's a header with a back arrow, the title 'Shared applications', and a save button. Below the header, a note says 'Enlists the applications that are reused by other applications built on it. Specifying an application here, will ensure the production ready artifacts are available for other Route to lives.' Under the heading 'Application name', there are four rows of application entries, each with a delete icon. A blue '+ Add' button is located below this section. The next section is titled 'Application artifact audit' with tabs for 'Published' (selected) and 'Available'. It includes a navigation bar with links 1 through 10 and 'Next'. A table follows, with columns: Application name, Version, Pipeline, Deployment, Artifact path, and Status. The status column contains green 'SUCCESS' icons for most rows, except for the last one which has a red 'FAILED' icon.

My Pega Cloud

Pega Cloud 3 clients can [reschedule Pega performed proactive maintenance](#) such as Infinity patches and hot-fixes and database updates without calling support. Maintenance cannot be rescheduled within 6 hours of the scheduled maintenance time. A single maintenance task can be rescheduled up to three times.

The screenshot shows the 'Upcoming maintenance tasks' page. On the left, there's a sidebar with sections for 'Maintenance type' (Pega Infinity patch, Database update, Pega Infinity patch, Pega Infinity patch, Pega Infinity patch, Pega Infinity patch), 'Environment' (Production, Test), and 'Completed maintenance tasks'. The main area lists maintenance tasks with columns: Maintenance type, Environment type, Ticket ID, Pega version, and Start time. One task is highlighted. A modal window titled 'Reschedule Task' is open over the list. It contains fields for 'Pega Infinity patch -' (with a dropdown menu showing 'Select...'), 'Available start times' (a dropdown menu with options like '10/12/23 3:00 AM', '10/12/23 7:15 AM', '10/12/23 7:15 AM', '10/12/23 7:15 AM', '10/12/23 7:15 AM'), 'Reason for rescheduling' (a text input field with placeholder 'Reason for rescheduling'), and a note stating 'Times are shown in the default time zone of the system if a time zone is not set in your Profile'. At the bottom of the modal are 'Cancel' and 'Submit' buttons.

Pega Cloud 3 clients can view the pool of static source IP addresses from My Pega Cloud to connect to their enterprise network. For more details see, [Environment connectivity overview](#).

Environment connectivity overview

Pega cloud offers a secure, flexible, and scalable way to integrate with your enterprise network, including connections that originate from a pool of static source IP addresses to connect to your enterprise network. All system instances in Pega Cloud share from this pool of static source IP addresses.

[Environment connectivity overview doc](#)

[Get pool of static IPs](#)

Q3 2023 enhancements

GenAI

GenAI is now available to clients on Pega Cloud 3. For more information, see [Enabling Pega GenAI in Pega Cloud](#). We also enabled GenAI for Partners on PegaLabs.

Update from Cloud 2 to Cloud 3

We have implemented new automation tools to streamline the update from Cloud 2 to Cloud 3. For more information about the update process, see [Process to update to Pega Cloud 3](#).

Logging Enhancements

[Splunk log streaming](#) now allows clients to stream logs over the public internet or internal to AWS via VPC-to-VPC communication.

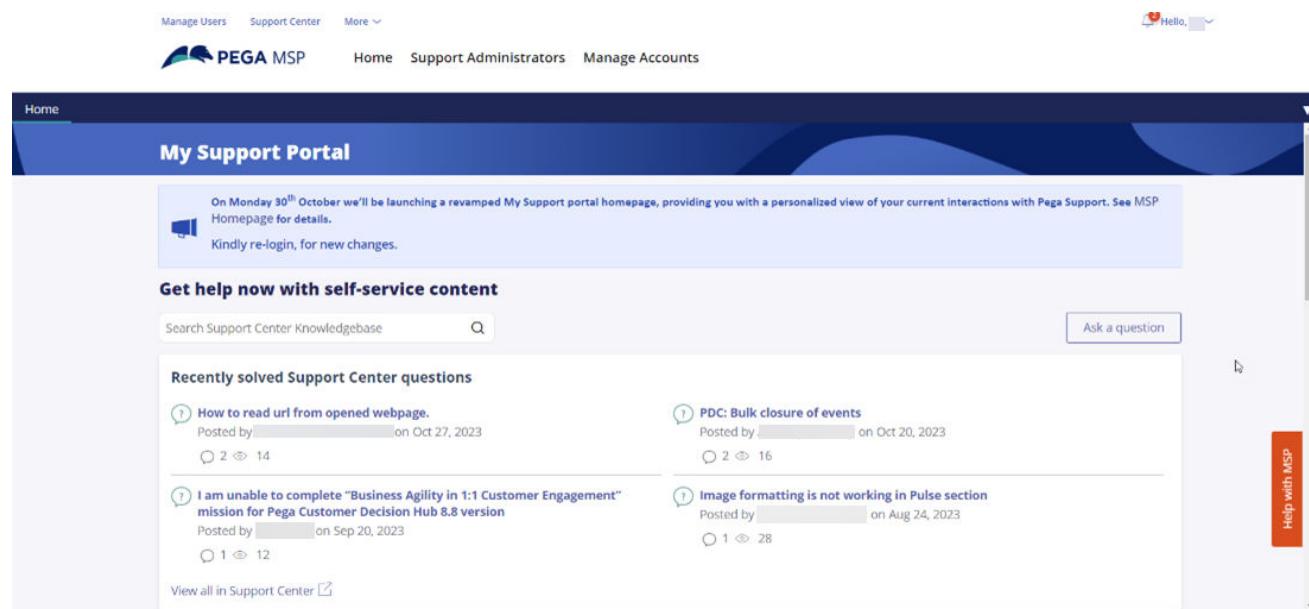
Pega Cloud on Google Cloud Platform (GCP)

Pega Cloud 3 on GCP supports the Milan region. See the full list of supported regions at [Deployment regions for Pega Cloud](#).

We also improved Recovery Point Objective (RPO). Client deployments in GCP now have a Recovery Point Objective (RPO) of less than 10 minutes, ensuring protection against data loss. For more information, see [Data backup, data-restoration, and data durability for Pega Cloud](#).

My Support Portal Enhancements

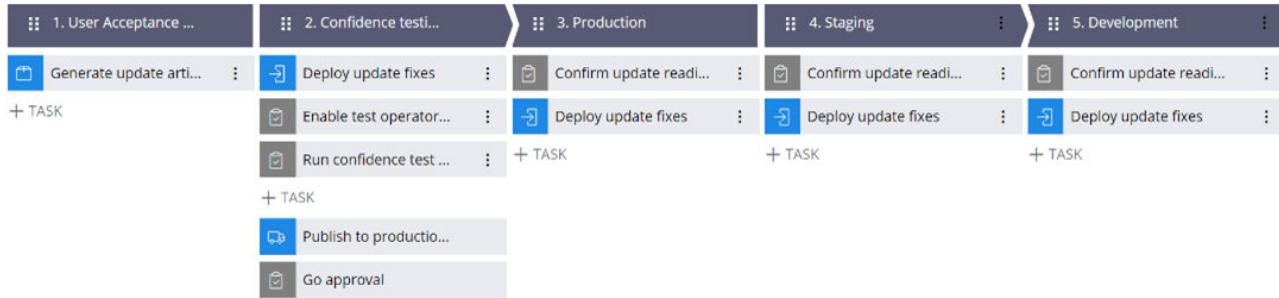
We released a new MSP home page design that will encourage the usage of Support Center resources before ticket submission, display open cases in a more streamlined layout, draw attention to proactive incidents created by Pega to avoid ticket duplication, and provide quick links to Pega Diagnostic Center and to My Pega Cloud. Also, clients will now receive a notification when they have reached 75% of their entitlement for their Relational Database Service (RDS) storage and again at 90%.



The screenshot shows the My Support Portal homepage. At the top, there's a banner with the text: "On Monday 30th October we'll be launching a revamped My Support portal homepage, providing you with a personalized view of your current interactions with Pega Support. See MSP Homepage for details. Kindly re-login, for new changes." Below the banner, there's a search bar labeled "Search Support Center Knowledgebase" and a button "Ask a question". The main content area is titled "Get help now with self-service content" and features a section for "Recently solved Support Center questions". It lists four questions with their respective details (posted by, date, and interaction counts). A red vertical bar on the right is labeled "Help with MSP".

Deployment Manager Enhancements

Deployment Manager v6 on Pega Cloud 3 enables users to manage the basic update process of a Pega Infinity minor version update. For more information, see [Working with update pipelines](#).



Users can [Run tasks on an environment](#) to move the assets required to complete the UAT phase during a Pega Infinity minor version update.

DEPLOYMENT MANAGER

Account: [redacted] Project: [redacted] 672 ⓘ

← Environment : Development

Environment ID	Environment template
Environment type	Development
DevTest	Last ping time
	Jul 3, 2023 3:28:45 AM
	production level
	2

Actions ▾

- Package product
- Deploy artifact**

Action history

Action	Created by	Started on	Completed on	Status	View details
Deploy artifact	[redacted]	Jun 30, 2023 3:21:34 AM	Jun 30, 2023 3:22:23 AM	SUCCESS	View details
Deploy artifact	[redacted]	Jun 30, 2023 2:00:23 AM	Jun 30, 2023 2:05:23 AM	FAILED	View details
Deploy artifact	[redacted]	Jun 30, 2023 1:57:13 AM	Jun 30, 2023 2:05:22 AM	FAILED	View details
Deploy artifact	[redacted]	Jun 30, 2023 1:50:37 AM	Jun 30, 2023 1:55:22 AM	FAILED	View details
Deploy artifact	[redacted]	Jun 27, 2023 9:10:13 AM	Jun 27, 2023 9:10:19 AM	FAILED	View details

Deployment Manager supports fixed inputs on pipelines to avoid manual interactions during deployment. With this feature, clients can process tasks based on the key information users provide during the deployment. For example, a user can provide a list of Jira IDs that will enable clients to pulse the deployment information to the specified Jira conversation.

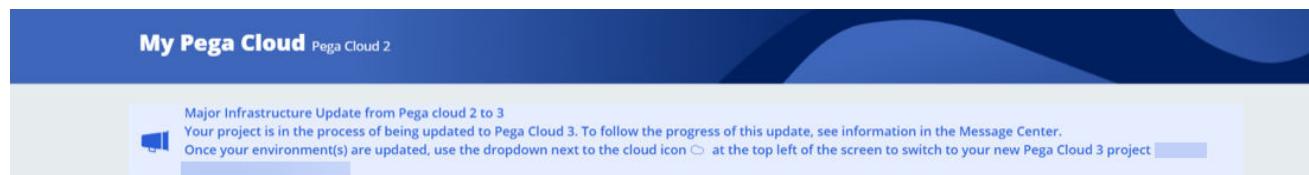
The automation to move Deployment Manager 5.x clients who use out of the box capabilities with no customizations to version 6.x is now available.

Pega Diagnostic Center enhancements

The home page now displays a unified view, with links to recent release notes, PDC training, and the Support Center along with the overview of systems. We also introduced consistency in UI display for events opened from the Reports page, notification emails, or from the Event Viewer.

My Pega Cloud

Clients can visualize the Major Infrastructure Update experience in My Pega Cloud through notifications and banner messages. For more information see, [Viewing the Pega Cloud update process in My Pega Cloud](#).



Environments (Pega Cloud 2)							
Name	Environment type	Type	Production level	Applications	Status		
Pega	Dev/Test	Standard Sandbox	2		UPDATED TO PEGA CLOUD 3	C	

Q2 2023 enhancements

Pega Cloud on Google Cloud Platform (GCP)

Pega Cloud 3 on GCP is GA in EMEA and North America regions! For more information, see [Pega Cloud 3 on Google Platform Overview](#). Google Peering is available via Pega Cloud Secure Connect in GCP [Deployment regions for Pega Cloud](#).

Pega Products on GCP

Pega Platform
Customer Service
Customer Decision Hub
Sales Automation

Minimal version required for GCP: Pega Platform Version: 8.8.2 | CloudK version: 3.8

(* Agile Studio, Language packs for Intelligent Automation and Customer Engagement are not yet certified on GCP. Coming soon!

(* Pega Workforce Intelligence, Pega Digital Messaging, Co-browse, and VoiceAI are deployed only in AWS, but accessible for Clients running on GCP.

Supported Regions

US-Northern Virginia | US-Oregon | Canada-Montreal | UK-London
EU- Germany | EU- Belgium | SA- Brazil

April 2023

Clients running on Pega Cloud 3 (AWS and GCP) can use TLS 1.2 or TLS 1.3 to establish secure connectivity. For details on supported TLS encryption settings, see [Data-in-transit encryption](#).

Improved autoscaling algorithm based on instance type availability per region.

Implemented a new endpoint to troubleshoot connectivity to applications running on Pega Cloud. The endpoint can be reached at <https://<environment domain>/user info>.

Logging Enhancements

Streaming Pega logs to external S3 now segregates log events by file to improve searchability. Added localhost logs as a log type.

Streaming Pega logs to Splunk now has a new configuration to request VPC (Virtual Private Cloud) connectivity. Users can now choose to exclude certain log types to reduce log volume.

List Prompts

Primary

Owner *	ClusterID *	HecUrl
HecToken	ExcludeLogTypes	CWLogGroup
EnvironmentGUID	NONE	

New!

Previous Create

My Support Portal

Enhanced the ticket intake experience in My Support Portal to improve ticket classification, prioritization, and communication frequency.

Deployment Manager

Enhanced diagnostics in Deployment Manager to verify application pipeline configurations. Users can also set the default Project as preference in Deployment

Manager v6. For more information see the [Deployment Manager Cloud services quarterly release notes 2023](#).

The left screenshot shows the 'Diagnostics: DemoDeployment' interface with four environment sections: Development (FAILED), Quality Assurance (SUCCESS), Staging (FAILED), and Production (SUCCESS). The right screenshot shows a detailed view of the Development section, highlighting errors related to access groups and application exits.

Name	Pega	Environment Type	Type	Production level	Applications	Status
selfserviceportal-prod	8.8.2	Production	Production	5	7	RUNNING
GOC-LPTrail	8.8.2	Staging	Sandbox	4	4	RUNNING
selfserviceportal-preprod	8.8.2	Staging	Production	4	8	RUNNING
selfserviceportal-stg1	8.8.2	Staging	LargeSandbox	4	7	RUNNING
selfserviceportal-UAT	8.8.2	DevTest	StandardSandbox	2	3	RUNNING
c3900c-ssp-devops	8.8.1	DevTest	StandardSandbox	2	1	Restart
selfserviceportal-dt4	8.8.2	DevTest	StandardSandbox	2	18	Download logs (tier & file type)

My Pega Cloud

My Pega Cloud allows users to schedule environment restarts.

The screenshot shows a table of environments with columns: Name, Pega, Environment Type, Type, Production level, Applications, and Status. A context menu is open over the 'selfserviceportal-dt4' row, showing options: Restart, Download logs (tier & file type), and Download logs (bundle). The 'Schedule' option is highlighted with a red box.

Name	Pega	Environment Type	Type	Production level	Applications	Status
selfserviceportal-prod	8.8.2	Production	Production	5	7	RUNNING
GOC-LPTrail	8.8.2	Staging	Sandbox	4	4	RUNNING
selfserviceportal-preprod	8.8.2	Staging	Production	4	8	RUNNING
selfserviceportal-stg1	8.8.2	Staging	LargeSandbox	4	7	RUNNING
selfserviceportal-UAT	8.8.2	DevTest	StandardSandbox	2	3	RUNNING
c3900c-ssp-devops	8.8.1	DevTest	StandardSandbox	2	1	Restart
selfserviceportal-dt4	8.8.2	DevTest	StandardSandbox	2	18	Download logs (tier & file type)

Pega Diagnostic Center enhancements

The PDC Scores now page provides information on Process Health, Reliability and Performance. The Home page in PDC now includes detailed connection status for each system, enabling faster troubleshooting of connectivity issues.

Q1 2023 enhancements

Pega Cloud on Google Cloud Platform (GCP)

As part of Pega's multicloud strategy, Pega Cloud® is available on Google Cloud Platform (GCP) and Amazon Web Services (AWS). To learn more, see [Pega Cloud 3 on Google Cloud Platform overview](#).

Logging Enhancements

Added filters in Log Streaming to Splunk that allow users to select the types of logs to be streamed.

Deployment Manager

[Deployment Manager 5.5.5](#) was released to address a page load performance issue on pipelines with a considerable number of deployments (>100).

Pega Cloud released the latest version of Deployment Manager for Pega Cloud services to the regions described in [Deployment regions for Pega Cloud](#). This new version of Deployment Manager includes an improved Route-to-Live (RTL) pipeline experience across your environments. For more information, see [Establishing a prescriptive Route to Live](#).

For a complete overview of features in this Deployment Manager release, see [Deployment Manager Cloud services quarterly release notes 2023](#).

To use this new version of the service, see [Getting started with Deployment Manager for Pega Cloud Services](#).

My Pega Cloud

Clients can use My Pega Cloud to view whether their environments are on Pega Cloud 2 or Pega Cloud 3.

The My Pega Cloud portal now supports environment restarts from My Pega Cloud portal, as shown in the following figure:

Name	Pega	Environment Type	Type	Production level	Applications	Status
pegasupport-prod1	8.8.1	Production	Production	5	23	RUNNING
PegaSupport-PreProd	8.8.1	Staging	LargeSandbox	4	23	RUNNING
pegasupport-stg1	8.8.1	Staging	LargeSandbox	3	28	RUNNING
pegasupport-dt1	8.8.1	DevTest	LargeSandbox	2	43	RUNNING
pegasupport-devops	8.8.1	DevTest	StandardSandbox	2	12	RUNNING

Production restart availability from your My Pega Cloud portal

For more information, [Environment restarts](#).

Pega Diagnostic Center enhancements

PDC now supports database statistics collection for Postgres 13 and later for Pega Platform™ versions 8.7.5, 8.8.3, and later. For more details, see [What's new in Predictive Diagnostic Cloud](#).

Pega Diagnostic Center supports operator privacy mode. Enable this mode to encrypt operator IDs, which prevents PDC from storing this ID data. Use this mode to comply with your company's security policies related to personally identifiable information (PII). For more information, see [Encrypting operator IDs in Pega Diagnostic Center](#).

Operational Enhancements

Added additional database monitors to measure application slowness and unresponsiveness.

Added additional monitors to notify Operations of updates that are delayed or running beyond their intended duration.

Autoscaling enhancements that optimize computing resource capacity.

Additional monitors help to optimize database services.

Supportability enhancements

Improved diagnostic capabilities that proactively identify potential issues.

Voice AI

Voice AI service on Pega Cloud 3 can process client phone calls that exceed ten minutes in length.

Pega Cloud 2 enhancements

Review the Pega Cloud® 2 continuous infrastructure updates that include critical security fixes and the following significant, client-oriented enhancements.

Q3 2023 enhancements

Q3 2023 enhancements include internal improvements to meet the prerequisites for the Cloud 2 to Cloud 3 update process.

Q2 2023 enhancements

Q2 2023 enhancements include the removal of Kibana Visualization (ELK).

Q1 2023 enhancements

Q1 2023 enhancements include a fix to prevent operational logs from quickly filling storage volumes.

Q4 2022 enhancements

Q4 2022 enhancements include internal storage enhancements that improve processing throughput.

Q3 2022 enhancements

Q3 2022 enhancements include an SFTP service-related enhancement to support file naming operations of large-sized files (2GB or more).

Q2 2022 enhancements

Q2 2022 enhancements include the following updates:

- Beginning in June 2022, clients on the latest Pega Cloud infrastructure can download and stream a new log, `localhost_access_log`. You can use this log to review requests to your application. For more information about all the available logs that you can track and manage, see [Understanding and obtaining Pega log files](#).
- With the introduction of Pega Cloud Secure Connect, you can take advantage of public peering and private connectivity options between your users and systems and Pega Cloud. For more information, see [Pega Cloud Secure Connect: your access to Pega Cloud](#).

Q1 2022 enhancements

Q1 2022 enhancements include the following updates:

- Support for [Private connectivity using AWS PrivateLink](#) and related new [End of Support statement](#).
- Pega Cloud received the Trusted Information Security Assessment Exchange (TISAX) AL2 Assessment from independent, accredited [TISAX](#) audit providers. This AL2 level assessment by independent audit providers confirms that Pega Cloud meets the high standards of data protection as defined by TISAX, such as data classified as confidential. While the auditor results for Pega Cloud are not

intended for the general public, clients can retrieve them exclusively through the TISAX portal to reflect this achievement.

Q4 2021 enhancements

Q4 2021 enhancements include:

- Use the new Filter Management feature, which provides a simple, secure method to manage the filters in Pega Cloud applications. With the introduction of Filter Management, you can now create and edit Java-based filters. For more information about the security configuration details, see [Filter management](#).
- Pega Cloud introduced Pega Status, a feature that provides you with a display of real-time information on the overall health of each active region in your subscription. After you sign up for Pega Status notifications, the system automatically sends email notifications any time an incident is created, updated, or resolved in your Pega Cloud subscription. Pega strongly recommends that clients subscribe to all components/regions that are relevant to services they receive from Pega Cloud. To explore Pega Status, go to [Pega Status](#). To learn more about the use of Pega Status and manage your notifications, see [Using Pega Status](#).
- New Pega Cloud deployments as of November 17, 2021 provide an SFTP service with one SFTP server for each client subscription that supports all your environments deployments, such as DevTest, Staging, and Production. Pega Cloud will continue to support existing client subscriptions with their existing SFTP service until you reach a service version that requires a migration of your service to the newer SFTP service. Pega Cloud support will communicate with you about planning a migration of your service. For more information, see [Using Pega Cloud SFTP service](#).

Q3 2021 enhancements

In September 2021, Pega Cloud updated its supported Transport Layer Security (TLS) encryption settings that support data-in-transit across its fleet of client environments. For more information, see [Data-in-transit encryption](#).

Q2 2021 enhancements

Review the following enhancements to your Pega Cloud services:

- Explore the new self-service [Pega Cloud](#) portal. You can use it for a variety of purposes:
 - Complete self-service tasks, such as restarts and log downloads.
 - View your upcoming, scheduled maintenance.
 - Participate in your upgrade journey.
 - Review Pega requests in a new Action Center folder, such as approving the UAT and Go-NoGo stages of the upgrade process. For more information, see [Administering your Pega Cloud service](#).
- Run your new Development, Test and Staging environments at production level 3. While Pega Cloud does not support client requests to modify these levels after the environments are running, you establish each environment run level during the questionnaire phase of onboarding. For more information about which levels are supported for different types of deployed Pega Cloud environments, see [Specifying the production level](#).
- Benefit from the enhanced auto-hibernation feature that gives you better visibility into the status of the hibernation and wake-up process through your self-service [Pega Cloud](#) portal. For more information about how Pega partners with you to reduce the energy consumption and the carbon footprint of your client environment portfolio and review the wake-up steps, see [Managing hibernated environments](#).
- Prevent insecure logins by adding or updating URL matching using the latest LDAP support for URL matching. Pega Cloud clients using IP addresses in their LDAP Authentication Service must update their service. For more information, see [Configuring login using a custom authentication service](#).
- Stream your Pega software-generated log files to an Amazon S3 bucket within your enterprise Amazon Web Services account. For more information, see [Streaming Pega logs to an external Amazon S3 bucket](#).
- Integrate your AWS Transit Gateway into your Pega Cloud services subscription. This enhancement allows you to centralize your external connections to your Pega

Cloud environments in a monitored and secure private network. For more information about the requirements and to complete your integration, see [Implementing a Transit Gateway integration](#).

Your Pega Platform™ version 8.6 application in your Pega Cloud environment can take advantage of the following enhancements and new features:

- Archive and purge cases in your Pega Platform database to improve its performance as part of your long-term data retention plan. For more information about this enhancement, see [Archiving and expunging case data](#).
- If you have purchased Pega Process AI, Pega Cloud enhances your Pega Cloud services infrastructure to support AI, Decisioning, & Event stream triage. For more information, see [Pega Process AI](#).
- Use the new Servlet Management feature in your Pega Platform application, which provides a simple, secure method of managing the servlets in Pega Cloud applications. With Servlet Management, you can customize the servlet name, authentication type, and related parameters. You also can add new servlets and disable and delete unused servlets. For more information about related security configuration details, see [Servlet and Filter management](#).
- Set up your streaming service through your Pega Platform application using enhanced support for streaming service authentication. For more information, see [Creating a Kafka configuration instance](#).
- New deployments of Pega Customer Decision Hub™ use your Decision Data Store (DDS) to store your action state data by default, which boosts your application performance and improves its stability. Along with this enhancement, new application versions also support changing your action state data to use an available database. Data storage configurations in existing deployments of Customer Decision Hub are not affected. To learn more or change this default behavior, see [Disabling the Decision Data Store as action state storage on Pega Cloud](#).

How Pega keeps your Pega Cloud service current

Pega Cloud® ensures that you have access to the latest features and capabilities of Pega Platform™ and your Pega applications by performing periodic system maintenance on your Pega Cloud environments.

This is part of the standard maintenance policy Pega provides to you as defined in [Pega Cloud maintenance and types of system updates](#).

Infrastructure updates

Pega updates the supporting infrastructure services of each environment, including:

- Database
- Latest security and performance benefits
- Service enhancements
- New capabilities

Infrastructure updates are zero-downtime and do not change the Pega software running in the Pega Cloud environment. For more information about the Pega Cloud infrastructure update process and the expected experience, see [Infrastructure update Process for Pega Cloud](#).

Software patches

Pega applies cumulative patch releases of the latest Pega Platform 8.x software to your environments and the patch-supported customer relationship management (CRM) applications running in Pega Cloud environments. Each patch includes important security, supportability, and reliability improvements and bug fixes. The bug fixes are based on a wide range of client feedback, which ensures that you have access to addressed issues across each Pega Infinity release. Patch installation is zero-downtime and includes only rule changes observed between the patch and the current version; patches do not require a cloned environment for validation. For more information

about Pega Platform and supported CRM patches, see [Pega Platform Resolved Issues and Application patch releases](#).

- Patch Process for Pega Infinity 8.3 and later
- Patch Process for Pega Infinity 8.2 versions
- To review the patch support policies, see [Pega Cloud maintenance and types of system updates](#).

Software updates

Pega updates the environment to the latest major or minor software versions of Pega Platform and the suite of CRM applications running in Pega Cloud services environments. With each software update, Pega commits to making Pega Platform and Pega application software changes that are backwards compatible and include the latest security updates, capabilities, feature enhancements, performance improvements, and supportability enhancements. Software updates for Pega Cloud environments include a cloned environment for validation.

Pega implements a two-phased software update process consisting of a basic update phase and a feature adoption phase. With the basic update phase, you can benefit from the latest performance and security improvements without affecting your existing Pega applications. After the basic update is complete, you can use the feature adoption phase to take advantage of the latest Pega Infinity and application features using your standard DevOps process. The update process features update assessment tools, an updated, cloned environment to complete compatibility testing, and testing orchestration with update pipeline in Deployment Manager. Pega supports near-zero downtime updates and updates with minimal downtime of the Pega Infinity software in your environment:

- Pega Infinity updates starting from version 8.4.2 feature a near-zero-downtime process, so your environment remains available throughout the update process. It also includes a Go-NoGo phase during the production update in which you perform a final confidence check of your applications. Pega updates the production environment only after you indicate a go approval. The entire update

process usually takes around 15 days. For details about the minor Pega Cloud update process and the expected experience, see [Pega Cloud update Process for Pega Infinity release 8.4.2 and later](#).

- Software updates from previous versions may require downtime and some post-update steps. The entire update process usually takes around 30 days. For more information about the major Pega Cloud update process and the expected experience, see [Pega Cloud update Process for Pega Infinity release 8.4.1 and earlier](#).

Process to update to Pega Cloud 3

As part of Pega's commitment to continuously evolve its cloud architecture standards that are based on the latest industry technologies and practices, Pega is moving all Pega Cloud® clients to Pega Cloud 3. Pega will work closely with your team to help you leverage our standard major infrastructure update automation to ensure the update is completed smoothly with minimal downtime.

As cloud technologies continue to rapidly advance, Pega is committed to continuously evolving its cloud architecture standards. Pega has years of experience managing client workloads running on cloud technologies and has mastered the management of Pega Cloud on public cloud platforms using its own automation tool suite, known as the Global Operations Center.

Benefits of updating to Pega Cloud 3

Pega Cloud 3 provides a microservices architecture and uses container orchestration capabilities provided by Kubernetes; Pega will work with you to schedule the update at a time convenient to you. Clients running applications on Pega Cloud 3 will continue to receive the same mission-critical resiliency and security standards, while experiencing the following key benefits:

Improved Scalability

Pega Cloud's services auto-scale to meet your application demand, beyond your "steady-state" level up to peak usage. Pega Cloud 3 scales dynamically, even if you have a sudden, unforeseen load increase. This enhances the reliability of your Pega Cloud service and minimizes the probability of service disruption related to infrastructure capacity.

Improved self-healing and fault-tolerant services

Pega Cloud 3 takes advantage of the self-healing capabilities of Kubernetes-based architecture to autonomously recover and restore services, while mitigating the client impact of the issue. This means that Pega Cloud 3 recovers faster than ever, while maintaining high-availability and performance for your application workloads.

Blazing fast maintenance

Pega Cloud 3 provides highly-available environment restarts, which allows Pega to quickly apply maintenance updates and patches across Pega Cloud.

Independent microservice updates

The microservices-based Pega Cloud 3 architecture allows for targeted, independent, and continuous service updates. This means that the latest Pega Cloud features and fixes become available to clients quickly. Pega handles the escalating velocity of change in the technology industry, so you can focus on your customers and business standards.

Update to Pega Cloud 3: High-Level Overview

The main screen in your My Pega Cloud portal will display whether your environments are on Pega Cloud 2 or Pega Cloud 3:

The screenshot shows the Pega MPC Home page. At the top, there are dropdown menus for 'Cloud System - Test Account1' and 'TSTAC1-CR149-PRMPC-us-east-1'. On the right, there's a greeting 'Hello, MPC Automation' with a dropdown arrow. The main header 'PEGA MPC' has 'Home' and 'Environments' tabs. Below the header, it says 'My Pega Cloud' and 'Pega Cloud 2'. The main content area has three main sections: 'My environment (Pega Cloud 2)' (with 1 Environment), 'Account users' (with 140 Users), and 'Updates' (showing 'Pega 8.8.3 Available'). Below these are 'Support tickets' (0 Ongoing requests) and 'Maintenance' (0 Upcoming maintenances). A red arrow points to the 'My environment' section, and a red box highlights the '(Pega Cloud 2)' part of the title.

If your deployments are on Pega Cloud 2, the update to Pega Cloud 3 requires a one-time major update with a very small amount of downtime. Pega manages the majority of the work needed for this update.

There are three main phases of this update:

- Preparation phase
- Update phase
- Post-update testing phase

During your major infrastructure update, Pega leverages a standard automated process of AWS replication to protect your data.

After this major update, Pega Cloud conducts maintenance processes as outlined in [Pega Cloud maintenance and types of system updates](#).

There are no changes to Pega Cloud SLAs

Updating to Pega Cloud 3: Detailed Process

Preparation phase

Determine eligibility for update

To ensure the most efficient and seamless transition for all our clients, Pega has adopted a strategic approach that considers individual client environment readiness for the Pega Cloud 3 update, as well as specific capabilities and requirements. This meticulous planning is designed to minimize downtime and reduce impact, resulting in an experience that is as smooth as possible.

Before your environments can be updated to Pega Cloud 3, some parts of your system need to be aligned with the Pega Cloud 3 architecture. Pega is conducting assessments of all client environments to determine what prerequisites need to be completed prior to moving from Pega Cloud 2 to 3.

Note: Pega Cloud clients, including those using Customer Service and Sales

- ⓘ Automation, will begin their update process in 2023. Customer Decision Hub clients will be updated starting in 2024.

To begin your process, Pega assesses your environments to determine if you're eligible for the Pega Cloud 3 update. You must be on the latest patch of Pega Platform™ version 8.7 or later.

Additional prerequisites for this update, depending upon your configuration, can include connectivity options. If you are using private connectivity, you must be on one of the current Pega Cloud Secure Connect options or have plans to move to one of these connectivity options as part of the update to Pega Cloud 3. For this update, Pega Cloud Secure Connect supports the following connection options:

- Cloud Exchange public connections
- AWS Direct Connect public VIF
- AWS PrivateLink

Note: Legacy connectivity options are not supported on Pega Cloud 3. If you

- ⓘ leverage legacy connectivity options, work with your Pega GSA representative

to determine the best schedule to update to one of our current Secure Connect options.

Initial Setup and Next Steps

After Pega determines one or more of your deployments is eligible for the move to Pega Cloud 3, Pega sends you an email from a Pega Global Service Assurance (GSA) representative, describing your Upcoming Pega Cloud 3 Update: Important Information. This email will:

- List the environments that will be updated.
- Explain that you will be assigned a new set of NAT Gateway IP addresses.
- State that your GSA representative will collaborate closely with your team to manage any necessary connectivity reconfigurations.
- Describe the downtime.
- Arrange a meeting to go through any questions or concerns you may have.

Your GSA representative will also discuss any potential changes to your system that may occur as a result of this update, such as Log Streaming enhancements and SFTP user names.

After this initial setup is complete, you will receive another email, describing the Next Steps. This email will:

- Include your new NAT Gateway IP addresses.
- State that you must integrate these new IPs into your allow lists.
- Specify any additional steps which are required. These will vary depending upon your setup (configuring Log Streaming to Splunk or your S3 buckets, SFTP user names, or other specific configurations).
- Describe how you need to go into your My Pega Cloud account and approve the case, to indicate your readiness to continue with the update process.
- Explain that your GSA representative will then work with you to determine suitable update dates for each of your environments.

Update Phase

During the update process, Pega will switch each of your Pega Cloud 2 environments over to Pega Cloud 3 and then hibernate your Pega Cloud 2 environments. The process involves updating one environment at a time (in an agreed-upon maintenance window), so only one environment at a time will experience this short outage.

Pega's automated update functionality will handle your ongoing processing so that your downtime is as short as possible with no loss of work. For example, an automatic flag is set so that any incoming batch requests get temporarily written to the database. After the Queue Processors have completed all work in queue, the Pega Cloud update process will occur. After the environments are updated to Pega Cloud 3, these stored requests will be processed, and the batch processing will automatically restart.

Post-update testing phase

After the update is complete and your environments are updated to Pega Cloud 3, you will need to perform your application smoke testing to verify that everything is working correctly.

If you leverage integration functionality, you will need to test that connectivity in your lower environments.

Post-update considerations

Pega Cloud 3 resources are dynamic. Resource names, counts, and sizes continuously adjust to fit your workload requirements. Use Pega Diagnostic Center to assess the performance and health of your applications by accurately tracking key Pega Cloud performance indicators. For more information, see [Monitor your system with Pega Diagnostic Center](#).

If you use log streaming, verify that your logs are going to the location you have specified (Splunk or your S3 bucket).

All data stored in Pega Cloud File Storage repositories will have had their creation timestamp updated as they were processed during the upgrade from Pega Cloud 2 to Pega Cloud 3.

To ensure the smoothest experience on Pega Cloud 3, clients using any version of Java Development Kit (JDK) earlier than JDK 11 are updated to JDK 11 as part of the major infrastructure update. Custom Java code written on a JDK version earlier than JDK 11 will need to be refactored after the major infrastructure update to be JDK 11 compliant. As a best practice, we recommend you leverage Pega out-of-the-box capabilities and refrain from writing custom Java code.

- [Viewing the Pega Cloud 3 update process in My Pega Cloud](#)
- [Client Pre-Update Actions and Approval](#)
- [Deployment Manager during the update to Pega Cloud 3](#)

Viewing the Pega Cloud 3 update process in My Pega Cloud

Pega Cloud® clients can track the progress of their update from Pega Cloud 2 to Pega Cloud 3 in their My Pega Cloud portal.

Pega Cloud 2 environments

For a full overview of this process, see [Process to update to Pega Cloud 3](#).

The updates to your environment(s) will be performed one after the other – not simultaneously. Once the update is scheduled for your environment(s), you will see a message on the Home screen of your My Pega Cloud Portal.

The screenshot shows the Pega Cloud 2 interface. At the top, there's a banner indicating a 'Major Infrastructure Update from Pega cloud 2 to 3'. It says 'Your project is in the process of being updated to Pega Cloud 3. To follow the progress of this update, see information in the Message Center. Once your environment(s) are updated, use the dropdown next to the cloud icon at the top left of the screen to switch to your new Pega Cloud 3 project TSTAC1-CR1234-Sftpdef1-us-east-1.' Below the banner, there are several cards: 'My environments (Pega Cloud 2)' (1 Environment), 'Account users' (159 Users), 'Support tickets' (0 Ongoing requests), 'Maintenance' (0 Upcoming maintenances), and 'Updates' (Pega 8.8.3 Available). A 'Start' button is visible in the Updates section.

Notifications for this update will be displayed on the Message Center when the update has been scheduled.



Note: If you wish to reschedule your update, please call Support.

To see the Status of your environment(s), click on the View Details link from the Home screen.

The screenshot shows the Pega Cloud 2 My Pega Cloud portal. At the top, there's a header with 'Cloud System' and 'Hello, MPC Automation'. Below the header, the main dashboard has several sections: 'My environments (Pega Cloud 2)' (1 Environment), 'Account users' (140 Users), 'Support tickets' (0 Ongoing requests), 'Maintenance' (0 Upcoming maintenances), and 'Updates' (Pega 8.8.3 Available). A large red arrow is overlaid on the screen, pointing upwards from the 'My environments' section towards the 'Account users' section.

The Status of your Pega Cloud 2 environments will remain green and be RUNNING until the update begins. During this time, you can continue to use your My Pega Cloud portal to perform self-service tasks as usual.

The screenshot shows a table titled 'Environments (Pega Cloud 2)'. The columns are: Name, Environment type, Type, Production level, Applications, and Status. There is one row visible with the following data: Name - Pega, Environment type - DevTest, Type - StandardSandbox, Production level - 2, Applications - (empty), and Status - RUNNING. The 'Status' column contains a green button labeled 'RUNNING'.

Client Action Needed to Proceed: Pega Cloud 3 Pre-Update Actions Approval

In your My Pega Cloud portal, go to the Action Center to find the following message:

The screenshot shows the Pega MPC Action Center interface. At the top, there are three notifications:

- Major Infrastructure Update from Pega cloud 2 to 3**: Your project has identified for major infrastructure update and progress has started. Once environment update is done, start using Project [REDACTED] and environment to experience self service capabilities.
- A major infrastructure update has been initiated for [REDACTED]**: Click here to view a list of actions you must take. After you have completed these actions, provide approvals so Pega can continue the update process.
- A major infrastructure update has been initiated for [REDACTED]**: Click here to view a list of actions you must take. After you have completed these actions, provide approvals so Pega can continue the update process.

Below the notifications, there are tabs for **Action center**, **Message center**, and **My cloud setup**. A red "Help with MPC" button is located on the right side.

When you click on the link in the message, a new window will appear requesting that you set certain network configurations before providing approval for Pega to proceed with the update. For more information on the actions you must take, see [Client Pre-Update Actions and Approval](#).

During the Update

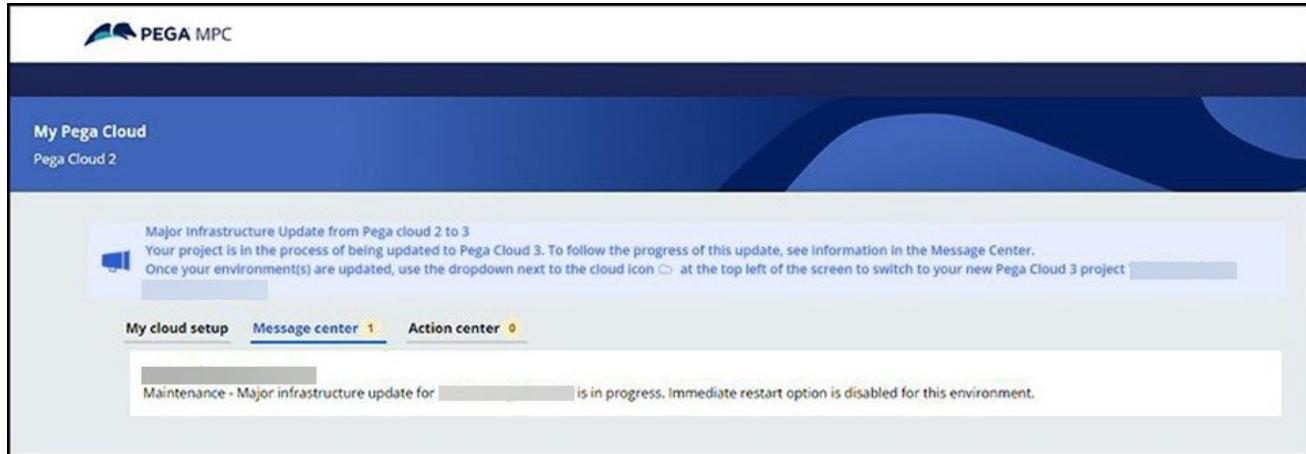
Once the automated update starts, the environment being updated will display a Status of Maintenance. At this point, you will temporarily not be able to perform your self-service tasks.

The screenshot shows the Pega MPC Environments page. It displays a table of environments, with one row highlighted:

Name	Environment type	Type	Production level	Applications	Status
Pega 8.5.0	Dev/Test	Standard Sandbox	2		Maintenance

At the bottom right of the table, there is a red "MAINTENANCE" button. The status column for the highlighted row shows "MAINTENANCE".

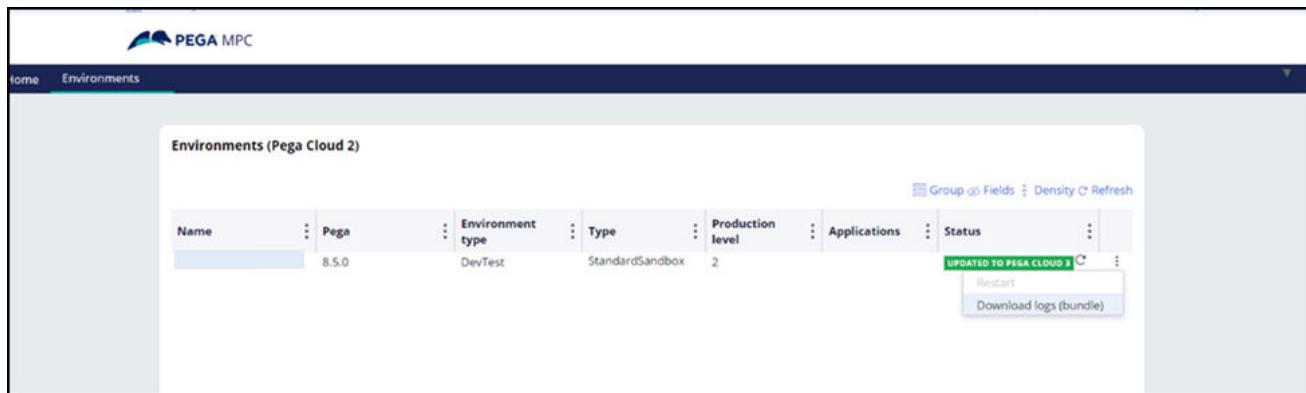
The Message Center will display a notice stating that the update is in progress, and the Restart option will be disabled.



A screenshot of the Pega MPC interface. The top navigation bar shows 'PEGA MPC'. Below it, a blue header bar says 'My Pega Cloud' and 'Pega Cloud 2'. The main content area has a message: 'Major Infrastructure Update from Pega cloud 2 to 3. Your project is in the process of being updated to Pega Cloud 3. To follow the progress of this update, see information in the Message Center. Once your environment(s) are updated, use the dropdown next to the cloud icon at the top left of the screen to switch to your new Pega Cloud 3 project.' Below this, there are tabs: 'My cloud setup', 'Message center 1' (which is selected), and 'Action center 0'. A message box states: 'Maintenance - Major infrastructure update for [redacted] is in progress. Immediate restart option is disabled for this environment.'

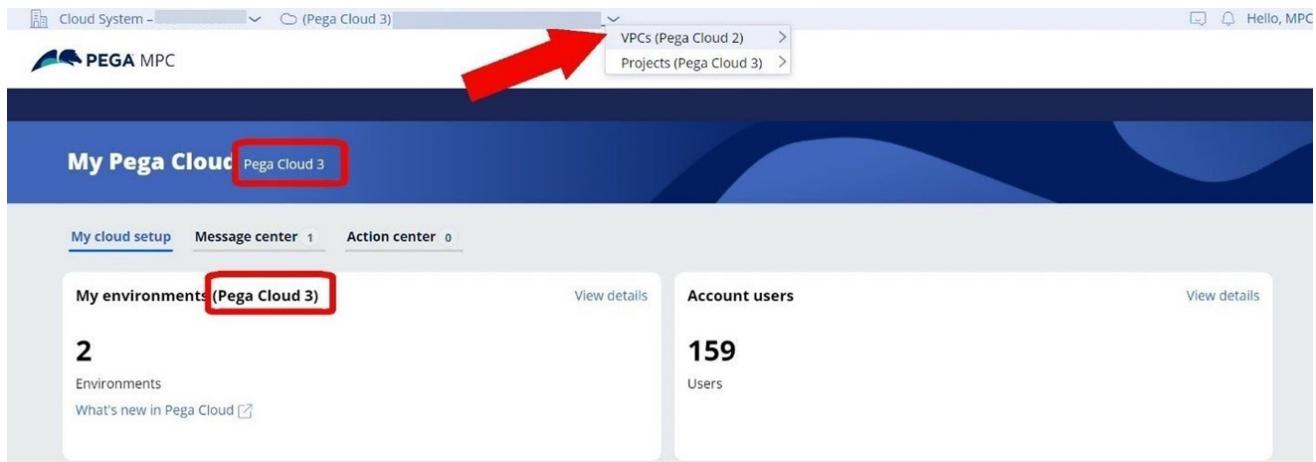
Pega Cloud 3 environments

After the update is complete for a particular environment, the Status for that environment will be marked as Updated to Pega Cloud 3.



A screenshot of the Pega MPC 'Environments' page. The top navigation bar shows 'PEGA MPC' and 'Environments'. The main content area displays a table titled 'Environments (Pega Cloud 2)'. The table has columns: Name, Environment type, Type, Production level, Applications, and Status. One row shows 'Name: Pega', 'Environment type: Dev/Test', 'Type: StandardSandbox', 'Production level: 2', 'Applications: 1', and 'Status: UPDATED TO PEGA CLOUD 3'. There are buttons for 'Group', 'Fields', 'Density', 'Refresh', 'Restart', and 'Download logs (bundle)'.

You can view the updated environment on Pega Cloud 3 by going to the Home page and clicking on the dropdown next to the cloud icon at the top left of the screen.



After you switch to the Pega Cloud 3 environment, you will also see that the Home screen displays "Pega Cloud 3."

Click on the View Details link to see details about your environments. The Status of your Pega Cloud 3 environment(s) which were updated should be green and be RUNNING. You can now perform the standard My Pega Cloud self-service capabilities in these environments, including restarts and log downloads.

Future maintenance activities will now be visible from these Pega Cloud 3 environments.

Downloading log bundles from Pega Cloud 2

You can still reach your Pega Cloud 2 environments by using the dropdown at the top of the page (shown in the prior section). You are still able to download log bundles from your Pega Cloud 2 prior activity; however, all activity going forward from the update will be on your Pega Cloud 3 environment. The Pega Cloud 2 log bundles will be available for the next 30 days, and then the Pega Cloud 2 environments will be decommissioned.

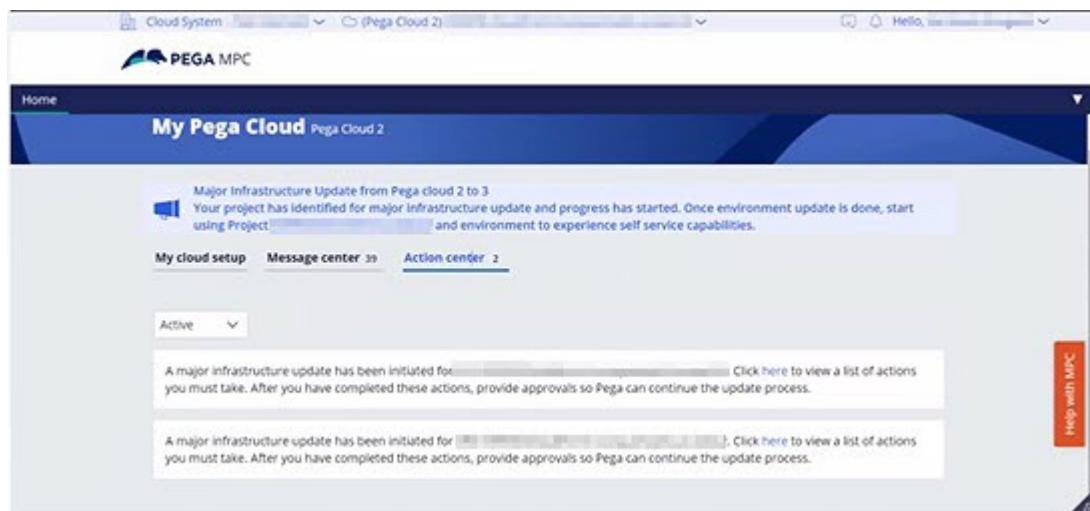
Client Pre-Update Actions and Approval

You will encounter the Client Pre-Update Actions and Approval page in My Pega Cloud as your environments are transitioned from Pega Cloud® 2 to Pega Cloud 3. At this point, your network engineers need to set certain network configurations, and then you need to provide approval for Pega to proceed with the Cloud 3 update.

For more information about viewing the status of your update in My Pega Cloud, see Viewing the Pega Cloud 3 update process in My Pega Cloud.

- Note:** As part of the pre-update actions, you may need to configure new IP addresses and DNS records. It is very important that you do NOT delete the old IP addresses and DNS records until at least thirty days after the completion of the update, so you have a chance to verify that the updated systems are working properly.

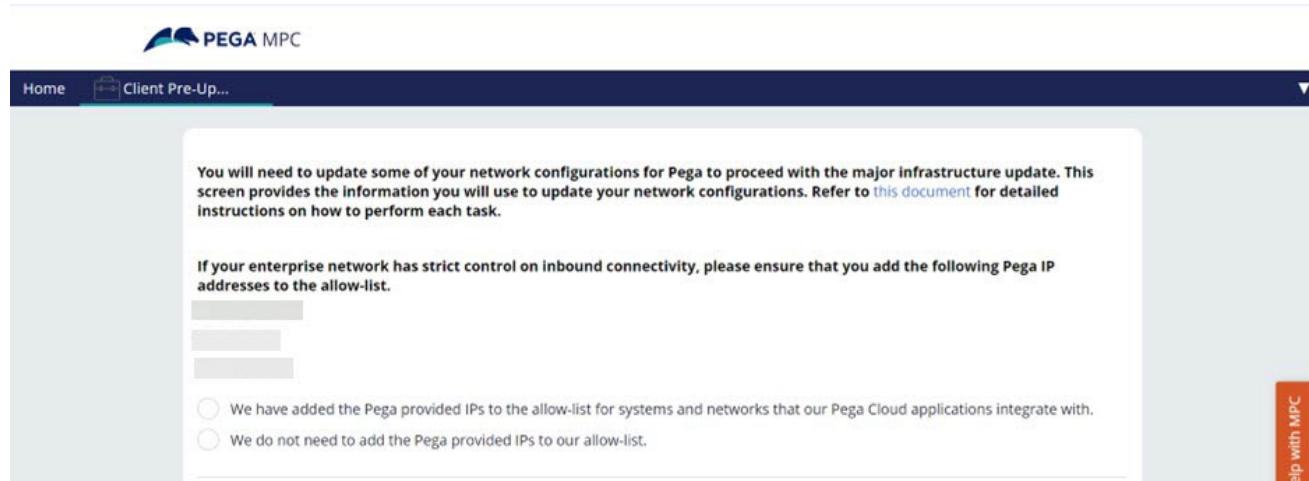
Once the Pega Cloud team prepares your environment(s) for the Pega Cloud 3 update, go to the Action Center in your My Pega Cloud portal to find the following message:



IMPORTANT: If you have more than one VPC that needs to be updated, more than one message will appear. You will need to click on each link to perform the following steps.

Add the Pega-provided IP addresses to your allow-list

When you click the link, the following message will appear:



Please add these Pega-provided IP addresses to your allow-list, and then check the box which states, "We have added the Pega-provided IPs to the allow-list for systems and networks that our Pega Cloud applications integrate with."

If you do not use allow-listing on your firewall configuration, please check the box that says, "We do not need to add the Pega-provided IPs to our allow-list."

Add the Pega SFTP IP Addresses to your allow-list

Follow this step if you have SFTP configured. If you do not use SFTP, this section will not display on this form.

There will be a list of IP addresses in the section marked "Add these Pega SFTP IPs to your allow-list if there is an outbound restriction at your end over Port <number>."

These are the IP addresses that Pega shares with the client and will need to be added to your allow-list.

Once you have done that, check the box labelled, “We have added the Pega SFTP IPs to our allow-list.”



Update the SFTP user names for all your environments

Underneath the allow-list section for SFTP, you will see a list with your environments and their hostnames. For each environment, click the arrow at the left of the environment name to display a table of the SFTP user names.



The table will show the “Old SFTP user names,” which is the list of names that you are currently using in Pega Cloud 2 to connect to the SFTP service. You must change your

SFTP service connection to use the “New SFTP user names” listed for the environment before updating the environment to Pega Cloud 3.

Once you have updated to the new SFTP user names, Pega strongly recommends that before the Cloud 3 update, you log in at least once using each new SFTP user name to confirm that you see the same information you see when logging in with the old SFTP user names. After the update to Cloud 3, log in to your updated environments with each SFTP user name to confirm that you still see the same information. You will be prompted to accept the HostKey here. Alternatively, you can create a Pega support ticket to receive the HostKey before making the connection to the SFTP server. Your old SFTP user names will no longer work after the update, and you can only access the SFTP server with your new user names on Cloud 3. If you receive errors logging in with your new SFTP user names, or if you do not see all the information you expect to see, contact Pega Support.

After you have verified your IP addresses and updated your SFTP user names, check the box for, “We have updated the SFTP user names for all our environments wherever applicable, and we have logged in with each user name to confirm they function correctly”.

This section of the Approval screen also shows the list of “IP addresses [that] are allowed to connect to Pega SFTP server.” These are your IP addresses on the allow-list for the Pega SFTP server site which have been moved from your Pega Cloud 2 environment to Pega Cloud 3.

We have provided these IP addresses with a wider CIDR range which includes your prior IP address ranges. We have also eliminated 0.0.0.0 IP addresses for greater security. Check these IP addresses to verify they are correct; if they are, you do not need to take any further action. If they are incorrect, contact Pega Support.

Add the DNS Records

Follow this step if you use Custom Domain Names. If you do not, this section will not display on this form.

Underneath the DNS records section, you will see a list of your environments. For each environment, click the arrow at the left of the environment name to display a table of the DNS information, including the Domain names, Record names, and other information.

Domain name	Record name	Record type	Record value	Status
pegaservice.net	ce9ecf455ce1082ff3787...	CNAME	a7704d8be2d03a65087...	Pending
pegaservice.net	6b77cbbfb105952f3d59b...	CNAME	7adc1176af3d9ad48054...	Pending

These DNS names are used to validate certificates for the Custom Domain Names that Pega creates for your environment.

The status for each domain name will be PENDING_VALIDATION when you first arrive at this page. Add the DNS records by following these steps.

Note: If you are not the person responsible for adding DNS records, click **Export to Excel** to download an Excel spreadsheet with all the relevant information. Then, share the spreadsheet and the link to this instruction document with the person who will perform the steps.

1. Access Your DNS Management Console

If you're using a cloud provider, log in to your provider's management dashboard via a web browser. If you're using on-premises software, access the DNS management interface, usually through a dedicated application or web portal.

2. Navigate to DNS or Domain Management

Look for a section labeled "DNS Management", "Domain Management", "DNS Zones", "Hosted Zones", or something similar.

3. Select Your Domain/Zone

From the list of domains or zones, click on the name of the domain for which you want to add the CNAME record.

4. Locate Record Management Option

Find an option that allows you to add or manage DNS records. This might be labeled as "Manage Records", "Edit Records", "Add Record", etc.

5. Add a New CNAME Record

- Click on the option to create a new DNS record.
- For the record type, choose or select 'CNAME' or 'Canonical Name'.
- Name/Host/Alias: Enter the subdomain or prefix provided for the CNAME record. You can find this in the "Record name" column. For example, if Pega Cloud provided _xxxx.example.com, you'd enter _xxxx or the full name, depending on your DNS system's requirements.
- Value/Points to/Destination: Input the target value provided for the CNAME record, like _xxxxx.acm-validations.provider-domain.com. You can find this in the "Record value" column.
- TTL (Time To Live): This determines how long the record will be cached by DNS resolvers. If given an option, you can set it to a default or preferred value (e.g., 300 seconds or 5 minutes). Some DNS systems might have this pre-configured.

6. Save or Confirm Changes

After you have entered the necessary details, save or confirm the changes to add the CNAME record to your domain.

When you return to the Client Pre-Update Actions and Approval page, the Validation status may still say PENDING_VALIDATION. Refresh the page. If the records were added correctly, the Validation status should now be ISSUED. Do not proceed to next steps until all environments have a Validation status of ISSUED.

After you have created the appropriate records and all environments have a Validation status of ISSUED, click "We have created the DNS record on our side."

- Note:** The new CNAME records you added in this step should never be
- ⓘ removed from your DNS. If you remove the records, the vanity URLs will stop working.

Give final approval

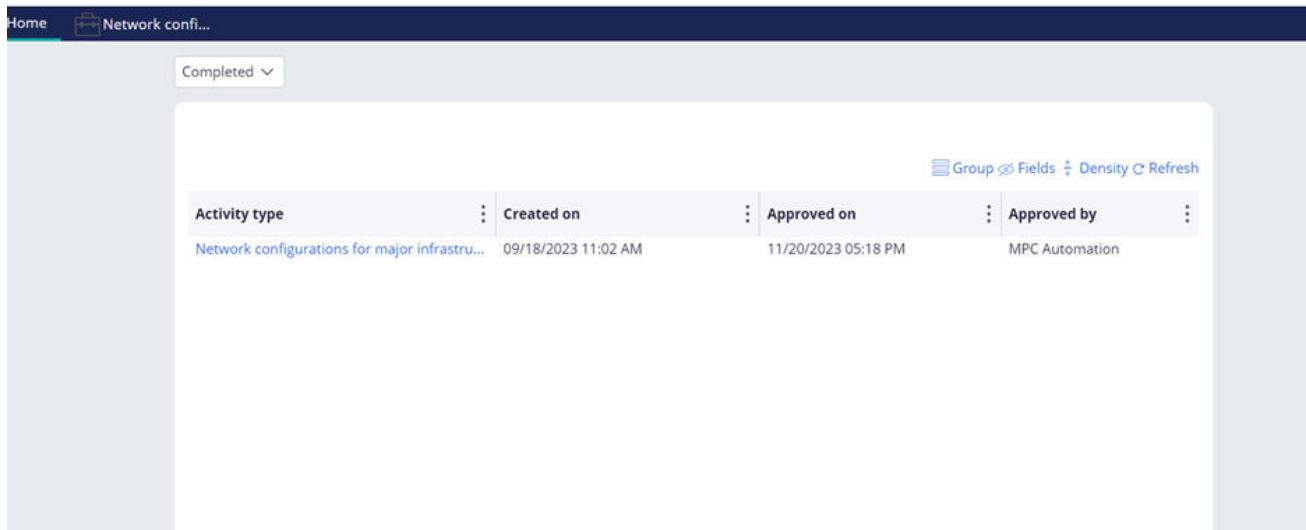
After you have completed all the above actions, check the box that says, "We have completed all the steps on this page and are ready for the major infrastructure update" and click Submit to move the update process forward.

Pega cannot schedule your updates without this approval. After you have given your approval, Pega will continue with the update process.

When you click Submit, Pega's automated process validates that the actions on this screen were done. Do not click Submit if you have not completed these actions. If you do click Submit before taking all the actions, an error message will appear telling you to complete all actions to proceed.

After you submit this form, the message with the link to the form will disappear from the landing screen of the MPC action center. However, you can access a read-only version of the completed form in the action center by selecting "Completed" in the

dropdown menu. This is an easy way to review any IP address, SFTP, or DNS information you received in the form.



Deployment Manager during the update to Pega Cloud 3

All clients on Pega Cloud® 3 have access to Deployment Manager, Pega's state-of-the-art automation tool for testing and deploying applications built on Pega Platform™. This article outlines everything you need to know about Deployment Manager during your update from Pega Cloud 2 to Pega Cloud 3.

Clients on Pega Cloud 3 can log in to Deployment Manager through My Pega Cloud by clicking on the Deployment Manager URL in the Environment details page for an environment. The URL may be different for environments in different projects, so be sure to always use the URL from an environment in the project you want to work on.

The update process and your login credentials differ slightly based on whether you were using Deployment Manager on Pega Cloud 2. Read the section below that applies to your situation.

For clients who were not using Deployment Manager on Pega Cloud 2

If you have not used Deployment Manager on Pega Cloud 2 within the last year, the Deployment Manager environment will be decommissioned to prepare for the update to Pega Cloud 3, and any data in the Deployment Manager environment will be deleted. If you need access to this data, contact [Pega Support](#) for assistance.

All clients will have access to Deployment Manager on Pega Cloud 3. We strongly recommend you adopt Deployment Manager as your DevOps, automation, and application testing and deployment tool. You can use your Pega Community credentials to log in to Deployment Manager from My Pega Cloud. For more information on Deployment Manager, see the [Deployment Manager Community page](#) and [Deployment Manager overview](#).

You will not need to take any additional steps during the Pega Cloud 2 to Pega Cloud 3 update process to have access to Deployment Manager on Pega Cloud 3.

For clients who were already using Deployment Manager on Pega Cloud 2

You will still have access to the same Deployment Manager on Pega Cloud 3 that you did on Pega Cloud 2, and you can log in using the same credentials you have always used. You will also have the option to log in through the URL on My Pega Cloud.

To ensure a smooth transition of Deployment Manager from Pega Cloud 2 to Pega Cloud 3, review the steps below. You can expect Deployment Manager to be offline for up to 2 hours during the update process. Your Service Advisor will provide you with a schedule, so you will be aware of the update window.

Deployment Manager update process

When the update process begins, Deployment Manager will be the first environment that will move to Pega Cloud 3. The recommended sequence of updates is Deployment Manager (DevOps) -> Development (dt1) -> Staging (stg1) -> Production (prd1).

Once the Development (dt1) or any Route to Live environment moves to Pega Cloud 3, you will be able to use the application pipelines to move application changes through the Route to Live.

Steps to follow during Deployment Manager update

Pre-update

Perform the following actions:

1. Confirm that all deployments are completed. There should be no in-progress, waiting, or failed deployments in the application pipelines. Confirming that all deployments are completed pre-update will help avoid any issues that may occur from resuming an ongoing deployment post-update.
2. Run diagnostics on the most recently used pipeline and document the results so you can refer to them post-update. You can run diagnostics by following the instructions in [Diagnosing a pipeline in 5.5.x](#).

Post-update

You can track the status of your environment updates in My Pega Cloud. For more information, see [Viewing the Pega Cloud 3 update process in My Pega Cloud](#).

Once all Route to Live environments (dt1, stg1, and prod1) are moved to Pega Cloud 3, re-run the diagnostics for the pipeline you ran diagnostics on in the pre-update phase. Ensure the results are the same as in pre-update phase. If the results are different, contact [Pega Support](#) for assistance.

Pega Cloud connectivity options

Use a Pega Cloud® services connectivity option to integrate Pega Cloud with your other cloud-based and enterprise solutions.

Pega Cloud is a public as-a-service solution. Pega recognizes that our clients typically run their Pega application as part of an integrated whole, with other solutions that support their organizations. Our clients commonly integrate their other cloud and enterprise solutions with Pega to drive maximum value. Accomplishing this requires robust connectivity that meets our clients' requirements in the following critical characteristics:

- Security
- Throughput, consistency, and performance
- Regulatory and compliance

By default, Pega provisions Pega Cloud for broad public access. If your organization requires a more dedicated path, with more predictable performance that is exclusive to your access, Pega Cloud Secure Connect supports additional options for access.

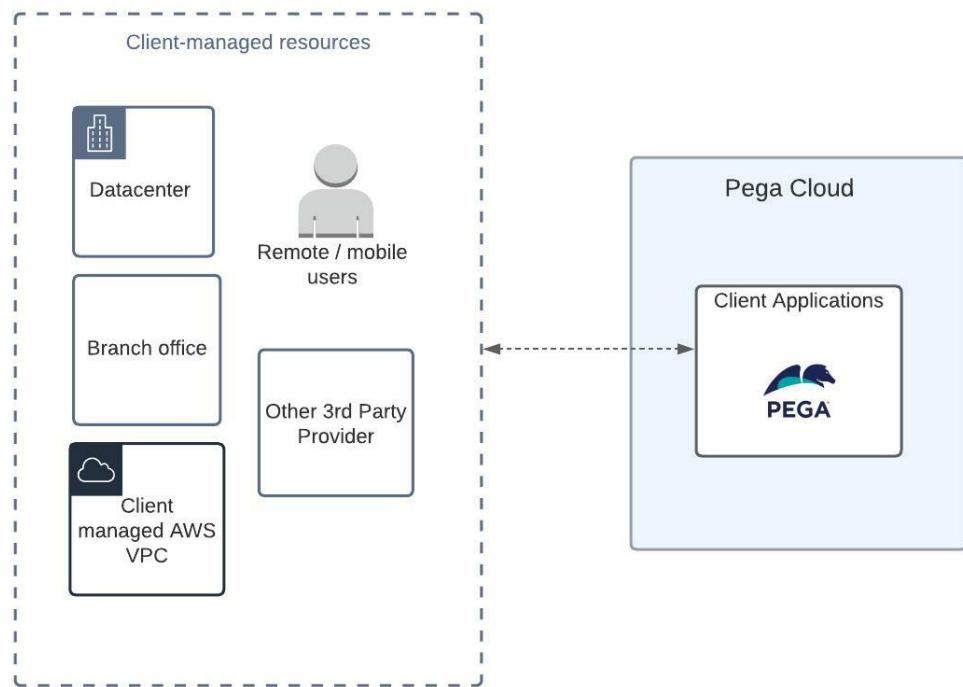
These options simplify connectivity and provide broad accessibility between Pega Cloud and your managed or remote systems and users. Click on a link to learn more:

- [Public Access \(Internet\)](#)
- Use [Pega Cloud Secure Connect](#) to secure your connectivity for your organization's mission-critical workloads using the following supported options:
 - [Cloud Exchanges](#)
 - [AWS Direct Connect public virtual interface](#)
 - [AWS PrivateLink](#)

Support for hybrid connectivity

Pega Cloud recognizes that your complex business requirements may drive the need for more than one type of connectivity between your enterprise resources and Pega Cloud. Pega Cloud connectivity options can be used flexibly in combination with one another to meet your needs. Your final connectivity solution requires your enterprise network team to review all network aspects, including routing and access controls.

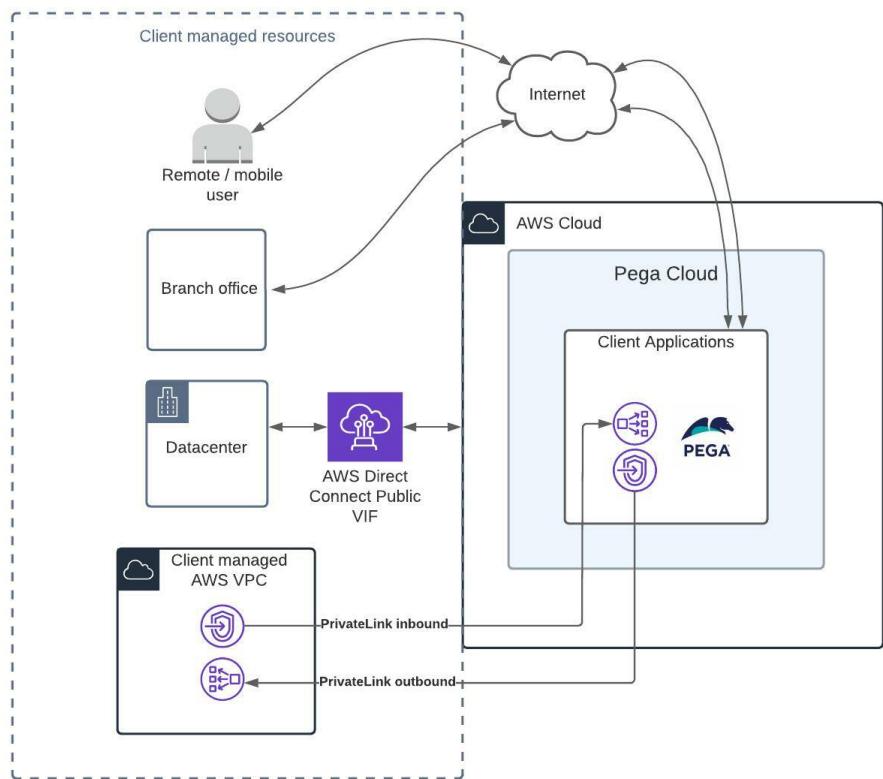
For example, your end users may need to access your Pega Cloud applications from anywhere on the internet, while the same applications may need to integrate with systems running on a secure network in your datacenter. Pega Cloud supports a range of locations as shown in the following illustration.



Pega Cloud supporting connections with your enterprise networks sourced from diverse locations

The following diagram shows an example of the different types of connectivity you can configure to support your complex access needs:

- Remote and branch office users are given access over the internet.
- Services located in your datacenter are given access over a Direct Connect Public VIF.
- Services running in your own AWS VPC are given access over AWS PrivateLink.



Pega Cloud supporting a diverse mix of public and private peering connections

- **Change of support for connectivity options**
- **Environment connectivity overview**
- **Pega Cloud Secure Connect: your access to Pega Cloud**
- **Configuring private access to Pega Cloud services (legacy options)**

Change of support for connectivity options

Pega Cloud® is an as-a-service solution that requires deep integrations into clients' connected systems to support mission-critical business applications. To support these critical integrations, it is essential to establish robust and secure connectivity between Pega and its clients, which is why Pega is updating your connectivity options to focus on those which provide broad accessibility and high reliability.

New connectivity options

Connectivity options supported by Pega Cloud services as of April 2022 include:

- Public Access (Internet)
- Using Cloud Exchange public connections
- Using AWS Direct Connect public VIF
- Using AWS PrivateLink

These new connectivity options:

- Provide high reliability.
- Can be implemented with robust security.

- Address system-to-system access across a broad set of interfaces.
- Represent the lowest time to value, because of their significantly reduced configuration complexity.

These options ensure that Pega and its clients have the most up-to-date and simplified operational path to establishing connectivity.

End of support for existing connectivity options

Starting April 2022, Pega Cloud services is ending support for all new configurations of the following legacy connectivity options:

- VPC peering
- AWS Transit Gateway
- Virtual Private Network service
- AWS Direct Connect Private Virtual Interface (VIF)

Existing clients who currently use a connectivity mechanism listed above will enter extended support. In an extended support period, you can expect support through December 31, 2023, unless you are contractually entitled beyond this date. If you are entitled beyond December 31, 2023, and your connectivity mechanism is listed as end of support, then on contract renewal, your connectivity mechanism will immediately reach the end of extended support. For clients with a contract expiring before the end of the extended support period, you may continue to use this option until the end of extended support. Clients are encouraged to immediately begin exploring the possibility of migrating away from end of support options to supported options.

Migrating existing connections to new connectivity options

Existing clients should review the following table to understand their options to migrate their existing connectivity options to the new connectivity model:

Legacy connectivity options	Alternative connectivity options supported after April 2022
Virtual Private Network (VPN) service	<ul style="list-style-type: none"> • Environment connectivity overview • Public connectivity using AWS Direct Connect public virtual interface • Public connectivity using Cloud Exchange • AWS PrivateLink
Transit Gateway	<ul style="list-style-type: none"> • AWS PrivateLink
VPC Peering	<ul style="list-style-type: none"> • AWS PrivateLink
Direct Connect Private VIF	<ul style="list-style-type: none"> • Environment connectivity overview • Public connectivity using AWS Direct Connect public virtual interface • Public connectivity using Cloud Exchange • AWS PrivateLink

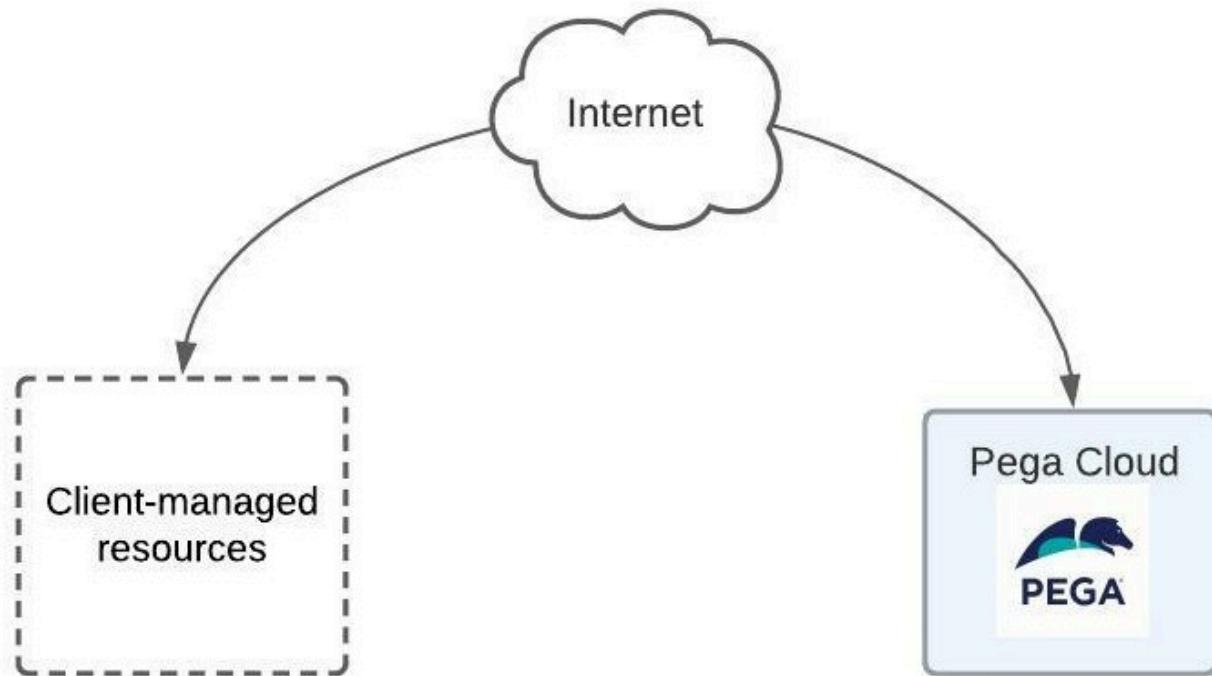
Environment connectivity overview

Pega Cloud® services offers Internet connectivity as the default option to securely connect Pega Cloud to your enterprise network.

Benefits include:

- Lowest cost, implementation time, and overall maintenance.
- Ubiquitous access for your users and systems.
- Highly scalable and reliable connection.

- Transport Layer Security (TLS) provides security for data in transit. For details, see [Data-in-transit encryption](#).

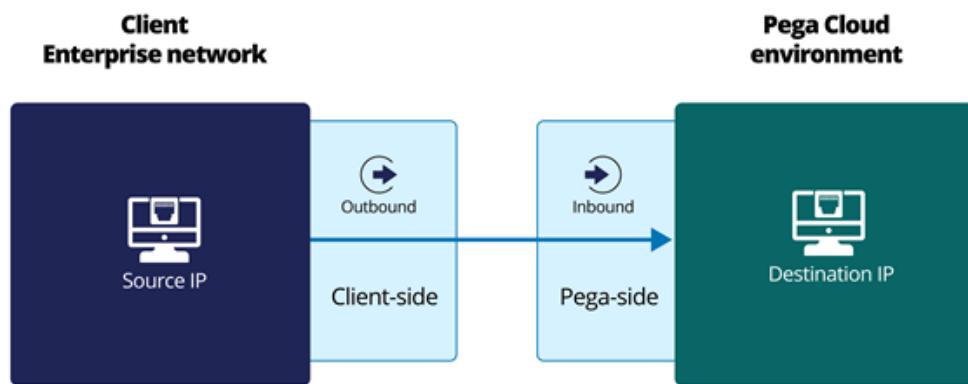


Public access connecting Pega Cloud to your enterprise resources over the Internet

If you choose Internet connectivity, no additional set up is generally required to access Pega Cloud services. However, Pega Cloud provides options to customize your access and connectivity if needed.

Public connectivity allows for connections to multiple sites including corporate datacenters and IaaS or other IaaS providers; however, it is limited to resources that are exposed publicly through secure gateways and well-defined APIs. If public connectivity does not fully meet your organization's needs, see [Pega Cloud Secure Connect: your access to Pega Cloud](#).

Inbound access configuration options



Inbound connections to Pega Cloud

The following items describe options to add Client-to-Pega public connections to an allow list.

Pega-side configuration (inbound traffic): By default, Pega Cloud does not restrict inbound connections at the network level with the exception of the SFTP service as mentioned below. To allow connectivity to Pega Cloud from only specific source IP addresses or networks, Pega can apply allow lists to your Pega Cloud on request.

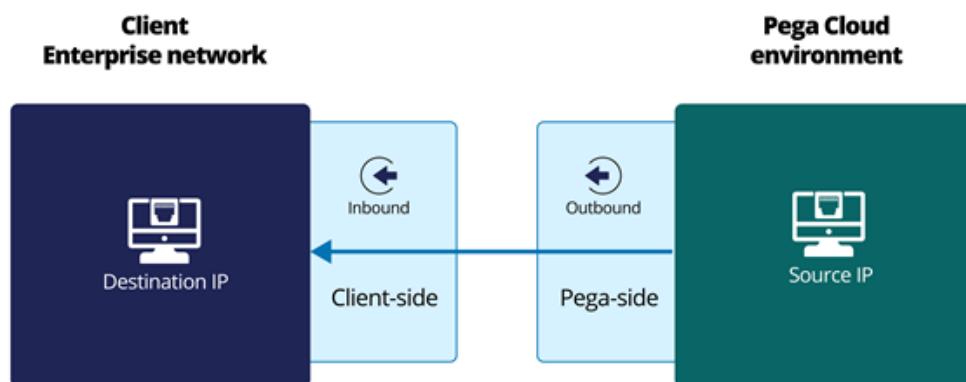
Client-side configuration (outbound traffic): Pega supports static IP addresses to Pega Cloud. If the security requirements of your enterprise network include restrictions on traffic leaving your network, provide Pega with your static source IP addresses and Pega will add them to an appropriate allow list.

Pega-side configuration for the SFTP service (inbound traffic): By default, Pega Cloud denies inbound connections to your Pega Cloud SFTP service. To enable access, provide Pega with a list of known source IP addresses so Pega adds them to an SFTP service-specific allow list.

Client-side configuration for the SFTP service (outbound traffic): Pega Cloud supports static destination IP addresses for outbound traffic to your Pega Cloud SFTP service. If your enterprise network security requirements include restrictions on traffic leaving your network, add the IP address of your Pega Cloud SFTP service to your outbound allow list.

For more information, see the Responsibility model table.

Pega-to-client allow list configuration options



Outbound connections from Pega Cloud

The following items describe configuration options to add Pega-to-client connections to an allow list.

Pega-side configuration (outbound traffic): Pega Cloud services does not restrict outbound traffic. This support model offers the most flexibility when you integrate with external services while maintaining client data security and confidentiality as described in [Pega Cloud Security and data protection](#).

Client-side configuration (inbound traffic): Pega Cloud services provides three static source IP addresses shared by Pega Cloud. Add these IP addresses on your enterprise network allow list.

Integration add-on services, such as log streaming to Splunk or your AWS S3 bucket, require client-side configuration of allow lists for inbound connections.

For more information, see the Responsibility model table.

Responsibility model for adding public connections

The process for adding public connections to an allow list relies on a shared responsibility model between you and Pega Cloud. To initiate any process involving adding a connection to an allow list, create a ticket with your regional Pega Support representative by using the [Create a ticket](#) button in [My Support Portal](#), and then follow the information in the *Client responsibilities* column of the following table. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

Configuration method	Connectivity	Client responsibilities	Pega responsibilities
Client provides Pega static source IP addresses for Pega Cloud services to add to the Pega Cloud allow list.	Client enterprise network to Pega Cloud.	Requests that includes a list of static source IP addresses for Pega Cloud services to add to the Pega Cloud allow list.	Adds client-provided static source IP addresses to the Pega Cloud allow list.

Configuration method	Connectivity	Client responsibilities	Pega responsibilities
Client adds three static IP addresses provided by Pega Cloud services for Pega Cloud to an allow list.	Pega Cloud to client enterprise network.	Obtains static source IP addresses at time of provisioning IP addresses, and then adds the static source IP addresses on your enterprise network allow list.	Provisions a pool of static source IP addresses and assigns them to Pega Cloud, and then sends static source IP addresses to client.
<p>Client provides Pega Cloud services a static source IP to allow connection to the Pega Cloud SFTP Service.</p> <p>Prerequisite: For clients still using legacy public connectivity, client environments must be migrated to use these static IP addresses. For details, see Infrastructure update Process for Pega Cloud.</p>	Client enterprise network to Pega Cloud.	<p>Requests and sends Pega Cloud services a list of static source IP addresses that are on an allow list to connect to the Pega Cloud SFTP Service.</p> <p>For more information, see Services SFTP Service.</p>	Adds client-provided static source IP addresses to an allow list on the Pega Cloud allow list.

Configuration method	Connectivity	Client responsibilities	Pega responsibilities
<p>Client adds the static destination IP of their Pega Cloud SFTP service to an allow list.</p>	<p>Client enterprise network to Pega Cloud.</p>	<p>Requests static destination IP addresses to your Pega Cloud SFTP service and then adds the static destination IP addresses to your enterprise network allow list.</p> <p>For more information, see Services SFTP Service.</p>	<p>Provisions an IP address, assigns the IP address to the Pega Cloud SFTP service, and then sends the static destination IP address to client.</p>
<p>Client provides Pega with service add-on connection information.</p>	<p>Pega Cloud to client enterprise network.</p>	<p>Adds add-on service static source IP addresses on your enterprise-network allow list, and then provides the add-on service connection information to Pega Cloud services.</p> <p>For an example add-on service, see Streaming Pega logs to Splunk.</p>	<p>Provisions a set of IP addresses assigned to the add-on service for outbound traffic.</p>

Pega Cloud Secure Connect: your access to Pega Cloud

Pega offers Pega Cloud® Secure Connect to enable connectivity between your users and systems and Pega Cloud with options beyond public Internet access.

Pega Cloud Secure Connect provides connectivity to Pega Cloud when the default public connectivity option does not meet the preapproved connectivity design pattern for your organization. Benefits of using Pega Cloud Secure Connect to implement a connectivity strategy to Pega Cloud include:

- Deliver secure, dedicated, and reliable access with your private and dedicated connection to Pega Cloud.
- Standardize your Pega Cloud connectivity strategy across third-party cloud providers by leveraging common design patterns.
- Future-proof your connectivity strategy with robust cloud scaling options that support multiple vendors.
- Securely integrate with enterprise services in the public cloud or behind your firewall.
- Meet zero trust architecture requirements by securing access to your third-party vendors directly through the application instead of by location.

Pega Cloud Secure Connect supports the following connection options:

- Cloud Exchange public connections
- AWS Direct Connect public VIF
- AWS PrivateLink
- GCP Private Service Connect

While both AWS Direct Connect Public VIF and Cloud Exchange rely on the use of internet-routable IP addresses, these connectivity options avoid traversal of the public internet. Instead, these solutions provide a private, dedicated path between your network and Pega Cloud. The result is a connectivity model that offers an enhanced

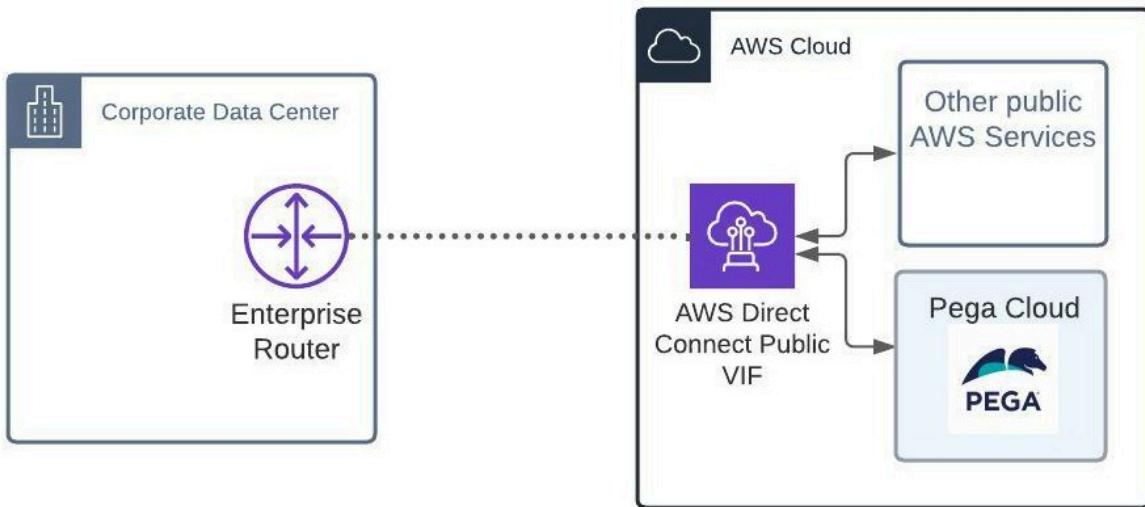
security posture and improved connection predictability, as compared with the public internet.

- **Public connectivity using AWS Direct Connect public virtual interface**
- **Public connectivity using Cloud Exchange**
- **Control public peering access to Pega Cloud with Border Gateway Protocol**
- **Google Peering**
- **Private connectivity using AWS PrivateLink**
- **Connect enterprise resources to Pega Cloud with AWS PrivateLink**
- **Private connectivity using GCP Private Service Connect**

Public connectivity using AWS Direct Connect public virtual interface

Pega Cloud® Secure Connect enables the use of AWS Direct Connect with a public virtual interface (VIF) service to establish a dedicated network connection from your enterprise and connected networks to Pega Cloud over public connections.

AWS Direct Connect public VIF provides a cost effective and reliable connectivity option to establish a dedicated network connection from your enterprise and connected networks to Pega Cloud services running in AWS over public networks. You can also use this connection to access other public AWS resources from multiple cloud providers.



AWS Direct Connect public VIF providing public connectivity between Pega Cloud and your enterprise network and other AWS public services

Establishing a new Direct Connect connection, depending on available options, requires lead time and a moderate-to-high level of technical complexity. For clients who prefer working with a Cloud Exchange provider who can add value and assist with implementation details, Pega Cloud Secure Connect supports Cloud Exchanges. For details, see [Public connectivity using Cloud Exchange](#).

Note: As of April 2022, Pega Cloud environments are incompatible with AWS

- ⓘ Direct Connect private VIF services. For more information, see [Change of support for connectivity options](#).

Benefits include:

- Low up-front and ongoing maintenance cost.
- SLA from AWS for high reliability.
- Low latency.

- High bandwidth support, from 50 Mbps to 100 Gbps.

Client responsibilities:

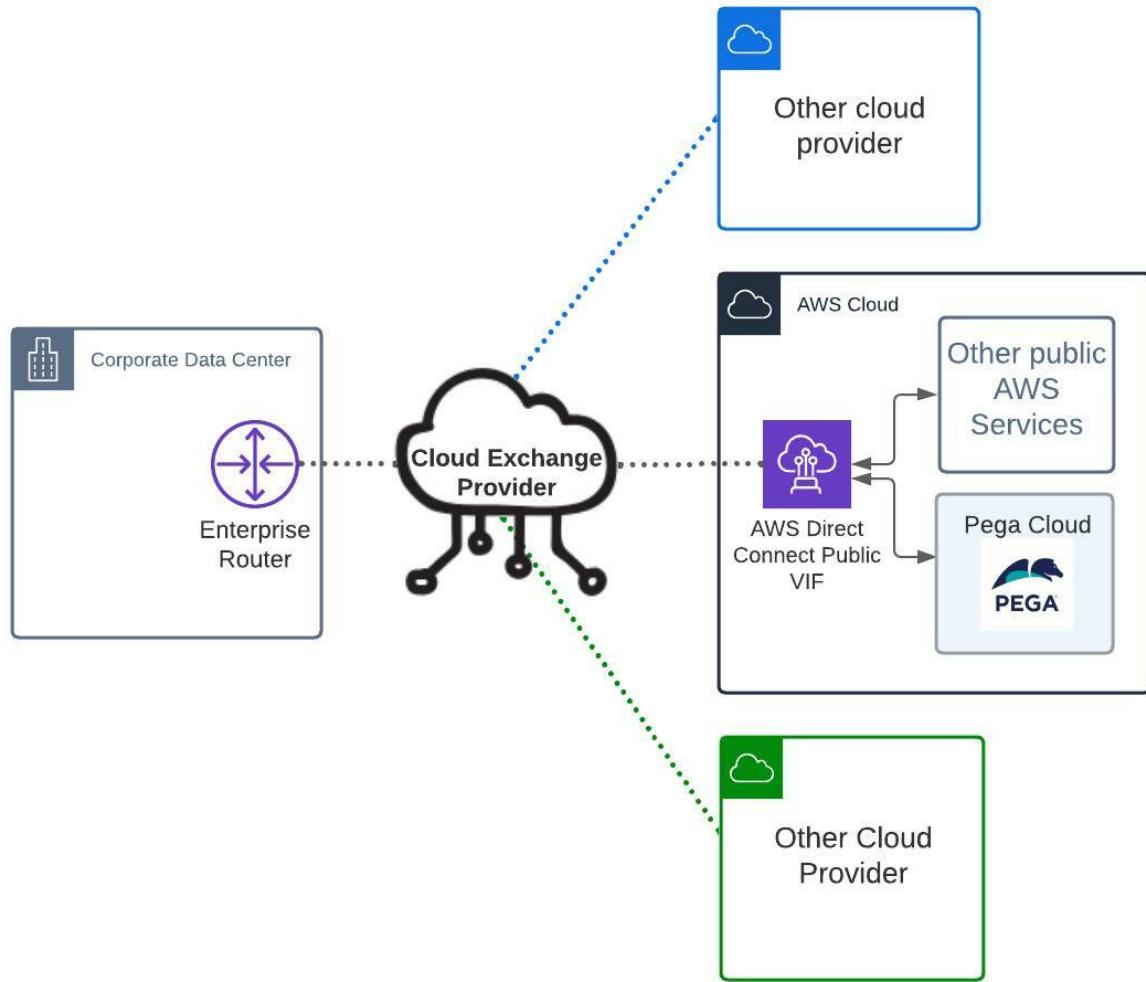
- Unless you have a presence in an AWS Direct Connect location, the most common way of obtaining AWS Direct Connect is through a third-party provider. Your organization must work with an approved provider to deploy and perform required configuration steps. To find a list of approved third-party providers, see [AWS Direct Connect Delivery Partners](#).
- Configure the following AWS Direct Connect components:
 - A connection type: Both hosted or dedicated connection types work with Pega Cloud Secure Connect. Configure your connection in the same region as your Pega Cloud. For connection details, see [AWS Direct Connect connections](#).
 - A public VIF: The most common configuration will be for your organization to create a public VIF using a Direct Connect Connection that you own. Some AWS Direct Connect delivery partners offer a service that will create a hosted VIF for you. Design and configure your network and equipment to leverage your connection to your AWS Direct Connect public VIF. For connection details, see [AWS Direct Connect virtual interfaces](#).
- Design and configure your network and equipment to leverage the Cloud Exchange connection and AWS Direct Connect public VIF, including, but not limited to, IP addressing, routing, security, and Border Gateway Protocol (BGP).
- Maintain the uptime and availability of your AWS Direct Connect connection and public VIF.

For guidance on best practices and options for controlling access between your enterprise network and Pega Cloud over these public peering options, see [Control public peering access to Pega Cloud with Border Gateway Protocol](#).

Public connectivity using Cloud Exchange

Pega Cloud® Secure Connect enables the use of Cloud Exchanges from industry-leading providers such as Equinix Fabric, Megaport MCR, and many others to integrate your enterprise networks with Pega Cloud over public connections.

Cloud Exchanges provide a cost-effective and reliable connectivity option to establish a dedicated network connection from your enterprise and connected networks to the Pega Cloud services running in AWS over public networks. Depending on your Cloud Exchange provider's available offerings, you may also be able to use this connection to access other public resources from multiple cloud providers.



Cloud Exchange providing public connectivity between your enterprise and connected networks and Pega Cloud

Benefits include:

- Short implementation time, leveraging your established IaaS relationships.
- High bandwidth, exceeding one Gbps, depending on your provider and location of choice.
- Diverse access to many services and other cloud-based systems throughout your corporate estate.

Client responsibilities:

- Purchase Pega Cloud Secure Connect from Pega to enable support.
- Identify and select a Cloud Exchange provider if your Enterprise has no provider.

"Cloud Exchange" is the industry-standard name for services that offer dedicated, highly available connectivity to many cloud services providers. However, your provider might use a different term, such as "Cloud Connectivity".

- Configure a Cloud Exchange connection to AWS with your provider.

Pega does not support connections directly to Pega Cloud environments over RFC 1918 space. For details, see [Public connectivity using AWS Direct Connect public virtual interface](#).

- Design and configure your network and equipment to leverage the Cloud Exchange connection, including but not limited to, IP addressing, routing, and Border Gateway Protocol (BGP).
- Maintain the uptime and availability of your Cloud Exchange connection to AWS.

For guidance on best practices and options for controlling access between your enterprise network and Pega Cloud over these public peering options, see [Control public peering access to Pega Cloud with Border Gateway Protocol](#).

Control public peering access to Pega Cloud with Border Gateway Protocol

Learn about the benefits and design options of the Pega Cloud® AWS Direct Connect Public Virtual Interface (VIF) integration feature for communication with external systems. AWS Direct Connect Public VIF provides dedicated connectivity from your enterprise network to public AWS networks. By working with your enterprise network team, you can implement an AWS Direct Connect Public VIF, either directly or by using the services of your preferred Cloud Exchange provider.

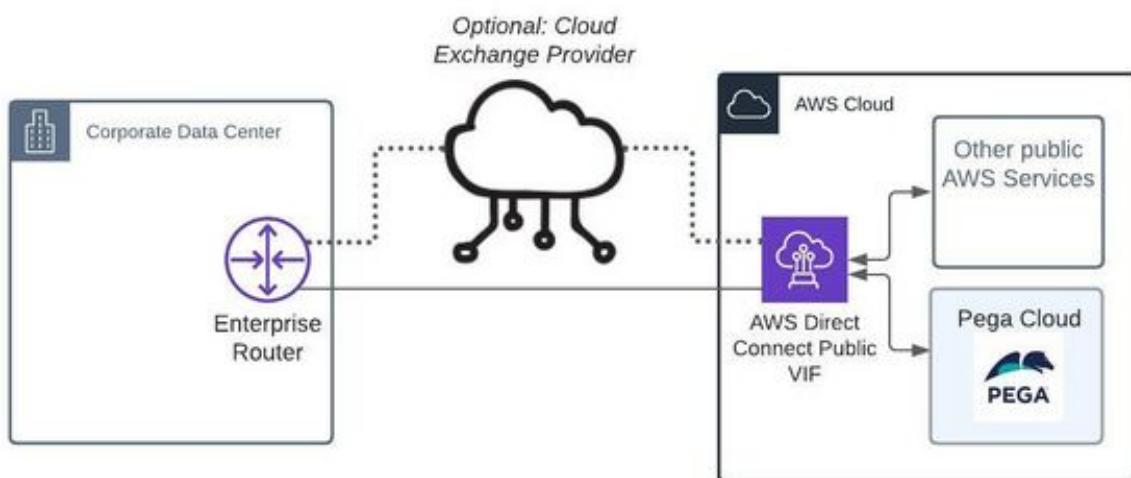
This connectivity model supports limiting access to your Direct Connect connection to ensure that only the appropriate traffic flows across it. Because Direct Connect relies on Border Gateway Protocol (BGP) to determine the traffic that traverses the link in both

directions, Pega recommends enforcing such restrictions by configuring and tuning BGP settings to meet your organization's requirements.

While Pega does not advise on the complexities of your local network configuration, certain best practices do apply. This design pattern contains guidance for controlling the scope of traffic that traverses your Direct Connect connection and avoiding some common configuration errors that can impact the flow of traffic.



Note: "Direct Connect" here refers to AWS Direct Connect Public VIF.



Different approaches to public peering when you include an AWS Direct Connect Public VIF in your design

Review the following sections to learn how to use BGP to configure routing from your enterprise network to public AWS networks using an AWS Direct Connect Public VIF.

Prerequisites

Understand the default behaviors of BGP before establishing a connection.

Review current AWS documentation, because AWS may add capabilities or change their products, product features, or default values at any time.

If you implement Direct Connect through a Cloud Exchange provider, consult your provider for additional guidance as needed.

Limit access and visibility between AWS and your network

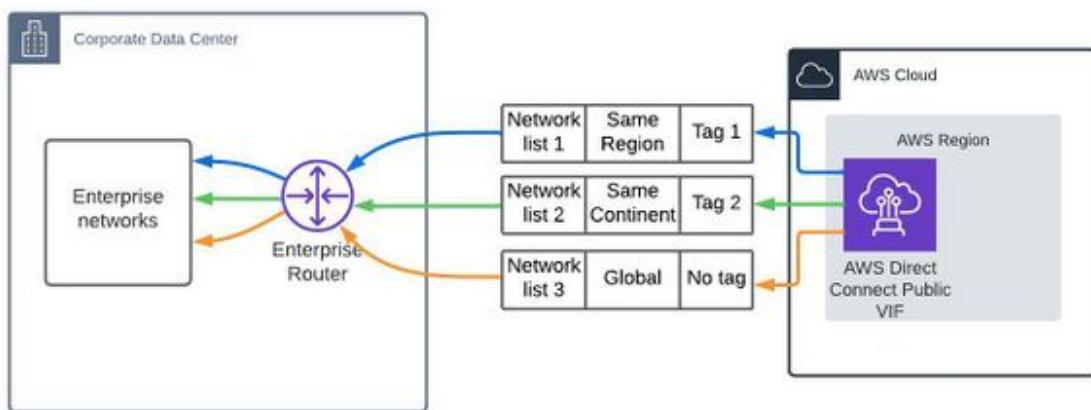
AWS offers three levels of control for both inbound and outbound routing advertisements:

- Region (the region where your Direct Connect terminates)
- Continent (the continent containing the region)
- Global (all AWS regions)

Configure inbound routes

Routes advertised by AWS to your enterprise router define the AWS public IP address ranges that are reachable from your network over Direct Connect.

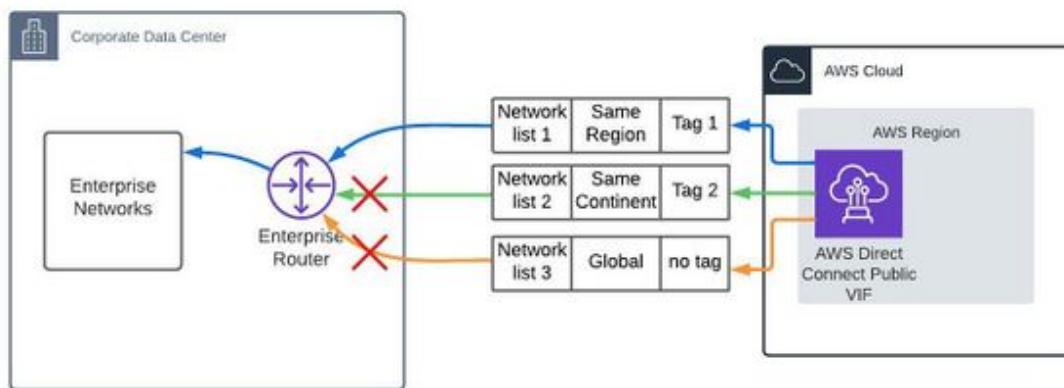
Default behavior: AWS advertises all their networks (prefixes) over Direct Connect, using BGP community tags to categorize those networks as shown in the following figure:



BGP community tagging allows for segmentation to regions, continents, or all (global)

Tuning options: You can use the tags provided by AWS to limit the networks that you receive from AWS.

Example: Your enterprise network team configures the enterprise router to only accept routes for AWS networks in us-east-1, because that is the only region your enterprise networks need to access over Direct Connect, as shown in the following figure:

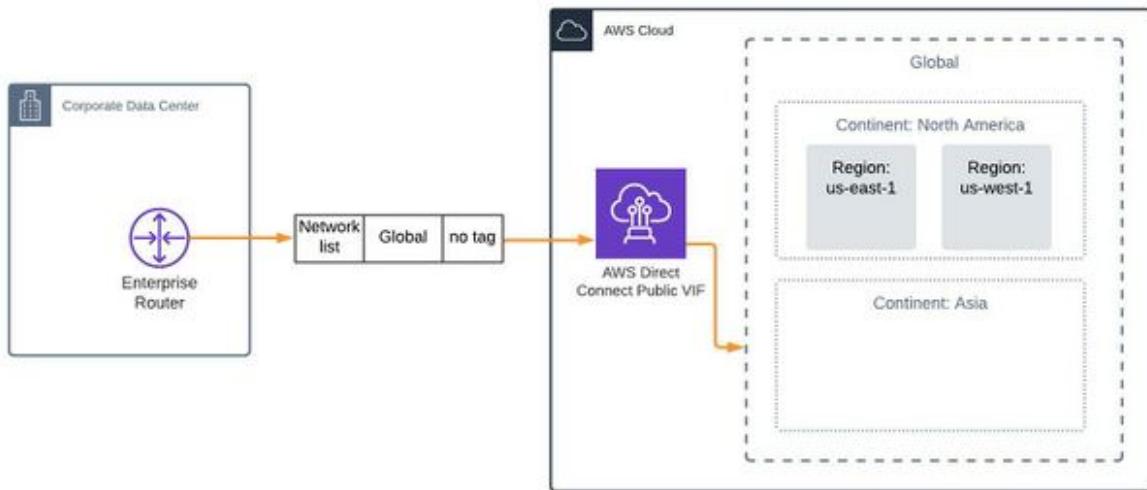


BGP community tagging allows you to filter inbound routing advertisements

Configure outbound routes

Definition: Routes that you advertise to AWS from your enterprise router.

Default behavior: If you do not apply any community tags, any networks that you advertise to AWS over Direct Connect are advertised by AWS to all regions, globally, as shown in the following figure:

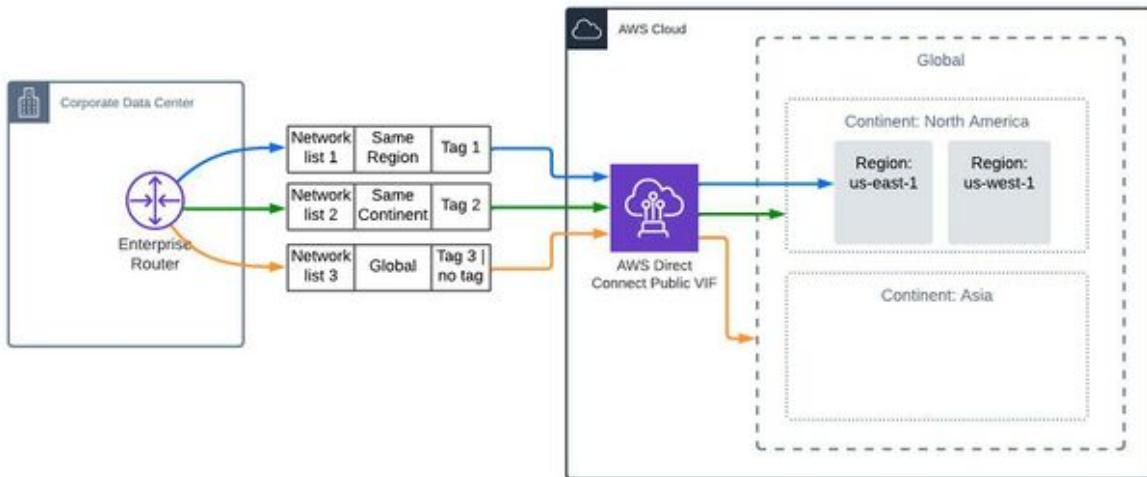


Without tuning BGP community tags, Direct Connect does not filter any outbound traffic routing advertisements

Tuning options: You can use BGP community tags to limit the scope of AWS' advertisement of your networks.

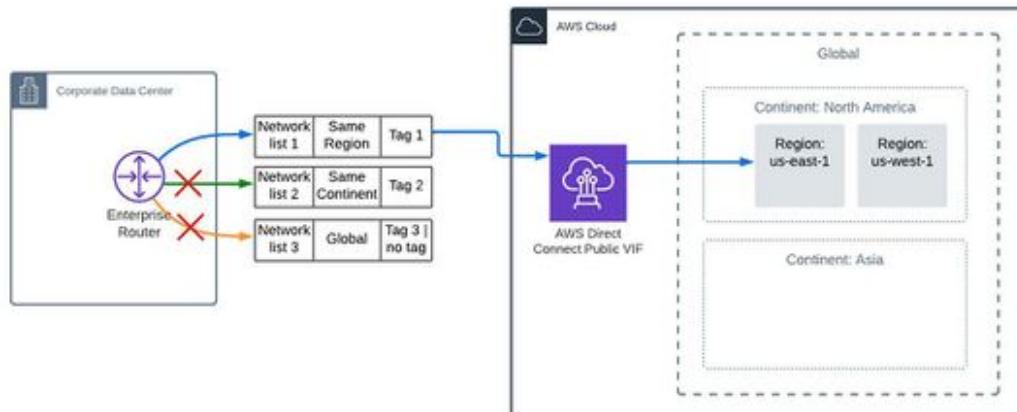
Note: In the two example figures below, your enterprise network team configured Direct Connect in us-east-1 (not shown, for readability).

Example 1: Your enterprise network team configures the enterprise router to advertise three enterprise networks to AWS, each with a different scope:



Using BGP community tagging to advertise routes to your networks to different areas within AWS

Example 2: Your enterprise network team configures the enterprise router to ensure that the networks it advertises to AWS over Direct Connect are only advertised in the **us-east-1** AWS region, as shown in the following figure:



Using BGP community tagging to limit outbound routing advertisements over Direct Connect to a specific region

Summary

To constrain the AWS resources that your Direct Connect connection can access in a specific AWS region or continent:

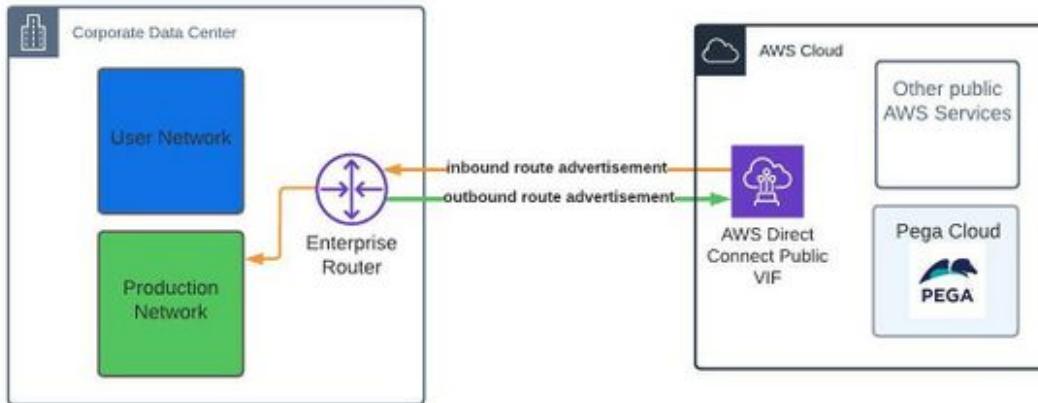
- Consider filtering both inbound and outbound routing advertisements using standard AWS community tags.
- Plan your inbound and outbound filtering carefully to avoid asymmetric routing, as discussed in later sections of this article.

Limit the scope of the routes seen on your local network and those advertised to AWS

Even when it makes sense to allow certain systems to access all AWS networks over Direct Connect (for example, to satisfy a performance or security requirement), you might not want to extend that ability to all enterprise networks. For example, you probably want your end users to reach www.amazon.com over the internet, not over Direct Connect.

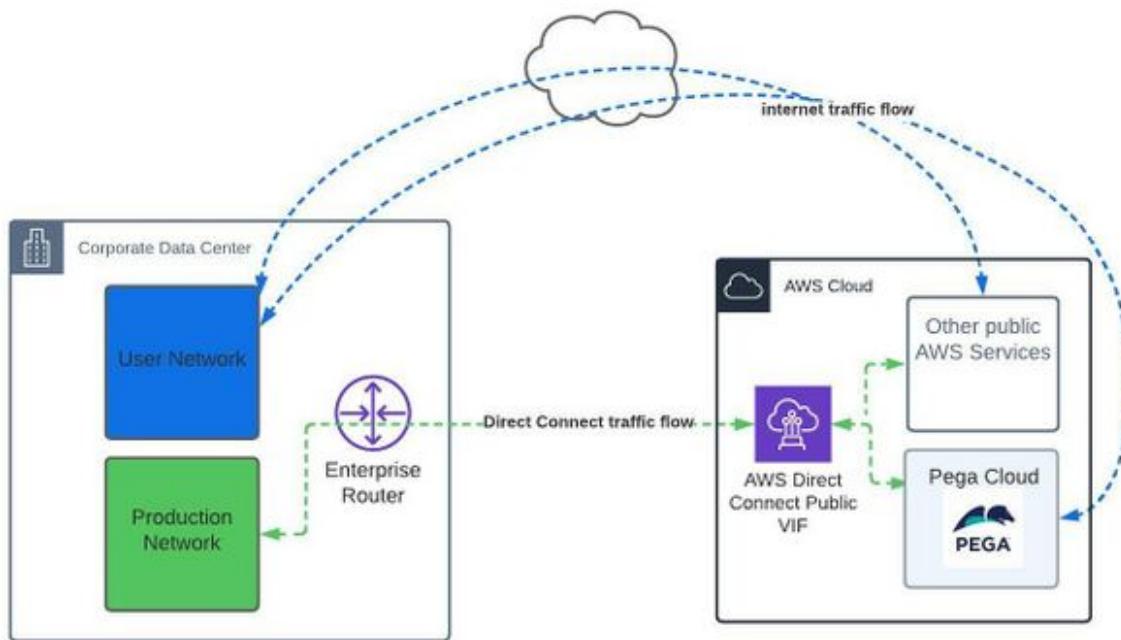
Constrain AWS access over Direct Connect

Your enterprise network team can configure the enterprise router to advertise the routes it receives from AWS Direct Connect to the Production Network, but not to the User network as shown in the following figure:



Your routing configuration determines the path that traffic takes to reach AWS from User and Production networks

Your enterprise network team also configures the enterprise router to advertise the Production Network to AWS over Direct Connect, but not the User Network. The following figure shows the resulting traffic flow. User traffic traverses the internet, while Production Network traffic traverses Direct Connect.



Use an enterprise router to limit the scope of routes advertised to only the Production network

Summary

If certain users or systems do not need to use Direct Connect to reach AWS resources (for example, user traffic to www.amazon.com or any service powered by AWS), configure connectivity appropriately to ensure that traffic routes over the internet:

- Ensure that those systems do not use IP addresses that fall within your advertised networks.
- Ensure that those systems do not see routing advertisements from Direct Connect.

Avoid asymmetric routing and other common mismatches

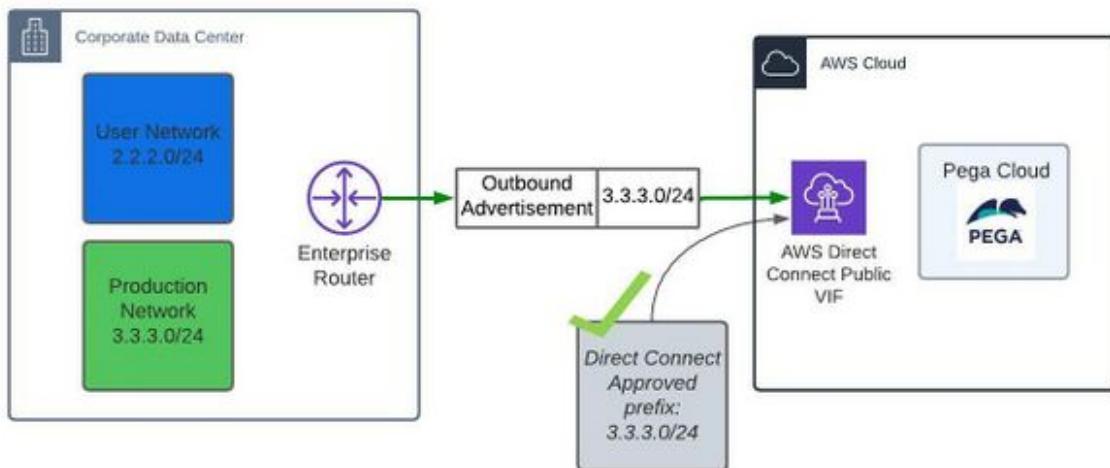
Asymmetric routing occurs when traffic reaches a network over one path, but replies are sent over a different path. This can cause unexpected behavior and broken

communication. In order to avoid asymmetric routing where Direct Connect is involved, consider using the following best practices:

Outbound advertisements match approved routes

One of the steps that you must take during the Direct Connect configuration process is to submit the list of networks you plan on advertising to AWS. AWS will review and approve those networks after confirming that they belong to your organization. Ensure that your enterprise network team configures the enterprise router to advertise the same networks that were submitted and approved during Direct Connect setup.

Example: Your enterprise network team configures the enterprise router to advertise the production network to AWS. This is the same network that was previously submitted and approved. This initial configuration state applies to all other examples in this section, as shown in the following figure:

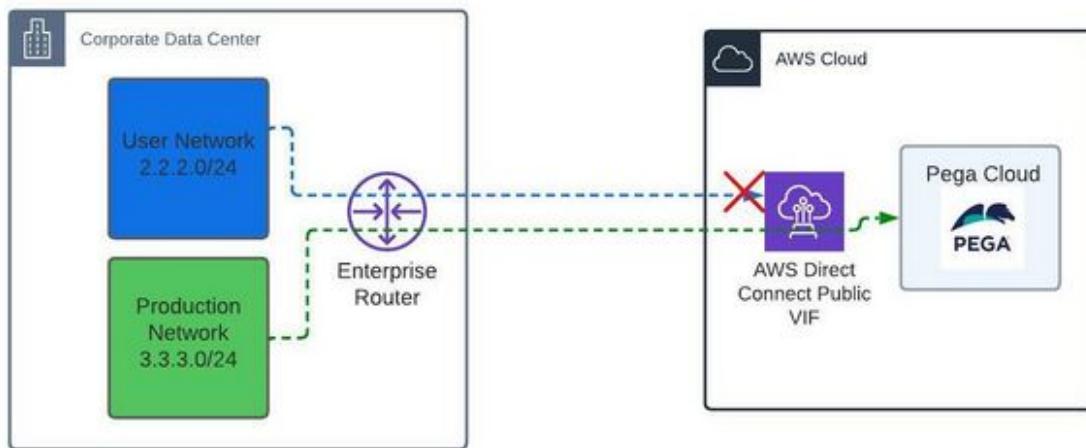


Match advertised routes to the routes approved by AWS for use in Direct Connect

Traffic is sourced from advertised networks

Ensure that the traffic you send over Direct Connect comes only from IP addresses within those approved and advertised networks. AWS will reject traffic from other networks.

Example: Direct Connect forwards traffic from the production network and rejects traffic from the user network, because these source IP addresses do not fall within the approved and advertised range, as shown in the following figure:

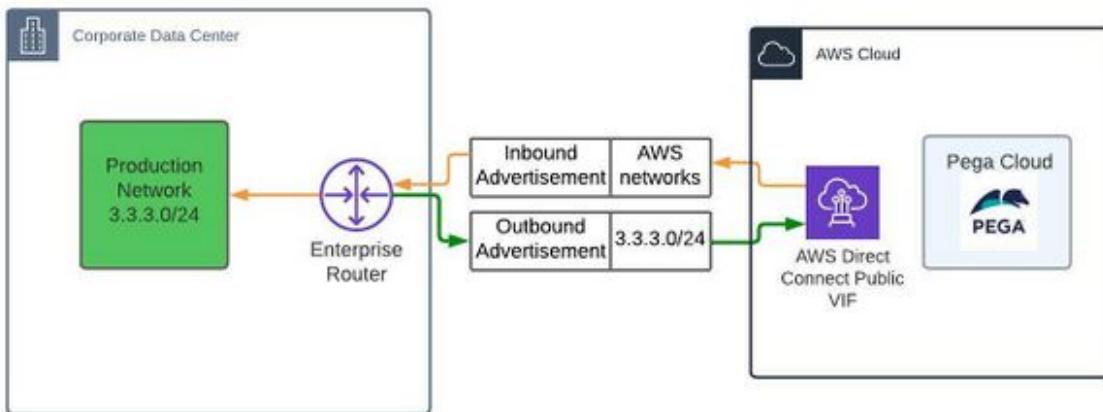


Source traffic from advertised and approved networks when communicating over Direct Connect

Inbound and outbound scopes match

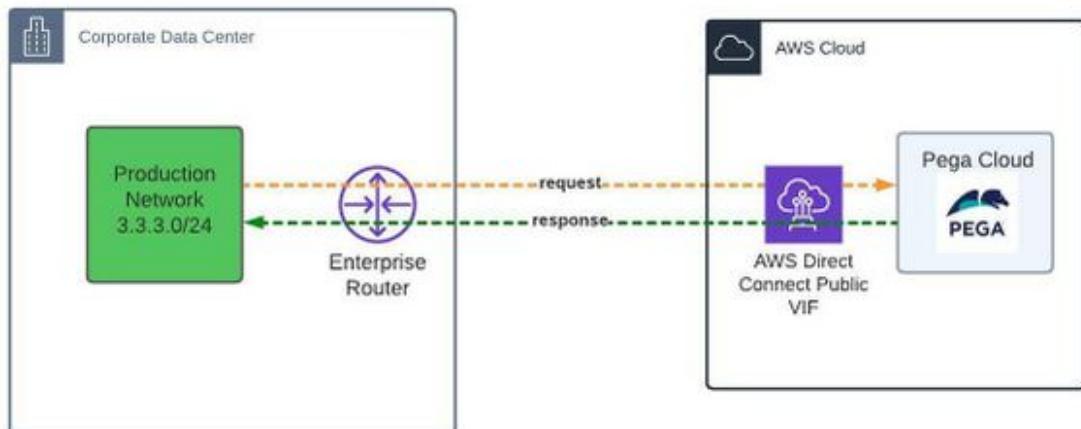
Match the scope of your inbound and outbound routing advertisements, so that the AWS networks to which you connect over Direct Connect also have a path back to you over Direct Connect.

Example 1. Symmetric routing configuration (correct): The production network has been advertised to AWS and inbound routes from AWS over Direct Connect are visible to the production network; the routing advertisements are as follows:



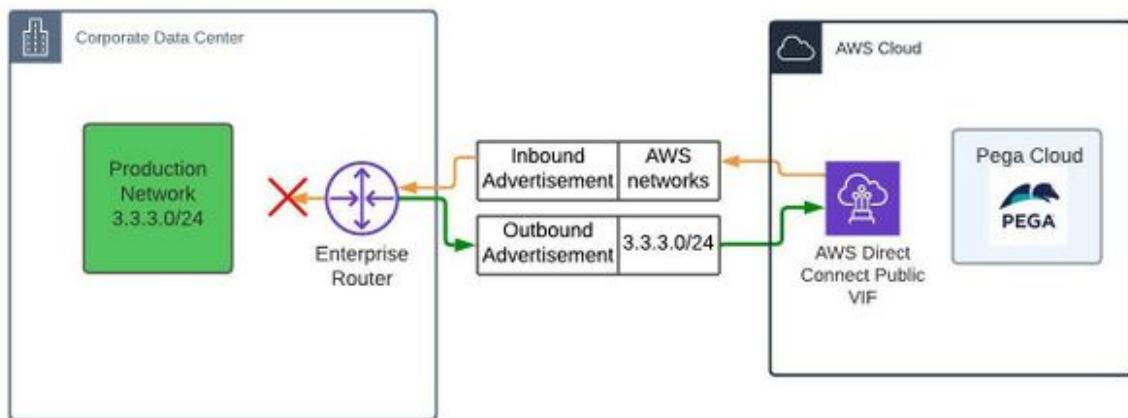
Symmetrical routing advertisement ensures that the correct networks on either side of Direct Connect have routes to one another over that connection

The resulting flow of traffic between the Production network and AWS is symmetrical: traffic sent to AWS from the Production network traverses Direct Connect, and return traffic from AWS flows back across the same connection, as shown in the following figure:



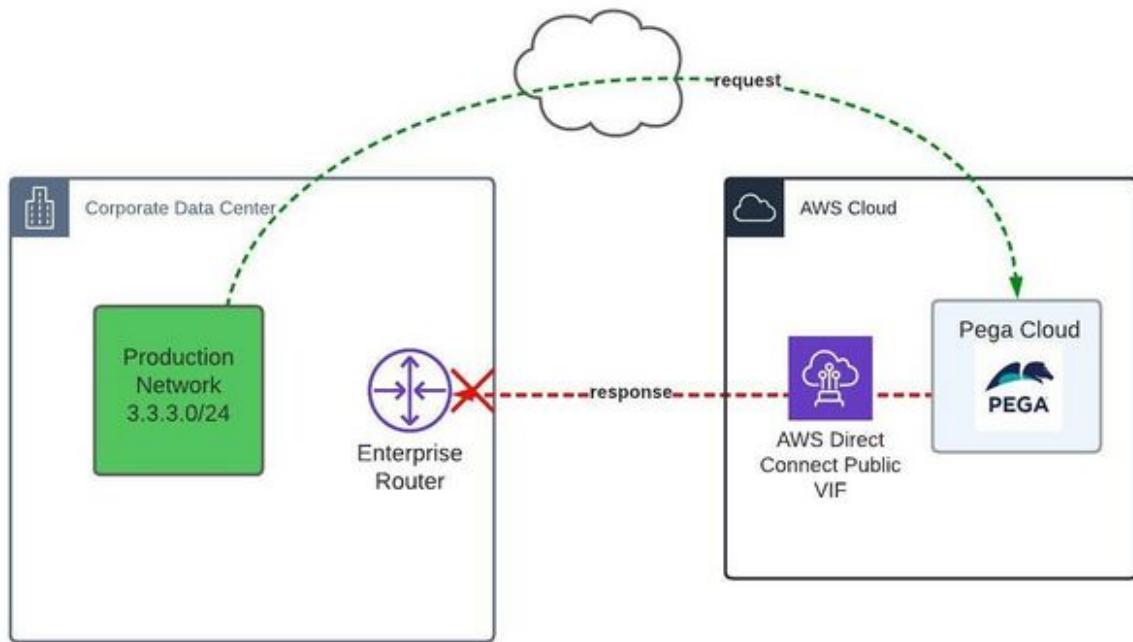
Symmetrical traffic flow resulting from correct symmetrical route advertisements

Example 2. Asymmetric routing configuration (incorrect): The Production network has been advertised to AWS over Direct Connect, but a route to AWS networks over Direct Connect has not been made available to the production network, so the routing advertisements are as follows:



Asymmetric routing advertisement results in networks on either side of the Direct Connect have mismatched routes to one another

The resulting flow of traffic between the production network and AWS is asymmetrical. Assuming a default route to the internet is available to the production network, that route is used to reach AWS; however, AWS sends responses back to the Production network over Direct Connect. This can cause unexpected behavior and broken communication, because many enterprise network configurations will block or drop this return traffic, as shown in the following figure:



Asymmetrical traffic flow resulting from incorrect asymmetrical route advertisements

Summary

To avoid routing-related problems with the flow of traffic, configure your Direct Connect connection such that the traffic paths are appropriately mirrored.

Additional options for limiting Direct Connect traffic

If your Pega Cloud applications are the only resources you need to access over Direct Connect and you are considering further traffic restrictions, capabilities for doing this depend on which side of the connection is the traffic initiator.

Routing and filtering capabilities when only egress traffic is needed

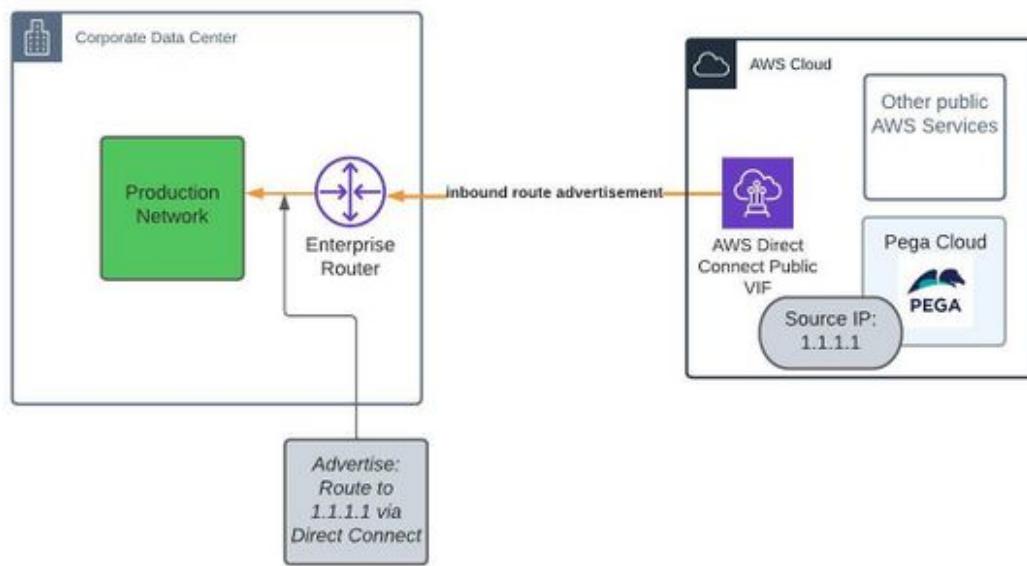
In this section, egress refers to traffic initiated by Pega.

Scenario: You only plan on using Direct Connect for integration traffic, which is outbound traffic initiated by your Pega application, connecting to integration endpoints on your enterprise network (for example, email systems or web service

providers). You plan on routing ingress traffic (inbound traffic to Pega from end users or other service consumers) over the internet.

Capabilities: Pega provides a set of static source IP addresses for egress traffic.

Example: If the source IP address for your Pega Cloud application traffic is 1.1.1.1, you can specify that your production network only sees a route to 1.1.1.1 over Direct Connect, even though you will receive all routes from AWS over Direct Connect. When a connection reaches a server on your production network from 1.1.1.1, the response will be sent back over Direct Connect. The routing configuration is as follows:

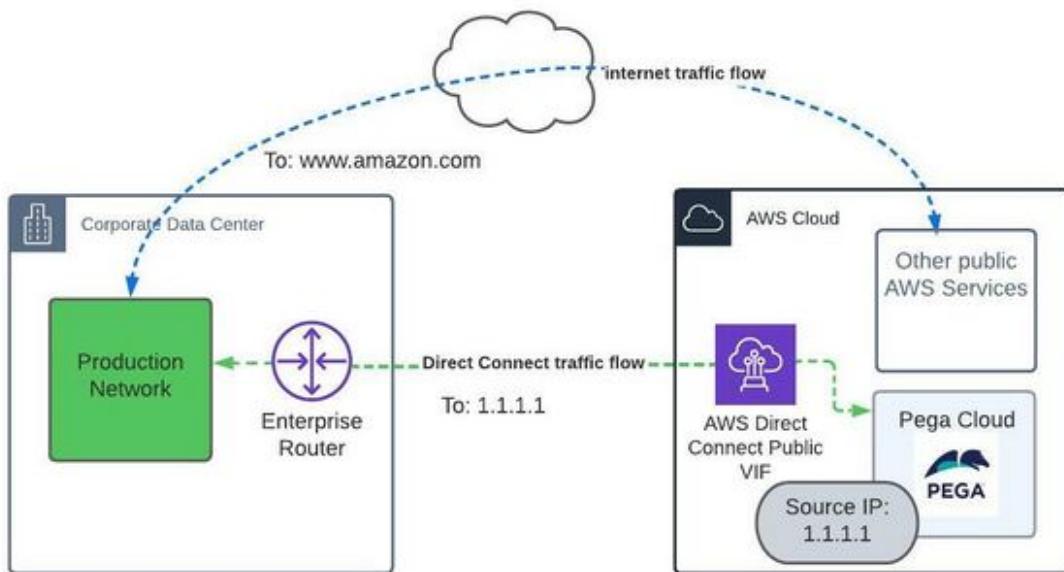


Highly restrictive route filtering for Pega Cloud egress traffic

To avoid asymmetric routing (discussed in the previous section), you may need to take additional steps. For example, you may want to use network address translation (NAT) to map your production network source IP addresses to an IP address outside the range of your Direct Connect outbound route advertisement.

With this configuration, traffic sent over the internet that reaches AWS is not incorrectly sent back via Direct Connect.

In this example, traffic between 1.1.1.1 and your production network flows over Direct Connect, but traffic to other AWS destinations is routed over the internet. The resulting traffic flow is shown in the following figure:



Egress traffic flow when Direct Connect routing is limited to Pega source IP addresses

Routing and filtering capabilities when ingress only or both ingress and egress are needed

In this section, egress refers to traffic initiated by Pega Cloud; ingress refers to traffic initiated by systems or users on your enterprise network.

Scenario: You plan on using your Direct Connect for inbound traffic to Pega Cloud, initiated by end users or other systems on your network.

Capabilities: Because Pega application endpoints do not use static destination IP addresses, it is not possible to limit Direct Connect traffic in this situation, other than as discussed in earlier sections.

Summary

If certain users and systems do not need to use Direct Connect to reach AWS resources (for example, user traffic to www.amazon.com or any service powered by AWS), configure connectivity appropriately to ensure that traffic routes over the internet:

- Ensure that those systems do not use IP addresses that fall within your advertised networks.
- Ensure that those systems do not see routing advertisements from Direct Connect.

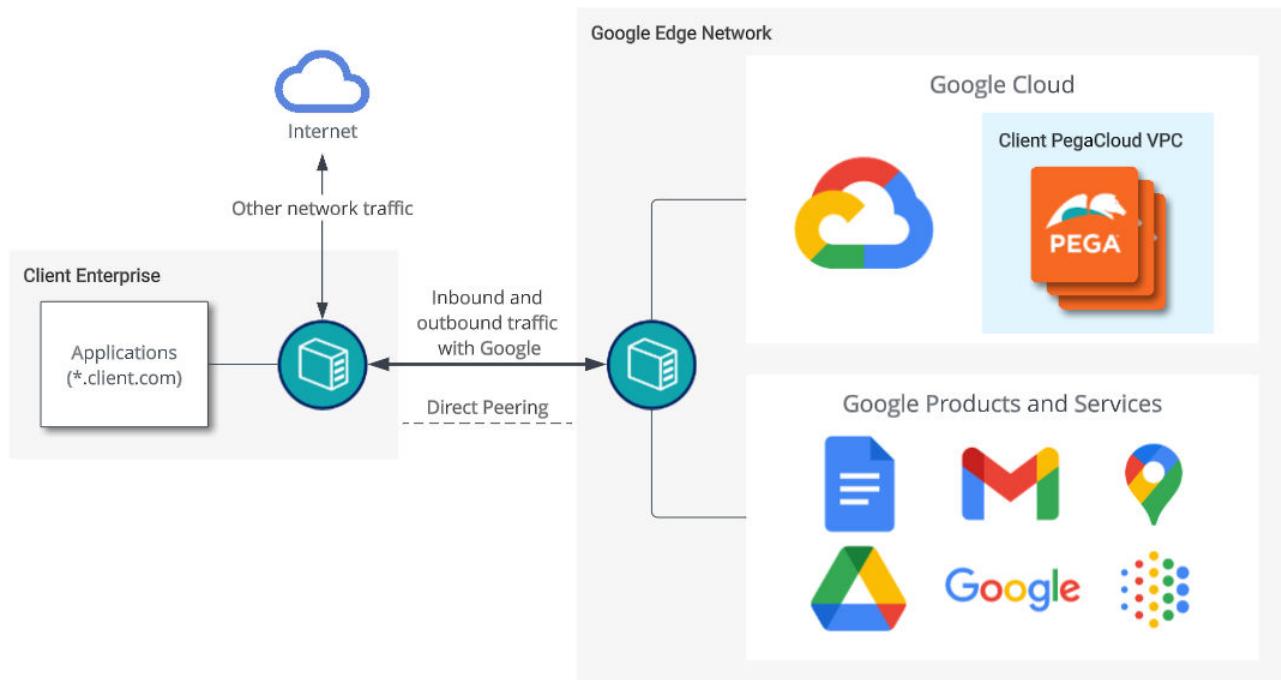
Google Peering

Pega Cloud® Secure Connect enables the use of Google Peering to establish a public peering connection with the Google network.



Note: [Google Peering](#) is only available via Pega Cloud Secure Connect in GCP Deployment regions for Pega Cloud. Clients who leverage Pega Cloud on AWS deployment regions will continue using one of the other options to them under [Pega Cloud Secure Connect](#).

Access points for the Google Network are listed in the [Google Peering Database](#).



An overview of Google Peering in Pega Cloud

Benefits include:

- Improved reachability, reliability, and resilience of the Google network due to its preexisting peering agreements with ISPs.
- Low up-front and ongoing maintenance cost.
- High bandwidth support.
- The option to use [Google Direct Peering](#) or [Google Carrier Peering](#).
- The ability to interface directly with Google and remove intermediate networks from the traffic path.

Note: It is the client's responsibility to establish and maintain the peering connection with Google. Pegasystems does not provide direct support for establishing or maintaining the Google Peering connections.

Pegasystems responsibilities:

- Enable Google Peering in GCP Deployment regions for Pega Cloud.
- Triage Pega Cloud client networking issues to help clients identify whether an issue is related to their Google Peering connection.

Client responsibilities

- Set up and maintain peering connection with Google.
- Work with Google directly to resolve peering connection issues.
 - Note: Google does not offer an SLA for Google Peering.
- Set up controls for public peering connections.
 - Note: Border Gateway Protocol (BGP) prefix filtering is not supported in Google Peering.
- Understand the performance impact of setting up Google Peering.
- Assess the cost implications of setting up Google Peering.

Setting up Google Peering

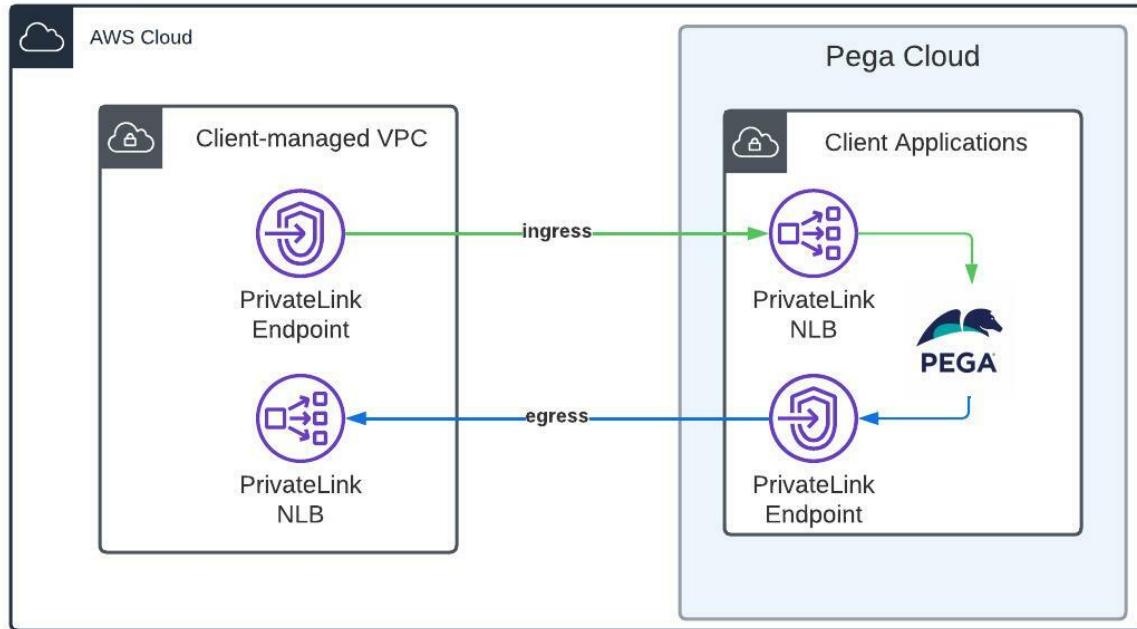
To establish a peering connection with Google:

1. Follow the prerequisites for establishing a Google Peering connection. For more information, see the [Google Peering documentation](#).
2. Submit a Peering Request in the Google ISP Portal. For information, see [Google Peering Request](#).
 - Note: Clients work directly with Google to set up the peering request.
3. Submit a Google ISP Portal Access Request in the Google ISP Portal. For more information see [Google ISP Portal Access Request](#).
 - Note: The public peering connection must be established before the client submits the request.

Private connectivity using AWS PrivateLink

Pega Cloud® Secure Connect enables using AWS PrivateLink as a cost-effective and reliable solution to securely connect Pega Cloud to your existing AWS VPC.

AWS recommends PrivateLink for connections to SaaS providers when the traffic is originated and destined for endpoints in AWS.



PrivateLink Endpoint Services providing connections you can use to communicate between Pega Cloud and your AWS resources and other enterprise networks

PrivateLink offers high reliability, given the simplicity of the connection, as well as security, because traffic remains within the AWS network.

Benefits include:

- Very high bandwidth of 20-80 Gbps with two endpoints configured.
- Connectivity can remain within the AWS network if required.
- Low maintenance requirements.
- Data exchanged over AWS PrivateLink is encrypted.

You can also make use of PrivateLink Endpoint Services for connectivity between Pega Cloud and enterprise resources outside of AWS. For guidance on best practices and

options for controlling access between your enterprise network and Pega Cloud over these private peering options, see [Connect enterprise resources to Pega Cloud with AWS PrivateLink](#).

To learn more about PrivateLink and its benefits, see [AWS PrivateLink and VPC endpoints](#).

Pega responsibilities:

- Pega completes inbound or outbound endpoint service requests.

Client responsibilities:

- You [create a ticket](#) using [My Support Portal](#) to establish inbound or outbound PrivateLink connections. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).
- Understand how the [Rules and limitations of AWS PrivateLink](#) affect your connections to and from Pega Cloud.
- To complete inbound connections, you are responsible for configuring your AWS VPC, including, but not limited to, security group rules, firewall, and DNS configuration.
- To complete outbound connections, you are responsible for initially configuring your organization's PrivateLink Endpoint Service, including the network load balancer and any AWS resources or software required, as well as completing any needed connection approval process.

Establishing an outbound connection

Send traffic from Pega Cloud to your AWS VPC by configuring your organization's PrivateLink Endpoint Service to which Pega Cloud connects and completing a cloud-change request.

Before you begin:

Keep in mind the following considerations for each outbound connection:

- You configure your Endpoint Services in the same region as your Pega Cloud. For High Availability, your Endpoint Services must exist in at least two of the same AWS Availability Zones as your Pega Cloud.
- AWS PrivateLink does not support DNS resolution. To access services over a PrivateLink outbound connection, your organization must do one of the following:
 - Configure a private DNS name for your organization's PrivateLink Endpoint Service. For details, see [Private DNS names for endpoint services](#). In this configuration, you can publish additional DNS records that map to your PrivateLink Endpoint Service. These records can be publicly resolvable or configured as private static DNS entries in Pega Cloud.
 - Create multiple PrivateLink Endpoint Services that map to one or more of your backend services.

1. Complete your PrivateLink Endpoint Service configuration.
For details, see [Create an endpoint service configuration for interface endpoints](#).
2. Make a cloud-change request to create an outbound connection by selecting [Create a ticket](#) in [My Support Portal](#).

In the request, include the Service name of your Endpoint Service.

Result:

In response to your request, Pega sends you the Amazon Resource Name (ARN) of the Pega Cloud principal that you must allow to make a service connection request to your Endpoint Service. For example,

`arn:aws:iam::aws-account-id:principal-id`.

3. Add the provided Pega Cloud principal to your Endpoint Service.
For details, see [Add and remove permissions for your endpoint service](#).
4. Update your cloud-change request to state that you have updated your permissions.
5. Pega creates a connection request in your Endpoint Service.
6. Accept the request in your Endpoint Service.

Result:

Pega completes the outbound connection in Pega Cloud. Pega verifies access from Pega Cloud to the services that you specify. When verified, Pega closes the cloud-change request ticket.

Establishing an inbound connection

Send traffic to one or more of your Pega Cloud environments from your AWS VPC by providing the AWS account ID for the VPC that you want to connect to Pega Cloud.

Before you begin:

Keep in mind the following considerations for each inbound connection:

- Inbound connections are only offered in the same region as your Pega Cloud.
- Pega Cloud services offers one inbound connection for each Pega Cloud environment. For example, `mycorp-dt1` will be a different inbound connection from `mycorp-dt2`.
- The Pega Cloud SFTP service does not support AWS PrivateLink inbound connections.

1. Make a cloud-change request to create an inbound connection by selecting [Create a ticket](#) in [My Support Portal](#).

In the request, include your AWS account ID for the VPC that you want to connect to Pega Cloud. Your cloud-change request can include one or more of your Pega Cloud environments.

Result:

In response to your request, Pega configures each Pega Cloud environment that you specify and then provides you with the Service name for each environment.

2. In your AWS account, create an endpoint in your VPC using the Pega-provided Service name.

For High Availability, Pega recommends configuring your endpoint in two AWS Availability Zones.

3. Configure the security group for your endpoint to allow inbound and outbound HTTPS traffic on port 443.
4. Update your cloud-change request to state that you have created the endpoints in your VPCs.

Result:

Pega activates the inbound connection for the specified Pega Cloud environments. Pega verifies that you can connect to the environments using the inbound connections. After verification is complete, Pega closes the cloud-change request ticket.

Connect enterprise resources to Pega Cloud with AWS PrivateLink

Learn about the benefits and design options of the Pega Cloud® PrivateLink integration feature for communication with external systems. AWS PrivateLink provides reliable, encrypted, fast connectivity between SaaS providers such as Pega Cloud and resources that are located in client-managed AWS virtual private clouds (VPCs), without the need to traverse a public connection. In addition, the use of AWS PrivateLink eliminates the risk of IP address conflicts between networks on either side of the connection.

While PrivateLink is ideal for making connections between endpoints in AWS, you can use a client-managed AWS VPC as a transit VPC to provide resources outside of AWS with access *to or from* Pega Cloud.

You can use the following design pattern to create a cloud-native, isolated, intelligent routing hub with which to connect a broad set of resources to your Pega Cloud. This connectivity design pattern is meant to provide general guidance to illustrate options that your enterprise network administrators can review to address the complexities of your specific connectivity requirements to Pega Cloud.

Note: Transit VPC refers to a client-managed, AWS VPC with inbound and outbound PrivateLink connections to Pega Cloud. This transit VPC can route traffic to or from Pega Cloud applications, based on the controls that you implement.

Benefits

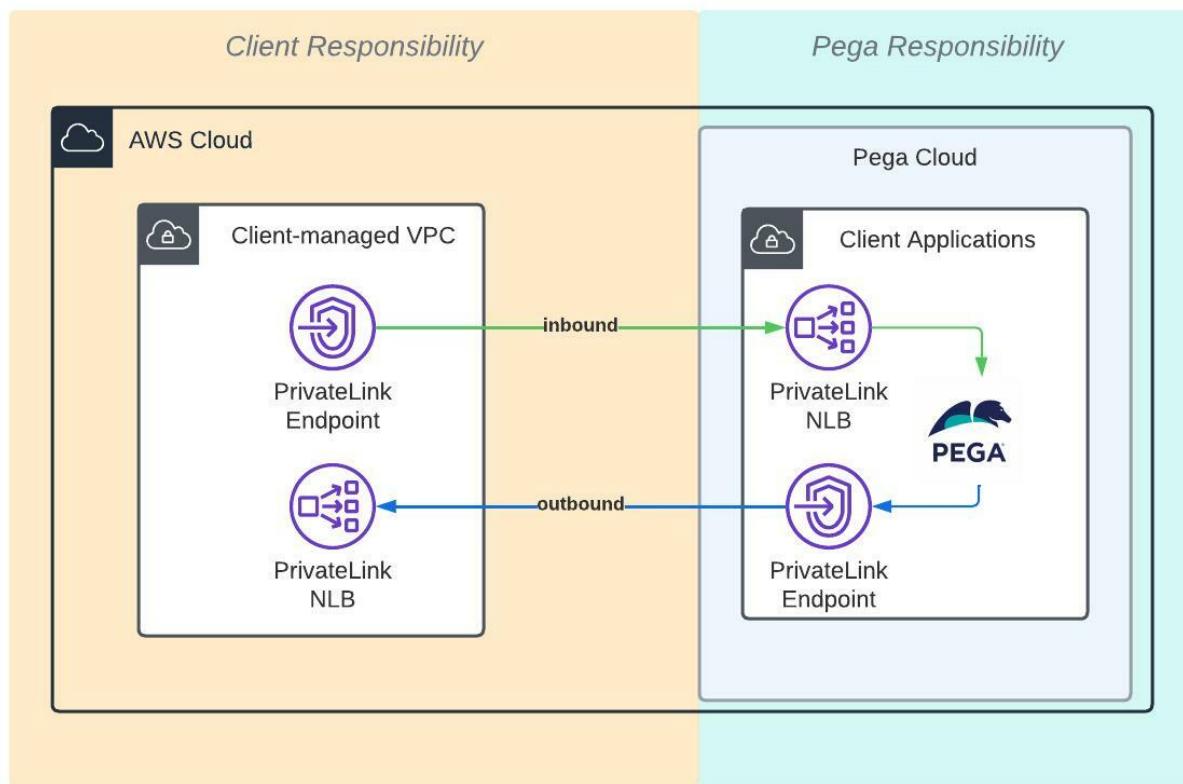
This design offers the flexibility of allowing you to choose your preferred method of connecting to your transit VPC, while retaining the advantages that PrivateLink provides for intra-AWS connectivity, particularly when the integration target is an as-a-Service provider such as Pega. You retain full control and responsibility over the connections that you make from external networks to your transit VPC. This design pattern includes the following key benefits:

- Centralized ingress and egress between trusted and third-party networks.
- Traffic inspection such as IDS and IPS to provide additional security.
- Layer 7 routing and filtering.
- Resolution of non-publicly resolvable DNS names.
- Traffic mirroring for advanced connection troubleshooting.
- Ability to reuse your transit VPC as a connection hub for other, similar integrations.

Before you create any of these configurations, review current AWS documentation in the event that AWS adds features or changes default service behaviors.

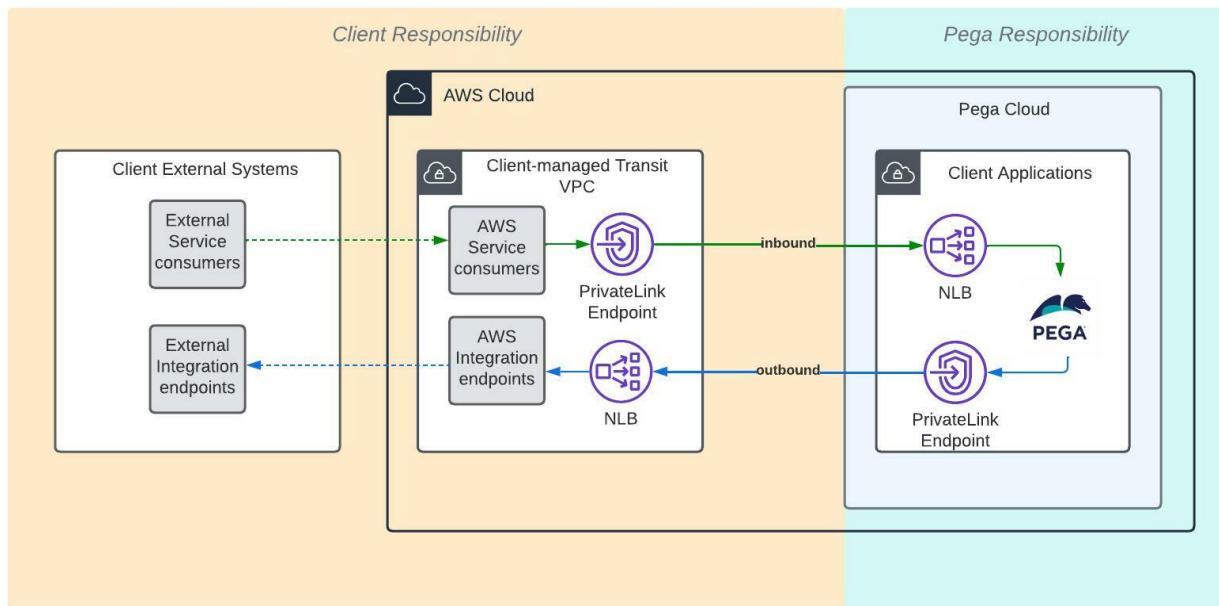
PrivateLink connectivity to overview

The basic design of PrivateLink connectivity to your Pega applications is shown in the following figure:



Cloud-to-cloud connectivity for as-a-Service solutions

You can extend the basic design to illustrate that your transit VPC can provide access to resources both inside and outside of AWS. For example, as shown in the following figure:



AWS PrivateLink support for transitive connections to your external systems

Connection from diverse locations and connection types

Depending on your requirements, you can provide access to your Pega applications through your transit VPC from different external locations using a variety of connection types.

Location types

Different external locations might warrant different connectivity and security requirements. The location types that can drive your requirements include:

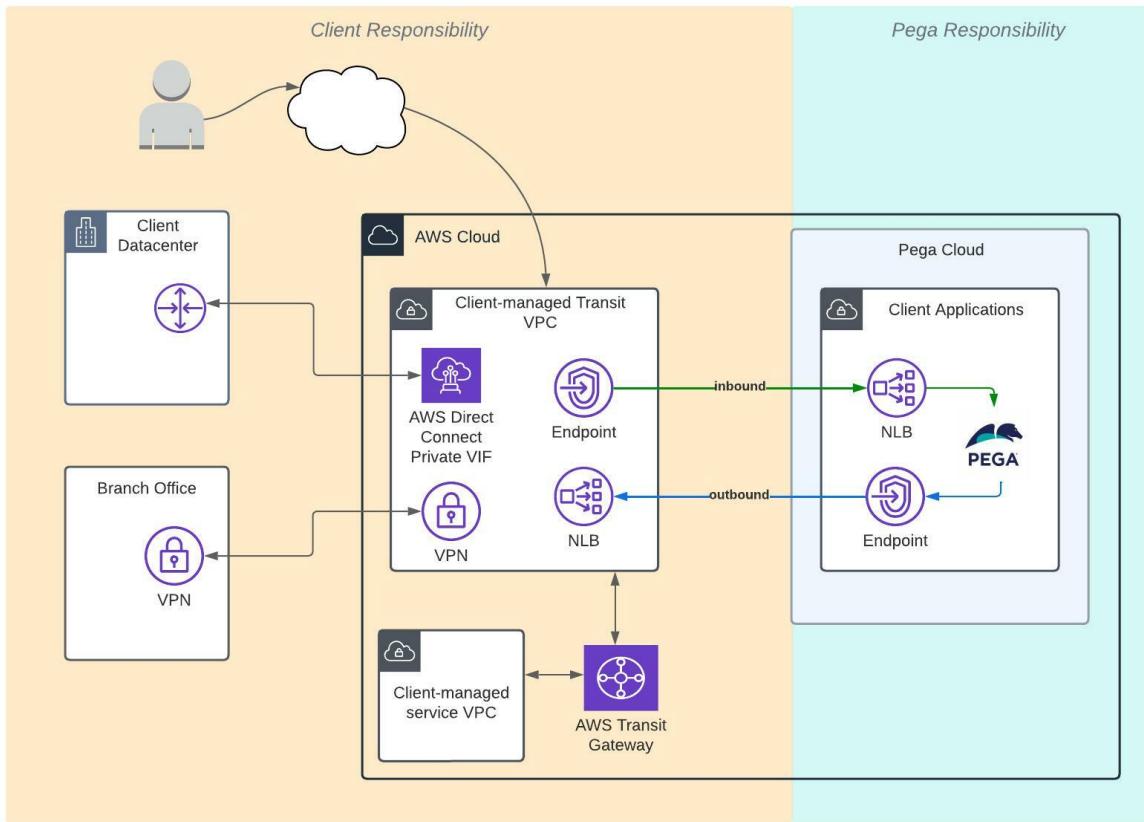
- Remote user
- Data center
- Corporate network or branch office
- Third-party provider network (for example, as-a-Service solutions other than Pega Cloud)
- Other AWS VPCs

Connection types

Your transit VPC gives you the ability to configure different connection types while maintaining a common method of forwarding those connections to your Pega applications using PrivateLink connections. The connection types that can drive your requirements include:

- Internet
- Site-to-site VPN
- Direct Connect private VIF
- AWS Transit Gateway (TGW) attachments

As an example of a diverse combination of location and connection types, you can establish a VPN with a branch office, a Direct Connect private VIF with a data center facility, an AWS TGW attachment to a separate AWS VPC, and internet access for end users, as shown in the following figure:



PrivateLink that facilitates Pega Cloud connections from many users and systems

Inbound (ingress) design pattern options

Inbound (ingress) traffic is traffic that originates from users and other service consumers, which connects to your Pega Cloud applications.

Inbound connectivity is a common use case because users are typical consumers of Pega Cloud services, and they are not likely to have a direct presence in an AWS VPC. You can use two methods to provide users with external access to your Pega applications through PrivateLink: direct access or through a forwarding service.

Direct access

Connect to your application by sending traffic directly to your PrivateLink endpoint.

Direct inbound connections to a your PrivateLink endpoint are only possible over a private connection: the endpoints resolve to private IP addresses that are only reachable from within your transit VPC or over networks that are connected to that VPC using a private connection such as a site-to-site VPN.

With this model, options for access control and inspection in your transit VPC are limited to the features of the endpoint itself (for example, you can configure AWS security groups on the endpoint).

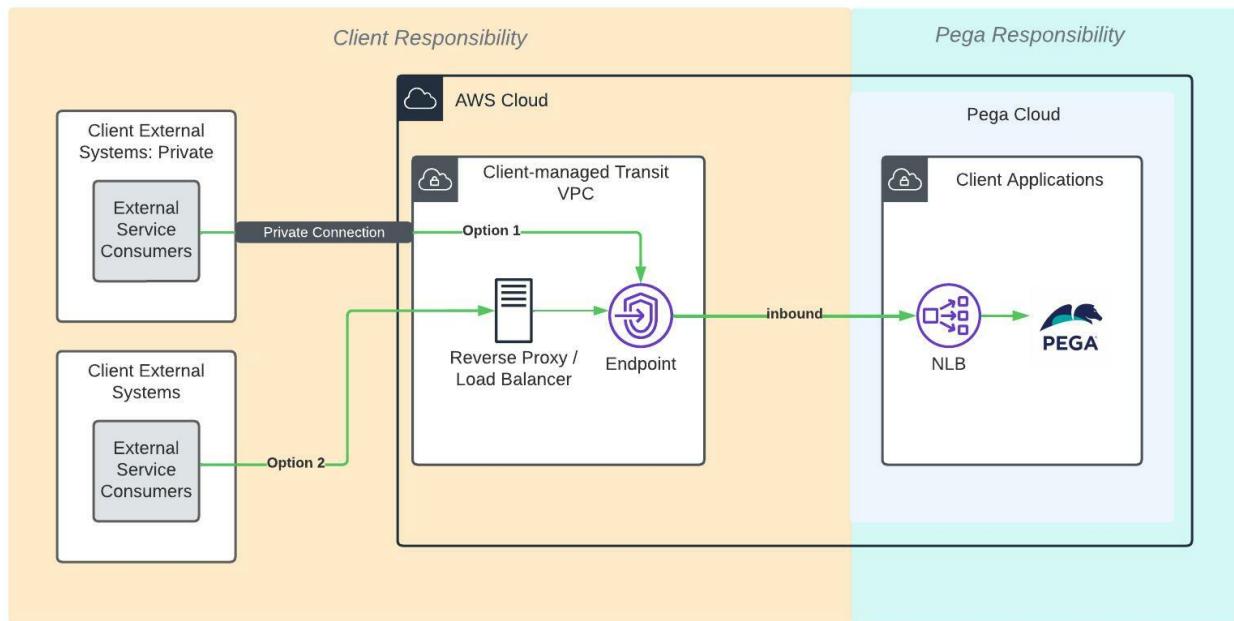
Through a forwarding device

Connect to your application by sending traffic through an intermediate device, such as a load balancer or reverse proxy, running within your transit VPC, which has been configured to forward traffic to your PrivateLink endpoint.

Inbound connections through a forwarding device are possible over a public or private connection.

With this model you can take advantage of enhanced features on the intermediate device like access control and traffic inspection.

For both inbound access options, you can provide direct access to your Pega applications over a private connection for one set of users and configure a forwarding device for a second set of users, as shown in the following figure:



Two design pattern options for configuring an ingress to Pega Cloud

Outbound (egress) design pattern options

Outbound (egress) traffic is integration traffic that your Pega application initiates to access data and processes on enterprise systems, such as email servers or web service providers.

Outbound connectivity is a common use case because modern enterprise data and systems often reside in diverse locations. You can use two methods to provide your Pega applications with access to systems that are outside your transit VPC: direct access or through a forwarding service.

Direct access

Configure your external systems directly as targets on the network load balancer (NLB) in your transit VPC that receives outbound traffic over PrivateLink.

Access between the NLB and its targets is possible over a private or a public connection.

With this model, options for access control and inspection in your transit VPC are limited.

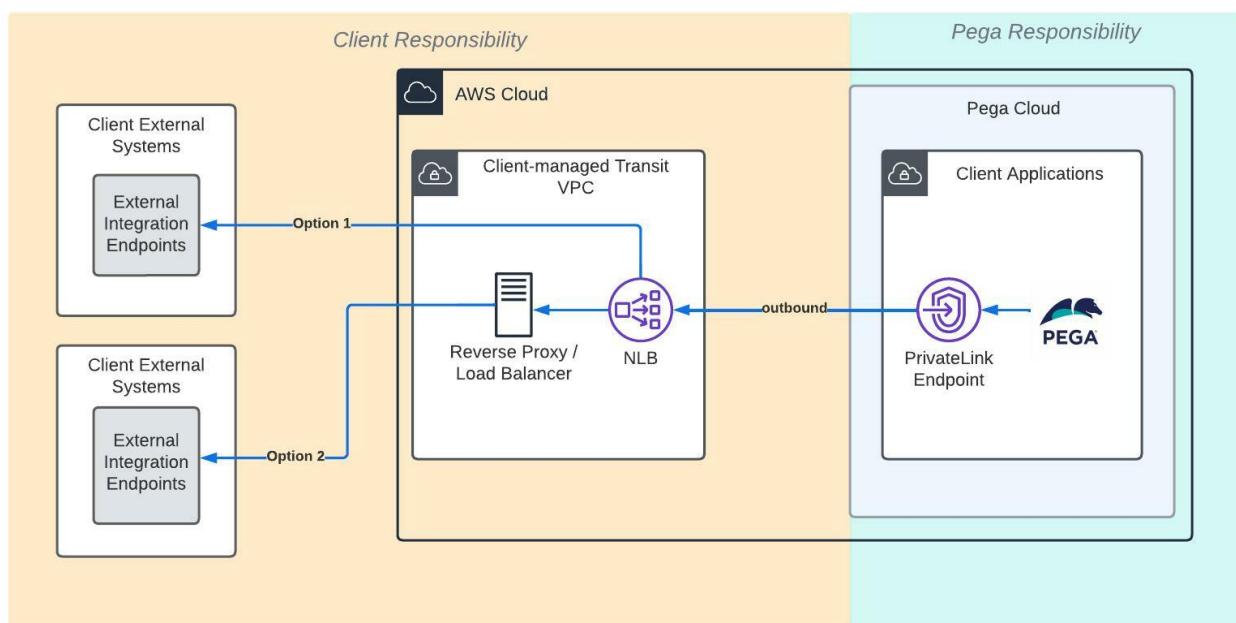
Through a forwarding device

Connect to your external systems by sending traffic through an intermediate device, such as a load balancer or reverse proxy, that runs in your transit VPC. You can use this forwarding device as the local target of your integration traffic, then forward that traffic to one or more external destination systems.

Access between the intermediate device and integration endpoints is possible over a private or a public connection.

With this model, you can take advantage of added features such as access control and inspection on the intermediate device.

For both outbound access options, you can provide direct access to some external systems using the network load balancer in your transit VPC and configure a forwarding device for access to other external systems, as shown in the following figure:



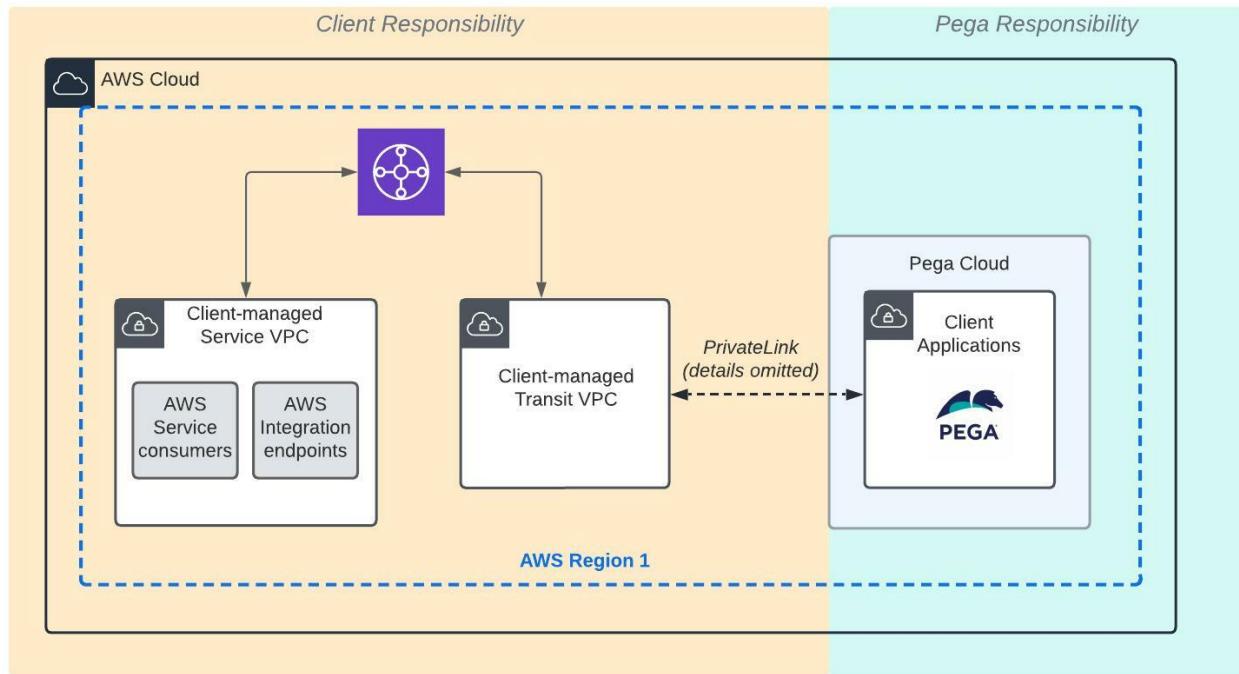
Two design pattern options for configuring an egress from Pega Cloud

Inter-region connectivity

AWS PrivateLink connections between VPCs require that the VPCs exist in the same AWS region. However, if you already have services in an AWS VPC in a region that differs from your Pega applications and need to connect those services to Pega Cloud, take advantage of AWS TGW support for inter-region peering with your transit VPC to bridge this gap.

Note: As with any design that spans a wide geographical area, performance and latency factors might apply. Review these factors before you implement this approach.

You can use your transit VPC to provide access to Pega Cloud from resources in a separate AWS VPC. While you have many different options for connecting your two AWS VPCs, AWS TGW is often an ideal choice. The following figure shows an example of a single region configuration:



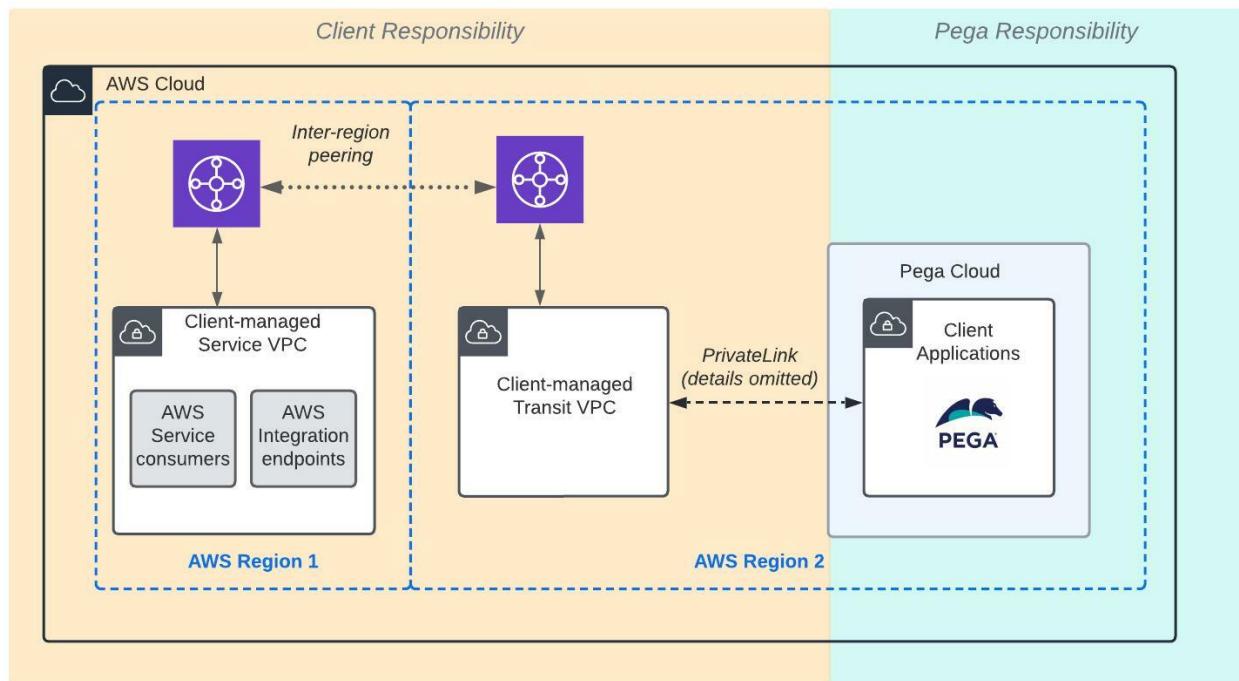
AWS TGW for same-region connectivity between managed AWS VPCs

When the VPC that contains your services is in a different AWS region from your Pega applications, you can configure your transit VPC in the same region as Pega Cloud, and then establish PrivateLink connections between your transit VPC and Pega Cloud. You can then use AWS TGW inter-region peering to establish end-to-end connectivity.

Ensure that you perform the following high-level actions to achieve connectivity:

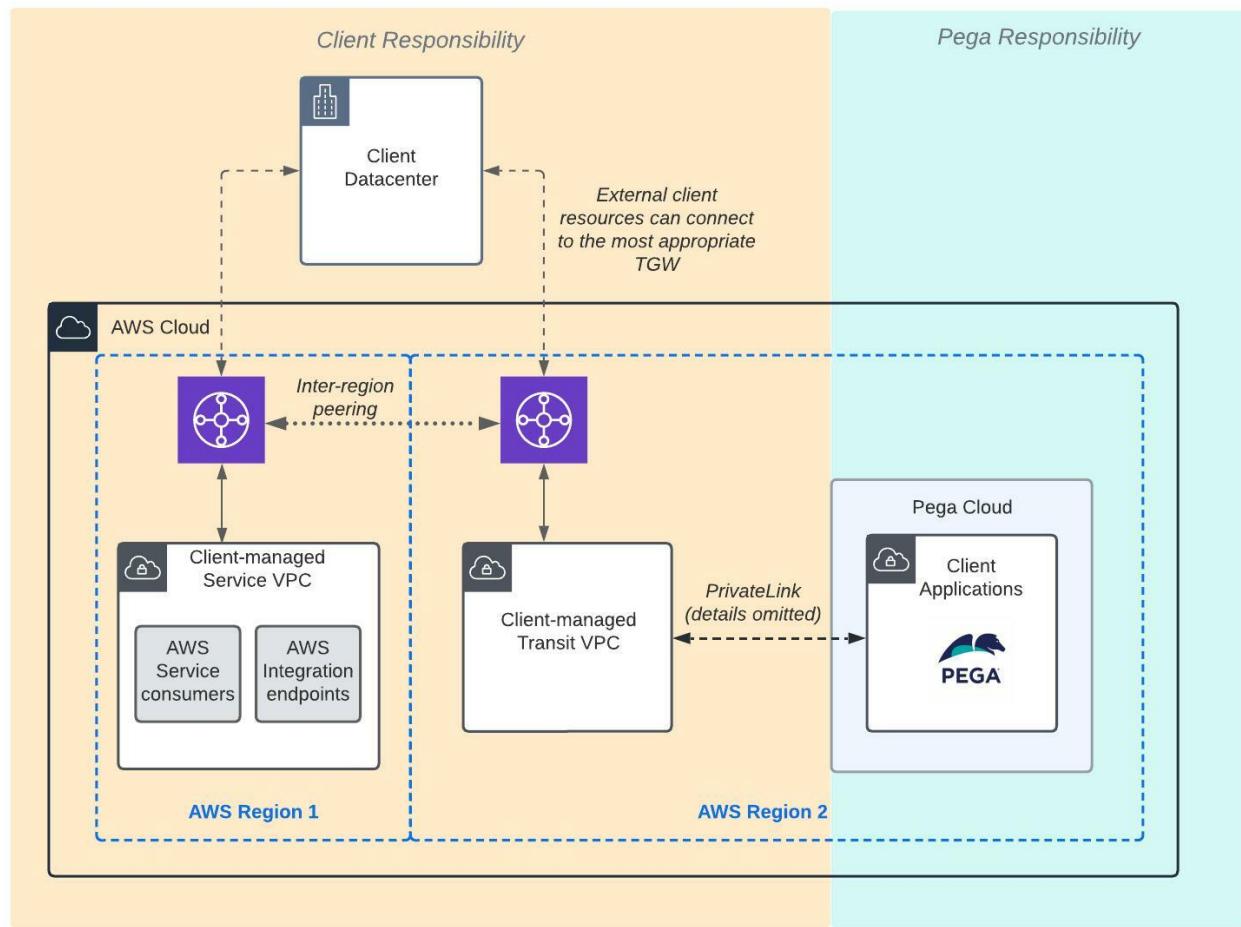
- Provision an AWS TGW in each of your regions.
- Create an inter-region peering connection between your two AWS TGWs.
- Create VPC attachments from each region's AWS TGW to your VPC in that region.
- Configure the appropriate routing to allow traffic flow.

Some high-level components and connections that you can use to achieve inter-region connectivity are shown in the following figure:



AWS TGW for inter-regional connectivity to Pega Cloud

You can also use this design to connect external networks to the most appropriate regional AWS TGW. There are multiple ways to connect your data center to your AWS-based components, as shown in the following figure:



A cross-region connectivity model provides flexibility for prioritizing your external connections to Pega Cloud

Results

After you implement this design pattern, you can use AWS PrivateLink and other forms of connectivity, such as the public internet or AWS Direct Connect, to facilitate secure and reliable connections between your external users and systems and your Pega Cloud applications.

One significant benefit of this connectivity model is your ability to establish a centralized point of ingress and egress for the traffic of Pega Cloud applications. By using a transit VPC, you can perform layer 7 routing and filtering, intrusion detection

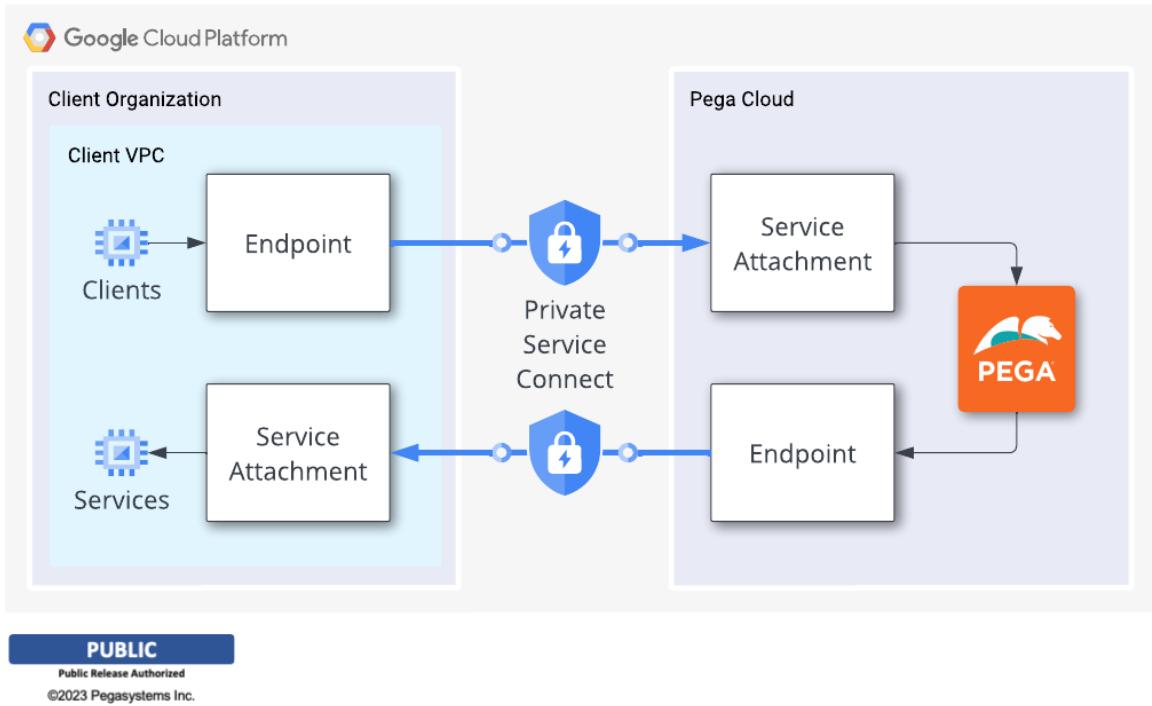
and prevention, and traffic mirroring. You can also use your transit VPC to establish a perimeter that creates clear lines of demarcation between your enterprise systems and as-a-Service providers.

Private connectivity using GCP Private Service Connect

Pega Cloud® Secure Connect enables the use of Private Service Connect from Google Cloud Platform (GCP) as a cost-effective and reliable solution to securely connect Pega Cloud to your existing Virtual Private Cloud (VPC) on GCP.

GCP recommends Private Service Connect for connections to software as a service (SaaS) providers when the traffic is originated and destined for endpoints in GCP. For more information about Private Service Connect and its benefits, see [Private Service Connect](#).

GCP Private Service Connect is available in Pega Cloud on GCP deployment regions. For more information, see [Deployment regions for Pega Cloud](#). Clients who leverage Pega Cloud on AWS deployment regions will continue using one of the options available to them under [Pega Cloud Secure Connect](#).



Private Service Connect providing connections you can use to communicate between Pega Cloud and your GCP resources and other enterprise networks

Private Service Connect offers high reliability, given the simplicity of the connection, as well as security, because traffic remains within the GCP network.

Benefits include:

- Very high bandwidth with two endpoints configured.
- Connectivity in the GCP network that provides high stability, security, and reliability.
- Low maintenance requirements.

You can also make use of Private Service Connect connectivity between Pega Cloud and enterprise resources outside of GCP. For guidance on best practices and options for

controlling access between your enterprise network and Pega Cloud over Private Service Connect, see [Access endpoints from hybrid networks](#).

Note: Pega Cloud does not support connecting client Private Service Connect configurations that use Global Access. For more information, see the use case [Use HTTP\(S\) load balancing for service controls](#).

Pega responsibilities:

- Pega completes the request for inbound and outbound endpoints.

Client responsibilities:

- Make a request in [My Support Portal](#) to use Private Service Connect to establish inbound and outbound connections from and to GCP, to and from Pega Cloud. For the latest documentation about making requests, see [How to Get Support](#).
- Understand how the [Private Service Connect compatibility](#) might affect your connections to and from Pega Cloud.
- Complete outbound connections, referred to in GCP as a consumer Private Service Connect endpoint. For an overview, see [About accessing published services through endpoints](#); for access configuration details, see [Access published services through endpoints](#).
- Complete inbound connections, referred to in GCP as a producer Private Service Connect service attachment. For an overview, see [About published services](#); for access configuration details, see [Publish services by using Private Service Connect](#).

Establishing an outbound connection

Send traffic from Pega Cloud to your GCP VPC by configuring an outbound connection from Pega Cloud using GCP Private Service Connect. Using GCP terminology, you configure a producer Private Service Connect service attachment and Pega Cloud will configure a corresponding consumer Private Service Connect endpoint for this

connection. You complete a cloud-change service request for Pega Cloud to complete this endpoint configuration.

Before you begin:

Keep in mind the following considerations the outbound connection from Pega Cloud:

- You configure your producer Private Service Connect service attachment in the same region as your Pega Cloud.
- Based on your preferred DNS resolution approach for Private Service Connect, Pega Cloud supports these DNS configurations:

Public DNS

Requires that your producer Private Service Connect service attachments use a private IP address that Pega Cloud provides as part of your outbound connection configuration.

Private DNS

Supports the following approaches for which you provide the Fully-Qualified Domain Name (FQDN) for this connection:

- A split DNS zone that shares private and public records. All Public records containing your Private DNS zone require manual entry, otherwise they will fail.
- Dedicated subdomains for Private Service Connect only.

To establish an outbound connection:

1. Make a cloud-change request for Pega Cloud to create a consumer Private Service Connect endpoint for this outbound connection by requesting a Cloud Assistance in [My Support Portal](#).

In the request, specify your DNS resolution approach for this connection and if it uses a Private DNS approach, include your producer Private Service Connect service attachment Fully-Qualified Domain Name (FQDN).

Result:

In response to your request, Pega sends you the GCP ProjectID.

2. Complete your producer Private Service Connect service attachment configuration in your GCP account that is based on your DNS resolution approach.
For details, see [Access published services through endpoints](#).
3. In the same cloud-change request, update the detail to include your producer Private Service Connect ServiceAttachmentID.

Result:

In response to your request, Pega completes the outbound connection.

4. If you have published a service with explicit project approval, accept the connect the connection request; otherwise the connection is completed automatically..
For more information, see [Manage requests for access to a published service](#)

Result:

Pega verifies access from Pega Cloud to the services that you specify. When verified, Pega closes the cloud-change request ticket.

Establishing an inbound connection

Send traffic from your GCP VPC to Pega Cloud by configuring an inbound connection using GCP Private Service Connect. Using GCP terminology, you configure a consumer Private Service Connect endpoint and Pega Cloud configures a corresponding producer Private Service Connect service attachment for this connection. You complete a cloud-

change service request for Pega Cloud to complete this service attachment configuration.

Before you begin:

Keep in mind the following considerations for the inbound connection to Pega Cloud:

- Pega Cloud services requires one consumer Private Service Connect endpoint in the inbound connection for each of your Pega Cloud environments.
- You configure your consumer Private Service Connect endpoint in the same region as your Pega Cloud.

To establish an inbound connection:

1. Make a cloud-change request for Pega Cloud to create a producer Private Service Connect service attachment for this inbound connection by requesting a [Cloud Assistance in My Support Portal](#).

In the request, include the GCP ProjectID in which Pega Cloud creates a producer Private Service Connect service attachment.

Result:

In response to your request, Pega sends you the producer Private Service Connect ServiceAttachmentID.

2. In your GCP account, create a consumer Private Service Connect endpoint in your VPC using the Pega-provided ServiceAttachmentID.
3. In the same cloud-change request, confirm that you have created the endpoints in your VPCs.

Result:

Pega activates the inbound connection for the specified Pega Cloud environments. Pega verifies that you can connect to this environment using the inbound connection. After verification is complete, Pega closes the cloud-change request ticket.

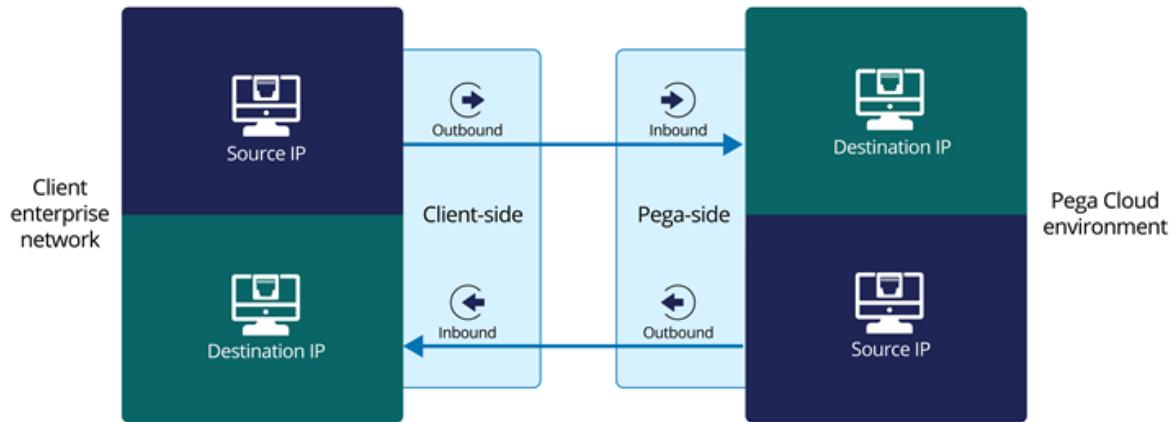
Configuring private access to Pega Cloud services (legacy options)

Pega Cloud® services supports several connectivity options to manage private network traffic between your Pega Cloud services environment and your enterprise network while fulfilling your network security requirements.

Important Pega Cloud networking definitions

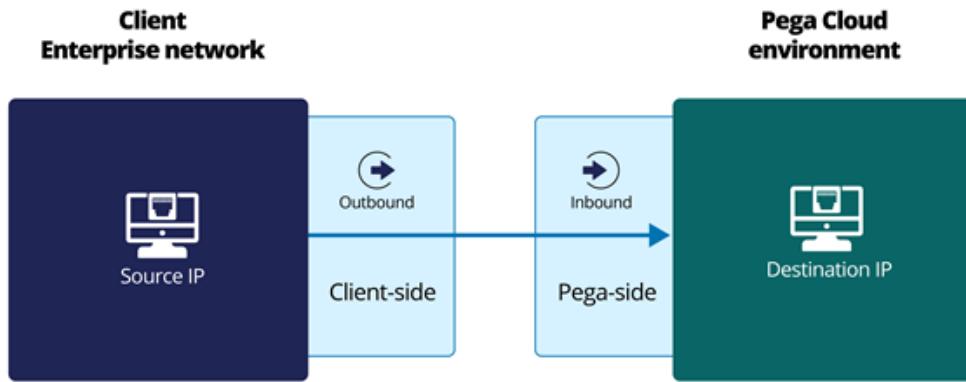
Pega Cloud uses precise terminology to describe the flow of network traffic between your enterprise network and your Pega Cloud environment from connection source to connection destination.

- **Inbound traffic:** Refers to traffic entering either your enterprise network or your Pega Cloud environment to the destination IP address.
- **Outbound traffic:** Refers to traffic leaving either your enterprise network or your Pega Cloud environment from the source IP address.



Network traffic flow definitions between client enterprise network and Pega Cloud environment

Client-to-Pega allow list configuration options



Outbound connection from client enterprise network; inbound connection to Pega Cloud environment

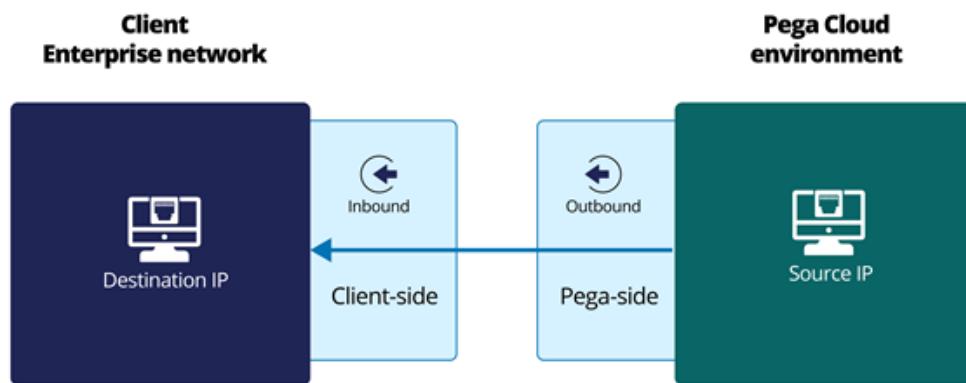
The following items describe options for to add Client-to-Pega private connections to an allow list.

By default, Pega only enables public-facing URLs for Pega applications. Create a service request to enable your Pega application URLs to be accessible over your private connection endpoints. For more information, see the row entitled "Client requests to enable private connection endpoints for their application."

- **Pega-side configuration (inbound traffic):** By default, Pega does not restrict external traffic from entering your private connection endpoints. To allow private connectivity only from specific private IP addresses, request Pega to apply allow lists to your Pega Cloud environments for private connections. For more information, see the row entitled "Client provides Pega private source IP addresses for Pega to add to an allow list on the Pega Cloud environment."
- **Client-side configuration (outbound traffic):** The Pega Cloud environment does not support static private destination IP addresses for private outbound traffic. Pega does provide three private IP address ranges for each of your Pega Cloud

environments. You can place these IP address ranges on an allow list on your enterprise network for private connectivity. For more information, see the row entitled "Client adds three private IP address ranges provided by Pega for their Pega Cloud environments to an allow list."

Pega-to-client allow list configuration options



Inbound connection to client enterprise network; outbound connection from Pega Cloud environment

The following items describe options for adding Client-to-Pega private connections to an allow list.

- **Pega-side configuration (outbound traffic):** Pega Cloud Services does not restrict outbound traffic for client environments. This support model offers the most flexibility for clients integrating with external services while maintaining client data security and confidentiality as described in [Pega Cloud Security and data protection](#).

- Client-side configuration (inbound traffic): Pega provides three private IP address ranges for each of your Pega Cloud environments. You must add these IP address ranges on an allow list on your enterprise network for private connectivity. For more information, see the row entitled "Client adds three private IP address ranges provided by Pega for their Pega Cloud environments to an allow list."

Private access services

To create a more secure network topology for your Pega Cloud, contact Pega Cloud support to integrate the following supported private access services:

Note: As of April 2022, Pega Cloud is ending support for all new

- ⓘ configurations of the following legacy connectivity options. For more information, please see [Change of support for connectivity options](#).

- Your own [Transit Gateway](#) to provide central management of connectivity between your external connections and your Pega Cloud environments in a monitored and secure private network.
- A [Pega VPN](#) connection to create a site-to-site encrypted connection to give your enterprise network secure remote access to your Pega Cloud environment.
- An [AWS Direct Connect](#) connection to create a dedicated connection from your enterprise network to your Pega Cloud environment that can provide dedicated bandwidth and increase network performance.
- A [VPC Peering](#) connection if you need to create a connection between your Pega Cloud VPC and an external AWS VPC in the same region.

Adding private connections responsibility model

The process for adding private connections to an allow list and configuring private access services relies on a shared responsibility model between you and Pega Cloud. To initiate any process involving adding a connection to an allow list, you must create a ticket with your regional Pega support representative by selecting [Create a ticket](#) in [My Support Portal](#), then follow the guidance in the *Client Responsibilities* column in the

following table. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

 **Note:** Pega Cloud cannot guarantee the absence of IP address conflicts when using private connections in a changing client environment. Pega Cloud will collaborate with you to identify potential overlap in IP address ranges during initial onboarding if you choose to use private connections.

If you require additional means of privately connecting to your Pega Cloud environment, contact your regional Pega support representative.

Configuration method	Connectivity	Client Responsibilities	Pega Responsibilities
Private connection through the Pega VPN service	Pega Cloud environment to client and client to Pega Cloud environment	Configure your enterprise VPN and provide requisite information to Pega. For more information, see Pega Cloud VPN service .	Provides a form to configure the Pega VPN service.
VPC Peering	Pega Cloud environment to an Amazon VPC	Make a request to obtain the information required for a VPC Peer connection to another Amazon VPC.	Provides client with the information required to create a VPC Peer connection with another Amazon VPC.

Configuration method	Connectivity	Client Responsibilities	Pega Responsibilities
		For more information, see Requesting a virtual private cloud (VPC) peering connection .	
AWS Direct Connect	Pega Cloud environment to client and client to Pega Cloud environment	Configure AWS Direct Connect with your Pega Cloud environment. For more information, see Configuring Amazon Web Services (AWS) Direct Connect in your Pega Cloud Services virtual private cloud .	Authenticates Amazon Direct Connect from Pega Cloud environment.
Client requests to enable private connection endpoints for their application	Client to Pega Cloud environment	Make a request for Pega to enable private endpoints for applications.	Enables internal connections for private connection endpoints.
Client adds three private IP address ranges provided by Pega for their Pega Cloud	Pega Cloud environment to client and client to Pega Cloud environment	Make a request to obtain three private IP address ranges, and add the static source IP address	Provisions private source IP address ranges for each Pega Cloud environment, and

Configuration method	Connectivity	Client Responsibilities	Pega Responsibilities
environments to an allow list		ranges to your enterprise network allow list.	then sends IP address ranges to client.
Client provides Pega private source IP addresses for Pega to add to an allow list on the Pega Cloud environment	Client to Pega Cloud environment	Make a request that includes a list of private source IP addresses for Pega to add to an allow list on the Pega Cloud environment.	Adds client-provided private source IP addresses on the Pega Cloud environments to an allow list.

- [AWS Transit Gateway](#)
- [VPC peering](#)
- [Virtual Private Network service](#)
- [AWS Direct Connect Private Virtual Interface \(VIF\)](#)

AWS Transit Gateway

Beginning April 2022, Pega Cloud® is ending support for all new configurations of the AWS Transit Gateway legacy connectivity option.

For more information, see [Change of support for connectivity options](#), which includes a recommended alternative to an AWS Transit Gateway private connection.

Pega Cloud services supports attaching your Pega Cloud environment to an AWS Transit Gateway that you manage. Your Transit Gateway can then act as a central hub to easily route traffic between your external connections and your Pega Cloud environment.

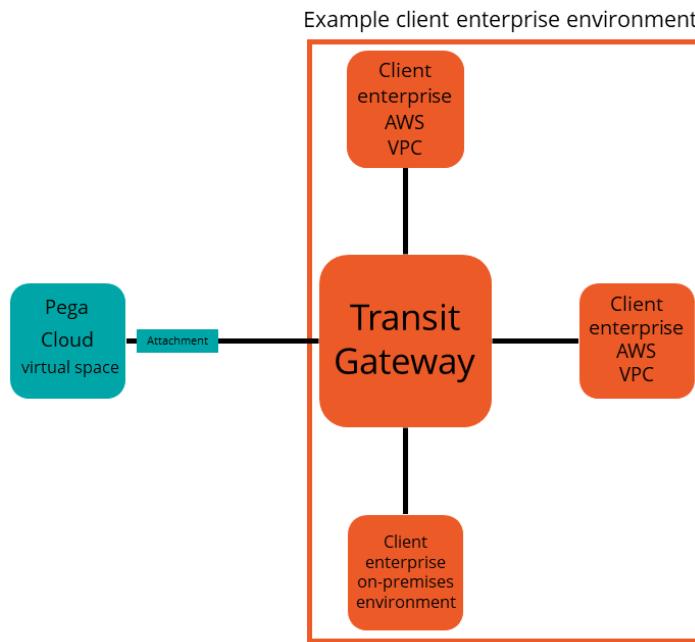
Using Transit Gateway puts you in full control of connectivity to Pega Cloud from your on-premise datacenter and your cloud applications or services and allows you to more quickly and easily connect new applications with your Pega application. While Pega Cloud services can attach your Pega Cloud environment to an existing AWS Transit Gateway, Pega Cloud services does not provide the Transit Gateway as a service.

For more information about subscribing to AWS Transit Gateway, see the official [AWS Transit Gateway](#) landing page.



Note: Pega currently does not support integrating VPN attachments to a Transit Gateway.

After you subscribe to the AWS Transit Gateway service through your AWS account, you can request that Pega Cloud services provides the information you need to integrate your service with your Pega Cloud environments. The following figure provides a model of how your Pega Cloud services VPC integrates with your AWS Transit Gateway Service.



Sample Transit Gateway topology

Integrating Pega Cloud environments with your Transit Gateway can simplify your enterprise network topology by providing the following benefits:

- Eliminating the need for complicated peering connections, especially in larger topologies, to let multiple environments communicate with one another
- Removing the requirement for multiple VPN connections between each of your AWS VPCs, including your Pega VPC, and on-premises environments
- Limiting traffic between your Pega Cloud environment and other VPCs
- Scaling your enterprise network topology to your Pega Cloud networking demands
- Responding to spikes in network traffic more resiliently through multiple interoperable VPCs

Implementing a Transit Gateway integration

Before you begin:

Before Pega Cloud services can complete the integration, you must:

- Ensure that you can access your AWS Resource Access Manager (RAM) and create a resource share for Pega Cloud services use.
- Have a management account with sharing enabled for AWS organizations to create the Transit Gateway resource share.

Pega Cloud supports attaching your Pega Cloud environment to an AWS Transit Gateway that you manage. Your Transit Gateway can then act as a central hub to easily route traffic between your external connections and your Pega Cloud environment.

To implement a Transit Gateway integration, complete the following steps:

1. Request a new service by selecting **Create a ticket** in [My Support Portal](#), or by using [Pega Support Contact Information](#) to complete a request to integrate your Transit Gateway with your Pega Cloud environments. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).
2. Update your Transit Gateway service by allowing Pega Cloud services to access your Transit Gateway:
 - a. In the AWS RAM console, create a resource share.
 - b. From the response to the request, or the from the call with your Pega representative, note the account number Pega Cloud services shares with you.
 - c. In your RAM console, in the **Principals** section, enter the account number that you receive from Pega Cloud services in response to your service request.
 - d. Select **Create resource share**.



Note: You can use the *create-resource-share* AWS API to enter the account number.

For more information on how to create a resource share through the RAM console or by using the API, see the [AWS Resource Management Documentation](#).

After you create a resource share of your Transit Gateway, Pega Cloud services creates a resource share attachment of your Pega Cloud environment.

3. Accept the resource share referencing your Pega Cloud environment.
 - a. In your RAM console, select the Shared with me, Resource shares pane.
 - b. On the **Pending** resource share page, add your Pega Cloud environment by selecting Accept Resource Share.

For more information on receiving a resource share, see the AWS Resource Access Manager documentation.

Result:

You integrated the Pega Cloud VPC and VPN service into your Transit Gateway, and can now use the Transit Gateway to connect your Pega Cloud VPC to the rest of your enterprise network topology.

VPC peering

Beginning April 2022, Pega Cloud® is ending support for all new configurations of the legacy VPC peering connectivity option.

For more information, see [Change of support for connectivity options](#), which includes a recommended alternative to a VPC peering connection private connection.

Pega Cloud services allows clients to use VPC peering connections between your Pega Cloud VPC and an external VPC that you control within the same AWS region.

To request a VPC peering connection:

1. Create a ticket by using [My Support Portal](#). Include your Amazon VPC Classless Inter-Domain Routing (CIDR) information in the request. In response to your request, Pega Cloud provides you with the following information:
 - The Pega Cloud AWS account ID
 - Your Pega Cloud VPC ID and region
 - Your Pega Cloud VPC address range (CIDR)
2. Using the information that you receive from Pega Cloud, create the VPC peering connection by sending a peering request to your Pega Cloud VPC from your AWS account.
 - a. From the [Amazon VPC console](#), in the navigation pane, click Peering Connections.
 - b. Click Create VPC Peering Connection, and configure the following fields for your peering request:
 - Name tag – Enter a name for the VPC peering connection.
 - Local VPC to peer – Select the VPC in your account with which you want to create the VPC peering connection.
 - Account – Select My account.
 - Account ID – Enter the Pega Cloud AWS account ID.
 - VPC ID – Enter your Pega Cloud VPC ID.
3. Click Create VPC Peering Connection, and click OK to confirm the request.



Note: The IPv4 CIDR blocks for the VPCs that you are establishing a peering connection between must not overlap. If the IPv4 CIDR blocks overlap, the VPC peering connection fails, even if the VPCs have unique IPv6 CIDR blocks.

4. After your VPC peering connection request is accepted, create a route table entry that includes the VPC peering connection information.
 - a. In the Amazon VPC console, in the navigation pane, click Route Tables.
 - b. Select the VPC that you are establishing the peering connection with.

c. On the Routes tab, click Add another route and provide the following information:

- Destination – Enter the CIDR for your Pega Cloud VPC.
- Target – Enter the information for the peered VPC.

Virtual Private Network service

Beginning April 2022, Pega Cloud® is ending support for all new configurations of the legacy Virtual Private Network (VPN) service connectivity option.

For more information, see [Change of support for connectivity options](#), which includes a recommended alternative to a VPN service connection.

Pega Cloud services allows clients to use the Pega Cloud VPN service to extend your private networks to Pega Cloud. This service helps you manage your proprietary data traffic, such as on-premises web services and data integrations.

Ensure that Pega Cloud services reviews and approves your settings for any VPN that you use to connect to a Pega Cloud environment. Pega Cloud services offers the Pega Cloud VPN service as a contractual feature. You violate your contract if you implement a VPN without the approval of Pega Cloud services.

Use the following requirements and recommended optimizations to plan and set up your VPN connection for the best performance, while preventing dropped connections or other issues.

Your Pega Cloud VPN service securely connects your existing network to your Pega Cloud environments through an IPSec VPN connection between the VPN gateway in your environment and the VPN endpoint gateway in your enterprise network. The service currently supports a single-gateway to single-gateway configuration, also known as a single site-to-site VPN. The Pega Cloud VPN service does not support the use of SSL VPN clients for remote user access.

Two tunnels are in the connection:

- Active
- Passive

Your enterprise network VPN gateway and the Pega VPN gateway each have two addresses that are assigned to this connection. Each gateway contains an outside address between that encrypted traffic flows, and each gateway also contains an inside address that is associated with the tunnel interface.

While the Pega Cloud VPN does not impose bandwidth limitations, the maximum bandwidth to which a VPN can scale to is about 1Gbps per tunnel. However, many different factors can affect actual performance. For this reason, Pegasystems does not guarantee minimum bandwidth and latency. For sustained network traffic throughput than 1Gbps, you should consider using Direct Connect for your Pega Cloud private connectivity.

Client responsibilities

- During onboarding, complete a questionnaire to help Pega Cloud services identify the most appropriate configuration settings for VPN interconnection with your Pega Cloud environment. Configure your gateway parameters using the settings that Pega Cloud services develops for your specifications. Pega Cloud services builds these details according to your hardware and software vendor and the individual VPN gateway configurations that you provide in the questionnaire.
- Have a VPN gateway, for which you are responsible, that is configured with a tunnel interface that is associated with the IPSec tunnel. This VPN gateway needs a static public IP address that should not change, to avoid re-creation of the tunnel.
- Use the configuration file that Pega Cloud services sends you to configure your VPN gateway. This file contains the requisite keys, IP addresses, and VPN parameters that are based on the information from the questionnaire.

Pega responsibilities

- Pega Cloud services creates networking artifacts for your subscription that include requisite keys, IP addresses, and other custom VPN parameters you require built from the information that you provided in the questionnaire.
- Pega Cloud services creates and sends you a VPN configuration file with settings that are based upon the hardware that you included in the VPN interconnect form in the onboarding questionnaire.

Supported client-managed VPN gateways

Amazon Web Services (AWS) provides a list of hardware devices that are known to work for VPN connections with the AWS Virtual Private Cloud and that are supported by command-line tools for automatic generation of configuration files. Pega Cloud services builds your configuration file to contain the requisite information required for your vendor, but cannot account for the way you configure your third-party hardware vendors or software that you may use when you implement a network configuration. For help with configuring your client gateway for use with your AWS Virtual Private Cloud, see *Amazon Virtual Private Cloud Network Administrator Guide* in the AWS documentation.

AWS VPN configuration requirements

When you initially configure the VPN gateway, your settings must comply with AWS VPN configuration requirements. Without complying with these requirements, you may lose your VPN connectivity during standard AWS routing maintenance or other incidents.

When you fill out the Pega Cloud services onboarding questionnaire, plan to meet the AWS VPN networking configuration requirements described in the table below. Reference the information provided in the configuration file.

Note: For internal Classless Inter-Domain Routing (CIDR) ranges, Pega Cloud  cannot guarantee that you will have no potential IP conflicts, but will make every effort to avoid them by using a non-Internet-routable public IP space.

AWS configuration requirement	Required actions
Internet Key Exchange Configuration	Set the lifetime configuration to 28800 seconds.
IPSec Configuration	Set the lifetime configuration to 3600 seconds.
VPN tunnel authentication	<p>Pega Cloud VPN service supports pre-shared key authentication where you either:</p> <ul style="list-style-type: none"> • Share a key you generate. • You agree to allow Pega to generate a key and share it during your initial VPC setup.
<p>Dual IPSec tunnel</p> <p>Dual tunnels offer failover capabilities. Because single tunnels rely on a single point of failure within your network, and can lose VPN connectivity during AWS routing maintenance, the use of dual tunnels maintains industry-standard failover capabilities for your Pega Cloud VPN.</p>	From the configuration file, use the two sets of the requisite keys, IP addresses, and VPN parameters to configure dual IPSec tunnels.
Ten-second keep-alive traffic.	Automate your traffic to your Pega Cloud services environments to use a ten-second keep-alive cron configuration that uses internal targets of your Pega Cloud services

AWS configuration requirement	Required actions
<p>AWS shuts down a tunnel after ten seconds if the tunnel has not received a keep-alive request.</p>	<p>environment, such as the internal URL of the internal load balancer, for your traffic destination.</p> <p>Use the scripting technique of your choice to write this automation.</p>
<p>IPSec ESP (Encapsulating Security Payload)</p> <p>This parameter inserts additional headers in transmit packets. To limit which headers in the transmit packets are inserted to IPSec, use these settings:</p>	<ul style="list-style-type: none"> • Set the TCP MSS Adjustment: 1387 bytes (Max session size: Layer4) • Enable Clear Don't Fragment Bit • Set fragmentation to before encryption
<p>Ten-second dead peer detection (DPD) with failure at 30 seconds.</p> <p>AWS sends a dead peer detection request every ten seconds for three intervals (30 seconds total), then takes down the tunnel at the virtual private cloud end upon not receiving a response from the client network.</p>	<p>Enable DPD to respond to a DPD request from the Pega Cloud services environment using a cron configuration. Use the scripting technique of your choice when writing your automation.</p>

VPN optimized configurations

After your Pega Cloud environment network meets the AWS VPN configuration requirements, Pega Cloud services recommends the additional best practice performance and security optimizations found in the table below. These optimizations bring your VPN gateway to parity with Pega Cloud services VPN gateway configurations to offer the best connectivity.

Optimizations	Configuration
Integration with an AWS Transit Gateway service for singular VPN configuration across your network topology.	See Integrating a new Transit Gateway .
Dynamic connections offer better performance and routing capabilities to support changes in your routing configuration.	Use a dynamic Border Gateway Protocol (BGP) over a static VPN connection. See the configuration file that contains required BGP information.
Dynamic dual IPSec tunnels can send traffic on either tunnel randomly which causes packet loss due to inconsistency in the routing path from the firewall. Using client-side BGP Path Selection controls the tunnel path to create a consistent network path.	When configuring BGP, use path selection in the dynamic VPN configuration to avoid asymmetric routing issues.
Configure a route-based VPN to create more than one pair of security associations (SA) to travel over your VPN tunnels to enhance your network security. Policy-based VPNs only support a single pair of SAs.	Use a route-based VPN as your primary connection type, and policy-based VPN as your secondary connection type.
Configure a VPN connection that uses perfect forward secrecy to create a new key that the network uses to connect to your VPN to improve security posture.	Enable perfect forward secrecy in your VPN hardware and software.

Optimizations	Configuration
Disable NAT-T to avoid potential issues with your connections when you do not want your traffic to translate to a destination that does not use a public IP address.	Disable Network Address Translation Traverse (NAT-T) if you do not intend to use it.
Keep your networking hardware and software updated to prevent further issues.	Ensure that you update the hardware regularly to use the latest vendor software and firmware releases.

Unsupported VPN configurations

To follow best practices with your VPN configurations, avoid the following unsupported configurations because of the issues that they can cause with your private site-to-site network.

Unsupported configuration	Known potential issue	Alternative implementation
For policy-based VPNs, do not add more than one network.	Policy-based VPNs only support a single pair of SAs in the VPN tunnel. When you configure more than one network on a policy-based VPN, you require more than one pair of SAs. This can cause SA competition in the tunnel and lead to packet loss.	Use route-based VPNs if supported by your vendor software or hardware.

Unsupported configuration	Known potential issue	Alternative implementation
Do not configure load balancing in dual IPsec configuration.	VPNs use dual IPsec tunnel configurations for failover, but not load-balancing purposes.	Configure dual IPsec tunnels for failover purposes only.
Do not enable the tunnel idle timeout in your VPN network software.	Setting a value for tunnel idle timeout can override the required Pega configuration of this parameter which prevents the tunnel from shutting down your connection.	Keep tunnel idle timeout off.
Do not configure two VPNs to the same IP address.	The AWS VPN public IP address can only support a single tunnel.	Configure VPNs to use separate IP addresses.
Do not use static VPN as a backup for AWS Direct Connect.	AWS Direct Connect uses a dynamic connection; static connections cannot properly back up dynamic connections.	Use Direct Connect as the primary connection with the BGP VPN as a back-up connection.

AWS Direct Connect Private Virtual Interface (VIF)

Beginning April 2022, Pega Cloud® is ending support for all new configurations of the legacy AWS Direct Connect Private VIF connectivity option.

For more information, see [Change of support for connectivity options](#), which includes a recommended alternative to an AWS Direct Private VIF connection.

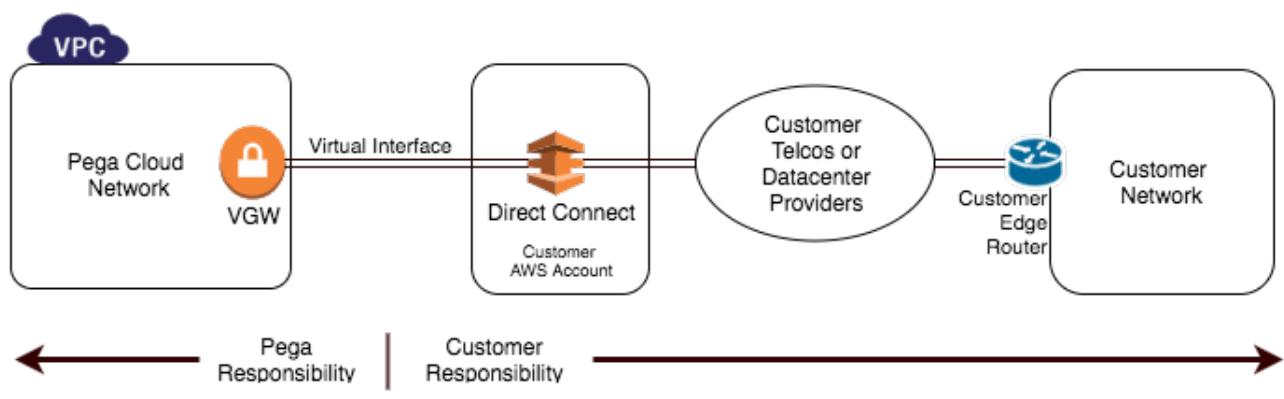
Pega Cloud services allows clients to connect using Amazon Web Services (AWS) Direct Connect Private Virtual Interface (VIF) within a geographical region.

Use this AWS service to connect from the following types of endpoints:

- A data center provider that is located within the same geographical region as your AWS service.
- A multiprotocol label switching (MPLS) VPN or other type of wide area network (WAN).

Direct Connection options

Pega Cloud supports AWS Direct Connect Private VIF connectivity so you can access your Pega Cloud DevTest, Staging, and Production subnets using AWS Direct Connect Private VIF. AWS Direct Connect Private VIF provides connectivity between these environments through a virtual interface, which is then physically connected through the AWS network to the customer network through a virtual gateway (VGW).



Prerequisite

If you are not already an AWS customer, set up an AWS account for your enterprise. Your account includes an AWS console through which you can order services.

After setting up an AWS account, create an AWS Direct Connect Private VIF.

For more information, see the Amazon Web Services article “AWS Direct Connect virtual interfaces”.

Setting up AWS Direct Connect

Complete the following process to set up AWS Direct Connect for your Pega Cloud VPC:

1. Provision Direct Connect ports in your AWS Console.
2. In My Support Portal, [create a ticket](#)to establish the direct connect virtual interface to your Pega Cloud VPC. The Service Request created in the ticket tracks the provisioning process as well as the information provided to you by Pega Cloud for your request.

Pega Cloud will provide your account and region information, which you need to complete your request.

3. In your AWS Console, initiate a request for a virtual interface to Pega Cloud.
4. Enter the Pega Cloud account and region information in your request and submit it.

After you submit the request in your AWS Console, Pega Cloud will receive the details and after approval, connects the virtual interface to your Pega Cloud VPC. Pega Cloud also sets up basic monitoring for the connection from your Pega Cloud VPC.

You can use a third-party portal to provision a direct network connection, such as one that is offered by your telecommunications provider. If you choose this option, consult the provider's support team about the request process.

Redundancy options for AWS Direct Connect

AWS Direct Connect Private VIF is a stand-alone connection, and you might want to configure a redundant connection to your network. Pega Cloud supports the following options for redundancy:

- An additional AWS Direct Connect service (redundant direct connection).
- Failover to customer VPN.

You can choose the option that works best for your requirements. You are responsible for the configuration and implementation of redundancy for AWS Direct Connect.

Administering your Pega Cloud service

The [My Pega Cloud portal](#) provides a connected experience for all of your environments in your My Pega Cloud subscription. My Pega Cloud is a one-stop control center in which you can complete restarts and log downloads, view your upcoming scheduled maintenance, and participate in your upgrade journey. You can also review Pega requests that require your action in the Action center banner.

Before you begin:

To use the My Pega Cloud portal, have the following:

- Cookies enabled in your browser settings.
- An appropriate role with access privileges to the portal. If you do not have access, contact your Account Administrator to secure those as described in [Defining your support contact roles](#).
- Your My Pega Cloud portal preferences configured. For details, see [Configuring your portal preferences](#).

To begin, login to [My Pega Cloud portal](#). If you require a password reset or have questions about account access and user or role changes in your account, refer to [My Support Portal Frequently Asked Questions](#).

- [Setting up Pega Cloud account users](#)
- [Setting up your Pega Cloud environments](#)
- [Viewing maintenance activity for your Pega Cloud environments](#)
- [Entering a Support Request in My Support Portal for Pega Cloud](#)
- [Initiating software updates in Pega Cloud](#)

- **Messages and actions for your Pega Cloud environments**
- **Troubleshooting using Pega log files in Pega Cloud**
- **Using Pega Cloud status**

Setting up Pega Cloud account users

Your My Pega Cloud portal Home page includes an Account users tile. This tile displays a count of the current number of permitted users in your Pega Cloud® environment. The tile also provides a View details link that goes to the **Account users** page, which shows more detailed information about the users.

Account users page options

After you log into the [My Pega Cloud portal](#), you can:

- View a table of all users of your account, including:

Item	Description
Full Name	Full name of user
Role	Cloud-specific role assigned to the user
Email address	Email address where the user receives email messages by using your default messaging service

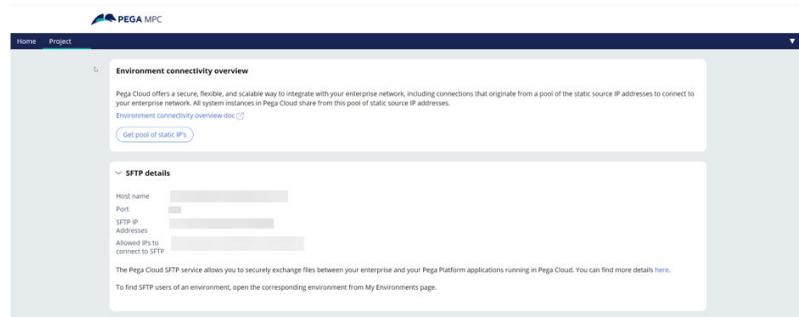
- Manipulate the table using Group, Fields, or Density, or click Refresh to refresh the list.
- Select Manage users in the upper right to manage access or request changes (Cloud Account Administrators only).

Setting up your Pega Cloud environments

Use the **My cloud setup** tile in the My Pega Cloud portal to access all your Pega Cloud® environments, download your Pega Cloud log bundles, and perform restarts on each environment.

In the My cloud setup tile, click **View details** to access the following functions in your environments:

Item	Description
Environments	<p>View all of the environments to which you have access with information that includes Environment Name, Pega Version, Environment type, service type or deployment, production level, applications, and status.</p> <p>For each environment, you can click the More icon, and then choose one of the options:</p> <ul style="list-style-type: none">• Download log files• Restart an environment• Manage a hibernated environment <p>If you expand the view for an environment, you can see:</p> <ul style="list-style-type: none">• A Database Storage section that includes database storage utilization details.• A Monitor on PDC link, a URL to the Pega Diagnostic Center (PDC) for the environment. For more information about how to log in, see Monitoring your application using Pega Predictive Diagnostic Cloud.• A Deployment Manager link, a URL to Deployment Manager for the environment. For more information, see Deployment Manager overview

Item	Description
	<ul style="list-style-type: none"> A Deployed Applications tab that shows the complete list of built-on applications that your organization has in your environments. An Activity Log tab that displays a list of the self-service operations clients have performed to date.
Project Info (Pega Cloud 3 only)	<p>View your static IP addresses in the Environment Connectivity Overview tab. For more information on static IP addresses, see Environment connectivity overview.</p> <p>If you are on AWS and use SFTP, you can view your SFTP IP addresses in the SFTP details tab.</p> 
Download log files	<p>Generate a bundle of specified log files that have been created from your environment during the last 30 days for internal analysis or to share with Pega Global Customer Support (GCS). The log bundle is a compressed TAR file that you can download to your local computer. If no logs are available that match your filter, the Generate log bundle button is not enabled.</p> <p>For more information about how to access your logs, see Accessing your log files for troubleshooting.</p>

Item	Description
Restart environments	<p>Restart one or more tiers in your environments. When you restart your environment tiers by using the self-service portal, the average time for the nodes in your tier to restart is about 30 minutes, while the maximum time is about 60 minutes.</p> <p>For more information about restarting, see Environment restarts</p> <div style="background-color: #e1f5fe; padding: 10px; margin-top: 20px;"> <p>Note: When you use the restart self-service, you do not impact your background processing tiers or the Search availability.</p> </div>
Manage a hibernated environment	<p>After a period of no-activity usage, your environment begins a hibernating phase before entering a hibernated state that pauses usage of system resources.</p> <p>For more information about waking up a hibernated environment, see Managing a hibernated environment.</p>

Reviewing environment status and database details

Review the database storage utilization and environment status for an environment.

1. In the **My environments** tile, click View details.
2. In the **Environments** section, click the environment name.
3. Here you will find your Database storage information.

Database Storage



4. You will also see one of the following environment status labels.

Option	Description
Active	Default environment status. Environment is fully operational.
Inactive	The environment is down or not accessible.
Hibernated	The environment is paused to reduce energy consumption.
Waking up	The environment is coming out of hibernation mode.
Maintenance	The environment is undergoing maintenance.
Low-space	Database storage utilization is over 90% for this environment.

Reviewing the activity log

Review the history of the self-service actions and activities your organization has completed on this environments.

The activity log for an environment displays the activities that have occurred on that environment, including the type of activity, the user who performed the action, the activity status, and when it was initiated. The Activity Log details can help you understand the actions that affect that environment.

1. In the **My environments** tile, click View details.
2. In the **Environments** section, click the environment name.
3. To see the deployed applications in your environment or the activity log of self-service actions that your organization performs in your environment, review the **Environment Details** section.
4. Click the Activity Log tab to view activities, their type, the user who performed the action, the activity status, and when it was initiated.

Reviewing SFTP users (Pega Cloud 3 on AWS only)

Review data about your SFTP users, such as user name, user type, and mapping directory.

1. In the **My environments** tile, click View details.
2. In the Environments section, click the environment name.
3. Review the **Environment Details** section.
4. Click the SFTP Users tab to view information about your SFTP user names, user types, and mapping directory.

User name	User type	Mapping directory
simulated user 1	Admin user	/filestorage/sftp
simulated user 2	Non-Admin user	/filestorage/sftp/opta
simulated user 3	CDH user (Read only)	/filestorage/simulation/decisionData

SFTP details like host name, SFTP IP Addresses and Allowed IPs to connect can be found [here](#).

Reviewing deployment applications

Review the complete list of built-on applications that your organization has in your environments.

View the deployed applications to see your applications by name, as well as the version of each application.

1. In the **My environments** tile, click View details.
2. In the **Environments** section, click the name of the environment.
3. **Optional:** To see the deployed applications in your environment or the activity log of self-service actions that your organization performs in your environment, review the **Environment Details** section.
4. Click the Deployed Applications tab to view the applications that are deployed in the environments and the version number that is associated with each application.

Viewing maintenance activity for your Pega Cloud environments

Your My Pega Cloud portal Home page includes a Maintenance tile. This tile displays a count of the number of Upcoming maintenance tasks for your Pega Cloud®. The tile also provides a View details link that goes to a Maintenance Task page where you can view upcoming, completed, and ongoing maintenance activities for all of your environments.

For more information on maintenance and updates, see [Pega Cloud maintenance and types of system updates](#).

1. In the **Maintenance Task** page, in the Upcoming Maintenance Tasks, Completed Maintenance Tasks, and Ongoing Maintenance Tasks sections, view the scheduled, completed, and ongoing maintenance tasks for your environments, respectively.
2. In the Maintenance Type column, view the type of maintenance that your environment is scheduled for or has undergone.
 - Patches
 - Hotfixes
 - Database updates
 - Pega Infinity™ updates

3. In the **Environment URL** column, view the environment URL to which the maintenance will be or was applied.

Click the URL to be redirected to the environment.

4. In the **Environment Type** column, view whether your environment is a **Production**, **Staging**, **DevTest**, **Agile Studio**, or Deployment Manager (**DevOps**), **Business operations**, **Clone**, or **Production mirror** type.
5. In the SR ID column, view the service request ID for the maintenance activity.

Click the support request ticket to be redirected to the support ticket on [My Support Portal](#).

6. In the **Start Time** column, view when the maintenance task started or when it is scheduled.

On the **Upcoming Maintenance Tasks** or the Ongong Maintenance Tasks sections, view the version of Pega Platform undergoing maintenance in the **Pega Version** column.

On the Completed Maintenance Tasks section, view the when the maintenance was completed in the Completed on column.

To reschedule an upcoming maintenance task, see [Rescheduling Maintenance through My Pega Cloud](#).

7. Manipulate the table using: Group, Fields, or Density, or click Refresh to refresh the list.

- [Rescheduling Maintenance through My Pega Cloud](#)

Rescheduling Maintenance through My Pega Cloud

Follow the steps below to reschedule an upcoming maintenance at a time that is convenient for you.



Note: This feature is only available on [Pega Cloud 3](#) and can only be used to reschedule maintenance activities labeled as Patch, Hotfix, or Database

update. To reschedule any other type of maintenance, reach out to [Pega Support](#).

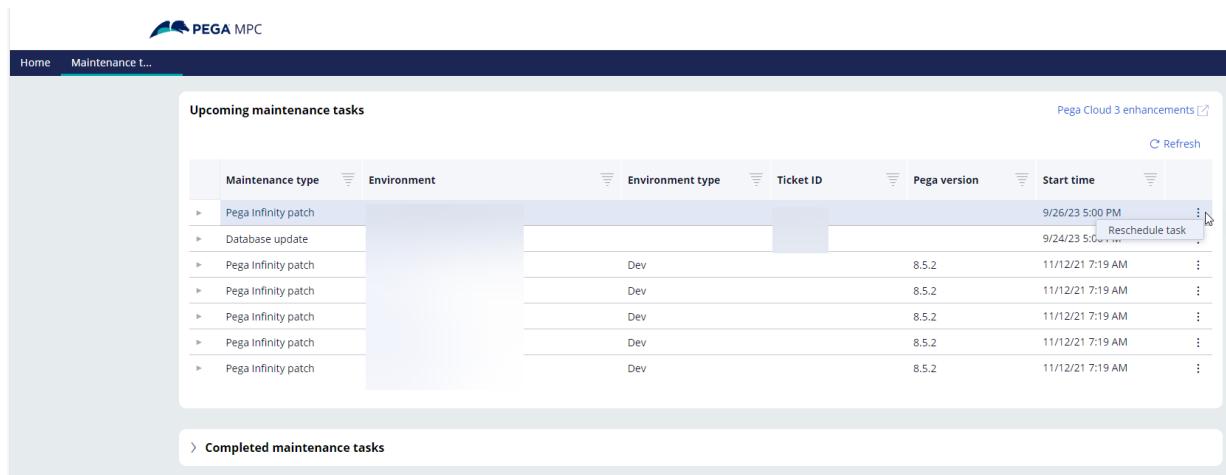
Maintenance cannot be rescheduled within 6 hours of the scheduled maintenance time. A single maintenance task can be rescheduled up to three times. After rescheduling three times, the maintenance date can no longer be rescheduled in My Pega Cloud.

For more information on maintenance and updates see [Pega Cloud maintenance and types of system updates](#).

How to reschedule maintenance in My Pega Cloud

1. Click on the Maintenance tile -> Upcoming maintenance tasks to view all upcoming maintenance.
2. Click on the vertical ellipsis icon on the right side of the maintenance you want to reschedule.
3. Click Reschedule task.

The Reschedule task option will not appear if the maintenance is scheduled to begin within the next 6 hours or if the maintenance has already been rescheduled three times.



The screenshot shows the 'Upcoming maintenance tasks' section of the Pega MPC interface. The table has columns for Maintenance type, Environment, Environment type, Ticket ID, Pega version, and Start time. The 'Maintenance type' column lists various patches and updates. The 'Start time' column shows dates like 9/26/23 5:00 PM and 9/24/23 5:00 AM. The 'Environment' column shows environments like Dev. The 'Pega version' column shows 8.5.2. The 'Start time' column includes a 'Reschedule task' button for certain entries. At the bottom, there is a link to 'Completed maintenance tasks'.

Maintenance type	Environment	Environment type	Ticket ID	Pega version	Start time
Pega Infinity patch				8.5.2	9/26/23 5:00 PM
Database update				8.5.2	9/24/23 5:00 AM
Pega Infinity patch	Dev			8.5.2	11/12/21 7:19 AM
Pega Infinity patch	Dev			8.5.2	11/12/21 7:19 AM
Pega Infinity patch	Dev			8.5.2	11/12/21 7:19 AM
Pega Infinity patch	Dev			8.5.2	11/12/21 7:19 AM
Pega Infinity patch	Dev			8.5.2	11/12/21 7:19 AM

- Select a new start time from the dropdown menu and provide a reason for the rescheduling.

Most maintenance tasks can be pushed back up to 15 days. Due to increased urgency, hotfixes can only be pushed back up to 5 days.

- Click Submit

The screenshot shows the 'Upcoming maintenance tasks' list on the left and a 'Reschedule Task' modal on the right. The modal title is 'Pega Infinity patch - Illuminati Restart Excluded Env'. It contains a dropdown menu labeled 'Available start times *' with 'Select ...' and a tooltip 'Times are shown in the default time zone of the system if a time zone is not set in your Profile'. Below the dropdown is a text area for 'Reason for rescheduling *' with a character count of 'Remaining: 256 characters'. At the bottom are 'Cancel' and 'Submit' buttons.

Maintenance type	Environment	Environment type	Ticket ID	Pega version	Start time
Pega Infinity patch					9/26/23 5:00 PM
Database update					9/24/23 5:00 PM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM
Pega Infinity patch					11/12/21 7:19 AM

- You should see the message, "This reschedule request was submitted successfully."

If you do not see this message, contact [Pega Support](#)

- Within a few minutes, the start time will update automatically in the Upcoming maintenance tasks list and in the ticket. You can view the reschedule history by clicking the arrow to the left of the maintenance task in the Upcoming maintenance tasks list.

The screenshot shows the 'Upcoming maintenance tasks' list on the left and a table on the right showing reschedule history for a specific task. The table has columns: 'Scheduled start time', 'Performed by', 'Performed on', and 'Reason for reschedule'. The first row shows the original scheduled start time of 9/29/23 5:00 PM and a reason for reschedule of 9/18/23 1:06 PM. The second row shows a rescheduled start time of 9/26/23 5:00 PM and a performed on date of 9/15/23 8:31 PM. The third row shows another rescheduled start time of 9/30/23 5:00 PM and a performed on date of 9/15/23 8:11 PM.

Scheduled start time	Performed by	Performed on	Reason for reschedule
9/29/23 5:00 PM		9/18/23 1:06 PM	
9/26/23 5:00 PM		9/15/23 8:31 PM	
9/30/23 5:00 PM		9/15/23 8:11 PM	

Entering a Support Request in My Support Portal for Pega Cloud

Your My Pega Cloud portal Home page includes a Support requests tile. This tile displays a count of the current number of ongoing requests you have in your . The tile also provides a View details link that goes to the **Support Requests** page. That page shows detailed information about all support requests submitted for this account and the environments in this Pega Cloud.

In the Support requests page, you can:

1. View a table of all support requests, including:

Item	Description
ID	Support request ticket code and number as a link. To view the ticket on My Support Portal , click the short description.
Short description	Note the user entered when creating the service request.
Environment Name	Environment name to which the request was applied.
Environment URL	Environment URL to which the request was applied. To be redirected to the environment, click the URL.
Severity	Level of severity entered for the issue in the request. For more information about severity levels, see Severity Levels and Response Times .
Status	Status details of the support request.
Created On	Date and time that the support request was created.

2. Manipulate the table view using Group, Fields, or Density.
3. To make a new request, click Create service request in the upper right. [My Support Portal](#) appears, and you can click [Create a ticket](#).

Initiating software updates in Pega Cloud

Your [My Pega Cloud portal](#) Home page includes a **Updates** tile to initiate and manage your software update journey in Pega Cloud®. You can view whether your environment is up-to-date, the schedule of any upcoming updates of your environments, take required action during each stage of the process, and provide feedback to streamline and facilitate your update journey.

Before you begin:

If you have an upcoming update, you can prepare for your update by reviewing the update checklist that is appropriate to your pre-update version:

- [Pega Cloud update checklist for Pega Infinity release 8.4.2 and later](#)
- [Pega Cloud update checklist for Pega Infinity release 8.4.1 and earlier](#)

Use the following definitions for the update journey and the Update tab in the My Pega Cloud portal.

Source version	Pega Platform version from which you are updating.
Target version	Pega Platform version to which you are updating.
Current state status bar	Control that displays the present stage of your update journey. The Update tab changes depending on the stage in your update journey. In the journey, there are six stages: <ol style="list-style-type: none">1. INITIALIZE

- | | |
|--|---|
| | <ul style="list-style-type: none">2. CLONE3. UAT4. UPDATES5. DECOMMISSION CLONE6. RESOLVE |
|--|---|

1. On the My Pega Cloud Home tab, in the **Updates** tile, initiate the update process by clicking Start.

Result:

You are redirected to the portal.

2. In **My Support Portal**, click [Create a ticket](#), and then specify a staging environment that you want Pega to clone and then update.



Important: This request takes five days to complete. Make the request at least three weeks before your targeted production environment update.

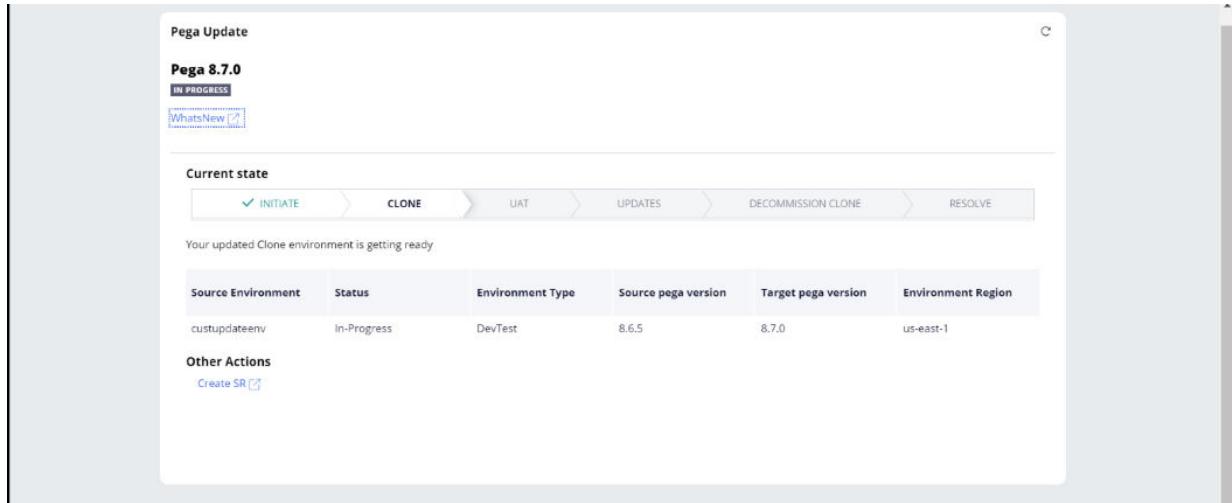
3. Once Pega initiates your update request, click the Update tab.

Result:

The process moves into the Clone stage.

4. View the status of your cloned environment as Pega Cloud provisions and updates the clone in the **Clone** stage view.

The checklist displays the status of your clone environment being provisioned, its infrastructure updated, and its Pega Platform version updated.



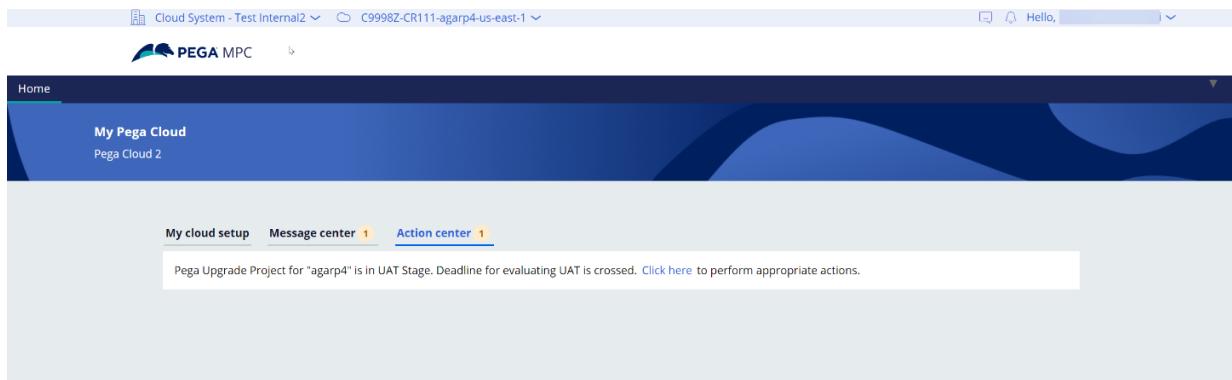
The checklist that displays the progress of your clone environment update

Result:

Pega Cloud provisions and updates your clone environment for your update application testing (UAT), and the update process moves to the UAT stage.

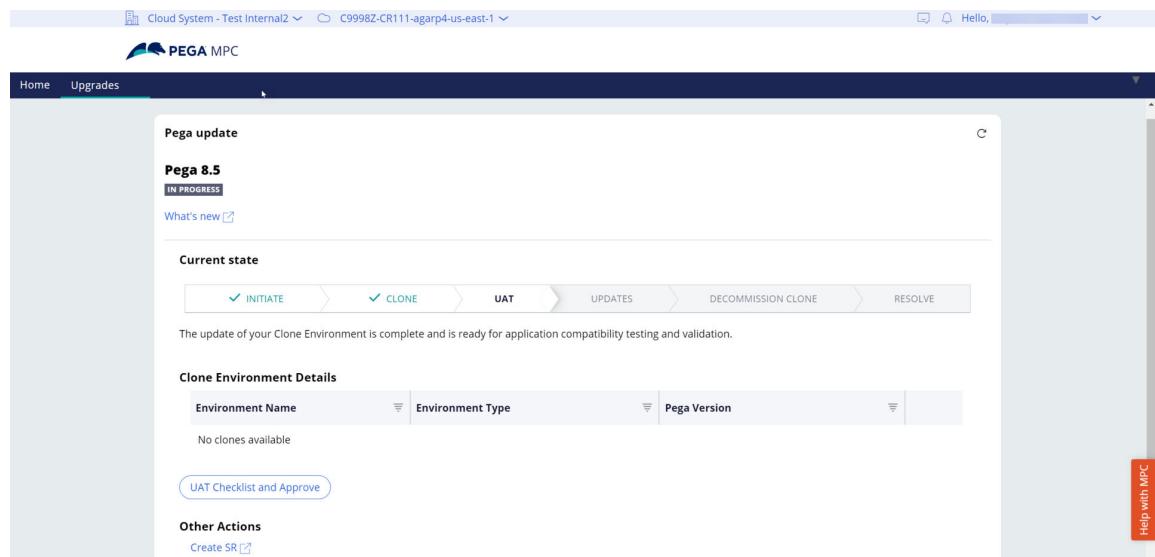
5. Within 10 business days, perform UAT on the cloned environments by testing all applications through automated and manual testing.

The Action center banner in the My Pega Cloud portal displays a link to your checklist with required UAT actions, as shown in the following example:



Action center banner for UAT

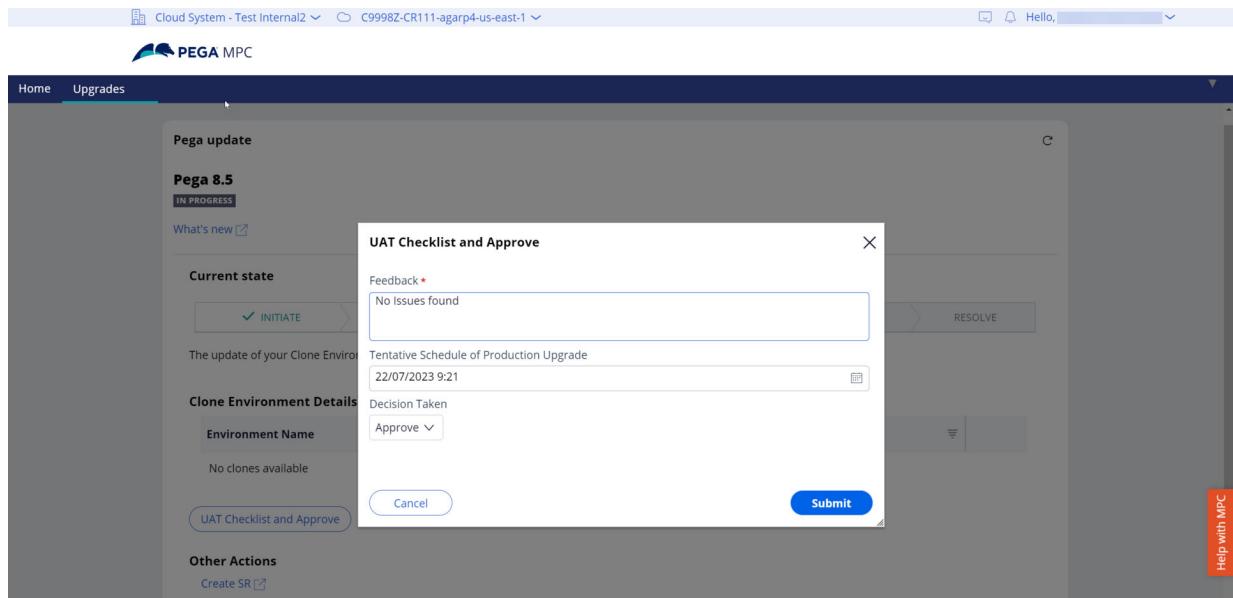
- In the UAT stage view, click the redirect icon for each clone environment (named <Environment Name>-CLONE) on which to perform UAT. The view updates to present a UAT Checklist and Approve button as shown.



Your clone environment view when you are ready to perform UAT testing

- Perform UAT testing as described in "Stage 3: Accept the Basic update of your production environment" in [Pega Cloud update checklist for Pega Infinity release 8.4.2 and later](#).

- After completing UAT testing, click UAT Checklist and Approve, and then enter your tentative schedule for the production update, provide feedback, and check off the required testing and update validation on the clone.



UAT Checklist and Approve dialog box

- In the Decision Taken list select whether you approve the testing on the clone environment for update, and then click Submit.

Result:

If you select Approve, the update process moves into the **Updates** stage.



Important: If you select Reject, the update case enters the Resolved status and stops. You can perform the update another time.

8. Under Updates, you can see the list of environments under the selected account and Project/VPC, scheduled maintenance start time for performing an update. The following image shows when no updates are scheduled.

Name	Type	Region	Pega Version	Target Pega Version	Update Status	MW start time	Temporary URL	Go-NoGO
custupdateenv	Dev/Test	us-east-1	8.6.5	8.7.0	Not Yet Scheduled	12/13/22 2:37 AM		

No update is currently scheduled for any environment within the view

The columns in the table provide different information depending on the update status:

Not yet Scheduled

Environment is not yet scheduled for update.

SCHEDULED

Environment has been scheduled for a certain time.

You can view the scheduled time for the update in the MW start time column.

The **Target Pega Version** column reflects the version to which the environment is to be updated.

ONGOING

The environment update is in progress.

ABORTED BY CUSTOMER

You have aborted the update by selecting Reject during the Go-NoGo action.

COMPLETED

The environment update is completed.

9. During the **ONGOING** status of your production environment update, finalize your update.

In this stage, you receive an **Action center** notification to go to a temporary production URL for your updated environment, and a Go-NoGo button to proceed with the update within the **Updates** tab.

From the point of receiving the notification, you have 60 minutes to promote any necessary changes from the updated staging clone to the temporary production URL, as stated in the message deadline.

For more information about finalizing the update process after using the production URL, see "Stage 4: Accept the Basic update "of your production environment in [Pega Cloud update checklist for Pega Infinity release 8.4.2 and later](#).

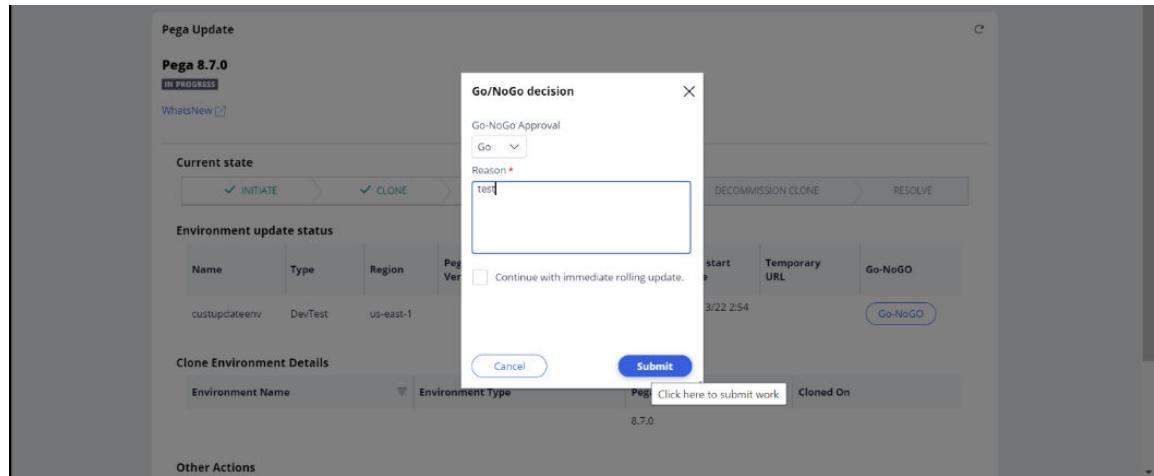
Environment update status table Go/No-Go button

10. In the Updates stage view, click the **Go-NoGo** button, to proceed with a Go/No-Go decision dialog box:

Important: The temporary URL is not displayed if you update from a source version of 8.4.1 or earlier.

⚠ For more information, see [Pega Cloud update checklist for Pega Infinity release 8.4.1 and earlier](#).

- a. Check off each required action of your confidence testing on your temporary production URL according to your requirements.
- b. Specify whether the confidence testing on the temporary production URL environment has met your approval for update:
 - To continue with the rolling update of the production environment, select **Go**, check **Continue with immediate rolling update**, and then click **Submit**.



The interactive Go/No-Go decision dialog box

- To stop the update, select No Go. The Update enters the **ABORTED BY CUSTOMER** status. You can reschedule the upatde at a later time.

Result:

The update process continues until the Completed status. The update process then moves to the **Decommission** stage view.

11. After completing the update process, the decommission of your clone is scheduled.
12. After the decommission of the clone environment, the update process enters the **Resolve** status.

Result:

Your update to the latest version of Pega Platform is successful.

Messages and actions for your Pega Cloud environments

Your My Pega Cloud portal provides you with two message centers about Pega actions that are performed on your environment: actions and messages. These messages help keep you aware of actions occurring or about to occur in your environments.

The portal delivers requests for actions that require your input by using context-sensitive banners below the tabs.

This screenshot shows the My Pega Cloud interface. At the top, there are navigation tabs: 'Cloud System - Test Internal2' and 'C9998Z-CR111-agarp4-us-east-1'. On the right side, there are icons for notifications and a greeting ('Hello,'). Below the tabs, the main header reads 'My Pega Cloud' and 'Pega Cloud 2'. A dark blue banner spans the width of the page. In the center of this banner, there is a white rectangular callout box. The callout box contains three tabs: 'My cloud setup', 'Message center 1', and 'Action center 1'. The 'Action center 1' tab is currently selected. Inside the callout box, the text reads: 'Pega Upgrade Project for "agarp4" is in UAT Stage. Deadline for evaluating UAT is crossed. [Click here](#) to perform appropriate actions.'

This screenshot shows the My Pega Cloud interface. At the top, there are navigation tabs: 'Cloud System - Test Account1' and 'TSTAC1-CR149-PRMPC-us-east-1'. On the right side, there are icons for notifications and a greeting ('Hello, Demo User'). Below the tabs, the main header reads 'My Pega Cloud' and 'Pega Cloud 2'. A dark blue banner spans the width of the page. In the center of this banner, there is a white rectangular callout box. The callout box contains three tabs: 'My cloud setup', 'Message center 1', and 'Action center 0'. The 'Message center 1' tab is currently selected. Inside the callout box, the text reads: 'tstac1-prmpc-mpcenv' and 'Upcoming maintenance - Major infrastructure update for tstac1-prmpc-mpcenv is scheduled on July 24, 2023 06:23 AM.'

Action center and Message center

Action center



The **Action center** provides links for your participation in your upgrade journey, such as a link for the upgrade application testing UAT approval or the go/no-go choice.

Message center

The **Message center** provides messaging about maintenance and self-services operations that you and Pega Cloud services perform on your environment, such as the wake-up progress for your hibernated environment or maintenance that is initiated by Pega.

Troubleshooting using Pega log files in Pega Cloud

Your My Pega Cloud portal provides you with a feedback or issue-reporting mechanism for your experience. You can also view notifications about your self-service actions on your environment. These features help improve your experience and let us know how we can improve the software.

You reach these features in the navigation bar at the upper right of the portal page.

Notifications include the following items for all the environments in the My Pega Cloud portal:

- Restart status of your environments.
 - Download link for your log file upon requesting a log bundle.
1. To report an issue or submit feedback, in the Navigation header, select the Submit feedback icon.
 2. To view available notifications about a self-service action you've made on one of your environments, select the Notifications icon.

The screenshot shows a status summary with three filter checkboxes: 'In Progress' (checked), 'Success/Completed' (checked), and 'Fail' (unchecked). Below the filters, a message states 'Executed PegaAppTierRestart in the environment'. Underneath this message, there is a summary section with the status 'Status: Completed', the reason 'Reason for Restart: Additional details', and the time '6 days ago'.

Example Notification

Using Pega Cloud status

Pega Status is a Pega Cloud® feature that provides you with a display of real-time information on the overall health of each active region in your subscription. You can also see the up-time performance of each component of your Pega Cloud within a deployment region.

One of the key benefits of Pega Cloud is the prioritization of transparency Pega provides clients. Pega understands that knowing the health of your business-critical solutions is important. Use Pega Status and a Status notification subscription to keep informed of the health and availability of your Pega Cloud services by exploring [Pega Status](#).

Using Pega Status, people in your organization with appropriate credentials can see various operational details like a degrade in up-time performance, partial or major outages, and maintenance activities. Furthermore, you can see historical information like past incidents and up-time statuses. A brief description of each region and component is provided for clarity.



Review displays of application or component snapshots which are associated in a specified region in your subscription over a chosen period

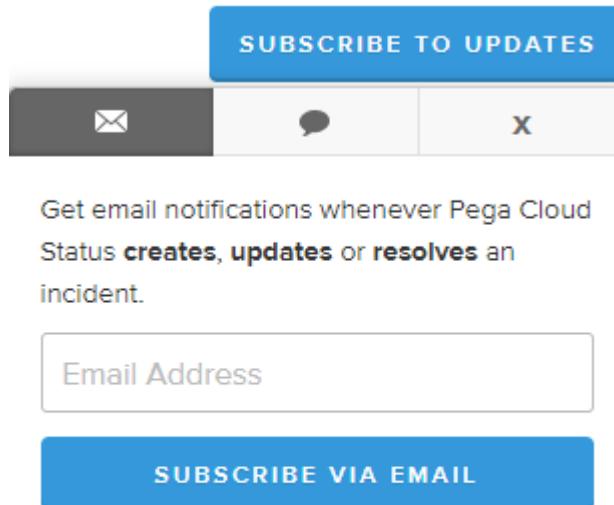
Pega Status options

Pega Status gives you the option to receive notifications about services that may impact your business. After you subscribe, Pega Status automatically sends email notifications any time an incident is created, updated, or resolved. Pega strongly recommends that clients subscribe to all components/regions that are relevant to services they receive from Pega Cloud.

- To subscribe to notifications relevant to your cloud subscription:
 1. Go to [Pega Status](#).

Pega recommends using a desktop browser instead of mobile for subscription configuration.

2. Click [Subscribe to Updates](#).



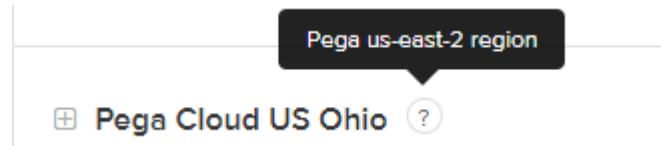
By subscribing you agree to our [Privacy Policy](#).
This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

3. Select the email icon.
4. Enter your email address.
5. Click Subscribe via email.

The system displays a list of supported AWS regions, and the components that are available in each.

6. Choose the components for which you would like to get status updates.
 - a. In the Pega Status page, you can use the tool tip to see what region designation is assigned to its human readable name for each region we support.

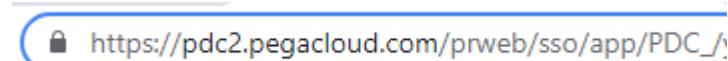
You can see that our US Ohio region is us-east-2 in the following image.



- b. For a list of all Pega Cloud services supported deployment regions, see [Deployment regions for Pega Cloud](#).

To identify the Pega PDC system in which your system is deployed, login to PDC and refer to the URL displayed in your browser.

For example, if you are deployed on PDC2, your browser displays something similar.



7. At the bottom of the page, click Save.

If you need further help deciding what services or regions to subscribe to, see [Pega Support Contact Information](#).

- To change your subscription options:
 1. Go to [Pega Status](#).
 2. Click [Subscribe to Updates](#).
 3. Select the email icon.
 4. Enter your contact information.
 5. Click [Subscribe](#).
 6. On the next page, modify your list of components/products that you wish to subscribe to.

For example, if you are deployed on PDC2, your browser displays something similar.

Components [Select none](#)

▼ Pega Cloud US Northern Virginia

Pega Cloud Services

Pega Chat

Pega CoBrowse

Pega Predicative Diagnostic Cloud 2

Pega Digital Messaging

Pega Search

Pega Content Delivery

Pega Predictive Diagnostic Cloud 5

7. At the bottom of the page, click Save.

- To cancel your subscription:

1. Go to Pega [Status](#).

Pega recommends using a desktop browser instead of mobile for subscription configuration.

2. Click **Subscribe to Updates**.
3. Select the email icon.
4. Enter your contact information.
5. Click **Subscribe**.

6. At the top of the page, click **Unsubscribe from Updates**.
7. Confirm your selection.

Working with your Pega Cloud service

Pega provides services and tools in your Pega Cloud® environments for use with your Pega applications running in your environments.

These services and tools can be divided into the following categories:

Item	Description
Data Management	Covers database maintenance, making external database connections, and other tasks.
Integrating Pega applications with external systems	Covers connecting to REST or SOAP services, and configuring enterprise messaging with either JMS or IBM MQ. It also includes information about the security best practices and the process for conducting security assessments for applications on Pega Cloud
Networking details for your Pega Cloud environments	Covers network migration, and information about using public and private connections.

To ensure your environments and applications work seamlessly together, Pega Cloud does not support customizing your deployment outside the use of Pega Platform™, because these types of customizations can impact your Pega application performance, reliability, and compatibility with future releases. For more information, see [Customizations in client Pega Cloud Service accounts](#).

- [Data management services](#)
- [Understanding and obtaining Pega log files](#)
- [Integrating Pega applications with external systems](#)

- **File management options**
- **Environment restarts**
- **Managing hibernated environments**
- **Change Management process**

Data management services

Pega Cloud® offers you a robust set of options to provide self-service for your data management requirements. Pega Cloud database management functionality lets you interact with your internal Pega Platform™ database directly, making management more accessible.

The database management functions allow you to store data within a secure cloud repository, restore data and attachments as needed, create external database instances for a variety of industry-standard database types, and extract data for use in other systems.

Pega Cloud provides the following database management options:

- Use Query Runner, Query Inspector, and Schema Tools to administer your database on Pega Cloud. For more information, see [Managing your Pega Platform database in Pega Cloud](#).
- Rely on a 30-day database backup and restore for all Pega Cloud environments and file attachments. For more information, see [Pega Cloud database backup and restore](#).
- Utilize Pega Cloud File Storage for a repository to place all your Pega Cloud environment application files. For more information, see [Pega Cloud Services File Storage](#).
- Apply Business Intelligence Exchange (BIX) to extract data from the your Pega Cloud application.

Pega offers BIX as an optional add-on product. Contact your Pega Account Executive to ensure that your license includes BIX access.

For more information, see [Business Information Exchange for Pega Cloud](#).

Note: As a customer, you are responsible for ensuring that production data is present only within production environments. And that all data within lower environments is sample data that does not contain protected health information (PHI), personally identifiable information (PII), and other confidential, classified, private, or sensitive information. Such data is unsuitable for use in non-production environments. Pegasystems is not responsible for classifying or confirming whether production data contains sensitive information and whether that data exists within any cloud environment.

For information about connecting to an external database from your Pega Cloud instance, see [Creating and updating external database instances with JDBC URLs](#).

- [Managing your cloud data storage effectively](#)
- [Database backup and restore](#)
- [Pega Platform database tools](#)
- [Database archiving, purging, and data retention](#)
- [Business Intelligence Exchange for Pega Cloud applications](#)

Managing your cloud data storage effectively

As part of your Pega Cloud® subscription, Pega provisions different types of data storage based on your projected number of users and business metrics. For more information, see [Understanding Pega Cloud services subscription provisioning](#).

As you use your Pega applications in Pega Cloud, your Pega Cloud Data Storage will fill with cases and other data associated with your work. Because this is your company's data, you are responsible for maintaining your Pega Cloud Data Storage as efficiently as possible.

After Pega provisions Cloud Data Storage to you based on your subscription contract, your provisioned space remains the same even as you add or delete cases. If your data storage level is increased as a result of reaching your consumption limits, this new level will become your new standard Cloud Data Storage entitlement. This is why it is critical to manage your storage to avoid reaching a 90 percent consumption threshold.

Pega monitors your Cloud Data Storage usage and notifies you if your usage begins to reach certain thresholds. These proactive notifications remind you to take action to prevent major issues that would occur if you were to use 100 percent of your Cloud Data Storage allocation. At 75 percent, Pega will notify you to take immediate action, such as the recommendations in this article. If you reach 90 percent of your allotted storage capacity, Pega will automatically add data storage to prevent major issues and bill you for the ongoing increased storage.

Another type of cloud storage, [Pega Cloud File Storage](#), stores archived cases and case attachments, and it is more cost effective and more suitable for long term storage than Cloud Data Storage.

Check My Pega Cloud for Cloud Data Storage usage

You can view your Cloud Data Storage usage in My Pega Cloud. In the Environments section of the My Pega Cloud portal home page, choose to View details. Review the amount and percentage of database storage used for the environment you want to manage. For more information, see the [Reviewing environment status and database details](#) section in [Setting up your Pega Cloud environments](#).

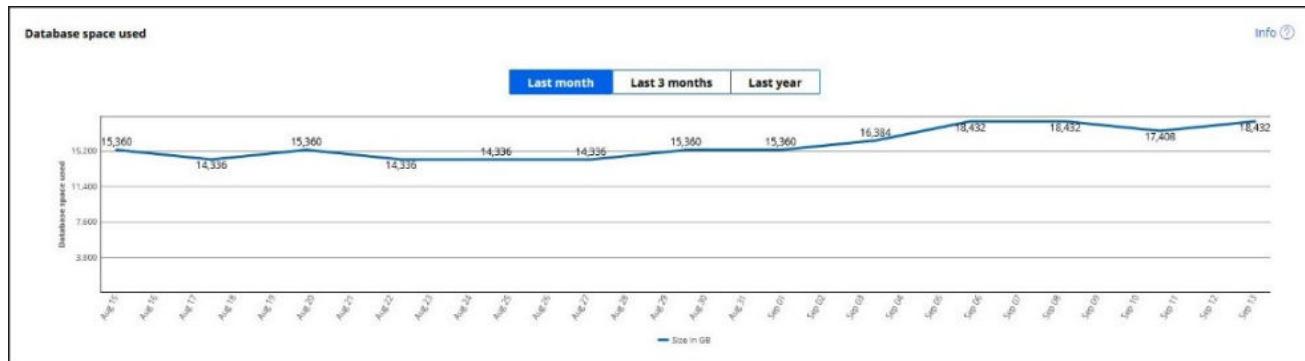
Review your Database metrics using PDC

Pega Diagnostic Center (PDC) is your monitoring tool for troubleshooting Pega application issues.

In PDC, under the System Resources tab, navigate to the Database landing page, and use the Metrics tab to review the database space used over time.

- Evaluate the usage trend for the last month and the last three (3) months.
- Check for the average amount of additional space consumed in the last month and the average increase per day.

If your database space used is continually trending upward, as in the image below, consider implementing a case archival policy.



PDC database Metrics graph

For more information on investigating issues and optimizing your Pega Cloud Data Storage, see [Database statistics in Pega Diagnostic Cloud](#).

Review your Database tables using PDC

Check table information in PDC by navigating to System Resources > Database > Tables > Schema.

Schema	Table	Total bytes	Row estimate	Table bytes	Index bytes	Toast bytes
pegadata	pegaam_db_stats	400,046,227,456	125,926,488	101,883,674,624	298,162,520,064	32,768

- Review your usage of the pc_data_workattach table. If the table has a large byte total, it can indicate that you are storing case attachments improperly, and you should explore migrating your case attachments to [Pega Cloud File Storage](#). For information on using external storage, see [Storing Case attachments using external storage](#).
- Review other relevant history tables, and tables that are not used, including the following tables:
 - pc_history_work
 - pr_history_data
 - pr_other
 - pr_data
 - custom history tables
- Review any tables that can indicate typical issues, where consumption can grow beyond 100,000 rows. For a list of tables, see [Managing table growth](#).
- Review tables for inefficient use of indexes. To perform this review, explore and identify tables in PDC where the index bytes is significantly large relative to table bytes. If you see this pattern, review your indexes, and consider adding or deleting

database indexes. For more information, see [Adding and deleting database indexes](#).

- Review your Index Used Info in System Resource > Database > Tables > Schema > Index Used Info in PDC for indexes that are not currently in use. Indexes that are not used are clearly marked in PDC in the Not used since column. Indexes with a red indicator around the number of days since last used are candidates for review and deletion. Unused indexes are highly inefficient uses of available cloud data storage. For more information, see [Adding and deleting database indexes](#).
- Review tables to ensure they are well designed to process case data storage without growing into oversized data tables. For example, look at the number of rows in the workbasket and worklist tables, which can indicate cases not being resolved in a timely manner. Worktables with a row size exceeding 100,000 often indicate the storage of large objects and inefficient application design, which will eventually cause a drop in case processing efficiency.

Create a Case Archival Policy

Case archival pipelines and the associated purging activity are effective tools for maintaining a predictable and consistent usage of Cloud Data Storage. They can also improve application performance. When a case archival pipeline is in place, case data is moved from Cloud Data Storage to [Pega Cloud File Storage](#).

Use the Pega Platform case archiving feature to move case data out of your Pega Cloud Data Storage to Pega Cloud File Storage. For more information, see [Secondary storage repository for archived data](#).

- Determine how long after a case resolves that you want it to remain in the database.
- Thoroughly plan your policy to exclude certain data from the case archival process. Excluding cases prevents the system from moving them to the Cloud File Storage. For example, you may exclude a case that has a legal hold.
- Archived cases moved to Pega Cloud File Storage remain available for informational purposes, addressing regulatory tasks for statutes such as HIPAA

(Health Insurance Portability and Accountability Act), and responding to questions about business history.

- For more information on setting up an archival process, see [Archiving and expunging case data](#).
- For more information on archiving cases in Pega Cloud, see [Database archiving, purging, and data retention](#).

Note: The Pega case archival and purge pipelines have automatic mechanisms for recovering and making storage available in the database. To fully reclaim

- ⓘ previously used database storage in your environment, [raise a ticket with Pega Support](#). To learn more about case archiving in Pega, review [The case archiving process](#), especially the section on case exclusions.

For information on the tools available to you to manage your Pega Cloud database, such as Query Runner, Query Inspector, and Schema tools, see [Pega Platform database tools](#).

Database backup and restore

Pega Cloud® provides the back-end database that supports your Pega Platform™ application. The system provisions each client environment with dedicated databases inside the client virtual private cloud.

Pega Cloud ensures a window of time for database recovery when you are building a new application in the Pega Platform or extending a Pega application by using Dev Studio. Proactively managing the Pega Platform database and your changes are critical to having a healthy, well-performing application

The database backup and restore service

Pega Cloud offers a data backup and restore service that continuously backs up your data for each environment. Pega Cloud maintains this backup data for the last 30 days. It is not necessary to contact Pega and request a backup; this occurs automatically.

Pega Cloud has the ability to restore your database instance to any time you specify within the 30-day period. If your database is less than 30 days old, Pega Cloud Services can restore your database instance to any point-in-time after its creation.

Pega Cloud also maintains case attachments stored in the Pega Cloud File storage for the 30-day period. For more information about restoring case attachments, see [Using Pega Cloud File storage repository records and sub-folders](#).

Before making changes to your application that might cause a disruption, or if you experience some other application disruption, note the date and time, so you know to what point you would like the data restored if an issue occurs. If the disruption is with the database server itself, that will be handled by a database recovery*, not a restoration.

As long as the requested restore point falls within the last 30 days, Pega Cloud services can restore the database instance. To request that your Pega Cloud database be restored from a prior backup, select [Create a ticket](#) in [My Support Portal](#). For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

Important:



- During the restoration of your database, your environment is not available for the duration of the restoration process.
- Database backup restoration time depends on the size of the deployed system. For systems with over 200 GB of data, restoration might take several hours.

Pega Cloud handles the database restorations; clients do not have to complete any backup or restore tasks. Therefore, clients do not receive “snapshot IDs”, a “backup file”, or a “snapshot” file (these are legacy terms and concepts, and no longer apply to Pega Cloud). The one thing that you must provide is the date and time of the restore point. That's the only identifying information that Pega Cloud uses to complete the

restoration. Following a data restoration, Pega Cloud notifies you that the operation is complete.

Note that database restoration (restoring a database from backup) is different from database recovery (failing over from the primary to the secondary database). For information about database recovery, see [Data backup, data restoration, and data recovery for Pega Cloud](#).

Pega Platform database tools

A Pega Platform™ instance within Pega Cloud® uses an internal database. You can interact with the database through Query Runner, Query Inspector, and Schema Tools after enabling them on your instance of Pega Platform. The functionality of these tools helps you manage your internal database to provide the same experience as on an on-premises system.

To access these tools, you must have the `PegaRULES:DatabaseAdministrator` role in your access group.

The following table describes the functionality each of these tools provides:

Item	Description
Query Runner	Offers options to retrieve data that you pull from your Pega Platform database by using <i>SELECT</i> SQL statements. Query Runner is optimized to use <i>SELECT</i> statements only (instead of other types of SQL statements) for operators with read-only access to the database for the fastest return on your query.
Query Inspector	Improves the <i>SELECT</i> statements that are used through the Query Runner. <i>SELECT</i> statements that you enter into the Query Runner generate the steps in the query statement through an <i>EXPLAIN PLAN</i> output. Use the <i>EXPLAIN PLAN</i> to improve query efficiency.

Item	Description
Schema Tools	Extends a robust set of tools to administer your Pega Platform database, including viewing schema, increasing column size, adding or deleting indexes, and optimizing tables.

Managing your Pega Platform database in Pega Cloud

Pega Cloud® supports certain database operations in Pega Platform™, including adding and deleting database columns and running queries on its composite schemas of *PegaRULES*, *PegaDATA*, and *CustomerData*.

To interact with your Pega Platform database, Pega Cloud provides the following resources:

- Schema Tools
- Query Runner
- Query Inspector
- Dynamic system settings for database retries

You can also use standard Pega Platform functions to configure database tables, for example:

- Increase column length
- Create a table
- Insert records into a table

Additionally, you can update records in the Pega Platform database by writing Java code or using executeRDB SQL run through an Activity. Pega also can help you to identify possible database optimizations that could improve system performance, minimize database size, and improve resource use.

Database management functionality

Pega gives you a range of capabilities to update your database schema, add or delete columns, insert database tables, and update records on your internal Pega Platform database.

You, as a Pega Cloud client, can use the following articles to understand how to perform standard database operations tasks:

Database task	Article
Add a database column	<ul style="list-style-type: none">• Exposing properties and populating database columns• Adding a database column by using the Data Type explorer in Dev Studio
Increase database column length	<ul style="list-style-type: none">• Changing database column length by using the Integration Designer
Alter a column type	<ul style="list-style-type: none">• Changing the type of a field
Create a database table	<ul style="list-style-type: none">• Creating local data storage• Creating classes
Insert records into the database	<ul style="list-style-type: none">• Adding records to a data object• Inserting data records by using SQL
Update records on the database	<ul style="list-style-type: none">• Importing updates from a file• Importing data from a file• Updating data records using SQL

Database task	Article
Deleting records from the database	<ul style="list-style-type: none"> • Deleting a data object • Deleting data records in bulk • Deleting data records by using SQL
Optimizing the database schema	<ul style="list-style-type: none"> • Optimizing a schema

SQL query management

You can use Query Runner and Query Inspector to manage your SQL queries with your internal database. Query Runner and Query Inspector offer Pega Cloud-only functionality for interacting with your internal database.

To learn how to manage SQL queries with Query Runner and Query Inspector, see the following corresponding articles for each database task:

Database task	Article
Run SQL queries	Running SQL queries on Pega Cloud
View SQL query history	Viewing previously run queries
Export SQL queries	Exporting previously run query results
Analyze SQL queries with <i>EXPLAIN PLAN</i>	Using Query Inspector to improve SQL queries

Schema tools for table viewing and interaction

You can use Schema Tools to view and interact with the tables in your internal database. Schema Tools offers Pega Cloud-only functionality to help you.

To learn how to view and interact with database schemas, see the following corresponding articles for each database task.

Database task	Article
View database schema	Viewing database schema information
Increase column length	Increasing column length
View column BLOB size	Viewing column BLOB size
Collect table statistics	Updating statistics
Schedule BLOB size and table statistic updates	Scheduling schema updates
Defragment tables	Defragmenting tables
Create and remove indexes	Adding and deleting database indexes
View the history of actions taken using Schema Tools	Viewing the history of Schema Tools actions

Database retry dynamic system settings

You, as a Pega Cloud client, can change the number of times Pega Platform retries a connection attempt to the internal database before timing out. Changing the number of retries to the internal database can be useful during troubleshooting scenarios.

Note: Pega Cloud permits changing only the parameters for database retries to the internal Pega Platform database. Pega Cloud does not permit you to edit any other parameter for the internal Pega database.

To edit the number of retry attempts Pega Platform makes to each schema for the internal Pega database, create, open, and change the value for the following dynamic system settings:

- `database/databases/PegaRULES/retryAttempts`
- `database/databases/PegaDATA/retryAttempts`

A value of 0 turns off retry attempts to the internal Pega database. Pega Platform defaults to 3 retries for each schema.

For more information about creating a dynamic system setting, see [Creating a dynamic system setting](#).

Database archiving, purging, and data retention

Pega Cloud® clients can archive your resolved case data to Pega Cloud File storage, and then purge the data from your Pega database. Archiving and purging this data can help you to improve system performance and other functionality.

You can also set a data retention policy on data archived to Pega Cloud File storage that expunges the archived data permanently. Periodically purging entries from your database has the following benefits:

- Improves application performance
- Improves search and reporting
- Increases performance for database queries
- Shortens database maintenance cycles
- Reduces primary database costs
- Creates better compliance with government compliance policies, such as the General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA).

For an overview for archiving and purging, see [Archiving and expunging case data](#).

Business Intelligence Exchange for Pega Cloud applications

Business Intelligence Exchange (BIX) provides extract and transform functions for Pega Cloud® clients. You can use BIX to extract application data from your Pega Cloud environments into industry-standard formats that you can import to other popular business intelligence applications.

These high-performance, multi-threaded extraction operations can function independently of Pega Platform™ and give you the option to schedule extracts automatically, which saves you time.

Pega offers BIX as an optional add-on product. To ensure your license includes BIX access, contact your Pega Account Executive.

In Pega Cloud applications that have BIX enabled, you can configure the following items to create an extraction process:

- A BIX extract rule for each rule that you want to use, which specifies the following information:
 - Properties to extract
 - Output file formats such as XML and CSV (delivered as a single compressed file) or a database schema
 - Class instances to extract each time that the extract rule runs (by specifying filter criteria or by choosing the incremental extraction option to select all instances created or modified since the last run of the Extract rule)
- An application connection that places extract files to your chosen directory using BIX FTP listener or the Pega SFTP service
- A Pega Job Scheduler rule to run each Extract rule periodically

For more information, see [Overview of BIX extractions in Pega Cloud environments](#).

Understanding and obtaining Pega log files

Using Pega Cloud® and the My Pega Cloud portal, you have many options for log file access and management to help you monitor and troubleshoot your applications in Pega Cloud.

You can obtain and view the types of logs in the following table for your Pega Cloud by using one of the following methods:

- Downloading log files for troubleshooting

- Streaming Pega logs to an external Amazon S3 bucket
- Streaming Pega logs to Splunk

Log Type	Log File Name	Description
Pega Application*	PegaRULES.log	<p>Contains useful debugging information about the system running your Pega application, including:</p> <ul style="list-style-type: none"> • System errors • Exceptions (with stack trace statements) • Debug statements • Messages not specified as alerts <p>This log includes Pega activity-related messages and standard rules-generated messages.</p>
Pega Application**	PegaRULES-2*.log	Contains similar content as outlined for PegaRULES.log
Cluster (Infrastructure) Logs	PegaCLUSTER*.log	Contains information about the setup and run time behavior of the underlying infrastructure on which your Pega environment runs.
Pega Alerts	PegaRULES-ALERT*.log	Contains diagnostic messages for failures and system events that exceed performance thresholds.

		<p>Each message includes the following type of details:</p> <ul style="list-style-type: none"> • Event description • Value that exceeded the threshold • Type of requestor (for example, browser) • Alert-triggering Pega activity or stream <p>The performance alert message name format is PEGAnnnn, where nnnn is the message ID of the system event that generated the alert.</p>
Security Alerts	PegaRULES-ALERTSECURITY*.log	<p>Contains messages about alerts Pega Platform generates when the security of a Pega web node is at risk.</p> <p>The security alert message name format is SECUnnnn, where nnnn is the message ID of the security event that generated the alert.</p>
Security Events	PegaRULES-SECURITYEVENT*.log	Contains messages about security events generated by a Pega web node. Each

		<p>message includes the following information:</p> <ul style="list-style-type: none"> • <code>appName</code> • <code>eventCategory</code> • <code>eventType</code> • <code>ID</code> • <code>ipAddress</code> • <code>nodeID</code> • <code>outcome</code> • <code>tenantID</code> • <code>timestamp</code> <p>Specific events may contain additional information (such as “message” or “failedOperator”).</p>
DataFlow	PegaDATAFLOW*.log	<p>Contains the events that affect the data flow runs and queue processors, which internally initiate data flow runs. These logs make it possible to view the events involved in the life cycle of the data flow run, which you can use to debug data flow issues on multinode setups.</p>
Usage	PegaUSAGE*.log	<p>Contains performance details for each requestor</p>

		<p>that Pega Platform generates once each hour and at logoff. For more details on these logs, see System-wide usage and the Log-Usage class.</p>
Localhost Access	localhost_access_log	<p>Contains a record of each request to your application as a separate log event that includes the following parameters:</p> <ul style="list-style-type: none">• X-Forwarded-For (XFF) HTTP Header (%i)• Remote IP address (%h) - Source IP address of the requestTime stamp <p>The IP address can be public (as observed by the load balancer) or can originate from infrastructure using a private subnet or the localhost address (for example, healthchecking).</p> <ul style="list-style-type: none">• Date and time (%t)• HTTP verb, URI, protocol and version.

		<p>For example: GET /prweb/PRRestService/monitor/pingService/ping HTTP/1.1 (%r)</p> <ul style="list-style-type: none">• HTTP Response code (%s)• Bytes sent, excluding HTTP headers (%b)• Response Time (%D)• Thread Name (%l) <p>For more information about the generation of and the attributes that are in this Tomcat log, see the Access Logging section of Apache Tomcat 9 Configuration Reference.</p>
--	--	--

*Only applicable on Pega Cloud v3.

**Only applicable on Pega Cloud v2.

- [Downloading log files for troubleshooting](#)
- [Streaming Pega logs to an external Amazon S3 bucket](#)
- [Streaming Pega logs to Splunk](#)

Downloading log files for troubleshooting

As a Pega Cloud® client, you can download log files from the My Pega Cloud portal for internal analysis or to share with Pega Global Client Support (GCS). Being able to download logs is an enhancement to the functionality of [Pega Predictive Diagnostic Cloud](#), which offers you the self-service ability to review alerts and exceptions.

From the My Pega Cloud tab, you can download a bundle of specified log files for up to seven full days of logs created from your environment during the last 365 days. Each download you complete using the My Pega Cloud portal supports up to seven days of logs; to download more additional logs, you must initiate a separate request for the additional day's logs.

Download entire log bundle

From To Time Zone

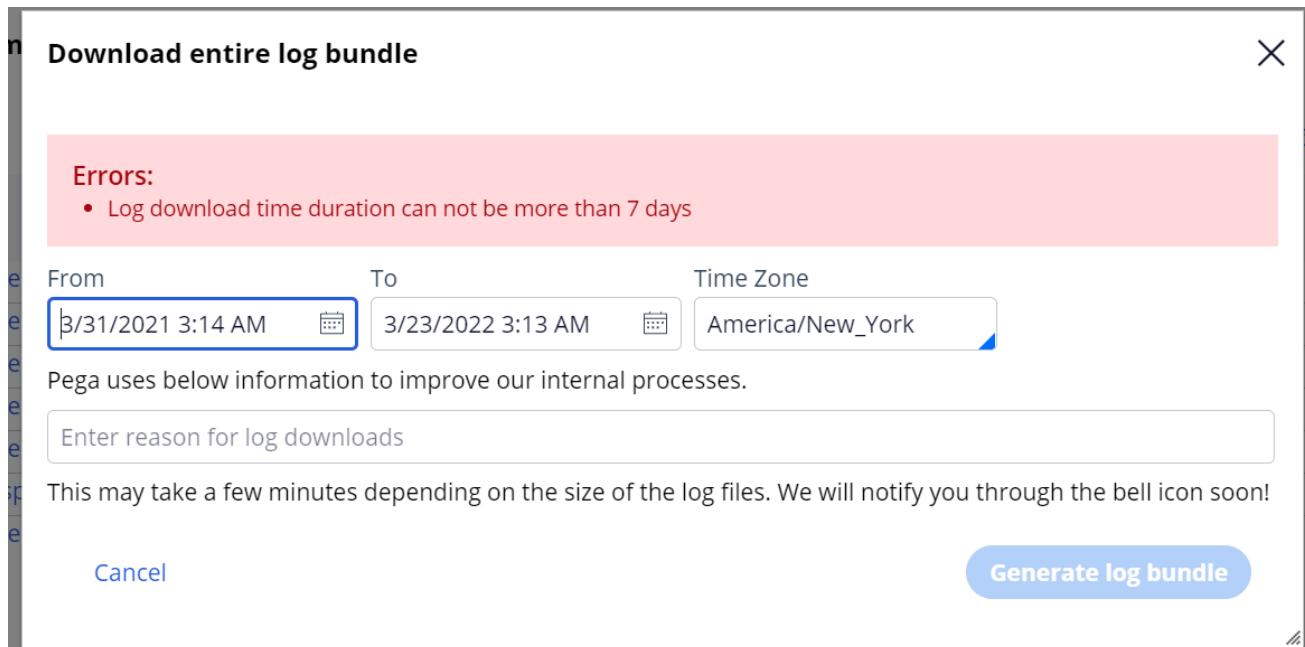
Start time can not be before 365 days from now

Pega uses below information to improve our internal processes.

This may take a few minutes depending on the size of the log files. We will notify you through the bell icon soon!

[Cancel](#) [Generate log bundle](#)

Pega Cloud services supports downloading logs created up to one year ago



Pega Cloud services supports downloading up to seven consecutive days of logs

The log bundle is a compressed TAR file you can download to your local computer.

Pega periodically performs standard maintenance on Pega Cloud systems to update your system to the latest system infrastructure. The system automatically enables this setting after your infrastructure is updated. For more information about standard maintenance policies, see [Pega Cloud maintenance and types of system updates](#).

The following figures shows the screen and dialog where you make your selections for downloading log files:

Environments

Environments					
Name	Pega	Environment Type	Type	Production level	Status
c9997z-hibernation-hibncasetest	8.5.2	DevTest	Sandbox (25 Users)	2	HIBERNATED C
c9997z-hibernation-hibtest3	8.5.2	DevTest	Sandbox (15 Users)	2	HIBERNATED C
c9997z-hibernation-hibtest1	8.5.2	DevTest	Sandbox (25 Users)	2	MAINTENANCE C
c9997z-hibernation-hibtest2	8.5.2	DevTest	Sandbox (25 Users)	2	RUNNING C

Restart
Download logs (tier & file type)
Download logs (bundle)

The Download Logs option is available from your Environments view

Download Logs

From To Time Zone America/New_York

Select Tier Type

<input checked="" type="checkbox"/>	Tier Type
<input checked="" type="checkbox"/>	PegaAppTier
<input checked="" type="checkbox"/>	PegaStreamTier
<input checked="" type="checkbox"/>	PegaUtilTier

Select File Type

<input checked="" type="checkbox"/>	File Type
<input checked="" type="checkbox"/>	PegaCLUSTER
<input checked="" type="checkbox"/>	PegaRULES-ALERT
<input checked="" type="checkbox"/>	PegaRULESv2

We are collecting data to improve log downloads

Enter reason for log downloads

This may take up to a few minutes depending on the size of the log files. We will notify you through the bell icon in a while!

Generate log bundle **Cancel**

Choose up to seven days and specify the types of logs to download

1. Log in to your My Pega Cloud account.
2. Navigate to the My cloud setup tab.
3. In the row containing the environment from which you want the log files, click the More icon.
 - To download logs from a specific tier and file type, select Download logs (tier & file type).
 - Modify the range of dates and time in the From and To fields using the embedded calendar function. Pega supports downloading log files created during the last 365 days.

- In the **Time Zone** field, specify the time zone applicable to your application. For example, if you want to download logs from 1 pm. to 5 pm. IST, select the IST timezone.
- Select a **Tier Type** for which you want to see available log files. You can select one or more available tiers for which you want to download a log bundle; you only see **Tier Types** for tiers with available log files generated within your selected date and time range.
- Select the **File Types** for which you want to see available log files. You only see **File Types** for log files that have been generated within your selected date and time range.
- Enter the reason you are downloading these log files. Pega uses this information to guide future improvements to this log download functionality.
- Click **Generate log bundle**. The **Action center** banner displays below the navigation pane to confirm that your log bungle is being generated.

If no logs are available that match your filter, the **Generate log bundle** button is not enabled.

- When your log bundle successfully completes generating, in the top navigation panel, select the notification icon, and then select **Download log bundle**.
 - Your log bundle downloads to your local system.
- To download all logs from a single point in time, select **Download logs (bundle)**.
 - In the **Download Logs** dialog window, enter the date and time range and associated timezone to download the log files from that environment for that period.
 - Enter the reason for downloading your log files for Pega to improve its client experience with log bundle downloads.

- Click Generate log bundle. The **Action center** banner is displayed below the navigation pane to confirm that your log bungle is being generated.
 - When your log bundle successfully completes generating, in the top navigation panel, select the notification icon, and then select Download log bundle.
 - Your log bundle downloads to your local system.
4. Go to the Activity Center to view the status and availability of your downloaded logs.

The screenshot shows the Pega Activity Center window. At the top, there are three filter checkboxes: 'In Progress' (unchecked), 'Success/Completed' (checked), and 'Fail' (unchecked). Below the filters, a message is displayed: 'Executed DownloadLogs in the environment'. Underneath this message, the status is listed as 'Status: Completed'. A reason for the log download is given as 'Reason for Log Download: Reason for log downloads'. A blue link labeled 'Download log bundle' is highlighted with a red box. The timestamp '8 minutes ago' is shown at the bottom of the message. The Activity Center window has a standard header with 'HOME', 'USERS', 'SUPPORT', and a notification bell icon. The notification bell icon is also highlighted with a red box.

Activity Center notifications for a downloaded log bundle

Streaming Pega logs to an external Amazon S3 bucket

You can configure your Pega Cloud® environment to stream log files to an Amazon Web Services (AWS) S3 bucket in your enterprise AWS account. Streaming logs to your AWS S3 bucket gives you immediate access to your log files without relying on third-party integrations or Pega-provided services.

 **Note:** Log streaming to an external Amazon S3 bucket is only available in AWS Deployment regions for Pega Cloud. Pega Cloud does not currently support streaming logs to an S3 bucket outside of the cloud region where your Pega Cloud environments live.

To complete your log streaming integration with your AWS S3 bucket, make a request by selecting [Create a ticket in My Support Portal](#). Include your AWS account information in the request as described below. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

Pega Cloud supports log streaming integration with your AWS S3 bucket to your Pega Cloud environment using the existing connectivity method already provisioned for your environment.

For more information on log streaming in Pega Cloud, review the [Pega Cloud Log Streaming FAQ](#) on the Pega Support Center.

 **CAUTION:** Pega supports streaming log files from a single environment to a single AWS S3 bucket or streaming the log files of multiple environments to a single S3 bucket. Streaming logs from multiple environments can lead to security vulnerabilities and resource consumption issues.

Enterprise roles required for this task

This task requires the network security administrator role in your enterprise with access to the AWS policies of an S3 bucket and customer managed keys.

Pega responsibilities

Pega Support Engineering will provide several pieces of information that you use to complete the connection and authentication for streaming logs to your S3 bucket:

- An Amazon Resource Name (ARN) that identifies an existing named Identity and Access Management (IAM) Role to allow streaming logs to your S3 bucket.
- An Amazon Resource Name (ARN) that identifies an existing named IAM Role to allow initial configuration and to begin streaming the logs to your S3 bucket.
- A policy statement you must add to the Trust Relationship of your S3 Bucket.
- The policy statements you must add to the Trust Relationship of your KMS Key.

Client responsibilities

You must complete the following tasks:

- Set up an Amazon S3 bucket as your log streaming destination. For information about creating S3 buckets, see [Creating, configuring, and working with Amazon S3 buckets](#).
- After Pega sends you policy statements, add those policies to your S3 bucket and KMS key Trust Statements as appropriate.
- Determine the compression format in which the service delivers logs to your repository. Choose from the following formats:
 - GZIP
 - HADOOP_SNAPPY
 - Snappy
 - ZIP
 - Uncompressed (default)
- Determine the type of customer master key (CMK) encryption that you want to use. For information about CMK encryption, [\(AWS KMS\) Custom Master Keys \(CMKs\)](#).
- Provide Pega Support Engineering with the ARNs of the following artifacts from your AWS account:
 - Your Amazon S3 custom master keys (CMKs) ARN

For example, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`

For more information, see [Finding the key ID and ARN](#).

- Your Amazon S3 bucket name ARN

For example, `arn:aws:s3:::bucket-name`

For more information, see [Amazon Resource Names](#).

- You note the name of your virtual space environment from which you want to stream your Pega logs.

Streaming your Pega logs to an S3 bucket

To stream your Pega logs directly to your S3 bucket, perform the following task:

1. Add the following Amazon S3 bucket details to a text file:
 - Amazon S3 bucket name
 - CMK
 - Compression format for log files sent to your S3 bucket. By default, the compression format is Uncompressed; Pega Cloud supports modifying the format to GZIP or ZIP.
 - The name of the environment from which you want to stream your logs to an S3 bucket
2. Log in to your [My Support Portal](#) account.
3. In the header of **My Support Portal**, click Create a ticket.
4. Use one of the following ways to send the information file securely to the Pega Cloud operations team:
 - Archiving your Amazon S3 log streaming information with a password:
 - In the **Details** section of the request, click Add attachments, and then add a compressed password-protected text file that contains the bucket name, the CMK, the compression format for your log files, and the environment from which you want to stream your logs.

- Continue through the form, and then click **Finish** to send the archive file with your service request.
- Contact the Pega Support team and tell them the password.
- Allowing Pegasystems to download the file from your personal SFTP server
 - Upload a text file that contains the bucket name, the CMK, the compression format for your log files, and the environment from which you want to stream your logs to your personal Secure File Transfer Protocol (SFTP) server.

For more information about SFTP, see [Pega Cloud SFTP service](#).

- Contact the Pega Support team and give them the credentials for the SFTP server.

After the Pega Cloud team receives your request and your Amazon S3 bucket details, in the request reply, Pega Cloud sends you two Amazon Resource Names (ARNs) that define the IAM policies that you need to stream logs to your Amazon S3 bucket in the following formats:

`<client>-delivery-stream-role ARN`

Grants the streaming service access to your Amazon S3 bucket

5. Sign into your Amazon S3 console.
6. Select the bucket to which you want to add the Amazon S3 log streaming service.
7. Click **Permissions**, and then enter the

`<client>-delivery-stream-role ARN` in the bucket policy editor.

For example,

```
{  
  "Version": "yyyy-mm-dd",  
  "Statement": [  
    {  
      "Sid": "PegaKinesisRoleWrite",  
      "Effect": "Allow",
```

```
"Principal": {  
    "AWS":"<>client>-delivery-stream-role ARN>"  
},  
"Action": [  
    "s3>ListBucket",  
    "s3>PutObject",  
    "s3>PutObjectAcl"  
],  
"Resource": [  
    "<>client>-bucket ARN>",  
    "<>client>-bucket ARN>",  
]  
}  
]  
}
```

Streaming logs from multiple environments to a single S3 bucket

If you stream logs from multiple environments, your Resource class must reflect each environment name from which you stream your logs.

CAUTION: This configuration is not the default, recommended option for S3 log streaming. Streaming logs from multiple environments to an S3 bucket can cause security vulnerabilities; the log streaming service can access all folders in the bucket: development, testing, and production. You might also reach the AWS resource consumption cap for your S3 bucket. Stream multiple environment logs to a single S3 bucket at your own risk.

For example,

```
{  
    "Version": "yyyy-mm-dd",  
    "Statement": [  
        {  
            "Sid": "PegaKinesisRoleWrite",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "<>client>-delivery-stream-role ARN>"  
            },  
            "Action": [  
                "s3>ListBucket",  
                "s3>PutObject",  
                "s3>PutObjectAcl"  
            ],  
            "Resource": [  
                "<clientS3bucket>/dev-test/*",  
                "<clientS3bucket>/dev-test-processing-failures/*",  
                "<clientS3bucket>/prod/*",  
                "<clientS3bucket>/prod-processing-failures/*",  
                "<clientS3bucket>/dt1/*",  
                "<clientS3bucket>/dt1-processing-failures/*",  
                "<clientS3bucket>/dt2/*",  
                "<clientS3bucket>/dt2-processing-failures/*",  
                "<clientS3bucket>"  
            ]  
        }  
    ]  
}
```

8. Click Save changes.

For more information about adding a policy to your Amazon S3 bucket, see [Adding a bucket policy using the Amazon S3 console](#).

9. Log in into your AWS KMS console.
10. In the navigation pane, click Customer managed keys.
11. Select the S3 CMK.
12. Select the Key policy tab, and in the key policy editor, add the `PEGA_CFN_ROLE_ARN` and `<client>-delivery-stream-role ARNs`.

For example,

```
{  
    "Version": "2012-10-17",  
    "Id": "key-default-1",  
    "Statement": [  
        {  
            "Sid": "Enable IAM User Permissions",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::<CLIENT_AWS_ACCOUNT>:root"  
            },  
            "Action": "kms:*",  
            "Resource": "*"  
        },  
        {  
            "Sid": "Enable Initial Create Grant",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "<PEGA_CFN_ROLE_ARN>"  
            },  
            "Action": "kms>CreateGrant",  
            "Resource": "<<client>-managed-key ARN>"  
        },  
        {
```

```
"Sid": "Enable Firehose KMS Access",
"Effect": "Allow",
"Principal": {
    "AWS": "<<client>-delivery-stream-service-role>"
},
>Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
],
"Resource": "<<client>-managed-key ARN>"
}
]
```

13. Click Save changes.

Your logs begin streaming, and you can now search for your Pega logs in your Amazon S3 bucket. For example, PegaCLUSTER, PegaRULES-ALERTSECURITY, PegaRULES-ALERT and PegaRULESV1.



Note: Log messages containing exceptions send each message line as an individual log event to avoid data loss.

Filtering unnecessary logs

You can reduce the volume of logs streaming by requesting Pega Support to exclude log types from streaming to your Splunk instance. This is also useful if there are certain logs that you do not wish to view.

In the initial support request for your log streaming Environment (or in a new, subsequent support request), specify which log types you wish to exclude from

streaming to Splunk. Pega Support will make the change during the next infrastructure maintenance update.

Eligible log types to be filtered can be viewed in the table in [Understanding and obtaining Pega log files](#).

S3 Bucket Structure for Pega Logs

After you set up streaming, Pega logs will continuously stream to your S3 bucket and create time-delimited file objects. Each log file in your S3 bucket will contain a mixture of Pega Log Type messages, such as PegaRules, PegaCluster, and PegaAlertSecurity. The folder structure in your S3 bucket will be created as such:

```
/{{S3-Bucket-Name}}/{{Pega-Environment-Name}}/{{YYYY}}/{{MM}}/{{DD}}/{{Auto-Generated-Filename}}
```

{{Pega-Environment-Name}} will be the name of your Pega environment (such as dt1, stg1, preprod, prod). If you do not specify a Pega environment, this field will default to "/logs".

Streaming Pega logs to Splunk

Pega Cloud® offers add-on Pega Platform™ log streaming. By integrating an existing Splunk service with Pega Cloud, you have continuous access to the logs in your Pega Cloud environments. The log streaming service allows to you to efficiently manage your Pega Platform logs dynamically and not have to download logs manually.



Note: Log streaming to Splunk is only available in AWS [Deployment regions for Pega Cloud](#).

To complete a Splunk integration, make a request by selecting [Create a ticket](#) in [My Support Portal](#). Include your Splunk authentication and connection information in the

request. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

Pega Cloud supports Splunk streaming integration to your Pega Cloud environment using the existing connectivity method already provisioned for your environment.

For more information on log streaming in Pega Cloud, review the [Pega Cloud Log Streaming FAQ](#) on the Pega Support Center.

Requirements and limitations

Streaming Pega Platform logs to a Splunk service requires that an administrator for your Pega Cloud account to complete a cloud change request that includes your Splunk authentication details with which Pega Cloud configures your Splunk connection.

To obtain these details, enable the HTTP Event Collector (HEC) for your organization's Splunk account. Enabling HEC requires a Splunk administrator role.

Provide the following details to Pega Support:

- **SPLUNK_HEC_URL:** The URL address for your Splunk HEC endpoint. Include `input-` before the URL. For example:

```
<input-splunkdomain:port>/services/collector
```

- **SPLUNK_HEC_TOKEN:** The authentication token to permit Pega Cloud access to Splunk for log streaming.

Gathering the required Splunk authentication information to include in your Pega Cloud Service Request

When creating your Splunk HEC token, perform the following tasks your Splunk account:

- Enable Secure Socket Layer (SSL) during the token creation.
- Disable the Indexer Acknowledgment.

- Edit the SPLUNK_HEC_URL port number during the token creation.
- Copy the SPLUNK_HEC_TOKEN into a text file.
- Copy the SPLUNK_HEC_URL into the same text file.

Include input- before the URL.

The procedure for enabling HEC for your Splunk account varies by the version of Splunk that you are using. See the Splunk documentation for more information.

Validating your authenticated Splunk connections

Before you send your connection details to permit Pega Cloud access to Splunk, you must validate your Splunk connectivity authentication from your machine to confirm they work. Pega Cloud recommends a temporary SSL test connection to Splunk:

1. From the command prompt, enter:

```
curl -k <SPLUNK_HEC_URL> -H "Authorization: Splunk  
<SPLUNK_HEC_TOKEN>" -d '{"event": "Pega Splunk Test"}' -v
```

2. Confirm the success or failure of the Splunk connection. If you successfully connect, the command returns the following JSON string:

```
{"text": "Success", "code": 0}
```

If you are not successful, you must troubleshoot your connection failure with your Splunk account. You must obtain a valid SPLUNK_HEC_URL and SPLUNK_HEC_TOKEN combination before you send these details to Pega Cloud.

Requesting the log streaming service

After you validate your Splunk authentication information, make a request that includes a securely encrypted archive of the Splunk authentication information that Pega Cloud will use to configure your Splunk connection. Use one of the following methods to send the information file securely to the Pega Cloud operations team:

- Share a password-protected archive:
 1. Log in to your My Support Portal account.
 2. Select [Create a ticket](#) in [My Support Portal](#).
 3. Add the text file that contains the SPLUNK_HEC_TOKEN and SPLUNK_HEC_URL to a compressed archive that is password-protected.
 4. Send the archive file with your service request.
 5. Contact the Pega Support team by email or call and tell them the password.
- Allow Pegasystems Inc. to download the file from your personal Secure File Transfer Protocol (SFTP) server
 1. Log in to your My Support Portal account.
 2. Select [Create a ticket](#) in [My Support Portal](#).
 3. Upload the text file that contains the SPLUNK_HEC_TOKEN and SPLUNK_HEC_URL to your personal Pega Cloud SFTP server. For more information about SFTP, see [Pega Cloud SFTP service](#).
 4. Contact the Pega Support team by email or by calling and give them the credentials for the SFTP server.

Filtering unnecessary logs

You can reduce the volume of logs streaming by requesting Pega Support to exclude log types from streaming to your Splunk instance. This is also useful if there are certain logs that you do not wish to view.

In the initial support request for your log streaming Environment (or in a new, subsequent support request), specify which log types you wish to exclude from streaming to Splunk. Pega Support will make the change during the next infrastructure maintenance update.

Eligible log types to be filtered can be viewed in the table in [Understanding and obtaining Pega log files](#).

Result:

After the Pega Cloud team receives your request and the authentication details file, Pega Cloud authenticates Splunk connectivity from your Pega Cloud environment.

After authenticating connectivity, the Pega Cloud team completes the add-on integration with Splunk and notifies you that your environment has been updated.

Confirming that the log streaming service is active

After you receive confirmation from the Pega Cloud team that the Splunk service integration is complete, your Pega Platform logs are searchable in the Splunk GUI. For example, PegaCLUSTER and PegaRULESV1.

Note that log messages containing exceptions transmit each message line as an individual log event to avoid data loss.

Integrating Pega applications with external systems

When you integrate Pega Platform™ and Pega industry applications, you allow the Pega applications to interact with the applications and your external systems.

To integrate your Pega applications running in Pega Cloud® services environments with your enterprise systems, use the following rule types:

- Resources maintain the connection properties and other configuration data for your Pega applications integrations. They configure services to accomplish work, such as Pega file and email listeners that establish connectivity and processing work rules. It also allows you to add operational meta-data controlling how and when these services get executed.

- Services are used to expose integration points into the application, such as REST APIs.
- Connectors enable your Pega Cloud application (acting as a client) to request information from external systems (servers).

The following resources, services, and connectors are available for integrating Pega applications running in Pega Cloud environments with resources across your enterprise. As with any external system connectivity, ensure that you follow security best practices to mitigate attacks and prevent data loss such as:

- Using strong authentication for all requests
- Ensuring correct authorization of application users
- Securing communications using TLS 1.2

Certificate management practices for developing applications to run in Pega Cloud

Pega Cloud secures inbound interfaces in AWS deployment regions using Amazon ACM root Certificate Authorities (CAs). Modern operating systems and browsers use the Amazon Trust Services CAs by default; if you use an older software or your application is using a custom trust store or certificate store, you must add Amazon Trust Services CAs to ensure seamless connectivity to Pega Cloud.

Due to the dynamic nature of certificates used in Pega Cloud, Pega recommends that source systems and your applications that interact with Pega Cloud environments do not use certificate pinning. This policy aligns with Amazon and Google best practices.

Pega recommends that source systems and your applications that interact with Pega Cloud environments adopt the use of a common alternative to certificate pinning known as Certificate Transparency (CT). For details, see [How CT fits into the wider Web PKI ecosystem](#).

If your application uses certificate pinning to leaf or intermediate certificates, please update your application to pin to all Amazon root certificates or adopt CT practices by April 10, 2023. By doing this, you can avoid any service issues that can occur during an automated certificate renewal by Pega or AWS. This request aligns

with the [AWS certificate manager best practices for certificate pinning](#); to review the latest certificates in use, review the Root CA Certificate Information section of [Amazon trust services Certification Authorities repository](#).

Resources and services

Pega applications running in Pega Cloud environments support integrating with resources in your enterprise using the following industry-standard protocols.

Protocols or services	Description	Related information
SOAP	Create secure SOAP service connections to your endpoint interfaces in Pega when your Pega application running in a Pega Cloud environment needs to act as a web service.	Service SOAP rules
REST	Create secure REST service connections to your endpoint interfaces in Pega when your Pega application running in a Pega Cloud environment needs to support interactions with external systems through web services. As a best practice, use REST connectors instead of HTTP connectors when possible. Service HTTP rules are no longer being actively developed and are	Service REST rules

Protocols or services	Description	Related information
	deprecated beginning in Pega Platform 8.7	
Email	Connect to your enterprise SMTP, IMAP, and POP3 mail server using the Pega Email service to manage your email in Pega applications.	Integrating your application with an email provider
SAP	Supports connecting a SAP system to your Pega Cloud application through the use of SOAP web service protocols.	Service SAP rules
Java Messaging Service	Supports sending messages using JNDI servers with the Java Messaging Service (JMS) standard. For details about using Pega Platform as a messaging service publisher and receiver, see Configuring enterprise messaging using JMS .	Messaging service overview
IBM MQ	Supports interactions with external systems using the IBM WebSphere MQ middleware messaging standard. For details about Pega Platform support for and interoperability with IBM MQ, see Configuring	Configuring enterprise messaging using IBM MQ

Protocols or services	Description	Related information
	<p>enterprise messaging using IBM MQ.</p>	
Secure File Transfer (SFTP)	<p>The Pega Cloud SFTP Service provides Pega Cloud clients with simple, secure file transfers to and from their Pega Cloud applications. The service supports file exchanges between your enterprise and your Pega applications powered by Pega Cloud and uses the Pega Cloud File Storage repository for reliable and resilient storage. Pega Cloud environments do not support using the SFTP connector rules in Pega Platform, because Pega Cloud does not support directly accessing files on the local filesystem of your environment.</p>	Pega Cloud Services SFTP Service

Connectors

Pega applications running in Pega Cloud environments can request data or services from another system using the following industry-standard protocols.

Connector	Description	Related information
SOAP	Use SOAP connector rules when your Pega Cloud application needs to call an external web service.	Connect SOAP rules
HTTP	Use HTTP connector rules when you want your Pega Cloud application to send XML or string data (text) as messages to an external system without the need to comply with messaging standards or protocols such as SOAP.	About Connect HTTP rules
REST	<p>Use REST connector rules in Pega Cloud applications to consume information exposed by REST web services (typically presented as JSON or XML).</p> <p>As a best practice, use REST connectors instead of HTTP connectors when possible.</p>	Connect REST rules
SAP	Use Connect SAP rules in your Pega Cloud application to connect to an existing SAP SOAP web service	Connect SAP rules
DocuSign	Use this smart shape in a flow to send documents for	Flow shapes

Connector	Description	Related information
	electronic signatures by using the DocuSign service.	
Java Messaging Service	<p>Use Java Messaging Service (JMS) rules in your Pega Cloud application to configure enterprise messaging while leveraging Pega Platform as a message publisher and receiver. For details about Pega Platform support for JMS, see Configuring enterprise messaging using JMS.</p>	Messaging service overview
IBM MQ	<p>Use Connect MQ rules in your Pega Cloud applications to configure enterprise messaging using the IBM MQ messaging standard. For details about Pega Platform support for and interoperability with IBM MQ, see Configuring enterprise messaging using IBM MQ.</p>	Connect MQ rules

- [Connecting to REST and SOAP services](#)
- [Configuring enterprise messaging using JMS](#)
- [Configuring enterprise messaging using IBM MQ](#)

Connecting to REST and SOAP services

Use Pega Platform™ REST and SOAP connectors to integrate common web protocols with your Pega Cloud services.

Enterprise roles required for this task

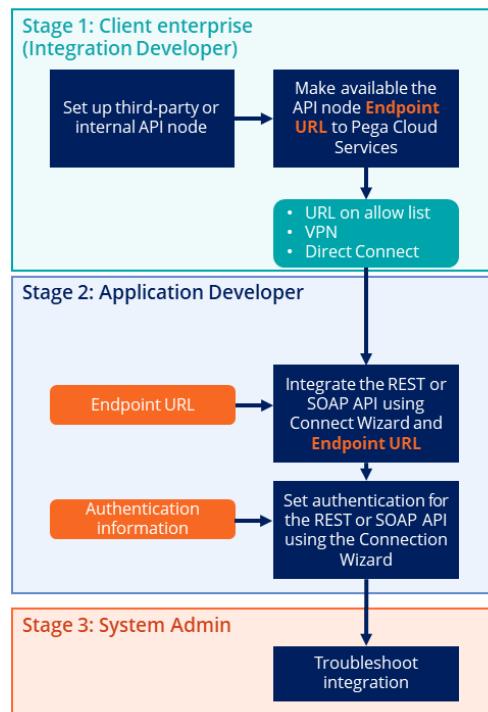
This task requires an integration developer with network administrative privileges that can set up a third-party or internal API node in your enterprise environment.

Pega project team members required for this task

This task requires an application developer role that integrates the source API URL with Pega Platform, and a system admin role that will troubleshoot API integration.

Before you begin:

- Your application developer must have the required access roles for use of the integration wizard.



Integrating REST or SOAP on a Pega Cloud environment

Stage 1

Prior to integrating your chosen REST or SOAP API with Pega Platform, your enterprise integration developer must perform the following tasks:

1. You (integration developer) sets up a third-party or internal API node.

The source API node renders a source URL.

2. Make the source URL available to Pega Cloud following your SaaS enterprise process.

Stage 2

After the REST or SOAP API URL is available to Pega Cloud, work with your integration developer to add the endpoint URL using the Pega Platform REST or SOAP integration wizard:

In the header of Dev Studio click Dev Studio > Integration > Connectors > Create REST Integration or Create SOAP Integration to open the appropriate integration wizard to connect to a REST or SOAP service. For more information, see [Creating a REST integration by using the Create REST integration wizard](#) or [Creating a SOAP integration](#) for their respective processes.

- To add the Endpoint URL to your REST connection, see [Configuring a REST connection](#).
- To add the Endpoint URL to your SOAP connection, see [Selecting operations for SOAP integration](#).

Stage 3

After completing your REST or SOAP integration, your system administrator can troubleshoot your REST or SOAP API integration.

For more information about testing your REST integration, see [Troubleshooting REST connectors](#).

Configuring enterprise messaging using JMS

Integrate a Java Messaging Service (JMS) model using your Pega Platform™ application running in your Pega Cloud® services environments. Pega supports configuring Pega Platform to act as both a JMS publisher (to send messages from your Pega application), and as a JMS receiver (to receive messages in your Pega application).

Pega Cloud services supports synchronous and asynchronous messaging between Pega Platform and other applications and their components, without requiring a direct, compatible integration with your Pega Cloud services environments. A JMS integration can send messages to other applications using that integration with JMS to deliver business data and events to and from your Pega Platform application.

JMS integration requires that you import the requisite JAR files from your JMS provider into your Pega Platform application. To determine the requirements for the JMS files

that you must import for your integration model, refer to your JMS provider documentation.

Note: The client assumes all responsibility for files imported into Pega Cloud. Pegasystems Inc. is not responsible for clients importing files that may contain malicious code. The client can refer to the [to understand the client responsibilities model](#).

Pega Cloud services can integrate the required JMS resources for your JMS model by creating an internal JNDI server, or by adding resource references to your environment for use in your JMS. To request this service, select [Create a ticket](#) in [My Support Portal](#) and include the required details, such as type of resource and connection details. The internal JNDI server and JMS resource go into effect for use in your JMS model after Pega Cloud services restarts your Pega Cloud environment.

For more information about JMS resources, see [Messaging service overview](#).

For more information on how to restart your Pega Cloud environment, see [Restarts in your Pega Cloud environment](#)

For more information about configuring a JMS model to exchange messages between an application and your Pega Cloud services environment, see the following articles:

- Configuring Pega Platform as a JMS publisher
- Testing JMS connectivity and capability
- Configuring Pega Platform as a Java Messaging Service receiver

Configuring enterprise messaging using IBM MQ

Pega Platform™ supports using IBM messaging queues (MQ) in your Pega applications running in Pega Cloud® services environments.

Before you begin:

To configure enterprise messaging for a Pega Platform environment, you must ensure the following conditions:

- IBM MQ servers must be available and accessible from your Pega Platform environment, and you must identify the topics and queues to use. If these servers are not available, you can create mock environments to facilitate integration with your application.
- The IBM MQ servers must be secure and you must configure the required authentication information for using the servers.
- You must install the appropriate Java client libraries installed onto the Pega Platform environment. Verify that you import the correct JAR files and that you have all of the requisite licenses. You may need to restart your system for the libraries to load correctly. For more information about the Java client libraries to install, see the IBM MQ documentation.

 **Note:** The client assumes all responsibility for files imported into Pega Cloud. Pegasystems Inc. is not responsible for clients importing files that may contain malicious code. The client can refer to the to understand the client responsibilities model.

The information here applies to software running both in Pega Cloud and on-premises applications.

Pega Platform supports asynchronous messaging integration configurations using IBM WebSphere MQ (IBM MQ). IBM MQ asynchronous messaging configurations are useful for Pega Cloud applications when REST or SOAP connectivity is not suitable for your application environment.

For asynchronous messaging integration configurations on your systems, Pega Cloud clients are solely responsible for any applications or software that you import into your Pega Cloud services environment, including libraries and requisite licenses: if you import incorrect files or unauthorized software and negatively affect your Pega Cloud services environment, this can result in system downtime and require you to work with Pegasystems Global Customer Support to restore your environment.

Pega Platform has proven interoperability with IBM MQ Version 9 or later.

Configuring messaging with IBM MQ

Configure message security in your IBM MQ server by enforcing encryption, identification, and authorization. For more information, see [Connect MQ rules](#).

File management options

Pega Cloud® gives you options for managing your files, such as Pega Cloud File storage and Pega Cloud SFTP service.

- [Using Pega Cloud File storage](#)
- [Secure Data Transfer service](#)
- [Using Pega Cloud SFTP service](#)

Using Pega Cloud File storage

Pega Cloud® services provides your Pega Cloud with a default repository called Pega Cloud File storage.

Pega Cloud provides this file storage solution as a repository for your Pega applications' case attachments, Pega Cloud SFTP service transactions, archived cases , BIX extracts, and [Exporting interactions and decision results](#).

Key benefits

- Integrated beginning with Pega Platform 7.3

Pega Cloud File storage is pre-configured to support your Pega Cloud applications. Disk space is pre-allocated with separate sub-folders for your cloud environments (development, staging, and production). Default paths are configured for each environment, and security settings used default to the credentials and keys in your Pega Cloud profile.

- **Cost-effective cloud file storage**

Pega Cloud File storage is a cost-effective solution for storing archived cases, case attachments, BIX data extracts, and data uploaded through the Pega Cloud SFTP service. Pega Cloud production subscription clients receive 500 GB of file storage to use across all environments in the subscription. Pega Cloud production subscribers can purchase additional Pega Cloud File storage in 500 GB increments. Pega Cloud File storage costs significantly less than our cloud database storage and is priced well below many of our competitors.

- **No limits on file counts or total storage size**

By not limiting the number or size of files stored, Pega Cloud File storage can scale to your business needs. Individual files can be up to 5 TB.

- **Secure, private, and reliable solution**

Pega Cloud File storage is highly reliable, private, and secure. Only your applications can access your storage space, and data is encrypted both in transit and at rest.

- **The same support staff for both your application and your cloud file storage**

The Pega Cloud Support team provides support for Pega Platform, strategic application solutions, and Pega Cloud File storage. This breadth of knowledge

results in faster and more effective responses, which third-party storage providers cannot match. Pega support services are available 24 hours a day, seven days a week.

- **Soft limits on storage space**

By providing soft limits on storage space, Pega Cloud File storage gives you time to clean up your storage space or purchase additional storage, averting an out-of-space crisis.

- **Data retention policy**

For archived case data, you can apply a data retention policy to delete archived files from Pega Cloud File storage. For more information, see [Archiving and expunging case data](#).

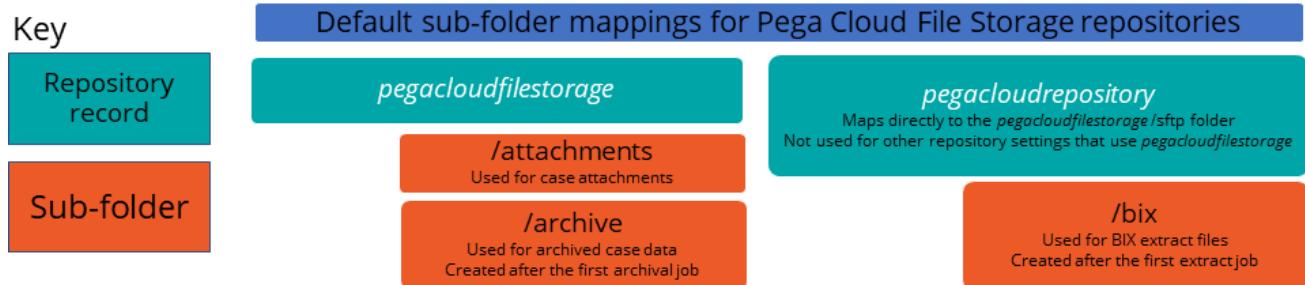
After you delete a file in Pega Cloud File storage, such as by using a data retention policy or REST API, you can recover the file within 30 days of deletion. To review this Pega Cloud services policy details, see [Database backup and restore](#).

Pega Cloud services will not delete any data in your Pega Cloud File storage repository until Pega Cloud services decommissions an environment at your request. For more information about Pega Cloud File storage, contact your Pega Account Executive.

Overview of repository names Pega Cloud services provides by default

When Pega Cloud services provisions your environment, it creates two repositories in your Pega Cloud File storage for your environment, `pegacloudfilestorage` and for SFTP, a mapping from `pegacloudrepository` to `pegacloudfilestorage/sftp`. To see both of these destinations in the Storage Destinations view in Dev Studio, from the header of Dev Studio, click **ConfigureSystemSettingsFile Storage**.

Pega Platform structures the Pega Cloud File storage directory using the logic displayed in the following image.



Pega Cloud File Storage directory structure

You must select or reference the appropriate repository record for your Pega Cloud File storage repository and the associated sub-folder when using Pega Platform to perform the following actions:

Using <code>pegaclo udfilestorag e (/ attachments, /archive)</code>	Method	Using <code>pegacloudre pository (/ bix)</code>	Method
To select Pega Cloud File storage for your application content storage; for an overview, see File and	Select <code>pegacloudfilestorage</code> from the repository list, then browse for the <code>/attachments</code> sub-folder.	To use a REST API to add or delete SFTP files; for an overview, see Using repository APIs in your application.	Enter <code>pegacloudre pository</code> in the destination field.

Using pegaclo udfilestorag e (/ attachments, /archive)	Method	Using pegacloudre pository (/ bix)	Method
content storage.			
To select Pega Cloud File storage for your application case or pulse attachments; for an overview, see Sourcing attachments from external storage.	Select pegacloudfilestorage from the repository list, then browse for the /attachments sub-folder.	To obtain your BIX extract files using an activity; for an overview, see Configuring an activity to access BIX extract files.	Enter pegacloudre pository in the repository name field. Pega Platform automatically creates the /bix sub- folder after you run an initial extraction process.
To send file attachments from Pega Cloud File storage using a REST or SOAP API; for an overview, see Use case: Send file	Select from the pegacloudfilestorage repository list, then browse for the /attachments sub-folder.	When configuring your Pega Cloud SFTP service or BIX FTP listener to access your BIX extract files; for an overview, see Overview of	In the BIX/ sharedpath DSS, enter the filespec file:// pegacloudre pository:/ bix.

Using pegaclo udfilestorag e (/ attachments, /archive)	Method	Using pegacloudre pository (/ bix)	Method
attachments from a repository.		BIX extractions in Pega Cloud environments.	
To process inbound file attachments for storage in Pega Cloud File storage using a REST or SOAP API; for an overview, see Use case: Process inbound file attachments for storage in a repository.	Enter pegacloudfilestorage in the repositoryName field, then / attachments in the folderPath field.	To create additional sub- folders in the / sftp directory.	For detailed steps, see Pega Cloud SFTP service FAQ .
To configure a file listener to process storage in a repository; for an overview, see Using file listeners . This	Enter filespec file:/// pegacloudfilestorage in the repositoryName field, then / attachments in the folderPath field.		

Using <code>pegaclo udfilestorag e(/ attachments, /archive)</code>	Method	Using <code>pegacloudre pository(/ bix)</code>	Method
does not apply to extract files.			
To obtain Pega Cloud File storage files using the Connect-FTP method, see Connect-FTP method .	Enter file spec <code>file:/// pegacloudfilestorage:/ attachments</code> in the <code>remoteFile</code> field as an example.	To obtain BIX extract files from Pega Cloud File storage using the Connect-FTP method, see Connect-FTP method .	Enter file spec <code>file:/// pegacloudre pository:/b ix</code> in the <code>remoteFile</code> field, as an example.
To improve your application performance you can archive outdated case files and place them in your Pega Cloud File storage repository; for an overview, see Archiving	Pega Platform automatically creates the <code>pegacloudfilestorage/ archive</code> repository record sub-folder when you run the initial archival job.		

Using <code>pegaclo</code>	Method	Using	Method
<code>udfilestorag</code> <code>e(/</code> <code>attachments,</code> <code>/archive)</code>		<code>pegacloudre</code> <code>pository(/</code> <code>bix)</code>	
<code>and expunging</code> <code>case data.</code>			

Accessing and managing files in your Pega Cloud File storage pegacloudfilestorage repository

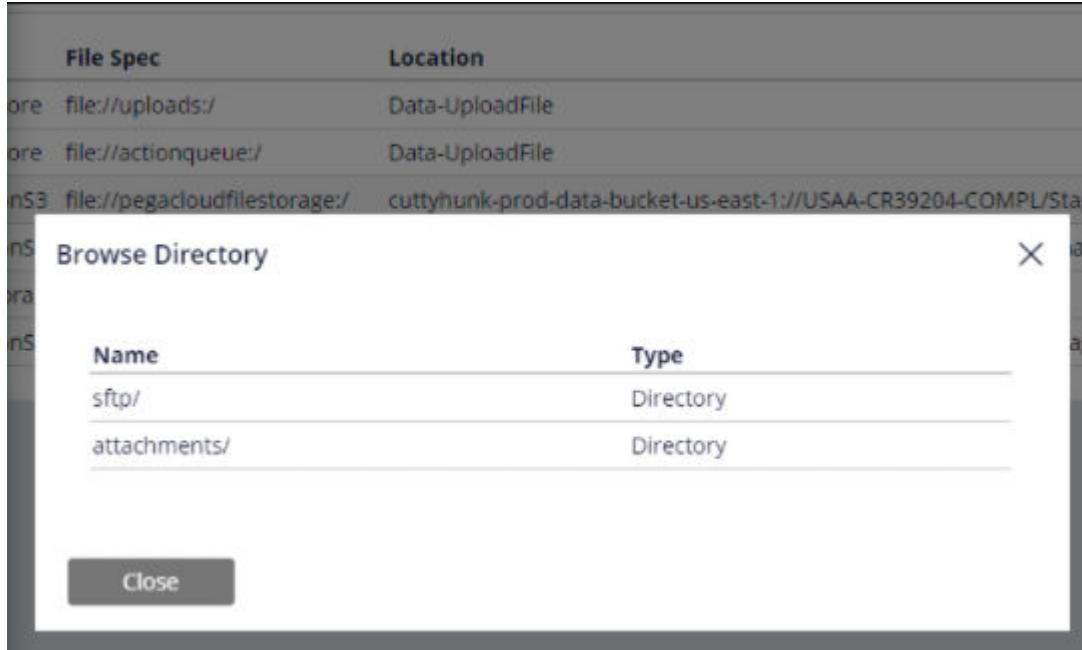
For Pega Cloud services environments, Pega uses Pega Cloud File storage as the default repository, which appears as `pegacloudfilestorage` in the list of repositories in `Records > SysAdmin > Repository`.

Pega Cloud services does not allow direct access to the filesystem in a Pega Cloud File storage repository; instead you manage your files in a Pega Cloud File storage repository with the following methods:

- Use a Pega Platform repository API to manage files in your repository; for an overview, see [Using repository APIs in your application](#).
- Use an SFTP client to interact with the Pega Cloud File storage dedicated SFTP sub-folder through the Pega Cloud services SFTP service, for an overview; for an overview, see [Using Pega Cloud SFTP service](#).
- Configure a file listener to process files in a repository; for an overview, see [Using file listeners](#).

Using Pega Cloud File storage repository records and sub-folders

Pega Cloud File storage stores applicable files in different sub-folders depending on the feature Pega Cloud File storage utilizes.



Pega Cloud File Storage default directory display using your browser

Select the appropriate record for the following Pega Platform features and use cases:

- The pegacloudfilestorage record maps to the sub-folders /attachments for case attachments and \archive for archived case files.

CAUTION: The pegacloudfilestorage record also contains the /sftp sub-folder, but do not select or use the /sftp sub-folder for case attachments and Pulse comments.

- To configure the location for Pega application case attachments, use the pegacloudfilestorage repository record and the /attachments sub-folder.
- To reference archived case data in Pega Cloud, use the pegacloudfilestorage/archive repository record sub-folder, which Pega Platform automatically creates when you run the initial archival job. For case archiving information, see [Archiving and expunging case data](#).

- To create a temporary file storage location sub-folder in `pegacloudfilestorage`, use the following method:
 1. In the navigation pane of Dev Studio, go to Records > Data Model > Data Page.
 2. In the Data Page instance list, filter the Page Name column for `D_pxNewFolder` and select it.
 3. In the Actions list, select Run.
 4. In the Run Data Page: New Folder dialog window, specify your new sub-folder by entering the following information:
 - a. In the repositoryName field, enter `pegacloudfilestorage`.
 - b. In the folderPath field, enter your new folder name. For example, enter `new_folder` to create `pegacloudfilestorage\new_folder`.
 5. To create the folder, in the **Run Data Page: New Folder** dialog window, select Run.

For more information about Pega repository APIs, see [Using repository APIs in your application](#).

- The `pegacloudrepository` record maps to the `pegacloudfilestorage /sftp` subfolder for files you export from Pega Platform using the [SFTP Service](#) and the `/bix` subfolder for extract files. To reference the location used by the Pega Cloud SFTP service, or BIX extract files, use `pegacloudrepository`.
 - When you manage files using an SFTP client configured to use your Pega Cloud SFTP service URL, the `pegacloudrepository` record in Pega Platform automatically directs your connection to the `pegacloudfilestorage /sftp` sub-folder. From the client, your access to this folder originates at the filepath, `/`. For example:

```
sftp> put test.txt  
Uploading test.txt to /test.txt
```

```
test.txt 100% xxxKB xxMB/s 00:01
sftp> get test.txt
Fetching /test.txt to test.txt
/test.txt 100% xxxKB xxMB/s 00:01
```

- To reference, export, or delete BIX extract files using the Pega Cloud SFTP service, BIX FTP server, or an activity, use `pegacloudrepository/bix` sub-folder.

Pega Platform creates the `/bix` sub-folder after you run an initial extraction process. For more information, see [Overview of BIX extractions in Pega Cloud environments](#).

- To send files to your FTP server through a Connect-FTP method, you can source the file location using either `pegacloudfilestorage` and `pegacloudrepository` with the file specification format `file://pegacloudfilestorage:/attachments` or `file://pegacloudrepository:/bix`.

For more information, see [Connect-FTP method](#).

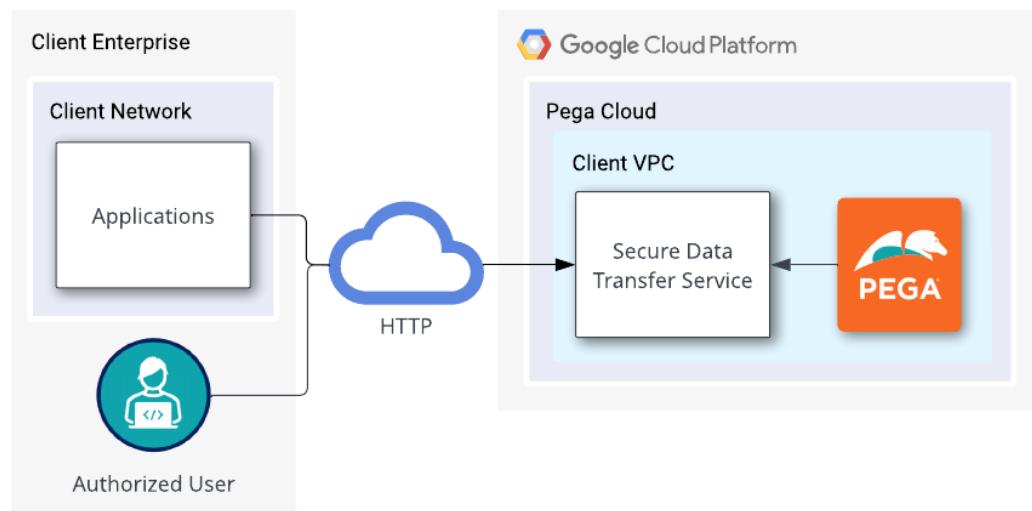
Secure Data Transfer service

The Pega Cloud® Secure Data Transfer service allows you to securely exchange files between your enterprise and your applications running in Pega Cloud. The service provides programmatic access for managing your data within the Pega Cloud File storage repository.

The Secure Data Transfer is an HTTPS service available in GCP deployment regions. For details, see [Deployment regions for Pega Cloud](#). Clients who leverage Pega Cloud on AWS deployment regions will continue using the [Pega Cloud SFTP service](#) which leverages the SFTP protocol.

The Pega Cloud Secure Data Transfer service provides the following features and functionality:

- Direct and secure mapping of an HTTPS connection to or from your Pega Cloud File storage repository. To learn more about file management in Pega Cloud, see [Using Pega Cloud File storage](#).
- Restricted access using a client-provided allow list of IP addresses.
- The option to limit user access to specified directories. By default, new users have access to all folders. User access can be limited to specific folders upon request by clicking [Creating a support ticket in My Support Portal](#).



An overview of the Secure Data Transfer Service in Pega Cloud

Requesting the Pega Cloud Secure Data Transfer Service

To request the Pega Cloud Secure Data Transfer service:

- Generate a public/private key pair using a key generator that leverages an RSA algorithm.
- Compile a list of public IP addresses or CIDR ranges as an allow list. If you request to allow list static IP addresses, add the static IP addresses to an allow list through your enterprise firewall.
- Submit a request in [My Support Portal](#) by clicking [Creating a support ticket](#) and including the following information:
 - The public key
 - The list of public IP addresses or CIDR ranges to allow list. By default, no IP addresses or CIDR ranges are provided access; you must specify which addresses to provide access.
 - Unique usernames to assign to each user. It is best practice to limit usernames to letters, numbers, underscores, and dashes.
 - Optional: the unique names of the subdirectories for each user.



Note: Give a minimum notice of five business days in advance for Pega to complete your request.

Pega Cloud services receives your request, then:

- Deploys the service based on the information you provided.
- Enables traffic from the static IP address you provided.
- Integrates the service with your Pega Cloud environments.
- Authenticates the service using the public keys you provided.
- Encrypts [data-in-transit](#) and [data-at-rest](#) using an environment-specific key.

Pega Cloud services provides you the following information to connect to the service:

- Pega Cloud Secure Data Transfer service hostname
- The authentication URL, client ID, scope, and audience that will be used to generate an OKTA token and authenticate your system with the service.

- Top-level directory within the Pega Cloud File storage `pegacloudrepository` folder.
- Unique subdirectories for each user, at your request.

Note: All new users will have access to the top-level directory folder in the

- ⓘ Pega Cloud File storage repository by default. It is not necessary to specify any directory name if you want the user to have access to all directories.

Security standard

The Pega Cloud Secure Data Transfer service security model supports multiple single-user access authentication using a private/public key pair. During the request process, Pega Cloud services stores the public key and associates it with a specific client. Pega Cloud uses this client-provided public key to configure authentication to the service.

Ensure that users of this service within your organization are informed of and adhere to your organization's internal security practices for protecting or masking sensitive data used within your Pega application. To transfer your data securely, review and implement the security practices outlined in [Security Checklist on Pega Cloud](#).

Data management considerations

As a best practice, follow these file storage and data management guidelines:

- **File storage utilization:** The Pega Cloud Secure Data Transfer service uses Pega Cloud File storage available within the dedicated `pegacloudrepository` directory. The amount of storage allocated is specified in your Pega Cloud subscription. For more information, see [Using Pega Cloud File storage](#).
- **File management:** To manage your files in the Pega Cloud File storage repository, use the Repository API to interact with your files or configure a file listener to process your files. For more information, see [Using Pega Cloud File storage](#).
- **Data cleanup:** You are responsible for managing your data files according to your enterprise's best business practices.

- **Authenticating your system with the Secure Data Transfer service**
- **Using the Secure Data Transfer service**

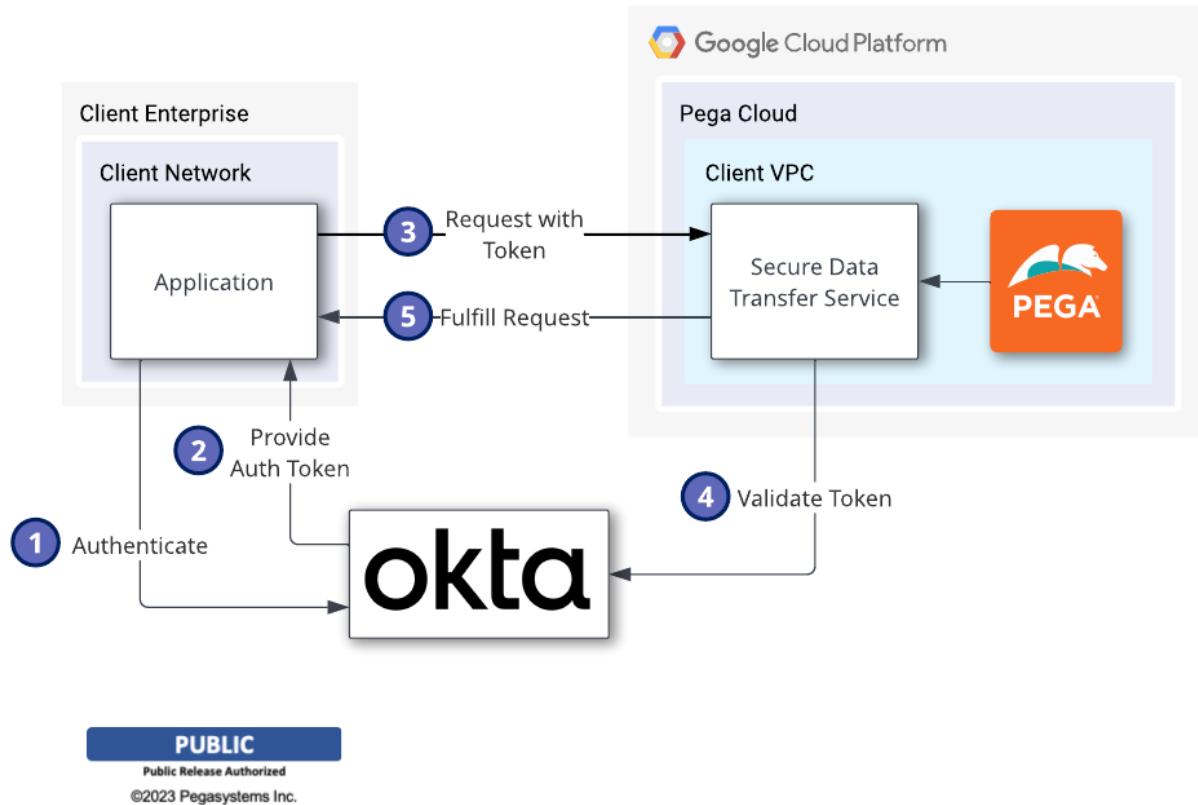
Authenticating your system with the Secure Data Transfer service

To authenticate your system with the Pega Cloud® Secure Data Transfer service, generate a token which can be used for Data Transfer API calls. Tokens expire after one hour, and new tokens need to be generated accordingly.

Before you begin:

It is the client's responsibility to generate tokens for authentication. Ensure that the private key and password are stored in a safe, secure manner so no external entities can access them and perform unauthorized actions.

Pega leverages [Okta](#) as its Identity Management provider to secure and authenticate data in the Secure Data Transfer service. Okta provides several Software Development Kits (SDKs) in different programming languages including Java, Python, Go, .NET, PHP, or Node.js which can be used in the token generation process. For more information, including example code snippets on how to do this, see [Okta SDK documentation](#) and [Build a JWT for Client Authentication](#).



An overview of authenticating with the Secure Data Transfer Service in Pega Cloud

Pega supports multiple methods to generate tokens. The example below is provided for your reference; however, other methods may be used to generate a token.

1. Create a .env file that stores your private key, its password, client ID, Okta URL, and the scopes. These values need to be provided as input, and they will be used to complete the entire procedure.
2. Satisfy the requirements within the requirements.txt file. All relevant file contents and commands are in the Python script below.
3. Run the Python script below in your environment.

When you execute the Python script below, Okta generates the token for authentication, which creates a JSON Web Token (JWT) based on your private key, client ID, scopes, and Okta server URL. Then, the script uses your authentication token to generate a token to authorize your system with the Secure Data Transfer Service, which enables you to [perform requests using the Data Transfer API](#).

The Python script below has descriptive comments and executes the entire process to generate a token for [running Data Transfer API calls](#).

```
.env
```

```
PRIVATE_KEY='-----BEGIN RSA PRIVATE KEY-----  
{PRIVATE-KEY-CONTENT}  
-----END RSA PRIVATE KEY-----  
'  
  
PRIVATE_KEY_PASSWORD={PRIVATE-KEY-PASSWORD}  
CLIENT_ID={CLIENT-ID}  
OKTA_URL=https://{{DOMAIN}}/oauth2/{{ID}}  
SCOPES=pega.oss:dtr.write
```

```
requirements.txt
```

```
ffi==1.15.1 # https://cffi.readthedocs.io/en/latest/  
cryptography==40.0.1 # https://cryptography.io/en/latest/  
pycparser==2.21 # https://pypi.org/project/pycparser/#history  
PyJWT==2.6.0 # https://pyjwt.readthedocs.io/en/stable/  
python-dotenv==1.0.0 # https://pypi.org/project/python-dotenv/#history  
$ pip install --upgrade pip  
$ pip install -r requirements.txt
```

```
token_generation.py
```

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import time
import os
import http.client

import jwt
import dotenv

from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import serialization

# Loading environment variables
dotenv_path = os.path.join(os.path.dirname(__file__), '.env')
dotenv.load_dotenv(dotenv_path)

# Environment variables to be used as an input for token generation
private_key_env = os.environ.get('PRIVATE_KEY')
private_key_password_env = os.environ['PRIVATE_KEY_PASSWORD']
client_id_env = os.environ.get('CLIENT_ID')
okta_url_env = os.environ.get('OKTA_URL')
scopes_env = os.environ.get('SCOPES')

# Extracting relevant information from URL
okta_url_env_split = okta_url_env[8:].split("/")
okta_url, okta_id = okta_url_env_split[0], okta_url_env_split[2]

# Expiration time in seconds
exp_time_seconds = 3600
```

```
# Step 1 - token generation for Okta authentication
pem_private_key = serialization.load_pem_private_key(
    str.encode(private_key_env),
    password=private_key_password_env.encode(),
    backend=default_backend()
)
private_key_jwt_token = jwt.encode({
    'iss': client_id_env,
    'sub': client_id_env,
    'aud': f'https://{{okta_url}}/oauth2/{{okta_id}}/v1/token',
    'exp': int(time.time()) + exp_time_seconds
},
    pem_private_key,
    algorithm='RS256',
)

# Step 2 - token generation for Data Transfer API authorization
https_connection = http.client.HTTPSConnection(okta_url)
payload = f'grant_type=client_credentials&scope={{scopes_env}}&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer&client_assertion={{private_key_jwt_token}}'
headers = {
    'Accept': 'application/json',
    'Content-Type': 'application/x-www-form-urlencoded'
}
https_connection.request('POST', f'/oauth2/{{okta_id}}/v1/token', payload, headers)
response = https_connection.getresponse()
data = response.read()
print("Data Transfer API Token: ", data)

$ chmod u+x token_generation.py
```

```
$ ./token_generation.py
```

What to do next:

To use the Secure Data Transfer service and the Data Transfer API, see [Using the Secure Data Transfer service](#).

Using the Secure Data Transfer service

The Pega Cloud Secure Data Transfer service allows you to securely exchange files between your enterprise and your applications running in Pega Cloud. The Data Transfer API allows you to execute requests to the Secure Data Transfer Service.

Before you begin, you must generate a token to authenticate your system with the Secure Data Transfer service. To learn more about authenticating with the Secure Data Transfer service, see [Authenticating your system with the Secure Data Transfer service](#).

Note: The process of making calls to the Data Transfer API is the client's responsibility. The examples provided in this document using cURL are provided for your convenience; however, other methods may be used to make calls to the Data Transfer API.

Authenticating your call using the token

Authenticate your call to the Data Transfer API using your token in a system of your choice. Ensure you provide the token in the correct format in the header of your call.

An example of authenticating an API call using cURL is shown below.

```
curl -i -X PUT -F file=@test.txt https://k7sm9rwtp4gsm36a.datatransfer.integration.pegaservice.net/v1/objects/tenant090523/test.txt -H "Authorization: Bearer eyJraWQiOij5d3l3Sk5..."
```

Endpoint Variables

The table below describes the variables within each API endpoint.

Variable	Description	Example
DTS_API_URL	Data Transfer API URL provided by Pega to the client.	https://k7sm9rwtp4gsm36a.datatransfer.integration.pegaservice.net
DT_CLIENT_NAME	Data Transfer username that the client provided when requesting the service	client_name
OBJECT_NAME	Name of the given object which either already exists or will exist in the Data Transfer Data Store	File.txt

Uploading objects with PUT Endpoint

The table below describes this endpoint, its parameters, and potential responses.

Method	PUT
Endpoint	<code> \${DT_API_URL}/v1/objects/\${DT_CLIENT_NAME}/\${OBJECT_NAME}</code>

Description	Used to upload the object with given name to the Data Transfer Data Store under the HOME directory or subdirectory.
Request Body	Type: multipart/form-data Key: file Value: file on local disk
Authorization Header	Authorization: Bearer TOKEN
Query Parameters	None
Responses	200 OK "Object uploaded" 400 Bad Request "Object name cannot end with slash (/)" "Object name cannot be empty" 401 Unauthorized 403 Access Denied 404 Not Found - "An error occurred when getting path and bucket name of tenant" 500 Internal Server Error - "An error occurred when forming a file for object"

An example of uploading an object to the HOME directory using cURL is shown below.

```
$ curl -i -X PUT -F file=@test.txt https://k7sm9rwtp4gsm36a.datatransfer.integration.pegaservice.net/v1/objects/tenant090523/test.txt -H "Authorization: Bearer eyJraWQiOiJ5d3l3Sk5..."
```

An example of uploading an object to a subdirectory using cURL is shown below.

```
$ curl -i -X PUT -F file=@test.txt https://k7sm9rwtp4gsm36a.datatransfer.integration.pegaservice.net/v1/objects/tenant090523/test%2Ftest.txt -H "Authorization: Bearer eyJraWQiOij5d3l3Sk5..."
```

Deleting objects with DELETE Endpoint

The table below describes this endpoint, its parameters, and potential responses.

Method	DELETE
Endpoint	<code> \${DT_API_URL}/v1/objects/\${DT_CLIENT_NAME}/\${OBJECT_NAME}</code>
Description	Used to delete an object with a given name from the Data Transfer Data Store from the HOME directory if not specified otherwise as a part of the request.
Authorization Header	Authorization: Bearer TOKEN
Query Parameters	None
Responses	<p>200 OK</p> <p>400 Bad Request - "The object name cannot be empty"</p> <p>401 Unauthorized</p> <p>403 Access Denied</p> <p>404 Not Found - "An error occurred when getting object for tenant on delete operation"</p> <p>500 Internal Server Error "An error occurred when getting path and bucket name of tenant"</p>

	<p>"An error occurred when getting object for tenant on delete operation"</p> <p>"An error occurred when deleting object for tenant"</p>
--	--

Downloading objects with GET Endpoint

The table below describes this endpoint, its parameters, and potential responses.

Method	GET
Endpoint	<code> \${DT_API_URL}/v1/objects/\${DT_CLIENT_NAME}/\${OBJECT_NAME}</code>
Description	Used to download the object with a given name from the Data Transfer Data Store from the HOME directory if not specified otherwise as a part of the request.
Authorization Header	Authorization: Bearer TOKEN
Query Parameters	None
Responses	<p>200 OK - Object content</p> <p>401 Unauthorized</p> <p>403 Access Denied</p> <p>404 Not Found</p> <p>"An error occurred when getting path and bucket name of tenant"</p> <p>"An error occurred when getting object attributes for tenant"</p> <p>"An error occurred when getting object for tenant"</p>

413 Request Entity Too Large - "Object size (%d bytes) exceeds download size limit of %d bytes"
 500 Internal Server Error - "An error occurred when reading object for tenant"

Listing all objects with GET Endpoint

The table below describes this endpoint, its parameters, and potential responses.

Method	GET
Endpoint	<code> \${DT_API_URL}/v1/objects/{DT_CLIENT_NAME}</code>
Description	Used to list all objects from the Data Transfer Data Store. The list can be limited to some specific objects if query parameters are provided as a part of the request.
Authorization Header	Authorization: Bearer TOKEN
Query Parameters	<ul style="list-style-type: none"> • maxKeys: A query parameter of type integer which specifies up to how many objects should be returned in the response (default and maximum possible value: 1000) • delimiter: A query parameter of type string which specifies a pattern to group the objects (case-sensitive) • prefix: A query parameter of type string which limits the objects in the response

to those that begin with the specific value (case-sensitive)

- **startAfter:** A query parameter of type string which limits the object in the response to those that are alphabetically after the specific value (case-sensitive)
- **continuationToken:** A query parameter of type string in base64 format which is used to determine which page of objects to start listing from (It can be retrieved from previous call from NextContinuationToken)



Note: All parameters for this endpoint are optional.

Responses

200 OK – List of Objects

400 Bad Request - "Invalid maxKeys value provided (%d) - argument maxKeys should be an integer between 1 and 1000"

401 Unauthorized

403 Access Denied

404 Not Found - "Bucket does not exist"

500 Internal Server Error

"An error occurred when getting path and bucket name of the tenant"

"An error occurred when trying to list objects from the page"

An example of listing an object with the maxKeys parameter using cURL is shown below.

```
$ curl -i -X GET https://k7sm9rwtp4gsm36a.datatransfer.integration.pegaservice.net/v1/objects/tenant090523?maxKeys=1 -H "Authorization: Bearer TOKEN"
```

Troubleshooting the Data Transfer API

If you experience any issues with the Secure Data Transfer service or the Data Transfer API, [create a ticket](#) in [My Support Portal](#) and provide the following information:

- Endpoint
- HTTP Method used to make the call (PUT/GET/DELETE)
- Parameters used in the call
- Whether a token was in use when the error occurred
- Error code and response

This information will help Pega Cloud services investigate why the call did not work as expected.

Using Pega Cloud SFTP service

The Pega Cloud® SFTP service allows you to securely exchange files between your enterprise and your Pega Platform™ applications running in Pega Cloud. The service automatically accesses your application data in your Pega Cloud File storage repository.

The Pega Cloud SFTP service provides the following features and functionality:

- Direct and secure mapping of your SFTP connection to or from your Pega Cloud File storage repository. To review the benefits and file management details, see [Using Pega Cloud File storage](#).
- Static IP addresses that do not change for the life of the service, which eliminates the need for you to add a broad range of IP addresses to a list of allowed connections for the service.

- New Pega Cloud deployments as of 17 November 2021 provide an SFTP service with one SFTP server for each client subscription that supports all your environments deployments, such as DevTest, Staging, and Production. Pega Cloud services continues to support existing client subscriptions that provide your SFTP service with a unique URL for each environment until you reach a service version that requires a migration of your service to the newer SFTP service. Pega Cloud services support will communicate with you well in advance of any migration plan for your service.
- Clients connect securely to your SFTP clients service in Pega Cloud from your enterprise data center over the Internet using your preferred SFTP connection method. Pega Cloud services does not support using private connectivity options.
- Admin user and, if requested, up to 10 additional standard-user credentials with unique file directories within your Pega Cloud File storage repository. You may have up to 20 additional standard-user credentials with unique file directories after upgrading to the newer SFTP service version (which requires Pega Cloud major infrastructure update). To add users, clients need to request Pega Cloud services to add access for any additional users with a minimum notice of five business days in advance for the request.
- Bulk data processing through file listeners in your Pega Cloud environment applications or integration with Pega Business Intelligence Exchange™ data extracts to your Pega Cloud File storage repository until you remove it.

Client responsibilities

Client responsibilities include the following actions:

- You install your preferred SFTP or SSH client to connect to the Pega Cloud SFTP service.
- You generate the public/private key pair for each user that you create for the Pega Cloud SFTP service to use with your preferred SSH client.
- You enable one or more users in your Pega Cloud subscription to authenticate and then connect to your SFTP service. To allow these additional users, the admin user of the service needs to [create a ticket](#) in [My Support Portal](#) by selecting New

request and include the following information for each additional user of the SFTP service:

- At least one public key to assign to the default admin user.
- A list of IP addresses or IP address ranges to add to an allow list for the Pega SFTP service.
- Unique user name to assign to each additional user (one per user).
- Unique directory name for each additional user.
 - Each user can only have one directory name, but one directory name can be used for multiple users.
- Public key for each additional user that you want to access the service.
- (Optional) If you have strict HostKey checks in your firewall or SFTP application, you can request the server HostKey in the ticket. This way, you can configure the HostKey before connecting to the server.



Note: Give a minimum notice of five business days in advance for Pega Cloud to complete your request.

For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

- You ensure that your developers are informed of and adhere to your organization's internal security practices pertaining to protecting or masking sensitive data used within your Pega application. To secure your data, review and implement the best security practices as outlined in [Security Checklist when deploying on Pega Cloud](#).
- You add the static IP for the Pega SFTP server to an allow list through your enterprise firewall that Pega Cloud services provides, for requests to implement a static IP address.

Pegasystems responsibilities

Pegasystems responsibilities include the following actions:

- Integrate the SFTP service with all of your Pega Cloud environments.
- Authenticate the SFTP service using the public keys that you provided.
- Provide you with the following information to connect to the SFTP service:
 - Pega SFTP hostname
 - Top-level SFTP directory within the Pega Cloud File storage `pegacloudrepository` folder
 - Admin username
 - Admin key
 - Additional user access, based on username, as requested by the client
 - Unique SFTP sub-directory for each username as requested by the client
 - Unique key associated with each additional user as requested by the client



Note: If you request only one user, that user as admin privileges with access to the top-level directory of the SFTP folder in the Pega Cloud File storage repository. It is unnecessary for the admin user to specify an additional directory name.

- Encrypt data-in-transit by using SSH and data-at-rest based using an environment-specific key.
- Deploy the SFTP service with the public key and public IP addresses that you provided.
- Provide you the static IP address of the SFTP server for you to add to a list of allowed connections for requests to implement a static IP address.

Connecting to the Pega Cloud SFTP service

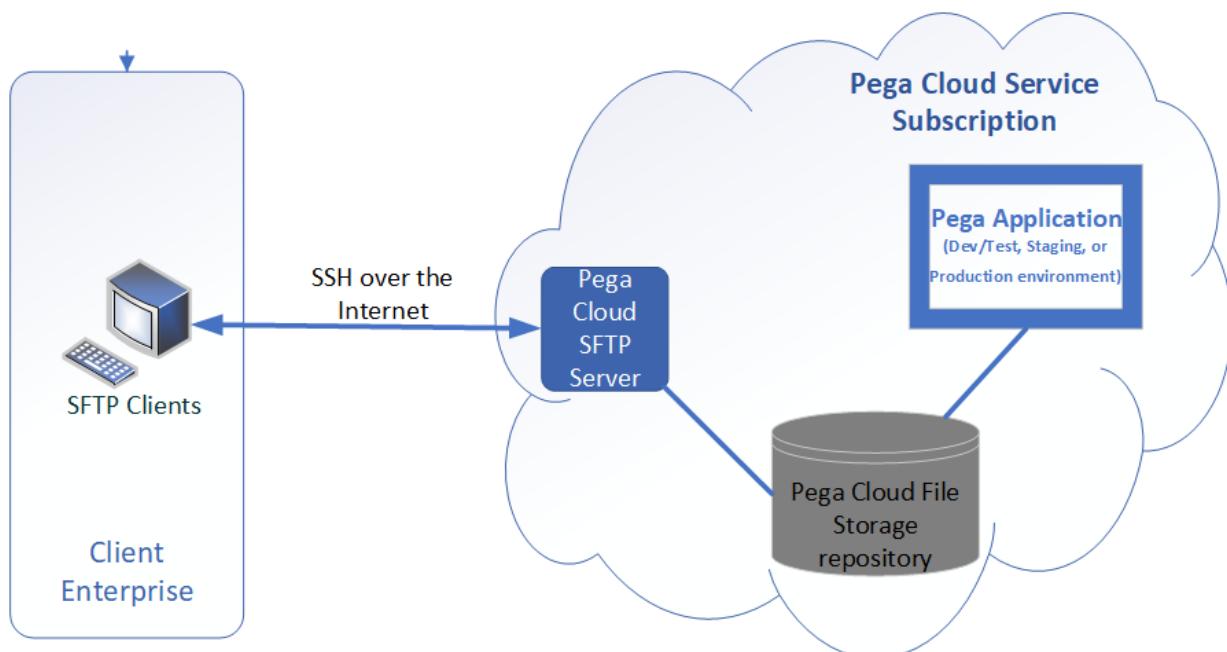
After compiling a list of public IP addresses and generating a public/private key pair, complete the following actions:

1. Log in to your My Support Portal account.
2. Click [Create a ticket](#), and include the public key and IP addresses that are already added to an allow list.



Note: Clients must give a minimum advance notice of 5 business days for the request.

3. Pega Cloud services receives your request then deploys your Pega Cloud SFTP service.
4. Pega Cloud services sends you a file that contains the SFTP hostname, SFTP username, and folder URL used to access the SFTP service.
5. Configure your SFTP client or SSH shell with the hostname, SFTP username, and folder URL to interact with the Pega Cloud SFTP service. Any added, non-admin-level users can access only their unique sub-directory in the admin account. The admin user can access all the sub-directories of the standard users.



Securely transfer data between your enterprise and your Pega applications running in Pega Cloud

Security standard

The Pega Cloud SFTP service security model supports multiple single-user access authentication using a private/public key pair. During client onboarding, Pega Cloud

uses a client-provided public key to configure authentication to the service. All SFTP services in the subscription require an environment-specific key for connectivity to your Pega Cloud environment.

Data management considerations

As a best practice, use the following file storage and data management guidelines:

- File storage utilization: The Pega Cloud SFTP service uses Pega Cloud File storage that is available within the SFTP-dedicated `pegacloudrepository` directory according to the allocation that is specified in your Pega Cloud subscription. For more information, see [Using Pega Cloud File storage](#).
- Data cleanup: You are responsible for managing your data files according to your enterprise best business practices by using your preferred SFTP client.
- To manage your files in the Pega Cloud File storage repository, use the Repository API to interact with your files or configure a file listener to process your files. For more information, see [Using Pega Cloud File storage](#).
- [Pega Cloud SFTP service FAQ](#)

Pega Cloud SFTP service FAQ

Consider these Frequently Asked Questions (FAQ) to become familiar with common inquiries about the Pega Cloud® SFTP service.

What environment types are supported for the Pega Cloud SFTP service?

Pega Cloud supports the use of the Pega Cloud SFTP service in Dev/Test, Staging, and Production environment deployments. Neither Deployment Manager nor Agile Studio environments support the use of the service.

Can I access data files associated with the Pega Cloud SFTP service in one environment (for example, prod1) from another environment (for example, prod2)?

No. Pega Cloud provisions environments to completely isolate data file storage by environment; therefore, files managed by the SFTP service in one environment are not accessible by other environments, including environments of the same type (for example, dev1, dev2).

Can I use files from my production environment's SFTP service in my Dev/Test or Staging environments?

No. You cannot access files directly from a different Pega Cloud environment in your subscription. However, you can use an SFTP client to manually download files from one environment and then use it to upload the same files to a different environment's SFTP server.

Does the Pega Cloud SFTP service support multiple users?

Yes. Pega Cloud provides one admin-level user and, if requested, up to 10 additional non-admin level users for each environment. The SFTP service allows each user with their own client-provided individual public keys to connect to a unique file directory for that environment. You may have up to a total of 20 additional non-admin-level users for all environments after upgrading to the newer SFTP service version (which requires a Pega Cloud major infrastructure update). Each user can access, add, or delete files in the /sftp sub-folder in their unique file directory. For information about how Pega Platform maps to repository records in Pega Cloud File storage, see [Using Pega Cloud File Storage](#).

Does the Pega Cloud SFTP service support different SFTP clients?

Yes. You can use your preferred SFTP client to upload or download files in your user's unique file directory.

Can I create additional sub-folders in the Pega Cloud SFTP service folder path?

Yes. Pega Cloud supports three methods to create sub-folders in your SFTP service folder path:



Restriction: Pega Cloud limits the ability of users to create additional sub-folders to your current environment; new sub-folders cannot transfer to other Pega Cloud environments in your Pega Cloud subscription.

- You can create additional sub-folders by using your preferred SFTP client. When you use your preferred SFTP client to create additional sub-folders in your user folder, the functionality depends upon the capabilities of your SFTP client and are limited to the unique file directory of each user.
- You can create additional sub-folders with Pega Platform by using with the following methods:
 - Create the new sub-folder by using the Pega-provided datapage *D_pxNewFolder*.
 1. In the navigation pane of Dev Studio, go to Records > Data Model > Data Page.
 2. In the Data Page instance list, filter the Page Name column for *D_pxNewFolder* and then select it.
 3. In the Actions list, select Run.
 4. In the Run Data Page: New Folder dialog window, specify your new sub-folder by entering the following information:
 - a. In the repositoryName field, enter *pegacloudrepository*.
 - b. In the folderPath field, enter your non-admin user folder path appended with your new sub-folder name. For example, to create the new sub-folder *new_folder*, enter *sftp/user1/new_folder*.
 5. In the **Run Data Page: New Folder** dialog box, select Run.

For more information about Pega repository APIs, see [Using repository APIs in your application](#).

- To accommodate a BIX extraction you can create a file folder within the /bix directory and then specify it as the target for your extract files. For more information, see [Creating and running an Extract rule](#).

Is my data secure when using the Pega Cloud SFTP service?

Yes. All Pega Cloud SFTP data transfers (data-in-transit) are encrypted by using SSH and data-at-rest is encrypted based on an environment-specific key.

Note: Ensure that your developers are informed of and adhere to your organization's internal security practices pertaining to protecting or masking sensitive data used within your Pega application. To secure your data, review and implement the best security practices as outlined in [Security Checklist when deploying on Pega Cloud](#).

What is the availability guarantee for the Pega Cloud SFTP service?

The Pega Cloud SFTP service is a highly-available robust service that is resilient to failures and monitored for stability by the 24/7 operations team. All files and folders are preserved across failures.

I accidentally deleted a file from the Pega Cloud SFTP service. Can it be restored?

You can recover files you delete from any folder in the pegacloudrepository record within 30 days of deletion.

For more information about recovering deleted files from your SFTP folder in Pega Cloud File storage, see the section, "Recovering deleted Pega Cloud File storage files" in the article [Using Pega Cloud File storage](#).

Can I customize the folder names provided by the Pega Cloud SFTP service?

Currently, there is no support to rename existing folders.

Can I have a custom domain configured for the Pega Cloud SFTP service?

No.

Environment restarts

Restart the tiers or only a specific tier by using the My Pega Cloud self-service portal. With this feature, you and your customers can continue to use environments with minimal disruption during a time that you control.

Considerations for any Pega Cloud restarts

Restarts occur gracefully, without data loss, while maintaining high availability of the environment. During environment restarts, users and customers, can continue to access and use their applications in the Pega Cloud®environments with minimal disruption.

Background processing differences in different versions of Pega Platform

Depending on the version of Pega Platform™ that runs in your Pega Cloud environment, the management of background processing changes.



Note: Clients can continue using their system through a restart without data loss.

The following table describes the differences in background processes across Pega Platform versions:

Item	Description
Pega Platform 8.3 and later	Tiers restart without impact to Pega Platform. The restart process includes automated stopping and restarting of background processing. Clients must ensure that

Item	Description
	background processes finish within seconds, not minutes, to avoid updates interrupting background processes and impacting zero downtime. Review and adhere to the best practices in Client responsibilities for Pega Platform 8.3.x and later .
Pega Platform 8.2 and earlier	Tier restarts might require client involvement as listed in the recommended best practices for using background processing as described in Client responsibilities for Pega Platform 8.2.x and earlier .

Impact on Search availability

Depending on the version of Pega Platform that runs in your Pega Cloud environment, you see the following types of impact to search functionality as a result of restarting the background processing tiers or all of the tiers in your environment:

Item	Description
Pega Platform 8.1.4 and later	Search is highly available throughout a restart and does not require reindexing.
Pega Platform 8.1 through 8.1.3	Search is not available until automated Search re-indexing completes. The system applies cumulative patch releases for the latest Pega Platform 8.x software to the environment. For more information, see Pega Cloud Services maintenance and types of system updates .
Pega Platform 7.4 and earlier	Search is not available during a restart and requires you to reindex the search.

Restarts for a Pega Cloud environment

When the option to restart your environment is available, depending on the type of environment, you can use the self-service function to restart immediately or you can schedule an environment restart.

- To immediately restart an environment, see [Restarting your Pega Cloud environment immediately](#).
- To schedule an environment restart, see [Scheduling a Pega Cloud environment restart](#).
- To edit or withdraw a scheduled environment restart, see [Editing or withdrawing a scheduled Pega Cloud environment restart](#).

Note: When you use the restart self-service, you do not impact your background processing tiers or the availability of Search. If a restart fails, the system automatically generates a new support request for the support team to complete the restart. For information about this failure-related support request, see [My Support Portal](#).

Environment availability during a restart

Pega Cloud restarts occur gracefully, without data loss, and maintain the high availability of the environment. To avoid unnecessary disruption and potential conflicts, plan your restart for a time period when use of the application is low. Review the following information to know when you should avoid an immediate environment restart and instead schedule a restart, so that you and your customers can continue to access and use your applications with minimal disruption:

- The average time for the nodes in your tier to restart is about 30 minutes, while the maximum time is about 60 minutes. This duration might cause disruption.
- Maintenance activities might temporarily disable your ability to restart the Web tier in an environment. For more information, see [Pega Cloud maintenance and types of system updates](#).

You cannot restart an environment when:

- Environments have a `hibernating`, `hibernated`, or `waking-up` status.
- Environments have thirty minutes before a scheduled maintenance activity begins; you must wait until it completes.

- Environments are actively undergoing maintenance activities.

Restart task responsibilities

For a successful restart of any Pega Cloud environment, certain tasks must be performed. During the Pega Cloud restart process, Pega is responsible for completing some tasks and you, the client, are responsible for completing other tasks. Use the information in the following to help you to understand who is responsible for which restart action and why the actions are necessary:

Item	Description
Pega responsibilities	<p>To ensure that a restart occurs with near-zero downtime impact to client environments, Pega responsibilities include the following actions:</p> <ul style="list-style-type: none"> Manage communications with the client throughout the restart process, including notification if a restart fails. Document any issue that was discovered during the restart and, if necessary, work with the client to resolve any restart issues.
Client responsibilities for Pega Platform 8.3.x and later	<p>To ensure that a restart occurs with near-zero downtime impact to the environment, perform the following actions:</p> <ul style="list-style-type: none"> For Pega Customer Decision Hub™ clients, reschedule any upcoming activities, such as campaigns or job schedulers, to run after the restart is complete. Any user-initiated activities that run during restart might not complete; jobs that run during the restart are not lost, but might require you to re-run them after the restart is complete. These activities include campaigns during the moment they are calculating volume constraints. All background processes in the application follow two guidelines:

Item	Description
	<ul style="list-style-type: none"> ◦ Best practices for writing activities for background jobs ◦ Best practices for processing files using the file listener
Client responsibilities for Pega Platform 8.2.x and earlier	<p>To ensure that a restart occurs with near-zero downtime impact to the environment, perform the following actions:</p> <ul style="list-style-type: none"> • Reschedule any upcoming activities, such as campaigns or job schedulers, to run after the restart is complete. • Avoid possible disruption to background processes by stopping all background processes before a restart begins, and then restarting Pega queue processors, job schedulers, and DSM dataflows after you receive notification that the restart is complete. A restart automatically restarts Pega agents and listeners after it is complete. For specific guidance to complete the pausing and subsequent resuming of background processes, see Patch Process for Pega Infinity 8.2 versions.

- [Restarting your Pega Cloud environment immediately](#)
- [Scheduling a Pega Cloud environment restart](#)
- [Editing or withdrawing a scheduled Pega Cloud environment restart](#)

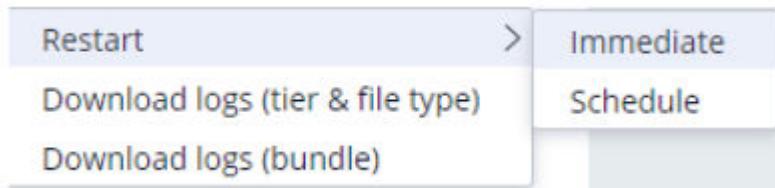
Restarting your Pega Cloud environment immediately

Immediately restart your Pega Cloud® environment when it is most convenient for your organization and your users without any internal or external dependencies.

All environment restarts require an appropriate role with access privileges to the My Pega Cloud portal. If you do not have portal access, contact your Account Administrator. For more information, see [Defining your support contact roles](#).

Note: Review and understand the considerations described in [Considerations for any Pega Cloud restarts](#). Environment availability during a restart depends on environment status, Pega Platform™ version, and other details. For more information, see [Background processing differences in different versions of Pega Platform](#).

1. Log in to your My Pega Cloud account.
2. In the **My cloud setup** tile, click **View details**.
3. In the **Environments** section, in the row for the environment that contains the tiers that you want to restart, click **More > Restart > Immediate**, as shown in the following figure:



Restart dialog window

4. In the **Immediate restart** dialog box, in the **Reason for restart** category list, select the category that best describes the reason why you want to restart your environment.
Pega uses this information to guide future improvements to this functionality.
5. Select the tier you want to restart:
 - To restart all tiers on the selected virtual space, select **All tiers**.
 - To specify the tiers you want to restart, select **Specific tier(s)**.

6. In the Reason for restart field, enter the details about why you want to restart your environment.
Pega uses this information to guide future improvements to this functionality.
7. Click Submit.

Important: If a restart fails, the system automatically generates a new request with your environment details. Do not attempt a second restart; instead, work with your support team to complete the restart.

The following figure shows an example of an immediate restart:

Immediate restart X

Pega Platform 8.3 and later supports zero-downtime restarts. Depending on the Pega Platform version, management of background processing or search functionality may be impacted. For more information, see [Restarts in Pega Cloud environments](#)

Reason for restart category *

-- Select --

Select tier *

All tiers Specific tier(s)

Pega uses the following information to improve our internal processes.

Reason for restart *

Cancel Submit

Add required details using the Immediate restart fields

What to do next:

In the top navigation panel, click the Notification icon to view the status of the restart process. After a successful restart, you receive a notification with details about the restart.

Scheduling a Pega Cloud environment restart

Schedule a restart of your Pega Cloud® environment when it is most convenient for your organization and your users without any internal or external dependencies.

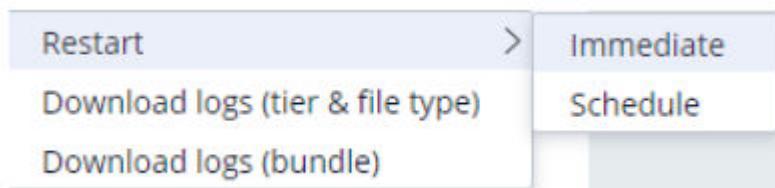
All environment restarts require an appropriate role with access privileges to the My Pega Cloud portal. If you do not have portal access, contact your Account Administrator. For more information, see [Defining your support contact roles](#).

Scheduling a restart supports only one environment restart at a time. Set a time zone in your User Profile before you can use the schedule or edit a scheduled restart. To update your profile, see [Configuring your portal preferences](#).

Use this procedure to schedule an environment restart by specifying a time within three hours from now up to the next seven days. Scheduling a restart supports only one environment restart at a time. If you need to edit or withdraw a scheduled restart, see [Editing or withdrawing a scheduled Pega Cloud environment restart](#).

Note: Review and understand the considerations described in [Considerations for any Pega Cloud restarts](#). Environment availability when the restart process begins depends on environment status, Pega Platform™ version, and other details. For more information, see [Background processing differences in different versions of Pega Platform](#).

1. Log in to your My Pega Cloud account.
2. In the **My cloud setup** tile, click **View details**.
3. In the **Environments** section, in the row for the environment that contains the tiers that you want to restart, click **More > Restart > Schedule**, as shown in the following figure:



Restart dialog window

4. In the **Schedule restart** dialog box, in the **Scheduled for** field, specify the time and date for this environment restart.
5. In the **Reason for restart** category list, select the category that best describes the reason why you want to schedule an environment restart.
Pega uses this information to guide future improvements to this functionality.
6. Select the tier that you want to restart:
 - To restart all tiers on the selected virtual space, select **All tiers**.
 - To specify the tiers you want to restart, select **Specific tier(s)**.
7. In the **Reason for restart** field, enter the details about why you want to schedule an environment restart.
Pega uses this information to guide future improvements to this functionality.
8. Click **Submit**.

Important: If a restart fails, the system automatically generates a new request with your environment details. Do not attempt a second restart; instead, work with your support team to complete the restart.

The following figure shows an example of a scheduled restart:

Schedule restart X

Pega Platform 8.3 and later supports zero-downtime restarts. Depending on the Pega Platform version, management of background processing or search functionality may be impacted.
For more information, see [Restarts in Pega Cloud environments](#)

Scheduled for *

Reason for restart category *

-- Select --

Select tier *

All tiers Specific tier(s)

Pega uses the following information to improve our internal processes.

Reason for restart *

[Cancel](#) [Submit](#)

Add required details using the Schedule restart fields

What to do next:

In the top navigation panel, click the Notification icon to view the status of the restart process. After you schedule a restart, you receive a notification with details about the restart that you just scheduled.

Editing or withdrawing a scheduled Pega Cloud environment restart

Edit or withdraw a scheduled Pega Cloud® environment restart. Update a scheduled restart when it is most convenient for your organization and your users without any internal or external dependencies. Withdraw a scheduled restart if the restart is no longer needed or if you no longer want the restart to occur at the scheduled time.

All environment restarts require an appropriate role with access privileges to the My Pega Cloud portal. If you do not have portal access, contact your Account Administrator. For more information, see [Defining your support contact roles](#).

Scheduling a restart supports only one environment restart at a time. Set a time zone in your User Profile before you can use the schedule or edit a scheduled restart. To update your profile, see [Configuring your portal preferences](#).

Use this procedure to edit a scheduled restart by updating the time and date to begin an environment restart or to withdraw a specified scheduled restart. Do not use this procedure to schedule a restart; instead, see [Scheduling a Pega Cloud environment restart](#).

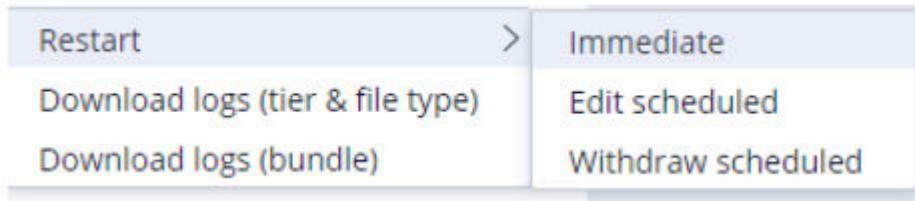
Note: Review and understand the considerations described in [Considerations for any Pega Cloud restarts](#). Environment availability when the restart process

- ① begins depends on environment status, Pega Platform™ version, and other details. For more information, see [Background processing differences in different versions of Pega Platform](#).

Editing or withdrawing a scheduled restart

1. Log in to your My Pega Cloud account.
2. In the **My cloud setup** tile, click **View details**.
3. In the **Environments** section, in the row for the environment that you want to reschedule, click the **More > Restart > Edit scheduled**, as shown in the following figure:

If you already have a restart scheduled, the **Edit scheduled** and **Withdraw restart** options are displayed.



Restart dialog window with Withdraw option if you already scheduled a restart

4. In the **Edit restart** dialog box, in the **Scheduled for** field, specify the new date and time for this environment restart.
5. In the **Reason for restart** category list, select the category that best describes the reason why you want to schedule an environment restart.
Pega uses this information to guide future improvements to this functionality.
6. Select the tier you want to restart.
 - To restart all tiers on the selected virtual space, select **All tiers**.
 - To specify the tiers you want to restart, select **Specific tier(s)**.
7. In the **Reason for restart** field, enter the details about why you want to schedule an environment restart.
Pega uses this information to guide future improvements to this functionality.

Important: If a restart fails, the system automatically generates a new request with your environment details. Do not attempt a second restart; instead, work with your support team to complete the restart.

The following figure shows an example of an edit to a restart:

Edit restart

<Operator> scheduled this environment to be restarted on Mar 24, 2023 11:13:00 AM

Pega Platform 8.3 and later supports zero-downtime restarts. Depending on the Pega Platform version, management of background processing or search functionality may be impacted. For more information, see [Restarts in Pega Cloud environments](#)

Scheduled for *

3/24/2023 11:13 AM



Reason for restart category *

Others



Select tier *



All tiers



Specific tier(s)

Tiers

Pega uses the following information to improve our internal processes.

Reason for restart *

test

[Cancel](#)

[Submit](#)

Edit the details for a scheduled restart

Withdrawing a scheduled restart

8. In the **Environments** section, in the row for the environment for which you want to withdraw a scheduled restart, click the More > Restart > Withdraw scheduled.

9. In the Withdraw restart window, in the Withdraw reason field, enter the details about why you want to withdraw this environment restart.
10. Click Submit.

The following figure shows an example of a withdrawn restart:

The screenshot shows a user interface titled "Withdraw restart". At the top, there is a green header bar with the text "<Operator> scheduled this environment to be restarted on Mar 24, 2023 11:13:00 AM". Below this is a form field labeled "Withdraw reason *". A large empty text area is provided for entering the reason. At the bottom right of the form is a blue "Submit" button. Below the form, a note says "Provide details about withdrawing a scheduled restart".

What to do next:

In the top navigation panel, click the Notification icon to view the status of the restart process. After you update a restart schedule or withdraw it, you receive a notification with appropriate details about the change you just made.

Managing hibernated environments

You can use Pega Cloud® to take action to reduce the energy consumption and carbon footprint of its client environment portfolio by implementing an auto-hibernation process. Pega pauses the cloud resources for your non-production environments,

which includes AgileStudio, DevOps, clone and mirror environments, during periods of no-activity use.

You can unpause a hibernated environment by using self-service controls in [My Pega Cloud portal](#). For more information about the auto-hibernation and wake-up process for your Pega Cloud environment, see the [Auto-hibernation FAQs](#).

Note: Pega Cloud performs auto-hibernation on qualifying environments roughly at the end of the business week. Automatic wakeup at the start of the business week takes place only if the environment was actively used in the previous week. If the environment was idle, it remains hibernated also during business weekdays. You can perform a self-service wake up on a hibernated environment as required for access at any time.

For more information, see the FAQ question *What qualifies my non-Production environment for auto-hibernation and auto-wake up?*

Auto-hibernated environments can be unpause following a wake-up process. When a client navigates to the URL of an auto-hibernated Pega Cloud environment, they can click on a My Pega Cloud link to go to their cloud setup, from where they can wake up their environment. Environments are typically ready within 25 minutes.

Benefits of auto-hibernation

By implementing and tracking auto-hibernation in client environments, Pega can:

- Reduce its overall carbon footprint
- Improve understanding about the usage of a client environment
- Improve the startup and shutdown performance and success

Customizing your auto-hibernation schedule

Clients can request to have their non-production environments automatically hibernate and wake-up. This support includes creating supporting an auto-hibernation cycle schedule that matches your teams' schedule. For example, you can schedule your hibernation cycle to start on 9:00 P.M. PST on Friday, and your wake-up cycle to start on 9:00 A.M. IST on Monday.

To customize your auto-hibernation cycle schedule, request a cloud-change by [creating a ticket](#) in [My Support Portal](#). In your request, include the following items:

- Environment name
- Day of the week, time, and time zone for hibernation start
- Day of the week, time, and time zone for wake-up start

Pega requires you to complete a separate cloud-change request for each environment for which you want to schedule an auto-hibernation cycle. For more information on the default hibernation and wake-up schedule, see the FAQ question "What qualifies my non-Production environment for auto-hibernation and auto-wake up?"

Waking up your hibernated Pega Cloud environment

After a period of no-activity usage, your environment will begin a hibernating phase before entering a hibernated state that pauses usage of system resources. Once hibernated, you wake up your environments through the following method:

1. Go to the URL of your Pega application that is hosted in your Pega Cloud environment.

The system replaces the display of your Pega Platform instance with a *hibernated environment* banner similar to that in the following image:



This environment is hibernated.

As part of Pegasystems' commitment to protect the environment and encourage social responsibility, Pega Cloud has temporarily hibernated your environment after an extended period with no activity to minimize global environmental impact.

Log in to [self-service portal](#) to wake it up.

Learn more about our environmental governance [policies](#) and [FAQs](#)



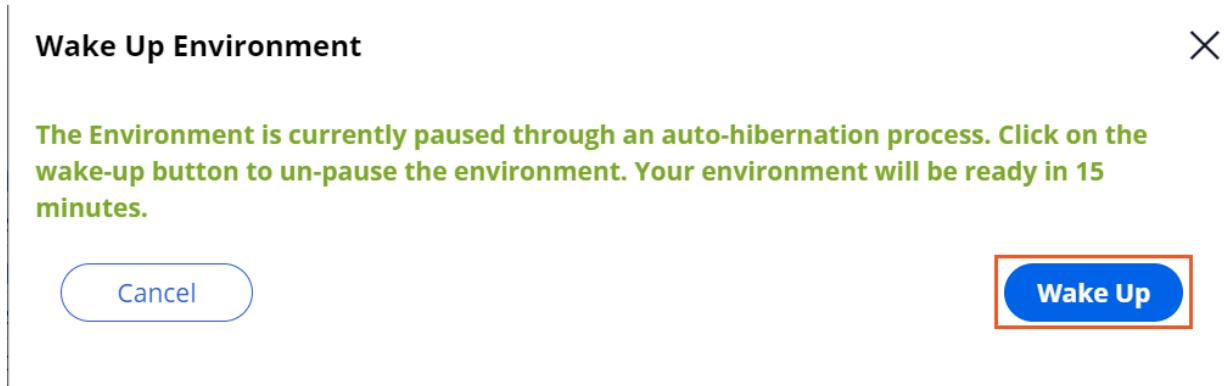
Hibernated environment

2. Click self-service portal to go to My Pega Cloud.
3. On the Home tab of My Pega Cloud, on the **My cloud setup** tile, click View details.
4. In the Environments section, in the row containing your hibernated environment, click the More icon.

Environments						
Name	Environment Type	Pega	Type	Production level	Status	
	Production	8.5.3	Production	5	RUNNING C	:
	Staging	8.5.3	LargeSand...	4	RUNNING C	:
	Staging	8.5.3	Production	4	RUNNING C	:
	Staging	8.5.1	Clone	4	HIBERNATED C	:
	DevTest	8.5.3	StandardS...	2	RUNNING C	:
	DevTest	8.5.3	StandardS...	2	RUNNING C	:
	DevTest	8.5.3	StandardS...	2	RUNNING C	:

The Environments tab

5. Select Wake up.
6. In the resulting **Wake Up Environment** dialog box, click Wake Up.

*Wake Up button for hibernating environment*

Your environment enters the **Waking Up** status, and will enter a **Running** state in approximately 25 minutes.

CLONE :	Staging	8.5.1	Clone	4	WAKING UP C	:
---	---------	-------	-------	---	-------------	-------------------------------------

Environment status changed to Waking Up

Auto-hibernation FAQs

Consider these Frequently Asked Questions (FAQ) to become familiar with common inquiries about the Pega Cloud® auto-hibernation process.

What qualifies my non-production environment for auto-hibernation and auto-wake up?

Pega Cloud automatically hibernates non-production environments, which includes AgileStudio, DevOps, clone and mirror environments, that meet the following criteria:

1. On a Friday, the time is roughly after when environments typically stop usage for the business week.
2. Within this time frame, Pega Cloud detects two consecutive hours of no activity on the environment.

After meeting these criteria, Pega Cloud initiates auto-hibernation on the environment.

On the following Monday, Pega Cloud initiates auto-wake up on the environment, beginning roughly at the time environments typically start usage for the business week.

Note: Automatic wakeup at the start of the business week takes place only if
① the environment was actively used in the previous week. If the environment was idle, it remains hibernated also during business weekdays.

Are Production environments affected by the auto-hibernation process?

No, production environments cannot be auto-hibernated. The system only performs auto-hibernation on qualifying non-production environments.

What are the different statuses of running and hibernated environments in My Pega Cloud?

My Support Portal uses the following statuses on the My cloud setup tab:

Running- The environment is running and available for use.

Hibernating- Pega Cloud has detected a period of no activity in your environment, and the auto-hibernation phase has begun but is not complete. You cannot wake up an environment while it is in Hibernating status.

Hibernated- The environment has paused resource consumption and must be woken up before it can run again.

Waking up - The environment has been woken up from its hibernated state, and will resume running and consuming cloud resources in roughly 25 minutes.

How long does it take to wake up my environment?

Typically, within 25 minutes.

Can I restart a hibernating or hibernated environment?

No, the option to restart a hibernating-status or hibernated-status environment is not available in My Pega Cloud. Once the environment has been woken up, the environment will be available for restart.

What if I can't wake up my environment?

There may be circumstances where this process takes longer than expected. In such circumstances, the process automatically creates a client-facing INC ticket on your behalf. To see the status of any issues, see the **Support requests** section in **My Pega Cloud**. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

What happens to data in my environment during auto-hibernation?

All of the data in the environment is safe. Data is persisted and fully encrypted prior to suspending cloud resources.

Who can wake up an environment?

Clients must have access to view and use the My Pega Cloud portal. For most clients, this means that they must be connected through their company network prior to accessing their Pega Cloud environment.

For more information about how to gain access to My Pega Cloud, see [Configuring your portal preferences](#).

How does Pega perform maintenance on hibernated environments?

Pega Cloud automatically wakes up hibernated environments prior to performing maintenance.

For more information about scheduled maintenance activities, see [Pega Cloud maintenance and types of system updates](#).

Can I proactively auto-hibernate My Pega Cloud environments?

To learn more about auto-hibernation or proactive auto-hibernation, you can contact Pega and request more information by selecting [Create a ticket](#) in [My Support Portal](#).

Can I use Deployment Manager while my environment is auto-hibernated?

No, you cannot use Deployment Manager while your environment is auto-hibernated.

Change Management process

Pega Cloud® provides comprehensive change management for our Pega Cloud clients. Pega efficiently and securely plans, reviews, tests, implements, and validates your requested changes.

Responsibilities

Pega manages the changes on Pega Cloud, which includes the underlying cloud infrastructure and patches to Pega-licensed products. You are responsible for the top-layer and application layer and must conform to the established Pega Platform best practice and Guardrail Compliance instructions.

For more information, see [Improving your compliance score](#).

For more information about client responsibilities pertaining to client requests to change access levels or data, see the *Access and data changes* section below.

Requesting changes

To request a Pega Cloud environment change, [create a ticket in My Support Portal](#). In this change request (i.e. Cloud Change - CC), provide the following items:

- All relevant change plan information, including:
 - Complete description of the change
 - Change plan with at least one task for the Pega Cloud team
- Major and Significant production change requests (CC) require approval from your organization's Security Contact.
- Supporting documentation
- Proposed start and end dates, times, and time zones for the change

Restriction:

All Major and Significant production change requests (CC) (as detailed in the [task table](#)) require Security Contact approval. For such cases we need the Security Contact to approve the CC support case in [My Support Portal](#). For guidance to complete the approval process, see the [Cloud Change approval process](#).

! Pega cannot make a change unless the change is explicitly mentioned in the request.

Client requests to migrate your customer data or other client-confidential information into a non-Production environment are not supported and such requests will be denied.

When submitting your Cloud Change request, you should provide a minimum two hour's notice for Pega Cloud to complete the change. If you require less time for a high priority change, the team will complete your request using a Severity 1 ticket; downtime is required. For such high-priority changes, use the [Pega Support Contact Information](#) link to request assistance from a representative.

After you submit the request, you can view the status and progress of the requested change within [My Support Portal](#) until you confirm with Pega Global Client Support that your requested change works satisfactorily. Pega Cloud coordinates and schedules all approved change requests with you to verify that the change has minimal impact to your Pega Cloud environment.

You should only submit change requests for activities that you cannot otherwise perform through the Dev Studio. For example, you can create and import RAP files that contain rules, classes, and data without Pega assistance. For Pega software upgrades and other changes required for the proper operation of cloud environments submit a request to [My Support Portal](#).

If you have change requests for multiple environments, please submit a separate request for each environment.

Change categories

The individual tasks in a change request are divided into the following three categories:

- Standard: Low-risk changes that are specific, concrete, and pose little information security or compliance risk.
- Significant: Higher-risk, critical changes that require technical review.
- Major: Changes with the highest criticality that need to be reviewed by the Pega Cloud Change Advisory board (CAB).

For more information about client responsibilities pertaining to client requests to change access levels or data, see the *Access and data changes* section below.

Change request tasks can be classified as singular or non-singular. For singular tasks, you cannot add additional tasks to your change request.

Production changes

To make sure that changes to production environments conform to security, compliance, and quality controls, change requests that include one or more Major or Significant-category change tasks to production environments must undergo technical review and be approved by the Pega Cloud Change Advisory Board (CAB) for security and business-risk purposes. Change requests for Standard change tasks do not require technical approval or CAB review. All Change Requests will be reviewed as per the task categorization as available in the [task table](#).

For Major and Significant change requests in production environments, Pega recommends that you test the change in a non-production environment (development or staging) before submitting the change request for the production environment. When submitting the production change request, provide the change request case ID from the test in the non-production environment. This best practice helps prevent untested and potentially harmful changes from being rolled out to production.

The CAB includes Security, Compliance, and Operations representatives; it meets three times weekly on Monday, Wednesday, and Friday mornings on Eastern Time. The CAB reviews all Major and Significant production changes (which qualify for CAB as detailed in the [task table](#)) from baseline, both before and after "Go live," so that Pega does not introduce security issues, performance problems, unapproved configurations, compliance deviations, or non-standard features. Pega Cloud cannot make a change that alters security control or violates industry and government compliance regulations.

All production environments change request that include one or more Major or Significant-category change tasks, with the exception of Emergency change requests (see section below), require the following items:

- A description of the change

- A completed Change Plan that details the required tasks
- A reference request for the change in the lower (non-production) environment
- Test results for full testing of the change in the lower (non-production) environment
- Requested start and end dates, times, and time zone for the requested change



Note: For production environments, the requested change can only be made during your specified maintenance window.

When you request a change, provide the above information in your request. If Pega is making the change for maintenance reasons, Pega Cloud will create the request and include the above information.

Pega Cloud Change Advisory Board might deny a requested change due to security, operations compliance, or other business reasons including, but not limited to, restrictions outlined by the Pega Cloud Subscription documentation. Pega Cloud will include the reason for denial in the request, as well as alternative options (when available) and additional instructions or questions.

You can appeal denied change requests by resubmitting the request with additional justification or by confirming you took rectifying steps as recommended.

Withdrawing or rolling back change requests

You can withdraw a change request up to 30 minutes before its scheduled start time. To withdraw a change request, use the [Pega Support contact Information](#) link or update a Pulse note in [My Support Portal](#) before the implementation starts. If the change request implementation has already started, you can request to roll back the change. After Pega Global Client Support implements your change request, it remains open for 96 hours so that you can validate it if needed.

Access and data changes

To protect the security of Pega Cloud client information in production environments, Pega requires written authorization from your Client Security Contact for access level changes and data changes. This written authorization must provide all the details necessary to implement the change. Make the authorization specific to one request only and provide it to Pega Cloud through email, document, or letter. Pega Cloud attaches the authorization to the Change Requested as an audited record of the request. For more information, see the [Cloud Change approval process](#). Additionally, Pega might require a signed liability release form for requests to directly access a production database.

- Access changes: Access level changes include requests to modify the authentication or authorization facilities of the environment, and other changes to access security files, such as certificates, ciphers, and network configuration files.
- Data changes: Data changes include requests to modify (update, delete, drop, truncate) production data and requests to copy, extract, or transmit production data in any way that could compromise data security.



Note: You cannot request to move your customer data or other client-confidential information to a non-Production environment.

Non-production changes

The Pega Cloud Change Advisory Board may not review change requests for non-production environments (as applicable), such as development, test, staging, user acceptance testing, because they do not require compliance or security impact analysis. However, they require a full change plan and a description of the proposed change.

Scheduling change requests

When you create a change request, you specify a **Start date and time**, which determines the urgency of your request. Based on the duration between the time of

submission and the scheduled start date and time, your request is classified with an urgency of either Normal or Emergency. The following table defines the criteria under which a change request is considered an emergency.

Standard change request for any environment	Standard changes are not classified as Emergency. However, the suggested planned schedule is > 48 hours from the time of submission.
Major or Significant change request for a non-production environment	If the Planned schedule is >72 hours from the time of submission, the urgency is classified as Normal; if not, it is classified as Emergency.
Major or Significant change request for a production environment	If the planned schedule is > 12 hours in the future or two hours after the CAB starts, whichever is greater, and the change request is submitted at least 4 hours before the next CAB meeting, the urgency is classified as Normal; if not, it is classified as Emergency.

Emergency changes

For a service outage or other critical change to a production environment that includes one or more Major or Significant-category change tasks and requires a response that cannot wait for the CAB, lower environment (non-production environment) testing is not required.

Emergency changes contain associated risks due to the reduced time and scope of the compliance and security review that can be performed.

The CAB must authorize requests for an emergency change upon confirmation of a justifiable emergency. For authorization, an emergency change must include the following information:

- Required change plan details
- Declaration that the request is an emergency
- Justification for the emergency change

- Name and title of the client contact requesting the emergency change
- Requested start date and time to implement the emergency change
- **Client-configured Pega Cloud changes**
- **Cloud Change approval process**

Client-configured Pega Cloud changes

Pega requires that you use Pega Platform™ for customizations in your Pega Cloud® environments. This ensures that you can keep your application current with the latest Pega Platform and Pega Cloud features.

Pega Cloud does not support customizing Pega Cloud environments outside the use of Pega Platform, because these types of customizations can impact your application performance, reliability, and compatibility with future releases.

Pega Platform offers robust features for customizing your Pega Cloud deployment. Review the following examples for supported methods to expand Pega Platform abilities to meet your specific needs. If your deployment needs a customization that standard Pega software does not support, you can request Pega to include the features in future Pega software releases, Select [Create a ticket in My Support Portal](#), or call the [Pega Support Contact Information](#) listed for your region. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

Resources for usage in JMS models

You can request the Pega Cloud operations team to add Java Messaging Service (JMS) resources that you need to support your JMS model by using the [Support Requests](#) tab in [My Pega Cloud portal](#). To complete your request for JMS resources, restart your Pega Cloud environment. For details, see [Environment restarts](#).

For more information about configuring JMS resources in your instance of Pega Platform, see [Messaging service overview](#).

Custom Login Screen

You can edit your application login screen to display a new logo or background image for your application, to maintain design consistency according to your enterprise style guide, or to change the single sign-on button appearance.

To create a Custom Login Screen, follow the steps provided in [Login screen customization](#).

Role-based Access Control

You can configure Pega Platform to access external systems to retrieve data and perform application processing. Similarly, you can allow external systems to access services in Pega Platform.

To configure role-based access control, follow the steps provided in [Role-based access control](#).

Setting Log Levels

With Pega Platform, you can set log levels for categories and for individual loggers. For more information on how to configure this, see [Understanding logs and logging messages](#).

Managing X.509 Certificates

Beginning with Pega Platform 8.4, you can import X.509 certificates directly into the Pega Platform truststore to authenticate external server hosts.

For details on how to configure this, see [Managing X.509 certificates](#).

Custom Fonts

Pega Platform supports importing web fonts for use in your Pega application. For details on how to configure this, see [Uploading custom font files](#).

Custom Java archives and classes

You can incorporate third-party Java functionality into Pega Platform by importing a Java archive (JAR) file or class.

Note: The client assumes all responsibility for files imported into Pega Cloud.

- ⓘ Pegasystems Inc. is not responsible for clients importing files that may contain malicious code. The client can refer to the to understand the client responsibilities model.

For support details and step-by-step instructions, see [Importing custom Java archives and classes](#).

Custom XML files for input streams

You can use custom XML files for use as an input stream by importing the XML files as a Java archive (JAR) and extracting the files using an activity.

Note: The client assumes all responsibility for files imported into Pega Cloud.

- ⓘ Pegasystems Inc. is not responsible for clients importing files that may contain malicious code. The client can refer to the to understand the client responsibilities model.

For support details and step-by-step instructions, see [Importing custom XML files for input streams](#).

Cloud Change approval process

The security contact approval process for all Major or Significant changes has now been embedded within Pega Support itself. Change request cases are requested by Cloud Specialist. If as a Cloud specialist, you also have the Security Contact role, then the Security Contact Approval process is not triggered, as approval is deemed to be

received. However, if you are not a Security Contact, we need to obtain an approval from any one of the identified Security contact(s) on your account before submitting your request to the support team.

Selecting a Security contact

Whilst creating a Major or Significant CC case you will be asked to obtain approval in the **Security approval** section of the **Communication Preferences** step.

There are 2 ways to provide approval i.e.

- The default: by requesting one or more security contacts to provide their approval (Select a security contact and Pega will send that Security contact an email requesting them to access MSP to provide the relevant approval.)
- Alternatively, by attaching an approval email from the security contact, to the CC, as you create it.

Security Approval

During the CC case creation process, on the Communication preferences screen, you will be presented with the **Security approval** section in the following circumstances:

- You are creating a Major or Significant Cloud change request.
- And you are not a Security contact.
- Or it is not a case which is auto created by Pega.

The following message is displayed:

"In order to process this significant production cloud change request, a security contact must provide approval."

Do you have an approval email from a security contact?"

By default, option No is selected.

Security approval

In order to process this significant production cloud change request, a security contact must provide approval.

Do you have an approval email from a security contact? *



Yes



No

Select security contact to request approval

Name



Email



Phone



No items

Add security contact

With No selected, you must click the Add security contact link to select a security contact from the Select security contact to request approval table. i.e., Select the relevant Security contact from the picklist, who can provide the approval. For example, a security contact associated with the environment concerned.



Note: Multiple Security contacts can be selected, as required.

If Yes is selected, you will be presented with a dropdown list with the names of the security contacts affiliated to the account. Pick the name of the security contact who provided the email approval. Then use the Upload button to upload the email approval to the case.

Security approval

In order to process this significant production cloud change request, a security contact must provide approval.

Do you have an approval email from a security contact? *

Yes

No

Approval email received from *

Select..



Security approval

File name	Category
No attachments	

On submit, system skips approval process and move to Pending-Triage.

No Security Contacts

If there are no security contacts available on the account, the requestor will be presented with the following message:

"There is no Security contact available for this account, please reach out to account administrator to have this role filled in order to approve change"

Once a Security contact is selected

- The CC support case will change to New-PendingSecurityApproval status.
- An approval email will be sent to the selected Security Contact containing a link to the case in MSP. e.g.

'This cloud change requires Security contact approval. You have been nominated to approve this case. Please access <link to case, show case ID> via My Support Portal to review.'

- A pulse post is also added to the cases with the following text:

'Cloud Change (Case ID: Title) : This change is waiting on approval from the following, authorized security contacts:

<Name>

<Name>'

(A list of the selected security contacts is provided)

- An email notification is sent to all parties on the case:

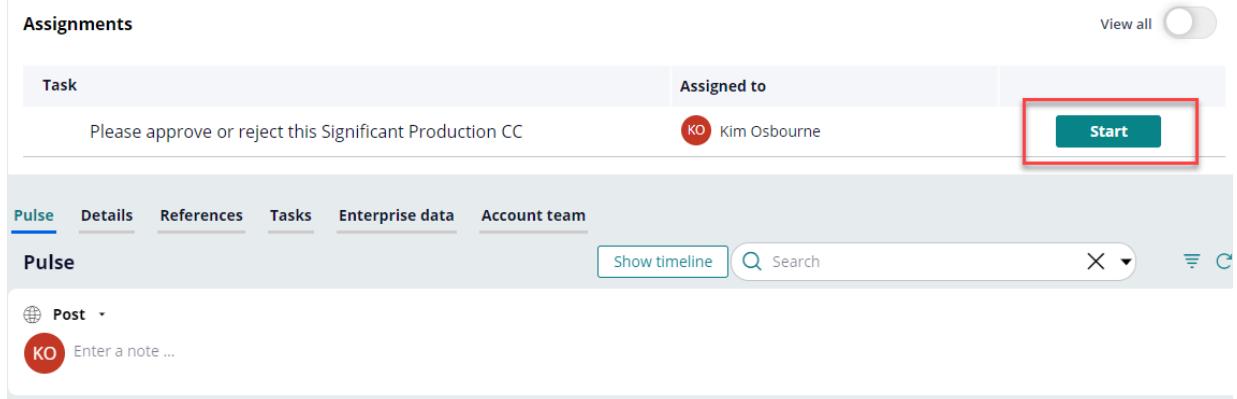
'Cloud Change <Case ID>: This change is waiting on approval from the following, authorized security contact:

<Name>

<Name>'

(A list of the selected security contacts is provided)

- On receiving the email notification, the Security Contact, can approve or reject the CC from My Support Portal. Upon clicking the case link in email, it opens the case for security contact as below. Security contact can approve / reject after clicking on Start button.



The screenshot shows a 'Pulse' post on a support portal. The post has the following details:

- Task:** Please approve or reject this Significant Production CC
- Assigned to:** Kim Osbourne (indicated by a red circular icon)
- Buttons:** A green 'Start' button is located to the right of the assignee's name, and it is highlighted with a red box.

Below the post, there is a navigation bar with tabs: Pulse, Details, References, Tasks, Enterprise data, and Account team. The 'Pulse' tab is currently selected. There are also buttons for Show timeline, Search, and other account management options.

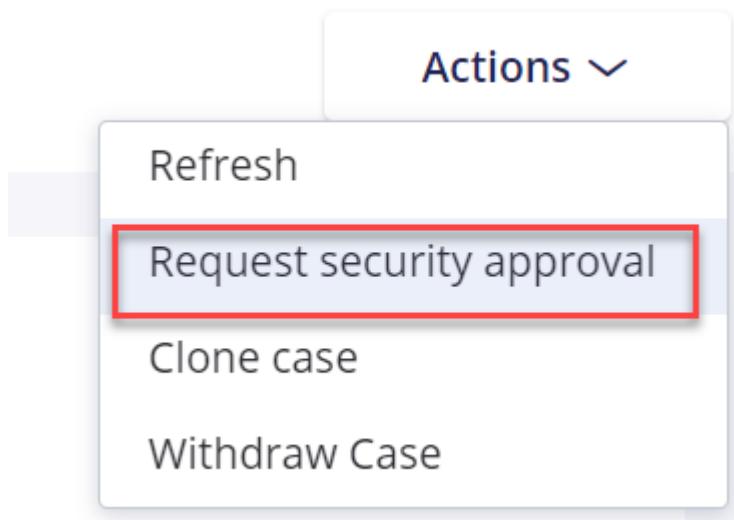
- Alternatively, any other Security Contact, on the account, can approve or reject the CC in MSP also. E.g. If a security contact, on the account selects the case from the Home page, (instead of clicking the link in the email) it will open with the Approval screen displayed.
- Note: Pega support engineers are not able to see CC's created by the client whilst they are in New-PendingSecurityApproval status. Pega support engineers are able to approve CC's from Interaction portal - only if they have created the CC themselves.
- The approval screen shows the list of the CC tasks, with Approve / Reject buttons at the bottom and a mandatory Note field, for the approver to provide a note.

Approval

Task	Category	Team responsible
▶ Data Changes	Significant	Pega

Note: *

- If any other user (without the Security Contact role) opens the case, it will open in the normal review harness.
- An additional local action is available on the CC case, to enable the requestor to select another security contact whilst in New-PendingSecurityApproval status. With this action the requestor can request approval from another Security Contact, if their original choice is unavailable e.g. Actions> Request security approval:



The following popup window is displayed:

Request security approval X

In order to process this significant production cloud change request, a security contact must provide approval.

Select security contact to request approval

Name	Email	Phone
No items		

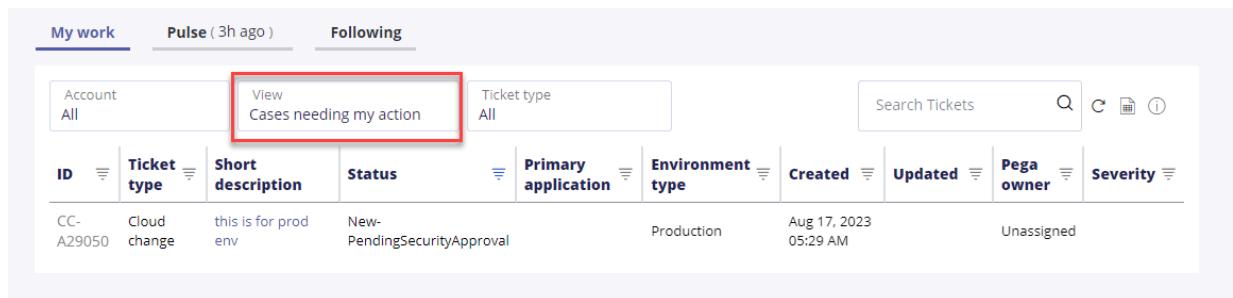
[Add security contact](#)

[Cancel](#) **Submit**

Whilst awaiting approval

- The CC case remains with the requestor.
- For requestor, and any Security Contact affiliated to the account, the CC case will be displayed in Cases needing my action, All cases, My Open cases, All open cases lists in My Support Portal.

For Example:



The screenshot shows the Pega My Work interface. At the top, there are three tabs: 'My work' (selected), 'Pulse (3h ago)', and 'Following'. Below the tabs is a search bar with filters for 'Account' (All) and 'Ticket type' (All). A red box highlights the 'View Cases needing my action' button. To the right of the search bar are icons for 'Search Tickets', 'New', and 'Help'. Below the search area is a table header with columns: ID, Ticket type, Short description, Status, Primary application, Environment type, Created, Updated, Pega owner, and Severity. The table contains one row of data:

ID	Ticket type	Short description	Status	Primary application	Environment type	Created	Updated	Pega owner	Severity
CC-A29050	Cloud change	this is for prod env	New-PendingSecurityApproval		Production	Aug 17, 2023 05:29 AM		Unassigned	

- Whilst in New-PendingSecurityApproval, requestor cannot edit the case.
- Likewise, Security contacts can see the details in assignment as read only. Only the approver Note field is editable.
- Pulse is also available to post messages.

Approval / Rejection

Approval

- Once approval is received from security contact, case is moved to either New-PendingDateVerification (see below for details) or Pending-Investigation.
- - A Pulse post is added: '*This change has been approved by the Security Contact, <Name>, with the following comment: <Comments:...>*'
- An Email Notification is sent to the parties on the case advising: '*This change has been approved by the Security Contact, <Name>, with the following comment: <Comments:...>*'

Rejection

- If the security contact rejects the case, it is moved to Resolved-Rejected and cannot be reopened.
- A pulse post is added to the CC case to confirm closure: '*This change has been rejected by the Security Contact, <Name>, with the following comment: <Comments:>*'
- An Email Notification is sent to the parties on the case advising them of case closure: '*This change has been rejected by the Security Contact, <Name>, with the following comment: <Comments:>*'

No Response

- If no approval is forthcoming, cases can only remain in a New-PendingSecurityApproval state for 30 days before being resolved automatically. The status is then updated to Resolved-PendingSecurityApproval'
- - A pulse post is added to the CC case to confirm closure: '*Case automatically withdrawn for no action after 30 days from last update*'
 - An Email Notification is sent to the CC Requestor advising them of case closure: '*Case automatically withdrawn for no action after 30 days from last update*'

Revalidate Date / Time

After the approval is received, the system will revalidate the scheduled start date to verify:

- If case falls under 2 hours to schedule start time.
- If case schedule start time is in the past.
- If emergency justification not provided earlier but since approval delayed, case schedule start time is within suggested schedule time and hence emergency justification needed.

During this process the case status is 'New-PendingDateVerification'.

Regardless of the scenario, the approver can still approve the CC case, but the case remains assigned to the CC requester to update the scheduled date or provide the relevant business justification.

The following message is shown: *"This Change has now been authorized by your security contact. However, the dates provided are no longer compliant with the date parameter. Please review the schedule and re-submit. This Change will not be required to be approved again."*

This message is added to the case as a pulse post and the parties to the case are notified by email.

When the case is opened, this message is also displayed on the top of the screen. MSP should suggest a suitable schedule.

Similarly, if the planned schedule date means that the CC has moved from being 'Normal' to 'Emergency' the approver can still approve the CC case, but the CC case remains assigned to the CC requester to either update the date or provide the business justification for an Emergency CC....

After the requestor updates the start date and time the case status moves directly to the Triage stage, since the case is already approved. As such it is routed to the for triage.

The case will be auto resolved (Resolved-PendingDateVerification) after 30 days if the date is not amended appropriately.

Details tab

The details tab now has a Security approval section to reflect who provided the approval.

Description

Change plan: Significant

Scheduled start time	Monday, August 28, 2023 7:32:00 PM AKDT
Scheduled end time	Monday, August 28, 2023 10:33:00 PM AKDT
Tested on a lower environment	No
Reason for not testing on lower environment	my reason
Is emergency	No

Task	Team responsible	Singular task
Data Changes	Pega	No

Primary application

Primary application	Test
---------------------	------

Security approval

Security contact	[Redacted]
Approver comments	—
Security approval email received	Yes
Approval email uploaded by	[Redacted]

Where the cloud specialist is also the security contact the following text is displayed:

'Security contact created this case'

Where Security approval is provided via an email attachment the Security Approval section will display the following additional text:

'Security approval email received'

'Approval email uploaded by'

If the CC is rejected the details tab will display the following additional text:

'Approver rejected this request'

Pega Cloud Security and data protection

Pega Cloud® provides a secure and robust environment that includes your environment infrastructure and the Pega software that you requested Pega to install in your environment for you.

For more on Pega Cloud Security, see [Security standards for Pega Cloud](#).

Every Pega Cloud environment offers a high level of security and data integrity, including the following:

- Host-based virus protection services, scans, and signature updates
- Protection against DDOS attacks
- Usage of known IP address reputation lists to block access from bad IP addresses
- Host-based Intrusion Prevention System (IPS) and File Integrity Monitoring
- Continuous security monitoring of Pega Cloud environments
- Pega Cloud client-specific [data-at-rest encryption](#) and [data-in-transit encryption](#)
- Dedicated security team that manages compliance, security monitoring, and [Incident response and management for Pega Cloud](#)
- Vulnerability and security management of Pega Cloud environments

Pega Cloud client vulnerability testing requests and other security reviews can be accommodated following the [Vulnerability testing policy for applications on Pega Cloud](#).

Pega Cloud clients are responsible for following application-design best practices and principles in building, maintaining, and securing the configured elements of their applications.

- [Data-at-rest encryption](#)
- [Data-in-transit encryption](#)

- **Vulnerability testing policy for applications on Pega Cloud**
- **Vulnerability testing process for applications on Pega Cloud**
- **Considerations when Pega decommissions a Pega Cloud environment**
- **Anti-virus on Pega Cloud**

Data-at-rest encryption

Pega Cloud® uses data-at-rest encryption (DARE) in all Pega Cloud environments to help secure your application data and comply with industry-standard security requirements. "Data at rest" refers to any content that the cloud service saves on a hard drive.

Encryption of data at rest is implemented for all sandbox and production environments. All client data stored in volumes, databases, and S3 buckets in a Pega Cloud environment are encrypted with 256-bit AWS encryption. The keys are rotated on a regular basis and are securely stored in Amazon KMS.

Data-in-transit encryption

Pega Cloud® maintains policies to implement data-in-transit encryption for Pega Cloud sandbox and production environments. Using data-in-transit encryption Pega Cloud ensures network connections meet the highest industry standards and helps your application comply with your enterprise security requirements.

Pega Cloud encrypts the following network connections:

- Internal connections in the service, such as service-to-service and node-to-node connections.
- External connections to the service, such as Pega environment-to-client data connections. To review how Pega Platform™ supports TLS and follow recommended practices, see [Transport Layer Security \(TLS\) best practices](#).

Certificate management practices for developing applications to run in Pega Cloud

Pega Cloud secures inbound interfaces in AWS deployment regions using Amazon ACM root Certificate Authorities (CAs). Modern operating systems and browsers use the Amazon Trust Services CAs by default; if you use an older software or your application is using a custom trust store or certificate store, you must add Amazon Trust Services CAs to ensure seamless connectivity to Pega Cloud.

Due to the dynamic nature of certificates used in Pega Cloud, Pega recommends that source systems and your applications that interact with Pega Cloud environments do not use certificate pinning. This policy aligns with Amazon and Google best practices.

Pega recommends that source systems and your applications that interact with Pega Cloud environments adopt the use of a common alternative to certificate pinning known as Certificate Transparency (CT). For details, see [How CT fits into the wider Web PKI ecosystem](#).

If your application uses certificate pinning to leaf or intermediate certificates, please update your application to pin to all Amazon root certificates or adopt CT practices by April 10, 2023. By doing this, you can avoid any service issues that can occur during an automated certificate renewal by Pega or AWS. This request aligns with the [AWS certificate manager best practices for certificate pinning](#); to review the latest certificates in use, review the Root CA Certificate Information section of [Amazon trust services Certification Authorities repository](#).

Required client reviews following infrastructure updates

As the Pega Cloud service evolves, Pega updates this page to show the most recent protocol and cipher support changes and protocols or ciphers that your service no longer supports. After Pega security-policy or infrastructure-update communications that include security protocol or cipher support changes, the Pega Cloud servers negotiate from this list of ciphers in order of preference. To support this change, review and make certain that any of your clients (such as a Web browser) that interact with Pega services support the updated list.

Pega provides this information as soon as possible so your environment's security administrators and network administrators can prepare for upcoming changes.

Latest supported protocols and cipher suites for data-in-transit

The following table lists the ciphers that clients can use for their data-in-transit inbound connections connections to Pega Cloud; the table does not apply to outbound connections from Pega Cloud.

Supported TLS encryption protocols and cipher suites effective June 2023	
Protocols	
TLSv1.2	
TLSv1.3	
Ciphers:	
TLS-AES-128-GCM-SHA256	
TLS-AES-256-GCM-SHA384	
TLS-CHACHA20-POLY1305-SHA256	
ECDHE-ECDSA-AES128-GCM-SHA256	
ECDHE-ECDSA-AES256-GCM-SHA384	
ECDHE-RSA-AES128-GCM-SHA256	
ECDHE-RSA-AES256-GCM-SHA384	

Vulnerability testing policy for applications on Pega Cloud

Pegasystems permits Pega Cloud® services clients and Pega Cloud® for Government clients (hereinafter referred to as "Pega Cloud" clients) to conduct security assessments for applications on Pega Cloud as needed, when such assessments are preauthorized and performed within the guidelines described in this article.

Pegasystems allows application-tier vulnerability scanning when Pega Cloud clients need to assess and report on the security of their cloud-delivered applications, client-directed development, and related services for the purposes of internal audit or compliance programs.

Environments that can be tested

Pegasystems permits Pega Cloud clients to conduct application vulnerability tests on their Pega Platform applications that are deployed in Preproduction (large sandbox) and Production environments. Pega Cloud clients are not permitted to conduct application vulnerability tests on any trial environments.

Pegasystems also permits Pega Cloud clients to conduct application vulnerability tests on their Pega applications that are deployed in Development and Test (small sandbox) environments. However, Pega Cloud clients must realize that Development and Test environments, by definition, are more open than Production environments, and can identify issues that will not be present in Production environments.

Testing should focus on Pega Cloud clients' applications rather than the Development environment. Testing of the Development environment itself is not recommended for several reasons:

- The Development environment, by design, allows for software development and modification of the running system. For example, clients can unlock RuleSets in a Development and Test environment, as development is still occurring and engineers are still making changes to rules. In a Production environment, RuleSets

should be locked. Testing in non-Production environments might find vulnerabilities that are inherent to a Development and Test environment. Testers and scanners will find issues in the Development environment that would be high risk in a Production environment, but that are necessary on a Development system.

- Penetration testing can damage the system being tested. It can include the application rules themselves. Be sure to completely back up your applications before doing any testing.
- The Pega application portals, such as AppStudio and DevStudio, are much larger in scope than most user-facing applications, and take more time and expense to test.

Do not use Development and Test environments for production services or for hosting sensitive or production data.

Policy Terms and Conditions

Each requestor must abide by and agree to the following terms that Pega outlines before being authorized to conduct any security assessment or penetration testing. All Security Testing must comply with the Pega Security Testing Term and Conditions.

Security Testing (the "Testing"):

1. The client must submit a service request to notify Pega of the vulnerability testing.

For more information, see *Initiate a Pega Support request* in [Vulnerability Testing Process](#).

2. Testing is limited to the services, network bandwidth, requests per minute, instance-type, and duration outlined in this agreement, the client's services agreement.
3. The client is only permitted to test their Pega applications. The client is not permitted to attempt to penetrate beyond their applications, or to attempt to breach the Pega Cloud infrastructure or supporting services.

4. The client is responsible for any damages to Pega Cloud or other Pega Cloud clients that are caused by their penetration testing activities.
5. If the client discovers any vulnerabilities or other security issues which are rated "very high" or "critical" within any Pega Cloud in the course of their security assessment, they must report this issue directly to Pegasystems within 24 hours of discovery. The client may continue their tests, but is not permitted to further exploit or test against any suspected critical or high vulnerability or other security issue.

For more information on how to report an issue, see *Reporting a finding* in the [Vulnerability Testing Process](#).

6. Upon completion of their testing, the client must submit an executive summary report (at minimum) to Pega GCS using a Service Request through the Support Portal, and request a review of the findings. Sending a full report is recommended.
7. Distribution of the report beyond Pegasystems and the client is subject to mutual written agreement.
8. To extend or modify the agreed-upon testing period, the client must submit a new request.

Permitted Services: Using Security Assessment Tools and Services

You have many public, private, commercial, and/or open-source tools and services to choose from for performing a security assessment of the client's Pega Cloud environments. The term "security assessment" refers to all activity engaged in for the purposes of determining the efficacy or existence of security controls, such as:

- port-scanning
- vulnerability scanning/checks
- penetration testing
- web application scanning
- Using an EICAR anti-virus test file to validate the presence of anti-malware scanning for file upload vectors.

The client is not limited in their selection of tools or services to perform a security assessment of their Pega Cloud environments. However, the client is prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such against any Pega Cloud environments, their own or otherwise. For a list of prohibited activities, see the next section.

A security tool that solely performs a remote query of your Pega Cloud environments to determine a software name and version, such as "banner grabbing," for the purpose of comparison to a list of versions known to be vulnerable to DoS, is not in violation of this policy.

Additionally, a security tool or service that solely crashes a running process on the client's Pega Cloud environment, temporary or otherwise, as necessary for remote or local exploitation as part of the security assessment, is not in violation of this policy. However, this tool cannot engage in protocol flooding or resource request flooding, as mentioned in the *Prohibited Activities* section.

A security tool or service that creates, determines the existence of, or demonstrates a DoS condition in any other manner, actual or simulated, is expressly forbidden.

Some tools or services include actual DoS capabilities as described, either silently/inherently if used inappropriately or as an explicit test/check or feature of the tool or service. Any security tool or service that has such a DoS capability, must have the explicit ability to disable, disarm, or otherwise render harmless, that DoS capability. Otherwise, that tool or service cannot be employed for any facet of the security assessment.

It is the sole responsibility of the Pega Cloud client to: (1) ensure the tools and services employed for performing a security assessment are properly configured and successfully operate in a manner that does not perform DoS attacks or simulations of such, and (2) independently validate that the tool or service employed does not perform DoS attacks, or simulations of such, prior to conducting the security assessment of any Pega Cloud environments. This Pega Cloud client responsibility

includes ensuring that contracted third parties perform security assessments in a manner that does not violate this policy.

Furthermore, the client is responsible for any damages to Pega Cloud environments or other Pega Cloud clients that are caused by the client's testing or security assessment activities.

Prohibited Activities

Some penetration-testing activities could trigger a number of security events or affect resources for other clients. Therefore, activities that can damage resources or cause harm to any clients' environments are prohibited, including but not limited to the following activities:

- DNS zone walking
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS or other activity with the intent to overload, flood, or spam any part of the services
- Port flooding
- Protocol flooding (for example, SYN flooding, ICMP flooding, UDP flooding)
- Request flooding (login request flooding, HTTP request flooding, API request flooding)
- Testing of environments, domains, or URLs not specifically contracted by the client
- Intentionally sending, injecting, or uploading a virus or a corrupt file, Trojan horse, or worm

Vulnerability testing process for applications on Pega Cloud

Pegasystems permits Pega Cloud® services clients and Pega Cloud for Government clients (hereinafter referred to as "Pega Cloud" clients) to conduct security assessments for applications on Pega Cloud as needed, when Pega Cloud clients perform such assessments within the guidelines described in this article.

Pegasystems permits application-tier vulnerability scanning when Pega Cloud clients need to assess and report on the security of their Pega Cloud-delivered applications, client-directed development, and related services for the purposes of internal audit or compliance programs.

Vulnerability Testing Process

Prerequisites

Pega Cloud clients must complete the following tasks before engaging in the Vulnerability Testing Process:

1. Adhere to the Pega Cloud [Vulnerability testing policy for applications on Pega Cloud](#).
2. Validate that the tool or service that you will employ for vulnerability testing is not configured to perform any of the functions described in the Prohibited Activities section of the Vulnerability Testing Policy.
3. Secure the deployed applications according to [Security Checklist on Pega Cloud](#).

Before clients can begin any vulnerability testing, Pegasystems requires that clients harden the Pega applications that will be tested. For details on application hardening, please review the checklist and complete all the applicable steps.

Some of the steps in this checklist do not apply to a Pega Cloud Development and Testing environment. For example, one step states to “set the system production level to 5.” Pega Cloud Development and Testing environments are set to “2” and cannot be changed. Clients must take these factors into account when reviewing vulnerability test results.

Test Process

1. Initiate a Pega Support request.

Authorized contacts for the client submit a service request ticket in the [My Support Portal](#) or call the help desk to initiate the process for the a client-led

vulnerability scan. Allow at least one business day for notice before the start of a vulnerability scan.

To submit this ticket directly, select [New Request](#) in [My Support Portal](#). In this request, choose **For something I need** and then click **Other**. For the latest documentation on making requests, see [Creating a support ticket](#).

Pega Cloud clients who employ allow lists or who limit access for their environments to private networks must include a temporary allow list for the source testing IP addresses in their service request.

Clients must provide the following information in this service request:

- Contact details, including email address and office and mobile phone numbers
- Description of the assessment and test cases
- Start and stop dates of the test
- Source IP address of the scanning tool or service

2. The Service Request is received.

Global Client Support receives the support request, documents it in our testing calendar, and closes the request. (There is no longer any need for authorization.)

3. Provide the report to Pega using [My Support Portal](#).

Authorized contacts for the client are required to share an executive summary report (at a minimum) of the results of the vulnerability tests with Pega to help the continuous improvement of cloud services. Pegasystems requests that clients send a full report, if possible. To enter a Service Request to submit this report, select [New Request](#) in [My Support Portal](#).

Distribution of the report beyond Pegasystems and the client is subject to mutual written agreement.

Reporting a finding

If the client discovers any vulnerabilities or other security issues which are rated “very high” or “critical” within any Pega Cloud in the course of their security assessment, an authorized contact for the client must report this issue directly to Pegasystems within 24 hours of discovery, by selecting New Request in [My Support Portal](#).

In this request, the client should choose For something I need and then click Other. For the latest documentation on making requests, see [Creating a support ticket](#).

Enter a Short Description of this issue similar to the following:

P1 Vulnerability Finding: <short description of issue>

For example, P1 Vulnerability Finding: activity should require permissions

(This description allows Pega to route this issue to the Cloud Security Operations team as quickly as possible.)

In the full description of the issue, please include:

- Date Issue was Discovered
- Who Discovered
 - Name
 - Company
- Contact Information (Who should be contacted about this issue?)
 - Contact Information
- Supporting Data and Screen Shots (excluding any sensitive or personally-identifiable information)

Tips for Security Testing

Pega Cloud client's security testing should be a positive experience that efficiently gathers the objective evidence you need, without errors or interruptions. Below are some helpful tips to ensure successful testing:

- Rate limits – Limit scanning to 1Gbps or 10,000 RPS.
- Source Testing IP Addresses – Because of the dynamic nature of cloud environments, verify all IP addresses in test plans prior to the beginning of a test to ensure current ownership of the IP address. Any attempt to test with unauthorized source IPs addresses will be considered a violation of the [Pega Products and Services Acceptable Use Policy](#).

Considerations when Pega decommissions a Pega Cloud environment

Pegasystems Inc. removes Pega Cloud environments using a standard process known as decommissioning.

The information in this document is for planning purposes only. It is subject to change at the discretion of Pegasystems Inc.

VPC and environment decommissioning scenarios

Pegasystems Inc. uses its standard decommissioning process for the removal of VPC or environments deployed within it for the following scenarios:

- The application moves to a client-managed cloud environment as part of cloud choice. For details, see [Get the flexibility you need – with cloud choice](#).
- The Pega Cloud Services contract expires, or you request to no longer subscribe to Pega Cloud Services.
- The 30-day trial period ends on the provided cloned environment used during the client upgrade assessment process. In this case, Pegasystems Inc. deletes the upgraded, cloned staging environment within 7 days of completing all of the live environment upgrades. For more information, see [Pega Cloud maintenance and types of system updates](#).

Pegasystems Inc. also decommissions environments as part of its standard reprovisioning process, which is a three step Pega Cloud process that includes:

1. Provisioning of a new environment
2. Migration data from the old environment to the new environment
3. Decommissioning the original environment

Pega Cloud reprovisions environments following client requests for the following configuration changes:

- A request to rename a current URL/environment. This request requires reprovisioning because renaming isn't supported. Instead, the client receives a newly provisioned environment with the new name.
- Moving environments to a different VPC in the same or another supported region that Pega Cloud supports.

Note: Pegasystems Inc. will make a reasonable effort to minimize the downtime and impact of migrating the client data and configurations to the new environment.

The data and resources deleted after a Pega Cloud decommissioning

After Pega Cloud decommissions a VPC or the environments deployed within it, the following data and resources are no longer recoverable:

- Pega application, configuration, and data
- Pega Cloud resources included but not limited to, resources listed in the table.

Resources	Following a VPC decommissioning	Following an environment decommissioning	Following a cloned environment decommissioning
Cloud file storage data		□	□

Resources	Following a VPC decommissioning	Following an environment decommissioning	Following a cloned environment decommissioning
IP address ranges on a list of allowed connections	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AWS authentication keystores	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN configurations	<input type="checkbox"/>		
Data snapshots	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pegasystems Inc. responsibilities

Pegasystems Inc. responsibilities include the following actions:

- Send notification of the 30-day window during which you can access your VPC and Pega Cloud environments before they are decommissioned which include the following items:
 - An e-mail confirmation of the start date of the 30-day window
 - A My Pega Cloud portal banner displaying the end date of the 30-day window of access
- Return your data persisted to Pega Cloud Services in a common industry-standard format (such as database export or snapshot) following your request for this data

Client responsibilities

If your deployment needs a customization that is not currently supported in standard Pega software functionality, you can request Pega to include such functionality in future Pega software releases by selecting [Create a ticket](#) in [My Support Portal](#) or by using the [Pega Support Contact Information](#) contact listed for your region. For the latest documentation, review [Creating a support ticket](#) and the [My Support Portal FAQ](#).

Depending on the type of decommissioning, you no longer have access to the Pega Cloud VPC or its environments.

Anti-virus on Pega Cloud

Anti-virus (AV) capabilities are deployed on all Pega Cloud environments for workload protection, file and attachment uploads that follow standard upload flows, SFTP uploads, Data Transfer Service, and Cloud File Storage. The Pega Cloud Security Operations Center (CSOC) is notified any time an Anti-virus scan detects potential malware, and the suspected file is quarantined. No client action is needed to handle the file. Review this table to learn about Pega's anti-virus strategies.

For more information on how Pega keeps you safe, see [Pega Cloud Security and data protection](#) and the Pega Platform [Security Checklist](#).

Category	Protected?	Response to flagged files	What will a user see if a file they upload is flagged by Pega's AV?
Pega Cloud Infrastructure Workload protection	Yes.	Quarantined.	Pega Platform will display an error message such as, "Unable to get the file from repository. There was issue with the file path or repository configuration/connection."
File and attachment uploads	Yes, for standard upload flows that use the out-of-the-	Quarantined.	Pega Platform will display an error message such as,

Category	Protected?	Response to flagged files	What will a user see if a file they upload is flagged by Pega's AV?
	box Pega file attachment rule. Client-created custom upload flows are not protected.		"Unable to get the file from repository. There was issue with the file path or repository configuration/connection."
SFTP Uploads	Yes.	Quarantined.	An error message will appear when the user attempts to access the file, but the message content will vary based on the access method.
Data Transfer Service (DTS)	Yes.	Quarantined.	Error 403 returned with scan results via API call.
Cloud File Storage (CFS)	Yes.	Quarantined.	An error message will appear when the user attempts to access the file, but the message content will vary based on the access method.