I'm not a robot

Skip to main content Official websites use .gov A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPS A lock (Locked padlock icon) or https:// means youve safely connected to the .gov website. Share sensitive information only on official, secure websites. Want to learn more about our services? Wed love to hear from you. You purchase access to cloud.gov by buying a tier with enough credits to support your needs. Credits can be spent on application memory or managed cloud services like databases. Additional professional services are available for $250/hr. Tier Credits (Annual) Credits (Monthly*) Annual Price Sandbox N/A 8 $0 Femto 600 50 $30,000 Pico 1200 100 $60,000 Nano 1800 150 $90,000 Micro 3000 250 $150,000 Milli 4200 350 $210,000 Centi 6000 500 $300,000 Deci 7800 650 $390,000 Deka 9600 800 $456,000 Hecto 12000 1000 $540,000 Kilo 15000 1250 $637,500 Mega 18000 1500 $720,000 Giga 24000 2000 $936,000 * All credits are available up-front when your IAA is executed. You can spend credits flexibly throughout the year if your compute needs change over time. Monthly credit amounts are provided for reference. Price per credit $50 Credits per GB of memory3 IAA Fee (yearly) $0 Contact us to learn more about available discounted enterprise pricing as well as pricing for brokered services. You can use our Cloud.gov Cost Estimator.xlsx (v1.6 published July 3, 2025) spreadsheet to estimate your system costs. Built-in FedRAMP compliance Resources and guidance Customer and community support Continuous security compliance Single-sign-on features Cloud.gov has a Provisional Authority to Operate (P-ATO) at the Moderate impact level from the FedRAMP Joint Authorization Board (JAB). This means Cloud.gov has undergone a significant, thorough security and compliance review so that your agency can focus on reviewing the parts of the system that serve your mission more directly.What is a P-ATO? The Federal Risk and Authorization Management Program (FedRAMP) evaluates cloud services and issues a Provisional Authority to Operate (P-ATO) to those that pass review. Those come in two flavors: Agency and JAB. Both authorizations look at a standardized set of FISMA and NIST requirements and both can be used by other agencies in their ATO process. The difference is, when the Joint Authorization Board (JAB) is convened, its to review a cloud service that is and should be used throughout the government. The members of the JAB are the CIOs of the General Services Administration, Department of Defense, and Department of Homeland Security. They issue a P-ATO for cloud services that pass their review and to be used to run systems holding any kind of government data at specific levels. Cloud.gov has an authorization at the moderate level which means it is a vetted and trustable service for data where the impact of loss is limited or serious but not catastrophic.Once that P-ATO is granted, FedRAMP requires Cloud.gov to undergo re-assessment every year and maintain continuous monitoring. This gives your agency ongoing assurance that Cloud.gov is compliant.For DoD teams: the Defense Information Systems Agency (DISA) has issued a DoD Provisional Authorization for Cloud.gov at DISA impact level two. Some points to bear in mind:The FedRAMP package (see below) includes the DISA Provisional Authorization (PA) letter for your reference.Per the PA and the DoD Cloud Computing SRG, the artifacts available to an Authorizing Official (AO) are those included in the FedRAMP-approved package. See Figure 5-2, DoD Continuous Monitoring for CSOs with a FedRAMP JAB PA in the Cloud Computing SRG for a useful illustration to that effect.To meet the intent of OMB and DoD policies that cloud authorization follow a do once, use many times framework, Cloud.gov will not provide artifacts that are already encompassed by the FedRAMP authorization and continuous monitoring program.How you can use this P-ATO Your agency still needs to grant your system an Authority to Operate, but FedRAMP has done the labor-intensive work of reviewing Cloud.govs security posture and endorsed it, which reduces the compliance work you need to do. Your agencys authorizing official can request the P-ATO documentation package from FedRAMP and accept that endorsement for your own system. See ATO process for the typical workflow.Heres how it works: Every moderate-impact federal system is required to account for a baseline of at least 261 controls (your agency may have additional controls) before it can be granted an ATO. The Cloud.gov platform provides you with 155 fully or partially inheritable controls. Once Cloud.govs P-ATO is reviewed and accepted, many of those requirements are already implemented and documented. Responsibility for most of the remaining requirements are shared between Cloud.gov and your application, and only a limited number are fully yours.Heres an example of a control breakdown for a simple moderate-impact system hosted on Cloud.gov: We publish two CIS/CRM documents, one for the Paas/Platform service and one for the Pages service:Cloud.gov Platform Cloud.gov PaaS CIS Worksheet summarizes each Low and Moderate security control and whether it is handled by Cloud.gov (inheritable), a shared responsibility, or a customer responsibility. It includes guidance on which controls a customer on the Platform can fully or partially inherit from Cloud.gov.Last Update: 2023-03-17 - Updated front matterCloud.gov Pages The updated CIS/CRM documents using FedRAMP rev5 templates has been uploaded to connect.gov. To download the documents, please complete the FedRAMP Package Access Request Form and follow your agencys access approval process.Updated: 2024-07-30 - Updated language to use new process for obtaining documentation through connect.govUpdated: 2024-04-09_ Updated the date of change to the CIS/CRM._ The CIS/CRM has been updated and revised using the latest FedRAMP rev5 template including Low andModerate controls. The CRM focuses on the consideration of Cloud.gov Pages static website customers.Updated: 2022-11-15 - First published CIS/CRM for Cloud.gov PagesStart the ATO process If you want to authorize Cloud.gov, request the P-ATO documentation package from FedRAMP (the Package ID for that form is F1607067912). GSA customers can use the DocuSign Template for a FedRAMP Package Access Request. You can also view the FedRAMP Marketplace page for Cloud.gov.Once the FedRAMP Program Office has granted you access, youll be able to access the Cloud.gov package within the CG-TTS folder of the FedRAMP Repository. If youre interested in using cloud.gov, email support@cloud.gov. Well schedule a call to answer your questions and help you get started.If you have a U.S. federal government email address, you can get access to a free sandbox space.Support for people who use cloud.gov Email support@cloud.gov. See our customer service objectives page for information about our support availability.If you need help with an application security incident, the request should come from the System Owner or Org Manager, to help us validate the request. For an active incident, refer to our standard security.txt file.You should not include any passwords or sensitive environment variables in your email (we dont need them to help you, and you should keep them protected).Report a vulnerability We welcome vulnerability reports according to our vulnerability disclosure policy, which includes how to best contact us for this kind of information.Questions from the public and industry If you have a question that isnt on behalf of a U.S. government organization (such as if youre a member of the public or representing a company), we invite you to post your question publicly as an issue on GitHub (requires a free GitHub account), so that we can write an answer available to everyone. If you prefer not to post publicly, you can email support@cloud.gov.If you are part of a company asking a question to help prepare a response to a RFI/RFQ/RFP (or a similar proposal process), we will ask you to post your question publicly as an issue on GitHub (requires a free GitHub account). We want to answer publicly so that our answer is available to all companies competing in that process.Interested in working on cloud.gov? Check out joining TTS if youd like to join cloud.gov or another TTS program. You can expand the functionality of your cloud.gov application by making use of services. Before your application can use a service, you must provision the service and supply the credentials for using the service to your application.There are two ways to provision services:User-provided service instances: You can provision a service manually outside of cloud.gov, then supply the credentials yourself.Managed service instances: You can provision a managed service instance through the marketplace in cloud.gov on demand, and let cloud.gov supply the credentials.When to use a user-provided service User-provided services enable developers to use services that are not available in the marketplace with their apps running on Cloud.gov.If the provisioning of the service is not automated or already existent, you should set up a user-provided service.You should use/setup a user-provided service when:You need to get credentials to a cloud.gov appYou are using third-party APIsYou want to link to a database external to cloud.govSetting up user-provided service instances Once youve provisioned a service manually, create a user-provided service instance to hold the credentials. Bind the service instance to your application to make the credentials available.Example of creating a service that requires username and password:cf create-user-provided-service -p "username, password"You will be prompted to enter a username and password for your app Or you can pass in your username and password in one line with:cf cups -p '{"username":"admin","password":"pa55woRD"}'Provisioning managed services through the marketplace cloud.gov offers a marketplace of FedRAMP-authorized managed services that we operate in a secure and compliant manner on your behalf. You can also extend the marketplace to include additional services run by other organizations.To list all the managed services and plans available to a given space, you run cf marketplace from your command line. Here is a list of the managed services that are generally available:Service NameDescriptionSupport Statusaws-rdsPersistent, relational databases using Amazon RDSProductionaws-elasticacheAWS ElastiCache Redis 5.0.6 as a serviceProductionaws-elasticsearchAWS Elasticsearch 7.4 as a serviceProductioncdn-routeCustom domains, CDN caching, and TLS certificates with automatic renewalDeprecatedexternal-domain-serviceCustom domains and TLS certificates with automatic renewalProductioncloud-gov-identity-providerAuthenticate cloud.gov users in your appProductioncloud-gov-service-accountcloud.gov service accounts for automated access by programsProductioncustom-domainsCustom domains and TLS certificates with automatic renewalDeprecateds3Amazon S3 provides developers with secure, durable, highly-scalable object storageProductionSupport Status Production: The service has been tested to ensure it has the resiliency required for a production system. Beta: The service is stable but still requires further development to ensure it can be deployed to production systems. Alpha: The service is under development and some downtime or data loss can occur. Deprecated: The service is deprecated and will be removed in a future release - please update.Extending the marketplace Brokers are the invisible integrators that enable you to set up managed service instances in cloud.gov in a consistent and self-service fashion. A broker offers a simple API that manages the service instance lifecycle. You can run your own broker to make a service from outside cloud.gov available through cloud.govs marketplace.Note that when you extend the cloud.gov marketplace with your own broker, the cloud.gov team cannot vouch for the security or compliance of the brokered services. You will need to document and authorize your own brokered services in accordance with your agencys compliance requirements.This tutorial includes instructions for integrating your own broker, and demonstrates how to deploy sample brokers into cloud.gov. Once youve reviewed this tutorial, you may want to investigate some of the community-supported broker add-ons for Cloud Foundry such as the app-autoscaler.The Open Service Broker API (OSBAPI) standardizes the way brokers work between Cloud Foundry and Kubernetes. Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure maintain open-source OSBAPI-compliant brokers. These brokers enable you to extend the cloud.gov marketplace with services from these providers.You can also write your own broker to manage the lifecycle of a service or automate a process unique to your organization. Check out the example service brokers for some interesting use-cases such as provisioning GitHub repositories or virtual machines.Note: If youre a vendor with a broker for a FedRAMP-authorized service that youd like to be made available for all users of cloud.gov, please contact us to discuss whether it can be included in our marketplace. cloud.gov is a secure and compliant Platform as a Service (PaaS). cloud.gov helps federal agencies deliver the services the public deserves in a faster, more user-centered way.cloud.gov allows your development team to focus on products that serve your agencys mission, without needing to manage the underlying server infrastructure. And cloud.govs built-in compliance support helps customers create the documentation and continuing assurance necessary for federal services to comply with FISMA regulations and agency-specific Authority to Operate (ATO) requirements.Platform as a Service The core of cloud.gov is a Platform as a Service built specifically for government work. The customer team is responsible for their own products code, and the cloud.gov platform handles the security and maintenance of everything underneath. Its built to keep applications online even with large numbers of users and sharp increases in usage.cloud.gov runs on top of industry-provided infrastructure (currently Amazon Web Services is the Infrastructure as a Service provider). The platform includes access to some of the most popular AWS services while removing the complexity of managing it from your experience. The cloud.gov Platform as a Service is open source. And because its based on the open source Cloud Foundry project, it provides portability to other cloud providers or your existing on-premise solution.cloud.gov provides Compliance as a Service cloud.gov was designed with FISMA compliance in mind. cloud.gov has a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the Moderate impact level. In most cases, the majority of Low and Moderate controls are managed for you. And because our documentation and controls are updated regularly, you can incorporate them directly into any compliance documentation your systems need.Why a government Platform as a Service works All federal agencies have a mandate to deploy products in the cloud. Any agency tackling this problem will face regulatory and compliance challenges. Some agencies tackle these problems with little cloud operations capability or experience. Even agencies with the right expertise can face resource shortages, confusion about the right solution, bureaucracy, or other limitations.One of our goals for cloud.gov is to give other agencies access to the same gains in productivity that we have seen from using cloud.gov. A centralized, open source PaaS model, one that is already compliant with federal rules, reduces the work and cost of cloud adoption. And the more widely its used, the more efficient it gets. Your agency can deliver more quickly and more securely with less effort.Learn more about the benefits of cloud.gov. cloud.gov allows your development team to focus on your applications. As a Platform as a Service (PaaS), cloud.gov eliminates the need to manage infrastructure such as virtual machines and servers. This enables your development team to rapidly iterate and quickly launch your application to ensure mission success. Because cloud.gov is based on open-source technologies, it provides portability to other cloud providers or your existing on-premise solution.cloud.gov is developed by a government team (housed within the U.S. General Services Administrations Technology Transformation Service), for government work.cloud.govs mission is to support agency efforts to improve the way they manage information technology. cloud.gov helps government teams gain expertise in cloud technology, and it supports partnerships with vendors and contractors that prefer to build using cloud platforms.Learn more about cloud.gov.Compliance cloud.gov was designed with FISMA compliance in mind. cloud.gov has a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the Moderate impact level. The vast majority of Low and Moderate controls are managed for you.Free sandboxes Anyone with a U.S. federal government email address can get access to a free sandbox space and try cloud.gov immediately. No paperwork required. Cloud.gov is a U.S. General Services Administration federal government service, for official use by U.S. government employees and contractors working on U.S. government digital services. All use of Cloud.gov may be monitored, recorded, and subject to audit, by Cloud.gov operations staff and other federal government authorities. There is no expectation of privacy for users of this system. By continuing to use this system, you consent to your use being monitored and recorded. Unauthorized use is prohibited, and individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution. Acceptable uses of Cloud.gov include building and managing government digital services, making and trying test services to learn about how Cloud.gov works, and activities contributing to the development of Cloud.gov itself. We describe these intended uses (along with guidelines and policies) in more detail in the Cloud.gov documentation. If you have questions about these conditions, please email cloud-gov-support@gsa.gov. cloud.gov is suitable for a wide range of applications, including websites and non-website applications for internal and public uses.Heres a process you can follow to identify the applications in your portfolio ready to move to cloud.gov. For help interpreting this list or evaluating specific cases, please email the cloud.gov team at inquiries@cloud.gov. The cloud.gov team can help you evaluate whether you application is easy to migrate to cloud.gov, as well as how to approach more complex applications that require more modification.Identify applications with a compatible security impact level FISMA LowFISMA ModerateDepartment of Defense Impact Level 2 (DoD CC SRG IL2) Identify applications with a supported technology stack Operating systems:Application hosting: Linux (64-bit ABI)Client workstation: AnyApplication runtime options:GoJava.NET Core (note, not .NET Framework!)Node.jsPHPPythonRRubyStatic HTML+JS+CSS64-bit Linux binary (including compiled C and C++ applications)Backing services:Relational databases: Search engines: Cache/queues: Blob stores: Bring your own broker and User-Provided Services In addition to above, you can extend your cloud.gov instance by setting up your own broker or user-provided service. Evaluate applications for cloud operations readiness Once you have a list of applications with a compatible impact level and technology stack, use these criteria to sort that list from those applications already ideally suited to running in a PaaS environment to those which are likely to require modification.Ideal applications follow as many of the 12-Factor App guidelines as possible. The more of the following questions you can answer with yes, the better. Applications that follow these guidelines are easier to migrate between modern hosting environments; the guidelines arent cloud.gov-specific except as noted!Codebase: Is the codebase tracked in version control?Dependencies: Are dependencies explicitly listed (such as package manager manifest)?Configuration: Can the configuration be retrieved from environment variables?Backing services: Does the application retry or fail gracefully if a service it connects to is unavailable?Build, release, run: Can you build the deployment artifacts outside of the deployment environment, for example in a continuous deployment system?Processes: Does the application keep its state in a backing service, rather than shared memory or filesystem?Port binding: Does the application listen for requests over HTTP?Applications that only accept requests over straight TCP are also possible, but may require additional work on the cloud.gov side to get going.Concurrency: Does the application scale correctly without modification when you run additional instances of it behind a load-balancer?Applications that require instances to be aware of each other are also possible, but may require additional work to configure correctly.Disposability: Can the application start quickly and shutdown gracefully?Dev/prod parity: Does the application exclude environment-sensitive code?Logs: Does the application emit logs as a streams of single events (eg timestamped on single lines or JSON stanzas)?Administrative processes: Can you run maintenance/management tasks as one-off processes?Watch out for networking complexity Does the application need to access services that reside in a private network (for example in your data center or in another cloud service provider)?This is supported, but adds complexity because you may need to coordinate with your agencys network security staff and cloud.gov staff.What now? Now that you have a sense of which applications are compatible with cloud.gov, and which will require more effort or are more complex, identify those which have the highest cost-of-delay That is, the systems which will deliver the most benefit and which will reduce operational and security overhead the most by being in the cloud. You may need to work with your agency leadership to come to a consensus about where theres the most pain to be relieved or the most gain to be received, from the mission and financial (rather than technical) side. cloud.gov runs on top of Infrastructure as a Service provided by Amazon Web Services (AWS) in the AWS GovCloud partition (specifically within the us-gov-west-1 region), which has a FedRAMP JAB P-ATO at the High impact level. GovCloud also offers support for other formal compliance needs such as ITAR compliance.Services in our marketplace cloud.gov brokers instances of:FedRAMP JAB-authorized services available in AWS GovCloud andServices run directly inside cloud.gov (which benefit from our own FedRAMP JAB authorization)In principle, cloud.gov can broker any service provider for which there is an implementation of the Open Service Broker API. For more information, see our docs on extending the marketplace.Other IaaS vendors we can support cloud.gov is a Platform as a Service (PaaS), which offers an additional level of services and functions beyond the basics offered by an Infrastructure as a Service (IaaS) provider. We built cloud.gov based on the Cloud Foundry open source project, which was designed to be compatible with multiple IaaS providers. For that reason, it would be possible to provide cloud.gov services using Google Cloud Platform, Microsoft Azure, or any public, commercial, or private OpenStack instance in the future.If youre an IaaS vendor interested in offering your solution to cloud.gov users We recommend examining the BOSH Cloud Provider Interface (CPI) documentation. Provide a CPI which makes it possible for BOSH to manipulate your cloud. This will enable cloud.gov (or any other PaaS based on Cloud Foundry) to offer alternative API endpoints corresponding to different IaaS providers with little effort. cloud.gov will deploy on new IaaS providers and expose those as new API endpoints as warranted by agency demand. cloud.gov offers a fast way for federal agencies to host and update websites, APIs, and other applications. Employees and contractors can focus on developing mission-critical applications, leaving server infrastructure management to us. cloud.gov has a FedRAMP Joint Authorization Board (JAB) authorization, which means it complies with federal security requirements. When you build a system on cloud.gov, you leverage this compliance and reduce the amount of work you need to do. During the Canadian wildfires in the summer of 2023, traffic to AirNow.gov surged to several orders of magnitude higher than ever before. But thanks to the ability to easily scale applications on cloud.gov, the site remained up and completely healthy. I will say this right up front Cloud.gov is the single biggest factor in our success last week. The traffic we saw was astounding and beyond anything we tested for or ever even anticipated. Our ability to expand resources, combined with the CDN service in front of AirNow, made us incredibly stable. Read the EPA AirNow customer story Phil Dickerson, Leader, Information Transfer Group EPA Office of Air Quality Planning and Standards By hosting FEC.gov on cloud.gov and moving its data to the cloud, the FEC anticipates saving 85% in hosting costs and is better prepared for peak traffic events. Although the dates of FECs traffic spikes may be predictable, its still hard to prepare for the extra demands on the system. A server thats still operable but near the end of its life can have unexpected problems and buying a new server can take months. But on cloud.gov, this isnt our problem. Read the FEC case study Wei Luo, Deputy CIO Federal Election Commission Bureau of Alcohol, Tobacco, Firearms, and Explosives National Institutes of Health Department of Education Federal Bureau of Investigation Environmental Protection Agency General Services Administration

Cute free house in toca world. How to make a cute toca house for free. Free cute house in toca boca. How to make a cute free house in toca world.