

	PROCEDURE 06_Cloud	Date de création : 04/12/25	Nombre de page : 6
		Date de révision : 09/01/26	Version : 1.1
Référence : AZR-STO-CFG	Déploiement du Stockage Blob et Sécurité		

Table des matières

1.	Introduction.....	1
2.	Contexte et Justification	1
3.	Concepts Clés et SKUs	1
3.1.	Type de Comptes	2
3.2.	Redondance.....	2
3.3.	Niveau d'accès	2
4.	Prérequis.....	2
5.	Configuration.....	2
5.1.	Création du Groupe de Ressources Stockage	2
5.2.	Création du Storage Account	3
5.3.	Création d'un Conteneur (Blob).....	4
5.4.	Upload d'un fichier de test	4
5.5.	Sécurisation et Accès temporaire (SAS Token)	4
6.	Vérifications	5
7.	Dépannage	6
8.	Conseils et Bonnes Pratiques	6

1. Introduction

L'objectif est de déployer un espace de stockage sécurisé et résilient pour héberger les fichiers non structurés de **NaCloud Inc** (logs, scripts d'installation, sauvegardes). Nous allons créer un « Compte de Stockage » (Storage Account) et comprendre comment optimiser les coûts grâce aux niveaux d'accès.

2. Contexte et Justification

Contrairement à un disque dur classique attaché à une VM (Block Storage), le stockage Blob (Object Storage) est conçu pour stocker des pétaoctets de données accessibles via HTTP/HTTPS. Pour **NaCloud Inc**, nous ne voulons pas saturer les disques de nos serveurs avec des fichiers logs archivés. Nous allons les décharger vers ce stockage Azure, beaucoup moins cher.

Déploiement du Stockage Blob et Sécurité

3. Concepts Clés et SKUs

3.1. Type de Comptes

General Purpose v2 (GPv2) : Le standard actuel. Supporte tout (Blob, File, Queue, Table). C'est celui qu'il faut choisir par défaut.

Premium Block Blob : Pour les applications nécessitant des temps de latence très faibles (ex: base de données transactionnelle). Coût de stockage plus élevé, coût de transaction plus faible.

3.2. Redondance

C'est la garantie de survie de la donnée.

- **LRS (Locally-redundant storage)** : 3 copies dans le même datacenter. (Le moins cher. Risque : Incendie du datacenter).
- **ZRS (Zone-redundant storage)** : 3 copies réparties dans 3 Zones de Disponibilité (AZ) différentes de la même région. (Risque : Destruction de toute la région, ex: Paris).
- **GRS (Geo-redundant storage)** : Copie les données en LRS dans la région principale (Paris), puis les réplique en LRS dans une région jumelle (ex: Pays-Bas).
- **GZRS (Geo-zone-redundant storage)** : Le top du top. ZRS dans la région principale + LRS dans la région jumelle.

3.3. Niveau d'accès

Hot (Chaud) : Pour les données accédées fréquemment. Coût de stockage élevé, accès gratuit.

Cool (Froid) : Pour les données gardées au moins 30 jours. Stockage moins cher, mais on paie l'accès (lecture/écriture).

Cold (Froid extrême) : Pour les données gardées au moins 90 jours.

Archive : Pour les données gardées au moins 180 jours. Stockage dérisoire, mais la donnée est « hors ligne ». Il faut 15h pour la récupérer (Réhydrations).

4. Prérequis

- 1) Avoir accès à la souscription Azure.
- 2) Nous créerons un nouveau Groupe de Ressources dédié au stockage pour séparer les responsabilités.

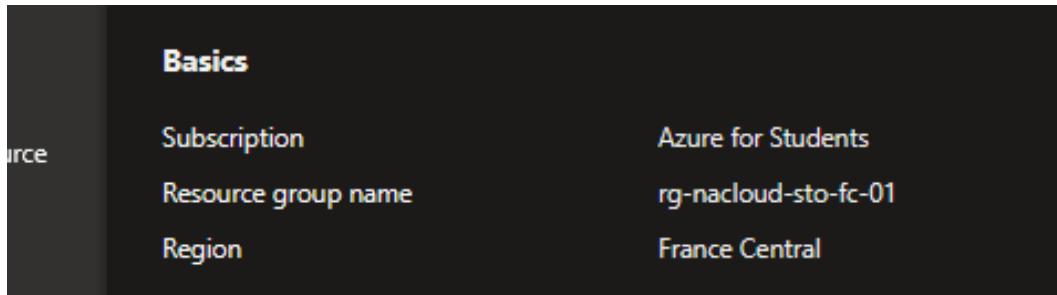
5. Configuration

5.1. Crédit du Groupe de Ressources Stockage

Déploiement du Stockage Blob et Sécurité

Justification : Séparation logique. L'équipe « Data » n'est pas forcément l'équipe « Réseau ».

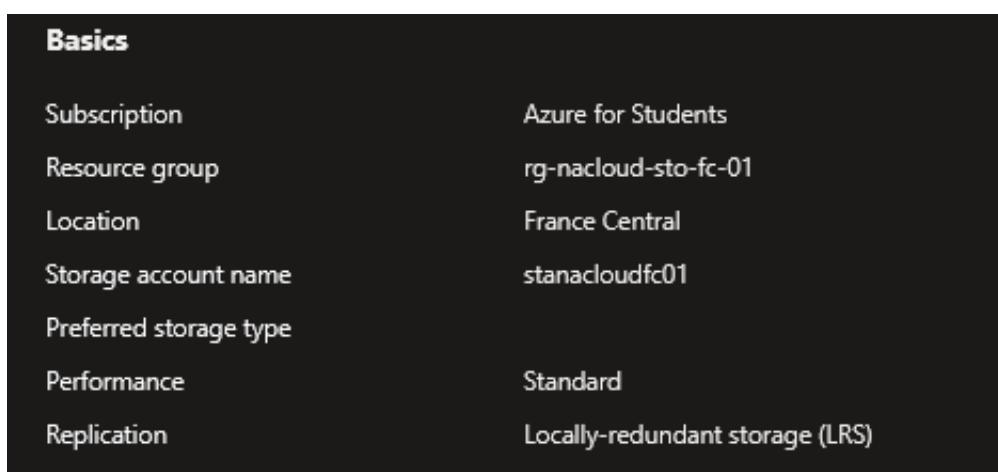
1. Recherchez « Groupes de ressources ».
2. Cliquez sur « Créer ».
 - **Groupe de ressources :** rg-nacloud-sto-fc-01
 - **Région :** France Central.
3. Validez et créez.



5.2. Crédit du Storage Account

Justification : Crédit du conteneur physique du service.

1. Recherchez « Comptes de stockage » (Storage accounts).
2. Cliquez sur « Créer ».
3. **Onglet Base :**
 - **Groupe de ressources :** rg-nacloud-sto-fc-01.
 - **Nom du compte de stockage :** stanacloudfc01.
 - **Région :** France Central.
 - **Performances :** Standard.
 - **Redondance :** Stockage localement redondant (LRS) . (Pour le lab, c'est suffisant et moins cher. En prod, on prendrait ZRS ou GRS).
4. Onglet Avancé :
 - **Niveau d'accès (Access Tier) :** Chaud (Hot).
5. Cliquez sur « Vérifier » puis « Créer ».

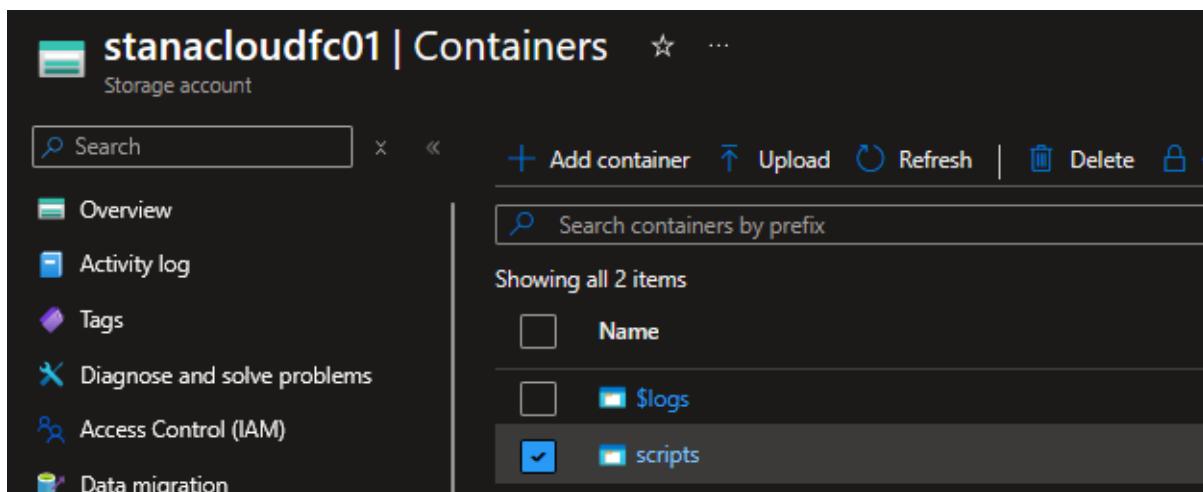


Déploiement du Stockage Blob et Sécurité

5.3. Création d'un Conteneur (Blob)

Justification : Le compte de stockage est comme un disque dur, le conteneur est comme un dossier.

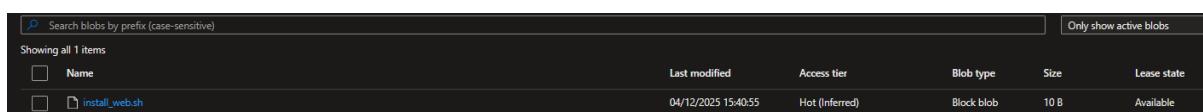
1. Allez sur la ressource stanacloudfc01....
2. Dans le menu de gauche, section « Stockage de données », cliquez sur « Conteneurs ».
3. Cliquez sur « + Conteneur ».
 - **Nom :** scripts.
 - **Niveau d'accès public :** Privé (pas d'accès anonyme). C'est la configuration la plus sécurisée.
4. Cliquez sur « Créer ».



The screenshot shows the 'Containers' page for the storage account 'stanacloudfc01'. On the left, there's a sidebar with links like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), and Data migration. The main area has a search bar at the top. Below it, there's a button to 'Add container', an 'Upload' button, and a 'Refresh' button. A 'Delete' button is also visible. There's also a 'Search containers by prefix' input field. The list shows 'Showing all 2 items': '\$logs' and 'scripts'. The 'scripts' container has a checked checkbox next to its name.

5.4. Upload d'un fichier de test

1. Créez un petit fichier texte sur votre ordinateur nommé install_web.sh (contenu vide ou simple texte « echo Hello »).
2. Entrez dans le conteneur scripts.
3. Cliquez sur « Charger » (Upload).
4. Sélectionnez votre fichier et validez.
5. Le fichier apparaît dans la liste. Regardez la colonne « Niveau d'accès », elle indique « Hot ».



The screenshot shows the 'Blobs' page for the 'scripts' container. At the top, there's a search bar and a 'Only show active blobs' checkbox. Below that, it says 'Showing all 1 items'. There's a table with columns: Name, Last modified, Access tier, Blob type, Size, and Lease state. One item is listed: 'install_web.sh' with a last modified date of '04/12/2025 15:40:55', access tier 'Hot (Inferred)', blob type 'Block blob', size '10 B', and lease state 'Available'.

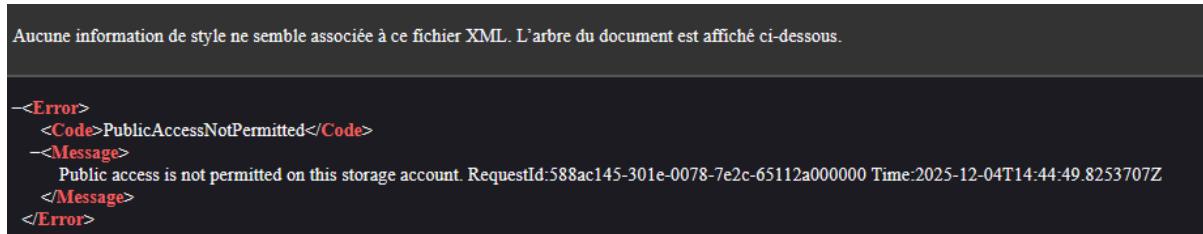
5.5. Sécurisation et Accès temporaire (SAS Token)

Justification : Le fichier est privé. Si vous tentez d'accéder à son URL, vous aurez une erreur. Pour donner un accès temporaire à un consultant externe sans lui créer de compte utilisateur, on utilise une signature d'accès partagé (SAS).

1. Cliquez sur le fichier install_web.sh dans la liste pour voir ses détails.

Déploiement du Stockage Blob et Sécurité

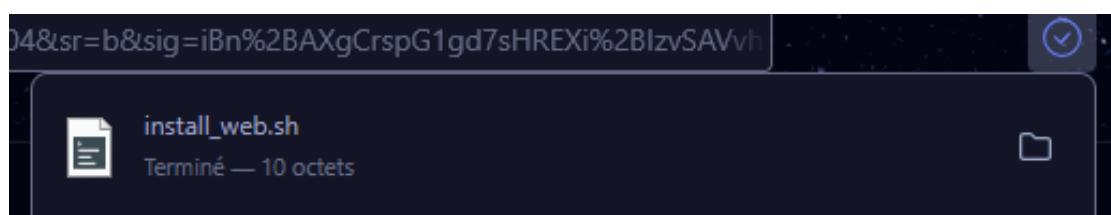
2. Copiez l'URL (ex:
https://stanacloud...blob.core.windows.net/scripts/install_web.sh) et collez-la dans un nouvel onglet de navigateur.
 - **Résultat :** Erreur XML ResourceNotFound ou PublicAccessNotPermitted. C'est normal.



3. Revenez sur le portail, toujours sur le détail du fichier.
4. Cliquez sur l'onglet (à gauche ou en haut selon la version) « Générer SAS ».
 - **Autorisations :** Lecture (Read) uniquement.
 - **Expiration :** Mettez une date de fin à demain.



5. Cliquez sur « Générer un jeton SAS et une URL ».
 6. Copiez le champ « URL SAS Blob ».
 7. Collez cette nouvelle URL dans votre navigateur.
- **Résultat :** Le navigateur télécharge ou affiche le fichier. L'accès est validé par le jeton ajouté à la fin de l'URL



6. Vérifications

Déploiement du Stockage Blob et Sécurité

Vérification de la redondance :

- Sur la page d'accueil du compte de stockage, menu de gauche « Redondance ».
- Vérifiez que « Stockage localement redondant (LRS) » est actif.
- Notez que vous pouvez changer en GRS à chaud ici (mais cela a un coût).

Vérification du Tiering :

- Allez dans le conteneur scripts.
- Sélectionnez le fichier.
- Cliquez sur « Modifier le niveau » (Change tier).
- Passez-le en « Cool ».
- Le statut change immédiatement. C'est ainsi qu'on optimise les coûts manuellement.

7. Dépannage

Erreur de nom de compte :

- Si vous avez une erreur indiquant que le nom est déjà pris, ajoutez plus de chiffres aléatoires à la fin. stanacloud est probablement déjà pris par un autre utilisateur Azure dans le monde.

Accès 403 Forbidden sur le SAS Token :

- Vérifiez les dates du SAS. Attention au fuseau horaire (UTC vs Heure locale). Par précaution, mettez l'heure de début à « hier » pour éviter les soucis de décalage horaire.
- Vérifiez que vous avez bien coché « HTTPS uniquement ».

8. Conseils et Bonnes Pratiques

Cycle de vie (Lifecycle Management) :

- Ne gérez pas les niveaux (Hot/Cool) à la main. Configurez une règle automatique : « Si un fichier n'est pas modifié depuis 30 jours, le passer en Cool. Si 365 jours, le supprimer ». (Menu « Gestion du cycle de vie »).

Sécurité des Clés :

- Un compte de stockage possède deux « Clés d'accès » (Access Keys) qui donnent un accès **Total** (Super Admin) aux données. Ne les utilisez jamais dans vos codes. Utilisez Entra ID (RBAC) ou des SAS Tokens limités.