|  |  |
| --- | --- |
|  | **STANDARD OPERATING PROCEDURE** |
| **SOP Number:** | PROC-001 **Page:12** |
| **Version Number:** | 1.0 |
| **SOP Title:** | **AWS Backup and Restore** |

**1.0 Objectif.**

Le but de cette procédure d’exploitation standard est de fournir les étapes à suivre pour créer le plan de sauvegarde natif AWS centralisé et pour ajouter un nouveau compte OU/fonctionnel ou les instances des systèmes d’exploitation linux et Windows dans le plan de sauvegarde approprie et pour restaurer la sauvegarde dans le paysage AWS.

**2. Portée**

|  |  |
| --- | --- |
| **Régions,**  **Domaines fonctionnels,**  **Fonctions de travail**. | Cette SOP s'applique à,  • Régions : mondiales  • Domaine fonctionnel : technologie informatique  • Fonctions professionnelles : personnel prenant en charge les activités de sauvegarde et de restauration dans le cadre de ce document |
| **Applications** | Cette SOP s'applique à,  • Instances Linux Amazon Elastic Compute Cloud (EC2)  • Instances Windows Amazon Elastic Compute Cloud (EC2) |

**3.0 DÉLÉGATION D'ACTIVITÉS**

Les activités requises pour exécuter cette SOP peuvent être déléguées à une personne ayant l'éducation, l'expérience et la formation appropriées pour exécuter l'activité avec succès. La partie responsable conserve l'entière responsabilité du résultat de toute activité déléguée.

**4.0 RESPONSABILITÉS ET PROCÉDURE**

SHQ utilisera AWS Backup comme outil de gestion de la sauvegarde et de la restauration pour les instances EC2 Windows et EC2 Linux. Pendant la phase de construction, les instances EC2 sont ajoutées à la politique de sauvegarde.

La vérification périodique de la sauvegarde et de la restauration, y compris les tests de restauration semestriels, fera partie du processus d'examen périodique global de Landing Zone.

**4.1 CRÉATION D'UN PLAN DE SAUVEGARDE / CONVENTION DE NOMMAGE**

|  |  |
| --- | --- |
| **Rôle responsable** | **Activité** |
| **Cloud Operations Engineer** | • Créez un rôle IAM pour AWS Backup pour assumer et effectuer des opérations de sauvegarde et de restauration à l'aide du modèle de Cloud Formation Template à **l'annexe 4.**  • Créez une Backup Policy, un Backup plan et un backup rules conformément **aux annexes 1 et 2**.  • Ajoutez des cibles au Backup Policy conformément à **l'annexe 3.** |

**4.2. ON-DEMAND BACKUP**

|  |  |
| --- | --- |
| **Rôle responsable** | **Activité** |
| Application Owner | Créez un ticket en utilisant <Nom de l'outil de ticket et URL du catalogue de services pour ouvrir la demande de sauvegarde> |
| Cloud Operations Engineer | • Examinez et vérifiez la demande.  • Créer la sauvegarde à la demande avec la rétention demandée conformément à **l'annexe 5** |

**4.3. PROCESSUS DE RESTAURATION**

|  |  |
| --- | --- |
| **Rôle responsable** | **Activité** |
| Application Owner | Créer un ticket <nom de l'outil de ticket> pour la restauration |
| Cloud Operations Engineer | • Examinez et vérifiez la demande.  • Créez la restauration à la demande avec l'ID d'instance demandé conformément à **l'annexe 6.**  • Vérifiez que l'instance restaurée est accessible via AWS Console/SSM et Okta ASA  • Informez le propriétaire de l'application pour vérifier et confirmer. |
| Application Owner | • Vérifiez la connectivité à la ressource restaurée  • Vérifiez que l'application fonctionne comme prévu  • Confirmer le statut à l'ingénieur CloudOps |
| Cloud Operations Engineer | Signaler <nom de l'outil de ticket> le statut et fermer le ticket |

**4.4. DELETE BACKUP PLAN**

|  |  |
| --- | --- |
| **Rôle responsable** | **Activité** |
| Cloud Operations Engineer | Créez <nom de l'outil de ticket> la requête de suppression du Backup plan |
| Change Approver | Examiner et approuver la demande de suppression |
| Cloud Operations Engineer | • Supprimer le Backup plan conformément à **l'annexe 7** une fois la demande de suppression approuvée.  • Signaler le statut et fermer le ticket |

**4.5. SURVEILLANCE DES SAUVEGARDES ET RAPPORTS**

|  |  |
| --- | --- |
| **Rôle responsable** | **Activité** |
| Cloud Operations Engineer | Surveillez les Backup jobs ayant échoué avec les métriques Cloud Watch/SNS topic conformément à **l'annexe 8.** |
| Cloud Operations Engineer | Examinez quotidiennement les rapports de sauvegarde stockés sur la console AWS et effectuez les actions appropriées telles que la nouvelle soumission des sauvegardes. |
| Cloud Operations Engineer | • Vérifiez l'état de la sauvegarde sur le tableau de bord du service de sauvegarde AWS.  • Créez un ticket d'incident <nom de l'outil de ticket> pour l'échec de la sauvegarde dans Gestion des services informatiques (ITSM) - Gestion des incidents. |
| Cloud Operations Engineer | Partagez un rapport de sauvegarde hebdomadaire avec le responsable des opérations ECS. |

**4.6. VÉRIFICATION PÉRIODIQUE POUR LA RESTAURATION**

|  |  |
| --- | --- |
| **Rôle responsable** | **Activité** |
| Cloud Operations Engineer | Effectuez une vérification semestrielle des sauvegardes et des restaurations dans l'environnement SHQ, dans le cadre de la vérification périodique.  • Créer un ticket pour les tests de restauration  • Les applications sont choisies dans chaque région AWS. Seuls les environnements non PROD seront utilisés pour effectuer les tests |
|  | • En cas d'échec, l'exécution du test échouera et le défaut sera enregistré  <Outil de billetterie>.  • Un dépannage sera effectué pour identifier la raison de l'échec.  • Pour tout problème dans le processus/l'outil AWS Backup ou au niveau de l'application, l'incident sera consigné. AWS sera engagé pour les problèmes dans l'outil, si nécessaire. |

**4.7. SUPPORT DE SAUVEGARDE**

La sauvegarde des supports utilisés pour stocker les sauvegardes est gérée par AWS et a été examinée dans le cadre du fournisseur AWS

# 5.0 REVISION HISTORY

|  |  |  |
| --- | --- | --- |
| Version | Date effective | Description des changements |
| 1.0 | Actuelle | Version initiale |
| 2.0 |  |  |

# 6.0 ANNEXES

|  |  |
| --- | --- |
| 1. | Annexe 1: Calendrier de sauvegarde |
| 2. | Annexe 2 : Création d'une politique de sauvegarde |
| 3. | Annexe 3 : Attacher des cibles à la politique de sauvegarde |
| 4. | Annexe 4 : Rôle IAM pour AWS Backup |
| 5. | Annexe 5 : Étapes pour créer une sauvegarde à la demande |
| 6. | Annexe 6 : Étapes pour restaurer une sauvegarde |
| 7. | Annexe 7 : Étapes pour supprimer le plan de sauvegarde |
| 8. | Annexe 8 : Étapes pour surveiller la sauvegarde |

**ANNEXE 1: BACKUP SCHEDULE**

Vous trouverez ci-dessous le calendrier de sauvegarde et la politique de rétention qui seront appliqués dans le paysage SHQ… sauf en cas de besoin spécifique à l'application, et si cette exigence est approuvée par l'équipe d'application.

|  |  |  |
| --- | --- | --- |
| **Backup Type** | **Schedule** | **Retention** |
| Daily (Production Tier 3 and 4) | 11:00 PM Regional time | 45 days |
| Every 4 Hrs (Production Tier 1 and 2) | 00:00, 04:00, 08:00, 12:00, 16:00 and 20:00 hrs  (Regional time) | 45 days |
| Weekly (Non-production) | Friday 11:00 PM Regional time | 45 days |

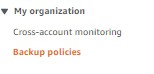
**ANNEXE 2 : CRÉATION D'UNE POLITIQUE DE SAUVEGARDE**

**A : Politique de sauvegarde - Prod (les politiques de sauvegarde sont créées dans le compte principal de l'organisation (Master Account)**)

1. Créez le rôle IAM requis sur AWS Backup pour assumer et effectuer les opérations de sauvegarde et de restauration à l'aide du modèle de formation Cloud (reportez-vous **à l'annexe 4** pour connaître les étapes).

2. Accédez à AWS Backup à l'aide du lien suivant https://aws.amazon.com/fr/backup/.

3. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page Politique de sauvegarde.



4. Entrez le nom de la politique conformément à la convention de dénomination <CLIENT NAME> <CLIENT NAME>-<ENV>-<REGION>-BACKUP\_POLICY

5. Entrez la description de la politique avec les détails du plan de sauvegarde

6. Sélectionnez l'éditeur visuel dans la section configurer le plan de sauvegarde

7. Entrez le nom du plan de sauvegarde

<NOM CLIENT>-<ENV>-<REGION>-BACKUP\_PLAN

8. Sélectionnez la région du plan de sauvegarde selon les besoins (exemple : us-east-1)

9. Accédez à la section Règles de sauvegarde dans l'éditeur visuel

10. Cliquez sur ajouter une règle de sauvegarde

• Saisissez le nom de la règle [<CLIENT NAME>-<ENV>-<REGION>-BACKUP\_RULE]

• Spécifiez le coffre-fort de sauvegarde spécifique à la région (exemple : PROD-NAM-BACKUP\_VAULT)

11. Sélectionnez la fréquence du programme = « QUOTIDIEN »

12. Spécifiez la fenêtre de sauvegarde avec les paramètres suivants

• Heure de début de la fenêtre de sauvegarde : 23h00, heure locale

• Commencer dans : 1 heure

• Réalisé en : 8 heures

13. Sélectionnez la politique de cycle de vie de la sauvegarde avec les paramètres suivants

• Transition vers l'entreposage frigorifique : Jamais

• Expire après : 45 jours

• Sélectionnez l'option de copie vers la région de destination (exemple : USA Ouest (Oregon)) et sélectionnez le coffre-fort de sauvegarde de destination (exemple : <NOM DU CLIENT>-PRD-USWest-BACKUP\_VAULT ).

14. Dans Paramètres avancés,

• Sélectionnez la transition vers le stockage à froid : Jamais

Délai de conservation : 45 jours

15. Sélectionnez la section Affecter des ressources et saisissez le nom du groupe d'affectation de ressources.

[<NOM DU CLIENT>-<ENV>-<REGION>-BACKUP\_ASSIGNMENT\_GROUP]

16. Spécifiez le rôle IAM créé avec la stratégie d'accès complet de sauvegarde

17. Attribuez la balise avec la cible KEY et VALUES

KEY : identifiant d'environnement

Valeur : produit

Ou

CLÉ : niveau de récupération

Valeur : Tier3 ou Tier4

18. Cliquez sur Ajouter une affectation

19. Cliquez sur créer une politique

20. Vérifiez les paramètres JSON pour la conformité de la configuration.

B : Politique de sauvegarde avec réplication de région distante-Prod (les politiques de sauvegarde sont créées dans le compte principal de l'organisation)

1. Créez le rôle IAM requis sur AWS Backup pour assumer et effectuer les opérations de sauvegarde et de restauration à l'aide du modèle de formation Cloud (reportez-vous à l'annexe 4 pour connaître les étapes).

2. Connectez-vous au compte membre et sélectionnez la région secondaire (exemple : ‘us-west-2’)

3. Accédez au service "AWS Backup" et sélectionnez Backup Vault

4. Créer un coffre-fort de sauvegarde Exemple :

Nom : <NOM DU CLIENT>-PRD-USWest-BACKUP\_VAULT

Clé de chiffrement : AWS/Backup

5. Connectez-vous au compte principal AWS, sélectionnez la région (par exemple : US-East-1) et accédez au service de sauvegarde

6. Accédez aux politiques de sauvegarde et cliquez sur créer une politique de sauvegarde

Nom : <NOM DU CLIENT>-PRD-NAM-Tier1-BACKUP\_POLICY

Description de la politique : politique de sauvegarde pour l'application de niveau 1 avec réplication de région distante

7. Dans la session de configuration du plan de sauvegarde, mettez à jour les détails ci-dessous,

Nom du plan de sauvegarde : <NOM DU CLIENT>-PRD-NAM-Tier1-BACKUP\_PLAN

Région du plan de sauvegarde : US-EAST-1

8. Dans Ajouter une session de règle de sauvegarde, mettez à jour les détails ci-dessous,

• Nom de la règle de sauvegarde : <NOM DU CLIENT>-PRD-NAM-Tier1-BACKUP\_RULE

• Spécifiez le coffre-fort de sauvegarde spécifique à la région (exemple : NONPROD-NAM-BACKUP\_VAULT).

• Fréquence de sauvegarde : expression cron personnalisée : cron (0 0,4,8,12,16,20 ? \* \* \*)

• Commencer dans : 1 heure

• Compléter en : 4 heures

• Passage en chambre froide : jamais

• Période de conservation : 45 jours

• Sélectionnez l'option de copie vers la région de destination (exemple : USA Ouest (Oregon)) et sélectionnez le coffre-fort de sauvegarde de destination (exemple : <NOM DU CLIENT>-PRD-USWest-BACKUP\_VAULT)

9. Dans Paramètres avancés,

• Sélectionnez la transition vers le stockage à froid : Jamais

• Période de conservation : 45 jours

10. Dans la mise à jour de la session d'affectation des ressources sous les paramètres,

• Nom d'affectation de ressource : <NOM DU CLIENT>-PRD-NAM-Tier1-BACKUP\_RESOURCE\_ASSIGNMENT1

• Rôle IAM : BackUpCrossAccountRole Par exemple :

Clé de balise de ressource : APP\_ID Valeurs de balise : APP-43125 ou

11. Enregistrez la politique

12. Ouvrez à nouveau la politique et sélectionnez la cible et cliquez sur attacher

13. Accédez au compte de membre applicable et joignez-le à la politique.

C : Politique de sauvegarde pour l'environnement hors production (les politiques de sauvegarde sont créées dans le compte principal de l'organisation)

1. Créez un rôle IAM pour AWS Backup pour assumer et effectuer des opérations de sauvegarde et de restauration à l'aide du modèle de formation Cloud

2. Accédez au service de sauvegarde AWS à l'aide du lien suivant https://console.aws.amazon.com/backup.

3. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page Politique de sauvegarde.

4. Entrez le nom de la politique conformément à la convention de dénomination <CLIENT NAME> <CLIENT NAME>-<ENV>-<REGION>-BACKUP\_POLICY

5. Entrez la description de la politique avec les détails du plan de sauvegarde

6. Sélectionnez l'éditeur visuel dans la section configurer le plan de sauvegarde

7. Entrez le nom du plan de sauvegarde <CLIENT NAME>-<ENV>-<REGION>-BACKUP\_PLAN

8. Sélectionnez la région du plan de sauvegarde selon vos besoins (exemple : us-east-1)

9. Accédez à la section Règles de sauvegarde dans l'éditeur visuel

10. Cliquez sur ajouter une règle de sauvegarde, entrez le nom de la règle [<NOM DU CLIENT>-<ENV>-<REGION>-BACKUP\_RULE] 11. Spécifiez le coffre-fort de sauvegarde spécifique à la région (exemple : NONPROD-NAM-BACKUP\_VAULT).

12. Sélectionnez la fréquence du programme = "Hebdomadaire"

13. Spécifiez la fenêtre de sauvegarde avec les paramètres suivants

• Heure de début de la fenêtre de sauvegarde : 23h00, heure locale (vendredi)

• Commencer dans : 2 heures

• Réalisé en : 1 jour

14. Sélectionnez la politique de cycle de vie de la sauvegarde avec les paramètres suivants

• Transition vers l'entreposage frigorifique : Jamais

• Expire après : 45 jours

15. Sélectionnez la section Affecter des ressources, entrez le nom du groupe d'affectation de ressources.

[<NOM DU CLIENT>-<ENV>-<REGION>-BACKUP\_ASSIGNMENT\_GROUP]

16. Spécifiez le rôle IAM créé avec la stratégie d'accès complet de sauvegarde

17. Attribuez la balise avec la cible KEY et VALUES

KEY : identifiant d'environnement

Valeur : dev ou test

18. Cliquez sur Ajouter une affectation

19. Cliquez sur créer une politique

20. Vérifiez les paramètres JSON pour la conformité de la configuration

**ANNEXE 3 : ATTACHEMENT DES CIBLES À LA POLITIQUE DE SAUVEGARDE**

1. Accédez au service de sauvegarde AWS à l'aide du lien https://console.aws.amazon.com/backup

2. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page Politique de sauvegarde

3. Sélectionnez la politique de sauvegarde créée dans l'ANNEXE 2

4. Naviguez dans la section Cibles dans la politique de sauvegarde

5. Cliquez sur Attacher pour joindre les cibles (UO) / comptes

6. Sélectionnez la liste des UO/comptes à ajouter en tant que cible pour la politique de sauvegarde créée à l'annexe 2.

Notes complémentaires:

je. Comme mentionné dans la section Annexe 2 - étape 17, une étiquette doit être attachée au serveur afin qu'il soit inscrit dans le calendrier de sauvegarde.

ii. Vérifiez le nouvel ID de ressource dans la sauvegarde AWS pour confirmer que la nouvelle instance est ajoutée à la sauvegarde. Chaque serveur sera intégré à la sauvegarde AWS pendant la phase de construction.

**ANNEXE 4 : RÔLE IAM POUR AWS BACKUP**

Le service de sauvegarde AWS a besoin d'une politique IAM exclusive comme condition préalable qui lui permet de se connecter à d'autres services dans AWS tels que EC2 et EBS. Ce rôle IAM doit être créé en tant qu'exigence unique dans le compte principal AWS et accordera l'autorisation au service AWS Backup d'accéder à EC2 dans le backend de l'unité d'organisation AWS.

1. Lancez un AWS CloudFormation StackSet dans le compte principal.

2. Fournissez un nom StackSet en tant que configuration AWS Backup US EAST.

3. Entrez BackUpCrossAccountRole dans la configuration IAM. Choisissez Suivant.

4. Choisissez les autorisations gérées par le service pour autoriser le déploiement automatique de ce rôle IAM sur tous les nouveaux comptes ajoutés aux unités d'organisation cibles à l'avenir. Choisissez Suivant.

5. Choisissez Déployer sur l'organisation. Choisissez USA Est, Francfort et Tokyo dans Spécifier les régions. Conservez les autres paramètres par défaut. Choisissez Suivant.

6. Cochez la case J'accepte qu'AWS CloudFormation puisse créer des ressources IAM avec des noms personnalisés. Choisissez Soumettre et vérifiez l'achèvement du déploiement des ensembles de piles sous l'onglet Instances de pile.

**ANNEXE 5 : ÉTAPES POUR CRÉER UNE SAUVEGARDE À LA DEMANDE**

Dans le cas où une sauvegarde à la demande est nécessaire ou demandée, la console de sauvegarde AWS le permet. La demande doit inclure l'ID d'instance et la période de conservation requise.

Les opérations cloud effectueront les étapes suivantes.

1. À partir de la sauvegarde AWS, sélectionnez l'option Créer une sauvegarde à la demande.

2. Sélectionnez le type de ressource et recherchez avec l'ID de ressource pour sélectionner la ressource à sauvegarder

3. Sélectionnez l'option "Créer une sauvegarde maintenant"

4. Sélectionnez l'expiration comme demandé dans la demande de ticket

5. Choisissez le coffre par défaut et le rôle IAM de sauvegarde

6. Cliquez sur créer une sauvegarde à la demande et vérifiez que la tâche est terminée.

ANNEXE 6 : ÉTAPES POUR RESTAURER UNE SAUVEGARDE

Pour une restauration de sauvegarde, un propriétaire d'application soulèvera une demande de restauration dans <ticketing tool>. La demande doit inclure l'identifiant de l'instance et la date à partir de laquelle la restauration doit être effectuée.

Pour restaurer une image spécifique, l'équipe des opérations Cloud :

1. Sélectionnez le coffre-fort de sauvegarde et recherchez avec l'ID d'instance (ID de ressource) qui répertoriera les points de récupération AWS disponibles pouvant être restaurés.

2. Sélectionnez l'image de date requise spécifique et cliquez sur restaurer (cette action restaurera les données à l'emplacement d'origine et il est donc important que l'approbation de l'utilisateur ou du propriétaire de l'application soit obligatoire avant qu'une action de restauration ne soit exécutée)

3. Vérifiez le formulaire d'état du travail de restauration de la session du travail et assurez-vous qu'il est terminé.

**ANNEXE 7 : ÉTAPES POUR SUPPRIMER LE PLAN DE SAUVEGARDE**

Pour supprimer un plan de sauvegarde, une analyse des risques appropriée et une approbation des modifications doivent être effectuées avant toute action. La mise en œuvre des suppressions du plan de sauvegarde comprend :

1. Cliquez sur Sauvegarde AWS/Plan de sauvegarde

2. Sélectionnez le plan de sauvegarde à supprimer

3. Tapez le plan de sauvegarde pour confirmer et supprimer le plan.

**ANNEXE 8 : ÉTAPES POUR SURVEILLER LA SAUVEGARDE**

AWS Backup fournit un tableau de bord qui simplifie l'audit de l'activité de sauvegarde et de restauration sur les services AWS. Cloud Ops affichera l'état des tâches de sauvegarde et de restauration récentes sur les services AWS. AWS Backup s'intègre à AWS CloudTrail, qui fournit une vue consolidée des journaux d'activité de sauvegarde qui permet de vérifier rapidement et facilement quelles ressources sont sauvegardées et comment elles sont sauvegardées. AWS Backup sera intégré à Amazon Simple Notification Service (SNS), qui alerte automatiquement l'équipe Cloud Ops sur l'activité de sauvegarde, par exemple lorsqu'une sauvegarde échoue ou qu'une restauration est lancée.

Les rapports de sauvegarde seront examinés quotidiennement et une action appropriée telle que la nouvelle soumission des sauvegardes ou la résolution de problèmes dans l'environnement sera effectuée.

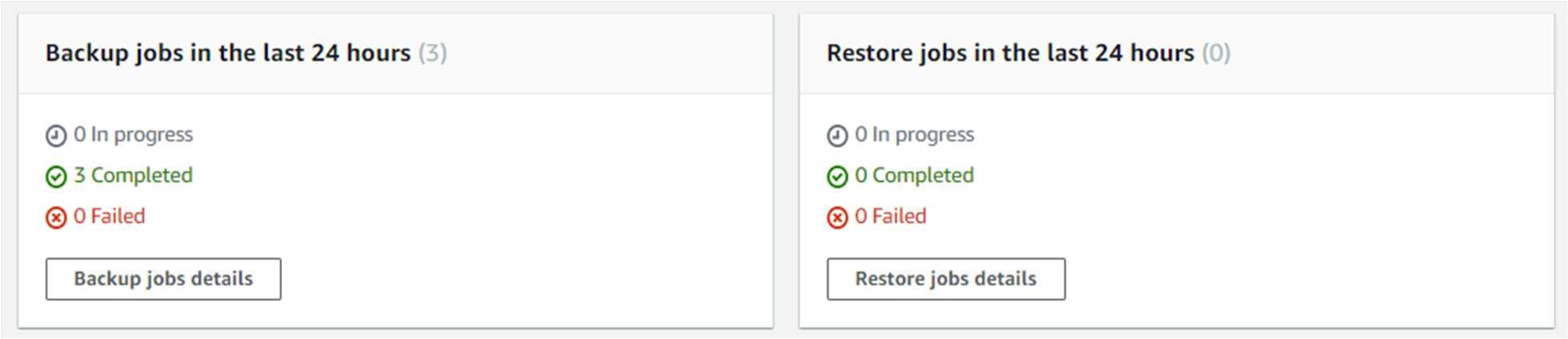
Pour les rapports de sauvegarde :

• Connectez-vous à la console AWS pour chaque compte et région, sélectionnez Tableau de bord du service de sauvegarde AWS

• Vérifiez l'état de la sauvegarde au cours des dernières 24 heures

• S'il y a des travaux en échec, créez un <nom de l'outil de ticket> Ticket d'incident pour l'échec de la sauvegarde

• L'équipe Cloud Operations partage un rapport de sauvegarde hebdomadaire.



Pour l'alerte de travaux ayant échoué, créez l'alarme CloudWatch avec les métriques ci-dessous :

Nom de la métrique : Sauvegarde => NumberOfBackupJobsFailed

Seuil : > 1

Période (Min) : 5

Point de données : 1 sur 1