Démarche : Accès à la console Cloud Pi Native - Hébergement Application (Béta)

Organisme : La direction de la transformation du numérique MIOM

Identité du demandeur

Email

Etablissement
SIRET

Dénomination

Forme juridique

Formulaire

Cette démarche vous permet d'obtenir un compte de responsable d'application sur la console Cloud Pi Native (Béta) dans l'objectif de disposer de ressources d'infrastructures et de services Cloud pour votre projet.
Cloud Pi Native est une offre moderne destinée aux administration centrales et territoriale de l'Etat.
Elle est basée exclusivement sur la conteneurisation native kubernetes et permet la mise en place d'un processus de déploiement continue hors des ministères.
Le projet devra être conforme au cadre de cohérence technique de l'offre.
cf. https://github.com/cloud-pi-native/CCT-Cloud-Native

Présentation et guide pour remplir le formulaire

Ce formulaire permet de soumettre une demande de création d'un compte principal dans un espace projet de la console Cloud Pi Native (en version Béta) afin d'obtenir les ressources d'hébergement pour votre projet. Nous avons conçu ce formulaire pour ne recueillir que le minimum d'information nécessaire pour démarrer le processus et établir la convention d'hébergement.
Lors de l'instruction vous serez mis en lien avec notre cellule d'instruction soit par échange de messagerie au sein de ce système ou bien lors d'une réunion. De votre préparation et de la qualité de vos réponses dépendrons la vitesse de traitement.

L'offre Cloud pi native est architecturées en 4 macros services :
- le compute : namespace kubernetes / openshift
- l'exposition réseau de vos namespace (RIE et/ou Internet)
- l'aide au maintien en disponibilité de votre service
- l'accélération de la construction applicative avec le couplage entre votre pipeline de développement et la chaine de construction / déploiement maitrisée par le ministère.

L'ensemble de l'offre est décrite aux l'URL suivantes :
- https://cloud-pi-native.fr/
- https://github.com/cloud-pi-native/CCT-Cloud-Native pour le cadre de cohérence associé.

Vous pouvez faire appel à un tiers, pour assister à la saisie par exemple une personne de votre équipe technique, cf fonctionnalité en haut de l'écran "*Inviter une personne à modifier ce dossier*".

En fin de dépôt vous serez invité à donner votre avis avec le bouton "je donne mon avis" afin de nous permettre d'améliorer la gestion du formulaire.

Si vous souhaitez contractualisez les services de supervision applicatives et de sécurité (SOC), demandez les guides et normes d'interface afférents lors de la contractualisation. Pour les entités du ministère de l'Intérieur, la supervision de sécurité nécessite une contractualisation spécifique avec le SOC ("C2MI").

A noter :
Ce formulaire concerne uniquement des applications fonctionnant exclusivement sur kubernetes / openshift au sein de namespace utilisant l'offre cloud pi native.

Pour les besoins de type vm / iaas, référez-vous à votre correspondant gouvernance et pour toute information sur l'offre Iaas : https://pi.interieur.rie.gouv.fr/home-dnum/cloud-%cf%80/ (uniquement accessible sur le RIE)

- Vous devrez pour soumettre votre demande, valider les champs obligatoire, tel que Conditions Générales D'usage (CGUs), respect du cadre de cohérence technique, etc... Ces éléments vous engage.
- L'hébergeur ministériel n'assure pas le support et l'exploitation, vous organisez donc votre équipe pour quelle soit capable de construire la solution applicative, gérer le run, maintenir en condition de sécurité et assurer le support vis à vis de vos usagers.
- Le compte principal est nominatif et doit être opéré par un agent de l'Etat qui s'assure de la mobilisation des ressources financières nécessaires et de l'acceptation de la convention.
- Vous serez autonome pour créer votre équipe et gérer les droits des acteurs. Vous devez préciser les éléments permettant d'établir la convention entre votre entités et l'hébergeur ministériel et vous serez en charge de valider cette proposition de convention.
- Votre équipe doit être autonome pour l'usage de l'offre à travers l'usage de la console qui permet d'interfacer vos repository applicatif et d'infrastructure avec la chaine de construction et de déploiement au sein du ministère de l'Intérieur et d'accéder aux outils fournis tel que Gitlab, Sonarcube, Registry d'image, scan de code, l'observabilité et la supervision de sécurité et argoCD pour le déploiement.
L'ensemble de vos ressources d'infrastructure seront gérées via la console dédiée.

Pour vous contactez rapidement
Les échanges lors de l'instruction seront menée via la messagerie interne de l'outils démarche simplifiée. Cependant nous pouvons être amené à vous contactez rapidement. (question rapide, prise de RDV)

Numéro de téléphone (mobile)
Indiquer ici votre numéro de téléphone (de préférence mobile pour un échange facilité pour la création ou en service opérationnel)

Echéance de mise en production / service
La mise en service de votre projet sur les environnements on-premise Cloud Pi nécessite de coordonner plusieurs activités, certaines avec des délais incompressibles.

Nous vous recommandons d'anticiper l'exposition réseau de votre projet en fournissant au plus tôt les URLs visées.
Dans l'attente de la fourniture des expositions réseau, ou d'autre service vous pouvez utiliser la plateforme d'accélérations sur Internet (secnumcloud) ou disposer d'urls temporaire @minint (uniquement accessible au ministère de l'intérieur)
A l'issus de l'instruction de votre dossier une planification estimée vous sera adressée.
La rapidité de traitement dépend de la qualité et la fiabilité des informations que vous nous transmettez

Cochez la mention applicable, une seule valeur possible
☐ Je suis prêt à héberger en production avec un développement conforme au cct

☐ Je construis actuellement ma solution et j'ai besoin de ressources pour soutenir mon développement et anticiper la mise en service

☐ Je démarre mon projet

Préciser les informations caractérisant votre projet
Ces informations aide à orienter l'instruction de votre dossier pour vous proposer l'offre la plus adaptée. Ces information seront ensuite disponibles pour automatiser la livraison et éviter de multiples resaisies. Vous devez confirmer la conformité de votre démarche au cadre étatique.

Nom du projet
Ce nom servira à créer ou rattacher votre demande dans la console. Il servira de concentrateur pour la facturation.

Descriptif de votre projet
Permet d'aider à l'instruction de votre dossier.

Je reconnais que mon système sera conforme au cadre de cohérence technique Cloud Pi Nativeen vigueur.
Le demandeur reconnais que le SI est ou sera conforme au CCT https://github.com/dnum-mi/CCT-Cloud-Native

Cochez la mention applicable
☐ Oui

☐ Non

Je confirme que mon équipe sera organisée pour construire, opérer et maintenir en conditions de disponibilité l'application.
L'équipe disposera d'outil permettant de l'aider à l'observabilité de l'application et d'une console permettant de connaitre la disponibilité des services socles pour soutenir l'activité de maintien en disponibilité.

Cochez la mention applicable
☐ Oui

☐ Non

Je confirme que le système fera l'objet d'une homologation avant la mise en service
L'homologation permet de s'assurer que le système sera opéré dans de bonnes conditions et maintenu en condition de disponibilité et de sécurité optimum.
cf : https://cyber.gouv.fr/la-methode-ebios-risk-manager

Les outils proposée par l'offre cloud pi native, vous fournissent l'inventaire des vulnérabilités identifiées selon le référentiel CVE. Vous serez en charge classiquement de faire l'analyser et de mettre en place un plan de mise à jour des dépendance ou de remédiation.

En étant conforme au volet du CCT Cloud Pi Native, vous bénéficiez de l'accès à des document pré-remplis conforme à

la démarche anssi (socle de sécurité, PES et plan d'assurance qualité).

Vous pouvez tester l'état de maturité de votre projet et recueillir des conseils avec l'outils suivant proposé par l'ANSSI: https://cyber.gouv.fr/actualites/monservicesecurise-une-nouvelle-solution-de-lanssi#:~:text=Ce%20service%20gratuit%20et%20collaboratif,d%C3%A9cid%C3%A9%20de%20donner%20la%20parole.&text=Gratuit%20et%20100%25%20en%20ligne.

Cochez la mention applicable
☐ Oui

☐ Non

Je confirme qu'un processus de maintien en condition de sécurité sera en place avant la mise en service.
Le demandeur s'engage à ce que les nouvelles vulnérabilités qui seraient susceptibles d' être découvertes seront remédiées même après un dernier déploiement stable.
Elle met en œuvre les plans d'exploitation de sécurité et de maintien en condition de sécurité décrite notamment dans le dossier d'homologation.
L'équipe prend en compte que si le suivi des plans d'action n'est pas mis en oeuvre et que de surcroît des vulnérabilités critiques sont détectées depuis le dernier déploiement stable et que l'équipe projet n'a pas pris en compte les injonctions de correction, l'application est susceptible d'être suspendu jusqu'à la remédiation pour garantir l'intégrité et la protection de ses données.

Cochez la mention applicable
☐ Oui

☐ Non

Je confirme qu'un processus de soutien usager sera mis en place dont l'équipe projet assurera la charge
Le projet doit s'organiser et communiquer autour des modalités de soutien vers ses utilisateurs. Pour les projets aux seins du ministère de l'intérieur prévoyez une fiche synthétique décrivant le service rendu et une fiche reflexe avec un point de contact à remettre au Centre National d'Assistance aux Usager (CNAU).

Cochez la mention applicable
☐ Oui

☐ Non

Le système héberge et procède au traitement de données personnelles ou personnelles sensibles au sens du RGPD sens RDH personnelles ou personnelles sensibles (au sens RGPD)
L'équipe s'engage à être conforme au RGPD, déclarer le traitement et mener une AIPD si nécessaire.

https://www.cnil.fr/fr/definition/donnee-personnelle
https://www.cnil.fr/fr/la-cnil-publie-un-guide-rgpd-pour-les-developpeurs
https://www.cnil.fr/fr/securite-cloud-informatique-en-nuage

Cochez la mention applicable, une seule valeur possible
☐ Ne contient pas de donnée personnelle

☐ Contient des données personnelles

Type de données manipulées par le SI, au sens de la classification Anssi II n°901/SGDSN/ANSSI
Cloud Pi permet d'héberger des systèmes hébergeant des données jusqu'au niveau DR.
Un hébergement de SI multi-niveaux Classe 0 et Classe 1 est possible via un hébergement dans les régions ad-hoc et l'usage d'une passerelle type Anssi adaptée (SADC).

Rappel, l'instruction interministérielle no 901/SGDSN/ANSSI (II 901) du 28 janvier 2015 définit les exigences organisationnelles et techniques applicables aux systèmes d'information amenés à traiter des informations sensibles, dont celles portant la mention de protection Diffusion Restreinte.

https://cyber.gouv.fr/instruction-interministerielle-n901

Cochez la mention applicable, plusieurs valeurs possibles
☐ Usuel / NP

☐ Diffusion restreinte

Accès à la console Cloud Pi Native - Hébergement Application (Béta)

☐ Double Niveau (classe O et Classe 1)

Système classé d'importance vitale ou essentiel.
Classification déclarée auprès de l'ANSSI. Implique la prise en compte de l'article 22 de la loi de programmation militaire.
https://www.ssi.gouv.fr/administration/protection-des-oiv/protection-des-oiv-en-france/

Cochez la mention applicable
☐ Oui

☐ Non

Plage d'ouverture d'utilisation pour les usagers
Cette information est utile pour caractériser l'application et peux servir aux équipes en charge du soutien
A ne pas confondre avec la disponibilité qui elle pourrait être de 24h/24
Indiquer 5/7 8h-18h (métropole) 7/7 24/24 ou autre à préciser.
Précisez en utilisant l'option autre sur quel(s) autre(s) territoire(s)

Cochez la mention applicable, une seule valeur possible
☐ 5/7 8h-18h métropole

☐ 5/7 8h-18h hors métropole

☐ 7/7 24/24

La DMIA (durée maximale d'interruption admissible)
Est la durée d'arrêt d'une application entre un incident et le redémarrage des premières fonctionnalités. Cette durée permet d'orienter, pour une direction métier ou une direction informatique, le choix du plan de reprise de l'activité.

Kubernetes est nativement construit pour gérer la résilience de votre application au sein du cluster avec des bascules et reprise automatisées.

Par défaut, 2 environnements de production sur 2 Datacenter sont fournis. (cf champs suivant)
Pour des DMIA inférieure à 24H, l'architecture interne de l'application et l'organisation projet doit être adaptée.

Conseils d'ordre général : veiller à ce que vos noeuds d'execution soient bien répartis sur des AZ différentes, qu'une organisation de surveillance et de prise en compte des incidents sera en place et rodée. Testez vos plans de reprise. Pensez microservices.

Littérature :
https://12factor.net/
https://developers.redhat.com/articles/2023/04/05/kubernetes-patterns-path-cloud-native

Cochez la mention applicable, une seule valeur possible
☐ 96H

☐ 24H

☐ 4H (Implique des mesures spécifiques portées par l'application)

☐ 1H (Implique des mesures spécifiques portées par l'application)

Mise à disposition de ressource de calcul
Par défaut nous mettons à disposition 1 environnement hors production et 2 environnements de productions sur 2 datacenters différents pour vous permettre de disposer immédiatement d'une solution hautement résiliante. Vous disposer d'outils d'accélération pour déployer vos clusters de base de donnée ainsi qu'un service de stockage objet S3 assurant une synchronisation asynchrone entre les DC.

La convention précise le tarif appliqué à partir des ressources consommées selon le tarif

interministériel établie par la direction interministérielle du numérique, l'exposition réseau, la supervision et la chaine de construction applicative. La convention est révisée annuellement.

Utilisation d'un environnement de travail Cloud sur Internet
Par défaut, votre équipe gère seule sa chaine de construction applicative et se dote d'un ou plusieurs environnement pour mener ses tests usines. Vous pouvez bénéficier d'un environnement sur Internet de confiance, avec un réplicat de la chaine de construction applicative (comptes séparés) et des clusters d'évaluation. Cette offre n'est pas destinée à faire de l'hébergement de production et les quotas sont limités. Le soutien est uniquement assuré en heures ouvrées hors we et jours fériés.

Cochez la mention applicable
- [ ] Oui
- [ ] Non

Quotas technique associés au namespace demandé pour faire fonctionner votre application (initiaux
Sélectionnez le template capacitaire initial. Si les quotas proposés en standard ne conviennent pas ou que vous n'êtes pas encore certain, utiliser la rubrique "Autre" et préciser votre demande.
L'hébergement d'une application sur kubernetes consomme généralement beaucoup moins de ressource qu'un hébergement classique sur VM car les services liés à l'OS hôtes sont plus optimisés. La prise en compte des bonnes pratique liés au développement permet également une élasticité horizontale native de vos "pods" selon la charge d'utilisation.

Cochez la mention applicable, une seule valeur possible
- [ ] template S (équivalent 8G RAM, 4 Vcpu)
- [ ] template M (équivalent 24G RAM, 8 Vcpu)
- [ ] template L (équivalent 48G RAM, 12Vcpu)

Capacité de stockage bloc estimée (Go) par namespace
Indiquer ici votre estimation gobale en terme de besoin de volume bloc.
Le stockage bloc est local à chaque datacenter (non répliqué)
Notes :
- votre application doit prendre en charge la sauvegarde des données stockées dans les volumes. (-> utilisation de bucket S3 pour la sauvegarde)
- les opérateurs kubernetes liés à des bases de données modernes prennent en charge directement le S3 pour les sauvegardes et restauration. Par exemple, cf l'opérateur cnpg (postgresql https://cloudnative-pg.io/)

Capacité de stockage totale objet estimée type S3 en Go
Indiquer ici votre estimation gobale en terme de besoin de volume bloc (en gigas).
Notes : Le stockage bloc est répliqué entre les DC.
Les buckets livrés sont affiliés par niveau de classification de la donnée et type d'environnement.

Options associées au stockage S3
le Service S3 offre plusieurs options qui peuvent être utiles pour votre projet. Cela dépend de l'architecture du logiciel, de la stratégie de backup etc...
- La synchronisation entre les régions permet de mettre en place un plan de continuité d'activité
- le versioning peux être une option à activer par une application gérant des documents en versions. (tableur type grist, etc...)

Cochez la mention applicable, plusieurs valeurs possibles
- [ ] Synchronisation entre les régions
- [ ] Versionning

Exposition réseau de votre application

Vous préciserez lors du dialogue d'instruction les urls pressenties pour l'exposition. Bien préciser la matrice de flux cela dans votre DAG/T. Anticipez vos demande, la mise en oeuvre pouvant prendre jusqu'a quelques semaines. A l'issue de l'instruction, vous recevrez une planification estimative de réalisation.
A titre informatif, le délai moyen est de 4 à 6 semaines selon la complexité de votre SI et hors période de forte demande.

Exposition réseau envisagée
L'exposition via un lien RIE dédié nécessite une étude avec vos ingénieurs ministériels.

Cochez la mention applicable, plusieurs valeurs possibles
- ☐ Exposition Internet (prévoir un CDN externe)
- ☐ Exposition MIOM
- ☐ Exposition RIE interministérielle
- ☐ Exposition RIE via VRF (lien spécifique) dédiée

Informations complémentaires nous permettant de mieux prendre en compte votre demande et établir la convention.
Toute information pour aider à bien comprendre votre besoin, votre calendrier, etc...
Note : nous pouvons fournir des postes d'administration à distance si vous n'en disposez pas. (indispensable si l'équipe est localisée hors miom) Précisez ce point ici.

Je comprend que l'offre est proposée en version Béta
Les services proposés sont en version Béta. L'offre Cloud Pi Native est en constante amélioration.
La primo convention tarifaire qui sera établie et validée par les 2 parties, est susceptible d'être révisée sous une période d'un an.

Cochez la mention applicable
- ☐ Oui
- ☐ Non

Financement / Code d'imputation
Pour établir la convention, indiquerez si votre budget est déjà pré-identifié auprès de votre programme financeur. Pour les usagers du ministère de l'Intérieur, s'il s'agit du P216, veuillez
reporter le n° de ligne PEC correspondante. Si aucun budget n'est déjà pré-identifié, merci de mentionner ce qui est envisagé.

Nom du service métier qui porte l'initiative
Cette information sera utilisée pour l'établissement de la convention et également pour mettre à jour le référentiel applicatif (CANEL) sur les aspects organisation et dans la console pour donner les droits de visualisation des vulnérabilités au responsable SSI de l'organisation.
Prendre les informations issues de votre annuaire ministérielle. format souhaité : SG/DLPAJ, attention à l'orthographe.

Pièce justificative à joindre en complément du dossier
- ☐ Dossier d'architecture

Joindre ici le dossier facilite le traitement de la demande. Si vous êtes à l'étape initale de votre projet transmettez un schéma d'architecture en format courant (draw.io, ppt, pdf) décrivant à minima les accès réseaux de votre SI et la structure interne pressentie.

Votre schéma devra reprendre à minima les blocs du socle d'infrastructure : (voir cct)

https://github.com/cloud-pi-native/cct-cloud-native/blob/main/cct-cloud-native.md#mod%C3%A8le-dint%C3%A9gration-dune-application-dans-le-cadre-cloud-native

Accès à la console Cloud Pi Native - Hébergement Application (Béta)

Si vous n'avez pas encore réalisé de schéma vous pouvez utiliser le lien suivant qui ouvre une fenêtre avec un schéma type sur Draw.io. Cela vous permet de disposer d'un exemple à adapter.
note : l'accès au lien peut être limité par votre FW d'entreprise.
https://app.diagrams.net/?url=https%3A%2F%2Fraw.githubusercontent.com%2Fcloud-pi-native%2Fcct-cloud-native%2Fmain%2FDAG-exemple.drawio

La fourniture du DAG / DAT finalisé sera nécessaire pour la mise en service.

Pièce justificative à joindre en complément du dossier

☐ Matrice des flux réseaul

Joindre ici la matrice des flux nécessaire pour votre application par exemple si votre DAG/DAT n'est pas initialisé. Cette information est indispensable pour établir les besoins d'exposition réseau de votre application et la mise en oeuvre des interfaçages spécifiques éventuels. Vous êtes responsable de vérifier l'exactitude de votre demande. Certaines informations peuvent renseignées par le service de mise en hébergement tel que les IP de votre cluster (les "FIP") .
L'utilisation du template suivant est recommandé (version béta) : https://github.com/cloud-pi-native/cct-cloud-native/raw/main/matrice-des-flux-generique-pour-client_master.xlsx

Informations techniques complémentaires

Toutes informations utiles pour aider à la compréhension de votre architecture.

Pièce justificative à joindre en complément du dossier

☐ autre document utile au traitement de la demande