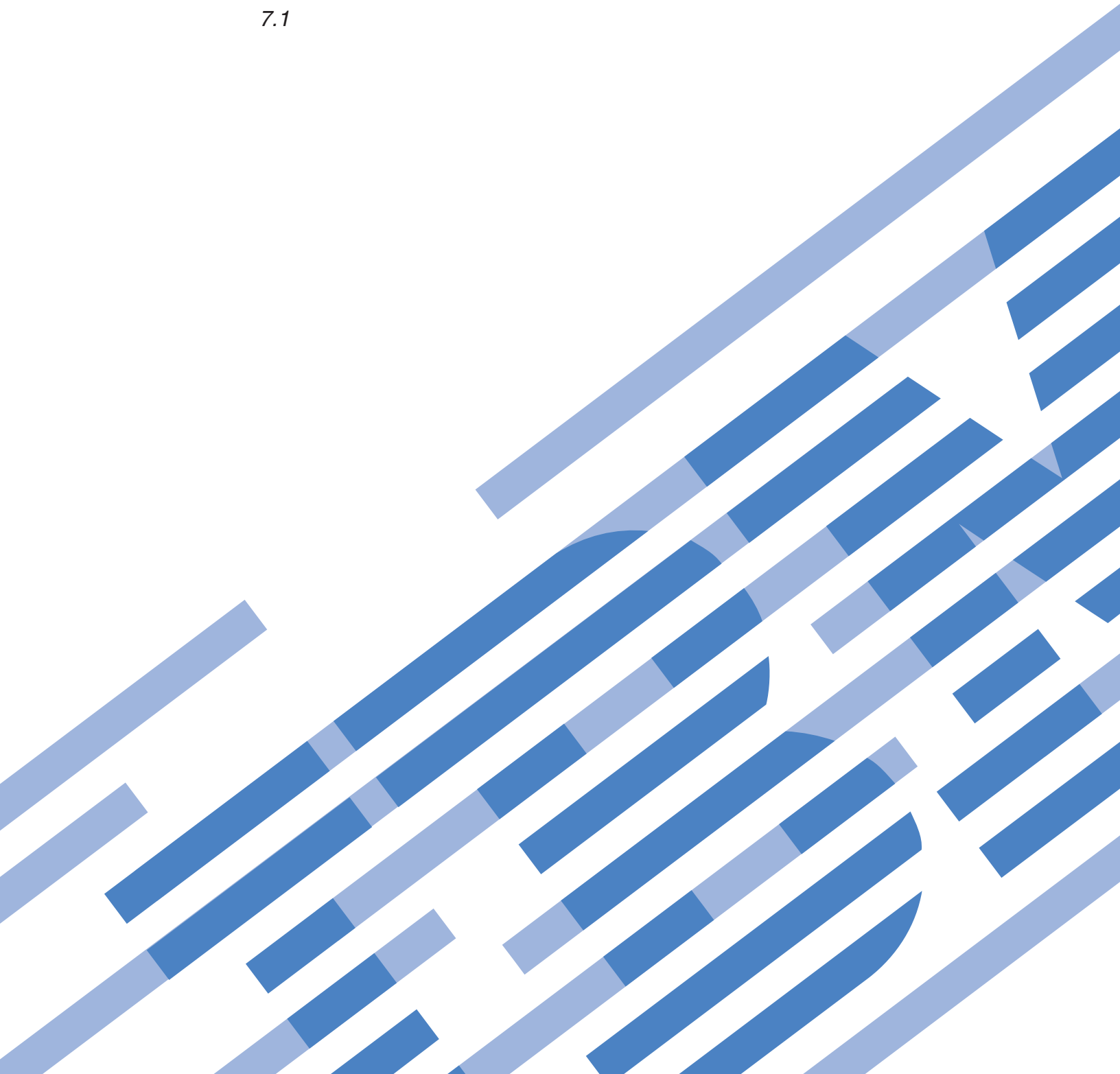
IBM i

Disponibilité
Implémentation de la haute disponibilité avec l'approche basée sur des tâches

7.1



IBM i

Disponibilité
Implémentation de la haute disponibilité avec l'approche basée sur des tâches

7.1

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 213.

Neuvième édition - février 2010

Réf. US : RZAI-G000-08

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Chapitre 1. Implémentation de la haute disponibilité avec l'approche basée sur des tâches

La configuration et la gestion de la haute disponibilité i5/OS à partir de tâches vous permet de configurer et de gérer une solution à haute disponibilité personnalisée en fonction de vos besoins. Des interfaces graphiques et de ligne de commande sont utilisées pour configurer et gérer votre solution à haute disponibilité.

Contrairement à l'approche à base de solutions, qui fait appel à l'interface graphique High Availability Solution Manager et dans laquelle une solution prédéfinie est configurée automatiquement avec une intervention limitée de l'utilisateur, l'approche à base de tâches donne à l'utilisateur chevronné les moyens de configurer et d'implémenter une solution personnalisée. Cependant, pour créer et gérer une solution à haute disponibilité dans cette optique, les utilisateurs doivent bien cerner leurs besoins en la matière et connaître pluieurs interfaces.

Interface des services-ressources de mises en grappe

L'interface des services-ressources de mise en grappe permet de configurer et de gérer les techniques de mise en grappe intégrées à une solution à haute disponibilité. Pour utiliser cette interface, vous devez avoir installé le logiciel sous licence 5770-HAS de IBM® PowerHA for i (iHASM). Cette interface permet d'effectuer les fonctions suivantes :

- Création et gestion d'une grappe
- Création et gestion de noeuds
- Création et gestion de groupes de ressources de grappe
- Création et gestion de domaines d'administration de grappe
- Création et gestion de ressources contrôlées
- Contrôle de la grappe pour les événements associés, tels que les partitions et les reprises en ligne
- Exécution de basculements manuels pour les indisponibilités prévues, par exemple pour la maintenance planifiée d'un système

Interface de gestion de disque

L'interface de gestion de disque permet de configurer et de gérer les pools de stockage de disque indépendants qui sont nécessaires lors de la mise en oeuvre de plusieurs techniques de test de résistance des données. Selon le type de technique mis en oeuvre, une configuration d'installation peut être requise pour utiliser certaines des fonctions suivantes :

- Création d'un pool de stockage sur disque
- Mise en fonction d'un pool de stockage sur disque
- Mise hors fonction d'un pool de stockage sur disque
- Configuration de la protection géographique par disque miroir
- Configuration de Metro Mirror
- Configuration de Global Mirror

Interface de ligne de commande

L'interface de ligne de commande permet d'effectuer de nombreuses tâches haute disponibilité à l'aide de commandes CL. Pour chaque tâche liée à une grappe, la commande CL correspondante est identifiée.

Information associée

IBM PowerHA for i commands

Planification de la solution à haute disponibilité

Avant de configurer une solution à haute disponibilité i5/OS, une planification adéquate est nécessaire pour réunir toutes les conditions requises.

Chaque technologie à haute disponibilité implique de réunir des conditions minimales avant la configuration d'une solution spécifique. Outre ces conditions, il est également important de déterminer quelles ressources doivent être rendues résilientes. Il convient d'évaluer ces ressources (applications, données et unités, par exemple) afin de déterminer si elles doivent être accessibles en haute disponibilité. Si elles exigent une haute disponibilité, il est important d'apporter les modifications nécessaires à l'environnement avant de configurer une solution à haute disponibilité. Par exemple, des données résidant dans SYSBAS doivent peut-être bénéficier d'une haute disponibilité. Avant de configurer une solution, il convient de déplacer ces données dans un pool de stockage sur disque indépendant. Certaines applications peuvent également exiger des modifications pour pouvoir prendre en charge la haute disponibilité.

Applications des grappes

Les tests de résistance des applications sont des éléments clés dans un environnement en grappes. Si vous envisagez d'écrire et d'utiliser des applications à haute disponibilité dans votre grappe, sachez que ces applications ont des spécifications de disponibilité particulières.

En tirant parti des applications résilientes de votre grappe, vous pouvez redémarrer une application sur un noeud de grappe différent sans qu'il y ait besoin de reconfigurer les clients. En outre, les données associées à l'application seront disponibles après un basculement ou une reprise en ligne. Cela signifie que l'utilisateur de l'application peut faire face à une interruption minimale ou quasi inexistante, tandis que l'application et ses données basculent du noeud principal vers le noeud de sauvegarde. L'utilisateur n'a pas besoin de savoir que l'application et les données ont été déplacées en arrière-plan.

Pour réaliser les tests de résistance des application dans votre grappe, les applications qui répondent à certaines spécifications de disponibilité doivent être utilisées. Certaines caractéristiques doivent être présentes dans l'application pour qu'elle soit commutable, et la rendre ainsi toujours disponible pour les utilisateurs de l'application de la grappe. Pour plus d'informations sur les caractéristiques de ces applications, voir la section High Availability and Clusters. Puisque de telles exigences existent, vous pouvez utiliser les options suivantes pour utiliser une application commutable de votre grappe :

1. **Acheter une application logicielle pour grappes**

   Les logiciels destinés aux grappes répondent à certaines exigences de haute disponibilité.
2. **Ecrire ou modifier votre propre application pour la rendre hautement disponible**

   Les éditeurs de logiciels indépendants et les programmeurs d'application peuvent personnaliser des applications pour les rendre commutables dans un environnement en grappes System i.

Quand vous êtes en présence d'une application résiliente, celle-ci doit être gérée dans votre grappe.

Information associée

High Availability and Clusters

Identification des applications résilientes

Toutes les applications n'offrent pas autant de disponibilité que la mise en grappe.

Une application doit être résiliente pour profiter des fonctions de basculement et de reprise en ligne qu'offre la mise en grappe. La résilience d'une application permet à celle-ci d'être redémarrée sur le noeud de secours sans devoir reconfigurer les clients utilisant cette application. Votre application doit donc respecter certaines exigences pour exploiter pleinement les fonctions offertes par la mise en grappe.

i5/OS architecture des applications de mise en grappe

Une valeur d'utilisateur final supplémentaire est fournie par toute application hautement disponible, tout en reconnaissant les applications qui continuent d'être disponibles en cas d'indisponibilité, prévue ou non.

i5/OS a fourni une architecture de résilience d'application qui prend en charge plusieurs degrés d'application hautement disponible. Les applications haut de gamme de ce type de produit démontrent des caractéristiques hautement disponibles, fournissent une automatisation de l'environnement hautement disponible, et sont gérées via des interfaces de gestion à haute disponibilité.

Ces applications possèdent les caractéristiques suivantes :

- L'application peut basculer vers un noeud de grappe de sauvegarde quand le noeud principal n'est plus disponible.
- L'application définit l'environnement résilient dans la Zone de définition résiliente et de données de statut pour activer la configuration et l'activation automatiques de l'application par une application de gestion de grappe.
- L'application fournit des tests de résistance d'application via un programme d'exit de groupe de ressources en grappe pour gérer des événements liés à une grappe, tout en tirant parti des capacités des services-ressources de mise en grappe i5/OS.
- L'application fournit une fonction de redémarrage d'application qui repositionne l'utilisateur sur un écran de menu de l'application ou au-delà.

Les applications qui font preuve d'une disponibilité plus solide et de caractéristiques de redémarrage possèdent les caractéristiques suivantes :

- L'application fournit une optimisation des tests de résistance d'application via une gestion plus robuste des événements de grappe (codes d'action) réalisée par le programme d'exit du groupe de ressources en grappe d'application.
- L'application fournit une prise en charge plus élevée du redémarrage des applications. Pour les applications centrées sur l'hôte, l'utilisateur sera repositionné sur une frontière de transaction par les fonctions de contrôle de validation ou de point de contrôle. Pour les applications centrées sur le client, l'utilisateur connaîtra un basculement sans heurt avec une interruption de service minimale.

Ecriture d'une application de grappe à haute disponibilité

Une application à haute disponibilité est une application qui peut être résiliente à une indisponibilité système dans un environnement mis en grappe.

Il existe plusieurs niveaux de disponibilité d'application :

1. Si une erreur d'application se produit, l'application redémarre automatiquement sur le même noeud et corrige toute cause potentielle de l'erreur (telle que des données de contrôle corrompues). Vous pouvez afficher l'application comme si elle avait démarrée pour la première fois.
2. L'application effectue une partie du traitement point de contrôle-redémarrage. Vous pouvez afficher l'application comme si elle était fermée au point de défaillance.
3. Si une indisponibilité système se produit, l'application redémarre sur un serveur de sauvegarde. Vous pouvez afficher l'application comme si elle avait démarrée pour la première fois.
4. Si une indisponibilité système se produit, l'application redémarre sur un serveur de sauvegarde et effectue une partie du traitement point de contrôle-redémarrage dans les serveurs. Vous pouvez afficher l'application comme si elle était fermée au point de défaillance.
5. Si une indisponibilité système se produit, une reprise en ligne coordonnée de l'application et de ses données associées vers un ou d'autres noeud(s) de la grappe se produit. Vous pouvez afficher l'application comme si elle avait démarrée pour la première fois.
6. Si une indisponibilité système se produit, une reprise en ligne coordonnée de l'application et de ses données associées vers un ou d'autres noeud(s) de la grappe se produit. L'application effectue une

partie du traitement point de contrôle-redémarrage dans les serveurs. Vous pouvez afficher l'application comme si elle était fermée au point de défaillance.

Remarque : Dans les cas 1 à 4 ci-dessus, vous êtes responsable de la restauration des données.

Rendre résilient des programmes d'application :

Découvrez comment rendre résilient des programmes d'application.

Une application résiliente est censée posséder les caractéristiques suivantes :

- L'application peut être redémarrée sur ce noeud ou sur un autre noeud
- L'application est accessible pour le client via l'adresse IP
- L'application est sans état ou l'information d'état est connue
- Les données associées à l'application sont disponibles après un basculement.

Les trois principaux éléments qui rendent résiliente une application aux indisponibilités système dans un environnement mis en grappe sont :

L'application elle-même
A quel point l'application tolère les erreurs ou les indisponibilités système, et comment l'application peut redémarrer d'elle-même ?

L'application peut gérer cela via l'utilisation des capacités de mise en grappe.

Les données associées
Quand une indisponibilité se produit, a-t-elle un impact sur la disponibilité des données associées ?

Vous pouvez stocker des données critiques dans disques commutés qui permettent aux données de rester disponible pendant une indisponibilité. Sinon, un produit de réplication middleware de grappe (IBM Business Partner) qui tire parti des fonctions de mise en grappe peut s'en charger.

Fonctions de contrôle et administration
Quel est le degré de facilité de définition de l'environnement qui prend en charge la disponibilité des données et de l'application ?

Le numéro de programme sous licence IBM PowerHA for i, fournit plusieurs interfaces pour configurer et gérer des solutions et une technologie à haute disponibilité. Le logiciel sous licence PowerHA fournit les interfaces suivantes :

Interface graphique du gestionnaire de solutions à haute disponibilité
Cette interface graphique vous permet de faire votre choix parmi plusieurs solutions à haute disponibilité IBM i prises en charge. Cette interface valide toutes les exigences technologiques pour votre solution sélectionnée, configure cette dernière et les technologies associés, et fournit une gestion simplifiée de toutes les technologies à haute disponibilité qui composent votre solution.

Interface graphique des services-ressources de mise en grappe
Cette interface graphique offre à un utilisateur expérimenté plus de souplesse pour la personnalisation d'une solution à haute disponibilité. Elle vous permet de configurer et de gérer des technologies de grappe, telles que les groupes de ressources en grappe. Vous pouvez également configurer des pools de stockage sur disque indépendants à partir de cette interface quand ils sont utilisés dans le cadre d'une solution à haute disponibilité.

Commandes IBM PowerHA for i
Ces commandes offrent des fonctions similaires mais elle sont disponibles via une interface de ligne de commande.

API Ces interfaces de programmation IBM PowerHA for i vous permettent d'utiliser la nouvelle fonction de pools de stockage sur disque indépendants.

En outre, vous pouvez également utiliser une interface de gestion de grappe tierce qui utilise les interfaces de programmation de mise en grappe et qui allie des applications résilientes à des données résilientes.

Information associée

High availability management

Redémarrage des applications de grappe à haute disponibilité :

Pour redémarrer une application, l'application doit connaître son état au moment du basculement ou de la reprise en ligne.

Les informations d'état sont propres à l'application ; par conséquent, l'application doit déterminer les informations nécessaires. Sans information d'état, l'application peut être redémarrée sur votre PC. Cependant, vous devez rétablir votre position dans l'application.

Il existe plusieurs méthodes pour enregistrer les informations d'état de l'application pour le système de sauvegarde. Chaque application doit déterminer la méthode la plus adaptée à son fonctionnement.

- L'application peut transférer toutes les informations d'état au système client demandeur. Lorsqu'une reprise en ligne ou un basculement se produit, l'application utilise l'état stocké sur le client pour rétablir l'état dans le nouveau serveur. Cela est possible via l'utilisation des API Distribute Information ou Clustered Hash Table.
- L'application peut répliquer en temps réel des informations d'état (telles que les informations relatives au travail et les autres structures de contrôle associées à l'application). Pour chaque modification apportée dans les structures, l'application envoie la modification au système de sauvegarde.
- L'application peut stocker des informations d'état pertinentes associées dans la portion de données du programme d'exit du groupe de ressources en grappe de cette application. Cette méthode suppose qu'un petite quantité d'informations d'état est nécessaire. Vous pouvez utiliser l'API QcstChangeClusterResourceGroup (Modification d'un groupe de ressources en grappe) pour y parvenir.
- L'application peut stocker des informations d'état dans un objet de données qui est en cours de réplication dans les systèmes de sauvegarde avec les données de l'application.
- L'application peut stocker des informations d'état dans un objet de données stocké dans l'IASP commutable qui contient également les données de l'application.
- L'application peut stocker des informations d'état relatives au client.
- Aucune information d'état n'a été enregistrée, et vous devez effectuez la récupération.

Remarque : La quantité d'informations requises pour la sauvegarde est moindre si l'application utilise une certaine forme de traitement point de contrôle-redémarrage. Les informations d'état sont uniquement enregistrées au niveau des points de contrôle prédéterminés. Un redémarrage vous emmène au dernier point de contrôle connu qui est semblable au fonctionnement du traitement du contrôle de validation de la base de données.

Appel d'un programme d'exit de groupe de ressources en grappe :

Le programme d'exit de groupe de ressources en grappe est appelé pendant plusieurs phases d'un environnement de grappe.

Ce programme établit les tests de résistance nécessaires à l'environnement pour les ressources d'une grappe. Il est facultatif pour un groupe de ressources en grappe d'unité résilient, mais il ne l'est pas pour les autres types de groupe de ressources en grappe. Quand un programme d'exit de groupe de ressources en grappe est utilisé, il est appelé sur l'occurrence des événements à l'échelle de la grappe, tels que les suivants :

- Un noeud quitte la grappe inopinément

- Un noeud quitte la grappe suite à l'appel de l'API QcstEndClusterNode (Arrêt du noeud de grappe) ou QcstRemoveClusterNodeEntry (Suppression d'un poste de noeud d'une grappe)
- La grappe est supprimée suite à l'appel de l'API QcstDeleteCluster (Supprimer la grappe)
- Un noeud est activé par l'appel de l'API QcstStartClusterNode (Démarrage d'un noeud de grappe)
- La communication avec un noeud partitionné est rétablie

Le programme d'exit effectue les processus suivants :
- Il s'exécute dans un groupe d'activation nommé ou dans le groupe d'activation de l'appelant (*CALLER).
- Il ignore le paramètre de redémarrage si le programme d'exit possède une exception non gérée ou est annulé.
- Il fournit un gestionnaire d'annulation.

Quand une API d'un groupe de ressources en grappe est exécutée, le programme d'exit est appelé depuis une autre tâche avec le profil utilisateur spécifié dans l'API QcstCreateClusterResourceGroup (Création d'un groupe de ressources en grappe). Le travail distinct est automatiquement créée par l'API lors de l'appel du programme d'exit. Si le programme d'exit d'un groupe de ressources en grappe de données n'aboutit pas ou s'arrête anormalement, le programme d'exit d'un groupe de ressources en grappe est appelé sur tous les noeuds actifs du domaine de reprise en utilisant un code d'action d'Annulation. Ce code d'action permet l'annulation de tout activité non terminée et la restauration de l'état d'origine du groupe de ressources en grappe.

Supposons qu'un basculement non abouti se produise pour un groupe de ressources en grappe d'unité. Après un nouveau basculement de toutes les unités, si la mise en fonction de toutes les unités a abouti sur le noeud principal d'origine, la mise en grappe appelle le programme d'exit sur le noeud principal d'origine en utilisant un code d'action de Démarrage.

Si le programme d'exit d'un groupe de ressources en grappe d'application n'aboutit pas ou s'arrête anormalement, les services-ressources de mise en grappe tentent de redémarrer l'application si l'état du groupe de ressources en grappe est actif. Le programme d'exit du groupe de ressources en grappe est appelé à l'aide d'un code d'action de redémarrage. Si l'application n'est toujours pas redémarrée après le nombre de tentatives indiqué, le programme d'exit du groupe de ressources en grappe est appelé à l'aide du code d'action Basculement. Le nombre de redémarrage est réinitialisé uniquement quand le programme d'exit est appelé à l'aide d'un code d'action de Démarrage, qui peut être le résultat d'un groupe de ressources en grappe de démarrage, d'une reprise en ligne ou d'un basculement.

Quand le groupe de ressources en grappe est démarré, le programme d'exit du groupe de ressources en grappe d'application appelé sur le noeud principal n'est pas censé redonner le contrôle aux services-ressources de mise en grappe tant que l'application ne s'arrête pas ou qu'une erreur ne se produit pas. Après l'activation d'un groupe de ressources en grappe d'application, si les services-ressources de mise en grappe doivent avertir le programme d'exit d'un groupe de ressources en grappe d'application de certains événements, une autre instance du programme d'exit sera lancée dans un autre travail. Les codes d'action Démarrage ou Redémarrage ne doivent pas être renvoyés.

Quand un programme d'exit d'un groupe de ressources en grappe est appelé, un ensemble de paramètres identifient l'événement de grappe en cours de traitement, l'état actuel des ressources de la grappe et l'état attendu des ressources mises en grappe.

Pour obtenir des informations complètes sur les programmes d'exit d'un groupe de ressources en grappe, y compris sur les informations transférées au programme d'exit pour chaque code d'action, consultez la section Programme d'exit du groupe de ressources en grappe dans la documentation de l'API de la grappe. Un exemple de code source a été fourni dans la bibliothèque QUSRTOOL qui peut être utilisé comme base d'écriture d'un programme exit. Consultez le membre TCSTAPPEXT dans le fichier QATTSYSC.

Considérations relatives au groupe de ressources en grappe d'application

Un groupe de ressources en grappe d'application gère la résilience de l'application.

Gestion des adresses IP de relais des groupes de ressources en grappe d'application :

Vous pouvez gérer les adresses IP de relais des groupes de ressources en grappe d'application à l'aide des services-ressources de mise en grappe. Vous pouvez également les gérer manuellement.

Il existe deux méthodes pour gérer l'adresse IP de relais d'application associée à un groupe de ressources en grappe d'application. La méthode la plus simple est de laisser les services-ressources de mise en grappe gérer l'adresse IP de relais (méthode par défaut). Cette méthode permet aux services-ressources de mise en grappe de créer l'adresse IP de relais sur tous les noeuds du domaine de reprise, y compris ceux ajoutés au domaine de reprise par la suite. Quand cette méthode est choisie, l'adresse IP de relais ne peut pas être définie simultanément sur les noeuds du domaine de reprise.

L'autre méthode consiste à gérer l'adresse IP de relais vous-même. Cette méthode permet aux services-ressources de mise en grappe de n'effectuer aucune action pour configurer l'adresse IP de relais ; l'utilisateur est seul responsable de cette configuration. Vous devez ajouter l'adresse IP de relais sur tous les noeuds du domaine de reprise (à l'exception des noeuds dupliqués) avant le démarrage du groupe de ressources en grappe. Avant d'ajouter un noeud au domaine de reprise d'un groupe de ressources en grappe actif, vous devez configurer l'adresse IP de relais qui correspond à ce noeud.

Concepts associés

«Exemple : actions de reprise en ligne d'un groupe de ressources en grappe d'application», à la page 11
Cet exemple explique le fonctionnement d'un scénario de reprise en ligne. D'autres scénarios peuvent fonctionner différemment.

Sous-réseaux multiples : L'adresse IP de relais de l'application peut être valide dans plusieurs sous-réseaux, bien que, par défaut, tous les noeuds du domaine de reprise se trouvent sur le même sous-réseau. Pour configurer l'adresse IP de relais de l'application quand les noeuds du domaine de reprise s'étendent sur plusieurs sous-réseaux, vous devez activer l'environnement de basculement.

Activation du basculement d'application via des sous-réseaux avec IPv4 :

En général, la mise en grappe nécessite que tous les noeuds de grappe du domaine de reprise d'un groupe de ressources en grappe d'application soient situés sur le même réseau local (qu'ils utilisent la même adresse de sous-réseau). Les services-ressources de mise en grappe prennent en charge une adresse IP de relais configurée par l'utilisateur lors de la configuration des groupes de ressources en grappe d'application.

Le protocole de résolution d'adresse (*Address Resolution Protocol - ARP*) est le protocole réseau sous-jacent utilisé pour basculer l'adresse IP de relais de l'application configurée à partir d'un noeud du domaine de reprise vers un autre. Pour activer le basculement d'application entre les sous-réseaux, vous devez utiliser la prise en charge des adresses IP virtuelles et le protocole de routage de données (RIP) pour IPv4.

Les étapes de configuration manuelle suivantes sont nécessaires à l'activation de l'environnement de basculement. **Cet ensemble d'instructions doit être appliqué à tous les noeuds du domaine de reprise, et répété sur tous les autres noeuds de la grappe qui deviendront des noeuds du domaine de reprise du groupe de ressources en grappe d'application donné.**

1. Sélectionnez une adresse IP de relais IPv4 à utiliser par le groupe de ressources en grappe d'application.
   - Pour éviter toute confusion, cette adresse ne doit pas interférer avec d'autres adresses existantes utilisées par les noeuds de grappe ou les routeurs. Par exemple, si vous choisissez 19.19.19.19, assurez-vous que 19.0.0.0 (19.19.0.0) ne sont pas des routes connues par les tables de routage du système.

- Ajoutez l'interface de relais (par exemple, 19.19.19.19). Créez-la avec une description de ligne *VIRTUALIP, un masque de sous-réseau 255.255.255.255 (route de l'hôte), une transmission maximale de 1500 (tout nombre entre 576 et 16388), et un démarrage automatique définie sur *NO. Cette adresse de relais (par exemple, 19.19.19.19) doit exister comme adresse *VIRTUALIP avant de l'identifier comme interface locale associée dans la prochaine étape. Mais elle ne doit pas être activée.

2. Associez l'adresse IP de relais souhaitée avec une ou les deux adresses IP qui doivent être utilisées par les communications de la grappe quand vous créez la grappe ou ajoutez un noeud à la grappe.
   - Par exemple, cela signifie que vous faites de l'adresse de relais 19.19.19.19 une interface locale associée à l'adresse IP du noeud de grappe. Ceci doit être effectué pour chaque adresse de grappe de chaque noeud de grappe.

     Remarque : Les adresses de la grappe doivent être interrompues pour réaliser cette modification sous la commande Configure TCP/IP (CFGTCP).
3. Créez la grappe et tous les groupes de ressources en grappe. Pour le groupe de ressources en grappe, spécifiez `QcstUserCfgsTakeoverIpAddr` dans le champ **Configuration de l'adresse IP de relais**. Ne lancez aucun groupe de ressources en grappe d'application.
4. L'utilisation de la configuration des applications TCP/IP (option 20) dans le menu Configuration, puis de Configurer RouteD (option 2), puis de Modifier les attributs RouteD (option 1), garantit que la champ Supply a la valeur *YES. Sinon, affectez-lui la valeur *YES. Puis, démarrez ou redémarrez RouteD (RIP ou RIP-2) sur chaque noeud de grappe.
   - L'option NETSTAT 3 indique la RouteD qui utilise un port local en cours d'exécution. RouteD doit être en cours d'exécution et doit afficher les routes (vérifiez que le champ Supply a la valeur *YES) sur chaque noeud de grappe du domaine de reprise du groupe de ressources en grappe.
5. Assurez-vous que tous les routeurs commerciaux du réseau qui connectent entre eux les réseaux locaux du domaine de reprise acceptent et affichent les routes hôte pour RIP.
   - Il ne s'agit pas nécessairement du paramètre par défaut des routeurs. Le langage varie en fonction du fabricant du routeur mais les paramètres des interfaces RIP doivent être définis de manière à envoyer les données via les routes hôtes et à les recevoir via les hôtes dynamiques.
   - Ceci s'applique aussi aux interfaces de routeur qui pointent vers les systèmes ainsi que vers les interfaces routeur à routeur.

     Remarque : N'utilisez pas une machine IBM i comme routeur dans cette configuration. Utilisez un routeur commercial (IBM ou autre) conçu pour le routage. Le routage IBM i ne peut pas être configuré pour gérer cette fonction.
6. Activez manuellement l'adresse de relais sur l'un des noeuds de grappe :
   a. Attendez 5 minutes pour que RIP propage les routes.
   b. Lancez une commande Ping sur l'adresse de relais à partir de tous les noeuds du domaine de reprise du groupe de ressources en grappe et de tous les clients sélectionnés sur les réseaux locaux qui utiliseront cette adresse.
   c. Assurez-vous à nouveau que l'adresse de relais est interrompue.

   (La mise en grappe démarrera l'adresse sur le noeud principal spécifié, une fois les groupes de ressources en grappe démarrés).
7. Démarrez les groupes de ressources en grappe d'application.
   - L'adresse de relais est démarrée par la mise en grappe du noeud spécifié et RIP promeut les routes dans la totalité du domaine de reprise. Il faut jusqu'à 5 minutes à RIP pour mettre à jour les routes dans le domaine. La fonction RIP est indépendante de la fonction de groupe de ressources en grappe de démarrage.

Important :

- Si la procédure indiquée ci-dessus n'est pas suivie pour tous les noeuds de grappe du domaine de reprise du groupe de ressources en grappe d'application, la grappe s'arrêtera pendant le processus de basculement.
- Même si vous n'effectuez pas une reprise en ligne vers les noeuds de réplique, il est astucieux d'effectuer la procédure sur ces noeuds au cas où ces derniers deviendraient une sauvegarde ultérieurement.
- Si vous voulez utiliser plusieurs adresses IP, chacune d'elle exigera un groupe de ressources en grappe d'application distinct et une adresse IP différente à laquelle l'associer. Cette adresse peut être une autre adresse IP logique se trouvant sur le même adaptateur physique ou il peut s'agir tout simplement d'un autre adaptateur physique. Vous devez également veiller à ne pas créer d'ambiguïtés dans les tables de routage. Pour y parvenir, suivez la procédure ci-dessous :
  - Ajoutez un *DFTROUTE à la table de routage pour chaque adresse IP virtuelle.
  - Pour utiliser plusieurs adresses IP, utilisez CFGTCP (option 2).
  - Définissez tous les paramètres, y compris le tronçon suivant, de la même façon pour atteindre le routeur choisi ; cependant, l'interface de liaison préférée doit être définie sur l'adresse IP du système locale associé à l'adresse IP virtuelle représentée par cette route.

Activation du basculement d'application via des sous-réseaux avec IPv6 :

En général, la mise en grappe nécessite que tous les noeuds de grappe du domaine de reprise d'un groupe de ressources en grappe d'application soient situés sur le même réseau local (qu'ils utilisent la même adresse de sous-réseau). Les services-ressources de mise en grappe prennent en charge une adresse IP de relais configurée par l'utilisateur lors de la configuration des groupes de ressources en grappe d'application.

Le protocole de résolution d'adresse (*Address Resolution Protocol - ARP*) est le protocole réseau sous-jacent utilisé pour basculer l'adresse IP de relais de l'application configurée à partir d'un noeud du domaine de reprise vers un autre. Pour activer le basculement d'application entre les sous-réseaux, vous devez utiliser la prise en charge des adresses IP virtuelles et le protocole de routage de données RIPng (Routing Information Protocol Next Generation) pour IPv6.

Les étapes de configuration manuelle suivantes sont nécessaires à l'activation de l'environnement de basculement. **Cet ensemble d'instructions doit être appliqué à tous les noeuds du domaine de reprise, et répété sur tous les autres noeuds de la grappe qui deviendront des noeuds du domaine de reprise du groupe de ressources en grappe d'application donné.**

1. Sélectionnez une adresse IP de relais IPv6 à utiliser par le groupe de ressources en grappe d'application.
   - Pour éviter toute confusion, cette adresse ne doit pas interférer avec d'autres adresses existantes utilisées par les noeuds de grappe ou les routeurs.
   - Il est recommandé de définir cette adresse avec un préfixe d'adresse IPv6 plus court que les autres adresses IPv6 qui partagent le même préfixe IPv6 afin de s'assurer que l'adresse appropriée sera choisie comme adresse source dans les paquets en sortie.
   - Ajoutez l'interface de relais (par exemple, 2001:0DB8:1234::1. Créez-la avec une description de ligne *VIRTUALIP, une transmission maximale de 1500 (tout nombre entre 576 et 16388), et un démarrage automatique définie sur *NO.
2. Créez la grappe et tous les groupes de ressources en grappe. Pour le groupe de ressources en grappe, spécifiez `QcstUserCfgsTakeoverIpAddr` dans le champ **Configuration de l'adresse IP de relais**. Ne lancez aucun groupe de ressources en grappe d'application.
3. Utilisez la commande Change RIP Attributes (CHGRIPA) pour définir les attributs du protocole RIPng. Exécutez la commande suivante : CHGRIPA AUTOSTART(*YES) IP6COND(*NEVER) IP6ACPDFT(*NO) IP6SNDONLY(*VIRTUAL).

4. Vérifiez qu'il existe une adresse de lien local IPv6 active sur le système. Une adresse de lien local IPv6 commence par ″fe80:″.
5. Utilisez la commande Add RIP Interface (ADDRIPIFC) pour ajouter une interface RIP utilisée par le serveur OMPROUTED afin de diffuser l'adresse virtuelle utilisée comme adresse IP de relais. Par exemple, si l'adresse de lien local IPv6 active est fe80::1, exécutez la commande suivante : ADDRIPIFC IFC('fe80::1') RCVDYNNET(*YES) SNDSTTRTE(*YES) SNDHOSTRTE(*YES) SNDONLY(*VIRTUAL).
6. Redémarrez le serveur OMPROUTED avec les commandes suivantes :
   a. ENDTCPSVR SERVER(*OMPROUTED) INSTANCE(*RIP)
   b. STRTCPSVR SERVER(*OMPROUTED) INSTANCE(*RIP)
7. Assurez-vous que tous les routeurs commerciaux du réseau qui connectent entre eux les réseaux locaux du domaine de reprise acceptent et affichent les routes hôte pour RIPng.
   - Il ne s'agit pas nécessairement du paramètre par défaut des routeurs. Le langage varie en fonction du fabricant du routeur mais les paramètres des interfaces RIPng doivent être définis de manière à envoyer les données via les routes hôtes et à les recevoir via les hôtes dynamiques.
   - Ceci s'applique aussi aux interfaces de routeur qui pointent vers les systèmes ainsi que vers les interfaces routeur à routeur.

   Remarque : N'utilisez pas une machine IBM i comme routeur dans cette configuration. Utilisez un routeur commercial (IBM ou autre) conçu pour le routage. Le routage IBM i ne peut pas être configuré pour gérer cette fonction.
8. Activez manuellement l'adresse de relais sur l'un des noeuds de grappe :
   a. Attendez 5 minutes pour que RIP propage les routes.
   b. Lancez une commande Ping sur l'adresse de relais à partir de tous les noeuds du domaine de reprise du groupe de ressources en grappe et de tous les clients sélectionnés sur les réseaux locaux qui utiliseront cette adresse.
   c. Assurez-vous à nouveau que l'adresse de relais est interrompue.

   (La mise en grappe démarrera l'adresse sur le noeud principal spécifié, une fois les groupes de ressources en grappe démarrés).
9. Démarrez les groupes de ressources en grappe d'application.
   - L'adresse de relais est démarrée par la mise en grappe du noeud spécifié et RIPng promeut les routes dans la totalité du domaine de reprise. Il faut jusqu'à 5 minutes à RIPng pour mettre à jour les routes dans le domaine. La fonction RIPng est indépendante de la fonction de groupe de ressources en grappe de démarrage.

Important :

- Si la procédure indiquée ci-dessus n'est pas suivie pour tous les noeuds de grappe du domaine de reprise du groupe de ressources en grappe d'application, la grappe s'arrêtera pendant le processus de basculement.
- Même si vous n'effectuez pas une reprise en ligne vers les noeuds de réplique, il est astucieux d'effectuer la procédure sur ces noeuds au cas où ces derniers deviendraient une sauvegarde ultérieurement.
- Si vous voulez utiliser plusieurs adresses IP, chacune d'elle exigera un groupe de ressources en grappe d'application distinct et une adresse IP différente à laquelle l'associer. Cette adresse peut être une autre adresse IP logique se trouvant sur le même adaptateur physique ou il peut s'agir tout simplement d'un autre adaptateur physique. Vous devez également veiller à ne pas créer d'ambiguïtés dans les tables de routage. Pour y parvenir, suivez la procédure ci-dessous :
  - Ajoutez un *DFTROUTE à la table de routage pour chaque adresse IP virtuelle.
  - Pour utiliser plusieurs adresses IP, utilisez CFGTCP (option 2).

– Définissez tous les paramètres, y compris le tronçon suivant, de la même façon pour atteindre le routeur choisi ; cependant, l'interface de liaison préférée doit être définie sur l'adresse IP du système locale associé à l'adresse IP virtuelle représentée par cette route.

Exemple : actions de reprise en ligne d'un groupe de ressources en grappe d'application

Cet exemple explique le fonctionnement d'un scénario de reprise en ligne. D'autres scénarios peuvent fonctionner différemment.

L'événement suivant se produit quand un groupe de ressources en grappe d'une application résiliente bascule en raison du dépassement du nombre de tentatives autorisées ou si le travail a été annulé :

- Le programme d'exit du groupe de ressources en grappe est appelé sur tous les noeuds actifs du domaine de reprise pour le groupe de ressources en grappe muni d'un code d'action de basculement. Ceci indique que les services-ressources de mise en grappe se préparent au basculement du point d'accès de l'application à la première sauvegarde.
- Les services-ressources de mise en grappe arrête la connexion IP (Internet Protocol) de relais sur le noeud principal.
- Les services-ressources de mise en grappe lance l'adresse IP de relais sur le premier noeud de sauvegarde (nouveau noeud principal).
- Les services-ressources de mise en grappe envoient un travail qui appelle le programme d'exit du groupe de ressources en grappe uniquement sur le nouveau noeud principal muni d'une code d'action de démarrage. Cette action redémarre l'application.

Concepts associés

«Gestion des adresses IP de relais des groupes de ressources en grappe d'application», à la page 7
Vous pouvez gérer les adresses IP de relais des groupes de ressources en grappe d'application à l'aide des services-ressources de mise en grappe. Vous pouvez également les gérer manuellement.

Exemple : programme d'exit d'application

Cet exemple de code contient un programme d'exit d'un groupe de ressources en grappe.

Vous pouvez trouver cet exemple de code dans la bibliothèque QUSRTOOL.

Remarque : En utilisant les exemples de codes, vous acceptez les termes des «Licence du code et informations de limitation de responsabilité», à la page 211.

```
/*****************************************************************************/
/*                                                                           */
/* Library:  QUSRTOOL                                                        */
/* File:     QATTSYSC                                                        */
/* Member:   TCSTAPPEXT                                                      */
/* Type:     ILE C                                                           */
/*                                                                           */
/* Description:                                                              */
/* This is an example application CRG exit program which gets called for    */
/* various cluster events or cluster APIs.  The bulk of the logic must      */
/* still be added because that logic is really dependent upon the unique    */
/* things that need to be done for a particular application.                */
/*                                                                           */
/* The intent of this example to to provide a shell which contains the      */
/* basics for building a CRG exit program.  Comments throughout the example*/
/* highlight the kinds of issues that need to be addressed by the real      */
/* exit program implementation.                                             */
/*                                                                           */
/* Every action code that applies to an application CRG is handled in this */
/* example.                                                                  */
/*                                                                           */
/* The tcstdtaara.h include is also shipped in the QUSRTOOL library.  See   */
/* the TCSTDTAARA member in the QATTSYSC file.                               */
/*                                                                           */
```

```
/* Change log:                                                          */
/* Flag Reason   Ver    Date   User Id   Description                     */
/* ____ _______ ______ ______ ____________________________________________ */
/* ...  D98332   v5r1m0 000509 ROCH     Initial creation.               */
/* $A1  P9950070 v5r2m0 010710 ROCH     Dataarea fixes                  */
/* $A2  D99055   v5r2m0 010913 ROCH     Added CancelFailover action code   */
/* $A3  D98854   v5r2m0 010913 ROCH     Added VerificationPhase action code*/
/* $A4  P9A10488 v5r3m0 020524 ROCH     Added example code to wait for data*/
/*                                      CRGs on switchover action code  */
/*                                                                      */
/************************************************************************/


/*----------------------------------------------------------------------*/
/*                                                                      */
/* Header files                                                         */
/*                                                                      */
/*----------------------------------------------------------------------*/
#include              /* Useful when debugging                  */
#include             /* offsetof macro                          */
#include             /* system function                         */
#include             /* String functions                        */
#include             /* Exception handling constants/structures  */
#include               /* Various cluster constants              */
#include           /* Structure of CRG information               */
#include "qusrtool/qattsysc/tcstdtaara" /* QCSTHAAPPI/QCSTHAAPPO data areas*/
#include           /* API to Retrieve contents of a data area     */
#include              /* API error code type definition          */
#include              /* mitime builtin                          */
#include           /* waittime builtin                           */


/*----------------------------------------------------------------------*/
/*                                                                      */
/* Constants                                                            */
/*                                                                      */
/*----------------------------------------------------------------------*/
#define UnknownRole -999
#define DependCrgDataArea "QCSTHAAPPO"
#define ApplCrgDataArea "QCSTHAAPPI"
#define Nulls 0x0000000000000000000


/*----------------------------------------------------------------------*/
/*                                                                      */
/* The following constants are used in the checkDependCrgDataArea()     */
/* function.  The first defines how long to sleep before checking the data */
/* area.  The second defines that maximum time to wait for the data area   */
/* to become ready before failing to start the application when the Start  */
/* CRG function is being run.  The third defines the maximum wait time for */
/* the Initiate Switchover or failover functions.                       */
/*                                                                      */
/*----------------------------------------------------------------------*/
#define WaitSecondsIncrement 30
#define MaxStartCrgWaitSeconds 0
#define MaxWaitSeconds 900

/*----------------------------------------------------------------------*/
/*                                                                      */
/* As this exit program is updated to handle new action codes, change the  */
/* define below to the value of the highest numbered action code that is   */
/* handled.                                                             */
/*                                                                      */
/*----------------------------------------------------------------------*/
#define MaxAc 21

/*----------------------------------------------------------------------*/
```

```
/*                                                                    */
/* If the exit program data in the CRG has a particular structure to it,   */
/* include the header file for that structure definition and change the    */
/* define below to use that structure name rather than char.              */
/*                                                                    */
/*--------------------------------------------------------------------*/
#define EpData char

/*--------------------------------------------------------------------*/
/*                                                                    */
/* Change the following define to the library the application resides in   */
/* and thus where the QCSTHAAPPO and QCSTHAAPPI data areas will be found.  */
/*                                                                    */
/*--------------------------------------------------------------------*/
#define ApplLib "QGPL"


/*--------------------------------------------------------------------*/
/*                                                                    */
/* Prototypes for internal functions.                                 */
/*                                                                    */
/*--------------------------------------------------------------------*/
static int getMyRole(Qcst_EXTP0100_t *, int, int);
#pragma argopt(getMyRole)
static int doAction(int, int, int, Qcst_EXTP0100_t *, EpData *);
#pragma argopt(doAction)
static int createCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int startCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int restartCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int endCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int verifyPhase(int, int, Qcst_EXTP0100_t *, EpData *);
static int deleteCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int memberIsJoining(int, int, Qcst_EXTP0100_t *, EpData *);
static int memberIsLeaving(int, int, Qcst_EXTP0100_t *, EpData *);
static int switchPrimary(int, int, Qcst_EXTP0100_t *, EpData *);
static int addNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int rmvNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int chgCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int deleteCrgWithCmd(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoPriorAction(int, int, Qcst_EXTP0100_t *, EpData *);
static int endNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int chgNodeStatus(int, int, Qcst_EXTP0100_t *, EpData *);
static int cancelFailover(int, int, Qcst_EXTP0100_t *, EpData *);
static int newActionCode(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoCreateCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoStartCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoEndCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoMemberIsJoining(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoMemberIsLeaving(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoSwitchPrimary(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoAddNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoRmvNode(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoChgCrg(int, int, Qcst_EXTP0100_t *, EpData *);
static int undoCancelFailover(int, int, Qcst_EXTP0100_t *, EpData *);
static void bldDataAreaName(char *, char *, char *);
#pragma argopt(bldDataAreaName)
static int checkDependCrgDataArea(unsigned int);
#pragma argopt(checkDependCrgDataArea)
static void setApplCrgDataArea(char);
#pragma argopt(setApplCrgDataArea)
static void cancelHandler(_CNL_Hndlr_Parms_T *);
static void unexpectedExceptionHandler(_INTRPT_Hndlr_Parms_T *);
static void endApplication(unsigned int, int, int, Qcst_EXTP0100_t *, EpData *);
#pragma argopt(endApplication)

/*--------------------------------------------------------------------*/
/*                                                                    */
```

```
/* Some debug routines                                                    */
/*                                                                        */
/*------------------------------------------------------------------------*/
static void printParms(int, int, int, Qcst_EXTP0100_t *, EpData *);
static void printActionCode(unsigned int);
static void printCrgStatus(int);
static void printRcvyDomain(char *,
                            unsigned int,
                            Qcst_Rcvy_Domain_Array1_t *);
static void printStr(char *, char *, unsigned int);


/*------------------------------------------------------------------------*/
/*                                                                        */
/* Type definitions                                                       */
/*                                                                        */
/*------------------------------------------------------------------------*/

/*------------------------------------------------------------------------*/
/*                                                                        */
/* This structure defines data that will be passed to the exception and   */
/* cancel handlers.  Extend it with information unique to your application.*/
/*                                                                        */
/*------------------------------------------------------------------------*/
typedef struct {
  int *retCode;             /* Pointer to return code                     */
  EpData *epData;           /* Exit program data from the CRG             */
  Qcst_EXTP0100_t *crgData; /* CRG data                                   */
  unsigned int actionCode;  /* The action code                            */
  int role;                 /* This node's recovery domain role           */
  int priorRole;            /* This node's prior recovery domainrole      */
} volatile HandlerDataT;


/*------------------------------------------------------------------------*/
/*                                                                        */
/* Function pointer array for handling action codes.  When the exit program*/
/* is updated to handle new action codes, add the new function names to   */
/* this function pointer array.                                           */
/*                                                                        */
/*------------------------------------------------------------------------*/
static int (*fcn[MaxAc+1]) (int role,
                            int priorRole,
                            Qcst_EXTP0100_t *crgData,
                            EpData *epData) = {
  newActionCode,   /* 0 - currently reserved */
  createCrg,       /* 1  */
  startCrg,        /* 2  */
  restartCrg,      /* 3  */
  endCrg,          /* 4  */
  verifyPhase,     /* 5 - currently reserved */
  newActionCode,   /* 6 - currently reserved */
  deleteCrg,       /* 7  */
  memberIsJoining, /* 8  */
  memberIsLeaving, /* 9  */
  switchPrimary,   /* 10 */
  addNode,         /* 11 */
  rmvNode,         /* 12 */
  chgCrg,          /* 13 */
  deleteCrgWithCmd,/* 14 */
  undoPriorAction, /* 15 */
  endNode,         /* 16 */
  newActionCode,   /* 17 - applies only to a device CRG */
  newActionCode,   /* 18 - applies only to a device CRG */
  newActionCode,   /* 19 - applies only to a device CRG */
  chgNodeStatus,   /* 20 */
  cancelFailover   /* 21 */
```

```
};

/*--------------------------------------------------------------------------*/
/*                                                                          */
/* Function pointer array for handling prior action codes when called with */
/* the Undo action code.  When the exit program is updated to handle       */
/* Undo for new action codes, add the new function names to this function  */
/* pointer array.                                                           */
/*                                                                          */
/*--------------------------------------------------------------------------*/
static int (*undoFcn[MaxAc+1]) (int role,
                                int priorRole,
                                Qcst_EXTP0100_t *crgData,
                                EpData *epData) = {
  newActionCode,       /* 0 - currently reserved */
  undoCreateCrg,       /* 1  */
  undoStartCrg,        /* 2  */
  newActionCode,       /* 3  */
  undoEndCrg,          /* 4  */
  newActionCode,       /* 5 - no undo for this action code */
  newActionCode,       /* 6 - currently reserved */
  newActionCode,       /* 7  */
  undoMemberIsJoining, /* 8  */
  undoMemberIsLeaving, /* 9  */
  undoSwitchPrimary,   /* 10 */
  undoAddNode,         /* 11 */
  undoRmvNode,         /* 12 */
  undoChgCrg,          /* 13 */
  newActionCode,       /* 14 */
  newActionCode,       /* 15 */
  newActionCode,       /* 16 */
  newActionCode,       /* 17 - applies only to a device CRG */
  newActionCode,       /* 18 - applies only to a device CRG */
  newActionCode,       /* 19 - applies only to a device CRG */
  newActionCode,       /* 20 */
  undoCancelFailover   /* 21 */
};


/****************************************************************************/
/*                                                                          */
/* This is the entry point for the exit program.                            */
/*                                                                          */
/****************************************************************************/
void main(int argc, char *argv[]) {

  HandlerDataT hdlData;


/*--------------------------------------------------------------------------*/
  /*                                                                        */
  /* Take each of the arguments passed in the argv array and castit to      */
  /* the correct data type.                                                 */
  /*                                                                        */

/*--------------------------------------------------------------------------*/
  int *retCode    = (int *)argv[1];
  unsigned int *actionCode = (unsigned int *)argv[2];
  EpData *epData           = (EpData *)argv[3];
  Qcst_EXTP0100_t *crgData = (Qcst_EXTP0100_t *)argv[4];
  char *formatName         = (char *)argv[5];


/*--------------------------------------------------------------------------*/
  /*                                                                        */
```

```
  /* Ensure the format of the data being passed is correct.  */
  /* If not, a change has been made and this exit program needs tobe      */
  /* updated to accomodate the change.  Add appropriate errorlogging for  */
  /* your application design.                                             */
  /*                                                                      */

/*----------------------------------------------------------------------*/
  if (0 != memcmp(formatName, "EXTP0100", 8))
    abort();


/*----------------------------------------------------------------------*/
  /*                                                                      */
  /* Set up the data that will be passed to the exception andcancel       */
  /* handlers.                                                            */
  /*                                                                      */

/*----------------------------------------------------------------------*/
  hdlData.retCode    = retCode;
  hdlData.epData     = epData;
  hdlData.crgData    = crgData;
  hdlData.actionCode = *actionCode;
  hdlData.role       = UnknownRole;
  hdlData.priorRole  = UnknownRole;
  _VBDY();  /* force changed variables to home storage location           */


/*----------------------------------------------------------------------*/
  /*                                                                      */
  /* Enable an exception handler for any and all exceptions.              */
  /*                                                                      */

/*----------------------------------------------------------------------*/
#pragma exception_handler(unexpectedExceptionHandler, hdlData, \
                          _C1_ALL, _C2_ALL, _CTLA_INVOKE )


/*----------------------------------------------------------------------*/
  /*                                                                      */
  /* Enable a cancel handler to recover if this job is canceled.         */
  /*                                                                      */

/*----------------------------------------------------------------------*/
#pragma cancel_handler(cancelHandler, hdlData)


/*----------------------------------------------------------------------*/
  /*                                                                      */
  /* Extract the role and prior role of the node this exit program is     */
  /* running on.  If the cluster API or event changes the recovery domain  */
  /* (node role or membership status), the new recovery domain's offset is */
  /* passed in Offset_Rcvy_Domain_Array and the offset of the recovery     */
  /* domain as it looked prior to the API or cluster event is passed in    */
  /* Offset_Prior_Rcvy_Domain_Array.  If the recovery domain isn't changed,*/
  /* only Offset_Rcvy_Domain_Array can be used to address the recovery     */
  /* domain.                                                              */
  /*                                                                      */

/*----------------------------------------------------------------------*/
  hdlData.role = getMyRole(crgData,
                           crgData->Offset_Rcvy_Domain_Array,
                           crgData->Number_Nodes_Rcvy_Domain);
  if (crgData->Offset_Prior_Rcvy_Domain_Array)
    hdlData.priorRole =
                  getMyRole(crgData,

crgData->Offset_Prior_Rcvy_Domain_Array,
```

```
crgData->Number_Nodes_Prior_Rcvy_Domain);
  else
    hdlData.priorRole = hdlData.role;
  _VBDY();  /* force changed variables to home storage location          */


/*--------------------------------------------------------------------------*/
  /*                                                                        */
  /* Enable the following to print out debug information.                   */
  /*                                                                        */

/*--------------------------------------------------------------------------*/
  /*
  printParms(*actionCode, hdlData.role, hdlData.priorRole, crgData,
epData);
  */


/*--------------------------------------------------------------------------*/
  /*                                                                        */
  /* Do the correct thing based upon the action code.  The return code      */
  /* is set to the function result of doAction().                           */
  /*                                                                        */

/*--------------------------------------------------------------------------*/
  *retCode = doAction(*actionCode,
                      hdlData.role,
                      hdlData.priorRole,
                      crgData,
                      epData);


/*--------------------------------------------------------------------------*/
  /*                                                                        */
  /* The exit program job will end when control returns to the operating    */
  /* system at this point.                                                  */
  /*                                                                        */

/*--------------------------------------------------------------------------*/
  return;

#pragma disable_handler  /* unexpectedExceptionHandler                    */
#pragma disable_handler  /* cancelHandler                                 */
}  /* end main()                                                          */


/****************************************************************************/
/*                                                                          */
/* Get the role of this particular node from one of the views of the        */
/* recovery domain.                                                         */
/*                                                                          */
/* APIs and cluster events which pass the updated and prior recovery domain*/
/* to the exit program are:                                                 */
/* QcstAddNodeToRcvyDomain                                                  */
/* QcstChangeClusterNodeEntry                                               */
/* QcstChangeClusterResourceGroup                                           */
/* QcstEndClusterNode (ending node does not get the prior domain)           */
/* QcstInitiateSwitchOver                                                   */
/* QcstRemoveClusterNodeEntry (removed node does not get the prior domain) */
/* QcstRemoveNodeFromRcvyDomain                                             */
/* QcstStartClusterResourceGroup (only if inactive backup nodes are         */
/*                                reordered)                                */
/* a failure causing failover                                               */
/* a node rejoining the cluster                                             */
/* cluster partitions merging                                               */
/*                                                                          */
```

```
/* All other APIs pass only the updated recovery domain.                  */
/*                                                                        */
/**************************************************************************/
static int getMyRole(Qcst_EXTP0100_t *crgData, int offset, int
count) {

  Qcst_Rcvy_Domain_Array1_t *nodeData;
  unsigned int iter = 0;


/*------------------------------------------------------------------------*/
  /*                                                                      */
  /* Under some circumstances, the operating system may not be able to    */
  /* determine the ID of this node and passes *NONE.  An example of such a */
  /* circumstance is when cluster resource services is not active on a    */
  /* node and the DLTCRG CL command is used.                              */
  /*                                                                      */

/*------------------------------------------------------------------------*/
  if (0 == memcmp(crgData->This_Nodes_ID, QcstNone,
sizeof(Qcst_Node_Id_t)))
    return UnknownRole;


/*------------------------------------------------------------------------*/
  /*                                                                      */
  /* Compute a pointer to the first element of the recovery domain array.  */
  /*                                                                      */

/*------------------------------------------------------------------------*/
  nodeData = (Qcst_Rcvy_Domain_Array1_t *)((char *)crgData +
offset);


/*------------------------------------------------------------------------*/
  /*                                                                      */
  /* Find my node in the recovery domain array.  I will not be in the     */
  /* prior recovery domain if I am being added by the Add Node to Recovery */
  /* Domain API.                                                          */
  /*                                                                      */

/*------------------------------------------------------------------------*/
  while (  0 != memcmp(crgData->This_Nodes_ID,
                       nodeData->Node_ID,
                       sizeof(Qcst_Node_Id_t))
         &&
           iter &lt; count
        ) {
    nodeData++;
    iter++;
  }

  if (iter &lt; count)
    return nodeData->Node_Role;
  else
    return UnknownRole;
}  /* end getMyRole()                                                     */


/**************************************************************************/
/*                                                                        */
/* Call the correct function based upon the cluster action code.  The     */
/* doAction() function was split out from main() in order to clarify the  */
/* example.  See the function prologues for each called function for      */
/* information about a particular cluster action.                         */
/*                                                                        */
/* Each action code is split out into a separate function only to help    */
```

```
/* clarify this example.  For a particular exit program, some action codes */
/* may perform the same function in which case multiple action codes could */
/* be handled by the same function.                                        */
/*                                                                         */
/***************************************************************************/
static int doAction(int actionCode,
                    int role,
                    int priorRole,
                    Qcst_EXTP0100_t *crgData,
                    EpData *epData) {


/*-------------------------------------------------------------------------*/
  /*                                                                       */
  /* For action codes this exit program knows about, call a function to    */
  /* do the work for that action code.                                     */
  /*                                                                       */

/*-------------------------------------------------------------------------*/

  if (actionCode &lt;= MaxAc )
    return (*fcn[actionCode]) (role, priorRole, crgData, epData);
  else

/*-------------------------------------------------------------------------*/
    /*                                                                     */
    /* IBM has defined a new action code in a new operating system release */
    /* and this exit program has not yet been updated to handle it.  Take a*/
    /* default action for now.                                             */
    /*                                                                     */

/*-------------------------------------------------------------------------*/
    return newActionCode(role, priorRole, crgData, epData);
}  /* end doAction()                                                       */


/***************************************************************************/
/*                                                                         */
/* Action code = QcstCrgAcInitialize                                       */
/*                                                                         */
/* The QcstCreateClusterResourceGroup API was called.  A new cluster       */
/* resource group object is being created.                                 */
/*                                                                         */
/* Things to consider:                                                     */
/*   - Check that the application program and all associated objects are on*/
/*     the primary and backup nodes.  If the objects are not there,        */
/*     consider sending error/warning messages or return a failure return  */
/*     code.                                                               */
/*   - Check that required data or device CRGs are on all nodes in the     */
/*     recovery domain.                                                    */
/*   - Perform any necessary setup that is required to run the             */
/*     the application on the primary or backup nodes.                     */
/*   - If this CRG is enabled to use the QcstDistributeInformation API,    */
/*     the user queue needed by that API could be created at this time.    */
/*                                                                         */
/***************************************************************************/
static int createCrg(int role,
                     int doesNotApply,
                     Qcst_EXTP0100_t *crgData,
                     EpData *epData) {

  return QcstSuccessful;
}  /* end createCrg()                                                      */


/***************************************************************************/
/*                                                                         */
```

```
/* Action code = QcstCrgAcStart                                          */
/*                                                                       */
/* The QcstStartClusterResourceGroup API was called.  A cluster resource   */
/* group is being started.                                               */
/* The QcstInitiateSwitchOver API was called and this is the second action */
/* code being passed to the exit program.                                */
/* The fail over event occurred and this is the second action code being   */
/* passed to the exit program.                                           */
/*                                                                       */
/* A maximum wait time is used when checking to see if all dependent CRGs  */
/* are active.  This is a short time if the CRG is being started because of*/
/* the QcstStartClusterResourceGroup API.  It is a longer time if it is    */
/* because of a failover or switchover.  When failover or switchover are   */
/* being done, it make take a while for data or device CRGs to become      */
/* ready so the wait time is long.  If the Start CRG API is being used, the*/
/* dependent CRGs should already be started or some error occurred, the    */
/* CRGs were started out of order, etc. and there is no need for a long    */
/* wait.                                                                 */
/*                                                                       */
/* Things to consider:                                                   */
/*   - If this node's role is primary, the application should be started.  */
/*     This exit program should either call the application so that it runs*/
/*     in this same job or it should monitor any job started by this       */
/*     exit program so the exit program knows when the application job     */
/*     ends.  By far, the simplest approach is run the application in this */
/*     job by calling it.                                                */
/*     Cluster Resource Services is not expecting this exit program to     */
/*     return until the application finishes running.                    */
/*   - If necessary, start any associated subsystems, server jobs, etc.    */
/*   - Ensure that required data CRGs have a status of active on all nodes */
/*     in the recovery domain.                                           */
/*                                                                       */
/*************************************************************************/
static int startCrg(int role,
                    int doesNotApply,
                    Qcst_EXTP0100_t *crgData,
                    EpData *epData) {

  unsigned int maxWaitTime;

  /* Start the application if this node is the primary                   */
  if (role == QcstPrimaryNodeRole) {

/*-----------------------------------------------------------------------*/
    /*                                                                   */
    /* Determine if all CRGs that this application CRG is dependent upon   */
    /* are ready.  If the check fails, return from the Start action code.  */
    /* Cluster Resource Services will change the state of the CRG to       */
    /* Inactive.                                                         */
    /*                                                                   */

/*-----------------------------------------------------------------------*/
    if (crgData->Cluster_Resource_Group_Status ==
QcstCrgStartCrgPending)
      maxWaitTime = MaxStartCrgWaitSeconds;
    else
      maxWaitTime = MaxWaitSeconds;
    if (QcstSuccessful != checkDependCrgDataArea(maxWaitTime))
      return QcstSuccessful;



/*-----------------------------------------------------------------------*/
    /*                                                                   */
    /* Just before starting the application, update the data area to       */
    /* indicate the application is running.                              */
    /*                                                                   */
```

```
/*--------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Running);


/*--------------------------------------------------------------------*/
    /*                                                                */
    /* Add logic to call application here.  It is expected that control    */
    /* will not return until something causes the application to end: a    */
    /* normal return from the exit program, the job is canceled, or an    */
    /* unhandled exception occurs.  See the cancelHandler() function for   */
    /* some common ways this job could be canceled.                       */
    /*                                                                */

/*--------------------------------------------------------------------*/




/*--------------------------------------------------------------------*/
    /*                                                                */
    /* After the application has ended normally, update the data area to   */
    /* indicate the application is no longer running.                     */
    /*                                                                */

/*--------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Ended);
  }
  else

/*--------------------------------------------------------------------*/
    /*                                                                */
    /* On backup or replicate nodes, mark the status of the application in */
    /* the data area as not running.                                      */
    /*                                                                */

/*--------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Ended);


  return QcstSuccessful;
}  /* end startCrg()
       */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgAcRestart                                     */
/*                                                                    */
/* The previous call of the exit program failed and set the return   */
/* code to QcstFailWithRestart or it failed due to an exception and the    */
/* exception was allowed to percolate up the call stack.  In either  */
/* case, the maximum number of times for restarting the exit program has   */
/* not been reached yet.                                              */
/*                                                                    */
/* This action code is passed only to application CRG exit programs which  */
/* had been called with the Start action code.                        */
/*                                                                    */
/**********************************************************************/
static int restartCrg(int role,
                      int doesNotApply,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {


/*--------------------------------------------------------------------*/
  /*                                                                */
```

```
  /* Perform any unique logic that may be necessary when restarting the    */
  /* application after a failure and then call the startCrg() function to  */
  /* do the start functions.                                               */
  /*                                                                       */

/*-----------------------------------------------------------------------*/


  return startCrg(role, doesNotApply, crgData, epData);
}  /* end restartCrg()                                                   */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcEnd                                            */
/*                                                                       */
/* The end action code is used for one of the following reasons:         */
/*   - The QcstEndClusterResourceGroup API was called.                   */
/*   - The cluster has become partitioned and this node is in the secondary*/
/*     partition.  The End action code is used regardless of whether the   */
/*     CRG was active or inactive.  Action code dependent data of          */
/*     QcstPartitionFailure will also be passed.                         */
/*   - The application ended.   Action code dependent data of            */
/*     QcstResourceEnd will also be passed.  All nodes in the recovery     */
/*     domain will see the same action code (including the primary).       */
/*   - The CRG job has been canceled.  The exit program on this node will */
/*     be called with the End action code.  QcstMemberFailure will be      */
/*     passed as action code dependent data.                             */
/*                                                                       */
/*                                                                       */
/*                                                                       */
/* Things to consider:                                                   */
/*   - If the CRG is active, the job running the application is canceled  */
/*     and the IP takeover address is ended AFTER the exit program is      */
/*     called.                                                           */
/*   - If subsystems or server jobs were started as a result of the        */
/*     QcstCrgAcStart action code, end them here or consolidate all logic  */
/*     to end the application in the cancelHandler() since it will be      */
/*     invoked for all Cluster Resource Services APIs which must end the   */
/*     application on the current primary.                               */
/*                                                                       */
/*************************************************************************/
static int endCrg(int role,
                  int priorRole,
                  Qcst_EXTP0100_t *crgData,
                  EpData *epData) {


/*-----------------------------------------------------------------------*/
  /*                                                                       */
  /* End the application if it is running on this node.                    */
  /*                                                                       */

/*-----------------------------------------------------------------------*/
  endApplication(QcstCrgAcRemoveNode, role, priorRole, crgData,
epData);

  return QcstSuccessful;
}  /* end endCrg()                                                       */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcVerificationPhase                              */
/*                                                                       */
/* The verification phase action code is used to allow the exit program to */
/* do some verification before proceeding with the requested function      */
```

```
/* identified by the action code depended data. If the exit program        */
/* determines that the requested function cannot proceed it should return  */
/* QcstFailWithOutRestart.                                                 */
/*                                                                         */
/*                                                                         */
/* NOTE: The exit program will NOT be called with Undo action code.        */
/*                                                                         */
/***************************************************************************/
static int verifyPhase(int role,
                       int doesNotApply,
                       Qcst_EXTP0100_t *crgData,
                       EpData *epData) {


/*-------------------------------------------------------------------------*/
  /*                                                                       */
  /* Do verification                                                       */
  /*                                                                       */

/*-------------------------------------------------------------------------*/
  if (crgData->Action_Code_Dependent_Data == QcstDltCrg) {
        /* do verification  */
        /* if ( fail ) */
          /* return QcstFailWithOutRestart */
  }

  return QcstSuccessful;
}  /* end verifyPhase()                                                    */


/***************************************************************************/
/*                                                                         */
/* Action code = QcstCrgAcDelete                                           */
/*                                                                         */
/* The QcstDeleteClusterResourceGroup or QcstDeleteCluster API was called. */
/* A cluster resource group is being deleted while Cluster Resource        */
/* Services is active.                                                     */
/* If the QcstDeleteCluster API was used, action code dependent data of    */
/* QcstDltCluster is passed.                                               */
/* If the QcstDeleteCluster API was used and the CRG is active, the exit   */
/* program job which is still active for the Start action code is canceled*/
/* after the Delete action code is processed.                              */
/*                                                                         */
/* Things to consider:                                                     */
/*   - Delete application programs and objects from nodes where they are   */
/*     no longer needed such as backup nodes.  Care needs to be exercised  */
/*     when deleting application objects just because a CRG is being       */
/*     deleted since a particular scenario may want to leave the           */
/*     application objects on all nodes.                                   */
/*                                                                         */
/***************************************************************************/
static int deleteCrg(int role,
                     int doesNotApply,
                     Qcst_EXTP0100_t *crgData,
                     EpData *epData) {

  return QcstSuccessful;
}  /* end deleteCrg()
       */


/***************************************************************************/
/*                                                                         */
/* Action code = QcstCrgAcReJoin                                           */
/*                                                                         */
/* One of three things is occurring-                                       */
/*  1. The problem which caused the cluster to become partitioned has been */
```

```
/*     corrected and the 2 partitions are merging back together to become  */
/*     a single cluster.  Action code dependent data of QcstMerge will be  */
/*     passed.                                                             */
/*  2. A node which either previously failed or which was ended has had    */
/*     cluster resource services started again and the node is joining the */
/*     cluster.  Action code dependent data of QcstJoin will be passed.    */
/*  3. The CRG job on a particular node which may have been canceled or   */
/*     ended has been restarted.  Action code dependent data of QcstJoin   */
/*     will be passed.                                                     */
/*                                                                         */
/* Things to consider:                                                     */
/*   - If the application replicates application state information to other*/
/*     nodes when the application is running, this state information will  */
/*     need to be resynchronized with the joining nodes if the CRG is      */
/*     active.                                                             */
/*   - Check for missing application objects on the joining nodes.         */
/*   - Ensure the required data CRGs are on the joining nodes.             */
/*   - If the application CRG is active, ensure the required data CRGs are */
/*     active.                                                             */
/*                                                                         */
/*-------------------------------------------------------------------------*/
static int memberIsJoining(int role,
                           int priorRole,
                           Qcst_EXTP0100_t *crgData,
                           EpData *epData) {


/*-------------------------------------------------------------------------*/
  /*                                                                       */
  /* Ensure the data area status on this node starts out indicating      */
  /* the application is not running if this node is not the primary.     */
  /*                                                                       */

/*-------------------------------------------------------------------------*/
  if (role != QcstPrimaryNodeRole) {
    setApplCrgDataArea(Appl_Ended);
  }


/*-------------------------------------------------------------------------*/
  /*                                                                       */
  /* If a single node is rejoining the cluster, you may do a certain set of*/
  /* actions.  Whereas if the nodes in a cluster which became partitioned  */
  /* are merging back together, you may have a different set of actions.   */
  /*                                                                       */

/*-------------------------------------------------------------------------*/
  if (crgData->Action_Code_Dependent_Data == QcstJoin) {
    /* Do actions for a node joining.                                      */
  }
  else {
    /* Do actions for partitions merging.                                  */
  }

  return QcstSuccessful;
}  /* end memberIsJoining()                                               */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcFailover                                       */
/*                                                                       */
/* Cluster resource services on a particular node(s) has failed or ended   */
/* for this cluster resource group.  The Failover action code is passed    */
/* regardless of whether the CRG is active or inactive.  Failover can      */
/* happen for a number of reasons:                                       */
/*                                                                       */
```

```
/*   - an operator canceled the CRG job on a node.  Action code dependent */
/*     data of QcstMemberFailure will be passed.                          */
/*   - cluster resource services was ended on the node (for example, the   */
/*     QSYSWRK subsystem was ended with CRS still active).  Action code    */
/*     dependent data of QcstNodeFailure will be passed.                  */
/*   - the application for an application CRG has failed on the primary    */
/*     node and could not be restarted there.  The CRG is Active.         */
/*     Action code dependent data of QcstApplFailure will be passed.      */
/*   - the node failed (such as a power failure).  Action code dependent   */
/*     data of QcstNodeFailure will be passed.                            */
/*   - The cluster has become partitioned due to some communication failure*/
/*     such as a communication line or LAN failure.  The Failover action   */
/*     code is passed to recovery domain nodes in the majority partition.  */
/*     Nodes in the minority partition see the End action code.  Action    */
/*     code dependent data of QcstPartitionFailure will be passed.        */
/*   - A node in the CRG's recovery domain is being ended with the         */
/*     QcstEndClusterNode API.  The node being ended will see the End Node */
/*     action code.  All other nodes in the recovery domain will see the   */
/*     Failover action code.  Action code dependent data of QcstEndNode    */
/*     will be passed for the Failover action code.                       */
/*   - An active recovery domain node for an active CRG is being removed   */
/*     from the cluster with the QcstRemoveClusterNodeEntry API.   Action  */
/*     code dependent data of QcstRemoveNode will be passed.  If an        */
/*     inactive node is removed for an active CRG, or if the CRG is        */
/*     inactive, an action code of Remove Node is passed.                 */
/*                                                                        */
/* The exit program is called regardless of whether or not the CRG is     */
/* active.  The exit program may have nothing to do if the CRG is not     */
/* active.                                                                */
/*                                                                        */
/* If the CRG is active and the leaving member was the primary node,      */
/* perform the functions necessary for failover to a new primary.         */
/*                                                                        */
/* The Action_Code_Dependent_Data field can be used to determine if:      */
/*  - the failure was due to a problem that caused the cluster to become   */
/*     partitioned (all CRGs which had the partitioned nodes in the       */
/*     recovery domain are affected)                                      */
/*  - a node failed or had cluster resource services ended on the node (all*/
/*    CRGs which had the failed/ended node in the recovery  domain are     */
/*    affected)                                                           */
/*  - only a single CRG was affected (for example a single CRG job was     */
/*    canceled on a node or a single application failed)                 */
/*                                                                        */
/*                                                                        */
/* Things to consider:                                                    */
/*   - Prepare the new primary node so the application can be started.    */
/*   - The application should NOT be started at this time.  The exit      */
/*     program will be called again with the QcstCrgAcStart action code if */
/*     the CRG was active when the failure occurred.                      */
/*   - If the application CRG is active, ensure the required data CRGs are */
/*     active.                                                            */
/*                                                                        */
/**************************************************************************/
static int memberIsLeaving(int role,
                           int priorRole,
                           Qcst_EXTP0100_t *crgData,
                           EpData *epData) {


/*------------------------------------------------------------------------*/
  /*                                                                      */
  /* If the CRG is active, perform failover.  Otherwise, nothing to do.   */
  /*                                                                      */

/*------------------------------------------------------------------------*/
  if (crgData->Original_Cluster_Res_Grp_Stat == QcstCrgActive) {
```

```
/*--------------------------------------------------------------------*/
    /*                                                                */
    /* The CRG is active.  Determine if my role has changed and I am now  */
    /* the new primary.                                               */
    /*                                                                */

/*--------------------------------------------------------------------*/

    if (priorRole != role && role == QcstPrimaryNodeRole) {


/*--------------------------------------------------------------------*/
      /*                                                              */
      /* I was not the primary but am now.  Do failover actions but don't  */
      /* start the application at this time because this exit program will */
      /* be called again with the Start action code.                  */
      /*                                                              */

/*--------------------------------------------------------------------*/


/*--------------------------------------------------------------------*/
      /*                                                              */
      /* Ensure the data area status on this node starts out indicating    */
      /* the application is not running.                              */
      /*                                                              */

/*--------------------------------------------------------------------*/
      setApplCrgDataArea(Appl_Ended);


/*--------------------------------------------------------------------*/
      /*                                                              */
      /* If the application has no actions to do on the Start action code  */
      /* and will become active as soon as the takeover IP address is      */
      /* activated, then this code should be uncommented.  This code will  */
      /* determine if all CRGs that this application CRG is dependent upon */
      /* are ready.  If this check fails, return failure from the action   */
      /* code.                                                        */
      /*                                                              */

/*--------------------------------------------------------------------*/
/*      if (QcstSuccessful != checkDependCrgDataArea(MaxWaitSeconds))  */
/*         return QcstFailWithOutRestart;                              */

    }
  }

  return QcstSuccessful;
}  /* end memberIsLeaving()                                           */


/************************************************************************/
/*                                                                      */
/* Action code = QcstCrgAcSwitchover                                    */
/*                                                                      */
/* The QcstInitiateSwitchOver API was called.  The first backup node in    */
/* the cluster resource group's recovery domain is taking over as the      */
/* primary node and the current primary node is being made the last backup.*/
/*                                                                      */
/* Things to consider:                                                  */
/*   - Prepare the new primary node so the application can be started.     */
/*   - The application should NOT be started at this time.  The exit       */
/*     program will be called again with the QcstCrgAcStart action code.   */
/*   - The job running the application is canceled and the IP takeover    */
/*     address is ended prior to the exit program being called on the      */
```

```
/*     current primary.                                                     */
/*   - Ensure required data or device CRGs have switched over and are       */
/*     active.                                                              */
/*                                                                          */
/****************************************************************************/
static int switchPrimary(int role,
                         int priorRole,
                         Qcst_EXTP0100_t *crgData,
                         EpData *epData) {


/*--------------------------------------------------------------------------*/
  /*                                                                        */
  /* See if I am the old primary.                                           */
  /*                                                                        */

/*--------------------------------------------------------------------------*/
  if (priorRole == QcstPrimaryNodeRole) {

/*--------------------------------------------------------------------------*/
    /*                                                                      */
    /* Do what ever needs to be done to cleanup the old primary before the */
    /* switch.  Remember that that job which was running the exit program  */
    /* which started the application was canceled already.                */
    /*                                                                      */
    /* One example may be to clean up any processes holding locks on the   */
    /* database.  This may have been done by the application cancel        */
    /* handler if one was invoked.                                          */

/*--------------------------------------------------------------------------*/
  }


/*--------------------------------------------------------------------------*/
  /*                                                                        */
  /* I'm not the old primary.  See if I'm the new primary.                  */
  /*                                                                        */

/*--------------------------------------------------------------------------*/
  else if (role == QcstPrimaryNodeRole) {

/*--------------------------------------------------------------------------*/
    /*                                                                      */
    /* Do what ever needs to be done on the new primary before the         */
    /* application is started with the QcstCrgAcStart action code.         */
    /*                                                                      */

/*--------------------------------------------------------------------------*/


/*--------------------------------------------------------------------------*/
    /*                                                                      */
    /* Ensure the data area status on this nodes starts out indicating     */
    /* the application is not running.                                      */
    /*                                                                      */

/*--------------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Ended);


/*--------------------------------------------------------------------------*/
    /*                                                                      */
    /* If the application has no actions to do on the Start action code    */
    /* and will become active as soon as the takeover IP address is        */
    /* activated, then this code should be uncommented.  This code will    */
    /* determine if all CRGs that this application CRG is dependent upon   */
    /* are ready.  If this check fails, return failure from the action     */
```

```
    /* code.                                                              */
    /*                                                                    */

/*--------------------------------------------------------------------*/
/*      if (QcstSuccessful != checkDependCrgDataArea(MaxWaitSeconds))     */
/*         return QcstFailWithOutRestart;                                */

  }
  else {

/*--------------------------------------------------------------------*/
    /*                                                                    */
    /* This node is one of the other backup nodes or it is a replicate    */
    /* node.  If there is anything those nodes must do, do it here.  If */
    /* not, remove this else block.                                       */
    /*                                                                    */

/*--------------------------------------------------------------------*/


/*--------------------------------------------------------------------*/
    /*                                                                    */
    /* Ensure the data area status on this nodes starts out indicating    */
    /* the application is not running.                                    */
    /*                                                                    */

/*--------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Ended);
  }

  return QcstSuccessful;
}  /* end switchPrimary()                                             */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgAcAddNode                                     */
/*                                                                    */
/* The QcstAddNodeToRcvyDomain API was called.  A new node is being added  */
/* to the recovery domain of a cluster resource group.                */
/*                                                                    */
/* Things to consider:                                                */
/*   - A new node is being added to the recovery domain.  See the     */
/*     considerations in the createCrg() function.                    */
/*   - If this CRG is enabled to use the QcstDistributeInformation API,    */
/*     the user queue needed by that API could be created at this time.    */
/*                                                                    */
/**********************************************************************/
static int addNode(int role,
                   int priorRole,
                   Qcst_EXTP0100_t *crgData,
                   EpData *epData) {


/*--------------------------------------------------------------------*/

  /*                                                                    */
  /* Determine if I am the node being added.                            */
  /*                                                                    */

/*--------------------------------------------------------------------*/

  if (0 == memcmp(&crgData->This_Nodes_ID,
                  &crgData->Changing_Node_ID,
                  sizeof(Qcst_Node_Id_t)))
  {
```

```
/*--------------------------------------------------------------------*/

    /*                                                                */
    /* Set the status of the data area on this new node.              */
    /*                                                                */

/*--------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Ended);


/*--------------------------------------------------------------------*/

    /*                                                                */
    /* Create the queue needed by the Distribute Information API.     */
    /*                                                                */

/*--------------------------------------------------------------------*/

    if (0 == memcmp(&crgData->DI_Queue_Name,
                    Nulls,
                    sizeof(crgData->DI_Queue_Name)))
    {
    }
  }

  return QcstSuccessful;
}  /* end addNode()
       */


/*********************************************************************/
/*                                                                   */
/* Action code = QcstCrgAcRemoveNode                                 */
/*                                                                   */
/* The QcstRemoveNodeFromRcvyDomain or the QcstRemoveClusterNodeEntry*/
/* API was called.  A node is being removed from the recovery domain of*/
/* a cluster resource group or it is being removed entirely from the */
/* cluster.                                                          */
/*                                                                   */
/* This action code is seen by:                                      */
/*  For the QcstRemoveClusterNodeEntry API:                          */
/*    - If the removed node is active and the CRG is Inactive, all nodes in*/
/*      the recovery domain including the node being removed see this*/
/*      action code.  The nodes NOT being removed see action code dependent*/
/*      data of QcstNodeFailure.                                     */
/*    - If the removed node is active and the CRG is Active, the node being*/
/*      removed sees the Remove Node action code.  All other nodes in the*/
/*      recovery domain see an action code of Failover and action code*/
/*      dependent data of QcstNodeFailure.                           */
/*    - If the node being removed is not active in the cluster, all nodes*/
/*      in the recovery domain will see this action code.            */
/*  For the QcstRemoveNodeFromRcvyDomain API:                        */
/*    - All nodes see the Remove Node action code regardless of whether or*/
/*      not the CRG is Active.  Action code dependent data of        */
/*      QcstRmvRcvyDmnNode will also be passed.                      */
/*                                                                   */
/* Things to consider:                                               */
/*   - You may want to cleanup the removed node by deleting objects no*/
/*     longer needed there.                                          */
/*   - The job running the application is canceled and the IP takeover*/
/*     address is ended after the exit program is called if this is the*/
/*     primary node and the CRG is active.                           */
/*   - If subsystems or server jobs were started as a result of the  */
/*     QcstCrgAcStart action code, end them here or consolidate all logic*/
/*     to end the application in the cancelHandler() since it will be*/
/*     invoked for all Cluster Resource Services APIs which must end the*/
/*     application on the current primary.                           */
```

```
/*                                                                    */
/**********************************************************************/
static int rmvNode(int role,
                   int priorRole,
                   Qcst_EXTP0100_t *crgData,
                   EpData *epData) {


/*--------------------------------------------------------------------*/

  /*                                                                  */
  /* Determine if I am the node being removed.                        */
  /*                                                                  */

/*--------------------------------------------------------------------*/

  if (0 == memcmp(&crgData->This_Nodes_ID,
                  &crgData->Changing_Node_ID,
                  sizeof(Qcst_Node_Id_t)))
  {

/*--------------------------------------------------------------------*/
      /*                                                              */
      /* End the application if it is running on this node.           */
      /*                                                              */

/*--------------------------------------------------------------------*/
      endApplication(QcstCrgAcRemoveNode, role, priorRole, crgData,
epData);

  }
  return QcstSuccessful;
}  /* end rmvNode                                                   */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgAcChange                                      */
/*                                                                    */
/* The QcstChangeClusterResourceGroup API was called.  Some attribute */
/* or information stored in the cluster resource group object is being*/
/* changed.  Note that not all changes to the CRG object cause the exit*/
/* program to be called.  As of V5R1M0, only these changes will cause the*/
/* exit program to be called-                                         */
/*   - the current recovery domain is being changed                   */
/*   - the preferred recovery domain is being changed                 */
/*                                                                    */
/* If any of the above changes are being made but additionally the exit*/
/* program is being changed to *NONE, the exit program is not called. */
/*                                                                    */
/* Things to consider:                                                */
/*   - None unless changing the recovery domain affects information or*/
/*     processes for this cluster resource group.  Note that the primary*/
/*     node cannot be changed with the QcstChangeClusterResourceGroup API*/
/*     if the CRG is active.                                          */
/*                                                                    */
/**********************************************************************/
static int chgCrg(int role,
                  int priorRole,
                  Qcst_EXTP0100_t *crgData,
                  EpData *epData) {

  return QcstSuccessful;
}  /* end chgCrg()                                                  */


/**********************************************************************/
```

```
/*                                                                    */
/* Action code = QcstCrgAcDeleteCommand                               */
/*                                                                    */
/* The Delete Cluster Resource Group (DLTCRG) CL command has been called   */
/* to delete a cluster resource group object, the QcstDeleteCluster API    */
/* has been called, or the QcstRemoveClusterNodeEntry API has been called. */
/* In each case, cluster resource services is not active on the cluster    */
/* node where the command or API was called.  Thus, this function is not   */
/* distributed cluster wide but occurs only on the node where the CL       */
/* command or API was called.                                         */
/*                                                                    */
/* If the QcstDeleteCluster API was used, action code dependent data of    */
/* QcstDltCluster is passed.                                          */
/*                                                                    */
/* See the considerations in the deleteCrg() function                 */
/*                                                                    */
/**********************************************************************/
static int deleteCrgWithCmd(int role,
                            int doesNotApply,
                            Qcst_EXTP0100_t *crgData,
                            EpData *epData) {

  return QcstSuccessful;
}  /* end deleteCrgWithCmd()                                          */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgEndNode                                       */
/*                                                                    */
/* The QcstEndClusterNode API was called or a CRG job was canceled.       */
/*                                                                    */
/* The QcstCrgEndNode action code is passed to the exit program only on the*/
/* node being ended or where the CRG job was canceled.  On the node where */
/* a Cluster Resource Services job is canceled, action code dependent data*/
/* of QcstMemberFailure will be passed.                               */
/* When Cluster Resource Services ends on this node or the CRG job ends, it*/
/* will cause all other nodes in the cluster to go through failover       */
/* processing.  The action code passed to all other nodes will be         */
/* QcstCrgAcFailover.   Those nodes will see action code dependent data of */
/* QcstMemberFailure if a CRG job is canceled or QcstNodeFailure if the   */
/* node is ended.                                                     */
/*                                                                    */
/* Things to consider:                                                */
/*   - The job running the application is canceled and the IP takeover    */
/*     address is ended after the exit program is called if this is the   */
/*     primary node and the CRG is active.                            */
/*   - If subsystems or server jobs were started as a result of the       */
/*     QcstCrgAcStart action code, end them here.                     */
/*                                                                    */
/**********************************************************************/
static int endNode(int role,
                   int priorRole,
                   Qcst_EXTP0100_t *crgData,
                   EpData *epData) {


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* End the application if it is running on this node.               */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  endApplication(QcstCrgEndNode, role, priorRole, crgData, epData);

  return QcstSuccessful;
}  /* end endNode()                                                   */
```

```
/*****************************************************************************/
/*                                                                           */
/* Action code = QcstCrgAcChgNodeStatus                                      */
/*                                                                           */
/* The QcstChangeClusterNodeEntry API was called.  The status of a node      */
/* is being changed to failed.  This API is used to inform cluster resource*/
/* services that the node did not partition but really failed.               */
/*                                                                           */
/* Things to consider:                                                       */
/*   - The exit program was called previously with an action code of         */
/*     QcstCrgAcEnd if the CRG was active or an action code of               */
/*     QcstCrgAcFailover if the CRG was inactive because cluster resource    */
/*     services thought the cluster had become partitioned.  The user is     */
/*     now telling cluster resource services that the node really failed     */
/*     instead of partitioned.  The exit program has something to do only    */
/*     if it performed some action previously that needs to be changed now   */
/*     that node failure can be confirmed.                                   */
/*                                                                           */
/*****************************************************************************/
static int chgNodeStatus(int role,
                         int priorRole,
                         Qcst_EXTP0100_t *crgData,
                         EpData *epData) {

  return QcstSuccessful;
}  /* end chgNodeStatus()                                                    */


/*****************************************************************************/
/*                                                                           */
/* Action code = QcstCrgAcCancelFailover                                     */
/*                                                                           */
/* Cluster resource services on the primary node has failed or ended         */
/* for this cluster resource group.  A message was sent to the failover      */
/* message queue specified for the CRG, and the result of that message       */
/* was to cancel the failover.  This will change the status of the CRG to    */
/* inactive and leave the primary node as primary.                           */
/*                                                                           */
/* Things to consider:                                                       */
/*   - The primary node is no longer participating in cluster activities.    */
/*     The problem which caused the primary node to fail should be fixed     */
/*     so that the CRG may be started again.                                 */
/*                                                                           */
/*****************************************************************************/
static int cancelFailover(int role,
                          int priorRole,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

  return QcstSuccessful;
}  /* end cancelFailover()                                                   */


/*****************************************************************************/
/*                                                                           */
/* Action code = exit program does not know it yet                           */
/*                                                                           */
/* A new action code has been passed to this exit program.  This can occur */
/* after a new i5/OS release has been installed and some new cluster API  */
/* was called or some new cluster event occurred.  The logic in this exit  */
/* program has not yet been updated to understand the new action code.     */
/*                                                                           */
/* Two different strategies could be used for the new action code.  The    */
/* correct strategy is dependent upon the kinds of things this particular  */
/* exit program does for the application.                                    */
```

```
/*                                                                    */
/* One strategy is to not do anything and return a successful return code. */
/* This allows the new cluster API or event to run to completion.  It      */
/* allows the function to be performed even though this exit program       */
/* did not understand the new action code.  The risk, though, is that the  */
/* exit program should have done something and it did not.  At a minimum,  */
/* you may want to log some kind of error message about what happened so   */
/* that programming can investigate and get the exit program updated.      */
/*                                                                    */
/* The opposite strategy is to return an error return code such as         */
/* QcstFailWithRestart.  Of course doing this means that the new cluster   */
/* API or event cannot be used until the exit program is updated for the   */
/* new action code.  Again, logging some kind of error message for         */
/* programming to investigate would be worthwhile.                         */
/*                                                                    */
/* Only the designer of the exit program can really decide which is the    */
/* better course of action.                                           */
/*                                                                    */
/**********************************************************************/
static int newActionCode(int role,
                         int doesNotApply,
                         Qcst_EXTP0100_t *crgData,
                         EpData *epData) {


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Add logic to log an error somewhere - operator message queue, job     */
  /* log, application specific error log, etc. so that the exit program    */
  /* gets updated to properly handle the new action code.                  */
  /*                                                                  */
  /* Note that if this is left coded as it is, this is the "don't do       */
  /* anything" strategy described in the prologue above.                   */
  /*                                                                  */

/*--------------------------------------------------------------------*/

  return QcstSuccessful;
}  /* end newActionCode()                                             */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgAcUndo                                        */
/*                                                                    */
/* Note: The exit program is never called with an undo action code for     */
/* any of these prior action codes:                                   */
/*   QcstCrgAcChgNodeStatus                                           */
/*   QcstCrgAcDelete                                                  */
/*   QcstCrgAcDeleteCommand                                           */
/*   QcstCrgEndNode                                                   */
/*   QstCrgAcRemoveNode (If the node being removed is active in the       */
/*                       cluster and the API is Remove Cluster Node.      */
/*                       The Remove Node From Recovery Domain will call   */
/*                       with Undo and the Remove Cluster Node API will   */
/*                       call with Undo if the node being removed is      */
/*                       inactive.                                        */
/*   QcstCrgAcRestart                                                 */
/*   QcstCrgAcUndo                                                    */
/*                                                                    */
/* APIs that call an exit program do things in 3 steps.               */
/*   1. Logic which must be done prior to calling the exit program.       */
/*   2. Call the exit program.                                        */
/*   3. Logic which must be done after calling the exit program.          */
/*                                                                    */
/* Any errors that occur during steps 2 or 3 result in the exit program    */
/* being called again with the undo action code.  This gives the exit      */
```

```
/* program an opportunity to back out any work performed when it was first */
/* called by the API.  The API will also be backing out any work it        */
/* performed trying to return the state of the cluster and cluster objects */
/* to what it was before the API was called.                               */
/*                                                                         */
/* It is suggested that the following return codes be returned for the     */
/* specified action code as that return code will result in the most       */
/* appropriate action being taken.                                         */
/*                                                                         */
/*   QcstCrgAcInitialize: QcstSuccessful; The CRG is not created.          */
/*   QcstCrgAcStart:      QcstSuccessful; The CRG is not started.          */
/*   QcstCrgAcEnd:        QcstFailWithOutRestart; The CRG is set to Indoubt*/
/*                                        The cause of the failure needs to*/
/*                                        investigated.                    */
/*   QcstCrgAcReJoin:     QcstFailWithOutRestart; The CRG is set to Indoubt*/
/*                                        The cause of the failure needs to*/
/*                                        investigated.                    */
/*   QcstCrgAcFailover:   QcstFailWithOutRestart; The CRG is set to Indoubt*/
/*                                        The cause of the failure needs to*/
/*                                        investigated.                    */
/*   QcstCrgAcSwitchover: QcstFailWithOutRestart; The CRG is set to Indoubt*/
/*                                        The cause of the failure needs to*/
/*                                        investigated.                    */
/*   QcstCrgAcAddNode:    QcstSuccessful; The node is not added.           */
/*   QcstCrgAcRemoveNode: QcstFailWithOutRestart; The CRG is set to Indoubt*/
/*                                        The cause of the failure needs to*/
/*                                        investigated.                    */
/*   QcstCrgAcChange:     QcstSuccessful; The recovery domain is not       */
/*                                        changed.                         */
/*                                                                         */
/*************************************************************************/
static int undoPriorAction(int role,
                           int priorRole,
                           Qcst_EXTP0100_t *crgData,
                           EpData *epData) {


/*-----------------------------------------------------------------------*/
  /*                                                                     */
  /* The prior action code defines what the exit program was doing when  */
  /* it failed, was canceled, or returned a non successful return code.  */
  /*                                                                     */

/*-----------------------------------------------------------------------*/
  if (crgData->Prior_Action_Code &lt;= MaxAc )
    return (*undoFcn[crgData-&lt;Prior_Action_Code])
                                      (role, priorRole, crgData,
epData);
  else

/*-----------------------------------------------------------------------*/
    /*                                                                   */
    /* IBM has defined a new action code in a new operating system release */
    /* and this exit program has not yet been updated to handle it.  Take a*/
    /* default action for now.                                           */
    /*                                                                   */

/*-----------------------------------------------------------------------*/
    return newActionCode(role, priorRole, crgData, epData);
}  /* end undoPriorAction()                                              */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcUndo                                           */
/*                                                                       */
/* Prior action code = QcstCrgAcInitialize                               */
```

```
/*                                                                    */
/* Things to consider:                                                */
/*   The CRG will not be created.  Objects that might have been created   */
/*   on nodes in the recovery domain should be deleted since a subsequent  */
/*   create could fail if those objects already exist.                */
/*                                                                    */
/**********************************************************************/
static int undoCreateCrg(int role,
                         int doesNotApply,
                         Qcst_EXTP0100_t *crgData,
                         EpData *epData) {

  return QcstSuccessful;
}  /* end undoCreateCrg()                                             */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgAcUndo                                        */
/*                                                                    */
/* Prior action code = QcstCrgAcStart                                 */
/*                                                                    */
/* Things to consider:                                                */
/*   Cluster Resource Services failed when it was finishing the Start CRG  */
/*   API after it had already called the exit program with the Start      */
/*   Action code.                                                     */
/*                                                                    */
/*   On the primary node, the exit program job which is running the       */
/*   application will be canceled.  The exit program will then be called  */
/*   with the Undo action code.                                       */
/*                                                                    */
/*   All other nodes in the recovery domain will be called with the Undo  */
/*   action code.                                                     */
/*                                                                    */
/**********************************************************************/
static int undoStartCrg(int role,
                        int doesNotApply,
                        Qcst_EXTP0100_t *crgData,
                        EpData *epData) {

  return QcstSuccessful;
}  /* end undoStartCrg()                                              */


/**********************************************************************/
/*                                                                    */
/* Action code = QcstCrgAcUndo                                        */
/*                                                                    */
/* Prior action code = QcstCrgAcEnd                                   */
/*                                                                    */
/* Things to consider:                                                */
/*   The CRG will not be ended.  If the exit program did anything to bring */
/*   down the application it can either restart the application or it can  */
/*   decide to not restart the application.  If the application is not     */
/*   restarted, the return code should be set to QcstFailWithOutRestart so */
/*   the status of the CRG is set to Indoubt.                         */
/*                                                                    */
/**********************************************************************/
static int undoEndCrg(int role,
                      int doesNotApply,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {

  return QcstFailWithOutRestart;
}  /* end undoEndCrg()                                                */
```

```
/*****************************************************************************/
/*                                                                           */
/* Action code = QcstCrgAcUndo                                               */
/*                                                                           */
/* Prior action code = QcstCrgAcReJoin                                       */
/*                                                                           */
/* Things to consider:                                                       */
/*   An error occurred which won't allow the member to join this CRG         */
/*   group.  Anything done for the Join action code needs to be looked at    */
/*   to see if something must be undone if this member is not an active      */
/*   member of the CRG group.                                                */
/*                                                                           */
/*****************************************************************************/
static int undoMemberIsJoining(int role,
                               int doesNotApply,
                               Qcst_EXTP0100_t *crgData,
                               EpData *epData) {

  return QcstFailWithOutRestart;
}  /* end undoMemberIsJoining()                                              */


/*****************************************************************************/
/*                                                                           */
/* Action code = QcstCrgAcUndo                                               */
/*                                                                           */
/* Prior action code = QcstCrgAcFailover                                     */
/*                                                                           */
/* Things to consider:                                                       */
/*   This does not mean that the node failure or failing member is being     */
/*   undone.  That failure is irreversible.  What it does mean is that the  */
/*   exit program returned an error from the Failover action code or         */
/*   Cluster Resource Services ran into a problem after it called the exit   */
/*   program.  If the CRG was active when Failover was attempted, it is      */
/*   not at this point.  End the resilient resource and expect a human to    */
/*   look into the failure.  After the failure is corrected, the CRG will    */
/*   must be started with the Start CRG API.                          */
/*                                                                           */
/*                                                                           */
/*****************************************************************************/
static int undoMemberIsLeaving(int role,
                               int doesNotApply,
                               Qcst_EXTP0100_t *crgData,
                               EpData *epData) {

  return QcstFailWithOutRestart;
}  /* end undoMemberIsLeaving()                                              */


/*****************************************************************************/
/*                                                                           */
/* Action code = QcstCrgAcUndo                                               */
/*                                                                           */
/* Prior action code = QcstCrgAcSwitchover                                   */
/*                                                                           */
/* Things to consider:                                                       */
/*   Some error occurred after the point of access was moved from the        */
/*   original primary and before it could be brought up on the new primary.*/
/*   The IP address was ended on the original primary before moving the      */
/*   point of access but is started on the original primary again.  Cluster*/
/*   Resource Services will now attempt to move the point of access back     */
/*   to the original primary.  The application exit program and IP takeover*/
/*   address will be started on the original primary.                        */
/*                                                                           */
/*                                                                           */
/*****************************************************************************/
static int undoSwitchPrimary(int role,
```

```
                          int doesNotApply,
                          Qcst_EXTP0100_t *crgData,
                          EpData *epData) {

  return QcstFailWithOutRestart;
}  /* end undoSwitchPrimary()                                              */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcUndo                                           */
/*                                                                       */
/* Prior action code = QcstCrgAcAddNode                                  */
/*                                                                       */
/* Things to consider:                                                   */
/*   If objects were created on the new node, they should be removed so  */
/*   that a subsequent Add Node to aRecovery Domain does not fail if it  */
/*   attempts to create objects again.                                   */
/*                                                                       */
/*                                                                       */
/*************************************************************************/
static int undoAddNode(int role,
                       int doesNotApply,
                       Qcst_EXTP0100_t *crgData,
                       EpData *epData) {

  return QcstSuccessful;
}  /* end undoAddNode()                                                  */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcUndo                                           */
/*                                                                       */
/* Prior action code = QcstCrgAcRemoveNode                               */
/*                                                                       */
/* Things to consider:                                                   */
/*   The node is still in the recovery domain.  If objects were removed  */
/*   from the node, they should be added back.                           */
/*                                                                       */
/*************************************************************************/
static int undoRmvNode(int role,
                       int doesNotApply,
                       Qcst_EXTP0100_t *crgData,
                       EpData *epData) {

  return QcstFailWithOutRestart;
}  /* end undoRmvNode()                                                  */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcUndo                                           */
/*                                                                       */
/* Prior action code = QcstCrgAcChange                                   */
/*                                                                       */
/* Things to consider:                                                   */
/*   Changes to the CRG will be backed out so that the CRG and its       */
/*   recovery domain look just like it did prior to the attempted change.*/
/*   Any changes the exit program made should also be backed out.        */
/*                                                                       */
/*************************************************************************/
static int undoChgCrg(int role,
                      int doesNotApply,
                      Qcst_EXTP0100_t *crgData,
                      EpData *epData) {
```

```
  return QcstSuccessful;
}  /* end undoChgCrg()                                                    */


/*************************************************************************/
/*                                                                       */
/* Action code = QcstCrgAcUndo                                           */
/*                                                                       */
/* Prior action code = QcstCrgAcCancelFailover                           */
/*                                                                       */
/* Things to consider:                                                   */
/*   This does not mean that the node failure or failing member is being */
/*   undone.  That failure is irreversible.  What it does mean is that   */
/*   Cluster Resource Services ran into a problem after it called the exit */
/*   program.  The CRG will be InDoubt regardless of what is returned from */
/*   this exit program call.  Someone will need to manually look into the */
/*   the failure.  After the failure is corrected, the CRG will must be */
/*   started with the Start CRG API.                                     */
/*                                                                       */
/*                                                                       */
/*************************************************************************/
static int undoCancelFailover(int role,
                              int doesNotApply,
                              Qcst_EXTP0100_t *crgData,
                              EpData *epData) {

  return QcstSuccessful;
}  /* end undoCancelFailover()                                           */


/*************************************************************************/
/*                                                                       */
/* A simple routine to take a null terminated object name and a null     */
/* terminated library name and build a 20 character non-null terminated  */
/* qualified name.                                                       */
/*                                                                       */
/*************************************************************************/
static void bldDataAreaName(char *objName, char* libName, char *qualName) {

  memset(qualName, 0x40, 20);
  memcpy(qualName, objName, strlen(objName));
  qualName += 10;
  memcpy(qualName, libName, strlen(libName));
  return;
}  /* end bldDataAreaName                                                */


/*************************************************************************/
/*                                                                       */
/* The data area is checked to see if all the CRGs that this application */
/* is dependent upon are ready.  If they are not ready, a wait for a     */
/* certain amount of time is performed and the data area is checked again. */
/* This check, wait loop continues until all dependent CRGs become ready or*/
/* until the maximum wait time has been reached.                         */
/* The length of the wait can be changed to some other value if a        */
/* particular situation would be better with shorter or longer wait times. */
/*                                                                       */
/*                                                                       */
/*************************************************************************/
static int checkDependCrgDataArea(unsigned int maxWaitTime) {

  Qus_EC_t errCode = { sizeof(Qus_EC_t), 0 };
  char dataAreaName[20];
  struct {
    Qwc_Rdtaa_Data_Returned_t stuff;
    char ready;
  } data;
```

```
/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* This is an accumulation of the time waited for the dependent CRGs to  */
  /* become ready.                                                    */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  unsigned int timeWaited = 0;


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Build definition of the amount of time to wait.                  */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  _MI_Time   timeToWait;
  int hours     = 0;
  int minutes   = 0;
  int seconds   = WaitSecondsIncrement;
  int hundreths = 0;
  short int options = _WAIT_NORMAL;
  mitime( &timeToWait, hours, minutes, seconds, hundreths );


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Build the qualified name of the data area.                       */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  bldDataAreaName(DependCrgDataArea, ApplLib, dataAreaName);


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Get the data from the data area that indicates whether or not the     */
  /* CRGs are all ready.  This data area is updated by the High       */
  /* Availability Business Partners when it is ok for the application to   */
  /* proceed.                                                         */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  QWCRDTAA(&data,
           sizeof(data),
           dataAreaName,
           offsetof(Qcst_HAAPPO_t,Data_Status)+1,  /* API wants a 1 origin */
           sizeof(data.ready),
           &errCode);


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* If the dependent CRGs are not ready, wait for a bit and check again.  */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  while (data.ready != Data_Available) {


/*--------------------------------------------------------------    */
    /*                                                                */
    /* If the dependent CRGs are not ready after the maximum wait time,    */
    /* return an error.  Consider logging some message to describe why the */
    /* application did not start so that  the problem can be looked into.  */
```

```
    /*                                                                  */

/*------------------------------------------------------------------*/
    if (timeWaited >= maxWaitTime)
      return QcstFailWithOutRestart;


/*------------------------------------------------------------------*/
    /*                                                                  */
    /* Wait to allow the data CRGs to become ready.                     */
    /*                                                                  */

/*------------------------------------------------------------------*/
    waittime(&timeToWait, options);
    timeWaited += WaitSecondsIncrement;


/*------------------------------------------------------------------*/
    /*                                                                  */
    /* Get information from the data area again to see if the data CRGs are*/
    /* ready.                                                           */
    /*                                                                  */

/*------------------------------------------------------------------*/
    QWCRDTAA(&data,
             sizeof(data),
             dataAreaName,
             offsetof(Qcst_HAAPPO_t,Data_Status)+1,  /* API wants a 1 origin */
             sizeof(data.ready),
             &errCode);
  }

  return QcstSuccessful;
}  /* end checkDependCrgDataArea                                    */


/**********************************************************************/
/*                                                                    */
/* The application CRG data area is updated to indicate that the      */
/* application is running or to indicate it is not running.  This data area*/
/* information is used by the High Availability Business Partners to  */
/* coordinate the switchover activities between CRGs that have dependencies*/
/* on each other.                                                     */
/*                                                                    */
/**********************************************************************/
static void setApplCrgDataArea(char status) {

  char cmd[54];
  char cmdEnd[3] = {0x00, ')', 0x00};


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Set up the CL command string with the data area library name, the data*/
  /* area name, and the character to put into the data area.  Then run the */
  /* CL command.                                                      */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  memcpy(cmd, "CHGDTAARA DTAARA(", strlen("CHGDTAARA DTAARA(")+1);
  strcat(cmd, ApplLib);
  strcat(cmd, "/");
  strcat(cmd, ApplCrgDataArea);
  strcat(cmd, " (425 1)) VALUE(");                              /* @A1C */
  cmdEnd[0] = status;
  strcat(cmd, cmdEnd);
```

```
  system(cmd);

  return;
}  /* end setApplCrgDataArea                                              */


/*************************************************************************/
/*                                                                       */
/* This function is called any time the exit program receives an exception */
/* not specifically monitored for by some other exception handler.  Add  */
/* appropriate logic to perform cleanup functions that may be required.  */
/* A failure return code is then set and control returns to the operating */
/* system.  The job this exit program is running in will then end.       */
/*                                                                       */
/* When this function gets called, myData->role may still contain the    */
/* UnknownRole value if an exception occurred before this node's role    */
/* value was set.  To be completely correct, the role should be tested   */
/* for UnknownRole before making any decisions based upon the value of   */
/* role.                                                                 */
/*                                                                       */
/*************************************************************************/
static void unexpectedExceptionHandler(_INTRPT_Hndlr_Parms_T
*exData) {


/*-------------------------------------------------------------------------  */
  /*                                                                       */
  /* Get a pointer to the structure containing data that is passed to the  */
  /* exception handler.                                                    */
  /*                                                                       */

/*-----------------------------------------------------------------------*/
  HandlerDataT *myData = (HandlerDataT *)exData->Com_Area;


/*-----------------------------------------------------------------------*/
  /*                                                                       */
  /* Perform as much cleanup function as necessary.  Some global state     */
  /* information may must be kept so the exception handler knows what   */
  /* steps were completed before the failure occurred and thus knows what  */
  /* cleanup steps must be performed.  This state information could be     */
  /* kept in the HandlerDataT structure or it could be kept in some other  */
  /* location that this function can address.                              */
  /*                                                                       */

/*-----------------------------------------------------------------------*/


/*-----------------------------------------------------------------------*/
  /*                                                                       */
  /* If this is the primary node and the application was started, end it.  */
  /* The application is ended because the exit program will be called again*/
  /* with the Restart action code and want the restartCrg() function to */
  /* always work the same way.  In addition, ending the application may    */
  /* clear up the condition that caused the exception.    */
  /* If possible, warn users and have them stop using the application so   */
  /* things are done in an orderly manner.                                 */
  /*                                                                       */

/*-----------------------------------------------------------------------*/
  endApplication(myData->actionCode,
                 myData->role,
                 myData->priorRole,
                 myData->crgData,
                 myData->epData);
```

```
/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Set the exit program return code.                                */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  *myData->retCode = QcstFailWithRestart;


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Let the exception percolate up the call stack.                 */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  return;
}  /* end unexpectedExceptionHandler                                 */


/**********************************************************************/
/*                                                                    */
/* This function is called any time the job this exit program is running in*/
/* is canceled.  The job could be canceled due to any of the following   */
/* (the list is not intended to be all inclusive)-                    */
/*   - an API cancels an active application CRG.  The End CRG, Initiate    */
/*     Switchover, End Cluster Node, Remove Cluster Node or Delete Cluster */
/*     API cancels the job which was submitted when the exit program was   */
/*     called with a Start action code.                               */
/*   - operator cancels the job from some operating system display such as */
/*     Work with Active Jobs                                          */
/*   - the subsystem this job is running in is ended                  */
/*   - all subsystems are ended                                       */
/*   - the system is powered down                                     */
/*   - an operating system machine check occurred                     */
/*                                                                    */
/* When this function gets called, myData->role may still contain the     */
/* UnknownRole value if cancelling occurred before this node's role       */
/* value was set.  To be completely correct, the role should be tested    */
/* for UnknownRole before making any decisions based upon the value of    */
/* role.                                                              */
/*                                                                    */
/**********************************************************************/
static void cancelHandler(_CNL_Hndlr_Parms_T *cnlData) {


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Get a pointer to the structure containing data that was passed to the */
  /* cancel handler.                                                  */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  HandlerDataT *myData = (HandlerDataT *)cnlData->Com_Area;


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Perform as much cleanup function as necessary.  Some global state     */
  /* information may must be kept so the cancel handler knows what      */
  /* steps were completed before the job was canceled and thus knows if   */
  /* the function had really completed successfully or was only partially  */
  /* complete and thus needs some cleanup to be done.  This state          */
  /* information could be kept in the HandlerDataT structure or it could   */
  /* be kept in some other location that this function can address.        */
  /*                                                                  */

/*--------------------------------------------------------------------*/
```

```
/*--------------------------------------------------------------------*/

  /*                                                                  */
  /* This job is being canceled.  If I was running the application as a   */
  /* result of the Start or Restart action codes, end the application now. */
  /* This job is being canceled because a Switch Over or some other      */
  /* Cluster Resource Services API was used which affects the primary node */
  /* or someone did a cancel job with a CL command, from a system display, */
  /* etc.                                                             */


/*--------------------------------------------------------------------*/
  endApplication(myData->actionCode,
                 myData->role,
                 myData->priorRole,
                 myData->crgData,
                 myData->epData);


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Set the exit program return code.                                */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  *myData->retCode = QcstSuccessful;


/*--------------------------------------------------------------------*/
  /*                                                                  */
  /* Return to the operating system for final ending of the job.      */
  /*                                                                  */

/*--------------------------------------------------------------------*/
  return;
}  /* end cancelHandler                                             */


/**********************************************************************/
/*                                                                    */
/* A common routine used to end the application by various action code     */
/* functions, the exception handler, and the cancel handler.          */
/*                                                                    */
/**********************************************************************/
static void endApplication(unsigned int actionCode,
                           int role,
                           int priorRole,
                           Qcst_EXTP0100_t *crgData,
                           EpData *epData) {

  if (  role == QcstPrimaryNodeRole
      &&
        crgData->Original_Cluster_Res_Grp_Stat == QcstCrgActive)
{

/*--------------------------------------------------------------------*/
    /*                                                                */
    /* Add logic to end the application here.  You may need to add logic   */
    /* to determine if the application is still running because this      */
    /* function could be called once for an action code and again from    */
    /* the cancel handler (End CRG is an example).                    */
    /*                                                                */

/*--------------------------------------------------------------------*/
```

```
/*--------------------------------------------------------------------*/
    /*                                                                */
    /* After the application has ended, update the data area to indicate   */
    /* the application is no longer running.                          */
    /*                                                                */

/*--------------------------------------------------------------------*/
    setApplCrgDataArea(Appl_Ended);
  }

  return;
}  /* end endApplication                                              */


/**********************************************************************/
/*                                                                    */
/* Print out the data passed to this program.                         */
/*                                                                    */
/**********************************************************************/
static void printParms(int actionCode,
                       int role,
                       int priorRole,
                       Qcst_EXTP0100_t *crgData,
                       EpData *epData) {

  unsigned int i;
  char *str;

  /* Print the action code.                                           */
  printf("%s", "Action_Code = ");
  printActionCode(actionCode);

  /* Print the action code dependent data.                            */
  printf("%s", "    Action_Code_Dependent_Data = ");
  switch (crgData->Action_Code_Dependent_Data) {
    case QcstNoDependentData:  str = "QcstNoDependentData";
                               break;
    case QcstMerge:            str = "QcstMerge";
                               break;
    case QcstJoin:             str = "QcstJoin";
                               break;
    case QcstPartitionFailure: str = "QcstPartitionFailure";
                               break;
    case QcstNodeFailure:      str = "QcstNodeFailure";
                               break;
    case QcstMemberFailure:    str = "QcstMemberFailure";
                               break;
    case QcstEndNode:          str = "QcstEndNode";
                               break;
    case QcstRemoveNode:       str = "QcstRemoveNode";
                               break;
    case QcstApplFailure:      str = "QcstApplFailure";
                               break;
    case QcstResourceEnd:      str = "QcstResourceEnd";
                               break;
    case QcstDltCluster:       str = "QcstDltCluster";
                               break;
    case QcstRmvRcvyDmnNode:   str = "QcstRmvRcvyDmnNode";
                               break;
    case QcstDltCrg:           str = "QcstDltCrg";
                               break;
    default: str = "unknown action code dependent data";
  }
  printf("%s \n", str);
```

```
  /* Print the prior action code.                                       */
  printf("%s", "  Prior_Action_Code = ");
  if (crgData->Prior_Action_Code)
    printActionCode(crgData->Prior_Action_Code);
  printf("\n");

  /* Print the cluster name.                                            */
  printStr("  Cluster_Name = ",
           crgData->Cluster_Name, sizeof(Qcst_Cluster_Name_t));

  /* Print the CRG name.                                                */
  printStr("  Cluster_Resource_Group_Name = ",
           crgData->Cluster_Resource_Group_Name,
sizeof(Qcst_Crg_Name_t));

  /* Print the CRG type.                                                */
  printf("%s \n", "  Cluster_Resource_Group_Type =
QcstCrgApplResiliency");

  /* Print the CRG status.                                              */
  printf("%s", "  Cluster_Resource_Group_Status = ");
  printCrgStatus(crgData->Cluster_Resource_Group_Status);

  /* Print the CRG original status.                                     */
  printf("%s", "  Original_Cluster_Res_Grp_Stat = ");
  printCrgStatus(crgData->Original_Cluster_Res_Grp_Stat);

  /* Print the Distribute Information queue name.                       */
  printStr("  DI_Queue_Name = ",
           crgData->DI_Queue_Name,
sizeof(crgData->DI_Queue_Name));
  printStr("  DI_Queue_Library_Name = ",
           crgData->DI_Queue_Library_Name,
           sizeof(crgData->DI_Queue_Library_Name));

  /* Print the CRG attributes.                                          */
  printf("%s", "  Cluster_Resource_Group_Attr = ");
  if (crgData->Cluster_Resource_Group_Attr &
QcstTcpConfigByUsr)
    printf("%s", "User Configures IP Takeover Address");
  printf("\n");

  /* Print the ID of this node.                                         */
  printStr("  This_Nodes_ID = ",
           crgData->This_Nodes_ID, sizeof(Qcst_Node_Id_t));

  /* Print the role of this node.                                       */
  printf("%s %d \n", "  this node's role = ", role);

  /* Print the prior role of this node.                                 */
  printf("%s %d \n", "  this node's prior role = ", priorRole);

  /* Print which recovery domain this role comes from.                  */
  printf("%s", "  Node_Role_Type = ");
  if (crgData->Node_Role_Type == QcstCurrentRcvyDmn)
    printf("%s \n", "QcstCurrentRcvyDmn");
  else
    printf("%s \n", "QcstPreferredRcvyDmn");

  /* Print the ID of the changing node (if any).                        */
  printStr("  Changing_Node_ID = ",
           crgData->Changing_Node_ID, sizeof(Qcst_Node_Id_t));

  /* Print the role of the changing node (if any).                      */
  printf("%s", "  Changing_Node_Role = ");
```

```
  if (crgData->Changing_Node_Role == -3)
    printf("%s \n", "*LIST");
  else if (crgData->Changing_Node_Role == -2)
   printf("%s \n", "does not apply");
  else
    printf("%d \n", crgData->Changing_Node_Role);

  /* Print the takeover IP address.                                    */
  printStr("  Takeover_IP_Address = ",
           crgData->Takeover_IP_Address,
sizeof(Qcst_TakeOver_IP_Address_t));

  /* Print the job name.                                               */
  printStr("  Job_Name = ", crgData->Job_Name, 10);

  /* Print the CRG changes.                                            */
  printf("%s \n", "  Cluster_Resource_Group_Changes = ");
  if (crgData->Cluster_Resource_Group_Changes &
QcstRcvyDomainChange)
    printf("      %s \n", "Recovery domain changed");
  if (crgData->Cluster_Resource_Group_Changes &
QcstTakeOverIpAddrChange)
    printf("      %s \n", "Takeover IP address changed");

  /* Print the failover wait time.                                     */
  printf("%s", "Failover_Wait_Time = ");
  if (crgData->Failover_Wait_Time == QcstFailoverWaitForever)
     printf("%d %s \n", crgData->Failover_Wait_Time, "Wait
forever");
  else if (crgData->Failover_Wait_Time == QcstFailoverNoWait)
     printf("%d %s \n", crgData->Failover_Wait_Time, "No wait");
  else
     printf("%d %s \n", crgData->Failover_Wait_Time, "minutes");

  /* Print the failover default action.                                */
  printf("%s", "Failover_Default_Action = ");
  if (crgData->Failover_Default_Action == QcstFailoverProceed)
     printf("%d %s \n", crgData->Failover_Default_Action,
"Proceed");
  else
     printf("%d %s \n", crgData->Failover_Default_Action,
"Cancel");

  /* Print the failover message queue name.                            */
  printStr("  Failover_Msg_Queue = ",
           crgData->Failover_Msg_Queue,
sizeof(crgData->Failover_Msg_Queue));
  printStr("  Failover_Msg_Queue_Lib = ",
           crgData->Failover_Msg_Queue_Lib,
           sizeof(crgData->Failover_Msg_Queue_Lib));

  /* Print the cluster version.                                        */
  printf("%s %d \n",
         "  Cluster_Version = ", crgData->Cluster_Version);

  /* Print the cluster version mod level                               */
  printf("%s %d \n",
         "  Cluster_Version_Mod_Level = ",
         crgData->Cluster_Version_Mod_Level);

  /* Print the requesting user profile.                                */
  printStr("  Req_User_Profile = ",
           crgData->Req_User_Profile,
sizeof(crgData->Req_User_Profile));

  /* Print the length of the data in the structure.                    */
  printf("%s %d \n",
```

```
        "  Length_Info_Returned = ",
crgData->Length_Info_Returned);

  /* Print the offset to the recovery domain array.                        */
  printf("%s %d \n",
        "  Offset_Rcvy_Domain_Array = ",
crgData->Offset_Rcvy_Domain_Array);

  /* Print the number of nodes in the recovery domain array.               */
  printf("%s %d \n",
        "  Number_Nodes_Rcvy_Domain = ",
crgData->Number_Nodes_Rcvy_Domain);

  /* Print the current/new recovery domain.                                */
  printRcvyDomain("   The recovery domain:",
                  crgData->Number_Nodes_Rcvy_Domain,
                  (Qcst_Rcvy_Domain_Array1_t *)
                  ((char *)crgData +
crgData->Offset_Rcvy_Domain_Array));

  /* Print the offset to the prior recovery domain array.                  */
  printf("%s %d \n",
        "  Offset_Prior_Rcvy_Domain_Array = ",
        crgData->Offset_Prior_Rcvy_Domain_Array);

  /* Print the number of nodes in the prior recovery domain array.         */
  printf("%s %d \n",
        "  Number_Nodes_Prior_Rcvy_Domain = ",
        crgData->Number_Nodes_Prior_Rcvy_Domain);

  /* Print the prior recovery domain if one was passed.                    */
  if (crgData->Offset_Prior_Rcvy_Domain_Array) {
    printRcvyDomain("   The prior recovery domain:",
                    crgData->Number_Nodes_Prior_Rcvy_Domain,
                    (Qcst_Rcvy_Domain_Array1_t *)
                ((char *)crgData +
crgData->Offset_Prior_Rcvy_Domain_Array));
  }

  return;
}  /* end printParms                                                       */


/*****************************************************************************/
/*                                                                           */
/* Print a string for the action code.                                       */
/*                                                                           */
/*****************************************************************************/
static void printActionCode(unsigned int ac) {

  char *code;
  switch (ac) {
    case QcstCrgAcInitialize: code = "QcstCrgAcInitialize";
                              break;
    case QcstCrgAcStart:      code = "QcstCrgAcStart";
                              break;
    case QcstCrgAcRestart:    code = "QcstCrgAcRestart";
                              break;
    case QcstCrgAcEnd:        code = "QcstCrgAcEnd";
                              break;
    case QcstCrgAcDelete:     code = "QcstCrgAcDelete";
                              break;
    case QcstCrgAcReJoin:     code = "QcstCrgAcReJoin";
                              break;
    case QcstCrgAcFailover:   code = "QcstCrgAcFailover";
                              break;
    case QcstCrgAcSwitchover: code = "QcstCrgAcSwitchover";
```

```
                            break;
    case QcstCrgAcAddNode:    code = "QcstCrgAcAddNode";
                            break;
    case QcstCrgAcRemoveNode: code = "QcstCrgAcRemoveNode";
                            break;
    case QcstCrgAcChange:     code = "QcstCrgAcChange";
                            break;
    case QcstCrgAcDeleteCommand: code = "QcstCrgAcDeleteCommand";
                            break;
    case QcstCrgAcUndo:       code = "QcstCrgAcUndo";
                            break;
    case QcstCrgEndNode:      code = "QcstCrgEndNode";
                            break;
    case QcstCrgAcAddDevEnt:  code = "QcstCrgAcAddDevEnt";
                            break;
    case QcstCrgAcRmvDevEnt:  code = "QcstCrgAcRmvDevEnt";
                            break;
    case QcstCrgAcChgDevEnt:  code = "QcstCrgAcChgDevEnt";
                            break;
    case QcstCrgAcChgNodeStatus: code = "QcstCrgAcChgNodeStatus";
                            break;
    case QcstCrgAcCancelFailover: code = "QcstCrgAcCancelFailover";
                            break;
    case QcstCrgAcVerificationPhase: code =
"QcstCrgAcVerificationPhase";
                            break;
    default:                code = "unknown action code";
                            break;
  }
  printf("%s", code);

  return;
}  /* end printActionCode                                                 */


/*********************************************************************/
/*                                                                   */
/* Print the CRG status.                                             */
/*                                                                   */
/*********************************************************************/
static void printCrgStatus(int status) {

  char * str;
  switch (status) {
    case QcstCrgActive:              str = "QcstCrgActive";
                                     break;
    case QcstCrgInactive:            str= "QcstCrgInactive";
                                     break;
    case QcstCrgIndoubt:             str = "QcstCrgIndoubt";
                                     break;
    case QcstCrgRestored:            str = "QcstCrgRestored";
                                     break;
    case QcstCrgAddnodePending:      str =
"QcstCrgAddnodePending";
                                     break;
    case QcstCrgDeletePending:       str = "QcstCrgDeletePending";
                                     break;
    case QcstCrgChangePending:       str = "QcstCrgChangePending";
                                     break;
    case QcstCrgEndCrgPending:       str = "QcstCrgEndCrgPending";
                                     break;
    case QcstCrgInitializePending:   str =
"QcstCrgInitializePending";
                                     break;
    case QcstCrgRemovenodePending:   str =
"QcstCrgRemovenodePending";
                                     break;
```

```
    case QcstCrgStartCrgPending:      str =
"QcstCrgStartCrgPending";
                                      break;
    case QcstCrgSwitchOverPending:    str =
"QcstCrgSwitchOverPending";
                                      break;
    case QcstCrgDeleteCmdPending:     str =
"QcstCrgDeleteCmdPending";
                                      break;
    case QcstCrgAddDevEntPending:     str =
"QcstCrgAddDevEntPending";
                                      break;
    case QcstCrgRmvDevEntPending:     str =
"QcstCrgRmvDevEntPending";
                                      break;
    case QcstCrgChgDevEntPending:     str =
"QcstCrgChgDevEntPending";
                                      break;
    case QcstCrgChgNodeStatusPending: str =
"QcstCrgChgNodeStatusPending";
                                      break;
    default: str = "unknown CRG status";
  }
  printf("%s \n", str);

  return;
}  /* end printCrgStatus                                                  */


/*****************************************************************************/
/*                                                                           */
/* Print the recovery domain.                                                */
/*                                                                           */
/*****************************************************************************/
static void printRcvyDomain(char *str,
                            unsigned int count,
                            Qcst_Rcvy_Domain_Array1_t *rd) {

  unsigned int i;
  printf("\n %s \n", str);
  for (i=1; i&lt;=count; i++) {
    printStr("    Node_ID = ", rd->Node_ID,
sizeof(Qcst_Node_Id_t));
    printf("%s %d \n", "      Node_Role = ", rd->Node_Role);
    printf("%s", "      Membership_Status = ");
    switch (rd->Membership_Status) {
      case 0: str = "Active";
              break;
      case 1: str = "Inactive";
              break;
      case 2: str = "Partition";
              break;
      default: str = "unknown node status";
    }
    printf("%s \n", str);
    rd++;
  }
  return;
}  /* end printRcvyDomain                                                 */

/*****************************************************************************/
/*                                                                           */
/* Concatenate a null terminated string and a non null terminated string   */
/* and print it.                                                             */
/*                                                                           */
/*****************************************************************************/
static void printStr(char *s1, char *s2, unsigned int len) {
```

```
  char buffer[132];
  memset(buffer, 0x00, sizeof(buffer));
  memcpy(buffer, s1, strlen(s1));
  strncat(buffer, s2, len);
  printf("%s \n", buffer);
  return;
}  /* end printStr                                                */
```

Planification du test de résistance des données

La résilience des données est la disponibilité des données pour des utilisateurs ou des applications. Vous pouvez effectuer un test de résistance des données à l'aide de la technologie de grappe IBM i avec des disques commutés, la protection par disque miroir d'un site à l'autre ou les technologies de réplication logique.

Pour les implémentations de résilience des données prises en charge par IBM i, plusieurs technologies s'offrent à vous. Lorsque ces technologies sont associées aux services de ressources de mise en grappe IBM i, vous pouvez créer une solution à haute disponibilité complète. Ces technologies peuvent être catégorisées comme suit :

Technologies de pools de stockage sur disque indépendant IBM i

Ces technologies reposent toutes sur l'implémentation de pools de stockage sur disque indépendant IBM i. Pour une haute disponibilité utilisant des technologies de pools de stockage sur disque indépendant, toutes les données devant être résilientes doivent être stockées dans un pool de stockage sur disque indépendant. Très souvent, cette opération implique la migration des données vers des pools de stockage sur disque indépendant. Ces informations supposent que la migration des données a été effectuée.

Les technologies IBM i prises en charge suivantes reposent sur des pools de stockage sur disque indépendant :

- Disques commutés
- Protection géographique par disque miroir
- Metro Mirror
- Global Mirror
- Unités logiques commutées

Technologies de réplication logique

La réplication logique est une technologie basée sur des journaux : les données sont alors répliquées vers un autre système en temps réel. Les technologies de réplication logique utilisent les services de ressources de mise en grappe IBM i et la journalisation avec des applications de partenaires commerciaux IBM. Ces solutions requièrent une application à haute disponibilité d'un partenaire commercial pour configurer et gérer l'environnement. Ces informations n'incluent pas d'exigences spécifiques pour ces solutions de partenaires commerciaux IBM. Si vous implémentez une solution de réplication logique pour la haute disponibilité, consultez les informations relatives à l'application ou contactez une revendeur.

Information associée

IBM eServer iSeries Independent ASPs: A Guide to Moving Applications to IASPs

Identification des données à rendre résilientes

Identifiez les types de données qui doivent selon vous devenir résilientes.

L'identification des données à rendre résilientes est similaire à celles des données à sauvegarder lorsque vous préparez une stratégie de sauvegarde et de reprise pour vos systèmes. Vous devez déterminer quelles données de votre environnement sont essentielles pour que votre activité continue.

Par exemple, si vous développez une activité sur le Web, les données vitales seraient :

- l'ordre du jour,
- le stock,
- les enregistrements client.

En général, il est inutiles que les informations qui ne changent pas souvent ou dont vous n'avez pas chaque jour besoin soient résilientes.

Planification de disques commutés

Une copie des données est conservée sur un matériel commutable, à savoir une unité d'extension (tour) ou un processeur d'E-S dans un environnement de partitions logiques. La commutation de tour ne sera pas disponible avec les matériels POWER7.

Lorsqu'une indisponibilité du système se produit sur le noeud principal, l'accès aux données sur le matériel commutable fait passer à un noeud de secours désigné. Par ailleurs, vous pouvez utiliser des pools de stockage sur disque indépendant dans un environnement de protection par disque miroir d'un site à l'autre (XSM). De cette façon, une copie miroir du pool de stockage sur disque indépendant peut être conservée sur un système (éventuellement) à distance du site d'origine pour des questions de disponibilité ou de protection.

Planifiez avec soin si vous envisagez d'employer des ressources commutables se trouvant sur des pools de stockage sur disque indépendant commutables ou la protection par disque miroir d'un site à l'autre (XSM).

Vous devez également évaluer la configuration de votre disque système pour déterminer si des unités de disque supplémentaires sont nécessaires. Comme pour toute configuration d'un disque système, le nombre d'unités de disques disponibles pour l'application peut avoir une incidence importante sur les performances. Si vous placez une charge de travail supplémentaire sur un nombre limité d'unités de disques, les temps de réponse des disques peuvent s'allonger, ainsi que les temps de réponse à l'application. Ce point est notamment important dans le cas d'une mémoire de travail dans un système configuré avec des pools de stockage sur disque indépendant. Tout stockage temporaire est écrit dans le pool de stockage sur disque SYSBAS. Si votre application n'utilise aucun stockage temporaire, vous pouvez alors utiliser moins d'ARM de disque dans le pool de stockage sur disque SYSBAS. Vous devez aussi penser que le système d'exploitation et les fonctions de base s'exécutent dans le pool de stockage sur disque SYSBAS.

Avant d'utiliser IBM Systems Director Navigator for IBM i pour réaliser des tâches de gestion de disques, telles que la création d'un pool de stockage sur disque indépendant, vous devez configurer les autorisations appropriées pour les outils de maintenance en mode dédié.

Tâches associées

Enabling and accessing disk units

Configuration matérielle requise pour les disques commutés

Vous devez posséder du matériel spécifique pour utiliser des disques commutés.

Vous devez posséder l'un des éléments suivants pour utiliser des disques commutés :

- Une ou plusieurs unités d'extension (armoire/unités) se trouvant sur une boucle de liaison HSL.
- Un ou plusieurs processeurs d'entrée-sortie sur un bus partagé ou un processus d'entrée-sortie affecté à un pool d'entrée-sortie. Dans un environnement LPAR, vous pouvez basculer le processeur

d'entrée-sortie qui contient les disques commutés indépendants entre les partitions système sans aucune unité d'extension. Le processeur d'entrée-sortie doit se trouver sur le bus partagé par plusieurs partitions ou être affecté à un pool d'entrée-sortie. Tous les adaptateurs d'entrée-sortie du processeur d'E-S seront commutés.

Outre cette configuration matérielle requise, la planification physique suivante est requise pour les disques commutés :

- Des câbles de liaison HSL doivent être utilisés pour connecter les unités d'extension aux systèmes de la grappe. L'unité d'extension doit être physiquement adjacente dans la boucle HSL au système alternatif ou à l'unité d'extension détenue par le système alternatif. Vous pouvez inclure un maximum de deux systèmes (noeuds de grappe) sur chaque boucle HSL, bien que chaque système puisse être connecté à plusieurs boucles HSL. Il vous est également possible d'inclure jusqu'à quatre unités d'extension sur chaque boucle HSL, bien qu'un maximum de trois unités d'extension peut être inclus sur chaque segment de boucle. Sur une boucle HSL contenant deux systèmes, il existe deux segments séparés par les deux systèmes. Toutes les unités d'extension se trouvant sur un segment de boucle doivent se trouver dans le même groupe de ressources en grappe d'unité.
- Pour qu'une unité d'extension devienne commutable, elle doit se trouver le plus loin possible du système propriétaire du segment de boucle. Remarque : une erreur peut se produire si vous essayez de rendre une unité d'extension commutable alors qu'une autre unité d'extension se trouve plus loin que le système propriétaire qui n'est pas commutable.
- L'unité d'extension commutable doit être raccordé entre le réseau de contrôle de l'alimentation système et l'unité système qui servira de noeud principal au groupe de ressources en grappe d'unité. Le noeud principal peut être une partition logique principale ou secondaire de l'unité système. Si vous utilisez des partitions logiques, les bus système de l'unité d'extension visée doivent être détenus par la partition impliquée dans la grappe et dédiés à celle-ci.

Configuration logicielle pour les basculements de disque

Si vous comptez utiliser des disques commutés pour une haute disponibilité IBM i, assurez-vous de disposer de la configuration logicielle minimale requise.

- Pour utiliser les nouvelles fonctions et fonctionnalités de cette technologie, il est recommandé d'installer l'édition et la version la plus à jour du système d'exploitation sur chaque système ou partition logique participant à une solution à haute disponibilité basée sur cette technologie. Si le système de production et le système de secours utilisent des systèmes d'exploitation de niveaux différents, le système de secours doit posséder la version la plus récente.

  Remarque : Pour les systèmes se trouvant sur la même boucle HSL, allez sur le site Web de la solution High Availability pour vérifier que vous disposez de versions compatibles de IBM i.
- Il est nécessaire que l'une des interfaces graphiques suivantes exécute certaines des tâches de gestion de disque requises pour implémenter les pools de stockage sur disque indépendants.
  - IBM Systems Director Navigator for i
  - System i Navigator
- Vous devez installer IBM i , Option 41 HA Switchable Resources. L'option 41 permet de faire basculer les pools de stockage sur disque indépendants entre systèmes. Pour faire basculer un pool de stockage sur disque indépendant entre des systèmes, ces derniers doivent faire partie d'une grappe et le disque basculé indépendant doit être associé à un groupe de ressources de grappe d'unité dans cette grappe. L'option 41 sert également pour travailler avec des interfaces à haute disponibilité fournies avec le logiciel sous licence IBM PowerHA for i.

Information associée

High Availability and Clusters

Conditions requises des communications pour les disques commutés

Les disques commutés nécessitent au moins une interface de communications TCP/IP entre les systèmes de la grappe.

Pour la redondance, nous vous conseillons d'avoir au moins deux interfaces distinctes entre les systèmes.

Planification de la protection par disque miroir d'un site à l'autre

La protection par disque miroir d'un site à l'autre offre plusieurs technologies de haute disponibilité et de reprise après incident i5/OS : la protection géographique par disque miroir, Metro Mirror et Global Mirror.

Les technologies de protection par disque miroir d'un site à l'autre implémentent la reprise après incident en conservant des sites distincts généralement à une certaine distance les uns des autres. Chacune de ces technologies implique des exigences de communication et un configuration logicielle et matérielle propres. Toutefois, avant d'implémenter l'une de ces technologies, vous devez aussi planifier vos sites. En général, un site est considéré comme site de production ou source. Il contient vos données de production qui sont en miroir ou copiées sur le site à distance. Ce dernier, parfois appelé site de secours ou cible, contient la copie en miroir des données de production. En cas de sinistre de l'ensemble du site de production, le site de secours reprend l'activité avec les données en miroir. Avant de configurer une technologie de protection par disque miroir d'un site à l'autre, respectez ce qui suit pour les plans de vos sites.

Choisissez les sites de production et de secours.
Accédez aux ressources matérielles et logicielles actuelles sur chaque site pour savoir s'il manque des composants nécessaires à la solution de protection par disque miroir d'un site à l'autre.

Déterminez la distance entre les sites de production et de secours.
En fonction de la bande passante de communication et d'autres facteurs, la distance séparant les sites peut avoir une incidence sur les performances et le temps d'attente de la technologie de protection par disque miroir d'un site à l'autre choisie. Certaines technologies s'adaptent mieux aux site très éloignés, alors que d'autres voient dans ce cas leurs performances se dégrader.

Vérifiez que vous avez le droit approprié pour les outils de maintenance en mode dédié.

Avant d'utiliser IBM Systems Director Navigator for i5/OS pour réaliser des tâches de gestion de disques, vous devez configurer les autorisations appropriées pour les outils de maintenance en mode dédié.

Tâches associées

Enabling and accessing disk units

Planification de la protection géographique par disque miroir

La protection géographique par disque miroir est une sous-fonction de la protection par disque miroir d'un site à l'autre. Cette technologie permet les reprises après incident et la haute disponibilité dans les environnements IBM i.

Configuration matérielle pour la protection géographique par disque miroir :

Si vous comptez utiliser la protection géographique par disque miroir pour une haute disponibilité IBM i, assurez-vous de disposer de la configuration matérielle minimale requise.

- La configuration matérielle pour le pool de stockage sur disque indépendant doit être respectée.
- Au moins deux modèles IBM i, qui peuvent être séparés géographiquement, sont requis.
- Au moins deux ensembles de disque approximativement de la même capacité sont requis sur chaque site.
- Un pool de stockage distinct pour les travaux doit être configuré à l'aide des pools de stockage sur disque indépendant protégés géographiquement par disque miroir. L'application de la protection géographique par disque miroir peut provoquer le blocage du système dans des conditions de chargement extrêmes.
- La protection géographique par disque miroir est effectuée quand le pool de stockage sur disque est disponible. Quand elle est appliquée, la valeur système de l'heure du jour (QTIME) ne doit pas être modifiée.

- Les exigences de communications pour les pools de stockage sur disque indépendant sont critiques car elles affectent le débit.
- Le trafic de la protection géographique par disque miroir est réparti de manière aléatoire entre les différents canaux de communication disponibles. Si plusieurs canaux sont disponibles pour la protection géographique par disque miroir, il est recommandé d'utiliser des canaux de même vitesse et de même capacité.
- Il est recommandé d'utiliser un canal de communication séparé pour le signal de présence de la mise en grappe afin d'éviter les encombrements dans le trafic de la protection géographique par disque miroir.

Concepts associés

«Exigences de communications pour la protection géographique par disque miroir»
Quand vous implémentez une solution à haute disponibilité IBM i qui utilise la protection géographique par disque miroir, vous devez prévoir des lignes de transmission de sorte que le trafic de la protection géographique par disque miroir n'affecte pas les performances système.

Configuration logicielle requise pour la protection géographique par disque miroir :

Si vous comptez utiliser la protection géographique par disque miroir dans le cadre d'une solution à haute disponibilité IBM i, les logiciels suivants sont requis.

- Pour utiliser les fonctions avancées de la protection géographique par disque miroir, le programme sous licence IBM PowerHA for i doit être installé.
- Pour utiliser les nouvelles fonctions et fonctionnalités de cette technologie, il est recommandé d'installer l'édition et la version la plus à jour du système d'exploitation sur chaque système ou partition logique participant à une solution à haute disponibilité basée sur cette technologie. Si le système de production et le système de secours utilisent des systèmes d'exploitation de niveaux différents, le système de secours doit posséder la version la plus récente.

  Remarque : Pour les systèmes se trouvant sur la même boucle HSL, allez sur le site Web de la solution High Availability pour vérifier que vous disposez de versions compatibles de IBM i.
- Il est nécessaire que l'une des interfaces graphiques suivantes exécute certaines des tâches de gestion de disque requises pour implémenter les pools de stockage sur disque indépendants.
  - IBM Systems Director Navigator for i
  - System i Navigator
- Vous devez installer IBM i , Option 41 HA Switchable Resources. L'option 41 permet de faire basculer les pools de stockage sur disque indépendants entre systèmes. Pour faire basculer un pool de stockage sur disque indépendant entre des systèmes, ces derniers doivent faire partie d'une grappe et le disque basculé indépendant doit être associé à un groupe de ressources de grappe d'unité dans cette grappe. L'option 41 sert également pour travailler avec des interfaces à haute disponibilité fournies avec le logiciel sous licence IBM PowerHA for i.

Information associée

High Availability and Clusters

Exigences de communications pour la protection géographique par disque miroir :

Quand vous implémentez une solution à haute disponibilité IBM i qui utilise la protection géographique par disque miroir, vous devez prévoir des lignes de transmission de sorte que le trafic de la protection géographique par disque miroir n'affecte pas les performances système.

Les éléments suivants sont recommandés :

- La protection géographique par disque miroir peut générer un important trafic de communications. Si elle partage la même connexion IP avec une autre application, par exemple la mise en grappe, alors la protection géographique par disque miroir risque d'être suspendue, ce qui résultera en une synchronisation. De la même façon, la réponse de la mise en grappe risque d'être inacceptable, ce qui

résultera en des noeuds partitionnés. La protection géographique par disque miroir doit avoir ses propres lignes de communication. Sans cela, elle peut entrer en confit avec d'autres applications qui utilisent la même ligne de transmission et affecter les performances et le débit du réseau de l'utilisateur. Ceci inclut également la possibilité d'avoir un mauvais impact sur le contrôle des signaux de la grappe, ce qui résulte en un état de partition de grappe. Par conséquent, nous vous recommandons d'avoir des lignes de transmission pour la protection géographique par disque miroir et les grappes. La protection géographique par disque miroir prend en charge jusqu'à quatre lignes de transmission.

La protection géographique par disque miroir distribue les modifications sur plusieurs lignes afin d'optimiser les performances. Les données sont envoyées perpétuellement sur chaque ligne de transmission configurée, de 1 à 4. Ces quatre lignes de transmission permettent des performances élevées mais vous pouvez obtenir des performances relativement bonnes avec deux lignes.

Si vous utilisez plus d'une ligne de transmission entre les noeuds de la protection géographique par disque miroir, il est préférable de séparer ces lignes en sous-réseaux différents, de sorte que l'utilisation de ces lignes soit équilibrée sur les deux systèmes.

- Si votre configuration implique que plusieurs applications ou services nécessitent l'utilisation de la même ligne de transmission, certains de ces problèmes peuvent être évités en implémentant Quality of Service (QoS) via les fonctions TCP/IP d'IBM i. La solution QoS d'IBM i active les règles pour demander la priorité réseau et le débit des applications TCP/IP via le réseau.
- Assurez-vous que le débit de chaque connexion de port de données correspond. Cela signifie que la vitesse et le type de connexion doivent être les mêmes pour toutes les connexions entre des paires de système. Si le débit est différent, les performances seront limitées à la connexion la plus lente.
- Prenez en compte la méthode de distribution pour une session ASP de protection géographique par disque miroir. Avant la version 7.1, la copie miroir utilisait une méthode de communication synchrone entre le système de production et le système de copie miroir. Cette méthode de distribution convient bien pour les environnements à faible temps d'attente. Dans la version 7.1, les communications asynchrones sont prises en charge et sont utilisées entre le système de production et le système de copie miroir. Cette méthode de distribution convient bien pour les environnements à fort temps d'attente. Cette méthode de distribution consomme davantage de ressources système sur le noeud de copie de production que la distribution synchrone.
- Envisagez de configurer un réseau privé virtuel pour les connexions TCP/IP pour les raisons suivantes :
  - la sécurité de la transmission des données par leur chiffrement
  - une fiabilité améliorée de la transmission des données en envoyant une plus grande redondance

Concepts associés

«Configuration matérielle pour la protection géographique par disque miroir», à la page 53

Si vous comptez utiliser la protection géographique par disque miroir pour une haute disponibilité IBM i, assurez-vous de disposer de la configuration matérielle minimale requise.

Référence associée

Quality of Service (QoS)

Planification du journal pour la protection géographique par disque miroir :

Vous devez planifier la gestion du journal lors de l'implémentation d'une haute disponibilité en fonction de la protection géographique par disque miroir i5/OS.

La gestion du journal empêche la perte des transactions si votre système s'arrête anormalement. Quand vous consignez un objet, le système conserve un enregistrement des modifications que vous apportez à cet objet. Quelle que soit la solution à haute disponibilité que vous implémentez, la journalisation est considérée comme un bon moyen pour prévenir la perte des données pendant des indisponibilités système anormales.

Information associée

Journal management

Planification de la sauvegarde pour la protection géographique par disque miroir :

Avant d'implémenter une haute disponibilité fondée sur la protection géographique par disque miroir, vous devez comprendre et planifier une stratégie de sauvegarde dans cet environnement.

Avant de configurer une solution à haute disponibilité, évaluez votre stratégie de sauvegarde en cours et effectuez des modifications si nécessaire. La protection géographique par disque miroir n'autorise pas l'accès simultané à la copie miroir du pool de stockage sur disque indépendant, qui est censé effectuer des sauvegardes à distance. Si vous voulez sauvegarder depuis la copie protégée géographiquement par disque miroir, vous devez mettre au repos la protection par disque miroir sur le système de production et interrompre la copie protégée par disque miroir avec le suivi activé. Le suivi permet d'effectuer des modifications sur la production qui doit être suivie afin qu'elles soient synchronisées quand la copie protégée par disque miroir est remise en ligne. Puis vous devez mettre en fonction la copie déconnectée du pool de stockage sur disque indépendant, effectuer la procédure de sauvegarde, mettre hors fonction la copie miroir interrompue puis redémarrer le pool de stockage sur disque indépendant sur l'hôte de production d'origine. Ce processus nécessite uniquement une resynchronisation partielle des données entre les copies de production et celles protégées par disque miroir.

Votre système est vulnérable lors des sauvegardes et de la synchronisation. Nous vous conseillons également de suspendre la protection par disque miroir avec le suivi activé, car cela accélère le processus de synchronisation. La synchronisation est également requise pour toute interruption de transmission permanente, telle que la perte de toutes les voies de communication entre les systèmes source et cible pour une période de temps étendue. Vous pouvez également utiliser des voies de communications redondantes pour éliminer les risques associées aux incidents de communication.

Nous vous conseillons d'utiliser également la protection géographique par disque miroir dans au moins trois partitions système ou logiques dans lesquelles la copie de production du pool de stockage sur disque indépendant peut être basculée vers un autre système du même site susceptible de conserver la protection géographique par disque miroir.

Concepts associés

«Scénario : Réalisation de sauvegardes dans un environnement de protection géographique par disque miroir», à la page 131
Ce scénario fournit une présentation des tâches nécessaires à la réalisation d'une sauvegarde distante dans une solution à haute disponibilité i5/OS qui utilise la protection géographique par disque miroir.

«Scénario : Disque commuté avec protection géographique par disque miroir», à la page 88
Ce scénario décrit une solution à haute disponibilité i5/OS qui utilise des disques commutés dans une grappe à trois noeuds. Cette solution fournit la reprise après incident et la haute disponibilité.

Planification des performances pour la protection géographique par disque miroir :

Lors de l'implémentation d'une solution de protection géographique par disque miroir, vous devez comprendre et organiser votre environnement afin de minimiser l'impact potentiel sur les performances.

Une variété de facteurs peut influencer les performances de la protection géographique par disque miroir. Les facteurs suivants fournissent des considérations de planification générales pour optimiser les performances dans un environnement de protection géographique par disque miroir :

Considérations relatives à l'unité centrale

La protection géographique par disque miroir augmente la charge de l'unité centrale, de sorte qu'il y ait une capacité suffisante d'excédent de l'unité centrale. Vous aurez peut-être besoin d'autres processeurs pour augmenter la capacité de traitement. En règle générale, les partitions que vous utilisez pour exécuter

la protection géographique par disque miroir ont besoin de plusieurs processeurs partiels. Dans une configuration d'unité centrale minimale, vous pouvez voir potentiellement entre 5 et 20 % de la surcharge de l'unité centrale lors de l'exécution de la protection géographique par disque miroir. Si votre système de sauvegarde par disque miroir possède moins de processeurs que votre système de production et que de nombreuses opérations d'écriture existent, la surcharge de l'unité centrale sera probablement remarquable et pourra affecter les performances.

Remarques relatives à la taille du pool de base

Si vous utilisez la distribution asynchrone pour la protection géographique par disque miroir, il peut être nécessaire d'augmenter également la quantité d'espace de stockage dans le pool de base du système. L'ampleur de cette augmentation dépend d'abord du temps d'attente existant lié à la distance entre les deux systèmes. Plus le temps d'attente est important, plus vous devrez augmenter l'espace de stockage du pool de base.

Considérations relatives à la taille du pool machine

Pour obtenir une protection géographique par disque miroir optimale, particulièrement lors de la synchronisation, augmentez la taille de votre pool machine par au moins la quantité indiquée par la formule suivante :

- La quantité de stockage supplémentaire du pool machine est : 300 Mo + 0,3 Mo x le nombre d'ARM de disque du pool de stockage sur disque indépendant. Les exemples suivants indiquent le stockage du pool machine supplémentaire nécessaire aux pools de stockage sur disque munis respectivement de 90 et 180 ARM :
  - 300 + (0,3 x 90 ARM) = 327 Mo supplémentaires de capacité de stockage pour le pool machine
  - 300 + (0,3 x 180 ARM) = 354 Mo supplémentaires de capacité de stockage pour le pool machine

La capacité de stockage supplémentaire du pool machine est requise sur tous les noeuds du groupe de ressources en grappe afin que les noeuds cible aient assez d'espace de stockage en cas de basculement ou de reprise en ligne. Comme toujours, plus il y a d'unités de disque dans le pool de stockage sur disque indépendant, plus les performances seront optimales, car plus d'opérations peuvent être effectuées en parallèle.

Pour empêcher que la fonction d'ajustement des performances réduise la taille du pool machine, effectuez l'une des tâches suivantes :

1. Définissez la taille minimale du pool machine sur la quantité calculée (la taille actuelle plus la taille supplémentaire de la protection géographique par disque miroir de la formule) à l'aide de la commande WRKSHRPOOL ou CHGSHRPOOL.

   Remarque : Nous vous conseillons d'utiliser cette option avec l'option WRKSHRPOOL.
2. Définissez la valeur système QPFRADJ (Ajuster automatiquement les pools de mémoire et les niveaux d'activité) sur zéro, ce qui empêche la fonction d'ajustement des performances de modifier la taille du pool machine.

Considérations relatives aux unités de disque

Les performances des unités de disque et de l'adaptateur d'E-S peuvent affecter les performances globales de la protection géographique par disque miroir. Ceci est particulièrement vrai quand le sous-système de disque est plus lent que le système protégé par disque miroir. Quand la protection géographique sur disque miroir est en mode miroir synchrone, toutes les opérations d'écriture de la copie de production sont protégées par les écritures de la copie miroir sur le disque. Par conséquent, un sous-système de disque cible lent peut affecter les performances côté source. Vous pouvez minimiser cet effet sur les performances en exécutant la protection géographique par disque miroir en mode miroir asynchrone. L'exécution en mode miroir asynchrone réduit l'attente du sous-système de disque du côté cible, et renvoie une confirmation au côté source quand la page de mémoire est enregistrée du côté cible.

Considérations relatives au pool de stockage sur disque système

Comme pour toute configuration d'un disque système, le nombre d'unités de disques disponibles pour l'application peut avoir une incidence importante sur les performances. Si vous placez une charge de travail supplémentaire sur un nombre limité d'unités de disques, les attentes des disques peuvent s'allonger, ainsi que les temps de réponse à l'application. Ce point est notamment important dans le cas d'une mémoire de travail dans un système configuré avec des pools de stockage sur disque indépendant. Toute la mémoire de travail est écrite dans le pool de stockage sur disque SYSBAS. Si votre application n'emploie pas de mémoire de travail, vous pouvez travailler avec moins de bras de disque dans le pool de stockage sur disque SYSBAS. Vous devez aussi penser que le système d'exploitation et les fonctions de base s'exécutent dans le pool de stockage sur disque SYSBAS. Ceci vaut également pour le système de copie miroir car les messages TCP envoyés à la copie miroir peuvent éventuellement charger des pages dans l'ASP système.

Considérations relatives à la configuration du réseau

Le câblage et la configuration du réseau peuvent affecter les performances de la protection géographique par disque miroir. Outre la garantie que l'adressage réseau est configuré dans plusieurs sous-réseaux différents pour chaque ensemble d'adresses IP de port de données, le câble et la configuration du réseau doivent également être configurés de la même manière.

Planification de Metro Mirror

La haute disponibilité i5/OS supporte Metro Mirror, qui offre une haute disponibilité et une reprise après incident. Pour configurer et gérer efficacement une solution à haute disponibilité qui utilise cette technologie, vous devez effectuer une planification adéquate.

Information associée

Guidelines and recommendations for using Copy Services functions with DS6000

Guidelines and recommendations for using Copy Services functions with DS8000

Configuration matérielle pour Metro Mirror :

Pour configurer et gérer une solution à haute disponibilité i5/OS utilisant la technologie Metro Mirror, vous devez vérifier que la configuration matérielle minimale est respectée.

La configuration matérielle minimale suivante est conseillée :

- Au moins deux modèles System i séparées géographiquement avec au moins une unité de stockage externe IBM System Storage DS8000 connectée à chaque système. Les unités de stockage externe DS8000 sont prises en charge sur tous les modèles System i prenant en charge la connexion Fibre Channel du stockage externe.
- L'un des adaptateurs de canal optique suivants est obligatoire :
  - Contrôleur de disques PCI de canal optique 2766 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 2787 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 5760 4 gigabits
- Un nouveau processeur d'E-S est obligatoire pour supporter l'unité source IPL externe sur le système DS8000 :
  - Processeur d'E-S 2847 PCI-X pour la source IPL du réseau de stockage
- Avant toute configuration, vous devez avoir défini la taille appropriée du disque pour la mémoire système. Il vous faut un ensemble de disques pour la source, un ensemble équivalent d'unités de disques pour la cible, et un autre pour chaque copie cohérente.

Information associée

iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5

IBM System Storage DS6000 Information Center

IBM System Storage DS8000 Information Center

Configuration logicielle requise pour Metro Mirror :

Avant de configurer une solution à haute disponibilité IBM i utilisant Metro Mirror, vérifiez que la configuration logicielle minimale est respectée.

La configuration logicielle minimale pour Metro Mirror est la suivante :

- Chaque modèle IBM i dans la solution à haute disponibilité doit exécuter au moins IBM i V6R1 pour une utilisation avec le programme sous licence IBM PowerHA for i.

  Remarque : Pour les éditions antérieures, vous pouvez toujours utiliser IBM Advanced Copy Services for PowerHA on i, édité par Lab Services, pour une utilisation avec les solutions IBM System Storage. Si vous utilisez Global Mirror sur plusieurs plateformes ou que vous voulez implémenter Global Mirror sur plusieurs partitionsIBM i, vous pouvez également utiliser le produit IBM Advanced Copy Services for PowerHA on i.
- Un programme sous licence IBM PowerHA for i installé sur chaque système participant à la solution à haute disponibilité qui utilise Metro Mirror.
- Vous devez installer IBM i , Option 41 HA Switchable Resources. L'option 41 permet de faire basculer les pools de stockage sur disque indépendants entre systèmes. Pour faire basculer un pool de stockage sur disque indépendant entre des systèmes, ces derniers doivent faire partie d'une grappe et le disque basculé indépendant doit être associé à un groupe de ressources de grappe d'unité dans cette grappe. L'option 41 sert également pour travailler avec des interfaces à haute disponibilité fournies avec le logiciel sous licence IBM PowerHA for i.
- Pour contrôler la mémoire, le logiciel sous licence IBM PowerHA for i a aussi besoin d'une interface de ligne de commande de mémoire (DSCLI). DSCLI est un logiciel obligatoire pour toutes les solutions IBM System Storage. Pour gérer l'une des solutions IBM System Storage, par exemple la fonction FlashCopy, Metro Mirror ou Global Mirror, l'interface DSCLI doit être installée sur chaque système ou partition prenant part à la solution à haute disponibilité qui utilise ces solutions de stockage. DSCLI demande en outre cette configuration logicielle :
  - Java version 1.4
  - Option 35 (fournisseur de service cryptographique) installé sur chaque système ou partition
- Vérifiez que les derniers PTF ont été installés.

Information associée

iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5

IBM System Storage DS6000 Information Center

IBM System Storage DS8000 Information Center

Exigences de communication pour Metro Mirror :

Avant de configurer la solution à haute disponibilité i5/OS utilisant Metro Mirror, vérifiez que les exigences de communication minimum ont été respectées.

Pour utiliser la technologie Metro Mirror, vous devez employer ou planifier l'emploi d'un réseau de stockage (SAN).

Un *SAN* est une infrastructure d'informations dédiée, gérée de façon centrale et sécurisée qui permet tout type d'interconnexion entre des systèmes et des systèmes de stockage. La connectivité du SAN est obligatoire pour utiliser des unités de mémoire externe IBM System Storage, par exemple des unités de mémoire externe systèmesDS8000.

Ci-après les exigences de communication minimum pour une solution à haute disponibilité i5/OS utilisant Metro Mirror :

- L'un des adaptateurs de canal optique suivants est obligatoire :
  - Contrôleur de disques PCI de canal optique 2766 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 2787 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 5760 4 gigabits
- Le produit System i supporte une variété de commutateurs et de directeurs SAN. Voir le site Web du réseau de stockage (SAN) pour obtenir la liste complète des commutateurs et des directeurs pris en charge.
- Par ailleurs, il est fortement conseillé d'exploiter le multi-accès d'entrée-sortie afin d'améliorer le test de résistance et les performances dans leur ensemble. Le multi-accès d'entrée-sortie permet d'avoir plusieurs unités de canal optique configurées pour les mêmes unités de disques logiques dans la mémoire. Si la configuration est correcte, des unités simples, des boîtiers d'entrée-sortie, voire des boucles de liaison HSL peuvent échouer sans perdre les connexions aux unités de disques. Le multi-accès offre aussi des performances accrues en répartissant les charges de travail entre toutes les connexions disponibles (chemins). Chaque connexion pour une unité de disques de multi-accès fonctionne de façon indépendante. Avec plusieurs connexions, le test de résistance est amélioré car la mémoire disque est utilisable même si un chemin échoue.

Référence associée

Site Web Storage area network (SAN)

Planification du journal pour Metro Mirror :

La journalisation est importante pour augmenter le temps de reprise de toutes les solutions à haute disponibilité. Dans le cas de technologies basées sur IBM System Storage, telles que Metro Mirror, il est indispensable d'utiliser la journalisation pour forcer les opérations d'écriture sur des unités de mémoire externe, sachant que la protection par disque miroir de données se produit hors de la mémoire System i.

La gestion du journal empêche la perte des transactions si votre système s'arrête anormalement. Quand vous consignez un objet, le système conserve un enregistrement des modifications que vous apportez à cet objet. Quelle que soit la solution à haute disponibilité que vous implémentez, la journalisation est considérée comme un bon moyen pour prévenir la perte des données pendant des indisponibilités système anormales.

Information associée

Journal management

Planification de sauvegarde pour Metro Mirror :

Avec Metro Mirror, vous pouvez utiliser la fonction FlashCopy afin de créer une copie des données stockées dans des unités de mémoire externe IBM System Storage.

Les opérations FlashCopy permettent de créer des copies instantanées. Dès que l'opération FlashCopy est traitée, les volumes source et cible sont disponibles pour l'application. La fonction FlashCopy peut être utilisée avec d'autres technologies IBM System Storage telles que Metro Mirror et Global Mirror, afin de créer une copie instantanée cohérente des données sur un site à distance, puis sauvegarder ces données avec vos procédures standard de sauvegarde. Pour implémenter la fonction FlashCopy, procédez comme suit :

- Identifiez les volumes source et cible pour les relations FlashCopy. Vous devez sélectionner des volumes cible FlashCopy dans différents rangs pour de meilleures performances.
- Assimilez les remarques sur la cohérence des données FlashCopy. Dans certains environnements, les données sont stockées dans le cache de mémoire système et écrites ultérieurement sur le disque. Pour éviter ces types d'actions de redémarrage, vérifiez que toutes les données liées au volume source FlashCopy ont été écrites sur le disque avant d'effectuer l'opération FlashCopy.
- Vous pouvez utiliser un volume source Metro Mirror existant comme volume cible FlashCopy. Vous pouvez ainsi créer une copie instantanée avec un volume cible d'une paire FlashCopy et appliquer la protection par disque miroir aux données sur un volume Metro Mirror source à un emplacement à distance.

Planification des performances pour Metro Mirror :

Vous devez comprendre ces remarques sur les performances avant de configurer Metro Mirror.

Avant d'utiliser Metro Mirror, prenez en compte les exigences et les instructions suivantes :

- Les volumes source et cible dans une relation Metro Mirror doivent être du même type de mémoire.
- Les volumes logiques source et cible doivent être de la même taille ou le volume cible doit être plus grand.
- Pour les environnements Metro Mirror, distribuez les charges de travail sans envoyer toutes les mises à jour à un petit nombre de volumes sur une même unité de stockage cible. L'impact sur les performances de l'unité de stockage du site cible se répercute sur celles du site source.
- Comme pour toute configuration d'un disque système, le nombre d'unités de disques disponibles pour l'application peut avoir une incidence importante sur les performances. Si vous placez une charge de travail supplémentaire sur un nombre limité d'unités de disques, les attentes des disques peuvent s'allonger, ainsi que les temps de réponse à l'application. Ce point est notamment important dans le cas d'une mémoire de travail dans un système configuré avec des pools de stockage sur disque indépendant. Toute la mémoire de travail est écrite dans le pool de stockage sur disque SYSBAS. Si votre application n'emploie pas de mémoire de travail, vous pouvez travailler avec moins de bras de disque dans le pool de stockage sur disque SYSBAS. Vous devez aussi penser que le système d'exploitation et les fonctions de base s'exécutent dans le pool de stockage sur disque SYSBAS.

Information associée

Guidelines and recommendations for using Copy Services functions with DS6000

Guidelines and recommendations for using Copy Services functions with DS8000

Planification de Global Mirror

La haute disponibilité i5/OS supporte Global Mirror, qui offre une haute disponibilité et une reprise après incident dans des environnements utilisant des solutions de mémoire externe. Pour configurer et gérer efficacement une solution à haute disponibilité qui utilise cette technologie, vous devez effectuer une planification adéquate.

La technologie Global Mirror d'IBM System Storage impose que tous les utilisateurs partagent une connexion Global Mirror. La fonction Global Mirror à haute disponibilité i5/OS permet à une seule partition System i d'être active dans la session Global Mirror sur un serveur System Storage donné. Les autres partitions ou serveurs System i d'autres plateformes ne peuvent pas utiliser simultanément Global Mirror. L'ajout de plusieurs utilisateurs à une session Global Mirror donne des résultats imprévisibles.

Si vous utilisez Global Mirror sur plusieurs plateformes ou si vous voulez implémenter Global Mirror sur plusieurs partitions System i, vous pouvez utiliser IBM Copy Services for System i. Cette offre est disponible auprès de Lab Services.

Information associée

Guidelines and recommendations for using Copy Services functions with DS6000

Guidelines and recommendations for using Copy Services functions with DS8000

Configuration matérielle requise pour Global Mirror :

Pour configurer et gérer une solution à haute disponibilité i5/OS qui utilise la technologie Global Mirror, vous devez vous assurer que la configuration matérielle minimale requise est respectée.

La configuration matérielle minimale suivante est requise pour Global Mirror :

- Au moins deux modèles System i séparées géographiquement avec au moins une unité de stockage externe IBM System Storage DS8000 connectée à chaque système. Les unités de stockage externe DS8000 sont prises en charge sur tous les modèles System i prenant en charge la connexion Fibre Channel du stockage externe.
- L'un des adaptateurs de canal optique suivants est obligatoire :
  - Contrôleur de disques PCI de canal optique 2766 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 2787 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 5760 4 gigabits
- Un nouveau processeur d'E-S est obligatoire pour supporter l'unité source IPL externe sur le système DS8000 :
  - Processeur d'E-S 2847 PCI-X pour la source IPL du réseau de stockage
- Avant toute configuration, vous devez avoir défini la taille appropriée du disque pour la mémoire système. Il vous faut un ensemble de disques pour la source, un ensemble équivalent d'unités de disques pour la cible, et un autre pour chaque copie cohérente.

Information associée

iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5

IBM System Storage DS6000 Information Center

IBM System Storage DS8000 Information Center

Configuration logicielle requise pour Global Mirror :

Avant de configurer une solution à haute disponibilité IBM i utilisant Global Mirror, vérifiez que la configuration logicielle minimale est respectée.

La configuration logicielle minimale requise pour Global Mirror est la suivante :

- Chaque modèle IBM i dans la solution à haute disponibilité doit exécuter au moins IBM i V6R1 pour une utilisation avec le programme sous licence IBM PowerHA for i.

  Remarque : Pour les éditions antérieures, vous pouvez toujours utiliser IBM Advanced Copy Services for PowerHA on i, édité par Lab Services, pour une utilisation avec les solutions IBM System Storage. Si vous utilisez Global Mirror sur plusieurs plateformes ou que vous voulez implémenter Global Mirror sur plusieurs partitionsIBM i, vous pouvez également utiliser le produit IBM Advanced Copy Services for PowerHA on i.
- Un programme sous licence IBM PowerHA for i installé sur chaque système participant à la solution à haute disponibilité qui utilise Global Mirror.
- Pour contrôler la mémoire, le logiciel sous licence IBM PowerHA for i a aussi besoin d'une interface de ligne de commande de mémoire (DSCLI). DSCLI est un logiciel obligatoire pour toutes les solutions IBM System Storage. Pour gérer l'une des solutions IBM System Storage, par exemple la fonction

FlashCopy, Metro Mirror ou Global Mirror, l'interface DSCLI doit être installée sur chaque système ou partition prenant part à la solution à haute disponibilité qui utilise ces solutions de stockage. DSCLI demande en outre cette configuration logicielle :
  - Java version 1.4
  - Option 35 (fournisseur de service cryptographique) installé sur chaque système ou partition
- Vérifiez que les derniers PTF ont été installés.

Information associée

iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5

IBM System Storage DS6000 Information Center

IBM System Storage DS8000 Information Center

Configuration minimale requise des communications pour Global Mirror :

Avant de configurer une solution à haute disponibilité i5/OS qui utilise Global Mirror, vous devez vous assurer que la configuration minimale requise des communications a été respectée.

Pour utiliser la technologie Global Mirror, vous devez utiliser ou envisager d'utiliser un réseau de stockage.

Un *SAN* est une infrastructure d'informations dédiée, gérée de façon centrale et sécurisée qui permet tout type d'interconnexion entre des systèmes et des systèmes de stockage. La connectivité du SAN est obligatoire pour utiliser des unités de mémoire externe IBM System Storage, par exemple des unités de mémoire externe systèmesDS8000.

Vous trouverez ci-après la configuration minimale requise des communications pour une solution à haute disponibilité i5/OS qui utilise Global Mirror :
- L'un des adaptateurs de canal optique suivants est obligatoire :
  - Contrôleur de disques PCI de canal optique 2766 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 2787 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 5760 4 gigabits
- Le produit System i supporte une variété de commutateurs et de directeurs SAN. Voir le site Web du réseau de stockage (SAN) pour obtenir la liste complète des commutateurs et des directeurs pris en charge.
- Par ailleurs, il est fortement conseillé d'exploiter le multi-accès d'entrée-sortie afin d'améliorer le test de résistance et les performances dans leur ensemble. Le multi-accès d'entrée-sortie permet d'avoir plusieurs unités de canal optique configurées pour les mêmes unités de disques logiques dans la mémoire. Si la configuration est correcte, des unités simples, des boîtiers d'entrée-sortie, voire des boucles de liaison HSL peuvent échouer sans perdre les connexions aux unités de disques. Le multi-accès offre aussi des performances accrues en répartissant les charges de travail entre toutes les connexions disponibles (chemins). Chaque connexion pour une unité de disques de multi-accès fonctionne de façon indépendante. Avec plusieurs connexions, le test de résistance est amélioré car la mémoire disque est utilisable même si un chemin échoue.

Référence associée

Site Web Storage area network (SAN)

Planification du journal pour Global Mirror :

La journalisation est importante pour réduire le temps de reprise de toutes les solutions à haute disponibilité. Si vous utilisez des technologies IBM System Storage, telles que Global Mirror, la journalisation impose les opérations d'écriture dans des unités de stockage externes, ce qui est nécessaire car la protection par disque miroir des données se produit en dehors du stockage System i.

La gestion du journal empêche la perte des transactions si votre système s'arrête anormalement. Quand vous consignez un objet, le système conserve un enregistrement des modifications que vous apportez à cet objet. Quelle que soit la solution à haute disponibilité que vous implémentez, la journalisation est considérée comme un bon moyen pour prévenir la perte des données pendant des indisponibilités système anormales.

Information associée

Journal management

Planification de la sauvegarde pour Global Mirror :

Quand vous utilisez la technologie Global Mirror dans votre solution à haute disponibilité, vous pouvez utiliser la fonctionnalité FlashCopy pour créer un copie instantanée de vos données.

Les opérations FlashCopy permettent de créer des copies instantanées. Dès que l'opération FlashCopy est traitée, les volumes source et cible sont disponibles pour l'application. La fonction FlashCopy peut être utilisée avec d'autres technologies IBM System Storage telles que Metro Mirror et Global Mirror, afin de créer une copie instantanée cohérente des données sur un site à distance, puis sauvegarder ces données avec vos procédures standard de sauvegarde. Pour implémenter la fonction FlashCopy, procédez comme suit :

- Identifiez les volumes source et cible pour les relations FlashCopy. Vous devez sélectionner des volumes cible FlashCopy dans différents rangs pour de meilleures performances.
- Assimilez les remarques sur la cohérence des données FlashCopy. Dans certains environnements, les données sont stockées dans le cache de mémoire système et écrites ultérieurement sur le disque. Pour éviter ces types d'actions de redémarrage, vérifiez que toutes les données liées au volume source FlashCopy ont été écrites sur le disque avant d'effectuer l'opération FlashCopy.

Planification des performances pour Global Mirror :

Vous devez comprendre ces considérations relatives aux performances avant de configurer Global Mirror.

Avant d'utiliser Global Mirror, lisez les instructions suivantes relatives aux performances :

- Les volumes source et cible dans une relation Metro Mirror doivent être du même type de mémoire.
- Les volumes source et cible dans une relation Metro Mirror doivent être du même type de mémoire.
- Comme pour toute configuration d'un disque système, le nombre d'unités de disques disponibles pour l'application peut avoir une incidence importante sur les performances. Si vous placez une charge de travail supplémentaire sur un nombre limité d'unités de disques, les attentes des disques peuvent s'allonger, ainsi que les temps de réponse à l'application. Ce point est notamment important dans le cas d'une mémoire de travail dans un système configuré avec des pools de stockage sur disque indépendant. Tout stockage temporaire est écrit dans le pool de stockage sur disque SYSBAS. Si votre application n'utilise aucun stockage temporaire, vous pouvez alors utiliser moins d'ARM de disque dans le pool de stockage sur disque SYSBAS. Vous devez aussi penser que le système d'exploitation et les fonctions de base s'exécutent dans le pool de stockage sur disque SYSBAS.

Information associée

Guidelines and recommendations for using Copy Services functions with DS6000

Guidelines and recommendations for using Copy Services functions with DS8000

Planification de la réplication logique

Plusieurs copies des données sont conservées avec la réplication logique. Les données sont répliquées (ou copiées) d'un noeud principal dans la grappe vers les noeuds de secours indiqués dans le domaine de reprise. Lorsqu'une indisponibilité du système se produit sur le noeud principal, les données restent disponibles car un noeud de secours désigné prend le relais comme point d'accès principal.

La *réplication logique* crée une copie d'un élément en temps réel. Il s'agit du processus de copie d'objets d'un noeud dans une grappe vers un ou plusieurs autres noeuds dans la grappe. La réplication logique rend et conserve les objets identiques sur vos systèmes. Si vous modifiez un objet sur un noeud dans une grappe, cette modification est répliquée sur les autres noeuds de cette grappe.

Vous devez décider quelle technologie utiliser pour la réplication logique. Les solutions suivantes sont disponibles pour effectuer une réplication logique dans votre grappe :

- **IBM iCluster for i**

  Produit de réplication logique IBM qui fournit une haute disponibilité sur IBM i.
- **Produits des partenaires commerciaux IBM**

  Le logiciel de réplication de données du partenaire commercial IBM vous permet de répliquer des objets depuis une grappe reconnue vers plusieurs noeuds.
- **Application de réplication personnalisée**

  La gestion de journaux IBM permet d'enregistrer l'activité des objets sur votre système. Vous pouvez écrire une application en recourant à la gestion de journaux pour effectuer une réplication logique.

Information associée

Journal management

Identification des systèmes à utiliser pour la réplication logique

Lorsque vous identifiez les systèmes à utiliser pour la réplication logique, plusieurs aspects clés sont à prendre en compte.

Ces aspects sont :

- les performances,
- la capacité disque,
- les données vitales,
- la prévention contre les sinistres.

Si votre système tombe en panne, vous devez savoir quelles données et quelles applications sont en cours d'exécution sur votre système principal et votre système de secours. Vous devez placer les données vitales sur le système le plus à même de gérer la charge de travail en cas de panne. L'objectif est d'éviter que l'espace disque devienne insuffisant. Si votre système principal manque d'espace et tombe en panne, il est fort probable que votre système de secours échoue à son tour par manque d'espace également. Pour être sûr que votre centre de données ne sera pas totalement détruit en cas de catastrophe naturelle (inondation, tornade, ouragan), vous devez placer le système répliqué à un autre emplacement à distance.

Produits de gestion de grappe proposés par les partenaires commerciaux IBM et disponibles

Il existe d'autres produits de gestion des grappes en plus d'IBM PowerHA for i.

IBM iCluster for i, ainsi que d'autres produits, proposent des solutions logicielles pour la réplication et la gestion des grappes. La plupart de ces solutions reposent sur la réplication logique. La réplication logique utilise la journalisation à distance ou des technologies similaires pour transférer les modifications des objets vers un système distant où elles sont appliquées à des objets cible. Outre les solutions de gestion PowerHA, vous pouvez acheter d'autres produits de gestion de grappe utilisant une technologie de réplication logique. Ces produits comprennent aussi une interface de gestion en général.

Planification du journal pour la réplication logique

Si vous utilisez une réplication logique, vous devriez utiliser la journalisation pour forcer l'écriture à partir de la copie des données de production vers la copie des données de sauvegarde.

La gestion du journal empêche la perte des transactions si votre système s'arrête anormalement. Quand vous consignez un objet, le système conserve un enregistrement des modifications que vous apportez à cet objet. Quelle que soit la solution à haute disponibilité que vous implémentez, la journalisation est considérée comme un bon moyen pour prévenir la perte des données pendant des indisponibilités système anormales.

Dans des environnements de réplication logique, la journalisation est la base de la solution, et en tant que telle, elle constitue une condition requise pour l'implémentation d'une solution fondée sur cette technologie. Avec une réplication logique, une copie en temps réel d'un système de sauvegarde peut être limitée en fonction de la taille de l'objet en cours de réplication. Par exemple, un programme met à jour un enregistrement qui se trouve dans un fichier consigné. Dans le cadre de cette même opération, il met également à jour un objet, tel qu'un espace utilisateur, qui n'est pas consigné. La copie de sauvegarde devient complètement cohérente quand l'espace utilisateur est entièrement répliqué dans le système de sauvegarde. En pratique, si le système principal tombe en panne, et que l'espace utilisateur n'est pas encore totalement répliqué, un processus de reprise manuelle est requis pour réconcilier l'état de l'espace utilisateur afin qu'il corresponde à la dernière opération valide dont les données ont été complètement répliqués.

Information associée

Journal management

Planification de la sauvegarde pour la réplication logique

Si vous utilisez une technologie de réplication logique, vous devez planifier les opérations de sauvegarde dans cet environnement.

La réplication logique réplique les modifications apportées aux objets, tels que les fichiers ou les programmes d'une copie de production, vers une copie de sauvegarde. La réplication se fait en quasi temps réel (en simultané). En règle général, si l'objet, tel qu'un fichier, est consigné, la réplication est gérée au niveau de l'enregistrement. L'avantage clé de cette technologie est que la copie de sauvegarde est accessible en temps réel pour les opérations de sauvegarde. Vous pouvez réaliser une sauvegarde distante sur la copie de sauvegarde des données sans interrompre la version de production des données.

Planification des performances pour la réplication logique

Si vous utilisez une technologie de réplication logique dans le cadre d'une solution à haute disponibilité, vous devez connaître les effets potentiels sur les performances de cette solution.

Avec la réplication logique, les effets potentiels sur les performances concernent le temps d'attente du processus de réplication. Ceci a un rapport avec la durée du temps de décalage entre l'heure à laquelle les modifications ont été apportées sur le système source et l'heure à laquelle ces modifications sont devenues disponibles sur le système de sauvegarde. La journalisation distante synchrone peut minimiser cela de façon considérable. Quel que soit le mécanisme de transmission utilisé, vous devez prévoir de façon adéquate votre volume de transmission et planifier correctement vos lignes et vitesses de transmission pour garantir que votre environnement peut gérer des volumes de réplication quand ils atteignent leur limite. Dans un environnement à volume élevé, le temps d'attente peut poser problème du côté cible même si vos fonctions de transmission sont correctement planifiées.

Chapitre 2. Planification du test de résistance de l'environnement

Grâce au test de résistance de l'environnement, vous savez que vos objets et vos attributs restent cohérents parmi les ressources définies dans l'environnement à haute disponibilité. Vous devez identifier les ressources qui requièrent un environnement cohérent afin de fonctionner correctement, puis créer un domaine d'administration de grappe pour que les attributs de ces ressources restent cohérents dans votre solution à haute disponibilité.

Planification pour un domaine d'administration de grappe

Le domaine d'administration de grappe suppose une planification pour contrôler des ressources synchronisées à travers les noeuds qu'il contient. Pour qu'une application s'exécute de façon cohérente sur n'importe quel système dans un environnement à haute disponibilité, toutes les ressources affectant le comportement de cette application doivent être identifiées, ainsi que les noeuds sur lesquels elle s'exécutera ou avec des données la concernant.

Un administrateur de grappe peut créer un domaine d'administration de grappe et ajouter des ressources contrôlées synchronisées à travers les noeuds. La grappe i5/OS fournit la liste des ressources système pouvant être synchronisées par un domaine d'administration de grappe et représentées par des entrées de ressources contrôlées.

Lors de la conception d'un domaine d'administration de grappe, vous devez répondre aux questions suivantes :

Quels noeuds seront inclus dans le domaine d'administration de grappe ?
Vous devez identifier les noeuds d'une grappe qui doivent être contrôlés par le domaine d'administration de grappe. Il s'agit des noeuds qui représentent les systèmes sur lesquels une application peut s'exécuter ou des données d'application figurent et qui ont besoin d'un environnement d'exécution cohérent. Les noeuds ne peuvent pas se trouver dans plusieurs domaines d'administration de grappe. Par exemple, s'il existe quatre noeuds dans une grappe (Noeud A, Noeud B, Noeud C et Noeud D), les noeuds A et B peuvent se trouver dans un domaine d'administration et les noeuds C et D dans un autre. Toutefois, les noeuds B et C ne peuvent pas aussi être dans un troisième domaine d'administration de grappe s'ils se trouvent toujours dans le domaine d'origine.

Quelle sera la convention de dénomination pour les domaines d'administration de grappe ?
En fonction de la complexité et de la taille de votre environnement groupé, vous devez établir une convention de dénomination standard pour les groupes de ressources en grappe homologues et les domaines d'administration de grappe. Comme un groupe de ressources en grappe est créé en même temps qu'un domaine d'administration, vous pouvez différencier les autres groupes de ressources homologues de ceux représentant des domaines d'administration. Par exemple, les groupes de ressources en grappe homologues qui représentent des domaines d'administration de grappe peuvent être nommés *ADMDMN1*, *ADMDMN2* et ainsi de suite, et les autres groupes homologues *PEER1*. Vous pouvez aussi utiliser l'API List Cluster Resource Group Information (QcstListClusterResourceGroupIn) pour savoir si le groupe de ressources en grappe homologue est utilisé comme domaine d'administration de grappe. Un groupe de ressources en grappe homologue qui représente un domaine d'administration de grappe peut être identifié par son identificateur d'application, à savoir QIBM.AdminDomain.

Planification des entrées de ressources contrôlées

Les ressources contrôlées sont des objets i5/OS pouvant être définis dans un domaine d'administration de grappe. Ces ressources doivent rester cohérentes à travers les systèmes dans un environnement à haute disponibilité ; sinon, en cas d'indisponibilité, le fonctionnement des applications peut être imprévu. Vous devez planifier les ressources prises en charge dans votre environnement qui doivent être contrôlées.

Vous devez déterminer les ressources système devant être synchronisées. Vous pouvez sélectionner des attributs pour chaque ressource afin de personnaliser ce qui est synchronisé. Les applications qui s'exécutent sur plusieurs noeuds ont éventuellement besoin de variables d'environnement spécifiques pour fonctionner correctement. Par ailleurs, les données étendues sur plusieurs noeuds peuvent également impliquer que certains profils utilisateur soient accessibles. Prenez garde aux exigences opérationnelles pour vos applications et données avant de déterminer les ressources qu'un domaine d'administration de grappe doit contrôler.

Chapitre 3. Planification de grappes

Avant d'implémenter une solution à haute disponibilité, vous devez vérifier que toutes les conditions requises sont remplies pour les grappes.

Configuration matérielle pour des grappes

Pour implémenter une solution à haute disponibilité, vous devez planifier et configurer une grappe. Une grappe regroupe des systèmes et des ressources dans un environnement à haute disponibilité.

Ci-après la configuration matérielle minimum pour des grappes :

- Vous devez avoir au moins deux partitions logiques ou modèles System i. Les grappes supportent jusqu'à 128 systèmes. Tous les modèles System i capables d'exécuter i5/OS V4R4M0 ou ultérieur sont compatibles pour la mise en grappe.
- Il est conseillé d'avoir une alimentation de secours externe ou équivalent en cas de coupure d'alimentation soudaine pouvant entraîner une partition de la grappe.
- La mise en grappe utilise les fonctions de multidiffusion du protocole IP. La multidiffusion ne crée pas une mappe correcte de tous les types de supports physiques.
- Si vous envisagez d'utiliser des technologies de test de résistance des données demandant des pools de stockage sur disque indépendant, vous devez aussi planifier le matériel spécifique nécessaire pour ce faire. Vous pouvez également utiliser différentes méthodes de protection des disques pour éviter une reprise en ligne en cas d'échec d'un disque protégé.

Concepts associés

«Planification du test de résistance des données», à la page 50
La résilience des données est la disponibilité des données pour des utilisateurs ou des applications. Vous pouvez effectuer un test de résistance des données à l'aide de la technologie de grappe IBM i avec des disques commutés, la protection par disque miroir d'un site à l'autre ou les technologies de réplication logique.

Référence associée

«Planification de la liste de contrôle des grappes», à la page 76
Complétez la liste de contrôle de la configuration de la grappe pour vous assurer que votre environnement est correctement préparé avant de commencer la configuration de votre grappe.

Information associée

Uninterruptible power supply

IP multicasting

Disk protection

Configuration logicielle pour des grappes

Pour utiliser la mise en grappe, vous devez disposer des logiciels et des licences appropriés.

1. Dernière version de IBM isystème d'exploitation prise en charge.
2. La fonction TCP/IP Connectivity Utilities doit être installée.
3. Si vous envisagez d'utiliser des technologies de test de résistance des données, telles que des disques commutés ou la protection par disque miroir d'un site à l'autre, d'autres exigences sont à respecter.
4. Option 41 (ressources commutables b) est obligatoire pour utiliser les interfaces suivantes :
   - Programme sous licence IBM PowerHA for i. Ce logiciel sous licence fournit les interfaces suivantes qui requièrent Option 41 :
     - Interface graphique de High Availability Solutions Manager

- Interface graphique des services de ressource de mise en grappe
- Commandes IBM PowerHA for i
- IBM PowerHA for iAPI

5. Vous pouvez aussi utiliser le produit d'un partenaire commercial IBM ou écrire votre propre application de gestion à haute disponibilité à l'aide d'API de grappe.

Concepts associés

«Planification de disques commutés», à la page 51
Une copie des données est conservée sur un matériel commutable, à savoir une unité d'extension (tour) ou un processeur d'E-S dans un environnement de partitions logiques. La commutation de tour ne sera pas disponible avec les matériels POWER7.

«Planification de la protection par disque miroir d'un site à l'autre», à la page 53
La protection par disque miroir d'un site à l'autre offre plusieurs technologies de haute disponibilité et de reprise après incident i5/OS : la protection géographique par disque miroir, Metro Mirror et Global Mirror.

«Planification du test de résistance des données», à la page 50
La résilience des données est la disponibilité des données pour des utilisateurs ou des applications. Vous pouvez effectuer un test de résistance des données à l'aide de la technologie de grappe IBM i avec des disques commutés, la protection par disque miroir d'un site à l'autre ou les technologies de réplication logique.

Référence associée

«Planification de la liste de contrôle des grappes», à la page 76
Complétez la liste de contrôle de la configuration de la grappe pour vous assurer que votre environnement est correctement préparé avant de commencer la configuration de votre grappe.

Information associée

Cluster APIs

Exigences de communication pour les grappes

Utilisez n'importe quel type de support de communication dans votre environnement groupé s'il supporte le protocole IP.

Les services-ressources de mise en grappe utilisent les protocoles TCP/IP et UDP/IP pour communiquer entre les noeuds. Les réseaux locaux (LAN), les réseaux longue distance (WAN), les réseaux de systèmes OptiConnect (SAN) ou toute combinaison de ces unités de connectivité sont pris en charge. Votre choix dépend des facteurs suivants :

- le volume des transactions,
- les exigences de temps de réponse,
- la distance entre les noeuds,
- les considérations de coûts.

Vous pouvez suivre les mêmes considérations pour déterminer le support de connexion à employer pour connecter des emplacements de ressources principaux et de secours. Lorsque vous planifiez votre grappe, il est conseillé de désigner un ou plusieurs noeuds de secours à des emplacements à distance afin de pouvoir continuer en cas de perte d'un site.

Pour éviter des incidents de performances dus à une capacité inappropriée, vous devez évaluer le support de communication employé pour gérer les volumes d'informations envoyées entre les noeuds. Vous pouvez choisir votre support physique préféré à utiliser, tel qu'un anneau à jeton, Ethernet, le mode de transfert asynchrone, SPD OptiConnect, une liaison HSL OptiConnect ou Virtual OptiConnect (connexion interne haut débit entre des partitions logiques).

La liaison HSL OptiConnect est une technologie fournie par OptiConnect pour le logiciel i5/OS (i5/OS Option 23 - i5/OS OptiConnect). Elle peut servir à construire des solutions à haute disponibilité. HSL OptiConnect est une réseau de systèmes offrant une connectivité point-à-point haut débit entre les noeuds d'une grappe via la technologie de liaison HSL. HSL OptiConnect requiert des câbles HSL standard mais aucun matériel supplémentaire.

Pour le matériel commutable, qui correspond aux groupes de ressources en grappe d'unités tolérantes aux pannes, votre environnement doit comporter une disque commuté. Dans un environnement de partitions logiques, il s'agit d'une collection d'unités de disques se trouvant sur le bus partagé par les partitions, ou bien associées à un processeur d'entrée-sortie affecté au pool d'entrée-sortie. Pour une environnement système multiple, il s'agit d'une ou plusieurs unités d'extension commutables correctement configurées sur la boucle de liaison HSL contenant aussi les systèmes dans le domaine de reprise. L'unité d'extension commutable peut aussi être utilisée dans un environnement LPAR. .

Remarque : Si vous employez des cartes LAN 2810 en utilisant uniquement TCP/IP et pas l'architecture SNA ou IPX, vous pouvez accroître les performances de la carte sur un système OS/400 V4R5M0 en indiquant Enable only for TCP(*YES) pour la description de ligne à l'aide de la commande Work with Line Descriptions (WRKLIND). L'option Enable only for TCP(*YES) est automatiquement définie dans OS/400 V5R1M0 et les versions ultérieures.

Concepts associés

«Planification de disques commutés», à la page 51
Une copie des données est conservée sur un matériel commutable, à savoir une unité d'extension (tour) ou un processeur d'E-S dans un environnement de partitions logiques. La commutation de tour ne sera pas disponible avec les matériels POWER7.

Référence associée

«Planification de la liste de contrôle des grappes», à la page 76
Complétez la liste de contrôle de la configuration de la grappe pour vous assurer que votre environnement est correctement préparé avant de commencer la configuration de votre grappe.

Réservation d'un réseau pour les grappes

Au cours d'opérations normales, le trafic de communication de la mise en grappe de base est minimal. Il est toutefois fortement conseillé de configurer des chemins de communication redondants pour chaque noeud d'une grappe.

Un chemin de communication redondant signifie que deux lignes sont configurées entre deux noeuds d'une grappe. Si le premier chemin de communication échoue, le second prend le relais pour que la communication se poursuive entre les noeuds, ce qui réduit le risque qu'un ou plusieurs noeuds soient placés dans une partition de grappe. Au moment de configurer ces chemins, pensez que si les deux lignes de communication passent par le même adaptateur sur le système, elles sont toujours menacées en cas d'échec de cet adaptateur. Sachez cependant qu'il n'est pas toujours possible d'éviter une partition de grappe. Si votre système subit une coupure d'alimentation ou si un incident matériel se produit, la grappe peut être partitionnée. En configurant deux lignes, vous pouvez en réserver une pour le trafic de mise en grappe et l'autre pour le trafic normal et la ligne de secours si la ligne spécialisée pour la mise en grappe est défaillante. La partition de grappe type par rapport au réseau est surtout évitable en configurant des chemins de communication redondants entre tous les noeuds de la grappe.

Astuces : Communications de grappe

Pensez à ces astuces quand vous configurez vos voies de communications.

- Assurez- vous que vous disposez d'une bande passante adéquate sur vos lignes de transmission pour gérer l'activité qui ne provient pas de la grappe, ainsi que la fonction des signaux de la mise en grappe, et pour continuer à surveiller l'augmentation de l'activité.
- Pour une fiabilité optimale, ne configurez pas une seule voie de communication qui relie un ou plusieurs noeuds.

- Ne surchargez pas la ligne qui garantit votre communication avec un noeud.
- Eliminez autant de points d'échec que possible, tels que le fait d'avoir deux lignes de transmission qui aboutissent dans un seul adaptateur, le même processeur d'entrée-sorte ou la même unité d'extension.
- Si vous avez un volume de données très important qui doit passer par vos lignes de transmission, vous devriez envisager de mettre la réplication de données et le moniteur de signaux sur des réseaux distincts.
- La multidiffusion du protocole de datagramme utilisateur (UDP) est le protocole préféré que l'infrastructure de transmission de la grappe utilise pour envoyer des informations de gestion de grappe entre les noeuds d'une grappe. Quand les supports physiques prennent en charge les fonctions de multidiffusion, les communications de grappe utilisent la multidiffusion UDP pour envoyer les messages de gestion d'un noeud donné vers tous les noeuds de grappe locaux prenant en charge la même adresse de sous-réseau. Les messages envoyés aux noeuds des réseaux distants sont toujours envoyés à l'aide des fonctions point-à-point UDP. Les communications de grappe ne reposent pas sur les fonctions de routage des messages multidiffusés.
- Le trafic de multidiffusion qui prend en charge la messagerie de gestion de la grappe a, par nature, tendance à varier. En fonction du nombre de noeuds d'un réseau local donné (prenant en charge une adresse de sous-réseau commune) et de la complexité de la structure de gestion de grappe choisie par l'administrateur de grappe, les paquets multidiffusés relatifs à la grappe peuvent facilement dépasser 40 paquets par seconde. Des fluctuations de cette nature peuvent avoir un effet négatif sur les équipements réseau anciens. Par exemple, cela peut entraîner des incidents de surcharge sur les unités du réseau local qui servent d'agents de protocole SNMP (Simple Network Management Protocol) qui doivent évaluer chacun des paquets multidiffusés en protocole UDP. Certains des premiers équipements réseau ne disposaient pas de la bande passante appropriée pour supporter ce genre de trafic. Vous devez vous assurer que l'administrateur réseau a vérifié l'aptitude du réseau à gérer le trafic multidiffusé en protocole UDP, afin de garantir que la mise en grappe n'aura pas de répercussion négative sur les performances des réseaux.

Planification des performances pour les grappes

Comme votre environnement de communications présente éventuellement d'importantes différences, vous pouvez optimiser des variables concernant les communications de grappe pour mieux respecter l'environnement.

Les valeurs par défaut doivent normalement être adaptées aux environnements les plus courants. Si ces valeurs ne s'adaptent pas bien au vôtre, vous pouvez optimiser les communications de grappe en conséquence. Vous disposez d'un niveau d'optimisation de base et avancé.

Optimisation de base

Elle vous permet de définir des paramètres d'optimisation avec un ensemble prédéfini de valeurs correspondant aux valeurs maximales, minimales et normales du délai d'attente et de la fréquence de génération des messages. Si vous sélectionnez le niveau normal, les valeurs par défaut sont utilisées pour les paramètres de configuration et de performances de communications de grappe. Avec la sélection du niveau inférieur, la mise en grappe augmente la fréquence des signaux de présence et les diverses valeurs de délai d'attente des messages. Si les signaux de présence sont moins nombreux et les délais d'attente plus longs, la grappe est moins sensible aux échecs de communication. Avec la sélection du niveau supérieur, la mise en grappe diminue la fréquence des signaux de présence et les diverses valeurs de délai d'attente des messages. Lorsque les signaux de présence sont plus fréquents et les délais d'attente plus courts, la grappe est plus sensible aux échecs de communication.

Optimisation avancée

Elle permet d'optimiser des paramètres individuels à l'aide d'une plage prédéfinie de valeurs. Dans ce cas, une optimisation plus granulaire peut répondre à des situations particulières dans l'environnement de communications. Si vous souhaitez un niveau avancé d'optimisation, il est conseillé de demander de

l'aide au service d'assistance d'IBM ou équivalent. La définition incorrecte des paramètres peuvent facilement dégrader les performances.

Paramètres de communication de grappe optimisables

L'API Change Cluster Resource Services (QcstChgClusterResourceServices) permet à certains services de topologie de grappe, à des performances de communications de grappe et à des paramètres de configuration d'être optimisés pour mieux s'adapter aux divers environnements d'applications et réseau uniques dans lesquels se produit une mise en grappe.

La commande Change Cluster (CHGCLU) offre un niveau de base d'optimisation, alors que l'API QcstChgClusterResourceServices offre des niveaux de base et avancés.

L'API QcstChgClusterResourceServices et la commande Change Cluster Configuration (CHGCLUCFG) peuvent être employées pour optimiser la configuration et les performances de grappe. Elles offrent un niveau de base d'optimisation pour adapter la grappe à un ensemble prédéfini de valeurs identifiées correspondant aux valeurs maximales, minimales et normales du délai d'attente et de la fréquence de génération des messages. Si vous souhaitez un niveau avancé d'optimisation, généralement prévu avec le soutien du personnel d'assistance IBM, vous pouvez optimiser des paramètres individuels avec l'API à l'aide d'une gamme de valeurs prédéfinies. Les modifications non appropriées de paramètres individuels peuvent facilement dégrader les performances de grappe.

Quand et comment optimiser des paramètres de grappe ?

La commande CHGCLU et l'API QcstChgClusterResourceServices permettent de définir rapidement des paramètres de configuration et de performances de grappe sans entrer dans le détail. Ce niveau d'optimisation de base concerne surtout les valeurs de sensibilité des signaux de présence et de délai d'attente des messages de grappe. Les valeurs valides pour le niveau d'optimisation de base sont les suivantes :

1 (Valeurs élevées de délai d'attente/Signaux de présence moins fréquents)
Des ajustements sont apportés aux communications de grappe pour diminuer la fréquence des signaux de présence ainsi que les différentes valeurs des délais d'attente des messages. Si les signaux de présence sont moins nombreux et les délais d'attente plus longs, la grappe répond plus lentement (sensibilité moindre) aux échecs de communication.

2 (Valeurs par défaut)
Les valeurs par défaut sont utilisées pour les performances des communications de grappes et pour les paramètres de configuration. Ce paramètre peut servir à restaurer les valeurs par défaut d'origine de tous les paramètres.

3 (Valeurs faibles de délai d'attente/Signaux de présence plus fréquents)
Des ajustements sont apportés aux communications de grappe pour réduire l'intervalle des signaux de présence et les différentes valeurs des délais d'attente des messages. Si les signaux de présence sont plus nombreux et les délais d'attente moins longs, la grappe répond plus vite (sensibilité accrue) aux échecs de communication.

Vous trouverez des exemples de temps de réponse dans le tableau ci-dessous pour un échec de signal de présence entraînant une partition de noeud :

Remarque : Les durées sont exprimées au format minutes:secondes.

	1 (Moins sensible)			2 (Par défaut)			3 (Plus sensible)		
	Détection d'un incident de signal de présence	Analyse	Total	Détection d'un incident de signal de présence	Analyse	Total	Détection d'un incident de signal de présence	Analyse	Total
Un seul sous-réseau	00:24	01:02	01:26	00:12	00:30	00:42	00:04	00:14	00:18
Plusieurs sous-réseaux	00:24	08:30	08:54	00:12	04:14	04:26	00:04	02:02	02:06

En fonction des charges réseau habituelles et des supports physiques utilisés, un administrateur de grappe peut décider d'optimiser les niveaux de sensibilité des signaux de présence et de délai d'attente des messages. Par exemple, avec un transport de grande vitesse et très fiable tel qu'OptiConnect et avec tous les systèmes dans la grappe sur un bus OptiConnect courant, vous pouvez établir un environnement plus sensible afin d'obtenir une détection et une reprise plus rapide. L'option 3 est choisie. Si l'exécution avait lieu sur un bus Ethernet 10 Mbs très chargé et que les paramètres par défaut provoquaient des partitions occasionnelles dues aux charges de pointe du réseau, l'option 1 pourrait être choisie afin de réduire la sensibilité de la mise en grappe lors de ces pics.

L'API Change Cluster Resource Services permet aussi d'optimiser des paramètres individuels spécifiques pour lesquels les exigences de l'environnement réseau correspondent à des cas uniques. Imaginez une fois de plus une grappe avec tous les noeuds sur un bus OptiConnect. Les performances des messages de grappe peuvent être améliorées dans une grande mesure en définissant le paramètre de taille de fragment de message à un maximum de 32 500 octets afin de respecter davantage la taille de l'unité de transmission maximale OptiConnect que ne le fait la valeur par défaut de 1 464 octets. Cette opération réduit le temps système de fragmentation et le réassemblage des messages volumineux. L'intérêt varie bien sûr selon les applications de grappe et l'utilisation des messages de grappe obtenus de ces applications. D'autres paramètres sont définis dans la documentation de l'API et peuvent être utilisés pour optimiser les performances des messages de grappe ou changer la sensibilité de la grappe au partitionnement.

Référence associée

QcstChgClusterResourceServices API

Information associée

Change Cluster (CHGCLU) command

Modification des paramètres des services-ressources de mise en grappe

Les valeurs par défaut qui affectent le délai d'attente et la relance des messages sont définies pour justifier les installations les plus typiques. Cependant, il est possible de modifier ces valeurs afin qu'elles correspondent mieux à vos environnements de communications.

Les valeurs peuvent être ajustées de l'une des façons suivantes :

- Définissez un niveau de performance général qui correspond à votre environnement.
- Définissez des valeurs pour les paramètres spécifiques d'optimisation des messages pour un ajustement plus spécifique

Dans la première méthode, le trafic de messages est ajusté à l'un des trois niveaux de communication. Le niveau normal est la valeur par défaut et il est décrit en détail dans le contrôle des signaux.

Normalement, la deuxième méthode doit être effectuée avec l'aval d'un expert.

L'API QcstChgClusterResourceServices (Modification des services-ressources de mise en grappe décrit en détail ces deux méthodes.

Référence associée

QcstChgClusterResourceServices API

Information associée

Heartbeat monitoring

Planification de grappes de plusieurs éditions

Si vous créez une grappe incluant des noeuds de plusieurs éditions, certaines étapes sont obligatoires.

Par défaut, la version actuelle de la grappe correspond à celle nominale du premier noeud ajouté à la grappe. Cette approche est appropriée si ce noeud est au niveau de version le plus bas dans la grappe. En revanche, si le noeud est à un niveau de version ultérieur, vous ne pouvez pas ajouter de noeuds d'une version inférieure. La solution consiste à utiliser la valeur de version de grappe cible lorsque vous créez une grappe, afin de définir la version actuelle à un chiffre en dessous de la version nominale du premier noeud ajouté à la grappe.

| **Remarque :** Si vous utilisez le logiciel sous licence IBM PowerHA for i, vous devez obligatoirement installer V6R1 sur tous les systèmes de la grappe.

Imaginez par exemple que vous devez créer une grappe avec deux noeuds. Ci-après les noeuds en question :

Identificateur noeud	Edition	Version de grappe nominale
Noeud A	V5R4	5
Noeud B	V6R1	6

Si la grappe doit être crée à partir du noeud B, veillez à indiquer qu'il s'agira d'une grappe de plusieurs éditions. La version de la grappe cible doit être définie pour indiquer que les noeuds qu'elle contient communiqueront dans une version inférieure d'un niveau à celle nominale du noeud de demande.

Planification des performances des grappes

Quand des modifications sont apportées à une grappe, le temps système nécessaire à la gestion de la grappe peut en être affecté.

Les seules ressources que la mise en grappe nécessite sont celles nécessaires à la réalisation du contrôle des signaux, à la gestion des groupes de ressources en grappe et des noeuds de grappe et à la gestion des messages survenant entre les groupes de ressources en grappe et les noeuds de grappe. Quand votre environnement de mise en grappe est opérationnel, la seule augmentation de temps système possible provient des modifications que vous apportez à la grappe.

Dans un environnement d'exploitation normal, l'activité de mise en grappe doit avoir un minimum d'impact sur les systèmes mis en grappe.

Planification de la détection avancée des incidents de noeud

Vous pouvez utiliser la fonction de détection avancée des incidents de noeud pour réduire le nombre d'incidents qui occasionnent des partitionnements de grappe.

Avant d'implémenter la détection avancée des incidents de noeud, vous devez vérifier que toutes les conditions requises sont remplies.

- Pour éviter le partitionnement des grappes lorsqu'un noeud de grappe tombe en panne, vous pouvez utiliser une partition Hardware Management Console (HMC) V7 ou Virtual I/O Server (VIOS).
- Déterminez quels noeuds de grappe sont gérés par la console HMC ou le serveur VIOS et à quels noeuds de grappe les incidents doivent être signalés.
- Vous devrez configurer un moniteur de grappe sur chaque noeud auquel les incidents seront signalés.

Configuration matérielle requise pour la détection avancée des incidents de noeud

Vous pouvez utiliser la fonction avancée de détection des incidents de noeud uniquement si tous les matériels requis sont installés.

La configuration matérielle minimum suivante est requise pour la fonction avancée de détection des incidents de noeud :

- Au moins deux partitions logiques ou modèles IBM i
- Hardware Management Console (HMC) ou Virtual I/O Server (VIOS)

Configuration logicielle requise pour la détection avancée des incidents de noeud

Pour utiliser la fonction de détection des incidents de noeud dans une solution à haute disponibilité IBM i, la configuration logicielle minimale requise doit être respectée.

Les logiciels suivants doivent être installés sur tous les noeuds appelés à utiliser la fonction avancée de détection des incidents de noeud :

- Système d'exploitation 5770-SS1
- Système d'exploitation de base (BOS) 5770-SS1, option 33 - Portable Application Solutions Environment
- Système d'exploitation de base 5770-SS1, option 30 - Qshell
- 5733-SC1 - IBM Portable Utilities for IBM i
- 5733-SC1, option 1 - OpenSSH, OpenSSL, zlib
- 5770-UME IBM Universal Manageability Enablement
- 5770-HAS IBM PowerHA for i LP

Planification de la liste de contrôle des grappes

Complétez la liste de contrôle de la configuration de la grappe pour vous assurer que votre environnement est correctement préparé avant de commencer la configuration de votre grappe.

Tableau 1. Liste de contrôle de la configuration TCP/IP pour les grappes

Conditions TCP/IP requises	
__	Lancez le protocole TCP/IP sur chaque noeud que vous comptez inclure dans la grappe avec la commande STRTCP (Démarrage TCP/IP).
__	Configurez l'adresse de bouclage TCP (127.0.0.1) et vérifiez qu'elle affiche un état Actif. Vérifiez l'adresse de bouclage TCP/IP en utilisant la commande WRKTCPSTS (Utilisation du statut réseau TCP/IP) sur chaque noeud de la grappe.
__	Vérifiez que les adresses IP utilisées pour la mise en grappe sur un noeud sont actives. Utilisez la commande Work with TCP/IP Network Status (WRKTCPSTS) pour vérifier l'état des adresses IP.
__	Vérifiez que le serveur Internet Daemon (INETD) est actif sur tous les noeuds de la grappe. Dans la négative, démarrez le serveur INETD. Pour plus d'informations sur le démarrage du serveur INETD, voir «Démarrage du serveur INETD», à la page 95.
__	Vérifiez que le profil utilisateur pour INETD, qui est spécifié dans /QIBM/ProdData/OS400/INETD/inetd.conf, ne possède pas plus qu'une autorité minimale. Si ce profil utilisateur possède plus qu'une autorité minimale, le démarrage du noeud de grappe échouera. Par défaut, QUSER est fourni comme profil utilisateur pour INETD.

Tableau 1. Liste de contrôle de la configuration TCP/IP pour les grappes (suite)

Conditions TCP/IP requises	
__	Vérifiez que chaque adresse IP de la grappe sur chaque noeud de la grappe permet d'envoyer et de recevoir des datagrammes UDP vers et depuis toutes les autres adresses IP de la grappe. Si un noeud de la grappe utilise une adresse IPv4, chaque noeud de la grappe doit posséder une adresse IPv4 active (pas nécessairement configurée comme adresse IP de grappe) permettant de router et d'envoyer des paquets TCP à cette adresse. De même, si un noeud de la grappe utilise une adresse IPv6, chaque noeud de la grappe doit posséder une adresse IPv6 active (pas nécessairement configurée comme adresse IP de grappe) permettant de router et d'envoyer des paquets TCP à cette adresse. Utilisez la commande PING en spécifiant une adresse IP locale, et la commande TRACEROUTE en spécifiant des messages UDP. Cela vous permettra de déterminer si deux adresses IP peuvent communiquer. Les commandes PING et TRACEROUTE ne fonctionnent pas entre les adresses IPv4 et IPv6 ou quand un pare-feu les bloque.
__	Vérifiez que les ports 5550 et 5551 ne sont pas utilisés par d'autres applications. Ces ports sont réservés pour la mise en grappe IBM. L'utilisation des ports peut être visualisée à l'aide de la commande WRKTCPSTS (Utilisation du statut réseau TCP/IP). Le port 5550 est ouvert et est en mode écoute par la mise en grappe effectuée après le démarrage de INETD.

Tableau 2. Liste de contrôle du domaine d'administration des grappes

Considérations relatives à l'interface de grappe des services-ressources de mise en grappe	
	Installez IBM PowerHA for i (logiciel sous licence iHASM (5770-HAS). Une clé de licence valide doit exister sur tous les noeuds de grappe qui feront partie de la solution à haute disponibilité.
__	Installez l'option 41 (i5/OS - HA Switchable Resources). Une clé de licence valide doit exister sur tous les noeuds de grappe qui feront partie du domaine d'unité.
__	Vérifiez que tous les serveurs hôte sont démarrés à l'aide de la commande STRHOSTSVR (Démarrage du serveur hôte) : STRHOSTSVR SERVER(*ALL)

Si vous comptez utiliser des unités commutables dans votre grappe, les exigences suivantes doivent être satisfaites :

Tableau 3. Liste de contrôle de la configuration des unités résilientes des grappes

Spécifications de l'unité résiliente	
__	Installez le programme sous licence IBM PowerHA for i. Une clé de licence valide doit exister sur tous les noeuds de grappe qui feront partie de la solution à haute disponibilité.
__	Vérifiez que l'option 41 (HA Switchable Resources) est installée et qu'une clé de licence valide existe sur tous les noeuds de grappe qui feront partie du domaine d'unité.
__	Pour accéder aux fonctions de gestion des disques, configurez le serveur d'outils de maintenance avec l'accès aux outils de maintenance en mode dédié et les profils utilisateur. Voir Activation et accès aux unités de disque pour obtenir des détails.
__	Si vous basculez des unités résilientes entre des partitions logiques d'un système, et que vous utilisez autre chose que la console HMC pour gérer vos partitions logiques, activez Virtual OptiConnect pour les partitions. Ceci peut être fait lors de la connexion aux outils de maintenance en mode dédié. Voir Virtual OptiConnect pour plus de détails. Si vous utilisez la console HMC pour gérer vos partitions, modifiez les propriétés du profil de votre partition dans l'onglet OptiConnect pour activer Virtual OptiConnect pour chaque partition de la configuration commutable. Vous devez activer le profil de partition pour appliquer la modification.

Tableau 3. Liste de contrôle de la configuration des unités résilientes des grappes (suite)

Spécifications de l'unité résiliente	
__	Si une unité d'extension d'une boucle HSL OptiConnect est commutée entre deux systèmes, et que l'un des systèmes possède des partitions logiques, activez HSL OptiConnect pour les partitions. Si vous utilisez autre chose que la console HMC pour gérer des partitions logiques, ceci peut être fait lors de la connexion aux outils de maintenance en mode dédié. Si vous utilisez la console HMC pour gérer vos partitions, modifiez les propriétés du profil de votre partition dans l'onglet OptiConnect pour activer HSL OptiConnect pour chaque partition de la configuration commutable. Vous devez activer le profil de partition pour appliquer la modification.
__	Si vous basculez des unités résilientes entre des partitions logiques, et que vous utilisez autre chose que la console HMC pour gérer vos partitions logiques, vous devez configurer le bus qui doit être partagé entre les partitions ou configurer un pool d'entrée-sortie. Le bus doit être configuré comme Propre bus partagé par une partition, et toutes les autres partitions qui participeront à la commutation de l'unité doivent être configurées sur Utiliser un bus partagé. Si vous utilisez la console HMC pour gérer vos partitions logiques, vous devez configurer un pool d'entrée-sortie qui inclut que le processeur d'entrée-sortie, l'adaptateur d'entrée-sortie et toutes les ressources connectées pour qu'un pool de stockage sur disque indépendant soit commutable entre plusieurs partitions. Chaque partition doit avoir accès au pool d'entrée-sortie. Voir Rendre votre matériel commutable pour plus de détails. Pour obtenir des détails sur les conditions requises de la planification matérielle, voir Configuration matérielle requises pour les disques commutés.
__	Lors de la commutation d'une unité d'extension sur une boucle HSL entre deux systèmes différents, configurez l'unité d'extension de sorte qu'elle soit commutable. Voir Rendre votre matériel commutable pour obtenir des détails.
__	Quand une unité d'extension est ajoutée à une boucle HSL existante, redémarrez tous les serveurs qui font partie de cette boucle.
__	L'unité de transmission maximale pour vos voies de communication doit être supérieure au paramètre ajustable des communications de la grappe, la taille des fragments du message. L'unité de transmission maximale pour l'adresse IP d'une grappe peut être vérifiée à l'aide de la commande WRKTCPSTS (Utilisation du statut réseau TCP/IP) sur le noeud en question. Elle doit également être vérifiée à chaque étape du chemin des communications. Il peut être plus aisé de réduire le paramètre de la taille des fragments du message après la création de la grappe que d'augmenter l'unité de transmission maximale de la voie de communication. Voir les Paramètres ajustables des communications de la grappe pour obtenir de plus amples informations sur la taille des fragments du message. Vous pouvez utiliser l'API QcstRetrieveCRSInfo (Récupération des services-ressources de mise en grappe) pour afficher les paramètres actuels des paramètres ajustables et l'interface de programmation QcstChgClusterResourceServices (Modification des services-ressources de mise en grappe) pour modifier les paramètres.
__	Pour la fonction de miroir géographique, assurez-vous que les deux noeuds sont affectés à un nom de site différent.

Tableau 4. Liste de contrôle de la configuration de la sécurité des grappes

Exigences en matière de sécurité	
__	Définissez l'attribut de réseau ALWADDCLU (Autoriser l'ajout à la grappe) de façon appropriée sur le noeud cible si vous essayez de démarrer un noeud distant. Il doit être paramétré sur *ANY ou *RQSAUT en fonction de votre environnement. Si cet attribut est paramétré sur *RQSAUT, alors l'option 34 (Digital Certificate Manager) et l'option 35 (CCA Cryptographic Service Provider) d'IBM i doivent être installées. Voir Activation d'un noeud à ajouter dans une grappe pour obtenir des détails sur la définition de l'attribut réseau ALWADDCLU.
__	Activez l'état du profil utilisateur pour INETD spécifié dans /QIBM/ProdData/OS400/INETD/inetd.conf. Il ne doit pas posséder les autorisations *SECADM ou *ALLOBJ. Par défaut, QUSER est fourni comme profil utilisateur pour INETD.
__	Vérifiez que le profil utilisateur qui appelle les interfaces de programmation des services-ressources de mise en grappe existe sur tous les noeuds de grappe et qu'il possède le droit d'accès *IOSYSCFG.

Tableau 4. Liste de contrôle de la configuration de la sécurité des grappes (suite)

Exigences en matière de sécurité	
__	Vérifiez que le profil utilisateur censé exécuter le programme d'exit d'un groupe de ressources en grappe existe sur tous les noeuds du domaine de reprise.

Tableau 5. Liste de contrôle de la configuration des travaux pour les grappes

Considérations relatives aux travaux	
__	Les travaux peuvent être envoyés par les interfaces de programmation des services-ressources de mise en grappe pour le traitement des requêtes. Les travaux sont exécutés dans le profil utilisateur qui exécute le programme exit spécifié lors de la création d'un groupe de ressources en grappe ou dans le profil utilisateur qui a demandé l'interface de programmation (pour la mise en fonction des unités des groupes de ressources en grappe d'unité résiliente uniquement). Assurez-vous que le sous-système que les services de la file d'attente de travaux ont associé au profil utilisateur est configuré de la façon suivante : *NOMAX pour le nombre de travaux qu'il peut exécuter depuis la file d'attente de travaux.
__	Les travaux sont envoyés à la file d'attente des travaux spécifiée par la description de travail obtenue à partir du profil utilisateur défini pour un groupe de ressources en grappe. La description de travail par défaut provoque l'envoi des travaux à la file d'attente QBATCH. Cette file d'attente de travaux étant utilisée pour plusieurs travaux d'utilisateur, le travail du programme d'exit risque de ne pas s'exécuter de façon opportune. Prenez une description de travail unique avec une file d'attente utilisateur unique.
__	Quand des travaux de programme d'exit sont exécutés, ils utilisent des données de routage issues de la description de travail pour déterminer quel pool de mémoire principale et quels attributs de phase d'exécution doivent être utilisés. Les valeurs par défaut ont pour résultat des travaux qui sont exécutées dans un pool avec d'autres travaux par lot qui possèdent une priorité d'exécution de 50. Aucun de ces éléments ne peut produire les performances souhaitées pour des travaux de programme d'exit. Le sous-système initiant les travaux du programme d'exit (le même sous-système qui utilise la file d'attente de travaux unique) doit attribuer les travaux du programme d'exit à un pool qui n'est pas utilisé par d'autres travaux initiés par le même sous-système ou d'autres sous-systèmes. En outre, les travaux du programme d'exit doivent bénéficier d'une priorité d'exécution de 15 de sorte qu'ils puissent s'exécuter avant presque tous les autres travaux d'utilisateur.
__	Définissez la valeur système QMLTTHDACN sur 1 ou 2.

Plusieurs interfaces logicielles sont disponibles pour la configuration et la gestion de votre grappe. L'une de ces interfaces est l'interface Services-ressources de mise en grappe. Si vous comptez utiliser les services-ressources de mise en grappe, les exigences suivantes doivent être satisfaites.

Tableau 6. Liste de contrôle de la configuration des services-ressources de mise en grappe pour les grappes

Considérations relatives à l'interface graphique des services-ressources de mise en grappe	
__	Installez le programme sous licence IBM PowerHA for i. Une clé de licence valide doit exister sur tous les noeuds de grappe qui feront partie de la solution à haute disponibilité.
__	Installez l'option 41 (HA Switchable Resources). Une clé de licence valide doit exister sur tous les noeuds de grappe qui feront partie du domaine d'unité.
__	Vérifiez que tous les serveurs hôte sont démarrés à l'aide de la commande STRHOSTSVR (Démarrage du serveur hôte) : STRHOSTSVR SERVER(*ALL)

Tableau 7. Liste de contrôle de la détection avancée des incidents de noeud pour les grappes

Remarques relatives à la détection avancée des incidents de noeud	
__	Déterminez les noeuds de grappe qui sont ou qui peuvent être gérés par Hardware Management Console (HMC) ou Virtual I/O Server (VIOS).
__	Déterminez le ou les noeuds de grappe qui doivent recevoir les messages quand un autre noeud de la grappe tombe en panne.

Tableau 7. Liste de contrôle de la détection avancée des incidents de noeud pour les grappes (suite)

Remarques relatives à la détection avancée des incidents de noeud	
__	Sur chaque noeud de grappe devant recevoir un message d'une partition HMC ou VIOS, exécutez les étapes suivantes :
	Installez le système d'exploitation de base, option 33 - IBM Portable Application Solutions Environment for i
	Installez le produit 5733-SC1 - IBM Portable Utilities for i
	Installez le produit 5733-SC1, option 1 - OpenSSH, OpenSSL, zlib
	Installez le produit 5770-UME - IBM Universal Manageability Enablement for i
	Configurez les propriétés enableAuthentication et sslClientVerificationMode pour le produit 5770-UME.
	Copiez le certificat numérique délivré par la partition VIOS ou HMC sur le noeud de grappe et ajoutez-le dans un fichier de clés certifiées IBM i.
	Démarrez le serveur *CIMOM avec la commande CL STRTCPSVR *CIMOM.
	Configurez le ou les moniteurs de grappe avec la commande CL ADDCLUMON.

Planification de la fonction FlashCopy

Vous pouvez utiliser la fonction FlashCopy pour réduire la fenêtre de sauvegarde dans des environnements à haute disponibilité i5/OS en utilisant des unités de mémoire externe IBM System Storage. Avant d'utiliser la fonction FlashCopy, vous devez vérifier que les exigences minimum ont été respectées.

Exigences matérielles pour la fonction FlashCopy

Pour utiliser la technologie FlashCopy dans une solution à haute disponibilité i5/OS, assurez-vous de disposer de la configuration matérielle minimum requise suivante.

La configuration matérielle minimum suivante est requise pour la fonction FlashCopy :

- Au moins deux modèles ou partitions logiques System i séparées géographiquement avec au moins une unité de stockage externe IBM System Storage DS8000 connectée à chaque système. Les unités de stockage externe DS8000 sont prises en charge sur tous les modèles System i prenant en charge la connexion Fibre Channel du stockage externe.
- L'un des adaptateurs de canal optique suivants est obligatoire :
  - Contrôleur de disques PCI de canal optique 2766 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 2787 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 5760 4 gigabits
- Avant toute configuration, vous devez avoir défini la taille appropriée du disque pour la mémoire système. Il vous faut un ensemble de disques pour la source, un ensemble équivalent d'unités de disques pour la cible, et un autre pour chaque copie cohérente.

Exigences logicielles pour la fonction FlashCopy

Pour utiliser la technologie FlashCopy dans une solution à haute disponibilité IBM i, assurez-vous de disposer de la configuration logicielle minimum requise suivante.

La fonction FlashCopy requiert la configuration logicielle minimum suivante :

- Chaque modèle IBM i dans la solution à haute disponibilité doit exécuter au moins IBM i V6R1 pour une utilisation avec le programme sous licence IBM PowerHA for i.

Remarque : Pour les éditions antérieures, vous pouvez toujours utiliser IBM Advanced Copy Services for PowerHA on i, édité par Lab Services, pour une utilisation avec les solutions IBM System Storage. Si vous utilisez Global Mirror sur plusieurs plateformes ou que vous

voulez implémenter Global Mirror sur plusieurs partitionsIBM i, vous pouvez également utiliser le produit IBM Advanced Copy Services for PowerHA on i.

- IBM PowerHA for i installé sur chaque système.
- Vérifiez que les derniers PTF ont été installés.

Exigences de communication pour la fonction FlashCopy

Pour utiliser la technologie FlashCopy dans une solution à haute disponibilité i5/OS, assurez-vous de disposer de la configuration matérielle minimum requise suivante.

Les conditions de communication minimales suivantes sont requises pour la fonction FlashCopy :

- Au moins deux modèles System i séparées géographiquement avec au moins une unité de stockage externe IBM System Storage DS8000 connectée à chaque système. Les unités de stockage externe DS8000 sont prises en charge sur tous les modèles System i prenant en charge la connexion Fibre Channel du stockage externe.
- L'un des adaptateurs de canal optique suivants est obligatoire :
  - Contrôleur de disques PCI de canal optique 2766 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 2787 2 gigabits
  - Contrôleur de disques PCI-X de canal optique 5760 4 gigabits
- Un nouveau processeur d'E-S est obligatoire pour supporter l'unité source IPL externe sur le système DS8000 :
  - Processeur d'E-S 2847 PCI-X pour la source IPL du réseau de stockage
- Avant toute configuration, vous devez avoir défini la taille appropriée du disque pour la mémoire système. Il vous faut un ensemble de disques pour la source, un ensemble équivalent d'unités de disques pour la cible, et un autre pour chaque copie cohérente.

Planification de la sécurité pour la haute disponibilité

Avant de configurer votre solution à haute disponibilité, vous devez évaluer les stratégies actuelles de sécurité dans votre environnement et apporter les modifications appropriées pour offrir une haute disponibilité.

Distribution des informations à l'échelle de la grappe

Découvrez les implications de sécurité de l'utilisation et de la gestion des informations à l'échelle de la grappe.

L'API QcstDistributeInformation (Distribution des informations) peut être utilisée pour envoyer des messages à partir d'un noeud faisant partie d'un domaine de reprise de groupes de ressources en grappes vers d'autres noeuds de ce domaine de reprise. Ceci peut être utile dans le traitement du programme d'exit. Cependant, il est important de noter que ces informations ne sont pas chiffrées. Des informations sécurisées ne doivent pas être envoyées à l'aide de ce mécanisme, sauf si vous utilisez un réseau sécurisé.

Les données temporaires peuvent être partagées et reproduites entre des noeuds de grappe à l'aide des interfaces de programmation de table de hachage groupée. Les données sont stockées dans une mémoire temporaire. Cela signifie que les données sont conservées uniquement jusqu'à ce que le noeud de grappe ne fasse plus partie de la table de hachage groupée. Ces interfaces de programmation peuvent uniquement être utilisées à partir d'un noeud de grappe défini dans le domaine de table de hachage groupée. Le noeud de grappe doit être actif dans la grappe.

Les autres informations distribuées à l'aide de la messagerie de la grappe ne sont pas sécurisées non plus. Ceci inclut les messages de grappe de niveau inférieur. Quand des modifications sont apportées dans les données du programme d'exit, le message contenant les données n'est pas chiffré.

Considérations relatives à l'utilisation des grappes avec des pare-feux

Si vous utilisez une mise en grappe dans un réseau qui utilise des pare-feux, notez ces quelques limitations et exigences.

Si vous utilisez une mise en grappe avec un pare-feu, vous devez donner à chaque noeud la possibilité d'envoyer des messages sortants et de recevoir des messages entrants provenant d'autres noeuds de grappe. Une ouverture du pare-feu doit exister pour chaque adresse de grappe sur chaque noeud afin de permettre la communication avec chaque adresse de grappe des autres noeuds. Les paquets IP qui voyagent au sein d'un réseau peuvent être de plusieurs types de trafic différents. La mise en grappe utilise la commande PING, qui est du type ICMP, et elle utilise également les protocoles UDP et TCP. Lorsque vous configurez un pare-feu, vous pouvez filtrer le trafic en fonction du type. Pour que la mise en grappe fonctionne, le pare-feu doit autoriser le trafic d'ICMP, UDP et TCP. Le trafic sortant peut être envoyé sur n'importe quel port et le trafic entrant est reçu sur les ports 5550 et 5551.

De plus, si vous utilisez la fonction avancée de détection des incidents de noeud, tout noeud de grappe devant recevoir des messages d'échec d'une console HMC (Hardware Management Console) ou d'un serveur VIOS (Virtual I/O Server) doit pouvoir communiquer avec cette console HMC ou ce serveur VIOS. Le noeud de grappe enverra les données à la console HMC ou au serveur VIOS via l'adresse IP associée au nom de domaine de la console HMC ou du serveur VIOS sur le port 5989. Le noeud de grappe recevra des données de la console HMC ou du serveur VIOS via l'adresse IP associée au nom du système du noeud de grappe sur le port 5989.

Gestion des profils utilisateur sur tous les noeuds

Vous pouvez utiliser deux mécanismes pour gérer des profils utilisateurs sur tous les noeuds d'une grappe.

Dans un environnement à haute disponibilité, un profil utilisateur est considéré comme étant le même sur les différents systèmes si les noms de profil sont identiques. Le nom est l'identificateur unique dans la grappe. Cependant, un profil utilisateur contient un ID utilisateur et un ID de groupe. Pour réduire la quantité de traitement interne qui se produit pendant un basculement, à l'emplacement où le pool de stockage sur disque indépendant est rendu indisponible sur un système, puis disponible sur un autre système, l'ID utilisateur et l'ID de groupe doivent être synchronisés dans le domaine de reprise du groupe de ressources en grappe d'unité. Vous pouvez utiliser le domaine d'administration pour synchroniser les profils utilisateur, avec les valeurs d'ID groupe et d'ID utilisateur, dans toute la grappe.

Un mécanisme consiste à créer un domaine d'administration de grappe pour contrôler les ressources partagées sur plusieurs noeuds d'une grappe. Un domaine d'administration de grappe peut contrôler plusieurs types de ressources en plus des profils utilisateur, tout en fournissant une gestion simple des ressources partagées entre les noeuds. Quand les profils utilisateur sont mis à jour, les modifications sont propagées automatiquement sur les autres noeuds si le domaine d'administration de grappe est activé. Si le domaine d'administration de grappe n'est pas activé, les modifications seront propagées après l'activation du domaine d'administration de grappe. Cette méthode est recommandée car elle gère automatiquement les profils utilisateur avec un environnement à haute disponibilité.

Avec la seconde machine, les administrateurs peuvent également utiliser la gestion centralisée de System i Navigator pour appliquer des fonctions sur plusieurs systèmes et groupes de systèmes. Cette fonction prend en charge certaines tâches d'administrateur communes que les opérateurs doivent réaliser dans plusieurs systèmes de leur grappe. Grâce à la gestion centralisée, vous pouvez appliquer des fonctions de profil utilisateur à des groupes de systèmes. L'administrateur peut spécifier une commande de post-propagation à exécuter sur les systèmes cible lors de la création d'un profil utilisateur.

Important :

- Si vous comptez partager des profils utilisateur qui utilisent une synchronisation par mot de passe dans une grappe, vous devez attribuer la valeur système 1 à QRETSVRSEC (Conservation de la sécurité du serveur).

- Si vous modifiez la valeur QRETSVRSEC par 0 après avoir ajouté un poste de ressource contrôlée pour un profil utilisateur, et que vous modifiez le mot de passe par la suite (si le mot de passe est sous surveillance), l'état global du poste de ressource contrôlée est défini sur Incohérent. Le poste de ressource contrôlée est marqué comme étant inutilisable. Toutes les modifications apportées au profil utilisateur après cette modification ne sont pas synchronisées. Pour résoudre ce problème, modifiez la valeur QRETSVRSEC par 1, supprimez le poste de ressource contrôlée et ajoutez-le à nouveau.

Tâches associées

«Création d'un domaine d'administration de grappe», à la page 117
Dans une solution à haute disponibilité, le domaine d'administration de grappe fournit le mécanisme qui garde les ressources synchronisées dans les systèmes et les partitions d'une grappe.

Chapitre 4. Configuration de la haute disponibilité

Pour pouvoir configurer une solution à haute disponibilité dans votre environnement i5/OS, assurez-vous que vous avez effectué la planification appropriée et cerné vos ressources et objectifs pour la haute disponibilité et la reprise après incident. Utilisez les scénarios de configuration pour la haute disponibilité et les tâches associées aux techniques à haute disponibilité pour créer votre propre solution à haute disponibilité.

Scénarios : Configuration de la haute disponibilité

Les scénarios de configuration fournissent des exemples d'environnements i5/OS à haute disponibilité différents et des tâches de configuration détaillées qui vous permettent d'implémenter une solution à haute disponibilité qui répond à vos besoins et à vos exigences en matière de test de résistance.

Ces scénarios contiennent des descriptions des objectifs métier pour la haute disponibilité et fournissent une image qui illustre les ressources dans la solution à haute disponibilité. Chaque exemple de solution contient des instructions détaillées pour configurer et tester la haute disponibilité. Cependant, ces informations ne couvrent pas tous les cas de configuration et des tests supplémentaires peuvent être requis pour vérifier la haute disponibilité.

Scénario : Disques commutés entre les partitions logiques

Ce scénario décrit une solution à haute disponibilité i5/OS qui utilise des pools de stockage sur disque qui sont commutés entre deux partitions logiques qui se trouvent sur un seul système.

Présentation

Le partitionnement logique consiste à faire fonctionner un seul système i5/OS comme s'il s'agissait d'au moins deux systèmes. Cette solution est un bon choix pour les entreprises possédant déjà des partitions logiques configurées dans leur environnement.

Ce scénario ne montre pas la configuration des partitions logiques.

Objectifs

Cette solution présente les avantages suivants :

- Il s'agit d'une solution peu coûteuse qui utilise les ressources système disponibles.
- Assure la disponibilité de vos ressources professionnelles pendant les indisponibilités prévues.
- Assure la disponibilité de vos ressources professionnelles pendant certaines indisponibilités non prévues, comme un échec sur une partition logique.
- Comme cette solution utilise une seule copie des données, le nombre d'unité de disque requises est limité.
- Cette solution contient les données à jour qu'il est inutile de synchroniser.

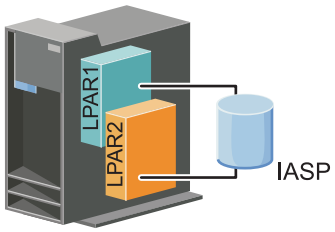
Cette solution présente les restrictions suivantes :

- La reprise après incident en cas d'une indisponibilité générale du site n'est pas possible.
- Il est nécessaire que vous configuriez une partition logique.
- Il est possible que du matériel redondant soit nécessaire entre les partitions.
- Il existe une seule copie logique des données dans le pool de stockage sur disque indépendant. Ceci peut constituer un point de défaillance unique, bien que les données puissent être protégées par une protection RAID.

- L'accès simultané au pool de stockage sur disque à partir des deux partitions logiques n'est pas possible.

Détails

Cette image illustre l'environnement pour ce scénario :



Etapes de configuration

Complétez les tâches suivantes pour configurer les technologies de haute disponibilité associées à ce scénario :

1. Achèvement de la liste de contrôle de la grappe
2. Création d'une grappe
3. Ajout d'un noeud
4. Démarrage d'un noeud
5. Ajout d'un noeud à un domaine d'unité
6. Création d'un domaine d'administration de grappe
7. Démarrage d'un domaine d'administration de grappe
8. Création d'un pool de stockage sur disque indépendant
9. Ajout de postes de ressource contrôlée
10. Rendre du matériel commutable
11. Création d'un groupe de ressources en grappe d'unité
12. Démarrage d'un groupe de ressources en grappe d'unité
13. Mise en fonction du pool de stockage sur disque
14. Réalisation d'un basculement pour tester votre solution à haute disponibilité.

Scénario : Disques commutés entre les systèmes

Ce scénario illustre une solution à haute disponibilité IBM i qui utilise des disques commutés entre deux systèmes et fournit une haute disponibilité aux données, applications ou unités lors des indisponibilités prévues ou imprévues. La prise en charge des tours commutables entre les systèmes n'existe pas sur le matériel POWER7.

Présentation

En utilisant la technologie de basculement sur disque, cette solution fournit la haute disponibilité. Avec cette solution, une copie unique des données enregistrée dans le disque basculé reste toujours à jour, ce qui évite de synchroniser les données entre systèmes et évite le risque de perte de données en cours de transmission.

Objectifs

Cette solution présente les avantages suivants :

- Assure la disponibilité de vos ressources professionnelles pendant les indisponibilités prévues

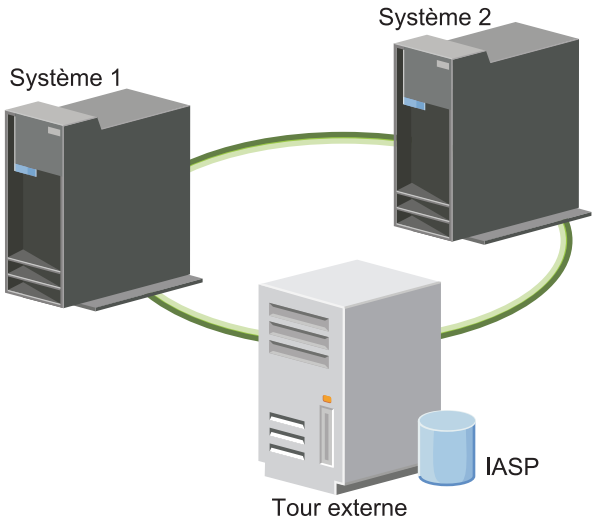
- Assure la disponibilité de vos ressources professionnelles pendant certaines indisponibilités non prévues
- Active une seule copie des données, ce qui réduit le nombre d'unité de disque requises
- Sollicite au minimum les performances
- Permet de conserver des données à jour sans avoir besoin de les synchroniser

Cette solution présente les restrictions suivantes :

- Les systèmes POWER7 ne prennent pas en charge les tours commutables. Cette solution ne doit donc pas être utilisée comme solution stratégique si vous utilisez ce type de matériel.
- La reprise après incident en cas d'une indisponibilité générale du site n'est pas possible.
- Il existe une seule copie logique des données dans le pool de stockage sur disque indépendant. Ceci peut constituer un point de défaillance unique, bien que les données puissent être protégées par une protection RAID.
- L'accès simultané au pool de stockage sur disque à partir des deux systèmes n'est pas possible.

Détails

Cette image illustre l'environnement pour ce scénario :



Etapes de configuration

1. Achèvement de la liste de contrôle de planification
2. Création d'une grappe
3. Ajout d'un noeud
4. Démarrage d'un noeud
5. Ajout de noeuds à des domaines d'unité
6. Création d'un domaine d'administration de grappe
7. Démarrage d'un domaine d'administration de grappe
8. Création d'un pool de stockage sur disque indépendant
9. Ajout de postes de ressource contrôlée
10. Rendre du matériel commutable
11. Création d'un groupe de ressources en grappe d'unité
12. Démarrage d'un groupe de ressources en grappe d'unité
13. Mise en fonction du pool de stockage sur disque

14. Réalisation d'un basculement pour tester votre solution à haute disponibilité.

Scénario : Disque commuté avec protection géographique par disque miroir

Ce scénario décrit une solution à haute disponibilité i5/OS qui utilise des disques commutés dans une grappe à trois noeuds. Cette solution fournit la reprise après incident et la haute disponibilité.

Présentation

Sur le site de production (Uptown), les disques basculés servent à déplacer des pools de stockage sur disque indépendants entre deux noeuds. La solution utilise également la protection géographique par disque miroir pour créer une copie du disque indépendant sur un deuxième site (Downtown). Ainsi, cette solution fournit à la fois la reprise après incident et la haute disponibilité. Les avantages de cette solution sont essentiellement les mêmes que ceux de la solution de basculement de disque de base, avec l'atout supplémentaire d'assurer une reprise après incident pour les données d'application en dupliquant ces données sur un autre emplacement. Le site de production (Uptown) possède un pool de stockage sur disque indépendant que vous pouvez basculer entre les partitions logiques pour permettre une haute disponibilité et des délais de basculement rapides en cas d'indisponibilité prévue, comme l'application de correctifs. Cette solution garantit également une reprise après incident avec sa fonction de mise en miroir entre sites et sa protection géographique par disque miroir.

| La protection géographique par disque miroir est une sous-fonction de la mise en miroir entre sites, qui
| permet la mise en miroir des données sur une copie du pool de stockage sur disque indépendant sur le
| site éloigné. Les données du pool de stockage sur disque indépendant se trouvant sur le site de
| production (Uptown) sont mises en miroir sur un pool de stockage sur disque indépendant se trouvant
| sur le site de secours (Downtown). Cette solution constitue une alternative simple et plus économique
| aux solutions externes basées sur stockage, telles que les produits Global Mirror et Metro Mirror d'IBM
| System Storage. Toutefois, la protection géographique par disque miroir ne garantit pas toutes les options
| de performances que fournissent les solutions avec stockage externe.

Objectifs

Cette solution présente les avantages suivants :

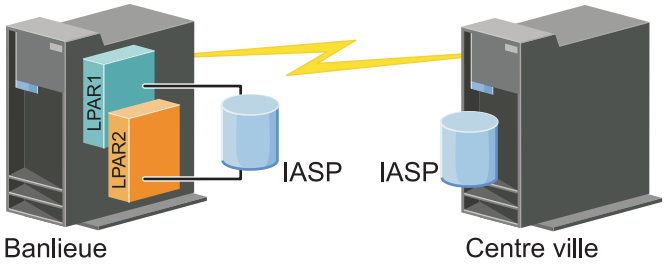
- Assure la disponibilité de vos ressources professionnelles pendant les indisponibilités prévues
- | Assure la disponibilité de vos ressources professionnelles pendant les indisponibilités non prévues
- Assure la disponibilité de vos ressources professionnelles pendant les désastres s'étendant sur l'ensemble du site
- Permet à chaque site de disposer d'une copie unique de données qui réduit le nombre d'unités de disque requises
- | Permet de conserver des données à jour sans avoir besoin de les synchroniser

Cette solution présente les restrictions suivantes :

- L'accès simultané au pool de stockage sur disque n'est pas possible. Vous pouvez toutefois détacher la copie sur miroir pour un traitement hors ligne d'une deuxième copie des données.
- Les performances risquent d'être amoindries, en raison de la sollicitation accrue de l'unité centrale requise pour la prise en charge de la protection géographique par disque miroir.
- Pensez à utiliser des chemins de communication redondants et une bande passante adéquate.

Détails

Cette image suivante illustre cette solution :



Etapes de configuration

1. Achèvement de la liste de contrôle de planification des grappes
2. Création d'une grappe
3. Ajout d'un noeud
4. Démarrage d'un noeud
5. Ajout d'un noeud à un domaine d'unité
6. Création d'un groupe de ressources en grappe d'unité
7. Définition des noms de site
8. Création d'un domaine d'administration de grappe
9. Démarrage d'un domaine d'administration de grappe
10. Création d'un pool de stockage sur disque indépendant
11. Ajout de postes de ressource contrôlée
12. Rendre du matériel commutable
13. Configuration de la protection géographique par disque miroir
14. Mise en fonction des pools de stockage sur disque
15. Réalisation d'un basculement pour tester la configuration.

Tâches associées

«Configuration de la protection géographique par disque miroir», à la page 128
La *protection géographique par disque miroir* est une sous-fonction de la protection par disque miroir d'un site à l'autre. Pour configurer une solution à haute disponibilité à l'aide de la protection géographique par disque miroir,vous devez configurer une session de protection par disque miroir entre le système de production et le système sauvegarde.

Scénario : Protection par disque miroir d'un site à l'autre via la protection géographique par disque miroir

Ce scénario décrit une solution à haute disponibilité IBM i qui utilise la protection géographique par disque miroir dans une grappe à deux noeuds. Cette solution fournit la reprise après incident et la haute disponibilité.

Présentation

La protection géographique par disque miroir est une sous-fonction de la mise en miroir entre sites, qui permet la mise en miroir des données sur une copie du pool de stockage sur disque indépendant sur le site éloigné. Cette solution fournit une reprise après incident en cas d'indisponibilité à l'échelle du site sur le système de production (Système 1). Dans cette situation, la reprise en ligne sur le site de secours (Système 2) se produit, et les opérations peuvent se poursuivre sur la copie en miroir des données. Cette solution constitue une alternative simple et plus économique aux solutions externes basées sur stockage,

telles que Global Mirror et Metro Mirror d'IBM System Storage. Toutefois, la protection géographique par disque miroir ne garantit pas toutes les options de performances que fournissent les solutions avec stockage externe.

Objectifs

Cette solution présente les avantages suivants :

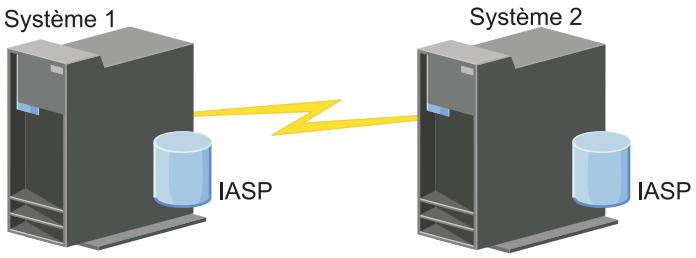
- Assure la disponibilité de vos ressources professionnelles pendant les indisponibilités prévues
- Assure la disponibilité de vos ressources professionnelles pendant les indisponibilités non prévues
- Assure la disponibilité de vos ressources professionnelles pendant un désastre
- Permet de conserver des données à jour sans avoir besoin de les synchroniser

Cette solution présente les restrictions suivantes :

- L'accès simultané au pool de stockage sur disque n'est pas possible. Vous pouvez toutefois détacher la copie sur miroir pour un traitement hors ligne d'une deuxième copie des données.
- Les performances risquent d'être amoindries, en raison de la sollicitation accrue de l'unité centrale requise pour la prise en charge de la protection géographique par disque miroir.
- Pensez à utiliser des chemins de communication redondants et une bande passante adéquate

Détails

L'image suivante illustre cette solution :



Etapes de configuration

1. Achèvement de la liste de contrôle de planification des grappes
2. Création d'une grappe
3. Ajout de noeuds
4. Démarrage des noeuds
5. Ajout de noeuds à des domaines d'unité
6. Création d'un domaine d'administration de grappe
7. Démarrage d'un domaine d'administration de grappe
8. Création d'un pool de stockage sur disque indépendant
9. Ajout de postes de ressource contrôlée
10. Création d'un groupe de ressources en grappe d'unité
11. Démarrage d'un groupe de ressources en grappe d'unité
12. Mise en fonction du pool de stockage sur disque
13. Configuration de l'écriture miroir géographique.
14. Réalisation d'un basculement pour tester la configuration.

Scénario : Protection par disque miroir d'un site à l'autre avec Metro Mirror

Ce scénario décrit une solution à haute disponibilité IBM i basée sur un stockage externe, qui fournit une reprise après incident et une haute disponibilité aux systèmes de stockage séparés par de petites distances. Metro Mirror est une solution IBM System Storage qui copie les données de façon synchronisée à partir de l'unité de stockage qui se trouve sur le site de production vers celle du site de sauvegarde. De cette façon, la cohérence des données est maintenue sur le site de sauvegarde.

Présentation

La solution de fonction miroir entre sites avec Metro Mirror offre une haute disponibilité et une reprise après incident grâce à l'utilisation d'unités de stockage externes à l'intérieur d'une zone métropolitaine. Le pool de stockage sur disque indépendant est dupliqué sur les unités de stockage externe pour fournir une disponibilité en cas d'indisponibilité prévue ou imprévue. Quand Metro Mirror reçoit une mise à jour d'hôte dans le volume de production, elle complète la mise à jour correspondante dans le volume de sauvegarde. Metro Mirror prend en charge une distance maximale de 300 kilomètres. Les retards des temps de réponse pour Metro Mirror sont proportionnels à la distance entre les volumes.

Ce scénario couvre la configuration de la technologie à haute disponibilité IBM i et ne fournit aucune instruction d'installation ou de configuration relatives aux produits IBM System Storage DS8000. Ces informations supposent qu'une solution IBM System Storage est déjà installée avant que la configuration à haute disponibilité i5/OS ne soit effectuée. Pour obtenir des informations d'installation et de configuration sur DS8000, voir IBM System Storage DS8000 Information Center .

Objectifs

Cette solution présente les avantages suivants :

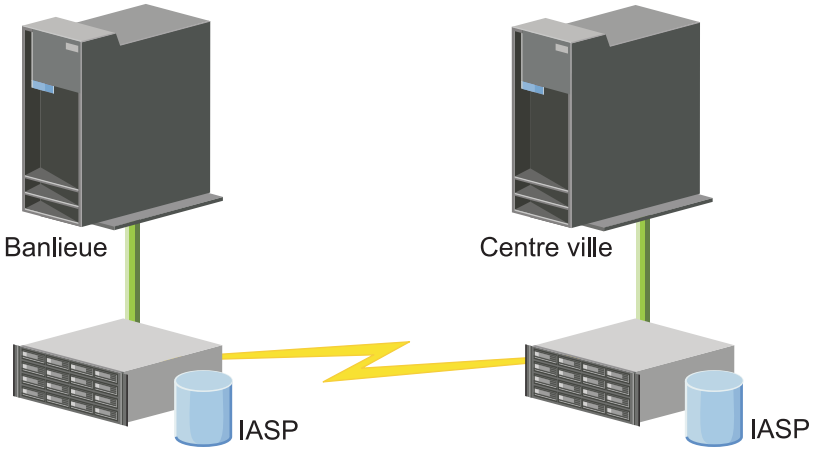
- La réplication est entièrement gérée par l'unité de stockage externe, ainsi aucune unité centrale IBM i n'est utilisée. La réplication se poursuit dans l'unité de stockage même quand le système subit une erreur de niveau système.
- La disponibilité des ressources professionnelles lors d'indisponibilités prévues ou imprévues, telles que les indisponibilités de maintenance ou celles liées aux logiciels/PTF, ainsi que la reprise sur incident.
- L'entrée-sortie reste cohérente et n'a pas besoin d'être synchronisée
- Temps de reprise rapide en cas d'utilisation avec la journalisation. La journalisation récupère les données plus rapidement en cas d'indisponibilité ou de reprise en ligne imprévue. Elle transfère les modifications apportées aux données vers le disque où l'écriture miroir se produit. Si vous n'utilisez pas la journalisation, vous pouvez perdre des données stockées dans la mémoire. La journalisation permet la restauration de ces transactions de données et l'accélère.
- La possibilité d'utiliser la fonction FlashCopy du côté source ou cible de Metro Mirror.

Cette solution présente les restrictions suivantes :

- Nécessite du matériel de stockage externe
- Envisagez d'utiliser des chemins de communication redondants et une bande passante appropriée.
- Il n'existe aucun accès simultané au pool de stockage sur disque

Détails

Le graphique suivant illustre cette solution :



Etapes de configuration

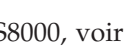
1. Achèvement de la liste de contrôle de planification des grappes
2. Création d'une grappe
3. Ajout de noeuds
4. Démarrage des noeuds
5. Ajout de noeuds à des domaines d'unité
6. Création d'un domaine d'administration de grappe
7. Démarrage d'un domaine d'administration de grappe
8. Création d'un pool de stockage sur disque indépendant
9. Ajout de postes de ressource contrôlée
10. Création d'un groupe de ressources en grappe d'unité
11. Démarrage d'un groupe de ressources en grappe d'unité
12. Mise en fonction du pool de stockage sur disque
13. Configuration de la session Metro Mirror
14. Réalisation d'un basculement pour tester la configuration.

Scénario : Protection par disque miroir d'un site à l'autre via Global Mirror

Ce scénario décrit une solution à haute disponibilité i5/OS basée sur un stockage externe et qui fournit une reprise après incident et une haute disponibilité aux systèmes de stockage séparés par de grandes distances. Global Mirror est une solution IBM System Storage qui copie les données de façon asynchrone à partir de l'unité de stockage qui se trouve sur le site de production vers celle du site de sauvegarde. De cette façon, la cohérence des données est maintenue sur le site de sauvegarde.

Présentation générale

La solution de fonction miroir entre sites avec Global Mirror permet une reprise après incident grâce à l'utilisation d'unités de stockage externes sur de longues distances. Le pool de stockage sur disque indépendant est dupliqué sur les unités de stockage externe pour fournir une disponibilité en cas d'indisponibilité prévue ou imprévue.

Ce scénario couvre la configuration de la technologie à haute disponibilité IBM i et ne fournit aucune instruction d'installation ou de configuration relatives aux produits IBM System Storage DS8000. Ces informations supposent qu'une solution IBM System Storage est déjà installée avant que la configuration à haute disponibilité i5/OS ne soit effectuée. Pour obtenir des informations d'installation et de configuration sur DS8000, voir IBM System Storage DS8000 Information Center  .

Objectifs

La protection par disque miroir d'un site à l'autre via Global Mirror présente les avantages suivants :

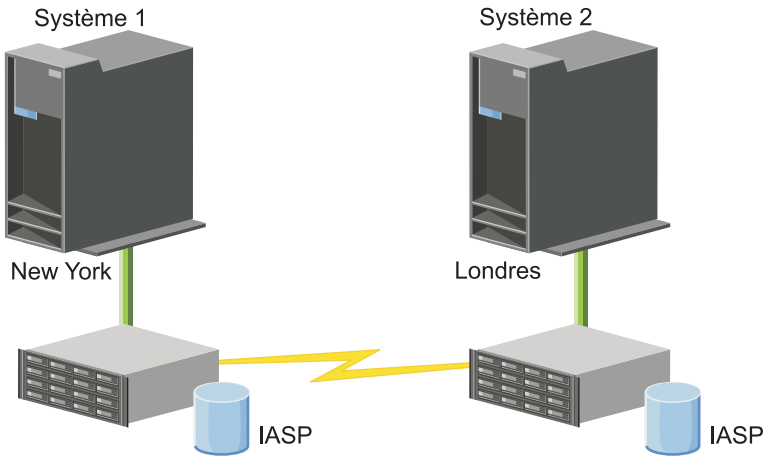
- La réplication est entièrement gérée par l'unité de stockage externe, ainsi aucune unité centrale IBM i n'est utilisée. La réplication se poursuit dans l'unité de stockage même quand le système subit une erreur de niveau système.
- La disponibilité des ressources professionnelles lors d'indisponibilités prévues ou imprévues, telles que les indisponibilités de maintenance ou celles liées aux logiciels/PTF, ainsi que la reprise sur incident.
- Temps de reprise rapide en cas d'utilisation avec la journalisation. La journalisation récupère les données plus rapidement en cas d'indisponibilité ou de reprise en ligne imprévue. Elle transfère les modifications apportées aux données vers le disque où l'écriture miroir se produit. Si vous n'utilisez pas la journalisation, vous pouvez perdre des données stockées dans la mémoire. La journalisation permet la restauration de ces transactions de données et l'accélère.
- La possibilité d'utiliser la fonction FlashCopy du côté source ou cible de Global Mirror.

Cette solution présente les restrictions suivantes :

- La solution requiert un poste serveur IBM System Storage DS8000.
- Pour obtenir des performances acceptables, pensez à utiliser des chemins de communication redondants et une bande passante adéquate.
- L'accès simultané au pool de stockage sur disque n'est pas possible.
- Seule une partition System i peut configurer Global Mirror sur un serveur System Storage donné. Aucune autre partition ou serveur System i d'une autre plateforme ne peut utiliser Global Mirror en même temps. L'ajout de plusieurs utilisateurs à une session Global Mirror entraînera des résultats imprévisibles.
- Un groupe de cohérence est obligatoire pour la copie cible Global Mirror. Le groupe de cohérence n'est pas obligatoire pour la copie source Global Mirror mais il est vivement recommandé.
- La réplication inverse s'exécute automatiquement sur un système de basculement uniquement si la nouvelle cible possède un groupe de cohérence. La réplication inverse ne s'exécute jamais automatiquement sur un système de reprise.
- Quand la réplication inverse ne s'exécute pas sur un système de basculement ou de reprise, la configuration comprend deux copies source.
  - Si le noeud de copie cible souhaité possède un groupe de cohérence, une opération de rattachement le convertit en copie cible et initialise automatiquement la réplication.
  - Dans le cas contraire, la reprise requiert une intervention manuelle avec l'interface System Storage DS8000 Storage Manager afin d'initialiser la réplication et de synchroniser la source et la cible actuelles.

Détails

L'image suivante illustre cette solution :



Etapes de configuration

1. Achèvement de la liste de contrôle de planification des grappes
2. Création d'une grappe
3. Ajout de noeuds
4. Démarrage des noeuds
5. Ajout de noeuds à un domaine d'unité
6. Création d'un domaine d'administration de grappe
7. Démarrage d'un domaine d'administration de grappe
8. Création d'un pool de stockage sur disque indépendant
9. Ajout de postes de ressource contrôlée
10. Création d'un groupe de ressources en grappe d'unité
11. Démarrage d'un groupe de ressources en grappe d'unité
12. Mise en fonction du pool de stockage sur disque
13. Configuration de la session Global Mirror
14. Réalisation d'un basculement pour tester la configuration.

Configuration du protocole TCP/IP pour la haute disponibilité

Comme les services-ressources de mise en grappe utilisent uniquement le protocole IP pour communiquer avec d'autres noeuds (à savoir des systèmes ou des partitions logiques dans un environnement à haute disponibilité), tous les noeuds de la grappe doivent être accessibles via IP : vous devez donc avoir des interfaces IP configurées pour connecter les noeuds dans votre grappe.

Les adresse IP doivent soit être configurées manuellement par l'administrateur de réseau dans les tables de routage du protocole TCP/IP sur chaque noeud de la grappe, soit générées par des protocoles de routage s'exécutant sur les routeurs en réseau. Cette table de routage du protocole TCP/IP est la mappe utilisée par la mise en grappe pour rechercher les noeuds ; chaque noeud doit donc posséder sa propre adresse IP.

Chaque noeud peut avoir jusqu'à deux adresses IP. Ces adresses ne doivent pas être modifiées par d'autres applications de communication réseau. Au moment d'attribuer une adresse, veillez à prendre en compte la ligne de communication qu'elle utilise. Si vous préférez un certain type de support de

communication, assurez-vous de configurer la première adresse IP avec ce support. La première adresse IP est traitée en priorité par la fonction de message fiable et le moniteur de signaux. Toutes les adresses IP de grappe de tous les noeuds doivent permettre de communiquer avec les autres adresses IP présentes dans la grappe. Si un noeud de la grappe utilise une adresse IPv4, chaque noeud de la grappe doit posséder une adresse IPv4 active (pas nécessairement configurée comme adresse IP de grappe) permettant de router et d'envoyer des paquets TCP à cette adresse. De même, si un noeud de la grappe utilise une adresse IPv6, chaque noeud de la grappe doit posséder une adresse IPv6 active (pas nécessairement configurée comme adresse IP de grappe) permettant de router et d'envoyer des paquets TCP à cette adresse. Pour vérifier si une adresse peut en atteindre une autre, vous pouvez exécuter la commande PING et utiliser une route de trace de messages UDP dans les deux sens. Notez toutefois que les commandes PING et TRACEROUTE ne fonctionnent pas entre une adresse IPv4 et une adresse IPv6 ou encore si un pare-feu les bloque.

Remarque : Vous devez vous assurer que l'adresse de bouclage (127.0.0.1) est active pour la mise en grappe. Normalement, cette adresse, qui sert à envoyer des messages au noeud local, est par défaut active. Toutefois, si elle a par erreur été arrêtée, la messagerie de la grappe ne fonctionne pas tant qu'elle n'est pas redémarrée.

Définition des attributs de configuration TCP/IP

Pour activer les services-ressources de mise en grappe, certains paramètres d'attributs sont obligatoires dans la configuration du protocole TCP/IP de votre réseau.

Vous devez définir ces attributs avant d'ajouter un noeud à une grappe :

- Définissez le réacheminement des datagrammes IP à *YES à l'aide de la commande CHGTCPA (Change TCP/IP Attributes) si vous envisagez d'utiliser un produit System i comme routeur pour communiquer avec d'autres réseaux et qu'aucun autre protocole de routage ne s'exécute sur ce serveur.
- Définissez le serveur INETD à START. Voir «Démarrage du serveur INETD» pour obtenir des informations sur le démarrage du serveur INETD.
- Définissez le total de contrôle du protocole de datagramme utilisateur à *YES à l'aide de la commande CHGTCPA (Change TCP/IP Attributes).
- Définissez le réacheminement MCAST à *YES si vous utilisez des ponts pour connecter vos réseaux à anneau à jeton.
- Si vous utilisez OptiConnect for i5/OS pour la communication entre des noeuds, démarrez le sous-système QSOC en indiquant STRSBS(QSOC/QSOC).

Démarrage du serveur INETD

Le serveur INETD (Internet Daemon) doit être démarré pour qu'un noeud soit ajouté ou démarré, et pour la fusion du traitement des partitions.

Il est conseillé de laisser le serveur INETD en exécution dans votre grappe.

Pour démarrer le serveur INETD avec IBM Systems Director Navigator for i5/OS, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans l'arborescence de navigation, développez **Gestion de i5/OS** puis sélectionnez **Réseau**.
4. Dans la page Réseau, sélectionnez **Serveurs TCP/IP**. La liste des serveurs TCP/IP disponibles s'affiche.
5. Dans la liste, sélectionnez **INETD**.
6. Dans le menu **Sélection d'une action**, sélectionnez **Démarrage**. L'état du serveur devient **Démarré**.

Le serveur INETD peut également être lancé en utilisant la commande Start TCP/IP Server (STRTCPSVR) et en spécifiant le paramètre SERVER(*INETD). Quand le serveur INETD est démarré, un travail d'utilisateur QTCP (QTOGINTD) se trouve dans la liste des travaux actifs sur le noeud.

Référence associée

STRTCPSVR (Start TCP/IP Server) command

Configuration des grappes

Toute implémentation i5/OS à haute disponibilité nécessite une grappe configurée pour contrôler et gérer des ressources résilientes. Quand elle est utilisée avec d'autres technologies de test de résistance, telles que le disque commuté, la protection sur disque miroir d'un site à l'autre ou la réplication logique, la technologie des grappes fournit l'infrastructure clé nécessaire aux solutions à haute disponibilité.

Les services-ressources de mise en grappe fournissent un ensemble de services intégrés qui conservent la topologie de la grappe, effectuent un contrôle des signaux et permettent la création et l'administration de la configuration de groupe et des groupes de ressources en grappe. Les services-ressources de mise en grappe fournissent également des fonctions de messagerie fiables qui suivent chaque noeud de la grappe et s'assurent que tous les noeuds possèdent des informations cohérentes sur l'état des ressources de la grappe. L'interface graphique des services-ressources de mise en grappe, qui font partie de IBM PowerHA for i (iHASM) numéro du logiciel sous licence (5770-HAS), vous permet de configurer et de gérer des grappes dans le cadre de votre solution à haute disponibilité. En outre, le logiciel sous licence fournit également un ensemble de commandes de langage de contrôle qui vous permettront d'utiliser des configurations de grappe.

Des interfaces de programmations et des fonctions peuvent également être utilisées par des fournisseurs d'application ou des clients pour améliorer la disponibilité de leur application.

Outre ces technologies IBM, des partenaires commerciaux à haute disponibilité fournissent des applications qui utilisent des grappes munies de la technologie de réplication logique.

Création d'une grappe

Pour créer une grappe, vous devez y inclure au moins un noeud et vous devez avoir accès à au moins l'un des noeuds qui fera partie de la grappe.

Si un seul noeud est spécifié, il doit s'agir du système auquel vous accédez. Pour obtenir la liste complète des spécifications pour la création des grappes, voir la section «Planification de la liste de contrôle des grappes», à la page 76.

Si vous comptez utiliser des unités commutables dans votre grappe ou des technologies de protection par disque miroir d'un site à l'autre pour configurer une solution à haute disponibilité, d'autres spécifications s'appliquent. Voir Scénarios : Configuration des solutions à haute disponibilité pour accéder à plusieurs exemples de configuration de solutions à haute disponibilité qui utilisent ces technologies. Chaque scénario fournit des tâches de configuration détaillées et une présentation de dépannage en cas d'indisponibilité proposé par cette solution. Vous pouvez utiliser ces exemples pour configurer votre solution à haute disponibilité ou les personnaliser pour qu'ils répondent à vos besoins.

Les étapes suivantes vous permettent de créer une grappe :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page de bienvenue, sélectionnez **Nouvelle grappe**.
5. Suivez les instructions de l'assistant de création de grappe pour créer la grappe.

Une fois que vous avez créé la grappe, la page de bienvenue change et affiche le nom de la grappe en début de page. La page de bienvenue répertorie maintenant les tâches qui vous permettront de gérer les grappes.

Une fois la grappe créée, vous devez ajouter des noeuds supplémentaires et créer des groupes de ressources en grappe.

Information associée

Create Cluster (CRTCLU) command

Create Cluster (QcstCreateCluster) API

Activation des noeuds à ajouter à une grappe

Avant d'ajouter un noeud à une grappe, vous devez définir une valeur pour l'attribut de réseau ALWADDCLU (Autorisation d'un ajout à la grappe).

Utilisez la commande CHGNETA (Modification des attributs réseau) sur les serveurs de votre choix que vous voulez configurer comme noeud de grappe. La commande CHGNETA modifie les attributs réseau d'un système. L'attribut réseau ALWADDCLU indique si un noeud autorise un autre système à l'ajouter comme noeud dans une grappe.

Remarque : Vous devez posséder les droits d'accès *IOSYSCFG pour modifier l'attribut réseau ALWADDCLU.

Les valeurs possibles sont les suivantes :

***SAME**
La valeur ne change pas. Le système est expédié avec une valeur de *NONE.

***NONE**
Aucun autre système ne peut ajouter ce système comme noeud dans une grappe.

***ANY** Tous les autres systèmes peuvent ajouter ce système comme noeud dans une grappe.

***RQSAUT**
Tous les autres systèmes peuvent ajouter ce système comme noeud dans une grappe seulement après que la demande d'ajout à la grappe a été authentifiée.

L'attribut de réseau ALWADDCLU est vérifié afin de définir si le noeud ajouté peut faire partie de la grappe et si la demande de grappe doit être validée à l'aide de certificats numériques X.509. Un *certificat numérique* est une forme d'identification personnelle qui peut être vérifiée électroniquement. Si la validation est obligatoire, les éléments suivants doivent être installés sur les systèmes du noeud qui effectue la demande et du noeud ajouté :

- i5/OS Option 34 (gestionnaire de certificats numériques)
- i5/OS Option 35 (fournisseur de service cryptographique CCA)

Quand *RQSAUT est sélectionnée pour l'attribut ALWADDCLU, la liste sécurisée de l'autorité de certification pour l'application du serveur de sécurité i5/OS doit être configurée correctement. L'identificateur de l'application serveur est QIBM_QCST_CLUSTER_SECURITY. Au minimum, ajoutez des autorités de certification pour les noeuds que vous autorisez à rejoindre le grappe.

Ajout de noeuds

L'interface graphique des services-ressources de mise en grappe vous permet de créer une grappe simple à deux noeuds lors de la création initiale de la grappe. Vous pouvez ajouter des noeuds supplémentaires à la grappe de votre solution à haute disponibilitéi5/OS.

Si vous créez une nouvelle grappe dans le cadre d'une solution à haute disponibilité, vous devez ajouter des noeuds supplémentaires via un noeud actif de la grappe.

Pour ajouter un noeud à une grappe existante, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans l'onglet **Noeuds**, cliquez sur le menu **Sélection d'une action** et sélectionnez l'option **Ajout noeud**. La page d'ajout d'un noeud s'affiche.
6. Sur la page d'ajout d'un noeud, spécifiez les informations du nouveau noeud. Cliquez sur **OK** pour ajouter le noeud. Le nouveau noeud apparaît dans la liste des noeuds. Une grappe peut contenir jusqu'à 128 noeuds.

Démarrage de noeuds

Le démarrage d'un noeud de grappe lance la mise en grappe et les services-ressources de mise en grappe sur un noeud dans un environnement à haute disponibilité i5/OS.

Un noeud peut démarrer seul et rejoindre la grappe active en cours, à condition qu'il trouve un noeud actif dans cette grappe.

Pour démarrer la mise en grappe sur un noeud, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans l'onglet **Noeuds**, sélectionnez le noeud à démarrer.
5. Cliquez sur le menu **Sélection d'une action** et sélectionnez **Démarrage**. Une fois les services-ressources de mise en grappe démarrés sur le noeud indiqué, l'état du noeud est Démarré.

Ajout d'un noeud à un domaine d'unité

Un domaine d'unité est un sous-réseau de noeuds dans une grappe qui partage des ressources en grappe.

Si vous implémentez une solution à haute disponibilité qui contient des technologies de pools de stockage sur disque indépendant, tels qu'un disque commuté ou une protection par disque miroir entre les sites, vous devez définir le noeud comme membre d'un domaine d'unité. Après avoir ajouté le noeud à un domaine d'unité, vous pouvez créer un groupe de ressources en grappe d'unité qui définit le domaine de reprise de la grappe. Tous les noeuds qui se trouveront dans le domaine de reprise d'un groupe de ressources en grappe d'unité doivent se trouver dans le même domaine d'unité. Un noeud de grappe peut appartenir à un seul domaine d'unité.

Pour créer et gérer des domaines d'unité, vous devez installer i5/OS Option 41 (HA Switchable Resources). Une clé de licence valide doit exister sur tous les noeuds de grappe du domaine d'unité.

Pour ajouter un noeud à un domaine d'unité, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.

4. Sur la page des services-ressources de mise en grappe, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste des noeuds de la grappe.
5. Dans l'onglet **Noeuds**, sélectionnez le noeud que vous voulez ajouter au domaine d'unité.
6. Dans le menu **Sélection d'une action**, sélectionnez les **Propriétés**.
7. Dans l'onglet **Mise en grappe**, spécifiez le nom du domaine d'unité auquel vous voulez ajouter le noeud dans la zone **Domaine d'unité**.

Création de groupes de ressources en grappe

Les groupes de ressources en grappe gèrent des ressources à haute disponibilité, telles que des applications, des données et des unités. Chaque type de groupe de ressources en grappe gère le type de ressource particulier à un environnement à haute disponibilité.

L'interface graphique des services-ressources de mise en grappe vous permet de créer des groupes de ressources en grappe différents pour la gestion de vos ressources à haute disponibilité. Chaque type de groupe de ressources en grappe peut être utilisé séparément ou conjointement avec d'autres groupes de ressources en grappe. Par exemple, vous pouvez posséder une application métier autonome qui nécessite une haute disponibilité. Une fois l'application activée pour la haute disponibilité, vous pouvez créer des groupes de ressources en grappe pour gérer la disponibilité de cette application.

Si vous ne voulez qu'une seule application, et que ses données ne soient pas disponibles en cas d'indisponibilité, vous pouvez créer un groupe de ressources en grappe d'application. Cependant, si vous voulez que les données et l'application soient disponibles, vous pouvez les stocker tous les deux dans un pool de stockage sur disque indépendant, que vous pouvez définir dans un groupe de ressources en grappe d'unité. Si une indisponibilité se produit, la totalité du pool de stockage sur disque indépendant est basculée vers un noeud de sauvegarde, ce qui rend disponible l'application et les données.

Création de groupes de ressources en grappe :

Si vous possédez plusieurs applications dans votre solution à haute disponibilité que vous voulez rendre hautement disponible, vous pouvez créer un groupe de ressources en grappe d'application pour gérer les reprises en ligne de cette application.

Vous pouvez indiquer une adresse IP de relais active lors de la création du groupe de ressources en grappe d'application. Quand vous lancez un groupe de ressources d'application, qui autorise une adresse IP de relais active, le groupe de ressources en grappe peut être démarré.

Pour créer un groupe de ressources en grappe d'application, procédez comme suite :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe de l'application** et cliquez sur **OK**. La page du nouveau groupe de ressources en grappe de l'application apparaît.
7. Dans la page **Général**, spécifiez les informations suivantes relatives au groupe de ressources en grappe de l'application :
   - Dans la zone **Nom**, indiquez le nom du groupe de ressources en grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - Dans la zone **Adresse IP de relais**, indiquez l'adresse IP qui doit être associée au groupe de ressources en grappe de l'application. Cette valeur doit être au format IPv4 ou IPv6. L'adresse IP de

relais permet d'accéder à l'application quel que soit le système sur lequel l'application s'exécute. La zone **Configuration de l'adresse IP de relais** détermine si l'utilisateur ou les services-ressources de mise en grappe sont responsables de la création de l'adresse IP.

- Dans la zone **Description**, saisissez une description du groupe de ressources en grappe. La description ne peut pas dépasser 50 caractères.
- Sélectionnez **Permettre le redémarrage** et indiquez le nombre de tentatives de redémarrage du groupe de ressources en grappe de l'application. Ces valeurs déterminent le nombre de tentatives de redémarrage de l'application sur le même noeud avant qu'une reprise en ligne vers le noeud de sauvegarde se produise.
- Dans la zone **Configuration de l'adresse IP de relais**, sélectionnez si vous voulez que les services-ressources de mise en grappe ou un utilisateur configurent et gèrent l'adresse IP de relais de l'application. Les valeurs possibles sont les suivantes :

  Services-ressources de mise en grappe
  Si vous spécifiez cette valeur, l'adresse IP de relais ne doit exister sur aucun noeud du domaine de reprise avant la création du groupe de ressources en grappe. Elle est créée pour vous sur tous les noeuds du domaine de reprise. Si l'adresse IP existe déjà, alors la création du groupe de ressources en grappe d'application échoue.

  Utilisateur
  Si vous indiquez cette valeur, vous devez ajouter l'adresse IP de relais sur tous les noeuds principaux et de sauvegarde du domaine de reprise avant de pouvoir démarrer le groupe de ressources en grappe.
- Sélectionnez **Permettre une adresse IP de relais active** pour permettre l'activation d'une adresse IP de relais, quand elle est affectée à un groupe de ressources en grappe de l'application. Cette zone est correcte uniquement lorsque la zone Configuration de l'adresse IP de relais est défini sur services-ressources de mise en grappe.
- Dans la zone **File d'attente utilisateur de distribution d'informations**, indiquez le nom de la file d'attente utilisateur censée recevoir les informations distribuées. Ce nom ne peut pas comporter plus de 10 caractères. Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente utilisateur censée recevoir les informations distribuées. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL. Ce nom ne peut pas comporter plus de 10 caractères.

  Remarque : Si vous ne renseignez pas la file d'attente utilisateur de distribution d'informations, vous devez également laisser la zone Nom de bibliothèque vide, définir le délai d'attente avant reprise en ligne sur 0 et l'action par défaut de reprise en ligne sur 0.
- Dans la zone **File de messages de reprise en ligne**, indiquez le nom de la file d'attente de messages censée recevoir les messages lorsqu'une reprise en ligne se produit pour ce groupe de ressources en grappe. Si cette zone est définie, la file d'attente de messages spécifiée doit exister sur tous les noeuds du domaine de reprise une fois le programme d'exit terminé. La file d'attente de messages de reprise en ligne ne peut pas faire partie d'un pool de stockage sur disque indépendant. Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL.
- Dans la zone **Délai d'attente avant reprise en ligne**, indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de la grappe. Les valeurs possibles sont les suivantes :

  Ne pas attendre
  La reprise en ligne se poursuit sans intervention de l'utilisateur.

  Toujours attendre
  La reprise en ligne est systématiquement mise en attente jusqu'à la réception d'une réponse au message de demande de reprise en ligne.

  numéro
  Indiquez le délai d'attente (en minutes) avant l'obtention d'une réponse au message de

demande de reprise en ligne. Si une réponse est reçue hors délai, la valeur dans la zone Action par défaut de reprise en ligne indique la procédure à suivre.

- Dans la zone **Action par défaut de reprise en ligne**, indiquez l'action que la mise en grappe doit effectuer lorsqu'une réponse au message relatif à la reprise en ligne sur la file d'attente de messages de grappe a été reçu au-delà du délai d'attente avant reprise en ligne. Vous pouvez définir cette zone sur **Poursuite du basculement** ou sur **Annulation du basculement**.

8. Dans la page **Programme d'exit**, vous pouvez indiquer les informations d'un programme d'exit pour un groupe de ressources en grappe. Les programmes d'exit sont requis pour tous les types de groupes de ressources en grappe à l'exception des groupes de ressources en grappe d'unité. Ils sont appelés après qu'un événement de groupe de ressources en grappe lié à la grappe se produise et réponde à cet événement.
9. Dans la page **Domaine de reprise**, ajoutez des noeuds au domaine de reprise et indiquez leur rôle dans la grappe.

Création de groupes de ressources en grappe de données :

Les groupes de ressources en grappe sont principalement utilisés avec des applications de réplication logique, fournies par des partenaires commerciaux à haute disponibilité. Si vous implémentez une solution à haute disponibilité fondée sur réplication logique, vous pouvez créer un groupe de ressources en grappe de données pour soutenir la réplication des données entre les noeuds principaux et les noeuds de sauvegarde.

Pour créer un groupe de ressources en grappe de données, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe de données** et cliquez sur **OK**. La page du nouveau groupe de ressources en grappe de données apparaît.
7. Dans la page **Général**, spécifiez les informations suivantes relatives au groupe de ressources en grappe de données :
   - Dans la zone **Nom**, indiquez le nom du groupe de ressources en grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - Dans la zone **Description**, saisissez une description du groupe de ressources en grappe. La description ne peut pas dépasser 50 caractères.
   - Dans la zone **File d'attente utilisateur de distribution d'informations**, indiquez le nom de la file d'attente utilisateur censée recevoir les informations distribuées. Ce nom ne peut pas comporter plus de 10 caractères. Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente utilisateur censée recevoir les informations distribuées. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL. Ce nom ne peut pas comporter plus de 10 caractères.

     Remarque : Si vous ne renseignez pas la file d'attente utilisateur de distribution d'informations, vous devez également laisser la zone Nom de bibliothèque vide, définir le délai d'attente avant reprise en ligne sur 0 et l'action par défaut de reprise en ligne sur 0.
   - Dans la zone **File de messages de reprise en ligne**, indiquez le nom de la file d'attente de messages censée recevoir les messages lorsqu'une reprise en ligne se produit pour ce groupe de ressources en grappe. Si cette zone est définie, la file d'attente de messages spécifiée doit exister sur tous les noeuds du domaine de reprise une fois le programme d'exit terminé. La file d'attente de messages de reprise en ligne ne peut pas faire partie d'un pool de stockage sur disque indépendant.

Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL.

- Dans la zone **Délai d'attente avant reprise en ligne**, indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de la grappe. Les valeurs possibles sont les suivantes :

  Ne pas attendre
  La reprise en ligne se poursuit sans intervention de l'utilisateur.

  Toujours attendre
  La reprise en ligne est systématiquement mise en attente jusqu'à la réception d'une réponse au message de demande de reprise en ligne.

  numéro
  Indiquez le délai d'attente (en minutes) avant l'obtention d'une réponse au message de demande de reprise en ligne. Si une réponse est reçue hors délai, la valeur dans la zone Action par défaut de reprise en ligne indique la procédure à suivre.

8. Dans la page **Programme d'exit**, vous pouvez indiquer les informations d'un programme d'exit pour un groupe de ressources en grappe. Les programmes d'exit sont requis pour tous les types de groupes de ressources en grappe à l'exception des groupes de ressources en grappe d'unité. Ils sont appelés après qu'un événement de groupe de ressources en grappe lié à la grappe se produise et réponde à cet événement.
9. Dans la page **Domaine de reprise**, ajoutez des noeuds au domaine de reprise et indiquez leur rôle dans la grappe.

Création de groupes de ressources en grappes d'unité :

Un groupe de ressources en grappe d'unité est constitué d'un groupe de ressources matériel pouvant être commuté en tant qu'entité. Pour créer des unités commutables dans une solution à haute disponibilité, les noeuds qui utilisent ces unités doivent faire partir d'un groupe de ressources en grappe d'unité.

Avant de créer un groupe de ressources en grappe d'unité, ajoutez tous les noeuds qui partageront une ressource commutable à un domaine d'unité.

Pour créer un groupe de ressources en grappe d'unité, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe d'unité** et cliquez sur **OK**. L'assistant **Nouveau groupe de ressources en grappe d'unité** apparaît. La tâche **Nouveau groupe de ressources en grappe d'unité** est disponible uniquement si tous les noeuds du domaine de reprise sont démarrés.
7. Suivez les instructions de l'assistant **Nouveau groupe de ressources en grappe d'unité** pour créer un nouveau groupe de ressources en grappe d'unité. Pendant l'exécution de cet assistant, vous pouvez créer un nouveau groupe de ressources en grappe d'unité. Vous pouvez également créer un nouveau pool de stockage sur disque indépendant ou en spécifier un existant.

   Le groupe de ressources en grappe d'unité conserve les informations de ressource matériel sur l'ensemble des noeuds du domaine de reprise et vérifie que les noms de ressource sont identiques. Vous pouvez également configurer un domaine d'administration de grappe pour conserver les

attributs inscrits des objets de configuration, lesquels peuvent inclure des noms de ressource, identiques sur l'ensemble du domaine d'administration. Si vous utilisez la protection par disque miroir d'un site à l'autre, créez des groupes de ressources de grappe d'unité séparés pour les pools de stockage sur disque indépendant et les autres types d'unité commutable sur chaque site.

Création de groupes de ressources en grappe homologues :

Vous pouvez créer un groupe de ressources en grappe homologue pour définir des rôles de noeud dans des environnements à équilibrage de charge.

Pour créer un groupe de ressources en grappe homologue, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe homologue** et cliquez sur **OK**. La page Nouveau groupe de ressources en grappe homologue apparaît.
7. Dans la page **Général**, spécifiez les informations suivantes relatives au groupe de ressources en grappe homologue :
   - Dans la zone **Nom**, indiquez le nom du groupe de ressources en grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - Dans la zone **Description**, saisissez une description du groupe de ressources en grappe. La description ne peut pas dépasser 50 caractères.
   - Dans la zone **ID application**, indiquez l'identificateur d'application des groupes de ressources en grappe homologues au format *[NomFournisseur].[NomApplication]*. Par exemple, MonEntreprise.MonApplication. L'identificateur ne peut pas dépasser 50 caractères.
8. Dans la page **Programme d'exit**, vous pouvez indiquer les informations d'un programme d'exit pour un groupe de ressources en grappe. Les programmes d'exit sont requis pour tous les types de groupes de ressources en grappe à l'exception des groupes de ressources en grappe d'unité. Ils sont appelés après qu'un événement de groupe de ressources en grappe lié à la grappe se produise et réponde à cet événement.
9. Dans la page **Domaine de reprise**, ajoutez des noeuds au domaine de reprise et indiquez leur rôle dans la grappe.

Démarrage d'un groupe de ressources en grappe

Le démarrage d'un groupe de ressources en grappe active la mise en grappe au sein de votre environnement à haute disponibilité i5/OS.

Pour démarrer un groupe de ressources en grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Dans l'onglet **Groupe de ressources en grappe**, sélectionnez le nom du groupe de ressources en grappe à démarrer.

6. Dans le menu **Sélection d'une action**, sélectionnez **Démarrage**. La colonne Etat indique que le groupe de ressources en grappe est démarré.

Information associée

Start Cluster Resource Group (STRCRG) command

Create Cluster Resource Group (QcstCreateClusterResourceGroup) API

Indication des files d'attente de messages

Vous pouvez indiquer une file d'attente de messages de grappe ou une file d'attente de message de basculement. Ces files d'attente de messages vous permettent de déterminer les causes des échecs dans votre environnement i5/OS à haute disponibilité.

Une file d'attente de messages en grappe est utilisée pour des messages au niveau de la grappe et fournit un message qui contrôle tous les groupes de ressources en grappe qui basculent vers un noeud spécifique. Une file d'attente de message en basculement est utilisée pour les messages au niveau du groupe de ressources en grappe et fournit un message pour chaque groupe de ressources en grappe en cours de basculement.

Indication d'une file d'attente de messages de grappe

Remarque : Vous pouvez également configurer une grappe pour utiliser une file d'attente de messages de grappe en spécifiant la file d'attente de messages tout en exécutant l'assistant de création de grappe.

Pour définir une file d'attente de messages de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Affichage des propriétés d'une grappe**.
5. Dans la page Ppriétés d'une grappe, cliquez sur **File d'attente de messages de grappe**.
6. Spécifiez les informations suivantes pour créer une file d'attente de messages de grappe :
   - Dans la zone **Nom**, indiquez le nom de la file d'attente de messages pour recevoir des messages qui traitent d'un basculement au niveau d'une grappe ou d'un noeud. Pour les reprises en ligne au niveau des noeuds, un message contrôlant la reprise en ligne de tous les groupes de ressources en grappe avec le même nouveau noeud principal est envoyé. Si un groupe de ressources en grappe effectue la reprise en ligne individuellement, un message contrôlant la reprise en ligne de ce groupe de ressources en grappe est envoyé. Le message est envoyé au nouveau noeud principal. Si cette zone est définie, la file d'attente de messages indiquée doit exister sur tous les noeuds dans la grappe lorsqu'ils sont démarrés. La file d'attente de messages ne peut pas faire partie d'un pool de stockage sur disque indépendant.
   - Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de la bibliothèque ne peut pas être *CURLIB, QTEMP, *LIBL, *USRLIBL, *ALL ou *ALLUSR.
   - Dans la zone **Délai d'attente avant reprise en ligne**, sélectionnez **Ne pas attendre** or **Toujours attendre** ou indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de grappe.
   - Dans la zone **Action par défaut de reprise en ligne**, spécifiez l'action que les services-ressources de mise en grappe doivent effectuer quand la réponse au message de reprise en ligne a dépassé la valeur de la durée d'attente avant la reprise en ligne. Vous pouvez définir cette zone sur **Poursuite du basculement** ou sur **Annulation du basculement**.

Indication d'une file d'attente de messages de basculement

Pour définir une file d'attente de messages de basculement, procédez comme suit :

1. Dans un navigateur Web, saisissez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre de votre IBM Systems Director Navigator for i5/OS.
4. Dans cette page, cliquez sur **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Dans la liste des groupes de ressources en grappe, sélectionnez le groupe de ressource en grappe avec lequel vous voulez travailler.
6. Dans la page Groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action** et sélectionnez **Propriétés**.
7. Sur la page Général, indiquez les valeurs suivantes pour indiquer une file d'attente de messages de reprise en ligne :
   - Dans la zone **File de messages de reprise en ligne**, indiquez le nom de la file d'attente de messages censée recevoir les messages lorsqu'une reprise en ligne se produit pour ce groupe de ressources en grappe. Si cette zone est définie, la file d'attente de messages spécifiée doit exister sur tous les noeuds du domaine de reprise une fois le programme d'exit terminé. La file d'attente de messages de reprise en ligne ne peut pas faire partie d'un pool de stockage sur disque indépendant.
   - Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de la bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL.
   - Dans la zone **Délai d'attente avant reprise en ligne**, indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de reprise en ligne. Vous pouvez également indiquer l'action que les services-ressources de mise en grappe doivent effectuer quand la réponse au message de basculement a dépassé la valeur de la durée d'attente avant le basculement.

Exécution de basculements

Vous pouvez effectuer des basculements pour tester la solution à haute disponibilité ou pour gérer une indisponibilité planifiée du système pour le noeud principal, telle qu'une opération de sauvegarde ou une maintenance système planifiée.

L'exécution d'un basculement manuel entraîne le basculement du noeud principal en cours vers le noeud de secours. Le domaine de reprise du groupe de ressources en grappe définit ces rôles. Lors d'un basculement, les rôles des noeuds actuellement définis dans le domaine de reprise changent comme suit :

- Le noeud principal actuel se voit affecter le rôle du dernier noeud secondaire actif.
- La première sauvegarde actuelle se voit affecter le rôle de noeud principal.
- Les sauvegardes suivantes sont montées d'un niveau dans l'ordre.

Un basculement est uniquement autorisé sur les groupes de ressources en grappe d'applications, de données et d'unités avec un état Actif.

Remarque : Si vous effectuez un basculement sur un groupe de ressources en grappe d'unités, vous devez synchroniser le nom de profil utilisateur, le numéro utilisateur et l'ID groupe pour des questions de performances. Le domaine d'administration de la grappe simplifie la synchronisation des profils utilisateur.

Pour exécuter un basculement sur une ressource, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sélectionnez le groupe de ressources en grappe sur lequel vous voulez effectuer le basculement. Pour ce faire, vous pouvez sélectionner des groupes de ressources en grappe d'applications, de données ou d'unités.
6. Dans le menu **Sélection d'une action**, sélectionnez **Basculement**.
7. Cliquez sur **Oui** dans le panneau de confirmation.

Le groupe de ressources en grappe sélectionné est maintenant commuté sur le noeud secondaire. La colonne Etat est mise à jour avec le nouveau nom du noeud.

Concepts associés

Cluster administrative domain

Tâches associées

«Configuration des domaines d'administration en grappe», à la page 117
Dans un environnement à haute disponibilité, l'application et l'environnement d'exploitation doivent rester cohérents entre les noeuds qui participent à la haute disponibilité. Le domaine d'administration en grappe est l'implémentation i5/OS des tests de résistance de l'environnement et il garantit la cohérence de l'environnement d'exploitation dans les noeuds.

Information associée

Change Cluster Resource Group Primary (CHGCRGPRI) command

Initiate Switchover (QcstInitiateSwitchOver) API

Configuration des noeuds

Les noeuds sont des systèmes ou des partitions logiques qui participent à une solution à haute disponibilité i5/OS.

Plusieurs tâches sont liées à la configuration des noeuds. Quand vous utilisez l'assistant de création de grappe, vous pouvez configurer une grappe simple à deux noeuds. Vous pouvez par la suite ajouter des noeuds supplémentaires jusqu'à un total de 128. En fonction des technologies qui composent votre solution à haute disponibilité, des tâches de configuration de noeuds supplémentaires peuvent être exigées.

Démarrage de noeuds

Le démarrage d'un noeud de grappe lance la mise en grappe et les services-ressources de mise en grappe sur un noeud dans un environnement à haute disponibilité i5/OS.

Un noeud peut démarrer seul et rejoindre la grappe active en cours, à condition qu'il trouve un noeud actif dans cette grappe.

Pour démarrer la mise en grappe sur un noeud, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans l'onglet **Noeuds**, sélectionnez le noeud à démarrer.

5. Cliquez sur le menu **Sélection d'une action** et sélectionnez **Démarrage**. Une fois les services-ressources de mise en grappe démarrés sur le noeud indiqué, l'état du noeud est Démarré.

Information associée

Start Cluster Node (STRCLUNOD)) command

Start Cluster Node (QcstStartClusterNode) API

Activation des noeuds à ajouter à une grappe

Avant d'ajouter un noeud à une grappe, vous devez définir une valeur pour l'attribut de réseau ALWADDCLU (Autorisation d'un ajout à la grappe).

Utilisez la commande CHGNETA (Modification des attributs réseau) sur les serveurs de votre choix que vous voulez configurer comme noeud de grappe. La commande CHGNETA modifie les attributs réseau d'un système. L'attribut réseau ALWADDCLU indique si un noeud autorise un autre système à l'ajouter comme noeud dans une grappe.

Remarque : Vous devez posséder les droits d'accès *IOSYSCFG pour modifier l'attribut réseau ALWADDCLU.

Les valeurs possibles sont les suivantes :

***SAME**
La valeur ne change pas. Le système est expédié avec une valeur de *NONE.

***NONE**
Aucun autre système ne peut ajouter ce système comme noeud dans une grappe.

***ANY** Tous les autres systèmes peuvent ajouter ce système comme noeud dans une grappe.

***RQSAUT**
Tous les autres systèmes peuvent ajouter ce système comme noeud dans une grappe seulement après que la demande d'ajout à la grappe a été authentifiée.

L'attribut de réseau ALWADDCLU est vérifié afin de définir si le noeud ajouté peut faire partie de la grappe et si la demande de grappe doit être validée à l'aide de certificats numériques X.509. Un *certificat numérique* est une forme d'identification personnelle qui peut être vérifiée électroniquement. Si la validation est obligatoire, les éléments suivants doivent être installés sur les systèmes du noeud qui effectue la demande et du noeud ajouté :

- i5/OS Option 34 (gestionnaire de certificats numériques)
- i5/OS Option 35 (fournisseur de service cryptographique CCA)

Quand *RQSAUT est sélectionnée pour l'attribut ALWADDCLU, la liste sécurisée de l'autorité de certification pour l'application du serveur de sécurité i5/OS doit être configurée correctement. L'identificateur de l'application serveur est QIBM_QCST_CLUSTER_SECURITY. Au minimum, ajoutez des autorités de certification pour les noeuds que vous autorisez à rejoindre le grappe.

Ajout de noeuds

L'interface graphique des services-ressources de mise en grappe vous permet de créer une grappe simple à deux noeuds lors de la création initiale de la grappe. Vous pouvez ajouter des noeuds supplémentaires à la grappe de votre solution à haute disponibilitéi5/OS.

Si vous créez une nouvelle grappe dans le cadre d'une solution à haute disponibilité, vous devez ajouter des noeuds supplémentaires via un noeud actif de la grappe.

Pour ajouter un noeud à une grappe existante, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.

2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans l'onglet **Noeuds**, cliquez sur le menu **Sélection d'une action** et sélectionnez l'option **Ajout noeud**. La page d'ajout d'un noeud s'affiche.
6. Sur la page d'ajout d'un noeud, spécifiez les informations du nouveau noeud. Cliquez sur **OK** pour ajouter le noeud. Le nouveau noeud apparaît dans la liste des noeuds. Une grappe peut contenir jusqu'à 128 noeuds.

Information associée

Add Cluster Node Entry (ADDCLUNODE) command

Add Cluster Node Entry (QcstAddClusterNodeEntry) API

Ajout d'un noeud à un domaine d'unité

Un domaine d'unité est un sous-réseau de noeuds dans une grappe qui partage des ressources en grappe.

Si vous implémentez une solution à haute disponibilité qui contient des technologies de pools de stockage sur disque indépendant, tels qu'un disque commuté ou une protection par disque miroir entre les sites, vous devez définir le noeud comme membre d'un domaine d'unité. Après avoir ajouté le noeud à un domaine d'unité, vous pouvez créer un groupe de ressources en grappe d'unité qui définit le domaine de reprise de la grappe. Tous les noeuds qui se trouveront dans le domaine de reprise d'un groupe de ressources en grappe d'unité doivent se trouver dans le même domaine d'unité. Un noeud de grappe peut appartenir à un seul domaine d'unité.

Pour créer et gérer des domaines d'unité, vous devez installer i5/OS Option 41 (HA Switchable Resources). Une clé de licence valide doit exister sur tous les noeuds de grappe du domaine d'unité.

Pour ajouter un noeud à un domaine d'unité, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste des noeuds de la grappe.
5. Dans l'onglet **Noeuds**, sélectionnez le noeud que vous voulez ajouter au domaine d'unité.
6. Dans le menu **Sélection d'une action**, sélectionnez les **Propriétés**.
7. Dans l'onglet **Mise en grappe**, spécifiez le nom du domaine d'unité auquel vous voulez ajouter le noeud dans la zone **Domaine d'unité**.

Information associée

Add Device Domain Entry (ADDDEVDMNE) command

Add Device Domain Entry (QcstAddDeviceDomainEntry) API

Configuration de la détection avancée des incidents de noeud

Vous pouvez utiliser la détection avancée des incidents de noeud pour éviter la partition des grappes quand un noeud de grappe est défaillant. Pour cela, vous pouvez utiliser une partition Hardware Management Console (HMC) ou Virtual I/O Server (VIOS).

Dans cet exemple, la console HMC est utilisée pour gérer deux systèmes IBM distincts. Par exemple, la console HMC peut mettre sous tension chaque système ou configurer des partitions logiques sur chaque système. De plus, la console HMC surveille l'état de chaque système et des partitions logiques associées. Supposons que chaque système est un noeud de grappe et que les services de ressource de mise en grappe surveillent le signal de présence entre ces deux noeuds de grappe.

Grâce à la fonction de détection avancée des incidents de noeud, vous pouvez utiliser les services de ressource de mise en grappe de manière à utiliser la console HMC. Par exemple, vous pouvez configurer le noeud Node A de manière qu'un moniteur de grappe utilise la console HMC. Si la console HMC détecte une défaillance sur le noeud Node B (dans le système ou la partition logique de Node B), elle en informe les services de ressource de mise en grappe sur Node A. Les services de ressource de mise en grappe sur Node A marquent alors Node B comme défaillant et exécutent un basculement au lieu de partitionner la grappe.

De même, vous pouvez configurer Node B de manière qu'il utilise un moniteur de grappe. Dans cet exemple, en cas de défaillance de Node A ou de Node B, la console HMC notifie l'incident à l'autre noeud.

Pour configurer la détection avancée des incidents de noeud, procédez comme suit :

1. Configurez la console HMC, ou
2. Installez VIOS et exécutez les étapes de configuration.
3. Le serveur TCP *CIMOM doit être configuré et démarré sur chaque noeud de grappe possédant un moniteur de grappe configuré. Vous devez modifier la configuration par défaut du serveur *CIMOM fourni par l'installation du logiciel sous licence 5770-UME afin que le système IBM i puisse communiquer avec le serveur CIM. Pour cela, vous devez modifier deux attributs de configuration qui contrôlent les paramètres de sécurité en exécutant la commande cimconfig dans un shell PASE.
4. Démarrez le serveur à partir de la ligne de commande avec **STRTCPSVR *CIMOM** .
5. Démarrez un shell PASE à partir de la ligne de commande avec **CALL QP2TERM**.
6. Entrez **/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimconfig -s enableAuthentication=false -p** Voir Authentification sur CIMOM pour plus d'informations sur l'attribut enableAuthentication.
7. Entrez **/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimconfig -s sslClientVerificationMode=optional -p** Voir Authentification sur CIMOM pour plus d'informations sur l'attribut sslClientVerificationMode.

8. Fermez le shell PASE en appuyant sur la touche **F3**.
9. Fermez le serveur *CIMOM avec la commande **ENDTCPSVR *CIMOM**.
10. Redémarrez le serveur *CIMOM à partir de la ligne de commande avec **STRTCPSVR *CIMOM** .
11. Vous devez copier un certificat numérique délivré par la partition VIOS ou HMC sur le noeud de grappe et l'ajouter au fichier de clés certifiées. Les certificats numériques sont auto-signés par la partition VIOS ou HMC. L'installation d'une nouvelle version de logiciel sur la partition VIOS ou HMC génère un nouveau certificat qui provoque l'arrêt des communications entre la partition HMC ou la partition VIOS et le noeud de grappe (l'erreur CPFBBCB s'affiche avec le code d'erreur 4). Dans ce cas, ajoutez le certificat numérique dans le fichier de clés certifiées des noeuds dont la partition VIOS ou HMC est configurée dans un moniteur de grappe.
12. Pour effectuer la configuration de la grappe, vous pouvez utiliser au choix l'interface de ligne de commande, la commande CL Add Cluster Monitor (ADDCLUMON) ou un navigateur Web. Si vous choisissez la dernière option, procédez comme suit :
    a. Dans un navigateur Web, saisissez ***http://monsystème:2001***, où ***monsystème*** est le nom d'hôte du système.
    b. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
    a. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM System Director Navigator.
    b. Sélectionnez **Gestion des noeuds de grappe**.
    c. Sélectionnez le menu instantané d'un noeud.
    d. Sélectionnez **Propriétés**.
    e. Sélectionnez **Moniteurs**.
    f. Sélectionnez l'action **Ajouter un moniteur de grappe**.
    g. Entrez le nom d'hôte, l'ID utilisateur et le mot de passe du serveur CIM.
    h. Appuyez sur OK.

Configuration de la console de gestion matérielle (HMC)

Vous pouvez utiliser une console de gestion matérielle (Hardware Management Console - HMC) pour éviter la partition des grappes quand un noeud de grappe est défaillant.

Pour configurer la console HMC, procédez comme suit :

1. Vérifiez que le serveur TCP *CIMOM est actif sur votre système IBM i. Vous pouvez rechercher le travail QUMECIMOM dans le sous-système QSYSWRK afin de vérifier s'il est actif. Si le travail est inactif, vous pouvez le démarrer avec la commande STRTCPSVR *CIMOM.
2. Vérifiez que le serveur TCP *SSHD est actif sur votre système IBM i (sur la ligne de commande de l'écran vert, entrez STRTCPSVR *SSHD). Pour démarrer le serveur *SSHD, vérifiez que le système QSHRMEMC a la valeur 1.
3. Vous devez utiliser le moniteur physique et le clavier attachés à la console HMC. Vous ne pouvez pas utiliser Telnet ou une interface Web pour vous connecter à la console HMC.
4. Ouvrez un shell restreint. Pour cela, cliquez avec le bouton droit sur le bureau puis sélectionnez terminals/xterm.
5. Le bureau affiche une nouvelle fenêtre de shell dans laquelle vous pouvez saisir des commandes.
6. Pour l'étape suivante, vous devrez utiliser la commande de copie sécurisée sur la console HMC. Toutefois, un répertoire de base doit être associé à votre profil sur le système IBM i. Par exemple, si vous utilisez QSECOFR comme nom de profil dans la commande scp, un répertoire /home/QSECOFR doit être créé dans le système de fichiers intégré du système IBM i.
7. Utilisez la commande de copie sécurisée pour copier un fichier sur votre noeud de grappe IBM i (scp /etc/Pegasus/server.pem QSECOFR@LP0236A:/server_name.pem). Dans la commande ci-dessus, remplacez LP0236A par le nom de votre système IBM i et remplacez server_name.pem par hmc_name.pem. Par exemple, nommez le fichier myhmc.pem.
8. Fermez la session de la console HMC.

9. Ouvrez une session sur le système IBM i et affichez la ligne de commande de l'écran vert.
10. Entrez dans l'environnement de shell PASE. (Sur la ligne de commande de l'écran vert, entrez call qp2term)
11. Déplacez le certificat numérique de la console HMC avec la commande mv /myhmc.pem /QOpenSys/QIBM/UserData/UME/Pegasus/ssl/truststore/myhmc.pem (dans la commande ci-dessus, remplacez myhmc.pem par le nom de votre fichier).
12. Ajoutez le certificat numérique dans le fichier de clés certifiées. Pour cela, entrez /QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimtrust -a -U QSECOFR -f /QOpenSys/QIBM/UserData/UME/Pegasus/ssl/truststore/myhmc.pem -T s.
13. Dans la commande ci-dessus, remplacez myhmc.pem par le nom de votre fichier.
14. Quittez le shell PASE en appuyant sur la touche F3.
15. Fermez le serveur CIM. Sur la ligne de commande de l'écran vert, entrez ENDTCPSVR *CIMOM.
16. Redémarrez le serveur CIM pour récupérer le nouveau certificat. Sur la ligne de commande de l'écran vert, entrez STRTCPSVR *CIMOM.

Configuration de Virtual I/O Server (VIOS)

Vous pouvez utiliser un serveur Virtual I/O Server (VIOS) pour éviter la partition des grappes quand un noeud de grappe est défaillant.

Pour une partition VIOS, procédez comme suit :

1. Vérifiez que le serveur TCP *SSHD est actif sur votre système IBM i. Sur la ligne de commande de l'écran vert, entrez la commande **STRTCPSVR *SSHD**.
2. Connectez-vous à la partition VIOS avec Telnet et ouvrez une session.
3. Activez un shell non restreint avec la commande oem_setup_env.
4. Utilisez la commande de copie sécurisée pour copier un fichier sur votre noeud de grappe IBM i. Par exemple, entrez /usr/bin/scp /opt/freeware/cimom/pegasus/etc/cert.pem QSECOFR@system-name:/server.pem. Remplacez **system-name** par le nom du système IBM i. Remplacez **server.pem** par vios-name.pem.
5. Démarrez le serveur CIMOM exécuté dans la partition VIOS en entrant la commande **startnetsvc cimserver**.
6. Déconnectez-vous de la partition VIOS.
7. Sur le système IBM i, activez la ligne de commande de l'écran vert.
8. Entrez dans l'environnement de shell PASE. Sur la ligne de commande de l'écran vert, entrez **call qp2term**.
9. Pour déplacer le certificat numérique HMC, entrez mv **/vios1.pem /QOpenSys/QIBM/UserData/UME/Pegasus/ssl/truststore/vios1.pem**. Remplacez vios1.pem par le nom de votre fichier.
10. Ajoutez le certificat numérique dans le fichier de clés certifiées. Pour cela, entrez **/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimtrust -a -U QSECOFR -f vios1.pem -T s**. Remplacez le nom vios1.pem par le nom de votre fichier.
11. Quittez le shell PASE en appuyant sur la touche **F3**.
12. Fermez le serveur CIMOM. Sur la ligne de commande de l'écran vert, entrez **ENDTCPSVR *CIMOM**.
13. Redémarrez le serveur CIMOM pour récupérer le nouveau certificat. Sur la ligne de commande de l'écran vert, entrez **STRTCPSVR *CIMOM**.

Configuration des groupes de ressources en grappe

Les groupes de ressources en grappe gèrent des ressources dans un environnement à haute disponibilité i5/OS. Plusieurs tâches permettent la gestion des ressources à haute disponibilité via des groupes de ressources en grappe.

Démarrage d'un groupe de ressources en grappe

Le démarrage d'un groupe de ressources en grappe active la mise en grappe au sein de votre environnement à haute disponibilité i5/OS.

Pour démarrer un groupe de ressources en grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Dans l'onglet **Groupe de ressources en grappe**, sélectionnez le nom du groupe de ressources en grappe à démarrer.
6. Dans le menu **Sélection d'une action**, sélectionnez **Démarrage**. La colonne Etat indique que le groupe de ressources en grappe est démarré.

Information associée

Start Cluster Resource Group (STRCRG) command

Create Cluster Resource Group (QcstCreateClusterResourceGroup) API

Création de groupes de ressources en grappe

Les groupes de ressources en grappe gèrent des ressources à haute disponibilité, telles que des applications, des données et des unités. Chaque type de groupe de ressources en grappe gère le type de ressource particulier à un environnement à haute disponibilité.

L'interface graphique des services-ressources de mise en grappe vous permet de créer des groupes de ressources en grappe différents pour la gestion de vos ressources à haute disponibilité. Chaque type de groupe de ressources en grappe peut être utilisé séparément ou conjointement avec d'autres groupes de ressources en grappe. Par exemple, vous pouvez posséder une application métier autonome qui nécessite une haute disponibilité. Une fois l'application activée pour la haute disponibilité, vous pouvez créer des groupes de ressources en grappe pour gérer la disponibilité de cette application.

Si vous ne voulez qu'une seule application, et que ses données ne soient pas disponibles en cas d'indisponibilité, vous pouvez créer un groupe de ressources en grappe d'application. Cependant, si vous voulez que les données et l'application soient disponibles, vous pouvez les stocker tous les deux dans un pool de stockage sur disque indépendant, que vous pouvez définir dans un groupe de ressources en grappe d'unité. Si une indisponibilité se produit, la totalité du pool de stockage sur disque indépendant est basculée vers un noeud de sauvegarde, ce qui rend disponible l'application et les données.

Création de groupes de ressources en grappe :

Si vous possédez plusieurs applications dans votre solution à haute disponibilité que vous voulez rendre hautement disponible, vous pouvez créer un groupe de ressources en grappe d'application pour gérer les reprises en ligne de cette application.

Vous pouvez indiquer une adresse IP de relais active lors de la création du groupe de ressources en grappe d'application. Quand vous lancez un groupe de ressources d'application, qui autorise une adresse IP de relais active, le groupe de ressources en grappe peut être démarré.

Pour créer un groupe de ressources en grappe d'application, procédez comme suite :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.

3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe de l'application** et cliquez sur **OK**. La page du nouveau groupe de ressources en grappe de l'application apparaît.
7. Dans la page **Général**, spécifiez les informations suivantes relatives au groupe de ressources en grappe de l'application :
   - Dans la zone **Nom**, indiquez le nom du groupe de ressources en grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - Dans la zone **Adresse IP de relais**, indiquez l'adresse IP qui doit être associée au groupe de ressources en grappe de l'application. Cette valeur doit être au format IPv4 ou IPv6. L'adresse IP de relais permet d'accéder à l'application quel que soit le système sur lequel l'application s'exécute. La zone **Configuration de l'adresse IP de relais** détermine si l'utilisateur ou les services-ressources de mise en grappe sont responsables de la création de l'adresse IP.
   - Dans la zone **Description**, saisissez une description du groupe de ressources en grappe. La description ne peut pas dépasser 50 caractères.
   - Sélectionnez **Permettre le redémarrage** et indiquez le nombre de tentatives de redémarrage du groupe de ressources en grappe de l'application. Ces valeurs déterminent le nombre de tentatives de redémarrage de l'application sur le même noeud avant qu'une reprise en ligne vers le noeud de sauvegarde se produise.
   - Dans la zone **Configuration de l'adresse IP de relais**, sélectionnez si vous voulez que les services-ressources de mise en grappe ou un utilisateur configurent et gèrent l'adresse IP de relais de l'application. Les valeurs possibles sont les suivantes :

     Services-ressources de mise en grappe
     Si vous spécifiez cette valeur, l'adresse IP de relais ne doit exister sur aucun noeud du domaine de reprise avant la création du groupe de ressources en grappe. Elle est créée pour vous sur tous les noeuds du domaine de reprise. Si l'adresse IP existe déjà, alors la création du groupe de ressources en grappe d'application échoue.

     Utilisateur
     Si vous indiquez cette valeur, vous devez ajouter l'adresse IP de relais sur tous les noeuds principaux et de sauvegarde du domaine de reprise avant de pouvoir démarrer le groupe de ressources en grappe.
   - Sélectionnez **Permettre une adresse IP de relais active** pour permettre l'activation d'une adresse IP de relais, quand elle est affectée à un groupe de ressources en grappe de l'application. Cette zone est correcte uniquement lorsque la zone Configuration de l'adresse IP de relais est défini sur services-ressources de mise en grappe.
   - Dans la zone **File d'attente utilisateur de distribution d'informations**, indiquez le nom de la file d'attente utilisateur censée recevoir les informations distribuées. Ce nom ne peut pas comporter plus de 10 caractères. Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente utilisateur censée recevoir les informations distribuées. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL. Ce nom ne peut pas comporter plus de 10 caractères.

     Remarque : Si vous ne renseignez pas la file d'attente utilisateur de distribution d'informations, vous devez également laisser la zone Nom de bibliothèque vide, définir le délai d'attente avant reprise en ligne sur 0 et l'action par défaut de reprise en ligne sur 0.
   - Dans la zone **File de messages de reprise en ligne**, indiquez le nom de la file d'attente de messages censée recevoir les messages lorsqu'une reprise en ligne se produit pour ce groupe de ressources en grappe. Si cette zone est définie, la file d'attente de messages spécifiée doit exister sur tous les noeuds du domaine de reprise une fois le programme d'exit terminé. La file d'attente de messages de reprise en ligne ne peut pas faire partie d'un pool de stockage sur disque indépendant.

Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL.

- Dans la zone **Délai d'attente avant reprise en ligne**, indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de la grappe. Les valeurs possibles sont les suivantes :

  Ne pas attendre
  La reprise en ligne se poursuit sans intervention de l'utilisateur.

  Toujours attendre
  La reprise en ligne est systématiquement mise en attente jusqu'à la réception d'une réponse au message de demande de reprise en ligne.

  numéro
  Indiquez le délai d'attente (en minutes) avant l'obtention d'une réponse au message de demande de reprise en ligne. Si une réponse est reçue hors délai, la valeur dans la zone Action par défaut de reprise en ligne indique la procédure à suivre.

- Dans la zone **Action par défaut de reprise en ligne**, indiquez l'action que la mise en grappe doit effectuer lorsqu'une réponse au message relatif à la reprise en ligne sur la file d'attente de messages de grappe a été reçu au-delà du délai d'attente avant reprise en ligne. Vous pouvez définir cette zone sur **Poursuite du basculement** ou sur **Annulation du basculement**.

8. Dans la page **Programme d'exit**, vous pouvez indiquer les informations d'un programme d'exit pour un groupe de ressources en grappe. Les programmes d'exit sont requis pour tous les types de groupes de ressources en grappe à l'exception des groupes de ressources en grappe d'unité. Ils sont appelés après qu'un événement de groupe de ressources en grappe lié à la grappe se produise et réponde à cet événement.
9. Dans la page **Domaine de reprise**, ajoutez des noeuds au domaine de reprise et indiquez leur rôle dans la grappe.

Information associée

Create Cluster Resource Group (CRTCRG) command

Create Cluster Resource Group (QcstCreateClusterResourceGroup) API

Création de groupes de ressources en grappe de données :

Les groupes de ressources en grappe sont principalement utilisés avec des applications de réplication logique, fournies par des partenaires commerciaux à haute disponibilité. Si vous implémentez une solution à haute disponibilité fondée sur réplication logique, vous pouvez créer un groupe de ressources en grappe de données pour soutenir la réplication des données entre les noeuds principaux et les noeuds de sauvegarde.

Pour créer un groupe de ressources en grappe de données, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe de données** et cliquez sur **OK**. La page du nouveau groupe de ressources en grappe de données apparaît.
7. Dans la page **Général**, spécifiez les informations suivantes relatives au groupe de ressources en grappe de données :

- Dans la zone **Nom**, indiquez le nom du groupe de ressources en grappe. Ce nom ne peut pas comporter plus de 10 caractères.
- Dans la zone **Description**, saisissez une description du groupe de ressources en grappe. La description ne peut pas dépasser 50 caractères.
- Dans la zone **File d'attente utilisateur de distribution d'informations**, indiquez le nom de la file d'attente utilisateur censée recevoir les informations distribuées. Ce nom ne peut pas comporter plus de 10 caractères. Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente utilisateur censée recevoir les informations distribuées. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL. Ce nom ne peut pas comporter plus de 10 caractères.

  Remarque : Si vous ne renseignez pas la file d'attente utilisateur de distribution d'informations, vous devez également laisser la zone Nom de bibliothèque vide, définir le délai d'attente avant reprise en ligne sur 0 et l'action par défaut de reprise en ligne sur 0.
- Dans la zone **File de messages de reprise en ligne**, indiquez le nom de la file d'attente de messages censée recevoir les messages lorsqu'une reprise en ligne se produit pour ce groupe de ressources en grappe. Si cette zone est définie, la file d'attente de messages spécifiée doit exister sur tous les noeuds du domaine de reprise une fois le programme d'exit terminé. La file d'attente de messages de reprise en ligne ne peut pas faire partie d'un pool de stockage sur disque indépendant. Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL.
- Dans la zone **Délai d'attente avant reprise en ligne**, indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de la grappe. Les valeurs possibles sont les suivantes :

  Ne pas attendre
  La reprise en ligne se poursuit sans intervention de l'utilisateur.

  Toujours attendre
  La reprise en ligne est systématiquement mise en attente jusqu'à la réception d'une réponse au message de demande de reprise en ligne.

  numéro
  Indiquez le délai d'attente (en minutes) avant l'obtention d'une réponse au message de demande de reprise en ligne. Si une réponse est reçue hors délai, la valeur dans la zone Action par défaut de reprise en ligne indique la procédure à suivre.

8. Dans la page **Programme d'exit**, vous pouvez indiquer les informations d'un programme d'exit pour un groupe de ressources en grappe. Les programmes d'exit sont requis pour tous les types de groupes de ressources en grappe à l'exception des groupes de ressources en grappe d'unité. Ils sont appelés après qu'un événement de groupe de ressources en grappe lié à la grappe se produise et réponde à cet événement.
9. Dans la page **Domaine de reprise**, ajoutez des noeuds au domaine de reprise et indiquez leur rôle dans la grappe.

Information associée

Create Cluster Resource Group (CRTCRG) command

Create Cluster Resource Group (QcstCreateClusterResourceGroup) API

Création de groupes de ressources en grappes d'unité :

Un groupe de ressources en grappe d'unité est constitué d'un groupe de ressources matériel pouvant être commuté en tant qu'entité. Pour créer des unités commutables dans une solution à haute disponibilité, les noeuds qui utilisent ces unités doivent faire partir d'un groupe de ressources en grappe d'unité.

Avant de créer un groupe de ressources en grappe d'unité, ajoutez tous les noeuds qui partageront une ressource commutable à un domaine d'unité.

Pour créer un groupe de ressources en grappe d'unité, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe d'unité** et cliquez sur **OK**. L'assistant **Nouveau groupe de ressources en grappe d'unité** apparaît. La tâche **Nouveau groupe de ressources en grappe d'unité** est disponible uniquement si tous les noeuds du domaine de reprise sont démarrés.
7. Suivez les instructions de l'assistant **Nouveau groupe de ressources en grappe d'unité** pour créer un nouveau groupe de ressources en grappe d'unité. Pendant l'exécution de cet assistant, vous pouvez créer un nouveau groupe de ressources en grappe d'unité. Vous pouvez également créer un nouveau pool de stockage sur disque indépendant ou en spécifier un existant.

   Le groupe de ressources en grappe d'unité conserve les informations de ressource matériel sur l'ensemble des noeuds du domaine de reprise et vérifie que les noms de ressource sont identiques. Vous pouvez également configurer un domaine d'administration de grappe pour conserver les attributs inscrits des objets de configuration, lesquels peuvent inclure des noms de ressource, identiques sur l'ensemble du domaine d'administration. Si vous utilisez la protection par disque miroir d'un site à l'autre, créez des groupes de ressources de grappe d'unité séparés pour les pools de stockage sur disque indépendant et les autres types d'unité commutable sur chaque site.

Information associée

Create Cluster Resource Group (CRTCRG) command

Create Cluster Resource Group (QcstCreateClusterResourceGroup) API

Création de groupes de ressources en grappe homologues :

Vous pouvez créer un groupe de ressources en grappe homologue pour définir des rôles de noeud dans des environnements à équilibrage de charge.

Pour créer un groupe de ressources en grappe homologue, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action**.
6. Sélectionnez **Nouveau groupe de ressources en grappe homologue** et cliquez sur **OK**. La page Nouveau groupe de ressources en grappe homologue apparaît.
7. Dans la page **Général**, spécifiez les informations suivantes relatives au groupe de ressources en grappe homologue :
   - Dans la zone **Nom**, indiquez le nom du groupe de ressources en grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - Dans la zone **Description**, saisissez une description du groupe de ressources en grappe. La description ne peut pas dépasser 50 caractères.

- Dans la zone **ID application**, indiquez l'identificateur d'application des groupes de ressources en grappe homologues au format *[NomFournisseur].[NomApplication]*. Par exemple, MonEntreprise.MonApplication. L'identificateur ne peut pas dépasser 50 caractères.

8. Dans la page **Programme d'exit**, vous pouvez indiquer les informations d'un programme d'exit pour un groupe de ressources en grappe. Les programmes d'exit sont requis pour tous les types de groupes de ressources en grappe à l'exception des groupes de ressources en grappe d'unité. Ils sont appelés après qu'un événement de groupe de ressources en grappe lié à la grappe se produise et réponde à cet événement.
9. Dans la page **Domaine de reprise**, ajoutez des noeuds au domaine de reprise et indiquez leur rôle dans la grappe.

Information associée

Create Cluster Resource Group (CRTCRG) command

Create Cluster Resource Group (QcstCreateClusterResourceGroup) API

Configuration des domaines d'administration en grappe

Dans un environnement à haute disponibilité, l'application et l'environnement d'exploitation doivent rester cohérents entre les noeuds qui participent à la haute disponibilité. Le domaine d'administration en grappe est l'implémentation i5/OS des tests de résistance de l'environnement et il garantit la cohérence de l'environnement d'exploitation dans les noeuds.

Création d'un domaine d'administration de grappe

Dans une solution à haute disponibilité, le domaine d'administration de grappe fournit le mécanisme qui garde les ressources synchronisées dans les systèmes et les partitions d'une grappe.

Pour créer le domaine d'administration de grappe, un utilisateur doit posséder des droits *IOSYSCFG et des droits d'accès au profil utilisateur QCLUSTER. Pour gérer un domaine d'administration de grappe, un utilisateur doit être autorisé à accéder au groupe de ressources en grappe qui représente le domaine d'administration de grappe, le profil utilisateur QCLUSTER et les commandes du groupes de resssources en grappe.

Pour créer un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page des services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour répertorier les domaines d'administration de la grappe. Si aucun domaine d'administration de grappe n'a été configuré, cette liste sera vide.
5. Dans l'onglet **Domaine d'administration**, sélectionnez **Nouveau domaine d'administration**.
6. Dans la page Nouveau domaine d'administration, spécifiez les informations suivantes relatives au domaine d'administration de grappe :
   - Dans la zone **Nom**, saisissez le nom du domaine d'administration de grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - La zone **Grappe** affiche le nom de la grappe. Vous ne pouvez pas modifier la valeur de cette zone.
   - Dans la zone **Option de synchronisation**, spécifiez le comportement de synchronisation quand un noeud rejoint un domaine d'administration d'une grappe. Cette zone est activée seulement si la grappe est de version 6 ou ultérieure. Les valeurs possibles sont les suivantes :

     Option de dernière modification (par défaut)
     Sélectionnez cette option si toutes les modifications apportées aux ressources contrôlées

doivent être appliquées à un domaine d'administration de grappe. La modification la plus récente apportée à une ressource contrôlée est appliquée à cette ressource sur tous les noeuds actifs.

Option de domaine actif
Sélectionnez cette option si seules les modifications apportées aux ressources contrôlées sont autorisées à partir des noeuds actifs. Les modifications apportées aux ressources contrôlées sur les noeuds inactifs sont éliminées lorsque le noeud rejoint le domaine d'administration de la grappe. L'option Domaine actif ne s'applique pas aux espaces de stockage des serveurs de réseau (*NWSSTG) ou aux configurations de serveurs de réseau (*NWSCFG). La synchronisation de ces ressources est toujours effectuée en fonction de la dernière modification apportée.

- Dans la liste **Noeuds du domaine d'administration**, sélectionnez les noeuds que vous aimeriez ajouter au domaine d'administration de grappe et cliquez sur **Ajouter**.

Concepts associés

«Gestion des profils utilisateur sur tous les noeuds», à la page 82
Vous pouvez utiliser deux mécanismes pour gérer des profils utilisateurs sur tous les noeuds d'une grappe.

Information associée

Create Cluster Administrative Domain (CRTCAD) command

Create Cluster Administrative Domain (QcstCrtClusterAdminDomain) API

Ajout d'un noeud au domaine d'administration de grappe

Vous pouvez ajouter des noeuds supplémentaires à un domaine administratif de grappe au sein d'une solution à haute disponibilité.

Avant d'ajouter un noeud à un domaine d'administration de grappe, assurez-vous que le noeud fait également partie de la grappe dans laquelle se trouve le domaine d'administration de grappe. Si tel n'est pas le cas, vous ne pouvez pas ajouter le noeud au domaine d'administration de grappe. Ce dernier n'a pas à être actif, mais les ressources ne seront pas mises en cohérence tant qu'il ne sera pas activé.

Quand vous ajoutez un noeud au domaine d'administration, les postes de ressource contrôlée du domaine sont copiés dans le noeud ajouté. Si la ressource contrôlée n'existe pas dans le nouveau noeud, elle est créée par le domaine d'administration de grappe. Si elle existe déjà dans le noeud ajouté, elle sera synchronisée avec le reste du domaine d'administration de grappe si le domaine est actif. Par conséquent, les valeurs des attributs de chaque ressource contrôlée du noeud en cours de connexion sont modifiées afin de correspondre aux valeurs globales des ressources contrôlées du domaine actif.

Pour ajouter un noeud à un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
5. Dans la page Domaines d'administration, sélectionnez un domaine d'administration de grappe.
6. Dans le menu **Sélection d'une action**, sélectionnez **Propriétés**.
7. Dans la page **Propriétés**, sélectionnez le noeud que vous voulez ajouter au domaine d'administration de grappe à partir de la liste **Noeuds du domaine d'administration**. Cliquez sur **Ajouter**.

Information associée

Add Cluster Administrative Domain Node Entry (ADDCADNODE) command

Add Node To Recovery Domain (QcstAddNodeToRcvyDomain) API

Démarrage d'un domaine d'administration de grappe

Les domaines d'administration de grappe fournissent un test de résistance d'environnement aux ressources d'une solution à haute disponibilité i5/OS.

Au démarrage du domaine d'administration de grappe, toute modification apportée aux ressources contrôlées alors que le domaine d'administration de grappe était en cours d'arrêt est propagée à tous les noeuds actifs du domaine.

Pour démarrer un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-Ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de la grappe.
5. Dans la page Domaines d'administration, sélectionnez un domaine d'administration de grappe.
6. Sélectionnez **Démarrage** dans le menu **Sélection d'une action**.

La colonne Status affiche que le domaine d'administration de grappe est démarré.

Concepts associés

«Synchronisation d'une ressource contrôlée»
La synchronisation des ressources contrôlées se produit en cas de modification des ressources contrôlées sur les noeuds qui ont été définis dans le domaine d'administration de la grappe.

Information associée

Start Cluster Administrative Domain (STRCAD) command

Synchronisation d'une ressource contrôlée

La synchronisation des ressources contrôlées se produit en cas de modification des ressources contrôlées sur les noeuds qui ont été définis dans le domaine d'administration de la grappe.

Au cours de ce processus de synchronisation, le domaine d'administration de la grappe tente de modifier chaque ressource avec des attributs dont les valeurs ne correspondent pas à ses valeurs globales, sauf en cas de modification en attente pour cette ressource. Toute modification en attente est répartie sur tous les noeuds actifs du domaine et appliquée à chaque ressource affectée sur chaque noeud. Lors de la distribution des modifications en attente, la valeur globale est modifiée et l'état global de chaque ressource affectée devient *Cohérent* ou *Incohérent*, suivant le résultat de l'opération de modification pour la ressource sur chaque noeud. Si la ressource affectée est modifiée avec succès sur chaque noeud du domaine, l'état global de cette ressource est *Cohérent*. Si l'opération de modification échoue sur un des noeuds, l'état global est défini sur *Incohérent*.

Si des modifications sont apportées à la même ressource à partir de plusieurs noeuds pendant que le domaine d'administration de la grappe est inactif, toutes ces modifications sont propagées sur tous les noeuds actifs, dans le cadre du processus de synchronisation au démarrage du domaine. Même si toutes les modifications en attente sont traitées lors de l'activation du domaine d'administration de la grappe, l'ordre de traitement des modifications n'est pas garanti. Si vous apportez des modifications à une ressource à partir de plusieurs noeuds de la grappe alors que les domaines d'administration de la grappe sont inactifs, l'ordre de traitement des modifications pendant l'activation n'est pas garanti.

Si un noeud est rattaché à un domaine d'administration de grappe inactif (le noeud est démarré pendant que le domaine est arrêté), les ressources contrôlées ne seront synchronisées qu'au démarrage du domaine d'administration de grappe.

Remarque : Le domaine d'administration de la grappe et son programme d'exit associé sont des objets fournis par IBM. Ne les modifiez pas avec l'API QcstChangeClusterResourceGroup ni avec la commande CHGCRG (Modif. groupe ressource grappe), sous peine d'obtenir des résultats imprévisibles.

Après la fin d'un noeud de grappe faisant partie d'un domaine d'administration de la grappe, il est toujours possible de modifier les ressources contrôlées sur le noeud inactif. Au redémarrage du noeud, les modifications seront resynchronisées par rapport au reste du domaine. Lors du processus de resynchronisation, le domaine d'administration de la grappe applique toute modification éventuelle provenant du noeud qui était inactif aux autres noeuds actifs du domaine, sauf si des modifications ont également été apportées dans le domaine actif pendant l'inactivité du noeud. En cas de modifications apportées à une ressource contrôlée à la fois dans le domaine actif et sur le noeud inactif, les modifications apportées au domaine actif sont appliquées au noeud associé. Autrement dit, aucune modification apportée à une ressource contrôlée n'est perdue, quel que soit l'état du noeud. Vous pouvez spécifier l'option de synchronisation pour contrôler le comportement de la synchronisation.

Si vous voulez mettre fin à un noeud de grappe faisant partie d'un domaine d'administration de la grappe sans autoriser que les modifications apportées au noeud inactif soient propagées au domaine actif au démarrage du noeud (par exemple, lors de l'arrêt du noeud de la grappe pour y effectuer des tests), vous devez préalablement supprimer le noeud du groupe de ressources en grappe homologue du domaine d'administration.

Concepts associés

Remove Admin Domain Node Entry (RMVCADNODE) command

Tâches associées

«Démarrage d'un domaine d'administration de grappe», à la page 119
Les domaines d'administration de grappe fournissent un test de résistance d'environnement aux ressources d'une solution à haute disponibilité i5/OS.

Information associée

Remove CRG Node Entry (RMVCRGNODE) command

Ajout de postes de ressource contrôlée

Vous pouvez ajouter un poste de ressource contrôlée à un domaine d'administration de grappe. Les postes de ressource contrôlée définissent des ressources critiques de sorte que les modifications apportées à ces ressources restent cohérentes dans un environnement à haute disponibilité.

Pour ajouter un poste de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
4. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
5. Dans la liste des types de ressource contrôlée, cliquez sur l'icône contextuelle en regard du type de ressource contrôlée, puis sur **Ajout d'un poste de ressource contrôlée**. La page Ajout d'un poste de ressource contrôlée apparaît.

6. Sélectionnez les attributs à contrôler pour le poste de ressource contrôlée, puis cliquez sur **OK**. Si l'objet de poste de ressource contrôlée est une bibliothèque, précisez-en le nom et la bibliothèque. Le nouveau poste de ressource contrôlée est ajouté à la liste des ressources contrôlées par le domaine d'administration de grappe. Les modifications apportées à la ressource contrôlée sont synchronisées sur l'ensemble des noeuds actifs du domaine d'administration de grappe lorsque celui-ci est actif. Par défaut, tous les attributs associés à un type de ressource contrôlée sont contrôlés ; cependant, vous pouvez déterminer les attributs que vous devez contrôler en les sélectionnant.

Tâches associées

«Sélection des attributs à contrôler», à la page 165
Après avoir ajouté des entrées de ressources contrôlées, vous pouvez sélectionner des attributs associés à ces ressources et que le domaine d'administration de grappe doit contrôler.

Information associée

Add Admin Domain MRE (ADDCADMRE) command

Add Monitored Resource Entry (QfpadAddMonitoredResourceEntry) API

Ajout de postes de ressource contrôlée

Vous pouvez ajouter un poste de ressource contrôlée à un domaine d'administration de grappe. Les postes de ressource contrôlée définissent des ressources critiques de sorte que les modifications apportées à ces ressources restent cohérentes dans un environnement à haute disponibilité.

Pour ajouter un poste de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
4. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
5. Dans la liste des types de ressource contrôlée, cliquez sur l'icône contextuelle en regard du type de ressource contrôlée, puis sur **Ajout d'un poste de ressource contrôlée**. La page Ajout d'un poste de ressource contrôlée apparaît.
6. Sélectionnez les attributs à contrôler pour le poste de ressource contrôlée, puis cliquez sur **OK**. Si l'objet de poste de ressource contrôlée est une bibliothèque, précisez-en le nom et la bibliothèque. Le nouveau poste de ressource contrôlée est ajouté à la liste des ressources contrôlées par le domaine d'administration de grappe. Les modifications apportées à la ressource contrôlée sont synchronisées sur l'ensemble des noeuds actifs du domaine d'administration de grappe lorsque celui-ci est actif. Par défaut, tous les attributs associés à un type de ressource contrôlée sont contrôlés ; cependant, vous pouvez déterminer les attributs que vous devez contrôler en les sélectionnant.

Tâches associées

«Sélection des attributs à contrôler», à la page 165
Après avoir ajouté des entrées de ressources contrôlées, vous pouvez sélectionner des attributs associés à ces ressources et que le domaine d'administration de grappe doit contrôler.

Information associée

Add Admin Domain MRE (ADDCADMRE) command

Add Monitored Resource Entry (QfpadAddMonitoredResourceEntry) API

Configuration des disques commutés

Les disques commutés sont des pools de stockage sur disque indépendant qui ont été configurés dans le cadre d'une grappe i5/OS. Ils permettent aux données et aux applications stockées dans un pool de stockage sur disque indépendant d'être basculées sur un autre système.

Création d'un pool de stockage sur disque indépendant

Pour créer un pool de stockage sur disque indépendant, vous pouvez utiliser l'assistant Nouveau pool de stockage sur disque. Cet assistant peut vous aider à créer un nouveau pool de stockage sur disque et à y ajouter des unités de disque.

Grâce à l'assistant Nouveau Pool de stockage sur disque, vous pouvez inclure des unités de disque non configurées dans un jeu d'unités à contrôle de parité intégré, et vous pouvez démarrer une protection par contrôle de parité intégré, ainsi qu'une compression de disque. A mesure que vous ajoutez des unités de disque, ne propagez pas des unités de disque qui se trouvent dans le même jeu d'unités à contrôle de parité intégré sur plusieurs pools de stockage sur disques, car si une erreur se produit dans un jeu d'unités à contrôle de parité intégré, cela affectera plusieurs pools de stockage sur disque.

Utilisez l'assistant Nouveau pool de stockage sur disque pour créer un pool de stockage sur disque indépendant à l'aide d'IBM Systems Director Navigator for i5/OS et procédez comme suit :

Remarque : pour utiliser un disque dans IBM Systems Director Navigator for i5/OS, vous devez posséder la bonne configuration de mot de passe pour les outils de maintenance en mode dédié.

IBM Systems Director Navigator for i5/OS

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans votre fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Unités de disque**.
5. Dans le menu **Sélection d'une action**, sélectionnez **Nouveau pool de stockage sur disque**.
6. Suivez les instructions de l'assistant pour ajouter des unités de disque au nouveau pool de stockage.
7. Imprimez votre configuration de disque pour pouvoir la consulter en cas de situation de reprise.
8. Enregistrez la relation entre le nom et le numéro du pool de stockage sur disque indépendant.

System i Navigator

Pour utiliser l'assistant Nouveau pool de stockage sur disque afin de créer un pool de stockage sur disque indépendant à l'aide d'System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence de **Mes connexions** (ou votre environnement actif).
2. Développez le système que vous voulez examiner, ainsi que **Configuration et maintenance** → **Matériel** → **Unités de disques**.

3. Cliquez avec le bouton droit de la souris sur **Pools de stockage sur disque** et sélectionnez **Nouveau pool de stockage sur disque**.
4. Suivez les instructions de l'assistant pour ajouter des unités de disque au nouveau pool de stockage.
5. Imprimez votre configuration de disque pour pouvoir la consulter en cas de situation de reprise.
6. Enregistrez la relation entre le nom et le numéro du pool de stockage sur disque indépendant.

Remarque : Ajoutez des pools de stockage sur disque indépendant une fois que votre système est entièrement redémarré. Si vous devez utiliser l'assistant Nouveau pool de stockage sur disque dans les outils de maintenance en mode dédiée, vous devez créer une description d'unité associée pour le pool de stockage sur disque indépendant une fois le système entièrement redémarré. Utilisez la commande Création d'une description d'unité (ASP) (CRTDEVASP) pour créer la description d'unité. Nommez la description d'unité et le nom de ressource de la même façon que le pool de stockage indépendant. Vous pouvez utiliser la commande WRKDEVD (Utilisation des descriptions d'unité) pour vérifier que la description d'unité et le nom du pool de stockage sur disque indépendant correspondent.

Démarrage de la protection par disque miroir

Les assistants Ajout d'une unité de disques et Nouveau pool de stockage sur disque vous aident à ajouter des paires d'unités de disques de capacité semblable à un pool de stockage sur disque protégé. Lorsque vos disques sont correctement configurés, vous pouvez démarrer la protection par disque miroir.

La protection par disque miroir est locale par rapport à un système et se distingue de la protection d'un site à l'autre. Si vous souhaitez démarrer la protection par disque miroir sur un pool de stockage sur disque indépendant à l'état Non disponible (hors fonction), vous pouvez le faire lors d'un redémarrage complet du système. Pour tous les autres pools de stockage sur disque, vous devez d'abord redémarrer votre système en mode DST (outils de maintenance en mode dédié).

Il existe des restrictions lorsque vous démarrez la protection par copie miroir sur l'unité de disque source du chargement.

- Le disque ayant la plus petite capacité doit démarrer en tant qu'unité source du chargement quand deux disques de capacités inégales sont associés en tant que paire miroir. La source de chargement peut ensuite être associée à l'unité de disque ayant la plus grande capacité. Par exemple, si l'unité de disque source du chargement est un disque de 35 giga-octets, elle peut être associée à un disque de 36 giga-octets. si l'unité de disque source du chargement est un disque de 36 giga-octets, elle ne peut pas être associée à un disque de 35 giga-octets.
- Le système doit être configuré pour associer l'unité de disque source du chargement à une unité de disque située à un emplacement physique que le processeur de service ne pourra pas utiliser pour amorcer (IPL) la partition. Dans SST, sélectionnez **Gestion des unités de disque->Gestion de la configuration de disque->Activer la copie miroir des sources de chargement distantes**. La fonction **Activer la copie miroir des sources de chargement distantes** permet d'associer un unité de disque avec l'unité de disque source de chargement même quand l'unité de disque réside dans un emplacement physique que le processeur de service ne peut pas utiliser pour amorcer la partition.

Pour démarrer la protection par disque miroir avec IBM Systems Director Navigator for i, procédez comme suit :

1. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
2. Sélectionnez **Pools de stockage sur disque**.
3. Sélectionnez le pool de stockage sur disque auquel appliquer la protection.
4. Dans le menu **Sélection d'une action**, sélectionnez **Démarrage de la protection par disque miroir**.

Pour démarrer la protection par disque miroir avec System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).

2. Développez le System i que vous voulez examiner, **Configuration et maintenance** → **Matériel** → **Unités de disques** → **Pools de stockage sur disque**.
3. Cliquez avec le bouton droit de la souris sur ces pools de stockage sur disque et sélectionnez **Démarrage de la protection par disque miroir**.

Arrêt de la protection par disque miroir

Quand vous arrêtez la protection par disque miroir, une unité de disque de chaque paire protégée par disque miroir est configurée. Avant d'arrêter une protection par disque miroir pour un pool de stockage sur disque, au moins une unité de disque de chaque paire protégée par disque miroir de ce pool de stockage sur disque doit être présente et activée.

Pour contrôler l'annulation de la configuration des unités de disque protégée par disque miroir de chaque paire, vous pouvez suspendre les unités de disque pour lesquelles vous voulez annuler la configuration. Pour les unités de disque qui ne sont pas suspendus, la sélection est automatique.

Si vous voulez arrêter la protection par disque miroir sur un pool de stockage sur disque indépendant qui n'est pas disponible, vous pouvez y parvenir quand votre système est entièrement redémarré. Pour tous les autres pools de stockage sur disque, vous devez redémarrer votre système via les outils de maintenance en mode dédié avant d'arrêter la protection par disque miroir.

La protection par disque miroir est dédiée à un système unique, et est différente de la protection par disque miroir d'un site à l'autre.

Pour arrêter la protection par disque miroir à l'aide d'IBM Systems Director Navigator for i5/OS, procédez comme suit :

1. Sélectionnez **Configuration et maintenance** dans votre fenêtre IBM Systems Director Navigator for i5/OS.
2. Sélectionnez **Pools de stockage sur disque**.
3. Sélectionnez le pool de stockage sur disque que vous voulez arrêter.
4. Dans le menu **Sélection d'une action**, sélectionnez **Arrêt de la protection par disque miroir**.

Pour arrêter la protection par disque miroir à l'aide d'System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence de **Mes connexions** (ou votre environnement actif).
2. Développez le System i que vous voulez examiner, **Configuration et maintenance** → **Matériel** → **Unités de disques** → **Pools de stockage sur disque**.
3. Sélectionnez l'unité de disque pour laquelle vous voulez arrêter la protection par disque miroir.
4. Cliquez avec le bouton droit sur un pool de stockage sur disque sélectionné et sélectionnez **Arrêt de la protection par disque miroir**.
5. Cliquez sur **Arrêt de la protection par disque miroir** dans la boîte de dialogue de confirmation qui s'affiche.

Ajout d'une unité de disques ou d'un pool de stockage sur disque

L'assistant Ajout d'unité de disques vous permet d'utiliser un pool de stockage sur disque existant afin d'ajouter de nouvelles unités de disques non configurées.

Les assistants Ajout d'unité de disques et Pool de stockage sur disque vous font gagner du temps en regroupant plusieurs fonctions de configuration fastidieuses en un même processus efficace. Ils permettent aussi de bien cerner la configuration des unités de disques en analysant les fonctions de votre système et en offrant uniquement des choix valides. Par exemple, l'assistant ne propose pas l'option de démarrage de la compression tant que votre système ne possède pas cette fonction.

Lorsque vous choisissez d'ajouter des unités de disques à un pool de stockage sur disque protégé, l'assistant vous oblige à les inclure dans la protection par contrôle de parité intégré ou à ajouter suffisamment d'unités de la même capacité pour lancer la protection par disque miroir. L'assistant vous permet aussi d'équilibrer les données dans le pool de stockage sur disque ou de lancer la compression du disque si ces actions sont autorisées pour votre configuration système. Vous choisissez les options à appliquer afin d'adapter l'opération à votre système.

Pour ajouter une unité de disques ou un pool de stockage sur disque avec IBM Systems Director Navigator for i5/OS, procédez comme suit :

1. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
2. Cliquez sur **Unités de disques**.
3. Dans le menu **Sélection d'une action**, sélectionnez **Ajout d'unité de disques**.
4. Suivez les instructions de l'assistant pour ajouter des unités de disques au pool de stockage sur disque.

Pour ajouter une unité de disques ou un pool de stockage sur disque avec System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez **Mes connexions** (ou votre environnement actif).
2. Développez le System i à analyser, puis **Configuration et maintenance** → **Matériel** → **Unités de disques**.
3. Pour ajouter des unités de disque, cliquez avec le bouton droit sur **Toutes les unités de disques** et sélectionnez **Toutes les unités de disques**.
4. Suivez les instructions dans l'assistant pour terminer cette tâche.

Evaluation de la configuration en cours

Avant de modifier la configuration du disque de votre système, il est important de savoir exactement où les unités de disques existantes se trouvent par rapport aux pools de stockage sur disque, aux adaptateurs d'entrée-sortie et aux armoires.

L'affichage graphique de System i Navigator élimine la compilation de toutes ces informations en offrant une représentation graphique de la configuration de votre système. Vous pouvez vous servir de cet affichage graphique pour exécuter toutes les fonctions possibles via la vue de liste Unités de disques de System i Navigator, avec comme avantage de disposer d'une représentation visuelle. Si vous cliquez avec le bouton droit sur un objet dans le tableau, tel qu'une unité de disques spécifique, un pool de stockage sur disque, un jeu d'unités à contrôle de parité intégré ou une armoire, vous voyez les mêmes options que dans la fenêtre principale de System i Navigator.

Vous pouvez choisir de voir le matériel dans la fenêtre d'affichage graphique de l'unité de disques. Par exemple, vous pouvez choisir un affichage selon les pools de stockage sur disque, puis, dans la liste obtenue, sélectionner un pool et n'afficher que les armoires contenant les unités de disques qui le constituent. Vous pouvez sélectionner Affichage de toutes les armoires pour voir si les armoires, contiennent ou non des unités de disque dans le pool de stockage sur disque sélectionné. Vous pouvez également sélectionner Affichage de tous les emplacements d'unité pour associer des noms d'unités de disques à l'emplacement où ces unités sont insérées.

Vous pouvez cliquer avec le bouton droit sur une unité de disques mise en évidence en bleu dans l'affichage graphique, puis sélectionner une action à réaliser sur cette unité. Par exemple, vous pouvez choisir de démarrer ou d'arrêter la compression d'une unité de disques, d'inclure ou d'exclure l'unité de disques d'un jeu d'unités à contrôle de parité intégré ou de renommer l'unité de disques. Si l'unité de disques est protégée par disque miroir, vous pouvez interrompre ou reprendre cette protection. Si vous cliquez avec le bouton droit sur un emplacement vide d'unité de disques, vous pouvez lancer l'assistant Installation d'une unité de disques.

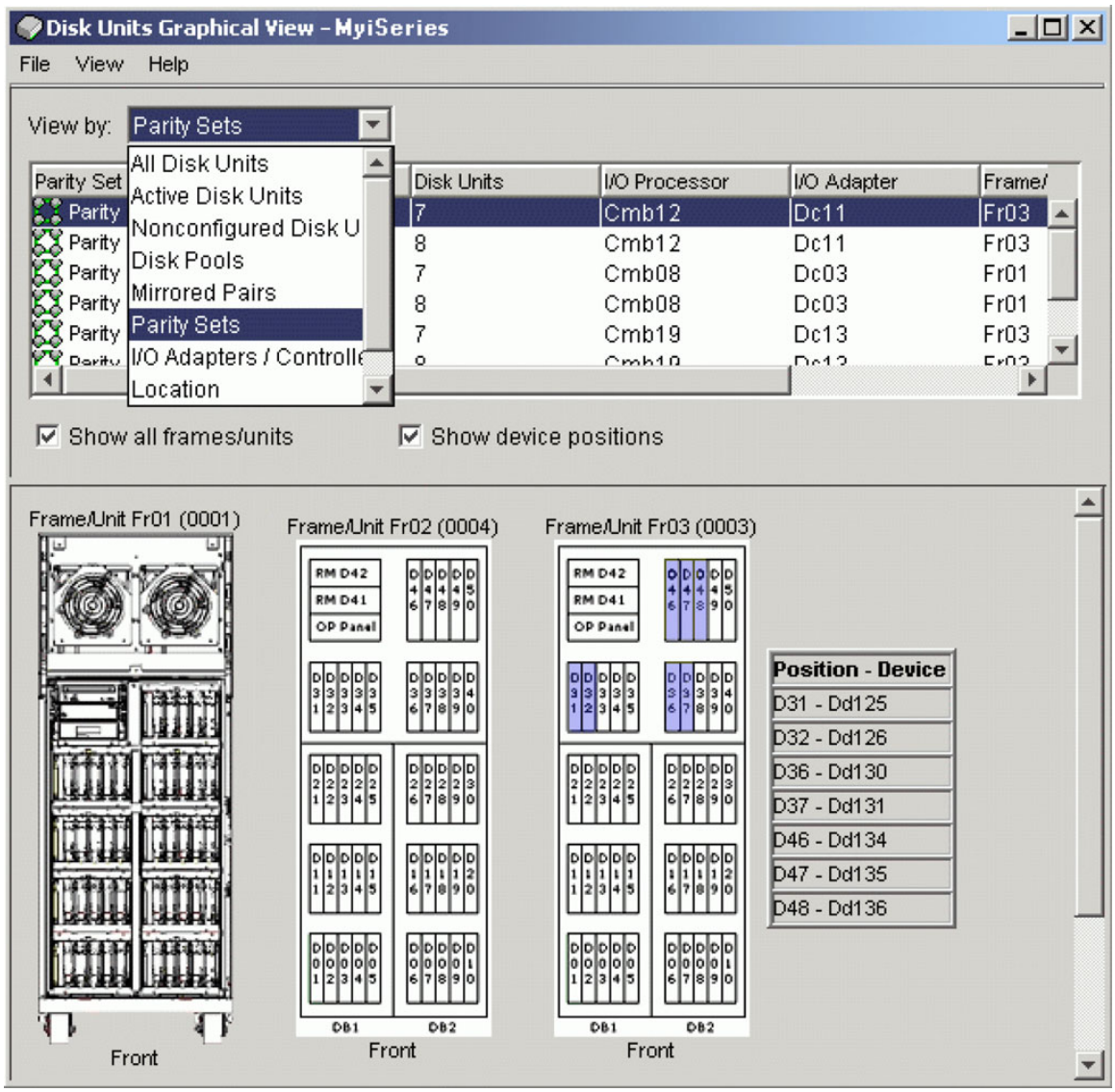
Pour activer l'affichage graphique des unités de disque depuis System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez le système que vous voulez examiner, sélectionnez **Configuration et maintenance** → **Matériel** → **Unités de disques**.
3. Cliquez avec le bouton droit sur **Toutes les unités de disque** et sélectionnez **Affichage graphique**.

Pour activer l'affichage graphique des unités de disque depuis IBM Systems Director Navigator for i, procédez comme suit :

1. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
2. Sélectionnez **Unités de disque** ou **Pools de stockage sur disque**.
3. Dans le menu **Sélection d'une action**, sélectionnez **Affichage graphique**.

Ci-après un exemple de l'affichage graphique des unités de disques dans System i Navigator. Le menu Affichage par répertorie plusieurs options pour l'affichage des unités de disques.



Mise en fonction d'un pool de stockage sur disque

Pour accéder aux unités de disque dans un pool de stockage sur disque indépendant, vous devez rendre disponible le pool de stockage su disque (le mettre en fonction).

Pour accéder aux unités de disque dans un pool de stockage sur disque indépendant et aux objets de la base de données correspondante, vous devez rendre le pool de stockage su disque disponible (le mettre en fonction). Si vous utilisez la protection géographique par disque miroir, vous devez créer la copie de production du pool de stockage sur disque disponible. La copie miroir peut uniquement être disponible quand elle est déconnectée. Pour un pool de stockage sur disque protégé géographiquement par disque miroir, vous devez également vous assurer que le groupe de matériel commutable a été démarré avant d'essayer de rendre disponible le pool de stockage sur disque sauf si la protection géographique par disque miroir est suspendue.

Dans un environnement multisystème mis en grappe, vous pouvez rendre le pool de stockage sur disque indépendant pour le noeud en cours ou pour l'autre noeud de la grappe. Le pool de stockage sur disque indépendant peut uniquement être mis en fonction pour un noeud à la fois. Quand vous voulez accéder à un pool de stockage sur disque indépendant, vous devez basculer le pool de stockage sur disque indépendant vers le noeud de la grappe de sauvegarde. Consultez Réalisation d'un basculement pour obtenir des détails sur le basculement d'un groupe de ressources en grappe d'unité (également appelé groupe matériel commutable dans System i Navigator) vers le noeud de sauvegarde.

Remarque : Si vous rendez disponible un pool de stockage sur disque principal ou secondaire, tous les pools de stockage sur disque du groupe de pools de stockage sur disque seront également disponibles au même moment.

Quand vous rendez disponible un pool de stockage sur disque ou réalisez des modifications de configuration de disque sur un pool de stockage sur disque indépendant, le traitement peut sembler s'arrêter. Si vous effectuez d'autres activités de description d'activité, rendez disponible et les modifications de la configuration des disques attendra.

Des échecs apparaissant au début du traitement de mise en fonction d'un pool de stockage sur disque protégé géographiquement par disque miroir peuvent provoquer une synchronisation complète lors de la prochaine mise en fonction ou reprise.

Pour rendre disponible un pool de stockage sur disque indépendant :

1. Dans System i Navigator, développez l'arborescence de **Mes connexions** (ou votre environnement actif).
2. Développez le système que vous voulez examiner, **Configuration et maintenance** → **Matériel** → **Unités de disques**.
3. Développez **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit sur le pool de stockage sur disque non disponible et sélectionnez **Mise en fonction**. Vous pouvez sélectionner plusieurs pools de stockage sur disque pour le rendre disponible en même temps.
5. Dans la boîte de dialogue affichée, cliquez sur **Mise en fonction** pour rendre disponible le pool de stockage sur disque.

Vous pouvez utilisez la commande VRYCFG (Changer l'état d'une configuration) dans l'interface en mode texte pour rendre disponible le pool de stockage sur disque.

Utilisez la commande DSPASPSTS (Afficher l'état ASP) pour identifier l'état d'avancement d'une étape dans le processus.

Configuration de la protection par disque miroir d'un site à l'autre

La protection par disque miroir d'un site à l'autre est un terme collectif utilisé pour décrire plusieurs technologies à haute disponibilité différentes, y compris la protection géographique par disque miroir, Metro Mirror et Global Mirror. Chacune de ces technologies possède des tâches de configuration spécifiques.

Configuration de la protection géographique par disque miroir

La *protection géographique par disque miroir* est une sous-fonction de la protection par disque miroir d'un site à l'autre. Pour configurer une solution à haute disponibilité à l'aide de la protection géographique par disque miroir,vous devez configurer une session de protection par disque miroir entre le système de production et le système sauvegarde.

Avant de configurer la protection géographique par disque miroir, vous devez disposer d'une grappe, de noeuds et d'un groupe de ressources en grappe actifs. Les pools de stockage sur disque indépendant que vous comptez utiliser pour la protection géographique par disque miroir doivent être mis hors fonction (indisponibles) pour compléter la configuration. La rubrique intitulée Scénario : protection par disque miroir d'un site site à l'autre avec protection géographique par disque miroir fournit des instructions détaillées pour la configuration d'une solution à haute disponibilité basée sur la protection géographique par disque miroir.

IBM Systems Director Navigator for i

Pour configurer la protection géographique par disque miroir à l'aide d'IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque que vous voulez utiliser comme copie (source) de production.
6. Dans le menu **Sélection d'une action**, sélectionnez **Nouvelle session**.
7. Suivez les instructions de l'assistant pour compléter la tâche.

System i Navigator

Pour configurer la protection géographique par disque miroir à l'aide de System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence de **Mes connexions** (ou votre environnement actif).
2. Développez le système que vous voulez utiliser comme copie de production.
3. Développez **Configuration et maintenance** → **Matériel** → **Unités de disque** → **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit de la souris sur le pool de stockage sur disque que vous voulez utiliser comme copie de production et sélectionnez **Sessions** → **Nouveau**.
5. Suivez les instructions de l'assistant pour compléter la tâche.

Concepts associés

«Scénario : Disque commuté avec protection géographique par disque miroir», à la page 88
Ce scénario décrit une solution à haute disponibilité i5/OS qui utilise des disques commutés dans une grappe à trois noeuds. Cette solution fournit la reprise après incident et la haute disponibilité.

Configuration d'une session Metro Mirror

Pour les solutions à haute disponibilité i5/OS qui utilisent la technologie Metro Mirror IBM System Storage, vous devez configurer une session entre la machine System i et les unités de stockage externe IBM System Storage pour lesquelles la fonction Metro Mirror est configurée. Dans i5/OS, les sessions Metro Mirror ne configurent pas la protection par disque miroir sur des unités de stockage externe, au lieu de cela elles configurent une relation entre les systèmes i5/OS et la configuration Metro Mirror existante sur des unités de stockage externes.

Avant de créer une session Metro Mirror sur i5/OS, vous devez configurer Metro Mirror sur les unités de stockage externes IBM System Storage. Pour plus d'informations sur l'utilisation de Global Mirror sur IBM System Storage DS8000, voir IBM System Storage DS8000 Information Center.

Pour configurer la session Metro Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque que vous voulez utiliser comme copie (source) de production.
6. Dans le menu **Sélection d'une action**, sélectionnez **Nouvelle session**.
7. Suivez les instructions de l'assistant pour compléter la tâche.

Information associée

Add ASP Copy Description (ADDASPCPYD) command

Start ASP Session (STRASPSSN) command

Configuration de la session Global Mirror

Pour les solutions à haute disponibilité i5/OS qui utilisent la technologie Global Mirror IBM System Storage, vous devez configurer une session entre la machine System i et les unités de stockage externe IBM System Storage pour lesquelles la fonction Global Mirror est configurée. Dans i5/OS, les sessions Global Mirror ne configurent pas la protection par disque miroir sur des unités de stockage externe, au lieu de cela elles configurent une relation entre les systèmes i5/OS et la configuration Global Mirror existante sur des unités de stockage externe.

La technologie Global Mirror d'IBM System Storage impose que tous les utilisateurs partagent une connexion Global Mirror. La fonction Global Mirror à haute disponibilité i5/OS n'autorise qu'une seule partition System i pour configurer Global Mirror sur un serveur System Storage donné. Aucune autre partition ou serveur System i d'une autre plateforme ne peut utiliser Global Mirror en même temps. L'ajout de plusieurs utilisateurs à une session Global Mirror donne des résultats imprévisibles.

Avant de créer une session Global Mirror sur i5/OS, vous devez avoir configuré Global Mirror sur les unités de stockage externe IBM System Storage. Pour plus d'informations sur l'utilisation de Global Mirror sur IBM System Storage DS8000, voir IBM System Storage DS8000 Information Center.

Pour configurer la fonction Global Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque que vous voulez utiliser comme copie (source) de production.
6. Dans le menu **Sélection d'une action**, sélectionnez **Nouvelle session**.
7. Suivez les instructions de l'assistant pour compléter la tâche.

Information associée

Add ASP Copy Description (ADDASPCPYD) command

Start ASP Session (STRASPSSN) command

Chapitre 5. Gestion de la haute disponibilité

Après avoir configuré une solution à haute disponibilité i5/OS, vous pouvez la gérer à l'aide de plusieurs interfaces liées à la haute disponibilité.

Scénarios : gestion de solutions à haute disponibilité

En tant qu'opérateur système ou administrateur de votre solution à haute disponibilité, vous devez réaliser des tâches courantes telles que la sauvegarde et la maintenance système de votre environnement à haute disponibilité.

Les scénarios suivants offrent des instructions sur la réalisation de tâches système courantes, comme des sauvegardes et des mises à jour, ainsi que des exemples de gestion d'événements à haute disponibilité, tels que des partitions de grappe et des basculements. Pour chaque scénario, un environnement modèle a été choisi. Les instructions pour chaque scénario correspondent à cette solution à haute disponibilité particulière et sont uniquement fournies à titre d'exemple.

Scénarios : Réalisation de sauvegardes dans un environnement à haute disponibilité

La méthode de sauvegarde des données peut différer en fonction de votre solution à haute disponibilité et de votre stratégie de sauvegarde. Cependant, il existe un ensemble de tâches communes à effectuer lorsque vous réalisez des opérations de sauvegarde pour les systèmes d'un environnement à haute disponibilité.

Dans plusieurs solutions à haute disponibilité, vous avez la possibilité de réaliser des sauvegardes distantes à partir de la seconde copie des données qui est stockée sur le système de sauvegarde. Les sauvegardes distantes vous permettent de garder votre système de production opérationnel, tandis que le deuxième système est sauvegardé. Chacun de ces scénarios fournit des exemples de deux solutions à haute disponibilité dans lesquelles des sauvegardes sont réalisées à distance sur le système de sauvegarde.

Dans le premier scénario, les sauvegardes distantes sont réalisées dans une solution à haute disponibilité qui utilise une technologie de protection géographique par disque miroir. Le deuxième scénario montre comment la fonction FlashCopy peut être utilisée dans un environnement à haute disponibilité qui utilise des solutions IBM System Storage telles que Metro ou Global Mirror.

Scénario : Réalisation de sauvegardes dans un environnement de protection géographique par disque miroir

Ce scénario fournit une présentation des tâches nécessaires à la réalisation d'une sauvegarde distante dans une solution à haute disponibilité i5/OS qui utilise la protection géographique par disque miroir.

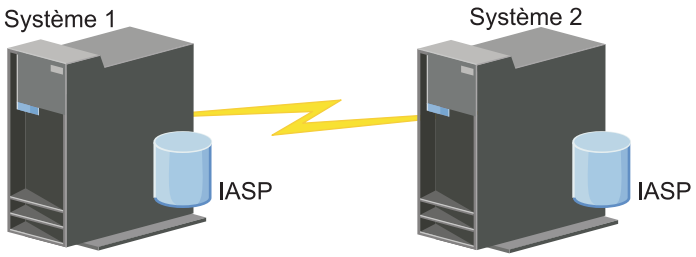
Présentation

Dans cet exemple, un administrateur système doit effectuer une sauvegarde des données stockées dans des pools de stockage sur disque indépendant utilisés dans une solution à haute disponibilité fondée sur une technologie de protection géographique par disque miroir. L'administrateur ne veut pas interférer sur le fonctionnement du système de production en le mettant hors ligne pour réaliser la sauvegarde. Au lieu de cela, l'administrateur compte déconnecter temporairement la copie protégée par disque miroir, puis effectuer une sauvegarde de la seconde copie des données située sur les pools de stockage sur disque indépendant vers un emplacement distant.

Remarque : La déconnexion de la copie protégée par disque miroir interrompt la protection géographique par disque miroir jusqu'à ce que la copie soit reconnectée à la production. Pendant la période de déconnexion, la haute disponibilité et la reprise après incident ne sont pas opérationnelles. Si une indisponibilité du système de production se produit pendant ce processus, certaines données seront perdues.

Détails

L'image suivante illustre cet environnement :



Etapes de configuration

1. Mise au repos du pool de stockage sur disque indépendant
2. «Déconnexion de la copie miroir», à la page 187
3. Rendre le pool de stockage sur disque disponible
4. Sauvegarde d'un pool de stockage sur disque indépendant
5. «Reprise d'un pool de stockage sur disque indépendant», à la page 184
6. «Reconnexion d'une copie miroir», à la page 188

Scénario : Exécution d'une fonction FlashCopy

Dans cet exemple, un administrateur souhaite effectuer une sauvegarde à partir de la copie distante des données stockées dans des unités de stockage externes sur le site de sauvegarde. Grâce à l'utilisation de la fonction FlashCopy fournie avec IBM Storage Solutions, l'administrateur réduit considérablement la durée de sa sauvegarde.

Présentation

Dans cet exemple, un administrateur système doit effectuer une sauvegarde des données stockées dans des unités de stockage externes IBM System Storage. L'administrateur ne veut pas interférer sur le fonctionnement du système de production en le mettant hors ligne pour réaliser la sauvegarde. Au lieu de cela, l'administrateur envisage de réaliser une opération FlashCopy, qui réalise une capture des données par point de cohérence. A partir de ces données, l'administrateur sauvegarde les données sur un support externe. Une sauvegarde FlashCopy ne prend que quelques minutes, et réduit donc la durée du processus de sauvegarde.

Bien que dans cet exemple, la fonction FlashCopy soit utilisée pour des opérations de sauvegarde, notez aussi que cette fonction peut avoir plusieurs utilisations. Par exemple, la fonction FlashCopy peut être utilisée pour la création d'entrepôts de données destinées à réduire la charge de travail des requêtes sur les systèmes de production ou pour la copie des données de production en vue de créer un environnement test.

Etapes de configuration

1. «Mise au repos d'un pool de stockage sur disque indépendant», à la page 184
2. «Configuration d'une session FlashCopy», à la page 195

3. Effectuez une sauvegarde FlashCopy sur des unités de stockage externes IBM System Storage. Pour plus d'informations sur l'utilisation de la fonction FlashCopy sur IBM System Storage DS8000, voir IBM System Storage DS8000 Information Center .
4. «Reprise d'un pool de stockage sur disque indépendant», à la page 184
5. Mise en fonction du pool de stockage sur disque
6. Sauvegarde d'un pool de stockage sur disque indépendant

Scénario : Mise à niveau du système d'exploitation dans un environnement à haute disponibilité

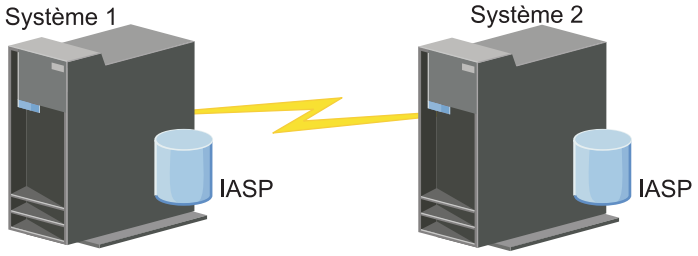
| Dans cet exemple, un administrateur système met à niveau le système d'exploitation pour deux systèmes
| IBM i dans une solution à haute disponibilité à partir d'une protection géographique par disque miroir.

Présentation

L'administrateur système doit mettre à niveau me système d'exploitation pour deux systèmes dans l'environnement à haute disponibilité. Dans cet exemple, il existe deux noeuds : System 1 et System 2.
| System 1 est la copie de production et System 2 la copie en miroir. Les deux systèmes utilisent IBM i V6R1. Le pool de stockage sur disque indépendant est en ligne, la protection géographique par disque miroir est active et les systèmes sont synchronisés. L'administrateur système souhaite mettre à niveau ces deux systèmes vers IBM i 7.1.

Détails

Le graphique suivant illustre l'environnement :



Etapes de configuration

1. Déconnectez la copie en miroir (System 2).
2. Arrêtez le groupe de ressources en grappe (System 2).
3. Arrêtez le noeud (System 2).
4. Mise à niveau du système 2 vers la nouvelle édition. Pour plus d'informations, voir Mise à niveau ou remplacement de i5/OS et des logiciels connexes.
| 5. Installez le programme sous licence IBM PowerHA for i.
6. Rendez le pool de stockage sur disque disponible et testez les applications sur System 2. Le test des applications garantit qu'elles fonctionnent comme prévu dans la nouvelle édition. Une fois les tests effectués, vous pouvez terminer la mise à niveau en exécutant le reste des étapes.
7. Rendez le pool de stockage sur disque disponible sur la copie en miroir déconnectée (System 2).
8. Reconnectez la copie en miroir. La resynchronisation des données en miroir a alors lieu. Au terme de la resynchronisation, vous pouvez poursuivre le processus de mise à niveau.
9. Exécution de basculementsDans ce cas, la copie en miroir (System 2) devient la nouvelle copie de production et la copie de production (System 1) devient la nouvelle copie en miroir.

Remarque : La protection géographique par disque miroir est suspendue car vous ne pouvez pas l'exécuter du noeud n-1 vers le noeud n. Vous pouvez en revanche l'exécuter sans problème du noeud n vers le noeud n-1. Dans ce scénario, la protection géographique par disque miroir est interrompue au terme d'un basculement. Les données ne seront plus copiées pendant la suite du processus de mise à niveau car il n'y a plus de système de secours valide.

10. Arrêtez le groupe de ressources en grappe (System 1).
11. Arrêtez le noeud (System 1).
12. Mise à niveau de System 1 vers la nouvelle édition. Pour plus d'informations, voir Mise à niveau ou remplacement de i5/OS et des logiciels connexes.
13. Installez le programme sous licence IBM PowerHA for i.
14. Démarrez les noeuds (System 1).
15. Démarrez les groupes de ressources en grappe (System 1).
16. Redémarrez la protection par disque miroir.
17. Effectuez un basculement. La copie en miroir en cours (System 1) redevient la copie de production et la copie de production(System 2) redevient la copie en miroir. Il s'agit de la configuration d'origine avant la mise à niveau.
18. Ajustement de la version de grappe d'une grappe
19. Modification de la version de haute disponibilité du logiciel sous licence PowerHA

Exemple : Mise à niveau du système d'exploitation

Dans les environnements à haute disponibilité, vous devez effectuer des opérations particulières avant toute mise à niveau du système d'exploitation.

Les exemples suivants peuvent vous aider à déterminer ce que vous devez faire pour procéder à une mise à niveau dans l'environnement de grappe. Avant d'effectuer la mise à niveau ou toute autre opération, vous devez déterminer la version en cours de la grappe.

Remarque : Remarque :

Remarques :

1. V6R1 représente l'édition actuelle du système d'exploitation.
2. 7.1 représente la nouvelle édition du système d'exploitation.
3. V5R4 représente l'édition précédente du système d'exploitation.

Exemple 1 : Le noeud à mettre à niveau est équipé d'IBM i V6R1. Tous les autres noeuds de la grappe ont IBM i V6R1 ou une version ultérieure. La version en cours de la grappe est la version 6.

Action : Mettez à niveau le noeud vers IBM i 7.1. Après la mise à niveau du noeud, démarrez la mise en grappe sur le noeud mis à niveau.

Exemple 2 : Le noeud à mettre à niveau est équipé d'IBM i V6R1. Tous les autres noeuds de la grappe ont IBM i V6R1. La version en cours de la grappe est la version 5.

Action : Mettez à niveau la grappe active vers IBM i 6. Mettez à niveau le noeud vers IBM i 7.1. Démarrez la mise en grappe sur le noeud mis à niveau.

Exemple 3 : Le noeud à mettre à niveau est équipé d'IBM i V5R4. Tous les autres noeuds de la grappe ont IBM i V6R1. La version en cours de la grappe est 5.

Action : Supprimez de la grappe le noeud mis à niveau vers IBM i 7.1 avant la mise à niveau. Passez la grappe active à la version 6. Mettez à niveau le noeud vers IBM i 7.1 et ajoutez-le de nouveau à la grappe.

Exemple 4 : Le noeud à mettre à niveau est équipé d'IBM i V6R1. La grappe contient uniquement des noeuds IBM i V5R4 et IBM i V6R1. La version en cours de la grappe est la version 5. La mise à niveau du noeud IBM i V6R1 vers IBM i 7.1 est moins importante que de laisser les noeuds à la version IBM

i V5R4.

Actions :

1. Supprimez de la grappe le noeud mis à niveau.
2. Mettez à niveau le noeud vers IBM i 7.1.
3. Mettez à niveau les autres noeuds IBM i V5R4 au moins vers IBM i V6R1.
4. Modifiez la version de la grappe en 5.
5. Ajoutez de nouveau le noeud mis à niveau dans la grappe.

Exemple 5 : Le noeud à mettre à niveau est équipé d'IBM i V6R1. La grappe contient uniquement des noeuds IBM i V5R4 et IBM i V6R1. La version en cours de la grappe est 5. La mise à niveau du noeud IBM i V6R1 vers IBM i 7.1 est plus importante que de laisser les noeuds à la version IBM i V5R4.

Actions :

1. Supprimez tous les noeuds IBM i V5R4 de la grappe.
2. Modifiez la version de la grappe en 5.
3. Mettez à niveau le noeud vers IBM i 7.1.
4. Démarrez le noeud mis à niveau.
5. Comme les noeuds IBM i V5R4 restants sont mis à niveau vers IBM i 7.1, ils peuvent être ajoutés de nouveau dans la grappe.

Exemple 6 : Le noeud à mettre à niveau est équipé d'IBM i V5R4. Au moins un autre noeud de la grappe est équipé d'IBM i V5R4. La version en cours de la grappe est inférieure ou égale à 3.

Action : Mettez à niveau tous les noeuds vers IBM i V6R1. Passez la la grappe à la version 5. Mettez à niveau tous les noeuds vers IBM i 7.1.

Le tableau suivant répertorie les actions que vous devez effectuer pour appliquer une mise à niveau dans un environnement de grappe.

Tableau 8. Mise à niveau de noeuds vers IBM i 7.1

Edition en cours du noeud que vous mettez à niveau	Version en cours de la grappe	Actions
V6R1	6	1. Mettez à niveau le noeud vers IBM i 7.1. 2. Démarrez le noeud mis à niveau.
V6R1	5	1. Passez la grappe à la version 6. 2. Mettez à niveau le noeud vers IBM i 7.1. 3. Démarrez le noeud mis à niveau. **Remarque :** Si d'autres noeuds de la grappe sont équipés d'IBM i V5R4, reportez-vous aux exemples 4 et 5 pour plus de détails.

Tableau 8. Mise à niveau de noeuds vers IBM i 7.1 (suite)

Edition en cours du noeud que vous mettez à niveau	Version en cours de la grappe	Actions
V5R4	Inférieure ou égale à 5	**Option A** 1. Supprimez de la grappe le noeud mis à niveau. 2. Passez la grappe à la version 6. 3. Mettez à niveau le noeud vers la version 7.1. 4. Ajoutez de nouveau le noeud dans la grappe. **Option B** 1. Mettez à niveau tous les noeuds vers V6R1. 2. Passez la grappe à la version 6. 3. Mettez à niveau tous les noeuds vers la version 7.1.

Scénario : rendre une unité hautement disponible

Outre les pools de stockage sur disque indépendant, vous pouvez doter de haute disponibilité d'autres unités prises en charge. Dans ce cas, l'administrateur de la haute disponibilité peut fournir une haute disponibilité à des lignes Ethernet.

Vue globale

L'administrateur système veut doter d'une haute disponibilité des lignes Ethernet utilisées dans la solution à haute disponibilité. La configuration en cours offre une haute disponibilité pour les indisponibilités planifiées, avec deux systèmes utilisant la technologie de disque commuté. Cette solution a aussi recours à un domaine d'administration de grappe pour gérer et synchroniser les modifications apportées à l'environnement d'exécution de la solution à haute disponibilité. Cet exemple suppose que la configuration de la haute disponibilité et la configuration Ethernet ont été effectuées avant de procéder. Il est aussi supposé que l'état en cours de la haute disponibilité est actif et que toutes les ressources contrôlées sont cohérentes dans l'environnement. Cet exemple indique les étapes à suivre pour configurer la haute disponibilité pour une ligne Ethernet.

Etapes de configuration

1. «Création d'unités commutables», à la page 151
2. «Ajout de postes de ressource contrôlée», à la page 120
3. «Sélection des attributs à contrôler», à la page 165

Gestion des grappes

A l'aide des interfaces graphiques des services-ressources de mise en grappe, vous pouvez réaliser plusieurs tâches associées à la technologie de grappe qui est la base de votre solution à haute disponibilité i5/OS. Ces tâches vous permettent de gérer et de maintenir votre grappe.

Les modifications que vous pouvez apporter à la grappe après sa configuration sont les suivantes :

Tâches relatives au grappe

- Ajout d'un noeud à une grappe
- Suppression de noeuds d'une grappe

- Démarrage d'un noeud de grappe
- Arrêt d'un noeud de grappe
- Ajustement de la version d'un grappe au dernier niveau
- Suppression d'une grappe
- Modification d'un noeud de grappe

Tâches du groupe de ressources en grappe

- Création d'un groupe de ressources en grappe
- Suppression de groupes de ressources en grappe
- Démarrage d'un groupe de ressources en grappe
- Ajout d'un noeud à un groupe de ressources en grappe
- Suppression d'un noeud à partir d'un groupe de ressources en grappe
- Arrêt d'un groupe de ressources en grappe
- Modification du domaine de reprise d'un groupe de ressources en grappe
- Réalisation d'un basculement
- Ajout d'un noeud à un domaine d'unité
- Suppression d'un noeud d'un domaine d'unité

Tâches du domaine d'administration de grappe

- Création d'un domaine d'administration de grappe
- Ajout de ressources contrôlées
- Suppression d'un domaine d'administration de grappe

Modification de la version de PowerHA

La version de PowerHA détermine le niveau auquel les noeuds d'une grappe gérée par le produit PowerHA peuvent communiquer entre eux.

Les valeurs de la version de PowerHA déterminent les fonctions que le produit PowerHA peut utiliser. La version de PowerHA peut nécessiter une certaine version de grappe pour fonctionner. Par exemple, la version PowerHA 2.0 demande une grappe de version 7.

La version active de PowerHA est définie lors de la création d'une grappe. S'il existe déjà une grappe, la version active de PowerHA est définie d'après la plus ancienne des versions prises en charge.

Tout comme les versions de grappe, PowerHA possède une version potentielle et une version active. La version active de PowerHA est la version dans laquelle les noeuds de la grappe qui sont reconnus par PowerHA communiquent entre eux. La version potentielle de PowerHA est la version la plus récente de PowerHA que le noeud puisse prendre en charge. Il est impossible de changer la version active de PowerHA tant que la même version potentielle de PowerHA n'est pas installée sur tous les noeuds PowerHA. La version potentielle de PowerHA est comprise entre n et n+1. Par exemple, NODE1 contient la version potentielle de PowerHA 2.0, NODE2 la version potentielle de PowerHA 2.0 et NODE3 la version potentielle de PowerHA 3.0. Les trois noeuds peuvent prendre en charge la version 2.0 ; la version active de PowerHA peut donc être la version 2.0.

A partir de PowerHA version 2.0, si un noeud contenant une version potentielle de PowerHA incompatible est ajouté à la grappe, il pourra s'ajouter mais il sera considéré comme un noeud inconnu par PowerHA. Si un noeud est inconnu de PowerHA, certaines fonctions du produit ne fonctionneront pas sur ce noeud. Un noeud est reconnu par PowerHA si le produit PowerHA y est installé et que sa version de PowerHA est compatible avec la version active de PowerHA.

Vous pouvez changer la version active de PowerHA avec la commande Change Cluster Version (CHGCLUVER).

Vous pouvez uniquement utiliser la commande Change Cluster Version (CHGCLUVER) pour passer à une version de grappe ou de PowerHA plus élevée. Si vous voulez augmenter la version de PowerHA de deux niveaux, vous devez exécuter la commande CHGCLUVER deux fois.

La version active de la grappe ne peut pas être supérieure à la plus basse des versions potentielles des noeuds de la grappe. De même la version active de PowerHA ne peut pas être supérieure à la version potentielle de PowerHA la plus basse présente dans les noeuds de la grappe ou à la version potentielle de PowerHA de n'importe quel noeud de la grappe. Pour afficher la version potentielle des noeuds et de PowerHA, utilisez la commande Display Cluster Information (DSPCLUINF).

Utilisez les instructions suivantes pour vérifier et modifier la version de grappe d'un noeud.

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise ne grappe, sélectionnez la tâche **Affichage des propriétés d'une grappe**.
5. Dans la page Propriétés de grappe, cliquez sur l'onglet **Général**.
6. Vérifiez le paramètre de version de grappe ou modifiez la version avec le paramètre qui convient.
7. Vérifiez le paramètre de version de PowerHA ou modifiez la version avec le paramètre qui convient.

Concepts associés

Version de grappe

Information associée

Change Cluster Version (CHGCLUVER) command

Ajustement de la version de grappe d'une grappe

La version de grappe définit le niveau auquel les noeuds de la grappe communiquent activement entre eux.

La fonction de contrôle des versions de grappe permet à la grappe de contenir des systèmes de niveaux d'édition différents pouvant fonctionner entre eux en identifiant le niveau de protocole de communication à utiliser.

Pour pouvoir modifier la version de grappe, tous les noeuds de cette dernière doivent être au même niveau de version nominale. La version de grappe peut alors être modifiée de manière à correspondre à la version nominale. Cette modification permet l'utilisation de la nouvelle fonction. La version ne peut être incrémentée que d'une unité. Pour la décrémenter, vous devez supprimer la grappe, puis la recréer avec un niveau de version antérieur. La version de grappe en cours est initialement définie par le premier noeud créé dans la grappe. Les noeuds suivants ajoutés à la grappe doivent être d'un niveau égal à la version de grappe en cours ou au niveau de version suivant. Si tel n'est pas le cas, leur ajout est impossible.

Si vous faites évoluer un noeud vers une nouvelle version, vous devez vous assurer que le noeud possède la bonne version de grappe. Les grappes prennent uniquement en charge une différence de version. Si tous les noeuds de la grappe sont de la même version, nous vous conseillons d'évoluer vers la nouvelle version avant de modifier la version de grappe. Ceci garantit que toutes les fonctions associées à la nouvelle version sont disponibles. Voir la rubrique «Scénario : Mise à niveau du système d'exploitation dans un environnement à haute disponibilité», à la page 133 pour obtenir des actions détaillées pour l'évolution vers une nouvelle version.

Utilisez les instructions suivantes pour vérifier et modifier la version de grappe d'un noeud.

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise ne grappe, sélectionnez la tâche **Affichage des propriétés d'une grappe**.
5. Dans la page Propriétés de grappe, cliquez sur l'onglet **Général**.
6. Vérifiez le paramètre de version de grappe ou modifiez la version avec le paramètre qui convient.

Concepts associés

Version de grappe

Information associée

Change Cluster Version (CHGCLUVER) command

Adjust Cluster Version (QcstAdjustClusterVersion) API

Suppression d'une grappe

Quand vous supprimez une grappe, les services-ressource de mise en grappe s'arrêtent sur tous les noeuds de grappe actifs, qui sont supprimés de la grappe.

Au moins l'un des noeuds doit être actif. Si vous disposez de disques commutés ou d'autres unités commutables dans votre grappe, supprimez tout d'abord chaque noeud du domaine d'unité avant de supprimer la grappe. Si vous ne procédez pas de cette manière, vous ne serez plus en mesure d'ajouter les disques sur une autre grappe.

Pour supprimer une grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise ne grappe**, sélectionnez **Suppression de grappe**.
5. La fenêtre de confirmation de la **suppression de la grappe** apparaît. Cliquez sur **Yes** pour supprimer la grappe. Une fois que vous avez supprimé la grappe, la page **Services-ressources de mise en grappe - Bienvenue** change et affiche la tâche **Nouvelle grappe**.

Tâches associées

«Suppression d'un noeud d'un domaine d'unité», à la page 145
Un *domaine d'unité* est un sous-ensemble de noeuds dans une grappe qui partagent des ressources d'unité.

Information associée

Delete Cluster (DLTCLU) command

Delete Cluster (QcstDeleteCluster) API

Affichage de la configuration des grappes

Vous pouvez afficher un rapport détaillé qui fournit des informations sur la configuration des grappes. Le rapport de configuration de la grappe fournit des informations détaillées sur la grappe, la liste d'appartenance du noeud, les paramètres de configuration et d'optimisation, ainsi que sur chaque groupe de ressources de la grappe.

Pour afficher la configuration des grappes, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise ne grappe**, sélectionnez la tâche **Affichage des informations de configuration** . Cela affiche la page de la configuration des grappes et des propriétés. Vous pouvez enregistrer cette page dans un fichier ou l'imprimer.

Information associée

Display Cluster Information (DSPCLUINF) command

Sauvegarde et restauration de la configuration des grappes

Si vous utilisez la mise en grappe sur vos systèmes, il est important de créer une stratégie de sauvegarde et de restauration pour protéger vos données.

Si vous comptez utiliser la mise en grappe comme stratégie de sauvegarde de sorte que vous ayez un système en cours de fonctionnement tandis que l'autre est arrêté lors de sa sauvegarde, nous vous recommandons d'avoir au moins trois systèmes dans la grappe. Ainsi, vous aurez toujours un système sur lequel basculer en cas d'incident.

Sauvegarde et restauration des groupes de ressources en grappe

Vous pouvez sauvegarder un groupe de ressources en grappe que la grappe soit active ou non. Les restrictions suivantes s'appliquent lors de la restauration d'un groupe de ressources en grappe :

- Si la grappe est en cours de fonctionnement et que le groupe de ressources en grappe n'est pas connu de cette grappe, vous ne pourrez pas restaurer le groupe de ressources en grappe.
- Si le noeud n'est pas configuré pour une grappe, vous ne pourrez pas restaurer un groupe de ressources en grappe.

Vous pouvez restaurer un groupe de ressources en grappe si la grappe est active, si le groupe de ressources en grappe n'est pas connu de cette grappe, si le noeud se trouve dans le domaine de reprise de ce groupe de ressources en grappe et si le nom de la grappe correspond à celui du groupe de ressources en grappe. Vous pouvez restaurer un groupe de ressources en grappe si la grappe est configurée, mais inactive sur ce noeud et si ce noeud se trouve dans le domaine de reprise de ce groupe de ressources en grappe.

Préparation à un incident

En cas d'incident, vous devrez probablement reconfigurer votre grappe. Pour vous préparer à un tel scénario, nous vous recommandons d'enregistrer les informations de configuration de votre grappe et de les conserver sur papier.

1. Utilisez la commande SAVCFG (Enregistrement de la sauvegarde) ou SAVSYS (Enregistrement du système) après avoir apportées des modifications à la configuration de sorte que les informations de grappe internes restaurées soient actualisées et cohérentes avec les autres noeuds de la grappe. Voir Enregistrement des informations de configuration pour obtenir des détails sur la réalisation d'une opération SAVCFG ou SAVSYS.
2. Imprimez une copie des informations de configuration de la grappe à chaque fois que vous les modifiez. Vous utilisez la commande DSPCLUINF (Affichage des informations de grappe) pour imprimer la configuration de la grappe. Conservez une copie de vos bandes de sauvegarde. En cas d'incident, vous devrez probablement reconfigurer la totalité de votre grappe.

Information associée

Saving configuration information

Save Configuration (SAVCFG) command

Save System (SAVSYS) command

Display Cluster Information (DSPCLUINF) command

Contrôle de l'état des grappes

L'interface graphique des services-ressources de mise en grappe contrôle l'état de la grappe et affiche un message d'avertissement quand des noeuds qui font partie de la solution à haute disponibilité ne sont plus cohérents.

L'interface graphique des services-ressources de mise en grappe affiche le message d'avertissement HAI0001W sur la page Noeuds si la grappe n'est pas cohérente. Un message incohérent signifique que les informations extraites de ce noeud peuvent ne pas être cohérentes avec celles des autres noeuds actifs de la grappe. Les noeuds deviennent incohérents quand ils sont désactivés dans la grappe.

Pour obtenir des informations cohérentes, accédez aux informations sur la grappe depuis un noeud actif de la grappe, ou démarrez ce noeud et renouvelez votre demande.

Pour contrôler l'état de la grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page du noeud, HAI0001W s'affiche si le noeud est incohérent : `Le noeud de grappe local n'est pas activé. Les informations de la grappe risquent de ne pas être précises tant que le noeud local est démarré.`

Tâches associées

«Démarrage de noeuds», à la page 106
Le démarrage d'un noeud de grappe lance la mise en grappe et les services-ressources de mise en grappe sur un noeud dans un environnement à haute disponibilité i5/OS.

Information associée

Display Cluster Information (DSPCLUINF) command

Display Cluster Resource Group Information (DSPCRGINF) command

List Cluster Information (QcstListClusterInfo) API

List Device Domain Info (QcstListDeviceDomainInfo) API

Retrieve Cluster Resource Services Information (QcstRetrieveCRSInfo) API

Retrieve Cluster Information (QcstRetrieveClusterInfo) API

List Cluster Resource Groups (QcstListClusterResourceGroups) API

List Cluster Resource Group Information (QcstListClusterResourceGroupInf) API

Indication des files d'attente de messages

Vous pouvez indiquer une file d'attente de messages de grappe ou une file d'attente de message de basculement. Ces files d'attente de messages vous permettent de déterminer les causes des échecs dans votre environnement i5/OS à haute disponibilité.

Une file d'attente de messages en grappe est utilisée pour des messages au niveau de la grappe et fournit un message qui contrôle tous les groupes de ressources en grappe qui basculent vers un noeud

spécifique. Une file d'attente de message en basculement est utilisée pour les messages au niveau du groupe de ressources en grappe et fournit un message pour chaque groupe de ressources en grappe en cours de basculement.

Indication d'une file d'attente de messages de grappe

Remarque : Vous pouvez également configurer une grappe pour utiliser une file d'attente de messages de grappe en spécifiant la file d'attente de messages tout en exécutant l'assistant de création de grappe.

Pour définir une file d'attente de messages de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Affichage des propriétés d'une grappe**.
5. Dans la page Ppriétés d'une grappe, cliquez sur **File d'attente de messages de grappe**.
6. Spécifiez les informations suivantes pour créer une file d'attente de messages de grappe :
   - Dans la zone **Nom**, indiquez le nom de la file d'attente de messages pour recevoir des messages qui traitent d'un basculement au niveau d'une grappe ou d'un noeud. Pour les reprises en ligne au niveau des noeuds, un message contrôlant la reprise en ligne de tous les groupes de ressources en grappe avec le même nouveau noeud principal est envoyé. Si un groupe de ressources en grappe effectue la reprise en ligne individuellement, un message contrôlant la reprise en ligne de ce groupe de ressources en grappe est envoyé. Le message est envoyé au nouveau noeud principal. Si cette zone est définie, la file d'attente de messages indiquée doit exister sur tous les noeuds dans la grappe lorsqu'ils sont démarrés. La file d'attente de messages ne peut pas faire partie d'un pool de stockage sur disque indépendant.
   - Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de la bibliothèque ne peut pas être *CURLIB, QTEMP, *LIBL, *USRLIBL, *ALL ou *ALLUSR.
   - Dans la zone **Délai d'attente avant reprise en ligne**, sélectionnez **Ne pas attendre** or **Toujours attendre** ou indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de grappe.
   - Dans la zone **Action par défaut de reprise en ligne**, spécifiez l'action que les services-ressources de mise en grappe doivent effectuer quand la réponse au message de reprise en ligne a dépassé la valeur de la durée d'attente avant la reprise en ligne. Vous pouvez définir cette zone sur **Poursuite du basculement** ou sur **Annulation du basculement**.

Indication d'une file d'attente de messages de basculement

Pour définir une file d'attente de messages de basculement, procédez comme suit :

1. Dans un navigateur Web, saisissez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre de votre IBM Systems Director Navigator for i5/OS.
4. Dans cette page, cliquez sur **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Dans la liste des groupes de ressources en grappe, sélectionnez le groupe de ressource en grappe avec lequel vous voulez travailler.

6. Dans la page Groupe de ressources en grappe, cliquez sur le menu **Sélection d'une action** et sélectionnez **Propriétés**.
7. Sur la page Général, indiquez les valeurs suivantes pour indiquer une file d'attente de messages de reprise en ligne :
   - Dans la zone **File de messages de reprise en ligne**, indiquez le nom de la file d'attente de messages censée recevoir les messages lorsqu'une reprise en ligne se produit pour ce groupe de ressources en grappe. Si cette zone est définie, la file d'attente de messages spécifiée doit exister sur tous les noeuds du domaine de reprise une fois le programme d'exit terminé. La file d'attente de messages de reprise en ligne ne peut pas faire partie d'un pool de stockage sur disque indépendant.
   - Dans la zone **Bibliothèque**, indiquez le nom de la bibliothèque qui contient la file d'attente de messages sensée recevoir le message relatif à la reprise en ligne. Le nom de la bibliothèque ne peut pas être *CURLIB, QTEMP ou *LIBL.
   - Dans la zone **Délai d'attente avant reprise en ligne**, indiquez le nombre de minutes d'attente avant l'obtention d'une réponse au message relatif à la reprise en ligne dans la file d'attente de messages de reprise en ligne. Vous pouvez également indiquer l'action que les services-ressources de mise en grappe doivent effectuer quand la réponse au message de basculement a dépassé la valeur de la durée d'attente avant le basculement.

Liste de contrôle d'annulation de la configuration de grappe

Pour garantir une annulation totale de la configuration d'une grappe, vous devez supprimer systématiquement les différents composants de grappe.

Tableau 9. Liste de contrôle d'annulation de la configuration du pool de stockage sur disque indépendant pour les grappes

Spécifications du pool de stockage sur disque indépendant	
__	Si vous utilisez des pools de stockage sur disque commutés, la tour doit être basculée vers un noeud qui est le propriétaire SPCN avant l'annulation de la configuration du groupe de ressources en grappe. Vous pouvez utiliser l'API QcstInitiateSwitchOver (Initialisation du basculement) ou la commande CHGCRGPRI (Modification du groupe de ressources en grappe principale) pour renvoyer le groupe de ressources en grappe vers le propriétaire SPCN. Si cette étape n'est pas effectuée, vous ne pourrez pas marquer la tour comme étant privée pour ce système.
__	Si vous comptez supprimer un sous-ensemble de groupes de pools de stockage sur disque indépendant ou le dernier pool de stockage sur disque indépendant dans les unités commutables, vous devez arrêter le premier groupe de ressources en grappe. Utilisez la commande (ENDCRG).
__	Si vous voulez supprimer un pool de stockage sur disque indépendant qui participe à une grappe, il est fortement recommandé de supprimer d'abord le groupe de ressources en grappe d'unité. Voir «Suppression d'un groupe de ressources en grappe», à la page 151 pour plus d'informations. Vous pouvez également utiliser la commande (RMVCRGDEVE) pour supprimer l'objet de configuration du pool de stockage sur disque indépendant du groupe de ressources en grappe.
__	Une fois l'objet de configuration supprimé du pool de stockage sur disque indépendant à partir de l'unité commutable de la grappe, vous pouvez supprimer un pool de stockage sur disque indépendant.
__	Supprimez la description d'unité d'un pool de stockage sur disque indépendant en complétant ces tâches : 1. Dans une interface de ligne de commande, saisissez WRKDEVD DEVD(*ASP) et appuyez sur Entrée. 2. Faites défiler la page vers le bas jusqu'à ce que vous voyiez la description d'unité du pool de stockage sur disque indépendant que vous voulez supprimer. 3. Sélectionnez l'option 4 (Supprimer) par le nom de la description d'unité et appuyez sur Entrée.

Tableau 10. Liste de contrôle de l'annulation de la configuration des groupes de ressource en grappe pour les grappes

Spécification du groupe de ressources en grappe	
__	Supprimez le groupe de ressources en grappe en complétant l'une des étapes suivantes : 1. Si la mise en grappe n'est pas activée sur le noeud, saisissez DLTCRG CRG(CRGNAME) dans une interface de ligne de commande. CRGNAME est le nom du groupe de ressources en grappe que vous voulez supprimer. Appuyez sur Entrée. 2. Si la mise en grappe est activée sur le noeud, saisissez DLTCRGCLU CLUSTER(CLUSTERNAME) dans une interface de ligne de commande. CLUSTERNAME est le nom de la grappe. CRGNAME est le nom du groupe de ressources en grappe que vous voulez supprimer. Appuyez sur Entrée.

Gestion des noeuds

Les partitions système et logiques qui font partie d'un environnement i5/OS à haute disponibilité sont appelées noeuds. Vous pouvez réaliser plusieurs tâches de gestion relatives aux noeuds.

Affichage des propriétés des noeuds

Vous pouvez afficher et gérer des propriétés associées aux noeuds configurés dans le cadre de votre environnement à haute disponibilité en utilisant l'interface graphique des services-ressources de mise en grappe.

Pour afficher les propriétés des noeuds, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans l'onglet **Noeuds**, cliquez sur le menu **Sélection d'une action** et sélectionnez **Propriétés**. Cliquez sur **OK**. Cela affiche la page des propriétés des noeuds.
   - La page Général affiche le nom du noeud et l'adresse IP système de ce noeud.
   - La page Mise en grappe affiche les informations suivantes :
     - Les adresses IP de l'interface de grappe qui sont utilisées par la grappe pour communiquer avec d'autres noeuds de la grappe.
     - La version potentielle du noeud indique le niveau de version et de modification utilisé par les noeuds de la grappe pour communiquer activement entre eux.
     - Les domaines d'unité qui sont affichés et configurés dans la grappe sélectionnée. Si vous sélectionnez un domaine d'unité dans la liste, les noeuds appartenant au domaine d'unité sélectionné le sont également.

Arrêt des noeuds

L'arrêt ou l'interruption d'un noeud arrête la mise en grappe et les services-ressources de mise en grappe de ce noeud.

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans l'onglet **Noeuds**, sélectionnez le noeud que vous voulez arrêter.

5. Cliquez sur le menu **Sélection d'une action** puis sélectionnez **Arrêt**. Quand les services de ressources de mise en grappe sont arrêtés correctement sur le noeud indiqué, l'état du noeud devient Arrêté.

Information associée

End Cluster Node (ENDCLUNOD) command

End Cluster Node (QcstEndClusterNode) API

Suppression de noeuds

Vous devrez éventuellement supprimer un noeud d'une grappe si vous en effectuez la mise à niveau ou si le noeud ne doit plus prendre part à l'environnement à haute disponibilité i5/OS.

Pour supprimer un noeud d'une grappe existante, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans la page Noeuds, cliquez sur le menu **Sélection d'une action** et sélectionnez **Supprimer**.
6. Cliquez sur **Oui** dans la fenêtre de confirmation de suppression d'un noeud de grappe.

Tâches associées

«Annulation de la configuration de la protection géographique par disque miroir», à la page 188
Si vous ne voulez plus que la fonction utilise la protection géographique par disque miroir pour un pool de stockage sur disque spécifique ou un groupe de pools de stockage sur disque, vous pouvez sélectionner **Annulation de la configuration de la protection géographique par disque miroir**. Si vous annulez la configuration de la protection géographique par disque miroir, le système arrête la protection géographique par disque miroir et supprime la copie miroir des pools de stockage sur disque sur les noeuds du site de la copie miroir.

Information associée

Remove Cluster Node Entry (RMVCLUNODE) command

Remove Cluster Node Entry (QcstRemoveClusterNodeEntry) API

Suppression d'un noeud d'un domaine d'unité

Un *domaine d'unité* est un sous-ensemble de noeuds dans une grappe qui partagent des ressources d'unité.

Important :

Soyez prudent au moment de supprimer un noeud d'un domaine d'unité. Si ce noeud est le point d'accès principal actuel pour des pools de stockage sur disque indépendant, ces derniers sont solidaires du noeud. Dans ce cas, ils ne sont plus accessibles depuis les autres noeuds du domaine d'unité.

Une fois un noeud supprimé d'un domaine d'unité, il est impossible de le rajouter au même domaine d'unité si un ou plusieurs noeuds de grappe existants appartiennent toujours à ce domaine d'unité. Pour rajouter le noeud au domaine d'unité, vous devez :

1. supprimer les pools de stockage sur disque indépendant actuellement détenus par le noeud ajouté au domaine d'unité ;
2. effectuer un démarrage du système sur le noeud ;
3. ajouter le noeud au domaine d'unité ;
4. recréer les pools de stockage sur disque indépendant supprimés à l'étape 1.

Pour supprimer un noeud d'une grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans l'onglet **Noeuds**, cliquez sur le menu **Sélection d'une action** et sélectionnez **Propriétés**. Cliquez sur **Go**. La page Propriétés du noeud apparaît.
6. Dans l'onglet **Mise en grappe**, supprimez le nom du noeud de la zone **Domaine de l'unité** et cliquez sur **OK**.

Tâches associées

«Suppression d'une grappe», à la page 139
Quand vous supprimez une grappe, les services-ressource de mise en grappe s'arrêtent sur tous les noeuds de grappe actifs, qui sont supprimés de la grappe.

Information associée

Remove Device Domain Entry (RMVDEVDMNE) command

Remove Device Domain Entry (QcstRemoveDeviceDomainEntry) API

Ajout d'un moniteur de grappe à un noeud

IBM i Cluster Resource Services peut à présent utiliser une partition Hardware Management Console (HMC) ou Virtual I/O Server (VIOS) pour détecter les défaillances des noeuds de grappe. Cette nouveauté permet d'identifier davantage de scénarios d'incident et d'éviter le partitionnement des grappes.

L'interface graphique des Services de ressources de mise en grappe vous permet d'utiliser une console HMC ou un serveur VIOS pour gérer et surveiller l'état de chaque système. Une fois le moniteur configuré, la console HMC ou le serveur VIOS envoie des notifications des incidents de noeud détectés. Vous pouvez utiliser un moniteur de grappe pour réduire le nombre d'incidents qui occasionnent des partitionnements de grappe.

Pour ajouter un moniteur de grappe à une grappe existante, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans l'onglet **Noeuds**, cliquez sur l'icône contextuelle à côté du noeud considéré, puis sélectionnez **Propriétés**. La page Propriétés du noeud apparaît.
6. Dans l'onglet **Moniteurs**, dans la table des données de moniteur, cliquez sur la liste déroulante **Sélection d'une action** puis cliquez sur l'action **Ajout d'un moniteur de grappe**.

Suppression d'un moniteur de grappe

Un *moniteur de grappe* fournit une autre source d'information aux services de ressource de grappe pour déterminer quand un noeud de grappe est tombé en panne.

Important :

Soyez prudent lorsque vous supprimez un moniteur de grappe. Si vous supprimez un noeud d'un moniteur de grappe et que ce noeud est le point d'accès principal actuel pour un groupe de ressources en grappe, ce noeud peut être partitionné alors qu'il est tombé en panne. Cela signifie que l'utilisateur devra exécuter des étapes manuelles pour rétablir la haute disponibilité.

Pour supprimer un moniteur de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Dans l'onglet **Noeuds**, cliquez sur l'icône contextuelle à côté du noeud considéré, puis sélectionnez **Propriétés**. Cliquez sur **OK**. La page Propriétés du noeud apparaît.
6. Sélectionnez l'onglet **Moniteurs** afin d'afficher la liste des moniteurs de grappe configurés pour le noeud.
7. Dans l'onglet **Moniteurs**, sélectionnez le moniteur désiré puis cliquez sur la liste déroulante **Sélection d'une action** et sélectionnez la fonction **Suppression**.

Chapitre 6. Gestion de groupes de ressources en grappe

Les groupes de ressources en grappe permettent de gérer des ressources résilientes dans un environnement haute disponibilité an i5/OS. Ils constituent une technologie de mise en grappe qui définit et contrôle la commutation des ressources vers des systèmes de sauvegarde en cas d'indisponibilité.

Affichage de l'état du groupe de ressources en grappe

Vous pouvez contrôler l'état des groupes de ressources en grappe dans votre environnement à haute disponibilité. Vous pouvez utiliser ces messages d'état pour valider des modifications apportées dans le groupe de ressources en grappe ou pour déterminer des problèmes liés à ce groupe.

Pour afficher l'état du groupe de ressources en grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, affichez l'état actuel d'un groupe de ressources en grappe dans la colonne Etat.

Voici la liste des valeurs d'état possibles pour un groupe de ressources en grappe :

Tableau 11. Valeurs d'état pour les groupes de ressources en grappe

Valeurs possibles	Description
Démarré	Le groupe de ressources en grappe est démarré.
Arrêté	Le groupe de ressources en grappe est arrêté.
En attente de validation	Les informations relatives à ce groupe de ressources en grappe de la solution à haute disponibilité ne sont peut-être pas exactes. Cet état indique qu'un programme d'exit de groupe de ressources en grappe est appelé avec une opération d'annulation et échoue.
Restauré	Le groupe de ressources en grappe a été restauré sur son noeud et n'a pas été copié sur d'autres noeuds de la grappe. Lors du démarrage de la mise en grappe sur le noeud, le groupe de ressources en grappe sera synchronisé avec les autres noeuds et son état sera défini sur Inactif.
Inactif	Les services-ressources de mise en grappe du groupe de ressources en grappe ne sont pas actifs sur le noeud. Les causes possibles sont les suivantes : le noeud est tombé en panne ou est arrêté, ou le travail du groupe de ressources en grappe est inactif sur ce noeud.
Suppression	Le groupe de ressources en grappe est en cours de suppression de la grappe.

Tableau 11. Valeurs d'état pour les groupes de ressources en grappe (suite)

Valeurs possibles	Description
Modification en cours	Le groupe de ressources en grappe est en cours de modification. Le groupe de ressources en grappe est réinitialisé une fois la modification effectuée.
Arrêt en cours	Le groupe de ressources en grappe est en cours d'arrêt.
Ajout en cours	Le groupe de ressources en grappe est en cours d'ajout à la grappe.
En cours de démarrage	Le groupe de ressources en grappe est en cours de démarrage.
Commutation	Le groupe de ressources en grappe est en cours de commutation sur un autre noeud.
Ajout de noeud en cours	Un nouveau noeud est en cours d'ajout à la grappe. Le groupe de ressources en grappe est réinitialisé une fois l'ajout du noeud effectué.
Suppression de noeud en cours	Un noeud est en cours de suppression du groupe de ressources en grappe. Le groupe de ressources en grappe est réinitialisé une fois la suppression du noeud effectuée.
Modification en cours de l'état du noeud	L'état d'un noeud dans le domaine de reprise du groupe de ressources en grappe est en cours de modification.

Arrêt d'un groupe de ressources en grappe

Les groupes de ressources en grappe gèrent des ressources résilientes dans un environnement à haute disponibilité i5/OS. Il s'agit d'une technologie de grappe qui définit et contrôle les ressources résilientes commutées vers des systèmes de sauvegarde en cas d'indisponibilité.

Vous risquez de vouloir arrêter le groupe de ressources en grappe pour interrompre automatiquement la fonction de reprise en ligne dans votre environnement à haute disponibilité. Par exemple si vous effectuez un IPL sur l'un des systèmes défini dans le groupe de ressources en grappe.

Pour arrêter un groupe de ressources en grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, sélectionnez un groupe de ressources en grappe que vous voulez arrêter.
6. Dans le menu **Sélection d'une action**, choisissez **Arrêt** et cliquez sur **OK**.

Information associée

End Cluster Resource Group (ENDCRG) command

End Cluster Resource Group (QcstEndClusterResourceGroup) API

Suppression d'un groupe de ressources en grappe

Vous pouvez supprimer un groupe de ressource en grappe à l'aide de l'interface des services-ressources de mise en grappe.

Pour supprimer un groupe de ressources en grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, sélectionnez un groupe de ressources en grappe que vous voulez supprimer.
6. Dans le menu **Sélection d'une action**, choisissez **Suppression** et cliquez sur **OK**.
7. Sélectionnez **Oui** dans la fenêtre de confirmation de la suppression du groupe de ressources en grappe d'unité.

Information associée

Delete Cluster Resource Group from Cluster (DLTCRGCLU) command

Delete Cluster Resource Group (QcstDeleteClusterResourceGroup) API

Création d'unités commutables

Outre celles de pools de stockage sur disque indépendant, plusieurs autres unités sont prises en charge pour la haute disponibilité. Par exemple, des lignes Ethernet, des lecteurs de disque optique et des serveurs réseau, entre autres, peuvent désormais faire partie d'une solution à haute disponibilité.

Un groupe de ressources en grappe d'unité contient la liste des unités commutables. Chaque unité de la liste identifie un pool de stockage sur disque indépendant commutable ou un autre type d'unité commutable (unités de bande, descriptions de ligne, contrôleurs, serveurs de réseau, etc.). La totalité des unités est commutée sur le noeud secondaire en cas d'indisponibilité. Vous pouvez également mettre les unités en fonction pendant la reprise en ligne ou le basculement.

Pour créer une unité commutable, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Dans la page Groupe de ressources en grappe, cliquez sur l'icône de contexte à côté du groupe de ressources de grappe d'unité pour lequel vous voulez ajouter une unité commutable existante et sélectionnez **Ajout d'une unité existante** dans le menu contextuel.
6. Dans la liste d'ajout d'une unité commutable, cliquez sur **Ajouter**.

7. Dans la fenêtre Ajout d'une unité commutable existante, indiquez le type d'objet de configuration et le nom d'objet de l'unité commutable. Cliquez sur **OK** pour ajouter l'unité commutable à la liste. Par exemple, si vous avez ajouté une ligne Ethernet commutable, sélectionnez cette entrée dans la liste.
8. Cliquez sur **OK** dans la liste pour ajouter la nouvelle unité au groupe de ressources de grappe d'unité.

Modification du domaine de reprise d'un groupe de ressources en grappe

Le domaine de reprise contrôle les actions de reprise d'un sous-ensemble de noeuds défini dans un groupe de ressources en grappe.

Pour modifier un domaine de reprise dans le groupe de ressources en grappe d'unité, le groupe de ressources en grappe d'application ou le groupe de ressources en grappe de données, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Sur la page des services-ressources de mise en grappe, sélectionnez **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Sur la page du groupe de ressources en grappe, sélectionnez un groupe de ressources en grappe que vous voulez modifier.
6. Dans le menu **Sélection d'une action**, choisissez **Propriétés** et cliquez sur **OK**.
7. Cliquez sur la page Domaine de reprise pour modifier les valeurs existantes du domaine de reprise. Sur cette page, vous pouvez modifier les rôles des noeuds dans le domaine de reprise de la grappe, et ajouter et supprimer des noeuds à partir du domaine de reprise. Dans le cas d'un groupe de ressources en grappe d'unité, vous pouvez également modifier le nom de site et les adresses IP du port de données pour un noeud du domaine de reprise.

Information associée

Add Cluster Resource Group Node Entry (ADDCRGNODE) command

Change Cluster Resource Group (CHGCRG) command

Remove Cluster Resource Group Node Entry (RMVCRGNODE) command

Add a Node to Recovery Domain (QcstAddNodeToRcvyDomain) API

Change Cluster Resource Group (QcstChangeClusterResourceGroup) API

Remove Node from Recovery Domain (QcstRemoveNodeFromRcvyDomain) API

Création des noms de site et des adresses IP du port de données

Si vous utilisez la protection géographique par disque miroir, les noeuds définis dans le noeud du domaine de reprise du groupe de ressources en grappe d'unité doivent posséder une adresse IP de port de données et un nom de site.

Le nom du site est associé à un noeud dans le domaine de reprise pour un groupe de ressources en grappe d'unité, applicable uniquement à la protection géographique par disque miroir. Quand vous configurez un environnement à haute disponibilité de protection géographique par disque miroir, chaque noeud se trouvant sur les différents sites doit être affecté à un nom de site différent.

Pour créer l'adresse IP du port de données et les noms de site des noeuds du domaine de reprise, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page des services-ressources de mise en grappe, cliquez sur la tâche **Gestion des groupes de ressources en grappe** pour afficher une liste des groupes de ressources de la grappe.
5. Dans l'onglet Groupe de ressources en grappe, cliquez sur l'icône contextuelle en regard du groupe de ressources en grappe d'unité, puis sur **Propriétés**.
6. Dans la page Domaine de reprise, sélectionnez **Modification**.
7. Pour utiliser une adresse IP de port de données existante, sélectionnez-la dans la liste et cliquez sur **OK**. Pour ajouter une adresse IP de port de données, cliquez sur **Ajout**. Dans la fenêtre Ajout d'adresse IP de port de données, saisissez l'adresse IP.
8. Dans la fenêtre de modification, indiquez le nom du site.

Chapitre 7. Gestion des événements d'indisponibilité avec reprise en ligne

Généralement, une reprise en ligne résulte d'une indisponibilité de noeud, mais d'autres causes sont possibles. Par exemple, différents types d'actions système ou utilisateur peuvent entraîner des situations de reprise en ligne.

Il est possible qu'un incident affectant un seul groupe de ressources en grappe entraîne une reprise en ligne pour ce groupe, mais pas pour un autre groupe.

Dans une grappe, quatre catégories d'indisponibilité sont possibles. Certains événements sont de véritables situations de reprise en ligne dans lesquelles le noeud devient indisponible, alors qu'il est nécessaire d'étudier certains autres événements avant de déterminer la cause et la réponse appropriée. Les tableaux suivants décrivent chacune de ces catégories d'indisponibilités et les types d'événements qu'elles comportent, ainsi que l'action de reprise appropriée.

Indisponibilités de catégorie 1 : Indisponibilité de noeud entraînant la reprise en ligne

Une reprise en ligne se produit au niveau du noeud, entraînant les événements suivants :

- Dans chaque groupe de ressources en grappe, le noeud principal est marqué *inactif* et devient le dernier noeud secondaire.
- Le noeud qui était le premier noeud secondaire devient le nouveau noeud principal.

Les reprises en ligne se produisent dans l'ordre suivant :

1. Tous les groupes de ressources en grappe d'unité
2. Tous les groupes de ressources en grappe de données
3. Tous les groupes de ressources en grappe d'application

Remarques :

1. Si la reprise en ligne d'un groupe de ressources en grappe détecte qu'aucun des noeuds secondaires n'est actif, l'état du groupe de ressources en grappe est défini sur *En attente de validation* et le domaine de reprise du groupe reste inchangé.
2. Si tous les services-ressources de mise en grappe échouent, les ressources (groupes de ressources en grappe) qu'ils gèrent suivent le processus de reprise en ligne.

Tableau 12. Indisponibilités de catégorie 1 : Indisponibilité de noeud entraînant la reprise en ligne

Evénement d'indisponibilité avec reprise en ligne
Emission de la commande ENDTCP (*IMMED ou *CNTRLD avec un délai).
Emission de la commande ENDSYS (*IMMED ou *CNTRLD).
Emission de la commande PWRDWNSYS (*IMMED ou *CNTRLD).
Activation du bouton d'IPL (démarrage du système) pendant que les services de ressources de mise en grappe sont activés sur le système.
Appel de l'API ou de la commande Arrêt du noeud de grappe sur le noeud principal du domaine de reprise du groupe de ressources en grappe.
Appel de l'API ou de la commande Suppression d'un poste de noeud d'une grappe sur le noeud principal du domaine de reprise du groupe de ressources en grappe.
Report par la console HMC de la mise hors tension de la partition ou activation de l'option d'écran 7.

Tableau 12. Indisponibilités de catégorie 1 : Indisponibilité de noeud entraînant la reprise en ligne (suite)

Evénement d'indisponibilité avec reprise en ligne
Emission de la commande ENDSBS QSYSWRK(*IMMED ou *CNTRLD).

Indisponibilités de catégorie 2 : Indisponibilité de noeud entraînant un partitionnement ou un basculement

Ces indisponibilités entraînent un partitionnement ou un basculement selon que la détection avancée des incidents de noeud est ou non configurée. Reportez-vous aux colonnes de la table. Si la détection avancée des incidents de noeud est configurée, un basculement se produit dans la plupart des cas et les informations de l'indisponibilité de catégorie 1 s'appliquent. Si la détection avancée des incidents de noeud n'est pas configurée, un partitionnement se produit et les informations suivantes s'appliquent :

- L'état des noeuds ne communiquant pas par la messagerie de grappe devient Partition. Pour plus d'informations sur les partitions, voir Partition de grappe.
- Tous les noeuds de la partition de grappe ne possédant pas le noeud principal comme membre de la partition mettront fin au groupe de ressources en grappe actif.

Remarques :

1. Si un noeud a réellement échoué, mais qu'il est détecté uniquement comme un incident de partition et qu'il s'agissait du noeud principal, vous perdez tous les services d'application et de données du noeud et aucune reprise en ligne automatique n'est démarrée.
2. Vous devez déclarer le noeud comme en échec ou le remettre en service et démarrer à nouveau la mise en grappe sur ce noeud. Pour plus d'informations, voir Passage des noeuds partitionnés à l'état Echec.

Tableau 13. Indisponibilités de catégorie 2 : Indisponibilité de noeud entraînant une partition

Evénement d'indisponibilité avec reprise en ligne	**Sans détection avancée des incidents de noeud**	**HMC**	**VIOS**
Indisponibilité matérielle du complexe électronique central (unité centrale, par exemple).	partitionnement	basculement	partitionnement ou basculement
Erreur machine sur le logiciel du système d'exploitation.	partitionnement	basculement	basculement
Mise hors tension immédiate de la console HMC ou activation de l'option d'écran 8.	partitionnement	basculement	basculement
Redémarrage de la partition de la console HMC ou activation de l'option d'écran 3.	partitionnement	basculement	basculement
Coupure d'alimentation du complexe électronique central.	partitionnement	partitionnement	partitionnement

Indisponibilités de catégorie 3 : Défaillance du groupe de ressources en grappe entraînant la reprise en ligne

Pour un système contenant un serveur VIOS, une panne matérielle CEC peut entraîner un basculement comme un partitionnement. Ce qui se produit dépend du type du système et de la panne matérielle. Par exemple, dans un système de lames, une panne du CEC qui empêche le fonctionnement du serveur VIOS entraîne un partitionnement car le serveur VIOS ne peut pas signaler les défaillances. Dans le même système, si une seule lame tombe en panne mais que le serveur VIOS continue de fonctionner, un basculement a lieu car le serveur VIOS peut signaler la panne.

Lorsqu'une défaillance d'un groupe de ressources en grappe entraîne une reprise en ligne, les événements suivants se produisent :

- Si un seul groupe de ressources en grappe est concerné, la reprise en ligne se produit groupe par groupe. En effet, les groupes de ressources en grappe sont indépendants les uns des autres.
- Si quelqu'un annule plusieurs travaux de ressource en grappe, ce qui a un impact simultané sur plusieurs groupes de ressources en grappe, aucune reprise en ligne coordonnée n'est effectuée entre les groupes.
- Le noeud principal est marqué Inactif dans chaque groupe de ressources en grappe et il devient le dernier noeud secondaire.
- Le noeud qui était le premier noeud secondaire devient le nouveau noeud principal.
- En l'absence de noeud secondaire actif, l'état du groupe de ressources en grappe est défini sur En attente de validation et le domaine de reprise reste inchangé.

Tableau 14. Indisponibilités de catégorie 3 : Défaillance du groupe de ressources en grappe entraînant la reprise en ligne

Evénement d'indisponibilité avec reprise en ligne
Le travail du groupe de ressources en grappe comporte une erreur logicielle entraînant son interruption anormale.
Le programme d'exit d'application échoue pour un groupe de ressources en grappe d'application.

Indisponibilités de catégorie 4 : Indisponibilité de communication entraînant une partition

Cette catégorie est similaire à la catégorie 2. Les événements suivants ont lieu :

- L'état des noeuds ne communiquant pas par la messagerie de grappe est défini sur Partition. Pour plus d'informations sur les partitions, voir Partition de grappe.
- Tous les noeuds et services-ressources de mise en grappe des noeuds sont toujours opérationnels, mais tous les noeuds ne communiquent pas entre eux.
- La grappe est partitionnée, mais le noeud principal de chaque groupe de ressources en grappe fournit toujours des services.

La reprise normale pour cet état de partition doit consister à remédier au problème de communication ayant entraîné la partition de la grappe. La grappe résoudra l'état de partition sans intervention supplémentaire.

Remarque : Si vous voulez que les groupes de ressources en grappe exécutent une reprise sur un nouveau noeud principal, vérifiez que l'ancien noeud principal n'utiliser pas les ressources avant que le noeud ne soit marqué comme étant en échec. Pour plus d'informations, voir Passage des noeuds partitionnés à l'état Echec.

Tableau 15. Indisponibilités de catégorie 4 : Indisponibilité de communication entraînant une partition

Evénement d'indisponibilité avec reprise en ligne
Défaillance du routeur, de la ligne ou de la carte de communication sur les lignes de l'adresse IP du signal de présence de la grappe.
Répercussion de ENDTCPIFC sur toutes les adresses IP du signal de présence de la grappe sur un noeud de grappe.

Indisponibilités avec des groupes de ressources en grappe actifs

- Si le groupe de ressources en grappe est actif et que le noeud défaillant *n'est pas* le noeud principal, les événements suivants se produisent :
  - La reprise en ligne met à jour l'état du membre du domaine de reprise en échec dans le domaine de reprise du groupe de ressources en grappe.
  - Si le noeud défaillant est un noeud secondaire, la liste des noeuds secondaires est réorganisée de façon à ce que les noeuds actifs se trouvent en tête de liste.
- Si le groupe de ressources en grappe est actif et que le membre du domaine de reprise est le noeud principal, les actions exécutées par le système dépendent du type d'indisponibilité qui s'est produit.
  - Indisponibilités de catégorie 1 : Indisponibilité de noeud entraînant la reprise en ligne
  - Indisponibilités de catégorie 2 : Indisponibilité de noeud entraînant une partition
  - Indisponibilités de catégorie 3 : Défaillance du groupe de ressources en grappe entraînant la reprise en ligne
  - Indisponibilités de catégorie 4 : Indisponibilité de communication entraînant une partition

Indisponibilités avec des groupes de ressources en grappe inactifs

En cas d'indisponibilité au niveau des groupes de ressources en grappe, les événements suivants se produisent :

- L'état d'appartenance du noeud en échec dans le domaine de reprise du groupe de ressources en grappe devient un état inactif ou de partition.
- Les rôles du noeud ne sont pas modifiés et les noeuds secondaires ne sont pas réorganisés automatiquement.
- Les noeuds secondaires sont réorganisés dans un groupe de ressources en grappe inactif à l'appel de la commande STRCRG (Démarrage d'un groupe de ressources en grappe) ou de l'API QcstStartClusterResourceGroup (Démarrage d'un groupe de ressources en grappe).

  Remarque : L'API Démarrage d'un groupe de ressources en grappe échoue si le noeud principal n'est pas actif. Vous devez lancer la commande CHGCRG (Modification d'un groupe de ressources en grappe) ou l'API QcstChangeClusterResourceGroup (Modification d'un groupe de ressources en grappe) pour désigner un noeud actif comme noeud principal, puis appeler à nouveau l'API Démarrage d'un groupe de ressources en grappe.

Chapitre 8. Gestion des domaines d'administration de grappe

Une fois un domaine d'administration de grappe créé et les entrées de ressources contrôlées ajoutées, l'administrateur de grappe doit surveiller l'activité dans le domaine d'administration afin que les ressources contrôlées restent cohérentes. Grâce à l'interface graphique des services-ressources de mise en grappe, vous pouvez gérer et surveiller un domaine d'administration de grappe.

Cette interface graphique permet de répertorier les entrées de ressources contrôlées avec l'état global de chaque ressource. Vous pouvez afficher des informations détaillées en sélectionnant une entrée. Ces informations incluent la valeur globale de chaque attribut associé à l'entrée et indique si cet attribut est cohérent ou non avec le domaine. Si l'état global d'une ressource contrôlée est incohérent, l'administrateur doit effectuer les étapes nécessaires pour comprendre pourquoi la ressource est incohérente, corriger l'incident et resynchroniser la ressource.

Si la ressource est incohérente car une mise à jour a échoué sur un ou plusieurs noeuds, les informations pouvant aider à identifier la cause de l'incident sont conservées pour l'entrée de ressource contrôlée. Sur le noeud où s'est produit l'incident, un message est journalisé avec l'entrée de ressource contrôlée avec la cause d'échec de la mise à jour. Sur les autres noeuds, un message d'information journalisé en interne signale qu'un incident s'est produit, ainsi que la liste des noeuds sur lesquels la mise à jour a échoué. Ces messages sont disponibles dans l'interface graphique des services-ressources de mise en grappe ou en appelant l'API Retrieve Monitored Resource Information (QfpadRtvMonitoredResourceInfo). Les messages d'échec sont également journalisés dans l'historique de travail du travail du groupe de ressources en grappe homologue.

Une fois la cause de l'incohérence identifiée, la ressource peut être resynchronisée, soit grâce à une opération de mise à jour sur le noeud où l'échec s'est produit, soit en arrêtant et en redémarrant le domaine d'administration. Par exemple, une entrée de ressource contrôlée pour un profil utilisateur peut être incohérente car vous avez changé le numéro utilisateur pour le profil utilisateur sur un noeud dans le domaine d'administration, mais ce numéro utilisateur était déjà utilisé par un autre profil sur l'un des noeuds. Si vous changez à nouveau la valeur du numéro utilisateur et que cette nouvelle valeur n'est pas utilisée par un autre profil utilisateur dans le domaine d'administration, le changement sera appliqué à tous les noeuds et l'état global pour l'entrée de ressource contrôlée du profil sera cohérente. Il est inutile d'intervenir davantage pour resynchroniser l'entrée de ressource contrôlée du profil utilisateur.

Dans certains cas, vous devez arrêter et redémarrer le groupe de ressources en grappe du domaine d'administration de grappe afin de resynchroniser les ressources incohérentes. Par exemple, si vous changez le numéro utilisateur pour un profil utilisateur auquel est associée une entrée de ressource contrôlée, mais que le profil est actif dans un travail sur l'un des autres noeuds de la grappe dans le domaine d'administration, la valeur globale pour l'entrée associée sera incohérente car le changement échoue sur le noeud où le profil est actif. Pour corriger cette situation, vous devez patienter jusqu'à la fin du travail, puis arrêter le domaine d'administration de grappe. Au redémarrage du domaine d'administration, la valeur globale pour chaque attribut qui est incohérente sera employée pour passer la ressource à un état cohérent.

L'état global pour une ressource contrôlée est toujours d'échec si la ressource est supprimée, renommée ou déplacée sur un noeud du domaine. Si tel est le cas, l'entrée de ressource contrôlée doit être supprimée, car la ressource n'est plus synchronisée par le domaine d'administration de grappe.

Lorsque vous restaurez une ressource contrôlée sur un système appartenant à un domaine d'administration de grappe, la ressource est de nouveau synchronisée avec la valeur globale actuellement connue dans le domaine lorsque le groupe de ressources en grappe homologue représentant ce domaine est actif.

Les commandes de restauration suivantes entraîne la resynchronisation d'objets système : RSTLIB, RSTOBJ, RSTUSRPRF et RSTCFG. Par ailleurs, RSTSYSINF et UPDSYSINF entraînent la resynchronisation de valeurs système et d'attributs du réseau. Pour resynchroniser des variables d'environnement système exécutant les commandes RSTSYSINF ou UPDSYSINF, le groupe de ressources en grappe homologue représentant le domaine d'administration de grappe doit être arrêté et redémarré.

Pour restaurer une ressource contrôlée à son état antérieur, supprimez l'entrée de ressource contrôlée représentant la ressource à restaurer. Une fois le ressource restaurée, ajoutez une entrée à partir du système où l'opération de restauration a lieu. Le domaine d'administration de grappe synchronise alors la ressource contrôlée avec les valeurs issues de la ressource contrôlée.

Pour surveiller un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher une liste de domaines d'administration dans la grappe.
4. Dans l'onglet **Domaine d'administration**, sélectionnez **Nouveau domaine d'administration**.
5. Dans la page Nouveau domaine d'administration, entrez les informations sur le domaine d'administration de grappe.

Arrêt d'un domaine d'administration de grappe

Les domaines d'administration de grappe fournissent un test de résistance d'environnement aux ressources d'une solution à haute disponibilité i5/OS. Il peut s'avérer nécessaire d'arrêter un domaine d'administration de grappe pour mettre provisoirement fin à la synchronisation des ressources contrôlées.

Un domaine d'administration de grappe devient inactif lorsqu'il est arrêté. Tant que le domaine est inactif, toutes les ressources contrôlées sont considérées comme incohérentes car les modifications qui leur sont apportées ne sont pas synchronisées. Bien que ces modifications fassent toujours l'objet d'un suivi, la valeur globale n'est pas modifiée et les modifications ne sont pas propagées au reste du domaine d'administration. Les modifications apportées aux ressources contrôlées alors que le domaine d'administration de grappe est inactif sont synchronisées sur tous les noeuds actifs au redémarrage du domaine.

Remarque : Le domaine d'administration de grappe et le programme d'exit qui lui est associé sont des objets fournis par IBM. Ils ne doivent pas être modifiés à l'aide de l'API QcstChangeClusterResourceGroup ou de la commande CHGCRG. Ces modifications risquent en effet de provoquer des résultats imprévisibles.

Pour arrêter un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
4. Dans la page Domaines d'administration, sélectionnez un domaine d'administration de grappe.
5. Sélectionnez **Arrêt** dans le menu **Sélection d'une action**.
6. Cliquez sur **Oui** dans la page de confirmation de l'arrêt du domaine d'administration.

Information associée

End Cluster Administrative Domain (ENDCAD) command

Suppression d'un domaine d'administration de grappe

Grâce à l'interface des services-ressources de mise en grappe, vous pouvez supprimer un domaine d'administration de grappe. La suppression d'un domaine d'administration de grappe arrête la synchronisation des ressources contrôlées qui sont définies dans le domaine d'administration de la grappe.

Pour supprimer un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
4. Dans la page Domaines d'administration, sélectionnez un domaine d'administration de grappe.
5. Dans le menu **Sélectionner une action**, choisissez **Suppression**.
6. Cliquez sur **Oui** dans la page de confirmation de la suppression du domaine d'administration.

Modification des propriétés d'un domaine d'administration de grappe

Grâce à l'interface graphique des services-ressources de mise en grappe, vous pouvez modifier les propriétés d'un domaine d'administration de grappe existant. Ces propriétés contrôlent la synchronisation des postes de ressource contrôlée définis dans le domaine d'administration de grappe.

Pour modifier les propriétés d'un domaine d'administration de grappe, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
4. Dans la page Domaines d'administration, sélectionnez un domaine d'administration de grappe.
5. Dans le menu **Sélection d'une action**, sélectionnez **Propriétés**.
6. Dans la page Propriétés, vous pouvez modifier les informations suivantes relatives au domaine d'administration de grappe :
   - Dans la zone **Nom**, saisissez le nom du domaine d'administration de grappe. Ce nom ne peut pas comporter plus de 10 caractères.
   - Dans la zone **Option de synchronisation**, spécifiez le comportement de synchronisation quand un noeud rejoint un domaine d'administration de grappe. Cette zone est activée seulement si la grappe est de version 6 ou ultérieure. Les valeurs possibles sont les suivantes :

     Option de dernière modification (par défaut)
     Sélectionnez cette option si toutes les modifications apportées aux ressources contrôlées doivent être appliquées à un domaine d'administration de grappe. Lorsqu'un noeud rejoint un domaine d'administration de grappe actif, toutes les modifications apportées aux ressources contrôlées sur ce noeud, lorsque ce domaine était inactif, sont appliquées aux ressources contrôlées sur les autres noeuds actifs du domaine, sauf si une modification plus récente a été apportée à la ressource dans le domaine actif. La modification la plus récente apportée à une ressource contrôlée est appliquée à cette ressource sur tous les noeuds actifs.

     Option de domaine actif
     Sélectionnez cette option si seules les modifications apportées aux ressources contrôlées

sont autorisées à partir des noeuds actifs. Les modifications apportées aux ressources contrôlées sur les noeuds inactifs sont éliminées lorsque le noeud rejoint le domaine d'administration de la grappe. L'option Domaine actif ne s'applique pas aux espaces de stockage des serveurs de réseau (*NWSSTG) ou aux configurations de serveurs de réseau (*NWSCFG). La synchronisation de ces ressources est toujours effectuée en fonction de la dernière modification apportée.

- Dans la liste **Noeuds du domaine d'administration**, vous pouvez ajouter un noeud au domaine d'administration de grappe en sélectionnant **Ajout** ou vous pouvez supprimer un noeud du domaine en sélectionnant **Suppression**.

Gestion d'entrées de ressources contrôlées

L'interface graphique des services-ressources de mise en grappe vous permet de gérer des entrées de ressources contrôlées dans votre domaine d'administration de grappe. Grâce au domaine d'administration, les modifications apportées à ces ressources contrôlées restent cohérentes sur chaque noeud dans l'environnement à haute disponibilité.

Utilisation de l'état d'une entrée de ressource contrôlée

L'interface graphique de service-ressource de mise en grappe présente des messages d'état pour les entrées de ressources contrôlées dans un domaine d'administration de grappe.

Lorsqu'une entrée de ressource contrôlée est ajoutée au domaine d'administration de grappe, la ressource est contrôlée pour détecter des modifications sur tous les noeuds de ce domaine ; de cette façon, les valeurs des attributs de la ressource peuvent être synchronisés à travers les noeuds dans le domaine d'administration de grappe en question. Le comportement de synchronisation dépend de plusieurs facteurs :

- l'état de la grappe,
- l'état du domaine d'administration de grappe,
- l'état du noeud,
- les actions entreprises sur la ressource.

Pour utiliser l'état d'une entrée de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
5. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
6. Dans le panneau d'options **Entrées de ressource contrôlée**, cliquez sur l'icône contextuelle à côté du type de ressource désiré, puis sélectionnez **Attributs**.
7. La liste des attributs de ressource contrôlée s'affiche. La colonne Etat global montre l'état actuel de cet attribut dans le domaine d'administration de grappe.

   Ces valeurs déterminent l'état d'une ressource contrôlée dans la grappe :

   Valeur globale
   La valeur de chaque attribut contrôlé qu'une ressource doit avoir sur tous les noeuds du

domaine d'administration. La valeur globale est identique sur tous les noeuds actifs et correspond au dernier changement synchronisé dans le domaine.

Etat global
L'état des ressources dans une domaine d'administration de grappe, en indiquant si les ressources sont totalement synchronisées. Les valeurs possibles sont les suivantes :

Cohérent
Les valeurs des attributs de ressource contrôlés par le système sont identiques sur tous les noeuds actifs du domaine d'administration de grappe. Cet état se produit dans un environnement d'exécution normal où la grappe, le domaine d'administration de grappe et tous les noeuds fonctionnent et sont actifs dans la grappe. Dans cet environnement, toute modification d'une valeur d'une ressource contrôlée est appliquée à tous les autres noeuds dans le domaine d'administration de grappe. Ce traitement est asynchrone par rapport à la modification d'origine mais donne des valeurs cohérentes pour les ressources inscrites dans le domaine d'administration. Dans ce cas, l'état global est Cohérent, la modification est effectuée sur chaque noeud et la valeur de la ressource sur les noeuds correspond à la valeur globale pour la ressource.

Incohérent
Les valeurs de l'ensemble des attributs de ressource contrôlés par le système ne sont pas identiques sur tous les noeuds actifs du domaine d'administration de grappe. Un message est journalisé et explique pourquoi l'état est Incohérent. Par exemple, si des modifications ont été apportées à des ressources contrôlées alors que le domaine d'administration de grappe était inactif, l'état est Incohérent.

En instance
Les valeurs des attributs contrôlés sont en cours de synchronisation dans le domaine d'administration de grappe.

Ajouté
L'entrée de ressource contrôlée a été ajoutée au domaine d'administration de grappe mais n'a pas encore été synchronisée.

Arrêté
La ressource contrôlée est dans un état inconnu car le domaine d'administration de grappe a été arrêté et les modifications apportées à la ressource ne sont plus traitées. Lorsque le domaine d'administration de grappe est arrêté, l'été global pour toutes les entrées de ressources contrôlées actuellement Cohérent passe à Arrêté.

Echec La ressource n'est plus contrôlée par le domaine d'administration de grappe et l'entrée doit être supprimée. Certaines actions sont déconseillées lorsqu'une ressource est synchronisée par un domaine d'administration de grappe. Si la ressource représentée par une entrée de ressource contrôlée est un objet système, elle ne doit pas être supprimée, renommée ou déplacée vers une autre bibliothèque avant d'avoir supprimé l'entrée correspondante. Si une ressource est supprimée, renommée ou déplacée vers une autre bibliothèque, l'état global de l'entrée de ressource contrôlée est Echec et toutes les modifications apportées à cette ressource sur un noeud ne sont propagées à aucun autre noeud dans le domaine d'administration de grappe.

Lorsque vous restaurez une ressource contrôlée sur un noeud dans le domaine d'administration de grappe, ses valeurs sont à nouveau modifiées pour correspondre aux valeurs globales synchronisées par le domaine d'administration de grappe.

Suppression des postes de ressource contrôlée

Les postes de ressource contrôlée sont en fait utilisés dans l'environnement à haute disponibilité et sont contrôlés pour toute modification via un domaine d'administration de grappe. Vous voudrez

probablement supprimer des postes de ressource contrôlée quand vous n'aurez plus besoin qu'ils soient contrôlés. Vous pouvez supprimer des postes de ressource contrôlée à l'aide de l'interface graphique des services-ressources en grappe.

Pour supprimer un poste de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
5. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
6. Dans la liste des types de ressource contrôlée, cliquez sur l'icône contextuelle en regard du type de ressource contrôlée, puis sur **Postes de ressource contrôlée**. La liste des objets de poste de ressource contrôlée s'affiche.
7. Cliquez sur l'icône contextuelle en regard du poste de ressource contrôlée que vous souhaitez supprimer, puis sur **Suppression d'un poste de ressource contrôlée**.
8. Cliquez sur **Oui** dans la fenêtre de confirmation de la suppression d'un poste de ressource contrôlée. Le poste de ressource contrôlée est supprimé du domaine d'administration de grappe.

Information associée

Remove Admin Domain MRE (RMVCADMRE) command

Remove Monitored Resource Entry (QfpadRmvMonitoredResourceEntry) API

Affichage de la liste d'entrées de ressources contrôlées

Les entrées de ressources contrôlées sont des ressources (comme des profils utilisateur et des variables d'environnement) qui ont été définies dans un domaine d'administration de grappe. Vous pouvez vous servir de l'interface graphique des services-ressources de mise en grappe pour répertorier les entrées de ressources contrôlées actuellement définies dans un domaine d'administration de grappe.

Pour afficher la liste des postes de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
5. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
6. Dans la liste des types de ressource contrôlée, cliquez sur l'icône contextuelle en regard du type de ressource contrôlée, puis sur **Postes de ressource contrôlée**.
7. Affichez et utilisez la liste des entrées de ressources contrôlées inscrites.

Sélection des attributs à contrôler

Après avoir ajouté des entrées de ressources contrôlées, vous pouvez sélectionner des attributs associés à ces ressources et que le domaine d'administration de grappe doit contrôler.

Pour sélectionner des attributs à contrôler pour une entrée de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
5. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
6. Dans la liste des types de ressource contrôlée, cliquez sur l'icône contextuelle en regard du type de ressource contrôlée, puis sur **Entrées de ressource contrôlée**. Le système affiche la liste des objets de poste de ressource contrôlée.
7. Cliquez sur l'icône contextuelle en regard de l'objet de poste de ressource contrôlée, par exemple un profil utilisateur ou une valeur système, puis sélectionnez **Gestion des attributs**. La liste des attributs d'entrées de ressource contrôlée s'affiche.
8. Dans la fenêtre de la liste d'attributs MRE, sélectionnez les attributs que vous voulez contrôler et cliquez sur **Fermeture**. Par exemple, si vous voulez contrôler la description de ligne Ethernet pour les modifications apportées à son attribut de nom de ressource, vous devez sélectionnez le nom de ressource comme attribut.

Tâches associées

«Ajout de postes de ressource contrôlée», à la page 120
Vous pouvez ajouter un poste de ressource contrôlée à un domaine d'administration de grappe. Les postes de ressource contrôlée définissent des ressources critiques de sorte que les modifications apportées à ces ressources restent cohérentes dans un environnement à haute disponibilité.

Attributs contrôlables

Une entrée de ressource contrôlée peut être ajoutée au domaine d'administration de grappe pour plusieurs types de ressources. Cette rubrique répertorie les attributs que chaque type de ressource peut contrôler.

Types de ressource

- Listes d'autorisation (*AUTL)
- Classes (*CLS)
- Descriptions de ligne Ethernet (*ETHLIN)
- Descriptions d'unité de pool de stockage sur disque indépendant (*ASPDEV)
- Descriptions de travail (*JOBD)
- Attributs de réseau (*NETA)
- Configuration du serveur de réseau pour la sécurité de connexion (*NWSCFG)
- Configuration du serveur de réseau pour des systèmes distants (*NWSCFG)
- Configurations du serveur de réseau pour des processeurs de service (*NWSCFG)
- Descriptions du serveur de réseau pour des connexions iSCSI (*NWSD)
- Descriptions du serveur de réseau pour des serveurs de réseau intégrés (*NWSD)

- Espaces de stockage pour serveurs de réseau (*NWSSTG)
- Descriptions d'unité d'adaptateur hôte pour serveurs de réseau (*NWSHDEV)
- Descriptions de lecteur de disque optique (*OPTDEV)
- Descriptions des périphériques d'impression pour les connexions LAN (*PRTDEV)
- Descriptions des périphériques d'impression pour les connexions virtuelles (*PRTDEV)
- Descriptions de sous-système (*SBSD)
- Variables d'environnement système (*ENVVAR)
- Valeurs système (*SYSVAL)
- Descriptions d'unité de bande (*TAPDEV)
- Descriptions de ligne d'anneau à jeton (*TRNLIN)
- Attributs TCP/IP (*TCPA)
- Profils utilisateur (*USRPRF)

Tableau 16. Tableau 1 - Attributs contrôlables pour des listes d'autorisation

Nom de l'attribut	Description
AUT	Autorité
TEXT	Description textuelle

Tableau 17. Attributs contrôlables pour des classes

Nom de l'attribut	Description
CPUTIME	Temps d'unité centrale maximal
DFTWAIT	Délai d'attente par défaut
MAXTHD	Nombre maximal d'unités d'exécution
MAXTMPSTG	Taille maximale de la mémoire de travail
RUNPTY	Priorité d'exécution
TEXT	Description textuelle
TIMESLICE	Tranche de temps

Tableau 18. Attributs contrôlables pour des descriptions de ligne Ethernet

Nom de l'attribut	Description
ASSOCPORT	Nom de ressource du port associé
AUTOCRTCTL	Création automatique de contrôleur
AUTODLTCTL	Suppression automatique de contrôleur
CMNRCYLMT	Nombre maximal de reprises
COSTBYTE	Coût relatif par octet pour l'envoi et la réception de données sur la ligne
COSTCNN	Coût relatif de la connexion sur la ligne
DUPLEX	Duplex
GENTSTFRM	Génération d'armoires de test
GRPADR	Adresse de groupe
LINESPEED	Débit de ligne
MAXFRAME	Longueur d'armoire maximale
MAXCTL	Nombre maximal de contrôleurs
MSGQ	File d'attente de messages

Tableau 18. Attributs contrôlables pour des descriptions de ligne Ethernet (suite)

Nom de l'attribut	Description
ONLINE	En ligne à l'IPL
PRPDLY	Temps de propagation
RSRCNAME	Nom de ressource
SECURITY	Niveau de sécurité de la ligne physique
SSAP	Liste des informations sur le SAP source (SSAP)
TEXT	Description textuelle
USRDFN1	Défini par l'utilisateur en premier
USRDFN2	Défini par l'utilisateur en deuxième
USRDFN3	Défini par l'utilisateur en troisième
VRYWAIT	Attente de mise en fonction

Tableau 19. Attributs contrôlables pour des descriptions d'unité de pool de stockage sur disque indépendant

Nom de l'attribut	Description
MSGQ	File d'attente de messages
BDR	Base de données relationnelle
RSRCNAME	Nom de ressource
TEXT	Description textuelle

Tableau 20. Attributs contrôlables pour des descriptions de travail

Nom de l'attribut	Description
ACGCDE	Code comptabilité
ALWMLTTHD	Autorisation de plusieurs unités d'exécution
DDMCNV	Conversation sur la gestion de fichiers distants
DEVRCYACN	Action de reprise d'unité
ENDSEV	Niveau de gravité pour arrêt
HOLD	Mise en attente de la file d'attente de travaux
INLASPGRP	Groupe ASP initial
INLLIBL	Liste des bibliothèques initiales
INQMSGRPY	Réponse au message d'interrogation
JOBMSGQFL	Action complète de la file d'attente de messages du travail
JOBMSGQMX	Taille maximale de la file d'attente de messages du travail
JOBPTY	Priorité du travail (sur JOBQ)
JOBQ	File d'attente de travaux
LOG	Historique des messages
LOGCLPGM	Historique des commandes de programme en langage de contrôle
OUTPTY	Priorité de sortie (sur OUTQ)
OUTQ	File d'attente en sortie
PRTDEV	Imprimante

Tableau 20. Attributs contrôlables pour des descriptions de travail (suite)

Nom de l'attribut	Description
PRTTXT	Impression du texte
RQSDTA	Données ou commande de requête
RTGDTA	Données de routage
SPLFACN	Action du fichier spoule
SWS	Indicateurs externes
SYNTAX	Vérification de la syntaxe du langage de contrôle
TEXT	Description textuelle
TSEPOOL	Pool de fin de tranche de temps
UTILISATEUR	Utilisateur

Tableau 21. Attributs contrôlables pour des attributs de réseau

Nom de l'attribut	Description
ALWADDCLU	Autorisation d'un ajout à la grappe
DDMACC	Accès aux requêtes DDM/DRDA
NWSDOMAIN	Domaine du serveur de réseau
PCSACC	Accès aux requêtes client
Remarque : chaque attribut de réseau est traité comme sa propre entrée de ressource contrôlée. Pour ceux-ci, le type de ressource et les noms d'attributs sont identiques.	

Tableau 22. Attributs contrôlables pour des configurations de serveur de réseau pour des processeurs de service

Nom de l'attribut	Description
EID	Identificateur de boîtier
INZSP	Initialisation du processeur de service
SPAUT	Droits du processeur de service
SPCERTID	Identificateur de certificat de processeur de service
SPINTNETA	Adresse Internet du processeur de service
SPNAME	Nom du processeur de service
TEXT	Description textuelle

Tableau 23. Attributs contrôlables pour la configuration du serveur de réseau pour des systèmes distants

Nom de l'attribut	Description
BOOTDEVID	Identificateur de l'unité d'amorçage
CHAPAUT	Authentification du protocole CHAP cible
DELIVERY	Méthode de distribution
DYNBOOTOPT	Options de démarrage dynamique
INRCHAPAUT	Authentification CHAP du demandeur
RMTIFC	Interfaces distantes
RMTSYSID	ID système distant
SPNWSCFG	Configuration du serveur de réseau pour le processeur de service utilisé pour gérer le serveur distant
TEXT	Description textuelle

Tableau 24. Attributs contrôlables pour la configuration du serveur de réseau pour la sécurité de connexion

Nom de l'attribut	Description
IPSECRULE	Règles de sécurité IP
TEXT	Description textuelle

Tableau 25. Attributs contrôlables pour les descriptions du serveur de réseau pour des serveurs de réseau intégrés

Nom de l'attribut	Description
CFGFILE	Fichier de configuration
CODEPAGE	Page de code ASCII représentant le jeu de caractères que ce serveur de réseau doit à utiliser
EVTLOG	Historique des événements
MSGQ	File d'attente de messages
NWSSTGL	Liens de l'espace de stockage
PRPDMNUSR	Propagation des utilisateurs du domaine
RSRCNAME	Nom de ressource
RSTDDEVRSC	Ressources des unités à accès restreint
SHUTDTIMO	Délai d'attente de l'arrêt
SYNCTIME	Synchronisation de la date et de l'heure
TCPDMNNAME	Nom de domaine local TCP/IP
TCPHOSTNAM	Nom d'hôte TCP/IP
TCPPORTCFG	Configuration du port TCP/IP
TCPNAMSVR	Système serveur de noms TCP/IP
TEXT	Description textuelle
VRYWAIT	Attente de mise en fonction
WINDOWSNT	Description du serveur de réseau Windows

Tableau 26. Attributs contrôlables pour les descriptions du serveur de réseau pour des connexions iSCSI

Nom de l'attribut	Description
ACTTMR	Délai d'activation
CFGFILE	Fichier de configuration
CMNMSGQ	File d'attente de messages des communications
CODEPAGE	Page de code ASCII représentant le jeu de caractères que ce serveur de réseau doit à utiliser
DFTSECRULE	Règle de sécurité IP par défaut
DFTSTGPTH	Chemin de stockage par défaut
EVTLOG	Historique des événements
MLTPTHGRP	Groupe multi-accès
MSGQ	File d'attente de messages
NWSCFG	Configuration du serveur de réseau
NWSSTGL	Liens de l'espace de stockage
PRPDMNUSR	Propagation des utilisateurs du domaine
RMVMEDPTH	Chemin d'accès au support amovible

Tableau 26. Attributs contrôlables pour les descriptions du serveur de réseau pour des connexions iSCSI (suite)

Nom de l'attribut	Description
RSRCNAME	Nom de ressource
RSTDDEVRSC	Ressources des unités à accès restreint
SHUTDTIMO	Délai d'attente de l'arrêt
STGPTH	Chemins de stockage iSCSI du serveur de réseau
SVROPT	Options de service
SYNCTIME	Synchronisation de la date et de l'heure
TCPDMNNAME	Nom de domaine local TCP/IP
TCPHOSTNAM	Nom d'hôte TCP/IP
TCPNAMSVR	Système serveur de noms TCP/IP
TCPPORTCFG	Configuration du port TCP/IP
TEXT	Description textuelle
VRTETHCTLP	Port de contrôle Ethernet virtuel
VRTETHPTH	Chemin d'accès au réseau Ethernet virtuel
VRYWAIT	Attente de mise en fonction

Tableau 27. Attributs contrôlables pour les espaces de stockage du serveur de réseau

Nom de l'attribut	Description
SIZE	Taille
TEXT	Description textuelle
TOTALFILES	Total de fichiers

Tableau 28. Attributs contrôlables pour les descriptions d'unité d'adaptateur hôte du serveur de réseau

Nom de l'attribut	Description
CMNRCYLMT	Nombre maximal de reprises
LCLIFC	Interface locale associée
MSGQ	File d'attente de messages
ONLINE	En ligne à l'IPL
RSRCNAME	Nom de ressource
TEXT	Description textuelle

Tableau 29. Attributs contrôlables pour des descriptions de lecteur de disque optique

Nom de l'attribut	Description
MSGQ	File d'attente de messages
ONLINE	En ligne à l'IPL
RSRCNAME	Nom de ressource
TEXT	Description textuelle

*Tableau 30. Attributs contrôlables pour les descriptions de périphérique d'impression pour les imprimantes *LAN*

Nom de l'attribut	Description
ACTTMR	Délai d'activation

*Tableau 30. Attributs contrôlables pour les descriptions de périphérique d'impression pour les imprimantes *LAN (suite)*

Nom de l'attribut	Description
ADPTADR	Adresse d'adaptateur distant LAN
ADPTTYPE	Type d'adaptateur
ADPTCNNTYP	Type de connexion d'adaptateur
AFP	Fonction d'impression avancée
CHRID	Identificateur de caractères
FONT	Police de caractères
FORMFEED	Alimentation papier
IMGCFG	Configuration d'image
INACTTMR	Temporisation d'inactivité
LNGTYPE	Type de langue
LOCADR	Adresse d'emplacement
MAXPNDRQS	Requête en attente maximum
MFRTYPMDL	Type et modèle de fabricant
MSGQ	File d'attente de messages
ONLINE	En ligne à l'IPL
PORT	Numéro de port
PRTERRMSG	Message d'erreur d'impression
PUBLISHINF	Données de publication
RMTLOCNAME	Emplacement distant
SEPDRAWER	Tiroir de séparateur
SEPPGM	Programme de séparateur
SWTLINLST	Liste de ligne commutée
SYSDRVPGM	Programme de pilote système
TEXT	Description textuelle
TRANSFORM	Transformation d'imprimante hôte
USRDFNOBJ	Objet défini par l'utilisateur
USRDFNOPT	Options définies par l'utilisateur
USRDRVPGM	Programme de pilote défini par l'utilisateur
USRDTATFM	Programme de transformation de données
WSCST	Objet de personnalisation de poste de travail

*Tableau 31. Attributs contrôlables pour les descriptions de périphérique d'impression pour les imprimantes *VRT*

Nom de l'attribut	Description
CHRID	Identificateur de caractères
FORMFEED	Alimentation papier
IGCFEAT	Fonction DBCS
IMGCFG	Configuration d'image
MAXLENRU	Longueur maximale de l'unité de requête
MFRTYPMDL	Type et modèle de fabricant

*Tableau 31. Attributs contrôlables pour les descriptions de périphérique d'impression pour les imprimantes *VRT (suite)*

Nom de l'attribut	Description
MSGQ	File d'attente de messages
ONLINE	En ligne à l'IPL
PRTERRMSG	Message d'erreur d'impression
PUBLISHINF	Données de publication
SEPDRAWER	Tiroir de séparateur
SEPPGM	Programme de séparateur
TEXT	Description textuelle
TRANSFORM	Transformation d'imprimante hôte
USRDFNOBJ	Objet défini par l'utilisateur
USRDFNOPT	Options définies par l'utilisateur
USRDRVPGM	Programme de pilote défini par l'utilisateur
USRDTAFM	Programme de transformation de données
WSCST	Objet de personnalisation de poste de travail
SEPPGM	Programme de séparateur
SWTLINLST	Liste de ligne commutée
SYSDRVPGM	Programme de pilote système
TEXT	Description textuelle
TRANSFORM	Transformation d'imprimante hôte
USRDFNOBJ	Objet défini par l'utilisateur
USRDFNOPT	Options définies par l'utilisateur
USRDRVPGM	Programme de pilote défini par l'utilisateur
USRDTATFM	Programme de transformation de données
WSCST	Objet de personnalisation de poste de travail

Tableau 32. Attributs contrôlables pour des descriptions de sous-système

Nom de l'attribut	Description
AJE	Poste de travail à démarrage automatique
CMNE	En ligne à l'IPL
JOBQE	File d'attente de travaux
MAXJOBS	Nombre maximal de travaux
PJE	Poste de travail à démarrage anticipé
RMTLOCNAME	Poste nom de lieu éloigné
RTGE	Entrée de routage
SGNDSPF	Affichage d'ouverture de session
SYSLIBLE	Bibliothèque de sous-système
TEXT	Description textuelle
WSNE	Entrée du nom de poste de travail
WSTE	Entrée du type de poste de travail

Tableau 33. Attributs contrôlables pour des variables d'environnement système

Toutes les variables d'environnement de niveau *SYS peuvent être contrôlées. L'attribut et le nom de ressource sont identiques au nom de la variable d'environnement.
Remarque : chaque variable d'environnement est traitée comme sa propre entrée de ressource contrôlée. Pour ceux-ci, le type de ressource et les noms d'attributs sont identiques.

Tableau 34. Attributs contrôlables pour des valeurs système

Nom de l'attribut	Description
QACGLVL	Niveau comptable
QACTJOBITP	Autorisation d'interruption des travaux
QALWOBJRST	Empêche quiconque de restaurer un objet d'état système ou un objet avec des droits d'adoption
QALWUSRDMN	Autorise les objets du domaine utilisateur
QASTLVL	Niveau d'assistance
QATNPGM	Programme de gestion de la touche ATTN
QAUDCTL	Contrôle d'audit
QAUDENDACN	Action d'erreur du journal d'audit
QAUDFRCLVL	Niveau de force de l'audit
QAUDLVL	Niveau de l'audit
QAUDLVL2	Extension du niveau de l'audit
QAUTOCFG	Configuration d'une unité automatique
QAUTORMT	Contrôleurs et unités éloignés
QAUTOVRT	Configuration d'une unité virtuelle automatique
QCCSID	ID jeu de caractères codés
QCFGMSGQ	File d'attente de messages pour les lignes, les contrôleurs et les unités
QCHRID	Jeu de caractères et page de codes d utilisés pour l'affichage et l'impression de données
QCHRIDCTL	Contrôle de l'identificateur de caractères pour le travail
QCMNRCYLMT	Récupération d'une erreur de communication automatique
QCNTRYID	Identificateur pays ou région
QCRTAUT	Droits pour les nouveaux objets
QCRTOBJAUD	Audit de nouveaux objets
QCTLSBSD	Contrôle d'un sous-système ou d'une bibliothèque
QCURSYM	Symbole monétaire
QDATFMT	Format de date
QDATSEP	Séparateur de date
QDBRCVYWT	Attente de restauration de la base de données avant l'exécution du redémarrage
QDECFMT	Format décimal
QDEVNAMING	Convention d'appellation des unités
QDEVRCYACN	Action de reprise d'unité
QDSCJOBITV	Intervalle de délai d'attente pour les travaux déconnectés

Tableau 34. Attributs contrôlables pour des valeurs système (suite)

Nom de l'attribut	Description
QDSPSGNINF	Contrôle l'affichage des informations de connexion
QENDJOBLMT	Temps maximal pour la fin immédiate
QFRCCVNRST	Restauration forcée de la conversion
QHSTLOGSIZ	Taille du fichier historique
QIGCCDEFNT	Nom de la police codée
QIGCFNTSIZ	Taille de la police codée
QINACTITV	Intervalle de délai d'attente du travail inactif
QINACTMSGQ	Action de l'intervalle du délai d'attente
QIPLTYPE	Type de redémarrage
QJOBMSGQFL	Action complète de la file d'attente de messages du travail
QJOBMSGQMX	Taille maximale de la file d'attente de messages du travail
QJOBMSGQSZ	Taille initiale de la file d'attente de messages du travail e, kilo-octets (ko)
QJOBMSGQTL	Taille maximale de la file d'attente de messages du travail (en ko)
QJOBSPLA	Taille initiale du bloc de contrôle de spoulage pour un travail (en octets)
QKBDBUF	Mémoire tampon de frappe
QKBDTYPE	Jeu de caractères de la langue du clavier
QLANGID	Identificateur de langue par défaut
QLIBLCKLVL	Verrouillage de bibliothèques dans la liste des bibliothèques d'un travail
QLMTDEVSSN	Limitation des sessions d'unités
QLMTSECOFR	Limitation de l'accès aux unités du responsable de la sécurité
QLOCALE	Environnement local
QLOGOUTPUT	Génération de la sortie imprimante pour l'historique de travail
QMAXACTLVL	Niveau d'activité maximal du système
QMAXJOB	Nombre maximal de travaux autorisés sur le système
QMAXSGNACN	Réponse du système lorsque la limite imposée par la valeur système QMAXSIGN est atteinte
QMAXSIGN	Nombre maximum de tentatives de connexion valides autorisé
QMAXSPLF	Nombre maximum de fichiers de sortie imprimante
QMLTTHDACN	Lorsqu'une fonction dans un travail à unités d'exécutions multiples n'autorise pas les unités d'exécution multiples
QPASTHRSVR	Travaux de serveur passe-système disponibles
QPRBFTR	Filtre d'historique des incidents
QPRBHLDITV	Conservation minimum
QPRTDEV	Imprimante par défaut

Tableau 34. Attributs contrôlables pour des valeurs système (suite)

Nom de l'attribut	Description
QPRTKEYFMT	Format de touche d'impression
QPRTTXT	Jusqu'à 30 caractères de texte peuvent être imprimés au bas des listes et des pages intercalaires
QPWDCHGBLK	Délai minimum entre les modifications de mot de passe
QPWDEXPITV	Nombre de jours qu'un mot de passe est valide
QPWDEXPWRN	Système d'intervalle d'avertissements d'expiration de mot de passe
QPWDLMTACJ	Limite l'utilisation de numéros adjacents dans un mot de passe
QPWDLMTCHR	Limite l'utilisation de certains caractères dans un mot de passe
QPWDLMTREP	Limite l'utilisation répétée de caractères dans un mot de passe
QPWDLVL	Niveau de mot de passe
QPWDMAXLEN	Nombre maximum de caractères dans un mot de passe
QPWDMINLEN	Nombre minimum de caractères dans un mot de passe
QPWDPOSDIF	Contrôle la position des caractères dans un nouveau mot de passe
QPWDRQDDGT	Nombre requis dans un nouveau mot de passe
QPWDRQDDIF	Contrôle si le mot de passe doit être différent des mots de passe précédents
QPWDRULES	Règles de mot de passe
QPWDVLDPGM	Programme d'approbation de mot de passe
QPWRDWNLMT	Délai fixé pour une mise hors tension immédiate
QRCLSPLSTG	Apurer automatiquement la mémoire affectée aux sorties imprimante inutilisée
QRETSVRSEC	Conservation de l'indicateur des données sur la sécurité du serveur
QRMTSIGN	Connexion éloignée
QRMTSRVATR	Attribut de service distant
QSCANFS	Analyse des systèmes de fichiers
QSCANFSCTL	Contrôler l'analyse
QSCPFCONS	Incident de la console
QSECURITY	Niveau de sécurité du système
QSETJOBATR	Définir les attributs du travail
QSFWERRLOG	Journal d'erreurs logicielles
QSHRMEMCTL	Autoriser l'utilisation de la mémoire partagée ou mappée avec possibilité d'écriture
QSPCENV	Environnement utilisateur par défaut
QSPLFACN	Action du fichier spoule
QSRTSEQ	Séquence de tri
QSRVDMP	Consigner les messages d'arrêt programme non interceptés

Tableau 34. Attributs contrôlables pour des valeurs système (suite)

Nom de l'attribut	Description
QSSLCSL	Liste de spécifications du chiffrement SSL
QSSLCSLCTL	Contrôle du chiffrement SSL
QSSLPCL	Protocoles SSL (Secure Sockets)
QSTRUPPGM	Définir le programme de démarrage
QSTSMSG	Affichage des messages d'état
QSYSLIBL	Liste des bibliothèques système
QTIMSEP	Séparateur horaire
QTSEPOOL	Indique si les travaux interactifs doivent être déplacés vers un autre pool de mémoire principale à la fin de la tranche de temps impartie
Remarque : chaque valeur système est traitée comme sa propre entrée de ressource contrôlée. Pour ceux-ci, le type de ressource et les noms d'attributs sont identiques.	

Tableau 35. Attributs contrôlables pour des descriptions d'unité de bande

Nom de l'attribut	Description
ASSIGN	Attribution de l'unité à la mise en fonction
MSGQ	File d'attente de messages
ONLINE	En ligne à l'IPL
RSRCNAME	Nom de ressource
TEXT	Description textuelle
UNLOAD	Déchargement de l'unité à la mise hors fonction

Tableau 36. Attributs contrôlables pour des descriptions d'anneau à jeton

Nom de l'attribut	Description
ACTLANMGR	Activation du gestionnaire LAN
ADPTADR	Adresse d'adaptateur local
AUTOCRTCTL	Création automatique de contrôleur
AUTODLTCTL	Suppression automatique de contrôleur
CMNRCYLMT	Nombre maximal de reprises
COSTBYTE	Coût relatif par octet pour l'envoi et la réception de données sur la ligne
COSTCNN	Coût relatif de la connexion sur la ligne
DUPLEX	Duplex
ELYTKNRLS	Libération anticipée du jeton
FCNADR	Adresse fonctionnelle
LINESPEED	Débit de ligne
LINKSPEED	Débit de liaison
LOGCFGCHG	Modification de configuration de l'historique
MAXCTL	Nombre maximal de contrôleurs
MAXFRAME	Longueur d'armoire maximale
MSGQ	File d'attente de messages

Tableau 36. Attributs contrôlables pour des descriptions d'anneau à jeton (suite)

Nom de l'attribut	Description
ONLINE	En ligne à l'IPL
PRPDLY	Temps de propagation
RSRCNAME	Nom de ressource
SECURITY	Sécurité pour la ligne
SSAP	Liste des informations sur le SAP source (SSAP)
TRNINFBDN	Notification d'alarme par le réseau en anneau à jeton
TRNLOGLVL	Niveau de consignation du gestionnaire de réseau en anneau à jeton
TRNMGRMODE	Mode du gestionnaire du réseau en anneau à jeton
TEXT	Texte descriptif de la ligne à anneau à jeton
USRDFN1	Défini par l'utilisateur en premier
USRDFN2	Défini par l'utilisateur en deuxième
USRDFN3	Défini par l'utilisateur en troisième
VRYWAIT	Attente de mise en fonction

Tableau 37. Attributs contrôlables pour des attributs TCP/IP

Nom de l'attribut	Description
ARPTIMO	Délai d'attente de mise en mémoire cache pour le protocole de résolution d'adresse
ECN	Activation de la fonction ECN (Explicit Congestion Notification)
IP6TMPAXP	Préfixe exclu de l'adresse temporaire IPv6
IPDEADGATE	IP détection de passerelle inactive
IPDTGFWD	Réacheminement des datagrammes IP
IPPATHMTU	Reconnaissance des unités de transmission maximales du chemin
IPQOSBCH	Lots de datagramme de qualité de service IP
IPQOSENB	Intégration de QoS IP
IPQOSTMR	Résolution du temporisateur de QoS IP
IPRSBTIMO	Délai de réassemblage IP
IPSRCRTG	Réacheminement source IP
IPTTL	Durée de vie IP (nombre de sauts)
LOGPCLERR	Consignation des erreurs de protocole
NFC	Cache du fichier réseau
TCPCLOTIMO	Délai du temps-attente du protocole TCP
TCPCNNMSG	Message de connexion fermée du protocole TCP
TCPKEEPALV	Maintien de la connexion TCP
TCPMINRTM	Temps de retransmission minimal du protocole TCP
TCPR1CNT	Comptage de retransmission R1 TCP
TCPR2CNT	Comptage de retransmission R2 TCP
TCPRCVBUF	Taille de la mémoire tampon de réception TCP

Tableau 37. Attributs contrôlables pour des attributs TCP/IP (suite)

Nom de l'attribut	Description
TCPSNDBUF	Taille de la mémoire tampon d'envoi TCP
TCPURGPTR	Pointeur d'urgence TCP
UDPCKS	Total de contrôle UDP
Remarque : chaque attribut TCP/IP est traité comme sa propre entrée de ressource contrôlée. Pour ceux-ci, le type de ressource et les noms d'attributs sont identiques.	

Tableau 38. Attributs contrôlables pour des profils utilisateur

Nom de l'attribut	Description
ACGCDE	Code comptabilité
ASTLVL	Niveau d'assistance
ATNPGM	Programme de gestion de la touche ATTN
CCSID	ID jeu de caractères codés
CHRIDCTL	Contrôle d'identificateur de caractères
CNTRYID	Identificateur pays ou région
CURLIB	Bibliothèque en cours
DLVRY	Livraison
DSPSGNINF	Affichage des informations de connexion
GID	Numéro d'ID groupe
GRPAUT	Droits du groupe
GRPAUTTYP	Type de droits du groupe
GRPPRF	Profil de groupe
HOMEDIR	Répertoire initial
INLMNU	Menu initial
INLPGM	Programme d'initialisation à appeler
JOBD	Description de travail
KBDBUF	Mémoire tampon de frappe
LANGID	Identificateur de langue
LCLPWDMGT	Gestion du mot de passe local
LMTCPB	Limitation des fonctions
LMTDEVSSN	Limitation des sessions d'unités
LOCALE	Environnement local
MAXSTG	Taille maximale autorisée de la mémoire
MSGQ	File d'attente de messages
OUTQ	File d'attente en sortie
OWNER	Propriétaire
PASSWORD	Mot de passe de l'utilisateur
PRTDEV	Imprimante
PTYLMT	Priorité de planification la plus élevée
PWDEXP	Définition du mot de passe sur expiré
PWDEXPITV	Intervalle d'expiration du mot de passe

Tableau 38. Attributs contrôlables pour des profils utilisateur (suite)

Nom de l'attribut	Description
SETJOBATR	Attributs du travail local
SEV	Filtre du code de gravité
SPCAUT	Droits spéciaux
SPCENV	Environnement spécial
SRTSEQ	Séquence de tri
STATUS	Etat
SUPGRPPRF	Groupes additionnels
TEXT	Description textuelle
UID	Numéro d'ID utilisateur
USRCLS	Classe d'utilisateur
USREXPDATE	Date d'expiration de l'utilisateur
USREXPITV	Intervalle d'expiration de l'utilisateur
USROPT	Options de l'utilisateur

Affichage des messages des postes de ressource contrôlée

L'interface graphique des services-ressources de mise en grappe permet d'afficher les messages associés aux postes de ressource contrôlée.

Pour afficher et examiner les messages des postes de ressource contrôlée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page Services-ressources de mise en grappe, cliquez sur **Gestion des domaines d'administration** pour afficher la liste des domaines d'administration de grappe.
5. Dans la page Domaines d'administration, cliquez sur l'icône contextuelle en regard du domaine d'administration de grappe, puis sur **Entrées de ressources contrôlées**.

   Remarque : L'option **Entrées de ressources contrôlées** est uniquement disponible si le noeud que vous gérez fait partie du domaine d'administration de grappe. La liste en cours des types de ressource contrôlée s'affiche.
6. Dans la liste des types de ressource contrôlée, cliquez sur l'icône contextuelle en regard du nom puis sélectionnez **Attributs**. Le système affiche la liste des objets de poste de ressource contrôlée.
7. Cliquez sur l'icône contextuelle en regard de l'objet de poste de ressource contrôlée, par exemple un profil utilisateur ou une valeur système, puis sélectionnez **Affichage des valeurs**.

Chapitre 9. Gestion des disques commutés

Les disques commutés sont des pools de stockage sur disque indépendant qui ont été configurés dans le cadre d'un groupe de ressources en grappe d'unité. La propriété des données et des applications stockées dans un disque commuté peut être basculée vers d'autres systèmes qui ont été définis dans le groupe de ressources en grappe d'unité. La technologie de disque commuté fournit une haute disponibilité pendant des indisponibilités planifiées et d'autres non planifiées.

Mise hors fonction d'un pool de stockage sur disque

Vous pouvez sélectionner un pool de stockage sur disque indépendant pour le rendre indisponible (le mettre hors fonction). Il est alors impossible d'accéder aux unités de disques ou objets de ce pool ou de la base de données correspondante tant qu'il n'est pas remis en fonction. Le pool peut devenir de nouveau disponible sur le même système ou sur un autre système dans le domaine de reprise du groupe de ressources en grappe.

Important : Pour qu'un pool de stockage sur disque indépendant puisse être rendu indisponible, aucun travail ne peut détenir de réservations sur ce pool. Pour savoir comment déterminer si les travaux utilisent un pool de stockage sur disque indépendant et comment libérer les réservations de travail, reportez-vous à la rubrique relative à la libération de réservations de travail sur disque indépendant.

Lorsque vous rendez un pool de stockage sur disque UDFS indisponible à l'aide de System i Navigator, des messages exigeant une réponse dans l'interface en mode texte peuvent être générés. System i Navigator ne fournit aucune indication qu'un message est en attente.

Pour rendre indisponible un pool de stockage sur disque indépendant :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez la plateforme System i que vous souhaitez examiner, **Configuration et maintenance** → **Matériel** → **Unités de disques**.
3. Développez l'arborescence **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit de la souris sur le pool de stockage sur disque que vous souhaitez rendre indisponible et sélectionnez **Mise hors fonction**.
5. Dans la boîte de dialogue qui apparaît, cliquez sur **Mise hors fonction** pour rendre indisponible le pool de stockage sur disque.

Vous pouvez utiliser la commande VRYCFG (Changer l'état d'une configuration) dans l'interface en mode texte afin de rendre indisponible le pool de stockage sur disque.

Utilisez la commande DSPASPSTS (Affichage de l'état de l'ASP) pour identifier à quel stade du processus se trouve une étape.

Utilisez l'API QYASPCTLAA (Contrôle de l'accès à l'ASP) pour restreindre les processus ayant accès à l'ASP.

Utilisez l'API QYASSDMO (Lancement d'une opération de gestion de DASD) pour réduire le temps nécessaire pour rendre indisponible un pool de stockage sur disque.

Rendre votre matériel commutable

Dans un environnement à haute disponibilité i5/OS, vous devez rendre une unité d'extension externe commutable.

Quand vous utilisez des pools de stockage sur disque indépendant dans un environnement commutable, le matériel associé doit être autorisé à commuter également. En fonction de votre environnement, ceci peut inclure une armoire, des unités ou des processeurs d'entrée-sortie, et leurs ressources associées. Consultez les étapes suivantes qui s'appliquent à l'environnement commutable.

Rendre une armoire ou une unité commutable

Un pool de stockage sur disque indépendant peut contenir des unités de disque au sein de plusieurs unités d'extension. Si vous possédez une unité d'extension autonome qui contient des unités de disque incluses à un pool de stockage sur disque indépendant, vous devez autoriser l'unité d'extension à accorder l'accès aux autres systèmes. Cette opération revient à rendre commutable une unité d'extension. Si vous ne voulez pas que d'autres systèmes puissent accéder à l'unité d'extension autonome, vous devez rendre privé l'unité d'extension.

Pour rendre commutable une armoire ou une unité, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez le système que vous voulez examiner, **Configuration et maintenance** → **Matériel** → **Unités de disques** → **Par emplacement** et sélectionnez l'armoire ou l'unité de disque que vous voulez rendre commutable.
3. Cliquez avec le bouton droit sur une armoire ou une unité de disque mise en évidence et sélectionnez **Rendre commutable**.
4. Suivez les instructions qui s'affichent dans la boîte de dialogue.

Rendre commutable un processeur d'entrée-sortie

Pour autoriser la commutation d'un processeur d'entrée-sortie, le bus qui contient le processeur d'entrée-sortie qui contrôle les unités de disque à commuter doit être partagé par le noeud principal (propriété partagée). Le noeud de sauvegarde doit également utiliser le bus (utiliser le bus partagé). Voir Commutation dynamique des processeurs d'entrée-sortie entre les partitions pour de plus amples informations.

Pour exécuter cette tâche, vous devez posséder un profil utilisateur de type Outils de maintenance disposant de droits d'opérations ou d'administration sur la fonction de gestion des Partitions système des Outils de maintenance en mode dédié (DST). Pour plus d'informations sur l'obtention des droits sur les partitions logiques, voir la section relative à l'autorisation de partition logique.

Pour modifier le type de propriété d'un bus à l'aide de la fonction de gestion centralisée, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Sélectionnez la partition principale du système.
3. Développez **Configuration et maintenance** et sélectionnez **Partitions logiques**.
4. Cliquez avec le bouton droit sur la **partition logique** et sélectionnez **Configuration des partitions**.
5. Dans la fenêtre Configuration des partitions logiques, cliquez avec le bouton droit sur le bus pour lequel vous voulez modifier la propriété et sélectionnez **Propriétés**.
6. Sélectionnez la page **Partitions**.

7. Sélectionnez la partition qui détient le bus dans **Partition logique propriétaire**, puis sélectionnez le type de propriété dans **Partage**. Si le type de propriété est partagé, les partitions qui partagent le bus apparaissent dans la liste. Cliquez sur Aide si vous avez besoin de plus amples informations sur ces options.
8. Cliquez sur **OK**.

Rendre commutable un pool d'E-S avec la console HMC

Si vous utilisez la console HMC pour gérer vos partitions logiques, vous devez créer un pool d'entrée-sortie qui inclut le processeur d'entrée-sortie, l'adaptateur d'entrée-sortie et toutes les ressources connectées pour qu'un pool de stockage sur disque indépendant soit commutable entre plusieurs partitions. Vous devez accorder l'accès à chaque partition pour laquelle vous voulez posséder le pool de stockage sur disque indépendant en affectant le pool d'entrée-sortie dans chaque profil de partition.

Pour créer un pool d'entrée-sortie qui peut être commuté entre des partitions, procédez comme suit :
1. Ouvrez la fenêtre Propriétés du profil de partition logique pour modifier les propriétés et affecter des ressources à un pool d'entrée-sortie.
2. Cliquez sur l'onglet **E/S physique**.
3. Dans la colonne Unités d'entrée-sortie du profil, développez le bus qui contient le processeur d'entrée-sortie que vous voulez rendre commutable.
4. Sélectionnez le processeur d'entrée-sortie que vous voulez attribuer à un pool d'entrée-sortie. Le processeur d'entrée-sortie doit être *désiré* (aucune coche dans la colonne **Requis**).
5. Cliquez sur la colonne du pool d'entrée-sortie de sorte que le curseur apparaît dans la ligne du processeur d'entrée-sortie que vous voulez affecter à un pool d'entrée-sortie, et tapez le nombre du pool d'entrée-sortie.
6. Répétez ces étapes pour ajouter chaque adaptateur d'entrée-sortie et ressource sous le contrôle du processeur d'entrée-sortie au pool d'entrée-sortie.
7. Cliquez sur **OK**.

Association du pool d'entrée-sortie avec les partitions

Une fois les ressources ajoutées au pool d'entrée-sortie, complétez les étapes suivantes pour associer le pool d'entrée-sortie à chaque partition supplémentaire qui doit détenir le pool de stockage sur disque indépendant de l'environnement commutable.
1. Ouvrez la fenêtre Propriétés du profil de partition logique pour modifier les propriétés de chaque partition supplémentaire qui doit accéder au pool de stockage sur disque indépendant.
2. Cliquez sur l'onglet **E/S physique**.
3. Cliquez sur **Options avancées**.
4. Dans la fenêtre Pools d'entrée-sortie, de la zone **pools d'entrée-sortie à ajouter**, tapez le numéro du pool d'entrée-sortie vers lequel vous avez affecté les ressources que vous voulez commuter par le pool de stockage sur disque indépendant.
5. Cliquez sur **Ajout → OK**.

Pour que les modifications du pool d'entrée-sortie soit appliquées, complétez les étapes suivantes de chaque partition dont le profil a été modifié :
1. Arrêtez la partition. Voir Redémarrage et arrêt de i5/OS dans une partition logique.
2. Démarrez la partition logique en activant le profil de partition afin qu'il applique les modifications.

Concepts associés

Dynamically switching IOPs between partitions

Logical partition authority

I/O pool

Tâches associées

Changing partition profile properties

Activating the partition profile

Restarting and shutting down i5/OS™ in a logical partition.

Mise au repos d'un pool de stockage sur disque indépendant

Dans une solution à haute disponibilité i5/OS, les pools de stockage sur disque indépendant servent à stocker des applications et des données résilientes. Certaines fonctions système, comme la réalisation de sauvegardes, supposent l'interruption temporaire des modifications apportées aux données pendant l'opération.

Pour réduire le temps nécessaire pour mettre au repos un pool de stockage sur disque indépendant, vous pouvez mettre en attente des files d'attente de travaux par lots, arrêter certains sous-systèmes ou envoyer un message d'interruption à des utilisateurs interactifs pour leur demander de différer un nouveau travail.

Pour mettre au repos un pool de stockage sur disque indépendant, procédez comme suit :

Dans une interface de ligne de commande, entrez la commande suivante : CHGASPACT ASPDEV(name) OPTION(*SUSPEND) SSPTIMO(30) SSPTIMOACN(*CONT),, où *name* est le nom du pool de stockage sur disque indépendant à interrompre. Dans cette commande, vous indiquez que le pool de stockage sur disque indépendant doit être interrompu avec un délai d'attente de 30 secondes et que l'étape suivante doit être effectuée si ce temps est dépassé.

Reprise d'un pool de stockage sur disque indépendant

Après avoir mis au repos un pool de stockage sur disque indépendant dans un environnement à haute disponibilité i5/OS pour des opérations de sauvegarde, vous devez reprendre ce pool afin de mettre à jour les modifications apportées aux données pendant la mise au repos.

Procédez comme suit pour reprendre un pool de stockage sur disque indépendant :

Dans une interface de ligne de commande, entrez la commande suivante : CHGASPACT ASPDEV(name) OPTION(*RESUME),, où `name` est le nom du pool de stockage sur disque indépendant que vous voulez reprendre.

Chapitre 10. Gestion de la protection par disque miroir d'un site à l'autre

Vous pouvez gérer trois technologies de protection par disque miroir d'un site à l'autre : géographique, Metro Mirror et Global Mirror. Ces technologies permettent une reprise après incident en copiant les données vitales d'unités de disques sur le site de production sur des unités de disques à l'emplacement de sauvegarde.

Gestion de la protection géographique par disque miroir

Utilisez les informations suivantes pour gérer la protection géographique par disque miroir. La protection géographique par disque miroir est une sous-fonction de la protection par disque miroir d'un site à l'autre, dans laquelle les données sont protégées par disque miroir dans des pools de stockage sur disque indépendant dans un environnement i5/OS.

Suspension de la protection géographique par disque miroir

Si pour une raison quelconque, vous devez mettre fin aux communications TCP, par exemple pour mettre le système en état restreint, vous devez au préalable suspendre la protection géographique par disque miroir. Cette action arrête temporairement la protection par disque miroir entre les systèmes d'une solution à haute disponibilité.

Lorsque vous suspendez la protection par disque miroir, les modifications apportées à la copie de production du pool de stockage sur disque indépendant ne sont pas transmises à la copie miroir.

Remarque : Lorsque vous reprenez la protection géographique par disque miroir, une synchronisation est requise entre les copies de production et miroir. Si la protection géographique par disque miroir a été suspendue sans suivi, une synchronisation complète a lieu. La procédure peut être longue.

Interruption de la protection géographique par disque miroir quand IBM PowerHA for i est installé

Pour interrompre la protection géographique par disque miroir avec IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez la copie de production du **pool de stockage sur disque** que vous souhaitez suspendre.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session que vous souhaitez suspendre.
8. Dans le menu **Sélection d'une action**, sélectionnez **Interruption avec suivi** ou **Interruption sans suivi**.

Interruption de la protection géographique par disque miroir quand IBM PowerHA for i n'est pas installé

Pour suspendre la protection géographique par disque miroir avec System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).

2. Développez le système possédant la copie de production du pool de stockage sur disque qui fait l'objet de la protection géographique par disque miroir et que vous souhaitez suspendre.
3. Développez **Configuration et maintenance** → **Matériel** → **Unités de disque** → **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit de la souris sur la copie de production du **pool de stockage sur disque** à suspendre, puis sélectionnez **Protection géographique par disque miroir** → **Suspension de la protection géographique par disque miroir**.

Si vous demandez une suspension avec suivi, le système tente de suivre les modifications apportées aux pools concernés. Cette option peut réduire la durée de la synchronisation puisque seule une synchronisation partielle est exécutée lors de la reprise de la protection géographique par disque miroir. Toutefois, si l'espace de suivi est saturé, une synchronisation complète est obligatoire lors de la reprise de la protection géographique par disque miroir.

Remarque : Si vous demandez une suspension sans suivi des modifications, lorsque vous reprenez la protection géographique par disque miroir, une synchronisation complète est requise entre les copies de production et miroir. Si vous suspendez la protection géographique en demandant le suivi des modifications, seule une synchronisation partielle est requise. La synchronisation complète peut être un processus très long (plusieurs heures). La durée de synchronisation dépend de la quantité de données synchronisées, de la vitesse des connexions TCP/IP et du nombre de lignes de communication utilisées pour la protection géographique par disque miroir.

Reprise de la protection géographique par disque miroir

Si vous interrompez la protection géographique par disque miroir, vous devez la reprendre pour activer à nouveau la protection par disque miroir entre les copies de production et en miroir.

Remarque : Lorsque vous reprenez la protection géographique par disque miroir, les copies de production et en miroir sont synchronisées en parallèle. Le processus de synchronisation peut s'avérer long. Si un pool de stockage sur disque qui devient indisponible interrompt la synchronisation, celle-ci continue depuis ce point lorsque le pool redevient disponible. Lorsqu'une synchronisation interrompue se poursuit, le premier message (CPI0985D) signale qu'elle est à 0 %.

Reprise de la protection géographique par disque miroir quand IBM PowerHA for i est installé

Pour redémarrer la protection géographique par disque miroir avec IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez la copie de production du **pool de stockage sur disque** à reprendre.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session à reprendre.
8. Dans le menu **Sélection d'une action**, sélectionnez **Reprise**.

Reprise de la protection géographique par disque miroir quand IBM PowerHA for i n'est pas installé

Pour reprendre la protection géographique par disque miroir avec System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez **Mes connexions** (ou votre environnement actif).

2. Développez le système possédant la copie de production du pool de stockage sur disque pour lequel vous voulez reprendre la protection géographique par disque miroir.
3. Développez **Configuration et maintenance** → **Matériel** → **Unités de disque** → **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit sur le **pool de stockage sur disque** que vous voulez reprendre et sélectionnez **Protection géographique par disque miroir** → **Reprise de la protection géographique par disque miroir**.

Déconnexion de la copie miroir

Si vous utilisez une protection géographique par disque miroir et que vous voulez accéder à la copie miroir pour sauvegarder des opérations ou des explorations de données ou pour créer des rapports, vous devez déconnecter la copie miroir de la copie de production.

Vous pouvez déconnecter la copie miroir en accédant à la copie de production du pool de stockage sur disque.

Déconnexion de la copie miroir quand IBM PowerHA for i est installé

Pour déconnecter la copie miroir à l'aide de IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où `monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez la copie de production du **Pool de stockage sur disque** que vous voulez déconnecter.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session que vous voulez déconnecter.
8. Dans le menu **Sélection d'une action**, sélectionnez **Déconnexion avec suivi** ou **Déconnexion sans suivi**.

Déconnexion de la copie miroir quand IBM PowerHA for i n'est pas installé

Nous vous conseillons de rendre le pool de stockage de disque indépendant indisponible pour vous assurer que la copie de production ne sera pas modifiée quand la déconnexion sera effectuée.

Pour déconnecter la copie miroir à l'aide de System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez le système qui détient la copie de production du pool de stockage de disque à partir duquel vous voulez déconnecter la copie miroir.
3. Développez **Configuration et maintenance** → **Matériel** → **Unités de disque** → **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit de la souris sur la copie de production du **Pool de stockage sur disque** que vous voulez déconnecter et sélectionnez **Protection géographique par disque miroir** → **Déconnexion de la copie en miroir**.

Si les options **Protection géographique par disque miroir** → **Déconnexion de la copie en miroir** sont grisées ou désactivées, la copie miroir n'est pas synchronisée avec la copie de production, la protection géographique disque miroir doit être reprise, le pool de stockage sur disque mis en fonction, et les copies de production et miroir synchronisées avant que la copie miroir puisse être déconnecté.

Avant de rendre disponible la copie miroir déconnectée, vous devriez créer une seconde description d'unité unique pour le pool de disque de stockage sur disque indépendant qui la différencie de la copie de production. Une description d'unité séparée pour la copie miroir évite l'existence de deux instances de la même base de données dans le réseau. Elle simplifiera également le travail effectué en dehors de System i Navigator. Utilisez la description d'unité de la copie miroir pour rendre disponible la copie miroir déconnectée.

Reconnexion d'une copie miroir

Si vous avez déconnecté une copie miroir et avez fini de l'utiliser, vous devez la reconnecter afin d'effectuer une reprise avec la protection géographique par disque miroir.

Vous reconnectez la copie miroir déconnectée en accédant à la copie de production du pool de stockage sur disque. La copie miroir déconnectée doit être indisponible lorsque vous la reconnectez à la copie de production.

Remarque : Lorsque vous reconnectez la copie miroir déconnectée, à partir de la version V6R1, vous pouvez choisir une déconnexion avec suivi, qui ne demandera qu'une synchronisation partielle au moment de la reconnexion.

Reconnexion de la copie miroir quand IBM PowerHA for i est installé

Pour reconnecter la copie miroir avec IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez la copie de production du **pool de stockage sur disque** que vous voulez reconnecter.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session à reconnecter.
8. Dans le menu **Sélection d'une action**, sélectionnez **Connexion**.

Reconnexion de la copie miroir quand IBM PowerHA for i n'est pas installé

Pour reconnecter la copie miroir avec System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez le système possédant la copie de production du pool de stockage sur disque auquel vous voulez reconnecter la copie miroir déconnectée.
3. Développez **Configuration et maintenance** → **Matériel** → **Unités de disque** → **Pools de stockage sur disque**.
4. Cliquez avec le bouton droit sur la copie de production du **pool de stockage sur disque** que vous voulez reconnecter et sélectionnez **Protection géographique par disque miroir** → **Reconnexion d'une copie en miroir**.

Annulation de la configuration de la protection géographique par disque miroir

Si vous ne voulez plus que la fonction utilise la protection géographique par disque miroir pour un pool de stockage sur disque spécifique ou un groupe de pools de stockage sur disque, vous pouvez sélectionner **Annulation de la configuration de la protection géographique par disque miroir**. Si vous annulez la configuration de la protection géographique par disque miroir, le système arrête la protection géographique par disque miroir et supprime la copie miroir des pools de stockage sur disque sur les noeuds du site de la copie miroir.

Le pool de stockage sur disque doit être déconnecté pour pouvoir annuler la configuration de la protection géographique par disque miroir.

Annulation de la configuration de la protection géographique par disque miroir quand IBM PowerHA for i est installé

Pour annuler la configuration de la protection géographique par disque miroir avec IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, saisissez **http://monsystème:2001**, où **monsystème** est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Développez le système que vous voulez examiner, cliquez sur **Configuration et maintenance** → **Pools de stockage sur disque**.
4. Fermez la session ASP ouverte pour la configuration de la protection géographique par disque miroir.
   a. Cliquez sur la flèche située en regard du pool de stockage sur disque dont vous voulez annuler la configuration. Sélectionnez **Session** → **Ouvrir...**
   b. Sélectionnez votre session ASP. Sélectionnez l'action Supprimer. Appuyez sur OK.
5. Annulation de la configuration de la protection géographique par disque miroir pour l'ASP
   a. Cliquez sur la flèche située en regard du pool de stockage sur disque dont vous voulez annuler la configuration. Sélectionnez **Session** → **Nouveau** → **Protection géographique par disque miroir** → **Annulation de la configuration de la protection géographique par disque miroir**.
   b. Cliquez sur Annuler la configuration dans l'écran de confirmation.
6. Mettez à jour la configuration de la grappe comme indiqué ci-après :
   a. Supprimé les noeuds associés à la copie miroir à partir du domaine de reprise du groupe de ressources en grappe d'unité.
   b. Supprimez le nom du site et les adresses IP du port de données à partir des noeuds restant dans la grappe.

Annulation de la configuration de la protection géographique par disque miroir quand IBM PowerHA for i n'est pas installé

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez le système que vous voulez examiner, **Configuration et maintenance** → **Matériel** → **Unités de disques** → **Pools de stockage sur disque**.
3. Cliquez avec le bouton droit de la souris sur la copie de production du **Pool de stockage sur disque** pour lequel vous voulez annuler la configuration et sélectionnez **Protection géographique par disque miroir** → **Annulation de la configuration de la protection géographique par disque miroir**.
4. Mettez à jour la configuration de la grappe comme indiqué ci-après :
   a. Supprimé les noeuds associés à la copie miroir à partir du domaine de reprise du groupe de ressources en grappe d'unité.
   b. Supprimez le nom du site et les adresses IP du port de données à partir des noeuds restant dans la grappe.

Tâches associées

«Suppression de noeuds», à la page 145
Vous devrez éventuellement supprimer un noeud d'une grappe si vous en effectuez la mise à niveau ou si le noeud ne doit plus prendre part à l'environnement à haute disponibilité i5/OS.

Modification des propriétés de la protection géographique par disque miroir

Vous pouvez modifier des informations associées à la protection géographique par disque miroir et changer les descriptions de copie associées.

Modification des propriétés de la protection géographique par disque miroir via IBM System Director Navigator for i5/OS

Pour modifier la session de protection géographique par disque miroir à l'aide d'IBM Systems Director Navigator for i5/OS, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session.
8. Dans le menu **Sélection d'une action**, sélectionnez **Propriétés**. Pour modifier la description d'une copie associée, sélectionnez la description de la copie et cliquez sur **Modification**.

Modification des propriétés de la protection géographique par disque miroir via System i Navigator

Pour modifier les propriétés de la protection géographique par disque miroir à l'aide de System i Navigator, procédez comme suit :

1. Dans System i Navigator, développez l'arborescence **Mes connexions** (ou votre environnement actif).
2. Développez le système qui stocke la copie de production du pool de stockage sur disque protégé géographiquement par disque miroir associé à la session de protection géographique par disque miroir pour laquelle vous voulez modifier les attributs,**Configuration et maintenance** → **Matériel** → **Unités de disque** → **Pools de stockage sur disque**.
3. Cliquez avec le bouton droit de la souris sur la copie de production du **Pool de stockage sur disque** pour lequel vous voulez modifier les attributs et sélectionnez **Sessions** → **Ouverture**.
4. Cliquez avec le bouton droit de la souris sur la copie de production de la **Session** pour laquelle vous voulez modifier les attributs et sélectionnez **Propriétés**. Pour modifier une description de copie associée, sélectionnez la description de copie et cliquez sur **Modification**.

Gestion des sessions Metro Mirror

Dans un environnement à haute disponibilité i5/OS qui utilise la technologie Metro MirrorIBM System Storage, vous devez configurer une session Metro Mirror entre les systèmes i5/OS et les unités de disque externes. Vous pouvez gérer ces sessions dans le système.

Suspension des sessions Metro Mirror

Il peut être nécessaire de suspendre les sessions Metro Mirror pour effectuer de la maintenance sur le système.

Pour suspendre une session Metro Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque que vous souhaitez suspendre.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.

7. Sélectionnez la session que vous souhaitez suspendre.
8. Sélectionnez **Suspension** dans le menu **Sélection d'une action**.

Reprise de sessions Metro Mirror

Après avoir effectué des opérations de routine, telle que la maintenance de votre système, vous devez reprendre une session Metro Mirror interrompue pour réactiver la haute disponibilité.

Pour reprendre une session Metro Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque interrompu.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session interrompue.
8. Dans le menu **Sélection d'une action**, sélectionnez **Reprise**.

Suppression d'une session Metro Mirror

Vous pouvez supprimer la session Metro Mirror afin de ne plus l'utiliser pour la haute disponibilité et la reprise après incident.

Pour supprimer une session metro Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans votre fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session que vous voulez supprimer.
6. Dans le menu **Sélection d'une action**, sélectionnez **Sessions**.
7. Sélectionnez la session que vous voulez supprimer.
8. Dans le menu **Sélection d'une action**, sélectionnez **Suppression**.

Affichage ou modification des propriétés de Metro Mirror

Affichez les informations sur une session Metro Mirror afin de modifier les descriptions de copies associées.

Pour modifier les propriétés de Metro Mirror à l'aide de IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.

7. Sélectionnez la session.
8. Dans le menu **Sélection d'une action**, sélectionnez **Propriétés**. Pour modifier la description d'une copie associée, sélectionnez la description de la copie et cliquez sur **Modification**.

Gestion de Global Mirror

Dans l'environnement à haute disponibilité i5/OS qui utilise la technologie Global MirrorIBM System Storage, vous devez configurer une session Global Mirror entre les systèmes i5/OS et les unités de disque externes. Vous pouvez gérer ces sessions dans le système.

Suspension des sessions Global Mirror

Il peut être nécessaire de suspendre les sessions Global Mirror pour effectuer de la maintenance sur le système.

Pour suspendre une session Global Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque que vous souhaitez suspendre.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session que vous souhaitez suspendre.
8. Sélectionnez **Suspension** dans le menu **Sélection d'une action**.

Reprise de sessions Global Mirror

Après avoir effectué des opérations de routine, telle que la maintenance de votre système, vous devez reprendre une session Global Mirror interrompue pour réactiver la haute disponibilité.

Pour reprendre une session Global Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque interrompu.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session interrompue.
8. Dans le menu **Sélection d'une action**, sélectionnez **Reprise**.

Suppression de sessions Global Mirror

Vous pouvez supprimer la session Global Mirror afin de ne plus l'utiliser pour la haute disponibilité et la reprise après incident.

Pour supprimer une session Global Mirror, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.

2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans votre fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session que vous voulez supprimer.
6. Dans le menu **Sélection d'une action**, sélectionnez **Sessions**.
7. Sélectionnez la session que vous voulez supprimer.
8. Dans le menu **Sélection d'une action**, sélectionnez **Suppression**.

Modification des propriétés d'une session Global Mirror

Affichez des informations relatives à une session Global Mirror pour modifier les descriptions de copie associées.

Pour modifier les propriétés de Global Mirror à l'aide de IBM Systems Director Navigator for i, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session.
8. Dans le menu **Sélection d'une action**, sélectionnez **Propriétés**. Pour modifier la description d'une copie associée, sélectionnez la description de la copie et cliquez sur **Modification**.

Gestion des unités logiques commutées (LUN)

Les unités logiques commutées sont des pools de stockage sur disque indépendant créés à partir des unités logiques créées dans un système IBM System Storage DS8000 ou DS6000 et configurées dans le groupe de ressources en grappe d'une unité.

La propriété des données et des applications stockées dans une unité logique commutée peut être basculée vers d'autres systèmes qui ont été définis dans le groupe de ressources en grappe de l'unité. La technologie de disque commuté fournit une haute disponibilité pendant des indisponibilités planifiées et d'autres non planifiées.

Mise à disposition des unités logiques commutées

Vous pouvez sélectionner un pool de stockage sur disque indépendant pour le rendre ou indisponible. Il est alors impossible d'accéder aux unités de disques ou objets de ce pool ou de la base de données correspondante tant qu'il n'est pas à nouveau disponible. Le pool peut devenir de nouveau disponible sur le même système ou sur un autre système dans le domaine de reprise du groupe de ressources en grappe.

Pour qu'un pool de stockage sur disque indépendant devienne indisponible, vous pouvez le désactiver. Il devient alors impossible d'accéder aux unités de disques ou aux objets de ce pool ou de la base de données correspondante tant qu'il n'est pas réactivé. Le pool peut devenir disponible sur le même système ou sur un autre système dans le domaine de reprise du groupe de ressources en grappe.

Mise au repos d'un pool de stockage sur disque indépendant

Dans une solution à haute disponibilité i5/OS, les pools de stockage sur disque indépendant servent à stocker des applications et des données résilientes. Certaines fonctions système, comme la réalisation de sauvegardes, supposent l'interruption temporaire des modifications apportées aux données pendant l'opération.

Pour réduire le temps nécessaire pour mettre au repos un pool de stockage sur disque indépendant, vous pouvez mettre en attente des files d'attente de travaux par lots, arrêter certains sous-systèmes ou envoyer un message d'interruption à des utilisateurs interactifs pour leur demander de différer un nouveau travail.

Pour mettre au repos un pool de stockage sur disque indépendant, procédez comme suit :

Dans une interface de ligne de commande, entrez la commande suivante : CHGASPACT ASPDEV(name) OPTION(*SUSPEND) SSPTIMO(30) SSPTIMOACN(*CONT),, où *name* est le nom du pool de stockage sur disque indépendant à interrompre. Dans cette commande, vous indiquez que le pool de stockage sur disque indépendant doit être interrompu avec un délai d'attente de 30 secondes et que l'étape suivante doit être effectuée si ce temps est dépassé.

Reprise d'un pool de stockage sur disque indépendant

Après avoir mis au repos un pool de stockage sur disque indépendant dans un environnement à haute disponibilité i5/OS pour des opérations de sauvegarde, vous devez reprendre ce pool afin de mettre à jour les modifications apportées aux données pendant la mise au repos.

Procédez comme suit pour reprendre un pool de stockage sur disque indépendant :

Dans une interface de ligne de commande, entrez la commande suivante : CHGASPACT ASPDEV(name) OPTION(*RESUME),, où `name` est le nom du pool de stockage sur disque indépendant que vous voulez reprendre.

Chapitre 11. Gestion de la fonction FlashCopy

FlashCopy est une technologie IBM System Storage qui vous permet de réaliser une copie instantanée des unités de disque externes. Dans les solutions à haute disponibilité i5/OS qui utilisent Metro ou Global Mirror, vous pouvez utiliser la fonction FlashCopy afin de réduire la fenêtre de sauvegarde en réalisant une copie de données qui peut ensuite être sauvegardée sur un support. Pour utiliser la fonction FlashCopy, vous devez créer une session entre le système et les unités de stockage externe.

Configuration d'une session FlashCopy

Pour les environnements à haute disponibilité i5/OS qui utilisent la technologie IBM System Storage, vous pouvez configurer une session FlashCopy pour créer une copie instantanée des données.

Pour plus d'informations sur l'utilisation de la fonction FlashCopy sur IBM System Storage DS8000, voir IBM System Storage DS8000 Information Center  .

Pour configurer une session FlashCopy, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque que vous voulez utiliser comme copie source.
6. Dans le menu **Sélection d'une action**, sélectionnez **Nouvelle session**.
7. Suivez les instructions de l'assistant pour compléter la tâche.

Mise à jour d'une session FlashCopy

Vous pouvez mettre à jour une session FlashCopy lors de la resynchronisation des volumes FlashCopy sur vos unités de stockage externe IBM System Storage. La resynchronisation vous permet de créer une copie sans recopier la totalité du volume. Ce processus est uniquement possible avec une relation permanente, par laquelle l'unité de stockage suit continuellement les mises à jour des volumes source et cible. Grâce aux relations permanentes, la relation entre les volumes source et cible est maintenue une fois la copie d'arrière-plan terminée. La session FlashCopy créée sur le système i5/OS fournit un moyen de gestion et de contrôle de l'activité liée à FlashCopy sur les unités IBM System Storage.

Pour mettre à jour une session FlashCopy, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session que vous voulez mettre à jour.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session que vous voulez mettre à jour.
8. Dans le menu **Sélection d'une action**, sélectionnez **Mise à jour FlashCopy**.

Reconnexion d'une session FlashCopy

Reconnectez une session FlashCopy.

Pour reconnecter une session FlashCopy, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session à reconnecter.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session à reconnecter.
8. Dans le menu **Sélection d'une action**, sélectionnez **Reconnexion**.

Déconnexion d'une session FlashCopy

Vous pouvez déconnecter les volumes cible à partir de la source d'une session FlashCopy sélectionnée.

Pour déconnecter des volumes cibles à partir de la source d'une session FlashCopy sélectionnée, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session que vous voulez déconnecter.
6. Dans le menu **Sélection d'une action**, sélectionnez **Sessions**.
7. Sélectionnez la session à partir de laquelle vous voulez déconnecter les volumes cibles et source.
8. Dans le menu **Sélection d'une action**, sélectionnez **Déconnexion de FlashCopy**.

Suppression d'une session FlashCopy

Supprimez une session FlashCopy.

Pour supprimer une session FlashCopy, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session que vous voulez supprimer.
6. Sélectionnez **Sessions** dans le menu **Sélection d'une action**.
7. Sélectionnez la session que vous voulez supprimer.
8. Dans le menu **Sélection d'une action**, sélectionnez **Suppression**.

Restauration des données à partir d'une session FlashCopy

A l'issue d'une session FlashCopy sur des unités IBM System Storage, vous pouvez restaurer ces données du volume cible vers le volume source en cas d'indisponibilité du système pour la copie source des données. Pour ce faire, vous devez inverser la session FlashCopy créée sur i5/OS. Le fait d'inverser la session copie des données de la cible vers la source et fait revenir la cible à une version antérieure.

Avertissement : L'inversion d'une session FlashCopy annule les modifications apportées à la copie source en copiant à nouveau les données de la cible dans la source. La source revient donc à un point antérieur dans le temps.

Pour inverser une session FlashCopy, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans la fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque de la copie source.
6. Dans le menu **Sélection d'une action**, sélectionnez **Open Sessions**.
7. Sélectionnez la session.
8. Dans le menu **Sélection d'une action**, sélectionnez **Reverse FlashCopy**.

Modification des propriétés FlashCopy

Affichez des informations relatives à une session FlashCopy pour modifier les descriptions de copie associées.

Pour modifier des informations relatives à une session FlashCopy, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Configuration et maintenance** dans votre fenêtre IBM Systems Director Navigator for i5/OS.
4. Sélectionnez **Pools de stockage sur disque**.
5. Sélectionnez le pool de stockage sur disque associé à la session
6. Dans le menu **Sélection d'une action**, sélectionnez **Sessions**.
7. Sélectionnez la session.
8. Dans le menu **Sélection d'une action**, sélectionnez **Propriétés**. Pour modifier une description de copie associée, sélectionnez la description de copie et cliquez sur **Modification**.

Chapitre 12. Identification et résolution des incidents d'une solution à haute disponibilité

Après avoir configuré une solution à haute disponibilité i5/OS, vous risquez de rencontrer des difficultés avec certaines technologies, dont les grappes et la fonction miroir entre sites.

Identification et résolution des incidents sur les grappes

Recherche de solutions de reprise sur incident pour les incidents propres aux grappes.

Il peut arriver parfois que la grappe ne fonctionne pas correctement. Cette rubrique donne des informations sur les incidents susceptibles de se produit sur les grappes.

Détermination de l'existence d'un incident sur une grappe

Commencez ici pour diagnostiquer les incidents sur les grappes.

Il peut arriver parfois que la grappe ne fonctionne pas correctement. Lorsque vous pensez avoir identifié un incident, suivez les étapes ci-après pour déterminer si c'est bien le cas et quelle est la nature de cet incident.

- **Déterminez si la mise en grappe est active sur le système.**

  Pour déterminer les services-ressources de mise en grappe sont actifs, recherchez les deux travaux QCSTCTL et QCSTCRGM dans la liste des travaux système. Si ces travaux sont actifs, c'est que les services-ressources de mise en grappe sont actifs. Vous pouvez utiliser la fonction Gestion des travaux dans IBM Director Navigator for i5/OS ou dans System i Navigator ou la commande WRKACTJOB (Gestion des travaux actifs) pour afficher les travaux. Vous pouvez également utiliser la commande DSPCLUINF (Affichage des informations de grappe) pour afficher des informations d'état relatives à la grappe.

  – D'autres travaux des services-ressources de mise en grappe peuvent également être actifs. La rubrique Cluster jobs fournit des informations sur le formatage des travaux des services-ressources de mise en grappe.

- **Déterminez la cause d'un message CPFBB26.**

```
Message . . . . : Cluster Resource Services not active or not responding.
Cause . . . . . : Les services-ressources de mise en grappe ne sont
pas actifs ou ne peuvent pas
répondre à cette demande parce qu'un ressource est indisponible ou
endommagée.
```

  Cette erreur peut vouloir dire soit que le travail du groupe de ressources en grappe n'est pas actif, soit que la grappe n'est pas active. Utilisez la commande DSPCLUINF (Affichage des informations de grappe) pour déterminer si le noeud est actif. Si ce n'est pas le cas, démarrez le noeud de grappe. S'il est actif, vous devez également vérifier le groupe de ressources en grappe pour déterminer s'il présente des erreurs.

  Recherchez le travail du groupe de ressources en grappe dans la liste des travaux système. Vous pouvez utiliser la fonction Gestion des travaux dans IBM Director Navigator for i5/OS or in System i Navigator ou la commande WRKACTJOB (Gestion des travaux actifs) pour afficher les travaux. Vous pouvez également utiliser la commande DSPCRGINF (Affichage des informations de groupe de ressources en grappe) pour afficher des informations d'état relatives au groupe, en indiquant le nom de ce dernier dans la commande. Si le travail du groupe de ressources en grappe n'est pas actif, recherchez l'historique du travail pour déterminer la cause de son arrêt. Une fois l'incident corrigé, redémarrez le travail du groupe de ressources en grappe avec la commande CHGCLURCY (Reprise de modification de grappe) ou en arrêtant puis en redémarrant la grappe sur ce noeud.

- **Recherchez les messages indiquant un incident.**
  - Assurez-vous que vous pouvez examiner tous les messages associés à une commande de grappe, en sélectionnant F10 qui alterne entre ″Include detailed messages″ et ″Exclude detailed messages″. Choisissez d'inclure tous les messages détaillés et passez-les en revue pour déterminer si d'autres actions sont nécessaires.
  - Recherchez dans QSYSOPR les messages d'interrogation qui attendent une réponse.
  - Recherchez dans QSYSOPR les messages d'erreur qui indiquent un incident de grappe. En général, ils sont compris dans la plage CPFBB00 à CPFBBFF.
  - Affichez l'historique de système (commande CL DSPLOG) pour rechercher les messages indiquant un incident de grappe. En général, ils sont compris dans la plage CPFBB00 à CPFBBFF.
- **Recherchez les erreurs graves dans les historiques de travail de grappe.**

  Ces travaux sont initialement définis avec le niveau de consignation (4 0 *SECLVL), pour vous permettre d'afficher les messages d'erreur nécessaires. Assurez-vous que le niveau de consignation approprié est défini pour ces travaux et les travaux du programme d'exit. Si la mise en grappe n'est pas active, vous pouvez quand même rechercher les fichiers spoule des travaux de grappe et du programme d'exit.
- **Si vous soupçonnez une erreur de type blocage, consultez les piles d'appel des travaux de grappe.**

  Déterminez si un programme se trouve dans un état de type DEQW (attente de suppression de file d'attente). Si c'est le cas, vérifiez la pile d'appel de chaque unité d'exécution et vérifiez la présence de getSpecialMsg.
- **Recherchez les éventuelles entrées de journal du microcode vertical sous licence (VLIC).**

  Ces entrées portent un code d'événement majeur 4800.
- **Utilisez la commande NETSTAT pour déterminer la présence d'anomalies dans l'environnement de communication.**

  NETSTAT renvoie des informations sur l'état des routes de réseau IP, des interfaces, des connexions TCP et des ports UDP sur le système.
  - Utilisez l'option 1 de Netstat (Work with TCP/IP interface status) pour vous assurer que les adresses IP choisies pour la mise en grappe indiquent un état 'Actif'. Assurez-vous aussi que l'adresse LOOPBACK (127.0.0.1) est également active.
  - Utilisez l'option 3 de Netstat (Work with TCP/IP Connection Status) pour afficher les numéros de port (F14). Le port local 5550 doit se trouver dans un état 'Ecoute'. Ce port doit être ouvert avec la commande STRTCPSVR *INETD mise en évidence par l'existence d'un travail QTOGINTD (QTCP utilisateur) dans la liste Travaux actifs. Si la mise en grappe est démarrée sur un noeud, le port local 5551 doit être ouvert et se trouver dans un état '*UDP'. Si la mise en grappe n'est pas démarrée, le port 5551 ne doit pas être ouvert sinon, il empêchera en fait le démarrage de la mise en grappe sur le noeud en question.
- Utilisez la commande PING pour vérifier s'il existe un problème de communication. Si vous tentez de démarrer un noeud de grappe et qu'il existe un problème de communication, vous recevez une erreur de mise en grappe interne (CPFBB46). Notez que la commande PING ne fonctionne pas entre une adresse IPv4 et une adresse IPv6 ou encore si un pare-feu la bloque.

Collecte d'informations de reprise pour une grappe

Vous pouvez utiliser la commande WRKCLU (Gestion de grappe) pour recueillir des informations complètes sur votre grappe. Ces informations peuvent servir à la résolution d'erreurs.

La commande WRKCLU (Gestion de grappe) permet d'afficher et d'utiliser les objets et les noeuds de grappe. Lorsque vous exécutez cette commande, l'écran de gestion de la grappe s'affiche. Outre l'affichage des noeuds d'une grappe et des informations de grappe, cette commande permet d'afficher les informations relatives à la grappe et de rassembler des données sur la grappe.

Pour recueillir des informations relatives à la reprise sur incident, procédez comme suit :

1. Dans une interface en mode texte, entrez `WRKCLU OPTION(OPTION)`. Vous pouvez définir les options suivantes pour indiquer les informations d'état de grappe que vous souhaitez utiliser.

   ***SELECT**
   Affiche le menu de gestion de la grappe.

   ***CLUINF**
   Affiche les informations sur la grappe.

   ***CFG** Affiche les paramètres de performance et de configuration de la grappe.

   ***NODE**
   Affiche le panneau de gestion des noeuds de grappe, lequel contient la liste des noeuds de la grappe.

   ***DEVDMN**
   Affiche le panneau de gestion des domaines d'unité, lequel contient la liste des domaines d'unité de la grappe.

   ***CRG** Affiche le panneau de gestion des groupes de ressources en grappe, lequel contient la liste des groupes de ressources en grappe de la grappe.

   ***ADMDMN**
   Affiche le panneau de gestion des domaines d'administration, lequel contient la liste des domaines d'administration de la grappe.

   ***SERVICE**
   Rassemble les informations de débogage et de trace pour tous les travaux du service-ressource de mise en grappe de la grappe. Ces informations sont écrites dans un fichier comportant un membre par travail du service-ressource de mise en grappe. Utilisez cette option uniquement lorsque votre fournisseur de services vous y invite. Elle affichera un panneau d'invite pour la commande DMPCLUTRC (Vidage des traces de la grappe).

Incidents courants sur les grappes

Recense les incidents les plus courants susceptibles de se produire dans une grappe, ainsi que les méthodes permettant de les éviter et de les corriger.

Il est facile d'éviter ou de corriger les incidents courants suivants.

Vous ne pouvez pas démarrer ou redémarrer un noeud de grappe

Cette situation est généralement due à un problème dans l'environnement de communication. Pour l'éviter, assurez-vous que vos attributs de réseau sont correctement définis, y compris l'adresse de bouclage, les paramètres INETD, l'attribut ALWADDCLU et les adresses IP pour les communications de grappe.

- L'attribut de réseau ALWADDCLU doit être défini de façon appropriée sur le noeud cible si vous essayez de démarrer un noeud distant. La valeur *ANY ou *RQSAUT doit lui être attribuée, en fonction de l'environnement.
- Les adresses IP choisies pour la mise en grappe locale et sur le noeud cible doivent présenter l'état *Actif*.
- L'adresse LOOPBACK (127.0.0.1) locale et sur le noeud cible doit également être active.
- Pour vérifier si le routage de réseau est actif, vous pouvez exécuter la commande PING avec les adresses IP utilisées pour la mise en grappe sur les noeuds distants et les noeud locaux. Notez toutefois que la commande PING ne fonctionne pas entre une adresse IPv4 et une adresse IPv6 ou encore si un pare-feu la bloque. Si un noeud de la grappe utilise une adresse IPv4, chaque noeud de la grappe doit posséder une adresse IPv4 active (pas nécessairement configurée comme adresse IP de grappe) permettant de router et d'envoyer des paquets TCP à cette adresse. De même, si un noeud de

la grappe utilise une adresse IPv6, chaque noeud de la grappe doit posséder une adresse IPv6 active (pas nécessairement configurée comme adresse IP de grappe) permettant de router et d'envoyer des paquets TCP à cette adresse.

- INETD doit être actif sur le noeud cible. Lorsqu'INETD est actif, le port 5550 sur le noeud cible doit être dans un état *Ecoute*. Reportez-vous au serveur INETD pour plus d'informations sur son démarrage.
- Avant toute tentative de démarrage d'un noeud, le port 5551 du noeud à démarrer ne doit pas être ouvert sinon, il empêchera en fait le démarrage de la mise en grappe sur le noeud en question.

Vous obtenez plusieurs grappes disjointes composées d'un seul noeud

Cela peut se produire lorsque le noeud en cours de démarrage ne peut pas communiquer avec les autres noeuds de la grappe. Vérifiez les chemins de communication.

Les programmes d'exit sont longs à réagir.

Cette situation est souvent due à un paramétrage incorrect de la description de travail utilisée par le programme d'exit. Il se peut que le paramètre MAXACT ait une valeur trop faible, de sorte, par exemple, qu'une seule instance du programme d'exit puisse être active à un moment donné. Il est recommandé d'attribuer la valeur *NOMAX à ce paramètre.

Les performances générales semblent lentes.

Ce symptômes peut avoir plusieurs causes courantes.

- La plus probable est un trafic de communication élevé sur une ligne de transmission partagée.
- Une autre cause possible est une incohérence entre l'environnement de communication et les paramètres d'optimisation des messages de la grappe. Vous pouvez utiliser l'API QcstRetrieveCRSInfo (Extraction d'informations des services-ressources de mise en grappe) pour afficher les valeurs en cours des paramètres d'optimisation et l'API QcstChgClusterResourceServices (Modification des services-ressources de mise en grappe) pour modifier ces valeurs. Les performances de grappe risquent d'être dégradées avec les valeurs par défaut des paramètres d'optimisation de grappe si vous utilisez une carte ancienne. Les types de cartes qui se qualifient comme *anciens* sont 2617, 2618, 2619, 2626 et 2665. Dans ce cas, il est souhaitable d'attribuer la valeur *Normal* au paramètre d'optimisation *Classe de performance*.
- Si tous les noeuds d'une grappe se trouvent sur un réseau local ou ont des fonctions d'acheminement qui peuvent traiter des tailles de paquets d'unité de transmission maximale (Maximum Transmission Unit, MTU) supérieures à 1 464 octets sur l'ensemble des routes réseau, les transferts de messages de grappe volumineux (supérieurs à 1 536 ko) peuvent être fortement accélérés grâce à l'augmentation de la valeur du paramètre d'optimisation de grappe de *Taille des fragments du message* afin de mieux s'adapter aux MTU de route.

Vous ne pouvez utiliser aucune fonction de la nouvelle édition.

Si vous tentez d'utiliser des fonctions de la nouvelle édition et que le message d'erreur CPFBB70 apparaît, c'est que la version en cours de la grappe est toujours définie au niveau de la version antérieure. Vous devez mettre à niveau tous les noeuds de grappe au niveau de la nouvelle édition, puis utilisez l'interface d'ajustement de la version de grappe pour définir la version en cours au nouveau niveau. Pour plus d'informations, reportez-vous à la rubrique relative à l'ajustement de la version d'une grappe.

Vous ne pouvez pas ajouter de noeud à un domaine d'unité ni accéder à l'interface de gestion de grappes de System i Navigator.

Pour accéder à l'interface de gestion de grappe de System i Navigator, ou utiliser des unités commutables, l'option 41 de i5/OS, HA Switchable Resources, doit être installée sur le système. Vous

devez également disposer d'une clé de licence valide pour cette option.

Vous avez appliqué une PTF de grappe mais elle ne semble pas fonctionner.

Vous devez vous assurer d'avoir effectué les tâches suivantes après l'application de la PTF :

1. Arrêt de la grappe
2. Déconnexion puis reconnexion

   L'ancien programme est toujours actif dans le groupe d'activation jusqu'à la destruction de ce dernier. Tout le code de gestion de grappe (même les API de grappe) est exécuté dans le groupe d'activation par défaut.
3. Démarrage de la grappe

   La plupart des PTF de grappe exigent l'arrêt de la mise en grappe et son redémarrage sur le noeud pour activer la PTF.

CEE0200 apparaît dans l'historique de travail du programme d'exit.

Dans ce message d'erreur, le module d'origine est QLEPM et la procédure d'origine est Q_LE_leBdyPeilog. Tout programme appelé par le programme d'exit doit être exécuté dans *CALLER ou dans un groupe d'activation nommé. Vous devez modifier le programme d'exit ou le programme qui présente l'erreur afin de corriger cette dernière.

CPD000D suivi de CPF0001 apparaît dans l'historique de travail des services-ressources de mise en grappe.

Lorsque vous recevez ce message d'erreur, assurez-vous que la valeur système QMLTTHDACN a la valeur 1 ou 2.

La grappe semble bloquée.

Assurez-vous que les programmes d'exit du groupe de ressources en grappe sont en attente. Pour vérifier le programme d'exit, utilisez la commande WRKACTJOB (Gestion des travaux actifs), puis recherchez PGM-QCSTCRGEXT dans la colonne Function.

Erreurs de partitionnement

Certaines erreurs de grappe sont faciles à corriger. Si un partitionnement de grappe s'est produite, vous pouvez apprendre à effectuer une reprise. Cette rubrique vous indique également comment éviter un partitionnement de grappe et donne un exemple de fusion des partitions.

Une partition se produit dans une grappe dès que le contact est perdu entre un ou plusieurs noeuds de la grappe, et qu'il est impossible de confirmer que les noeuds perdus sont en panne. Cette situation ne doit pas être confondue avec un partitionnement dans un environnement de partition logique (LPAR).

Si vous recevez le message d'erreur CPFBB20 dans l'historique de système (QHST) ou dans l'historique du travail QCSTCTL, une partition de grappe s'est produite et vous devez savoir comment procéder à la reprise. L'exemple suivant montre une partition de grappe impliquant une grappe composée de quatre noeuds : A, B, C et D. L'exemple dénote une perte de communication entre les noeuds de grappe B et C, ce qui entraîne la division de la grappe en deux partitions. Avant la partition, il y avait quatre groupes de ressources en grappe, qui peuvent être de n'importe quel type, appelées CRG A, CRG B, CRG C et CRG D. L'exemple indique le domaine de reprise de chaque groupe de ressources.

Tableau 39. Exemple de domaine de reprise au cours d'une partition de grappe

Noeud A	Noeud B	x	Noeud C	Noeud D
CRG A (secondaire1)	CRG A (principal)			
	CRG B (principal)		CRG B (secondaire1)	
	CRG C (principal)		CRG C (secondaire1)	CRG C (secondaire2)
CRG D (secondaire2)	CRG D (principal)		CRG D (secondaire1)	
Partition 1			**Partition 2**	

Une grappe peut être partitionnée si la MTU à un point quelconque du chemin de communication est inférieure à la taille du fragment de message du paramètre optimisable de communication de la grappe. La MTU pour une adresse IP de grappe peut être vérifiée à l'aide de la commande WRKTCPSTS (Gestion de l'état du réseau TCP/IP) sur le noeud sujet. La MTU doit également être vérifiée à chaque étape du chemin de communication. Si elle est inférieure à la taille du fragment de message, augmentez la MTU du chemin ou diminuez la taille du fragment. Vous pouvez utiliser l'API QcstRetrieveCRSInfo (Extraction d'informations des services-ressources de mise en grappe) pour afficher les valeurs en cours des paramètres d'optimisation et l'API QcstChgClusterResourceServices (Modification des services-ressources de mise en grappe) pour modifier ces valeurs.

Une fois la cause de l'erreur de partitionnement de grappe corrigée, la grappe détecte la liaison de communication rétablie et émet le message CPFBB21 dans l'historique de système (QHST) ou l'historique du travail QCSTCTL. L'opérateur est ainsi informé que la grappe a été reprise à partir de la partition de grappe. Sachez toutefois qu'une fois l'erreur corrigée, la fusion de la grappe peut prendre quelques minutes.

Détermination des partitions de grappe principale et secondaire

Pour déterminer les types d'actions de groupe de ressources en grappe que vous pouvez effectuer dans une partition de grappe, vous devez savoir s'il s'agit d'une partition de grappe principale ou secondaire. Lorsqu'une partition est détectée, elle est désignée comme principale ou secondaire pour chaque groupe de ressources en grappe défini dans la grappe.

Pour un modèle principal-secondaire, la partition principale contient le noeud dont le rôle en cours est principal. Toutes les autres partitions sont secondaires. La partition principale peut ne pas être la même pour tous les groupes de ressources en grappe.

Un modèle homologue obéit aux règles de partitionnement suivantes :

- Si les noeuds du domaine de reprise sont entièrement contenus dans une partition, il s'agi de la partition principale.
- Si les noeuds du domaine de reprise s'étendent sur deux partitions, il n'y a pas de partition principale. Les deux partitions sont des partitions secondaires.
- Si le groupe de ressources en grappe est actif et qu'il n'y a pas de noeud homologue dans la partition indiquée, le groupe de ressources en grappe est arrêté dans cette partition.
- Des modifications opérationnelles sont autorisées dans une partition secondaire du moment que les restrictions imposées soient respectées.
- Aucune modification de la configuration n'est autorisée dans une partition secondaire.

Les restrictions s'appliquant à chaque API de groupe de ressources en grappe sont les suivantes :

Tableau 40. Restrictions de partitionnement des API de groupe de ressources en grappe

API de groupe de ressources en grappe	Autorisée dans la partition principale	Autorisée dans les partitions secondaires
Ajout de noeud au domaine de reprise	X	

Tableau 40. Restrictions de partitionnement des API de groupe de ressources en grappe (suite)

API de groupe de ressources en grappe	Autorisée dans la partition principale	Autorisée dans les partitions secondaires
Ajout d'entrées d'unité à un groupe de ressources en grappe		
Modification d'un groupe de ressources en grappe	X	
Modification d'entrées d'unité d'un groupe de ressources en grappe	X	X
Création d'un groupe de ressources en grappe		
Suppression d'un groupe de ressources en grappe	X	X
Diffusion d'informations	X	X
Arrêt d'un groupe de ressources en grappe[1]	X	
Lancement de basculement	X	
Liste des groupes de ressources en grappe	X	X
Liste des informations relatives aux groupes de ressources en grappe	X	X
Suppression de noeud du domaine de reprise	X	
Suppression d'entrées d'unité d'un groupe de ressources en grappe	X	
Démarrage d'un groupe de ressources en grappe[1]	X	

Remarque :

1. Autorisé dans toutes les partitions pour les groupes de ressources en grape homologues, mais ne porte que sur la partition sur laquelle l'API est exécutée.

En appliquant ces restrictions, il est possible de synchroniser les groupes de ressources en grappe lorsque la grappe n'est plus partitionnée. Au fur et à mesure que des noeuds rejoignent la grappe à partir d'un état partitionné, la version du groupe de ressources en grappe dans la partition principale est copiée sur les noeuds provenant d'une partition secondaire.

Lors de la fusion de deux partitions secondaires pour le modèle homologue, c'est la partition dotée d'un groupe de ressources en grappe à l'état Actif qui l'emporte. Si les deux partitions ont le même état pour le groupe de ressources en grappe, c'est la partition qui contient le premier noeud répertorié dans le domaine de reprise du groupe de ressources en grappe qui l'emporte. La version du groupe de ressources en grappe dans la partition gagnante est copiée sur les noeud de l'autre partition.

Lorsqu'une partition est détectée, les API Ajout d'entrée noeud de grappe, Ajustement de la version de grappe et Création de grappe ne peuvent être exécutées dans aucune des partitions. L'API Ajout entrée domaine d'unité ne peut être exécutée que si aucun des noeuds du domaine d'unité n'est partitionné. Toutes les autres API de contrôle de grappe peuvent être exécutées dans n'importe quelle partition. Cependant, l'action effectuée par l'API ne prend effet que dans la partition qui exécute cette API.

Passage de noeuds partitionnés à l'état Echec

Il arrive qu'un erreur de partitionnement soit signalée alors qu'il s'agissait en réalité d'un noeud indisponible. Cela peut se produire lorsque les services-ressources de grappe perdent leurs communications avec un ou plusieurs noeuds, sans pouvoir détecter si ces noeuds sont toujours opérationnels. Lorsque cette condition se produit, un mécanisme simple vous permet d'indiquer que le noeud a échoué.

Avertissement : Lorsque vous informez les services-ressources de mise en grappe qu'un noeud a échoué, la reprise à partir de l'état de partition est plus simple. Cependant, l'état du noeud ne doit pas être modifié en Echec lorsque, en réalité, le noeud est toujours actif et qu'une véritable partition a été effectuée. En effet, cette modification risque d'attribuer à un noeud dans plusieurs partitions le rôle principal d'un groupe de ressources en grappe. Lorsque deux noeuds se considèrent respectivement comme noeud principal, certaines données (fichiers ou bases de données, par exemple) peuvent être disjointes ou endommagées si plusieurs noeuds effectuent chacun indépendamment des modifications sur des copies de leurs fichiers. En outre, les deux partitions ne peuvent pas être fusionnées de nouveau lorsqu'un noeud de chaque partition s'est vu affecter le rôle principal.

Lorsqu'un noeud passe à l'état Echec, il est possible de réordonner le rôle des noeuds dans le domaine de reprise pour chaque groupe de ressources en grappe de la partition. Le noeud passant à l'état Echec est affecté en tant que dernier noeud secondaire. Si plusieurs noeuds ont échoué et que leur état doit être modifié, l'ordre dans lequel les noeuds sont modifiés affectera l'ordre final des noeuds secondaires du domaine de reprise. Si le noeud ayant échoué était le noeud principal d'un groupe de ressources en grappe, le premier noeud secondaire actif sera réaffecté en tant que nouveau noeud principal.

Lorsque les services-ressources de mise en grappe ont perdu les communications avec un noeud mais ne peuvent pas détecter si ce dernier est toujours opérationnel, un noeud de grappe aura l'état **Non en cours de communication**. Vous devrez peut-être faire passer l'état du noeud de **Non en cours de communication** à **Echec**. Vous pourrez alors redémarrer le noeud.

Pour faire passer l'état d'un noeud de **Non en cours de communication** à **Echec**, procédez comme suit :

1. Dans un navigateur Web, entrez `http://monsystème:2001`, où`monsystème` est le nom d'hôte du système.
2. Connectez-vous au système avec votre profil utilisateur et votre mot de passe.
3. Sélectionnez **Services-ressources de mise en grappe** dans la fenêtre IBM Systems Director Navigator for i.
4. Dans la page **Services-ressources de mise en grappe**, sélectionnez la tâche **Gestion des noeuds de grappe** pour afficher une liste de noeuds de la grappe.
5. Cliquez sur le menu **Sélection d'une action** et sélectionnez l'option **Modification d'état**. Modifiez l'état du noeud en Echec.

Information associée

Change Cluster Node (CHGCLUNODE) command

Change Cluster Node Entry (QcstChangeClusterNodeEntry) API

Domaine d'administration de grappe partitionnés

Prenez en compte les informations suivantes lorsque vous travaillez avec des domaines d'administration de grappe partitionnés.

Si un domaine d'administration de grappe est partitionné, les modifications restent synchronisées parmi tous les noeuds actifs dans chaque partition. Lorsque les noeuds sont à nouveau fusionnés, le domaine d'administration de grappe propage toutes les modifications apportées dans chaque partition afin que les ressources soient cohérentes dans le domaine actif. Plusieurs remarques sont à prendre en compte pour le processus de fusion pour un domaine d'administration de grappe :

- Si toutes les partitions étaient actives et que des modifications ont été apportées à la même ressource dans différentes partitions, la modification la plus récente est appliquée à la ressource sur tous les noeuds lors de la fusion. Cette modification est identifiée à l'aide du temps universel coordonné de chaque noeud ayant subi un changement.
- Si toutes les partitions étaient inactives en revanche, les valeurs globales pour chaque ressource sont résolues en fonction de la dernière modification effectuée alors qu'aucune partition n'était active. L'application réelle de ces modifications n'a pas lieu tant que le groupe de ressources en grappe homologue représentant le domaine d'administration de grappe n'est pas démarré.

- Si certaines partitions étaient actives et d'autres inactives avant la fusion, les valeurs globales correspondant aux modifications apportées dans les partitions actives sont propagées aux partitions inactives. Ces dernières sont alors démarrées, ce qui entraîne la propagation au domaine fusionné des modifications en attente sur les noeuds des partitions inactives.

Conseils : Partitions de grappe

Utilisez les conseils suivants pour les partitions de grappe.

1. Les règles permettant de limiter les opérations dans une partition sont conçues pour faciliter la fusion des partitions. Sans ces restrictions, la reconstruction de la grappe est un travail de longue haleine.
2. Si les noeuds de la partition principale ont été détruits, un traitement spécial peut s'avérer nécessaire dans une partition secondaire. Le scénario le plus courant qui provoque cette condition est la perte du site ayant constitué la partition principale. Utilisez l'exemple de reprise des erreurs de partitionnement en partant de l'hypothèse que la partition 1 a été détruite. Dans ce cas, le noeud principal des groupes de ressources en grappe B, C et D doit être situé dans la partition 2. La reprise la plus simple consiste à utiliser la commande Modif. entrée noeud de grappe pour définir les noeuds A et B à l'état Echec. Pour plus d'informations, voir la section Passage de noeuds partitionnés à l'état Echec. La reprise peut également être effectuée manuellement. Pour ce faire, procédez comme suit :
   a. Supprimez les noeuds A et B de la grappe dans la partition 2. La partition 2 est maintenant la grappe.
   b. Définissez les environnements de réplication logique nécessaires dans la nouvelle grappe. Autrement dit, lancez l'API/commande CL Démarrage d'un groupe de ressources en grappe, etc.

   Comme les noeuds ont été supprimés de la définition de grappe dans la partition 2, toute tentative de fusion des partitions 1 et 2 est vouée à l'échec. Pour corriger la non concordance des définitions de grappe, exécutez l'API QcstDeleteCluster (Suppression de grappe) sur chaque noeud de la partition 1. Ajoutez ensuite les noeuds de la partition 1 à la grappe et rétablissez toutes les définitions de groupe de ressources en grappe, tous les domaines de reprise et la réplication logique. Cela exige beaucoup de travail et comporte un risque d'erreur. Il est très important de réserver cette procédure aux situations de perte de site.
3. Le traitement d'une opération de démarrage de noeud dépend de l'état du noeud démarré :

   Le noeud a échoué ou il a été arrêté :
   a. Les services-ressources de mise en grappe sont démarrés sur le noeud qui est ajouté
   b. La définition de grappe est copiée à partir d'un noeud actif dans la grappe vers le noeud en cours de démarrage.
   c. Le groupe de ressources en grappe qui contient le noeud démarré dans le domaine de reprise est copié à partir d'un noeud actif dans la grappe vers le noeud en cours de démarrage. Aucun groupe de ressources en grappe n'est copié à partir du noeud en cours de démarrage vers un noeud actif de la grappe.

   Le noeud est un noeud partitionné :
   a. La définition de grappe d'un noeud actif est comparée à celle du noeud en cours de démarrage. Si les définitions sont identiques, le démarrage continue en tant qu'opération de fusion. Si les définitions ne concordent pas, la fusion est arrêtée et l'utilisateur doit intervenir.
   b. Si la fusion continue, le noeud en cours de démarrage est défini à l'état Actif.
   c. Le groupe de ressources en grappe qui contient le noeud démarré dans le domaine de reprise est copié à partir de la partition principale vers la partition secondaire du groupe de ressources en grappe. Les groupes de ressources en grappe peuvent être copiés à partir du noeud en cours de démarrage vers des noeuds déjà actifs dans la grappe.

Reprise de grappe

Donne des informations sur la reprise après d'autres éventuels incidents sur une grappe.

Reprise après des échecs de travaux de mise en grappe

L'échec d'un travail de services-ressources de mise en grappe dénote généralement un autre incident.

Consultez l'historique associé au travail ayant échoué et recherchez les messages décrivant la cause de l'échec. Corrigez les éventuelles erreurs.

Vous pouvez utiliser la commande CHGCLURCY (Reprise de modification de grappe) pour relancer un travail de groupe de ressources en grappe sans avoir besoin d'arrêter et de redémarrer la mise en grappe sur un noeud.

1. `CHGCLURCY CLUSTER(EXAMPLE)CRG(CRG1)NODE(NODE1)ACTION(*STRCRGJOB)` Cette commande entraîne la soumission du travail de groupe de ressources en grappe, CRG1, sur le noeud NODE1. Le démarrage du travail de groupe de ressources en grappe sur NODE1 exige que la mise en grappe soit active sur NODE1.
2. Redémarrez la mise en grappe sur le noeud.

Si vous utilisez un produit de gestion de grappe d'un partenaire commercial IBM, reportez-vous à la documentation fournie avec ce produit.

Information associée

Change Cluster Recovery (CHGCLURCY) command

Reprise d'un objet de grappe endommagé

Bien qu'il soit peu probable que le cas se produite, il arrive que des objets des services-ressources de mise en grappe soient endommagés.

Le système, s'il s'agit d'un noeud actif, tente alors une reprise à partir d'un autre noeud actif de la grappe. Il procède aux étapes de reprise suivantes :

Pour un objet interne endommagé

1. Le noeud endommagé est arrêté.
2. S'il y a au moins un autre noeud actif dans la grappe, le noeud endommagé redémarre automatiquement et rejoint la grappe. La procédure d'ajout corrige la situation.

Pour un groupe de ressources en grappe endommagé :

1. Le noeud qui comporte un groupe de ressources en grappe endommagé fait échouer toute opération en cours associée à ce groupe. Le système tente alors une reprise automatique du groupe de ressources en grappe à partir d'un autre noeud actif.
2. S'il y a au moins un membre actif dans le domaine de reprise, la reprise du groupe de ressources en grappe aboutit. Sinon, le travail du groupe de ressources en grappe est arrêté.

Si le système ne parvient pas à identifier ou à atteindre un autre noeud actif, vous devrez effectuer ces étapes de reprise.

Pour un objet interne endommagé

Vous recevez une erreur de mise en grappe interne (CPFBB46, CPFBB47 ou CPFBB48).

1. Arrêtez la mise en grappe pour le noeud endommagé.
2. Relancez la mise en grappe pour le noeud endommagé, à partir d'un autre noeud actif dans la grappe.
3. Si les étapes 1 et 2 ne résolvent pas l'incident, supprimez le noeud endommagé de la grappe.
4. Rajoutez le système dans la grappe et dans le domaine de reprise des groupes de ressources en grappe appropriés.

Pour un groupe de ressources en grappe endommagé :

Vous recevez une erreur indiquant qu'un objet est endommagé (CPF9804).

1. Arrêtez la mise en grappe sur le noeud contenant le groupe de ressources en grappe endommagé.

2. Supprimez le groupe de ressources en grappe à l'aide de la commande DLTCRG.
3. Si aucun autre noeud n'est actif dans la grappe contenant l'objet de groupe de ressources en grappe, restaurez à partir du support.
4. Démarrez la mise en grappe sur le noeud contenant le groupe de ressources en grappe endommagé. La procédure peut être effectuée à partir de n'importe quel noeud actif.
5. Lorsque vous démarrez la mise en grappe, le système resynchronise tous les groupes de ressources en grappe. Il peut être nécessaire de recréer le groupe de ressources en grappe s'il n'est présent dans aucun autre noeud de la grappe.

Reprise d'une grappe après une perte totale de système

Utilisez ces informations avec la liste de contrôle appropriée de la rubrique relative à la récupération du système pour récupérer l'ensemble du système après une perte totale lorsque l'alimentation du système est coupée de façon inattendue.

Scénario 1 : Restauration sur le même système

1. Afin d'éviter toute incohérence dans les informations du domaine d'unité entre le microcode sous licence et i5/OS, il est recommandé d'installer le microcode sous licence par l'intermédiaire de l'option 3 (Install Licensed Internal Code and Recover Configuration).

   Remarque : Pour que l'opération Install Licensed Internal Code and Recover Configuration aboutisse, vous devez avoir les mêmes unités de disques, à l'exception de l'unité de disques du source IPL si elle a échoué. Vous devez également récupérer la même édition.
2. Après avoir installé le microcode sous licence, suivez la procédure Recovering Your Disk Configuration à la rubrique *Recovering your system*. Ces étapes vous permettent d'éviter d'avoir à reconfigurer les pools de stockage sur disque.
3. Après avoir récupéré les informations système, lorsque vous êtes prêt à démarrer la mise en grappe sur le noeud que vous venez de récupérer, vous devez lancer la mise en grappe à partir du noeud actif. Les informations de configuration les plus récentes sont ainsi propagées sur le noeud récupéré.

Scénario 2 : Restauration sur un autre système

Après avoir récupéré les informations système et consulté l'historique du travail pour vérifier que tous les objets ont été récupérés, vous devez procéder comme suit pour configurer correctement le domaine d'unité de grappe.

1. A partir du noeud que vous venez de restaurer, supprimez la grappe.
2. A partir du noeud actif, procédez comme suit :
   a. Supprimez le noeud récupéré de la grappe.
   b. Ajoutez de nouveau le noeud récupéré dans la grappe.
   c. Ajoutez le noeud récupéré au domaine d'unité.
   d. Créez le groupe de ressources en grappe ou ajoutez le noeud au domaine de reprise.

Reprise d'une grappe après un sinistre

Dans le cas d'un sinistre ayant entraîné la perte de tous les noeuds, vous devez reconfigurer la grappe.

En prévision d'un tel scénario, il est recommandé de sauvegarder les informations relatives à la configuration de la grappe et d'en conserver un exemplaire imprimé.

Restauration d'une grappe à partir de bandes de sauvegarde

En fonctionnement normal, vous ne devez jamais effectuer une restauration à partir d'une bande de sauvegarde.

Cette opération n'est nécessaire que lorsqu'un sinistre se produit et que tous les noeuds de la grappe ont été perdus. En cas de sinistre, vous procédez à la reprise en suivant les procédures normales mises en place après l'élaboration d'une stratégie de sauvegarde et de reprise.

Identification et résolution des incidents dans la fonction de miroir entre sites

Ces informations peuvent vous aider à résoudre les incidents liés à la copie miroir entre sites que vous pourrez rencontrer.

Messages de la protection géographique par disque miroir

Consultez les descriptions et récupérations des messages de la protection géographique par disque miroir pour résoudre vos problèmes de protection géographique par disque miroir.

0x00010259

Description : L'opération a échoué car le système n'a pas trouvé la copie miroir.

Récupération : Tous les noeuds du domaine d'unité n'ont pas répondu. Vérifiez que la mise en grappe est active. Si nécessaire, démarrez les grappes du noeud. Voir «Démarrage de noeuds», à la page 106 pour plus de détails. Renouvelez la requête. Si l'incident persiste, prenez contact avec votre centre de support technique.

0x0001025A

Description : Tous les pools de stockage sur disque du groupe de pools de stockage sur disque ne sont pas protégés géographiquement par disque miroir.

Récupération : Si un pool de stockage sur disque du groupe est protégé géographiquement par disque miroir, tous les pools de stockage sur disque de ce groupe doivent l'être. Effectuez l'une des actions suivantes :

1. Configurez la protection géographique par disque miroir pour les pools de stockage sur disque qui ne sont pas protégés géographiquement par disque miroir.
2. Annulez la configuration de la protection géographique par disque miroir pour les pools de stockage sur disque qui sont protégés géographiquement par disque miroir.

0x00010265

Description : La copie en miroir déconnectée est disponible.

Récupération : Rendez la copie en miroir déconnectée indisponible, puis renouvelez l'opération de reconnexion.

0x00010380

Description : L'unité de disques est absente du système.

Récupération : Localisez ou réparez l'unité de disques absente dans la copie en miroir. Vérifiez l'historique de l'activité produit sur le noeud de destination. Récupérez de l'antémémoire.

0x00011210

Description : Le second pool de stockage sur disque proposé pour le groupe de pools de stockage sur disque n'est pas protégé géographiquement par disque miroir.

Récupération : Si un pool de stockage sur disque du groupe est protégé géographiquement par disque miroir, tous les pools de stockage sur disque de ce groupe doivent l'être. Vous devez configurer la protection géographique par disque miroir pour le second pool de stockage sur disque qui n'est pas protégé géographiquement par disque miroir, maintenant ou à la fin de cette opération.

0x00011211

Description : Il existe des copies en miroir en double.

Récupération : Recherchez les unités de disques protégées localement par disque miroir qui peuvent exister sur deux systèmes, Enterprise Storage Server FlashCopy, ou restaurez des copies de niveau précédent de pool de stockage sur disque. Pour plus d'informations, consultez l'historique d'activité produit sur le noeud de copie miroir. Eliminez les doublons et renouvelez votre demande. Si l'incident persiste, prenez contact avec votre centre de support technique ou consultez la section d'i5/OSassistance technique pour obtenir des informations sur l'assistance et la maintenance IBM.

Installation du programme sous licence IBM PowerHA for i

Avant d'implémenter une solution à haute disponibilité IBM i , vous devez installer le programme sous licence IBM PowerHA for i (5770-HAS) sur chaque système qui participe à la solution de haute disponibilité.

Avant d'installer le programme sous licence IBM PowerHA for i, vous devez exécuter les étapes d'installation suivantes :

1. Installez le programme ou une mise à niveau de i 7.1 Operating System.
2. Installez IBM i Operating System Option 41 (HA Switchable Resources).

Pour installer le logiciel sous licence IBM PowerHA for i, procédez comme suit :

1. Saisissez GO LICPGM dans une ligne de commande.
2. Dans l'écran Gestion des logiciels sous licence, sélectionnez l'option 11 (Installation des logiciels sous licence).
3. Sélectionnez le produit 5770-HAS, option *BASE pour installer IBM PowerHA for i Standard Edition. Appuyez sur la touche Entrée.
4. A l'affichage des options d'installation, saisissez le nom de votre unité d'installation comme requis. Appuyez sur Entrée pour démarrer l'installation.
5. L'utilisation de la protection géographique par disque miroir asynchrone, de Metro Mirror ou de Global Mirror requiert d'installer IBM PowerHA for i Enterprise Edition (option 1). Sélectionnez le produit 5770-HAS, option 1 pour installer IBM PowerHA for i Enterprise Edition. Appuyez sur la touche Entrée.

Une fois terminée l'installation du programme sous licence IBM PowerHA for i, vous devez redémarrer le serveur INETD. Pour plus d'informations sur le démarrage du serveur INETD, voir «Démarrage du serveur INETD», à la page 95.

Licence du code et informations de limitation de responsabilité

IBM vous concède une licence non exclusive de droits d'auteur vous autorisant à utiliser tous les exemples de code de programmation à partir desquels vous pouvez générer des fonctions similaires adaptées à vos besoins spécifiques.

SOUS RESERVE DE TOUTE GARANTIE LEGALE QUI NE PEUT ETRE EXCLUE, IBM, SES DEVELOPPEURS ET SES FOURNISSEURS NE FOURNISSENT AUCUNE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS, ET DE FACON NON LIMITATIVE, TOUTE GARANTIE IMPLICITE D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE, ET TOUTE GARANTIE EN NON-CONTREFACON CONCERNANT LE LOGICIEL OU LE SUPPORT TECHNIQUE, LE CAS ECHEANT.

IBM, SES DEVELOPPEURS OU FOURNISSEURS NE PEUVENT EN AUCUN CAS ETRE TENUS RESPONSABLES DES DOMMAGES SUIVANTS, ET CE, MEME S'ILS ONT ETE INFORMES DE LEUR POSSIBLE SURVENANCE :

1. PERTE OU DETERIORATION DE VOS DONNEES ;
2. PREJUDICES MORAUX, ACCESSOIRES, DIRECTS OU INDIRECTS ; OU

3. PERTE DE BENEFICE, D'ACTIVITE COMMERCIALE, DE REVENU, DE CLIENTELE, OU D'ECONOMIES ESCOMPTEES.

CERTAINES LEGISLATIONS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DE PREJUDICES ACCESSOIRES, DIRECTS OU INDIRECTS, AUQUEL CAS CERTAINES DE CES EXCLUSIONS OU LIMITATIONS QUI PRECEDENT NE VOUS SERONT PAS APPLICABLES.

Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
3-2-12, Roppongi, Minato-ku, Tokyo 106-8711

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LES PUBLICATIONS SONT LIVREES «EN L'ETAT» SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Livret Contractuel IBM, des Conditions Internationales d'Utilisation de Logiciels IBM, des Conditions d'Utilisation du Code Machine ou de tout autre contrat équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent document contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir

expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les programmes exemples sont livrés "en l'état", sans aucune garantie. IBM ne saura être responsable des dommages causés par l'utilisation de ces exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre société) (année). Certaines parties de ce code sont dérivées des programmes exemples d'IBM Corp. © Copyright IBM Corp. _indiquez l'année ou les années_.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Documentation sur l'interface de programmation

La présente publication "Implémentation de la haute disponibilité avec l'approche basée sur des tâches" décrit des interfaces de programmation que le Client peut utiliser pour écrire des programmes permettant d'exploiter les services d'IBM i5/OS.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. aux Etats-Unis et/ou dans certains autres pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information à www.ibm.com/legal/copytrade.shtml.

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

i5/OS
IBM
IBM (logo)
System i
System i5
System Storage
TotalStorage
FlashCopy

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que toutes les marques et tous les logos incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Dispositions

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Usage personnel : Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial : Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.