### **Title: Technical Architecture Document for IRP APPLICATIONS Hub**

#### **I. Introduction**

* Brief overview of the purpose and scope of the technical architecture document.

#### **II. Azure Subscriptions Overview**

* Explanation of the three subscriptions: IRP APPLICATIONS HUB, IRP APPLICATIONS NonProd, and IRP APPLICATIONS PROD.

#### **III. Architecture Components**

**A. Hub d'Applications IRP**

**2. Registre de Conteneurs Azure (Azure Container Registry - ACR)**

**Objectif :** Le Registre de Conteneurs Azure (ACR) avec le nom acrappshub001 est un service de stockage de conteneurs basé sur Azure. Son objectif principal est de stocker, gérer et organiser les images des conteneurs Docker utilisées par les applications déployées dans l'environnement Azure.

**Role dans architecture:**

* **Stockage d'Images de Conteneurs :** L'ACR stocke les images des conteneurs Docker, offrant un référentiel centralisé pour les applications utilisant des conteneurs.
* **Gestion des Images :** Il permet la gestion, le versioning et la sécurisation des images des conteneurs, facilitant ainsi le déploiement d'applications cohérentes et fiables.

**Détails de Mise en Œuvre :**

* **Groupe de Resources:** rg-apps-security-shared-001
* **Localisation :** France centrale
* **Abonnement:** Hub applications IRP
* **Nom:** acrappshub001

**Rôle dans l'Architecture Globale :** Le Registre de Conteneurs Azure (ACR) joue un rôle central dans l'environnement cloud, facilitant le déploiement et la gestion des applications basées sur des conteneurs. Il assure également la sécurité et la cohérence des images de conteneurs utilisées par les différentes parties de l'architecture.

**3. Instances de Conteneurs Azure (Azure Container Instances - ACI)**

**Objectif :** Les Instances de Conteneurs Azure (ACI), avec le nom cin-apps-devops-agent-001, sont utilisées pour héberger des agents auto-hébergés permettant le déploiement de ressources dans un point de terminaison privé. Ces instances sont configurées pour déployer des ressources en utilisant des images stockées dans le registre de conteneurs Azure décrit précédemment.

**Rôle dans architecture:**

* **Hébergement des Agents Auto-hébergés :** Les ACI servent de plateforme pour héberger des agents auto-hébergés, facilitant le déploiement de ressources dans un environnement sécurisé via des points de terminaison privés.
* **Utilisation d'Images Stockées :** Elles utilisent les images stockées dans le registre de conteneurs Azure pour le déploiement des ressources.

**Détails de Mise en Œuvre :**

* **Groupe de Ressources :** rg-apps-security-shared-001
* **Localisation :** France centrale
* **Abonnement:** Hub d'Applications IRP
* **Nom : cin-apps-devops-agent-001**

**Rôle dans l'Architecture Globale :** Les Instances de Conteneurs Azure (ACI) hébergeant les agents auto-hébergés ont un rôle crucial dans le processus de déploiement. Elles garantissent un déploiement sécurisé des ressources via des points de terminaison privés, en utilisant les images stockées dans le registre de conteneurs Azure.

**4. Espace de Travail Log Analytics (Log Analytics Workspace)**

**Objectif :** L'Espace de Travail Log Analytics avec le nom log-apps-nonprod-001 est une ressource Azure conçue pour recueillir, stocker et analyser les données de journalisation et de diagnostic générées par les applications et les ressources déployées dans l'environnement non productif.

**Rôle dans architecture:**

* **Centralisation des Données de Journalisation :** L'Espace de Travail Log Analytics centralise les données de journalisation provenant des applications et des services, permettant une analyse approfondie des performances et de la santé du système.
* **Configuration des Paramètres de Diagnostic :** Il contient les paramètres de diagnostic nécessaires pour collecter les journaux et les métriques des applications connectées.

**Détails de Mise en Œuvre :**

* **Groupe de Ressources :** rg-apps-monitoring-nonprod-001
* **Localisation :** France centrale
* **Abonnement:** Hub d'Applications IRP
* **Nom:** log-apps-nonprod-001

**Rôle dans l'Architecture Globale :** L'Espace de Travail Log Analytics est essentiel pour surveiller, analyser et diagnostiquer les performances et le comportement des applications connectées dans l'environnement non productif, offrant ainsi des informations cruciales pour l'optimisation et la résolution des problèmes.

**Utilisations Préconisées:**

* **Analyse des Performances :** Utiliser les données de journalisation pour surveiller les performances et la santé des applications.
* **Diagnostic et Résolution des Problèmes :** Utiliser les informations collectées pour diagnostiquer et résoudre les problèmes potentiels.

**5. Application Insights**

**Objectif :** Application Insights avec le nom appi-apps-nonprod-hub est un service Azure conçu pour surveiller et visualiser les performances des applications web connectées à l'environnement non productif.

**Rôle dans l'Architecture :**

* **Surveillance des Performances :** Application Insights collecte les données de télémétrie pour surveiller et analyser les performances des applications web.
* **Intégration avec les Applications Web :** Il est intégré aux applications web telles que web-app-apps-outil-get-interne-nonprod et web-app-apps-tarificateur-nonprod pour collecter des données de télémétrie.

**Détails de Mise en Œuvre :**

* **Groupe de Ressources :** rg-apps-monitoring-nonprod-001
* **Localisation:** France centrale
* **Abonnement:** Hub d'Applications IRP
* **Nom:** appi-apps-nonprod-hub

**Rôle dans l'Architecture Globale :** Application Insights offre une visibilité approfondie sur les performances des applications web, permettant de détecter les goulots d'étranglement et d'optimiser les fonctionnalités pour une meilleure expérience utilisateur.

**Utilisations Préconisées:**

* **Surveillance des Performances :** Utiliser les données de télémétrie pour analyser les performances des applications web et détecter les problèmes potentiels.
* **Optimisation des Applications :** Utiliser les informations recueillies pour améliorer les fonctionnalités et l'expérience utilisateur des applications web.

**6. Zones DNS Privées (Private DNS Zone)**

**Objectif :** Les Zones DNS Privées, comprenant les domaines privatelink.azurewebsites.net, privatelink.database.windows.net et privatelink.vaultcore.azure.net, sont des ressources partagées utilisées pour configurer les points de terminaison privés des ressources dans les environnements non productifs (nonprod) et productifs (prod). Elles sont liées aux réseaux virtuels (VNets) vnet-apps-hub-shared-frace-001 dans l'abonnement du hub, vnet-apps-nonprod-frace-001 (abonnement non prod) et vnet-apps-prod-frace-001 (abonnement prod).

**Rôle dans l'Architecture :**

* **Configuration des Points de Terminaison Privés :** Les Zones DNS Privées sont utilisées pour configurer les points de terminaison privés des ressources Azure, telles que les applications web, les bases de données et les coffres de clés.
* **Liens avec les Réseaux Virtuels :** Elles sont associées aux réseaux virtuels spécifiques pour permettre la résolution des noms DNS et faciliter la connectivité via ExpressRoute.

**Détails de Mise en Œuvre :**

* **Groupe de Ressources :** rg-apps-security-shared-001
* **Localisation :** Globale
* **Abonnement :** Hub d'Applications IRP

**Rôle dans l'Architecture Globale :** Les Zones DNS Privées jouent un rôle crucial dans la configuration des points de terminaison privés pour les ressources Azure, assurant une connectivité sécurisée et une résolution DNS pour les applications, bases de données et coffres de clés dans les environnements non productifs et productifs.

**Utilisations Préconisées :**

* **Configuration des Points de Terminaison :** Utiliser les Zones DNS Privées pour configurer et gérer les points de terminaison privés des ressources Azure.
* **Résolution DNS pour Connectivité :** Assurer la résolution DNS des noms depuis les serveurs DNS sur site pour permettre la connectivité via ExpressRoute.

**7. Identité Gérée Affectée à l'Utilisateur (User Assigned Managed Identity)**

**Objectif :** L'Identité Gérée affectée à l'utilisateur, associée à la ressource nommée userAssignedIdentityForcontainerGroup, est une entité de sécurité utilisée pour authentifier et autoriser les actions effectuées par les Azure Container Instances (ACI). Elle est spécifiquement liée aux instances de conteneurs hébergeant les agents privés de DevOps.

**Rôle dans l'Architecture :**

* **Authentification et Autorisation :** L'Identité Gérée permet d'authentifier et d'autoriser les actions réalisées par les ACI, notamment les actions de tirage (pull) d'images à partir du registre de conteneurs Azure.
* **Association avec les Instances de Conteneurs :** Elle est associée aux instances de conteneurs hébergeant les agents privés de DevOps, permettant ainsi des opérations sécurisées et contrôlées.

**Détails de Mise en Œuvre :**

* **Groupe de Ressources :** rg-apps-security-shared-001
* **Localisation :** France centrale
* **Abonnement :** Hub d'Applications IRP

**Rôle dans l'Architecture Globale :** L'Identité Gérée affectée à l'utilisateur garantit une authentification et une autorisation sécurisées pour les opérations effectuées par les instances de conteneurs, en particulier les actions liées au tirage d'images depuis le registre de conteneurs Azure.

**Utilisations Préconisées:**

* **Contrôle d'Accès :** Utiliser cette identité pour contrôler et restreindre l'accès aux actions spécifiques des instances de conteneurs.
* **Sécurisation des Opérations :** Garantir des opérations sécurisées et autorisées, notamment pour le tirage d'images depuis le registre de conteneurs.

**A. NON PROD d'Applications IRP**

### 5. Components in IRP APPLICATIONS PROD

* Similarly, list and describe each resource in the PROD subscription.
* Draw comparisons/differences from the NONPROD environment and highlight any additional resources or changes.

### 6. Architecture Diagram

* Provide a visual representation of how these resources are connected within each environment and how the environments relate to each other.

### 7. Best Practices and Recommendations

* General best practices for managing Azure resources.
* Recommendations for optimizing resource usage, improving security, scalability, etc.

### 8. Conclusion

* Recap the main points covered in the document.
* Any future plans or considerations for the architecture.

### 9. References

* Links to official Azure documentation, guidelines, or any other external resources used in the document.

1. **App Service - web-app-apps-outil-ged-interne-nonprod-001**

**2. App Service - web-app-apps-outil-ged-interne-nonprod-001**

1. **Objectif :** Le service web "web-app-apps-outil-ged-interne-nonprod-001" est une application hébergée dans l'environnement de non-production du cadre IRP APPLICATIONS NonProd. Son objectif principal est de fournir une plateforme pour l'outil de gestion électronique de documents interne.
2. **Role dans l'architecture :** • **Hébergement d'Applications :** Le service web héberge et exécute l'outil de gestion électronique de documents interne pour les utilisateurs et les processus métier. • **Plateforme de Gestion de Documents :** Il sert de plateforme centrale pour la gestion, le stockage et la manipulation de documents internes, offrant des fonctionnalités pour les utilisateurs autorisés.
3. **Détails de Mise en Œuvre :** • **Groupe de ressources :** rg-apps-outil-ged-interne-nonprod-001 • **Localisation :** France Centrale • **Abonnement :** IRP APPLICATIONS NonProd • **Nom :** web-app-apps-outil-ged-interne-nonprod-001
4. **Rôle dans l'Architecture Globale :** Le service web "web-app-apps-outil-ged-interne-nonprod-001" joue un rôle essentiel en fournissant une plateforme sécurisée et dédiée à la gestion électronique de documents dans l'environnement non-production. Il contribue à la mise à disposition d'outils de productivité, tout en maintenant la sécurité et la disponibilité des documents pour les utilisateurs autorisés.

**CDN Profile "cdn-apps-nonprod"**

**Description :**  
Le CDN (Content Delivery Network) "cdn-apps-nonprod" fait partie des ressources du groupe de ressources "rg-apps-cdn-nonprod-001", situé dans la région "West Europe", sous l'abonnement "IRP APPLICATIONS NonProd".

Ce profil CDN est une configuration clé dans Azure CDN, regroupant plusieurs endpoints CDN, des règles de mise en cache, et d'autres paramètres qui définissent la manière dont le contenu est distribué aux utilisateurs. Il est probable que le CDN "cdn-apps-nonprod" contienne diverses configurations pour les endpoints CDN associés, et contrôle le comportement de la diffusion de contenu à travers le réseau.

**Objectif :**  
Le profil CDN a pour objectif d'optimiser la diffusion de contenu en mettant en cache de manière stratégique le contenu au niveau des points d'accès les plus proches des utilisateurs finaux. Il vise à améliorer les performances, la scalabilité et la disponibilité des applications web, des sites web, des fichiers multimédias, et autres contenus en réduisant la latence et les temps de chargement.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, le profil CDN joue un rôle crucial en améliorant la diffusion de contenu en le mettant en cache et en le distribuant efficacement à travers les points d'accès CDN. Cela réduit la charge sur le serveur d'origine et améliore l'expérience utilisateur en assurant une diffusion de contenu plus rapide et fiable.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-cdn-nonprod-001/providers/Microsoft.Cdn/profiles/cdn-apps-nonprod
* **Type :** Profil Front Door et CDN
* **Groupe de Ressources :** rg-apps-cdn-nonprod-001
* **Localisation :** West Europe
* **Abonnement :** IRP APPLICATIONS NonProd

Ce profil CDN contient plusieurs configurations clés telles que des règles de mise en cache, des paramètres d'origine, des réglages de performances, des règles de sécurité, ainsi que des configurations de surveillance et d'analyse du trafic pour optimiser la diffusion de contenu et améliorer les performances globales des applications.

**Key Vault "kv-apps-nonprod-001"**

**Description :**  
Le Key Vault "kv-apps-nonprod-001" est situé dans le groupe de ressources "rg-apps-security-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Un Key Vault est un service Azure qui permet de stocker et de gérer des secrets, des certificats et des clés d'authentification. Il offre un stockage sécurisé et centralisé pour les informations sensibles, garantissant leur protection et leur utilisation sécurisée par les applications.

**Objectif :**  
Ce Key Vault a pour objectif principal de sécuriser et de gérer les informations sensibles telles que les secrets, les certificats, et les clés utilisées par les différentes applications et services au sein de l'environnement "IRP APPLICATIONS NonProd". Il assure la confidentialité et la gestion sécurisée des données sensibles.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, le Key Vault joue un rôle crucial en tant que coffre-fort sécurisé pour stocker et gérer les secrets, les certificats et les clés d'authentification. Il fournit un point centralisé pour la gestion des informations sensibles, assurant leur sécurisation et leur disponibilité pour les applications autorisées.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-security-nonprod-001/providers/Microsoft.KeyVault/vaults/kv-apps-nonprod-001
* **Type :** Key Vault
* **Groupe de Ressources :** rg-apps-security-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

Le Key Vault "kv-apps-nonprod-001" peut contenir des secrets, des certificats et des clés d'authentification nécessaires au fonctionnement sécurisé des applications et des services déployés dans l'environnement "IRP APPLICATIONS NonProd". Il fournit un moyen sécurisé et centralisé pour la gestion et la protection des données sensibles.

**Passerelle NAT (NAT Gateway) "ng-apps-nonprod"**

**Description :**  
La Passerelle NAT "ng-apps-nonprod" est située dans le groupe de ressources "rg-apps-security-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

La Passerelle NAT est un composant d'Azure Network permettant de fournir une connectivité Internet sortante à des ressources hébergées dans un réseau virtuel (VNet) privé. Elle agit comme une passerelle de traduction d'adresses réseau (NAT), permettant aux ressources du VNet d'accéder à Internet tout en masquant leurs adresses IP internes.

**Objectif :**  
La Passerelle NAT "ng-apps-nonprod" vise à permettre aux ressources situées dans le réseau virtuel privé (VNet) de se connecter à Internet de manière sécurisée. Elle garantit une connectivité sortante tout en protégeant les adresses IP internes des ressources.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, la Passerelle NAT joue un rôle essentiel en fournissant une connectivité Internet sortante sécurisée pour les ressources du réseau virtuel privé. Elle assure le masquage des adresses IP internes tout en permettant aux ressources d'accéder à Internet de manière sécurisée.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-security-nonprod-001/providers/Microsoft.Network/natGateways/ng-apps-nonprod
* **Type :** NAT Gateway
* **Groupe de Ressources :** rg-apps-security-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

La Passerelle NAT "ng-apps-nonprod" facilite la connectivité sortante sécurisée des ressources situées dans le réseau virtuel privé vers Internet tout en préservant la confidentialité des adresses IP internes. Elle est essentielle pour les opérations nécessitant un accès à des ressources externes tout en assurant la sécurité du réseau privé.

### **Réseau Virtuel (Virtual Network) "vnet-apps-nonprod-frace-001"**

**Description :**  
Le Réseau Virtuel "vnet-apps-nonprod-frace-001" est situé dans le groupe de ressources "rg-apps-security-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Le Réseau Virtuel (VNet) est une ressource Azure qui permet d'isoler et de connecter les ressources cloud de manière sécurisée, simulant un réseau local dans le cloud.

**Objectif :**  
Le VNet "vnet-apps-nonprod-frace-001" vise à fournir un environnement réseau sécurisé et isolé pour les ressources hébergées dans l'environnement Azure NonProd. Il permet de segmenter les ressources et de gérer leur connectivité de manière centralisée.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, le Réseau Virtuel joue un rôle fondamental en permettant l'isolation des ressources, la définition de sous-réseaux, et le contrôle des communications entre les différentes ressources au sein de l'environnement "IRP APPLICATIONS NonProd". Il offre également des options de connectivité avec d'autres réseaux virtuels ou locaux.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-security-nonprod-001/providers/Microsoft.Network/virtualNetworks/vnet-apps-nonprod-frace-001
* **Type :** Virtual network
* **Groupe de Ressources :** rg-apps-security-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

Le Réseau Virtuel "vnet-apps-nonprod-frace-001" garantit un environnement réseau sécurisé, isolé et hautement configurable pour les ressources hébergées dans l'environnement Azure NonProd, facilitant la gestion des communications et la sécurité des données.

### **Groupe de Sécurité Réseau (Network Security Group - NSG) "nsg-apps-backend-nonprod-001" et "nsg-apps-frontend-nonprod-001"**

**Description :**  
Les Groupes de Sécurité Réseau "nsg-apps-backend-nonprod-001" et "nsg-apps-frontend-nonprod-001" sont situés dans le groupe de ressources "rg-apps-security-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Les NSG sont des pare-feu virtuels permettant de contrôler le trafic réseau entrant et sortant des ressources Azure basé sur des règles de sécurité.

**Objectif :**  
Les NSG "nsg-apps-backend-nonprod-001" et "nsg-apps-frontend-nonprod-001" visent à sécuriser le trafic réseau en appliquant des règles de sécurité spécifiques pour les ressources Backend et Frontend hébergées dans l'environnement Azure NonProd.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, les Groupes de Sécurité Réseau jouent un rôle crucial en filtrant et en contrôlant le trafic réseau des ressources Backend et Frontend. Ils permettent de spécifier des règles de sécurité pour autoriser ou bloquer le trafic en fonction des besoins de sécurité.

**Détails de Mise en Œuvre :**

* **Resource ID (Backend) :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-security-nonprod-001/providers/Microsoft.Network/networkSecurityGroups/nsg-apps-backend-nonprod-001
* **Resource ID (Frontend) :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-security-nonprod-001/providers/Microsoft.Network/networkSecurityGroups/nsg-apps-frontend-nonprod-001
* **Type :** Network security group
* **Groupe de Ressources :** rg-apps-security-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

Les NSG "nsg-apps-backend-nonprod-001" et "nsg-apps-frontend-nonprod-001" permettent d'appliquer des règles de sécurité personnalisées pour contrôler et sécuriser le trafic réseau entrant et sortant des ressources Backend et Frontend dans l'environnement Azure NonProd.

### **Serveur SQL (SQL Server) "sql-apps-nonprod-001"**

**Description :**  
Le Serveur SQL "sql-apps-nonprod-001" est localisé dans le groupe de ressources "rg-apps-data-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Le serveur SQL est un service de base de données relationnelles géré par Azure qui héberge plusieurs bases de données SQL.

**Objectif :**  
Le serveur SQL "sql-apps-nonprod-001" a pour objectif de gérer et d'héberger des bases de données SQL pour les applications déployées dans l'environnement Azure NonProd.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, le Serveur SQL joue un rôle central en hébergeant et en gérant plusieurs bases de données SQL critiques pour les applications. Il offre un environnement fiable et sécurisé pour stocker et gérer les données.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-data-nonprod-001/providers/Microsoft.Sql/servers/sql-apps-nonprod-001
* **Type :** SQL server
* **Groupe de Ressources :** rg-apps-data-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

Le Serveur SQL "sql-apps-nonprod-001" est la plaque tournante des opérations de base de données dans l'environnement Azure NonProd, offrant une infrastructure robuste pour stocker et gérer les données de manière sécurisée.

### **Bases de Données SQL "sqldb-apps-outil-ged-nonprod", "sqldb-apps-requeteur-metier-nonprod" et "sqldb-apps-tarificateur-nonprod"**

**Description :**  
Les Bases de Données SQL "sqldb-apps-outil-ged-nonprod", "sqldb-apps-requeteur-metier-nonprod" et "sqldb-apps-tarificateur-nonprod" sont hébergées sur le Serveur SQL "sql-apps-nonprod-001". Elles se trouvent dans le groupe de ressources "rg-apps-data-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Les bases de données SQL stockent et gèrent les données spécifiques à chaque application.

**Objectif :**  
Les bases de données SQL servent à stocker et gérer les données des applications spécifiques, telles que les données des outils GED, des requêteurs métier et des tarificateurs dans l'environnement Azure NonProd.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, chaque base de données SQL contient des données spécifiques à une application. Elles stockent des informations critiques utilisées par ces applications, offrant un accès sécurisé et structuré aux données.

**Détails de Mise en Œuvre :**

* **Resource ID (Outil GED) :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-data-nonprod-001/providers/Microsoft.Sql/servers/sql-apps-nonprod-001/databases/sqldb-apps-outil-ged-nonprod
* **Resource ID (Requêteur Métier) :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-data-nonprod-001/providers/Microsoft.Sql/servers/sql-apps-nonprod-001/databases/sqldb-apps-requeteur-metier-nonprod
* **Resource ID (Tarificateur) :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-data-nonprod-001/providers/Microsoft.Sql/servers/sql-apps-nonprod-001/databases/sqldb-apps-tarificateur-nonprod
* **Type :** SQL database
* **Groupe de Ressources :** rg-apps-data-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

Les bases de données SQL "sqldb-apps-outil-ged-nonprod", "sqldb-apps-requeteur-metier-nonprod" et "sqldb-apps-tarificateur-nonprod" jouent un rôle crucial en stockant et en gérant les données spécifiques à chaque application, fournissant ainsi un accès sécurisé et structuré aux données essentielles des applications dans l'environnement Azure NonProd.

### **Compte de Stockage "stappscdnnonprod001"**

**Description :**  
Le Compte de Stockage "stappscdnnonprod001" est localisé dans le groupe de ressources "rg-apps-cdn-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Ce compte de stockage est un service Azure qui fournit un espace de stockage sécurisé et évolutif pour divers types de données et d'objets.

**Objectif :**  
Le Compte de Stockage "stappscdnnonprod001" vise à stocker et à gérer les données associées au contenu diffusé via le CDN dans l'environnement Azure NonProd.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, ce compte de stockage joue un rôle clé en fournissant un espace de stockage fiable et sécurisé pour le contenu du CDN. Il stocke des données telles que des images, des vidéos ou d'autres éléments multimédias diffusés via le réseau de diffusion de contenu.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-cdn-nonprod-001/providers/Microsoft.Storage/storageAccounts/stappscdnnonprod001
* **Type :** Storage account
* **Groupe de Ressources :** rg-apps-cdn-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

Le Compte de Stockage "stappscdnnonprod001" constitue une pièce essentielle pour stocker le contenu diffusé via le CDN dans l'environnement Azure NonProd, offrant une solution de stockage fiable et sécurisée pour les objets multimédias et autres fichiers utilisés pour la diffusion de contenu.

### **Passerelle de Réseau Virtuel "vgw-apps-vnet-nonprod-frace-001"**

**Description :**  
La Passerelle de Réseau Virtuel "vgw-apps-vnet-nonprod-frace-001" se trouve dans le groupe de ressources "rg-apps-security-nonprod-001" de la région "France Central", sous l'abonnement "IRP APPLICATIONS NonProd".

Cette passerelle de réseau virtuel permet l'accès sécurisé et le routage du trafic réseau entre les réseaux locaux ou on-premises et le réseau virtuel dans Azure NonProd.

**Objectif :**  
La Passerelle de Réseau Virtuel "vgw-apps-vnet-nonprod-frace-001" a pour objectif de fournir une connectivité sécurisée et fiable entre le réseau virtuel NonProd dans Azure et les réseaux locaux/on-premises.

**Rôle dans l'Architecture :**  
Dans l'architecture globale, cette passerelle joue un rôle crucial en facilitant la connectivité sécurisée entre les ressources Azure NonProd et les réseaux locaux. Elle assure un passage sécurisé pour le trafic réseau, permettant une communication fiable entre ces différentes infrastructures.

**Détails de Mise en Œuvre :**

* **Resource ID :** /subscriptions/{subscriptionid}/resourceGroups/rg-apps-security-nonprod-001/providers/Microsoft.Network/virtualNetworkGateways/vgw-apps-vnet-nonprod-frace-001
* **Type :** Virtual network gateway
* **Groupe de Ressources :** rg-apps-security-nonprod-001
* **Localisation :** France Central
* **Abonnement :** IRP APPLICATIONS NonProd

La Passerelle de Réseau Virtuel "vgw-apps-vnet-nonprod-frace-001" est essentielle pour établir une connectivité sécurisée entre le réseau virtuel Azure NonProd et les réseaux locaux/on-premises, facilitant ainsi la communication entre ces environnements distincts.

### **Private Endpoints dans Azure**

#### **Description :**

Les Private Endpoints sont des entités Azure qui permettent de connecter de manière sécurisée des services Azure (comme les PaaS - Platform as a Service) à un réseau virtuel de manière privée. Ils fournissent une adresse IP privée sur le réseau virtuel, permettant aux ressources du réseau virtuel d'accéder aux services Azure de manière sécurisée sans exposer ces services publiquement sur Internet.

#### **Fonctionnement :**

1. **Connectivité privée** : Les Private Endpoints fournissent un point de terminaison privé dans le réseau virtuel d'un abonné Azure.
2. **Liens avec des Services Azure** : Ils sont associés à des services Azure spécifiques tels que Azure Storage, Azure SQL Database, Azure Cosmos DB, etc.
3. **Attribution d'une Adresse IP Privée** : Chaque Private Endpoint est doté d'une adresse IP privée du réseau virtuel, permettant aux ressources du réseau d'accéder aux services associés.
4. **Sécurité accrue** : Ils améliorent la sécurité en restreignant l'accès aux services Azure à travers une connexion privée sans exposer les services sur Internet.

#### **Objectif :**

Les Private Endpoints sont conçus pour sécuriser l'accès aux services Azure en créant un chemin d'accès privé entre les services Azure et un réseau virtuel spécifique. L'objectif principal est de garantir une connectivité sécurisée, restreinte au réseau virtuel, éliminant ainsi la nécessité d'une connectivité publique sur Internet pour accéder à ces services.

#### **Rôle dans l'Architecture Azure :**

Dans l'architecture Azure, les Private Endpoints jouent un rôle crucial en sécurisant les connexions aux services Azure sensibles. Ils permettent de :

* Assurer une connectivité privée entre le réseau virtuel et les services Azure sans exposer les services sur Internet.
* Renforcer la sécurité des données et des applications en réduisant la surface d'attaque.
* Réaliser des configurations de réseau hybrides pour accéder aux services Azure via des réseaux locaux tout en maintenant un niveau élevé de sécurité.

En résumé, les Private Endpoints constituent un élément essentiel pour sécuriser et contrôler l'accès aux services Azure sensibles dans une infrastructure cloud Azure.