



System i

Verfügbarkeit

Hochverfügbarkeit - Implementierung
mit taskbasiertem Ansatz

Version 6 Release 1





System i

Verfügbarkeit

Hochverfügbarkeit - Implementierung
mit taskbasiertem Ansatz

Version 6 Release 1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen“, auf Seite 185 gelesen werden.

Diese Ausgabe bezieht sich auf Version 6, Release 1, Modifikation 0 von IBM i5/OS (Produktnummer 5761-SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (RISC = Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM System i, Availability, Implementing High Availability with the task-based approach,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1998, 2008
© Copyright IBM Deutschland GmbH 1998, 2008

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2008

Inhaltsverzeichnis

Hochverfügbarkeit - Implementierung mit taskbasiertem Ansatz 1

Hochverfügbarkeitslösung planen	2
Ausfallsichere Anwendungen planen	2
Ausfallsichere Anwendungen identifizieren	2
i5/OS-Architektur für clusterfähige Anwendungen	3
HA-Clusteranwendung schreiben	3
Anwendungsprogramme ausfallsicher machen	4
HA-Clusteranwendungen erneut starten	5
Exitprogramm für Clusterressourcengruppe aufrufen	5
Hinweise für Anwendungs-CRGs	6
Übernahme der IP-Adressen von Anwendungs-CRGs verwalten	6
Beispiel: Failoveraktionen für eine Anwendungs-CRG	9
Beispiel: Anwendungsexitprogramm	9
Ausfallsichere Daten planen	48
Welche Daten müssen ausfallsicher sein?	49
Umschaltbare Platten planen	49
Hardwarevoraussetzungen für umschaltbare Platten	50
Softwarevoraussetzungen für umschaltbare Platten	50
Kommunikationsvoraussetzungen für umschaltbare Platten	51
Standortübergreifende Spiegelung planen	51
Geographische Spiegelung planen	51
Metro Mirror planen	56
Global Mirror planen	59
Logische Replikation planen	63
Systeme zur Verwendung für die logische Replikation auswählen	63
IBM Business Partner für Cluster-Middleware und verfügbare Clustering-Produkte	63
Journalplanung für logische Replikation	64
Planung einer Sicherungsstrategie für logische Replikation	64
Leistungsplanung für logische Replikation	64
Ausfallsichere Umgebung planen	65
Clusterverwaltungsdomäne planen	65
Einträge für überwachte Ressourcen (MREs) planen	65
Cluster planen	66
Hardwarevoraussetzungen für Cluster	66
Softwarevoraussetzungen für Cluster	66
Kommunikationsvoraussetzungen für Cluster	67
Dediziertes Netzwerk für Cluster planen	68
Tipps für die Clusterkommunikation	68
Leistungsplanung für Cluster	69
Cluster mit verschiedenen Releases planen	72
Leistungsplanung für Cluster	72
Planungsprüfliste für Cluster	73

FlashCopy planen	76
Hardwarevoraussetzungen für FlashCopy	76
Softwarevoraussetzungen für FlashCopy	76
Kommunikationsvoraussetzungen für FlashCopy	76
Sicherheitsplanung für Hochverfügbarkeit	77
Clusterweite Informationen verteilen	77
Hinweise zur Verwendung von Clustern mit Firewalls	77
Benutzerprofile auf allen Knoten verwalten	78
Hochverfügbarkeitslösung konfigurieren	78
Szenarios: Hochverfügbarkeitslösungen konfigurieren	79
Szenario: Zwischen logischen Partitionen umschaltbare Platte	79
Szenario: Zwischen Systemen umschaltbare Platte	80
Szenario: Umschaltbare Platte mit geographischer Spiegelung	81
Szenario: Standortübergreifende Spiegelung mit geographischer Spiegelung	83
Szenario: Standortübergreifende Spiegelung mit Metro Mirror	84
Szenario: Standortübergreifende Spiegelung mit Global Mirror	86
TCP/IP für hohe Verfügbarkeit konfigurieren	88
TCP/IP-Konfigurationsattribute	88
INETD-Server starten	88
Cluster konfigurieren	89
Cluster erstellen	89
Knoten aktivieren und einem Cluster hinzufügen	90
Knoten hinzufügen	91
Knoten starten	91
Knoten zu einer Einheitendomäne hinzufügen	91
Clusterressourcengruppe erstellen	92
Clusterressourcengruppe starten	96
Nachrichtenwarteschlangen angeben	97
Switchover ausführen	98
Knoten konfigurieren	99
Knoten starten	99
Knoten aktivieren und einem Cluster hinzufügen	99
Knoten hinzufügen	100
Knoten zu einer Einheitendomäne hinzufügen	101
Clusterressourcengruppen konfigurieren	101
Clusterressourcengruppe starten	101
Clusterressourcengruppe erstellen	102
Clusterverwaltungsdomänen konfigurieren	106
Clusterverwaltungsdomäne erstellen	106
Knoten zu einer Clusterverwaltungsdomäne hinzufügen	107
Clusterverwaltungsdomäne starten	108
Synchronisation gespiegelter Ressourcen	108

	Einträge für überwachte Ressourcen hin-	Unabhängigen Plattenpool wieder aufneh-
	zufügen	men
	109	160
	Umschaltbare Platten konfigurieren	Standortübergreifende Spiegelung verwalten
	110	160
	Unabhängigen Plattenpool erstellen	Geographische Spiegelung verwalten
	110	160
	Spiegelschutz starten	Geographische Spiegelung aussetzen
	111	160
	Spiegelschutz stoppen	Geographische Spiegelung wieder aufneh-
	112	men
	Platteneinheit oder Plattenpool hinzufügen	161
	113	Spiegelkopie abhängen
	Aktuelle Konfiguration auswerten	162
	113	Spiegelkopie wieder anhängen
	Plattenpool verfügbar machen	163
	115	Geographische Spiegelung dekonfigurie-
	Standortübergreifende Spiegelung konfigurieren	ren
	115	164
	Geographische Spiegelung konfigurieren	Eigenschaften der geographischen Spiege-
	116	lung ändern
	Metro-Mirror-Sitzung konfigurieren	165
	116	Metro-Mirror-Sitzungen verwalten
	Global Mirror-Sitzung konfigurieren	165
	117	Metro-Mirror-Sitzungen aussetzen
Hochverfügbarkeit verwalten	118	Metro-Mirror-Sitzungen wieder aufneh-
	Szenarios: HA-Lösungen verwalten	men
	118	166
	Szenarios: Sicherungen in einer HA-Umge-	Metro-Mirror-Sitzung löschen
	bung ausführen.	166
	118	Metro-Mirror-Eigenschaften anzeigen
	Szenario: Sicherungen in einer Umgebung	166
	mit geographischer Spiegelung durchfüh-	Global Mirror verwalten.
	ren	167
	118	Global-Mirror-Sitzungen aussetzen
	Szenario: FlashCopy ausführen	167
	119	Global-Mirror-Sitzungen wieder aufneh-
	Szenarios: Betriebssystemupgrades in einer	men
	HA-Umgebung ausführen	167
	120	Global-Mirror-Sitzungen löschen
	Beispiel: Betriebssystemupgrade durchfüh-	167
	ren	Eigenschaften der Global-Mirror-Sitzung
	121	ändern
	Szenario: Einheit hochverfügbar machen	168
	122	FlashCopy verwalten
Cluster verwalten	123	168
	Clusterversion eines Clusters ändern	FlashCopy-Sitzung konfigurieren
	124	168
	Cluster löschen	FlashCopy aktualisieren
	124	169
	Clusterkonfiguration anzeigen.	FlashCopy wieder anhängen
	125	169
	Clusterkonfiguration sichern und wiederher-	FlashCopy abhängen
	stellen	169
	125	FlashCopy löschen
	Clusterstatus überwachen	170
	126	Daten von FlashCopy wiederherstellen
	Nachrichtenwarteschlangen angeben	170
	127	FlashCopy-Eigenschaften ändern
	Prüfliste zur Aufhebung der Konfiguration	170
	128	Fehlerbehebung für HA-Lösung
	Knoten verwalten	171
	129	Fehlerbehebung für Cluster durchführen
	Knoteneigenschaften anzeigen	171
	129	Feststellen, ob ein Clusterproblem besteht
	Knoten stoppen	171
	129	Wiederherstellungsinformationen für einen
	Knoten entfernen	Cluster erfassen
	130	172
	Knoten aus einer Einheitendomäne entfer-	Allgemeine Clusterfehler
	nen.	173
	130	Partitionsfehler
	Clusterressourcengruppen verwalten	175
	131	Primäre und sekundäre Clusterpartitionen
	CRG-Status anzeigen	festlegen
	131	176
	CRG stoppen	Status partitionierter Knoten in "Ausgefal-
	132	len" ändern
	Clusterressourcengruppe löschen	177
	133	Partitionierte Clusterverwaltungsdomänen
	Umschaltbare Einheiten erstellen	178
	133	Tipps zu Clusterpartitionen.
	Wiederherstellungsdomäne für eine	179
	Clusterressourcengruppe ändern	Wiederherstellung von Clustern
	134	180
	Failover bei Ausfallereignissen verwalten	Wiederherstellung nach Clusterjobfehlern
	135	180
	Clusterverwaltungsdomänen verwalten.	Beschädigtes Clusterobjekt wiederherstel-
	138	len
	Clusterverwaltungsdomäne stoppen	180
	139	Clusterwiederherstellung nach Komplett-
	Clusterverwaltungsdomäne löschen	ausfall.
	140	181
	Eigenschaften einer Clusterverwaltungs-	Clusterwiederherstellung nach Katastro-
	domäne ändern.	phenfall
	140	182
	Einträge für überwachte Ressourcen ver-	Cluster von Sicherungsbändern wiederher-
	walten.	stellen
	141	182
	Umschaltbare Platten verwalten	Fehlerbehebung bei standortübergreifender
	157	Spiegelung
	Plattenpools sperren	182
	157	Nachrichten für geographische Spiegelung
	Hardware umschaltbar machen	182
	157	
	Unabhängigen Plattenpool stilllegen.	
	160	

Anhang. Bemerkungen 185
| Informationen zu Programmierschnittstellen 186

Marken 187
Bedingungen 187

Hochverfügbarkeit - Implementierung mit taskbasiertem Ansatz

Der taskbasierte Ansatz zum Konfigurieren und Verwalten von i5/OS mit hoher Verfügbarkeit ermöglicht Ihnen, eine angepasste Hochverfügbarkeitslösung (High Availability = HA) in Abhängigkeit von Ihren Geschäftsanforderungen zu konfigurieren und zu verwalten. Für die Konfiguration und Verwaltung der HA-Lösung werden grafische Oberflächen und Befehlszeilenschnittstellen verwendet.

Anders als beim lösungsbasierten Ansatz, der die grafische Oberfläche des High Availability Solution Manager verwendet, wobei eine vordefinierte Lösung automatisch konfiguriert wird und nur wenige Eingaben durch den Benutzer erforderlich sind, ermöglicht der taskbasierte Ansatz dem sachkundigen Benutzer die Anpassung und Implementierung einer individuellen Lösung. Zur Erstellung und Verwaltung einer HA-Lösung mit diesem Ansatz müssen die Benutzer ihre Anforderungen an die Hochverfügbarkeit genau kennen und mit mehreren Schnittstellen vertraut sein.

Grafische Oberfläche der Cluster Resource Services

Über die grafische Oberfläche der Cluster Resource Services können Clustertechnologien konfiguriert und verwaltet werden, die Bestandteil einer HA-Lösung sind. Diese grafische Oberfläche kann nur verwendet werden, wenn das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS installiert wird. Folgende Funktionen können über diese grafische Schnittstelle ausgeführt werden:

- Cluster erstellen und verwalten
- Knoten erstellen und verwalten
- Clusterressourcengruppen (CRGs) erstellen und verwalten
- Clusterverwaltungsdomäne erstellen und verwalten
- Überwachte Ressourcen erstellen und verwalten
- Den Cluster auf clusterbezogene Ereignisse wie Clusterpartitionen und Failover überwachen
- Manuelle Switchover bei geplanten Betriebsunterbrechungen durchführen, wie z. B. bei einer planmäßigen Systemwartung

Plattenverwaltungsschnittstelle

Über die Plattenverwaltungsschnittstelle können unabhängige Plattenpools konfiguriert und verwaltet werden, die notwendig sind, wenn mehrere Technologien für Datenausfallsicherheit implementiert werden. Abhängig von der implementierten Technologie müssen bestimmte Installationsvoraussetzungen erfüllt sein, damit einige der folgenden Funktionen verwendet werden können:

- Plattenpool erstellen
- Plattenpool verfügbar machen
- Plattenpool sperren
- Geographische Spiegelung konfigurieren
- Metro Mirror konfigurieren
- Global Mirror konfigurieren

Befehlszeilenschnittstelle

Über die Befehlszeilenschnittstelle können viele verschiedene Hochverfügbarkeitstasks mit CL-Befehlen ausgeführt werden. Für jede clusterbezogene Task gibt es einen entsprechenden CL-Befehl.

Zugehörige Informationen

Befehle für IBM System i High Availability Solutions Manager (iHASM)

Hochverfügbarkeitslösung planen

Vor der Konfiguration einer i5/OS-Hochverfügbarkeitslösung ist eine sorgfältige Planung erforderlich, damit sichergestellt ist, dass alle Voraussetzungen für die Lösung erfüllt sind.

Bei jeder Hochverfügbarkeitstechnologie bestehen Mindestvoraussetzungen, die erfüllt sein sollten, bevor eine bestimmte Lösung konfiguriert wird. Neben diesen Voraussetzungen ist es wichtig zu entscheiden, welche Ressourcen ausfallsicher sein sollen. Diese Ressourcen, z. B. Anwendungen, Daten und Einheiten, sollten daraufhin überprüft werden, ob sie hoch verfügbar sein müssen. Ist dies der Fall, müssen alle erforderlichen Änderungen an der Umgebung vor der Konfiguration einer HA-Lösung durchgeführt werden. Beispielsweise könnten Daten im SYSBAS vorhanden sein, die hoch verfügbar sein sollen. Vor der Konfiguration einer Lösung sollten diese Daten auf einen unabhängigen Plattenpool verschoben werden. Unter Umständen müssen auch bestimmte Anwendungen geändert werden, um Hochverfügbarkeit zu ermöglichen.

Ausfallsichere Anwendungen planen

Die Ausfallsicherheit von Anwendungen ist eines der Schlüsselemente in einer HA-Umgebung. Wenn Sie beabsichtigen, Anwendungen mit hoher Verfügbarkeit zu schreiben und im Cluster einzusetzen, sollten Sie bedenken, dass diese Anwendungen bestimmten Verfügbarkeitspezifikationen unterliegen.

Der Vorteil ausfallsicherer Anwendungen in einer Umgebung besteht darin, dass eine Anwendung auf einem anderen Clusterknoten erneut gestartet werden kann, ohne dass die Clients rekonfiguriert werden müssen. Darüber hinaus sind die der Anwendung zugeordneten Daten nach einem Switchover oder Failover ebenfalls verfügbar. Dies bedeutet, dass der Anwendungsbenutzer diesen Vorgang, mit dem die Anwendung und ihre Daten vom Primärknoten auf den Ausweichknoten umgeschaltet werden, nur als kurzzeitige Unterbrechung oder überhaupt nicht wahrnimmt. Es besteht keine Notwendigkeit, den Benutzer darüber zu informieren, dass die Anwendung samt Daten intern verschoben wurde.

Um Ausfallsicherheit von Anwendungen in einem Cluster zu erreichen, müssen Anwendungen verwendet werden, die bestimmte Verfügbarkeitspezifikationen erfüllen. Die Anwendung muss bestimmte Merkmale aufweisen, damit sie verschoben werden kann und somit den Anwendungsbenutzern im Cluster permanent zur Verfügung steht. Aufgrund dieser Anforderungen haben Sie folgende Möglichkeiten, wenn eine umschaltbare Anwendung in Ihrem Cluster eingesetzt werden soll:

1. Clusterfähige Softwareanwendung kaufen

Softwareprodukte, die clusterfähig sind, erfüllen bestimmte Voraussetzungen für die Hochverfügbarkeit.

2. Eigene Anwendungen mit hoher Verfügbarkeit schreiben oder vorhandene Anwendungen entsprechend ändern

Unabhängige Softwareanbieter und Anwendungsprogrammierer können Anwendungen so anpassen, dass sie in einer i5/OS-Hochverfügbarkeitsumgebung verschoben werden können.

Ausfallsichere Anwendungen müssen innerhalb des Clusters verwaltet werden.

Zugehörige Informationen

High Availability and Clusters

Ausfallsichere Anwendungen identifizieren

Der Vorteile des Clustering in Bezug auf die Verfügbarkeit können nicht mit jeder Anwendung genutzt werden.

Eine Anwendung muss ausfallsicher sein, um die Vorteile der vom Clustering bereitgestellten Switchover- und Failoverfunktionen nutzen zu können. Ausfallsichere Anwendungen können auf dem Ausweichknoten erneut gestartet werden, ohne dass die Clients, die die Anwendung nutzen, rekonfiguriert werden müssen. Daher muss Ihre Anwendung bestimmte Voraussetzungen erfüllen, um die durch das Clustering angebotene Funktionalität optimal nutzen zu können.

i5/OS-Architektur für clusterfähige Anwendungen

Hoch verfügbare Anwendungen bieten dem Endbenutzer einen zusätzlichen Nutzen, da sie im Falle einer Betriebsunterbrechung, ob geplant oder ungeplant, weiterhin ausführbar sind.

i5/OS stellt eine Architektur für ausfallsichere Anwendungen bereit, die verschiedene Stufen der Anwendungsverfügbarkeit unterstützt. Anwendungen im oberen Spektrum zeichnen sich durch Hochverfügbarkeitsmerkmale aus, bieten Automatisierung für eine HA-Umgebung und werden über HA-Managementschnittstellen verwaltet.

Diese Anwendungen haben folgende Merkmale:

- Die Anwendung kann auf einen Ausweichclusterknoten umgeschaltet werden, wenn der Primärknoten gesperrt wird.
- Die Anwendung definiert die ausfallsichere Umgebung im Resilient Definition and Status Data Area (Bereich zur Definition der Ausfallsicherheit und Statusdaten), um eine automatische Konfiguration und Aktivierung der Anwendung durch eine Clusterverwaltungsanwendung zu ermöglichen.
- Die Anwendung bietet Ausfallsicherheit durch ein Exitprogramm für Anwendungs-CRGs, um clusterbezogene Ereignisse zu verarbeiten, indem sie die Vorteile der i5/OS Cluster Resource Services-Funktionalität nutzt.
- Die Anwendung verfügt über eine Neustartfunktion, die den Benutzer bei einem Neustart in einem Anwendungsmenü oder einer weiterführenden Anzeige positioniert.

Anwendungen mit noch höherem Anspruch hinsichtlich Verfügbarkeit und Neustartfunktionalität haben folgende Merkmale:

- Die Anwendung bietet ein höheres Maß an Ausfallsicherheit aufgrund einer leistungsfähigeren Verarbeitung von Clusterereignissen (Aktionscodes) durch das Exitprogramm für Anwendungs-CRGs.
- Die Anwendung bietet umfassendere Unterstützung für Neustartfunktionen. Bei hostbasierten Anwendungen wird der Benutzer über Commitsteuerungs- oder Prüfpunktfunktionen wieder auf einer Transaktionsgrenze positioniert. Bei clientbasierten Anwendungen findet ein reibungsloses Failover statt, das der Benutzer nur als minimale Serviceunterbrechung wahrnimmt.

HA-Clusteranwendung schreiben

Eine hoch verfügbare Anwendung (HA-Anwendung) ist eine Anwendung, die sich bei einem Systemausfall in einer Clusterumgebung als ausfallsicher erweisen kann.

Mehrere Stufen der Anwendungsverfügbarkeit sind möglich:

1. Tritt ein Anwendungsfehler auf, startet die Anwendung auf demselben Knoten erneut und korrigiert potenzielle Fehlerursachen (wie z. B. beschädigte Steuerdaten). Die Anwendung verhält sich so, als würde sie zum ersten Mal gestartet.
2. Die Anwendung führt Verarbeitungsschritte für einen Neustart am Prüfpunkt aus. Die Anwendung wird in dem Zustand wiederhergestellt, in dem sie sich befand, als der Fehler auftrat.
3. Falls ein Systemausfall eintritt, wird die Anwendung auf einem Ausweichserver erneut gestartet. Die Anwendung verhält sich so, als würde sie zum ersten Mal gestartet.
4. Falls ein Systemausfall eintritt, wird die Anwendung auf einem Ausweichserver erneut gestartet und führt Verarbeitungsschritte für einen Neustart am Prüfpunkt auf den Servern durch. Die Anwendung wird in dem Zustand wiederhergestellt, in dem sie sich befand, als der Fehler auftrat.
5. Falls ein Systemausfall eintritt, findet ein koordiniertes Failover sowohl der Anwendung als auch der zugeordneten Daten auf einen oder mehrere andere Knoten im Cluster statt. Die Anwendung wird in dem Zustand wiederhergestellt, in dem sie sich befand, als der Fehler auftrat.
6. Falls ein Systemausfall eintritt, findet ein koordiniertes Failover sowohl der Anwendung als auch der zugeordneten Daten auf einen oder mehrere andere Knoten im Cluster statt. Die Anwendung führt Verarbeitungsschritte für einen Neustart am Prüfpunkt auf den Servern aus. Die Anwendung wird in dem Zustand wiederhergestellt, in dem sie sich befand, als der Fehler auftrat.

Anmerkung: In den Fällen 1 bis 4 sind Sie für die Wiederherstellung der Daten verantwortlich.

Anwendungsprogramme ausfallsicher machen:

Hier erfahren Sie, wie Sie Anwendungsprogramme ausfallsicher machen können.

Eine ausfallsichere Anwendung sollte folgende Merkmale aufweisen:

- Die Anwendung kann auf diesem oder einem anderen Knoten erneut gestartet werden.
- Der Client kann über die IP-Adresse auf die Anwendung zugreifen.
- Die Anwendung ist statusunabhängig (stateless), oder Statusinformationen sind bekannt.
- Die der Anwendung zugeordneten Daten sind nach einem Switchover verfügbar.

Die drei wesentlichen Elemente, die eine Anwendung bei Systemausfällen in einer Clusterumgebung ausfallsicher machen, sind folgende:

Die Anwendung selbst

Wie tolerant verhält sich die Anwendung bei Fehlern oder Systemausfällen, und kann die Anwendung erneut gestartet werden, ohne dass der Benutzer dies bemerkt?

Die Anwendung nutzt hierzu die Clustering-Funktionalität.

Zugeordnete Daten

Hat eine Betriebsunterbrechung Auswirkungen auf die Verfügbarkeit der zugeordneten Daten?

Sie können kritische Daten auf umschaltbaren Platten speichern, damit die Daten während einer Betriebsunterbrechung verfügbar bleiben. Alternativ kann ein Cluster-Middleware-Replikationsprodukt eines IBM Business Partners, das die Vorteile der Clustering-Funktionalität nutzt, dafür eingesetzt werden.

Steuerungsfunktionalität und Verwaltung

Wie schnell kann die Umgebung, die die Verfügbarkeit von Daten und Anwendung unterstützt, definiert werden?

IBM System i High Availability Solutions Manager (iHASM), Lizenzprogrammnummer 5761-HAS, verfügt über mehrere Schnittstellen zum Konfigurieren und Verwalten von HA-Lösungen und HA-Technologie. Das Lizenzprogramm iHASM stellt folgende Schnittstellen bereit:

Grafische Oberfläche des High Availability Solutions Manager

Diese grafische Oberfläche bietet Ihnen die Möglichkeit, aus mehreren von i5/OS unterstützten HA-Lösungen auszuwählen. Die Schnittstelle prüft alle Technologievoraussetzungen für die ausgewählte Lösung, konfiguriert die Lösung und die zugehörigen Technologien und bietet eine vereinfachte Verwaltung aller Hochverfügbarkeitstechnologien für Ihre Lösung.

Grafische Oberfläche der Cluster Resource Services

Diese grafische Oberfläche ermöglicht einem erfahrenen Benutzer eine höhere Flexibilität beim Anpassen einer HA-Lösung. Mit Hilfe dieser Schnittstelle können Clustertechnologien, wie beispielsweise Clusterressourcengruppen (CRGs), konfiguriert und verwaltet werden. Über diese Schnittstelle können außerdem unabhängige Plattenpools konfiguriert werden, wenn sie als Bestandteil einer HA-Lösung verwendet werden.

Befehle für IBM System i High Availability Solutions Manager

Diese Befehle bieten ähnliche Funktionen, sind jedoch über eine Befehlszeilenschnittstelle verfügbar.

APIs für IBM System i High Availability Solutions Manager (iHASM)

Diese APIs ermöglichen das Arbeiten mit neuen Funktionen, die unabhängige Plattenpools betreffen.

Sie können auch eine Clusterverwaltungsschnittstelle eines anderen Anbieters einsetzen, die die Clustering-APIs verwendet und ebenfalls ausfallsichere Anwendungen mit ausfallsicheren Daten verbindet.

Zugehörige Informationen

Hochverfügbarkeit - Verwaltung

HA-Clusteranwendungen erneut starten:

Damit eine Anwendung erneut gestartet werden kann, muss die Anwendung ihren Status zum Zeitpunkt des Failover oder Switchover kennen.

Statusinformationen sind anwendungsspezifisch; daher muss die Anwendung entscheiden, welche Informationen erforderlich sind. Auf Ihrem PC kann eine Anwendung ohne Statusinformationen erneut gestartet werden. Sie müssen jedoch selbst an die Stelle in der Anwendung zurückkehren, an der Sie weiterarbeiten möchten.

Es gibt mehrere Methoden, um Statusinformationen über die Anwendung für das Ausweichsystem zu speichern. Jede Anwendung muss selbst entscheiden, welche Methode die am besten geeignete ist.

- Die Anwendung kann alle Statusinformationen an das anfordernde Clientsystem übertragen. Bei einem Switchover oder Failover verwendet die Anwendung die auf dem Client gespeicherten Statusinformationen, um den ursprünglichen Status auf dem neuen Server wiederherzustellen. Dazu können die Cluster-Hash-Tabellen-APIs oder die Distribute-Information-API verwendet werden.
- Die Anwendung kann Statusinformationen (wie Jobinformationen und andere Steuerstrukturen, die der Anwendung zugeordnet sind) auf Echtzeitbasis replizieren. Bei jeder Änderung in den Strukturen überträgt die Anwendung diese auf das Ausweichsystem.
- Die Anwendung kann die für ihre Ausführung relevanten Statusinformationen im Datenteil des Exitprogramms der Clusterressourcengruppe speichern. Bei dieser Methode wird vorausgesetzt, dass nur wenige Statusinformationen erforderlich sind. Sie können dazu die API `QcstChangeClusterResourceGroup` (Change Cluster Resource Group) verwenden.
- Die Anwendung kann Statusinformationen in einem Datenobjekt speichern, das zusammen mit den Daten der Anwendung auf die Ausweichsysteme repliziert wird.
- Die Anwendung kann Statusinformationen in einem Datenobjekt speichern, das sich auf dem umschaltbaren IASP befindet, der auch die Daten der Anwendung enthält.
- Die Anwendung kann Statusinformationen über den Client speichern.
- Es werden keine Statusinformationen gespeichert, und Sie müssen die Wiederherstellung selbst durchführen.

Anmerkung: Wenn die Anwendung Verarbeitungsschritte für einen Neustart am Prüfpunkt ausführt, müssen weniger Statusinformationen gespeichert werden, da Statusinformationen nur an vordefinierten Anwendungsprüfpunkten gespeichert werden. Bei einem Neustart setzt die Anwendung beim letzten bekannten Prüfpunkt wieder auf; diese Vorgehensweise ist vergleichbar mit der Commitsteuerungsverarbeitung einer Datenbank.

Exitprogramm für Clusterressourcengruppe aufrufen:

Das Exitprogramm für die Clusterressourcengruppe (CRG-Exitprogramm) wird in unterschiedlichen Phasen in einer Clusterumgebung aufgerufen.

Dieses Programm sorgt für die notwendige Ausfallsicherheit der Umgebung im Hinblick auf die Ressourcen im Cluster. Für eine ausfallsichere Einheiten-CRG ist dieses Exitprogramm optional, für andere CRG-Arten ist es jedoch erforderlich. Wenn ein CRG-Exitprogramm verwendet wird, wird es bei Auftreten clusterweiter Ereignisse, einschließlich der folgenden, aufgerufen:

- Ein Knoten verlässt unerwarteterweise den Cluster.

- Ein Knoten verlässt den Cluster, weil die API End Cluster Node (QcstEndClusterNode) oder die API Remove Cluster Node Entry (QcstRemoveClusterNodeEntry) aufgerufen wurde.
- Ein Cluster wird gelöscht, weil die API Delete Cluster (QcstDeleteCluster) aufgerufen wurde.
- Ein Knoten wird durch Aufrufen der API Start Cluster Node (QcstStartClusterNode) aktiviert.
- Die Kommunikation mit einem partitionierten Knoten wird wiederhergestellt.

Das Exitprogramm führt folgende Prozesse aus:

- Es wird in der genannten Aktivierungsgruppe oder der Aktivierungsgruppe des Aufrufers (*CALLER) ausgeführt.
- Es ignoriert den Neustartparameter, wenn es eine nicht behandelte Ausnahmebedingung antrifft oder abgebrochen wird.
- Es stellt einen Abbruchhandler zur Verfügung.

Bei Ausführung einer Clusterressourcengruppen-API wird das Exitprogramm in einem separaten Job mit dem Benutzerprofil aufgerufen, das in der API QcstCreateClusterResourceGroup (Create Cluster Resource Group) angegeben ist. Der separate Job wird beim Aufruf des Exitprogramms von der API automatisch erstellt. Wenn das Exitprogramm für eine Daten-CRG nicht erfolgreich oder abnormal endet, wird das CRG-Exitprogramm auf allen aktiven Knoten in der Wiederherstellungsdomäne mit dem Aktionscode für "Rückgängig" aufgerufen. Mit diesem Aktionscode können alle nicht beendeten Aktivitäten zurückgesetzt und der ursprüngliche Status der Clusterressourcengruppe wiederhergestellt werden.

Angenommen, das Switchover ist für eine Einheiten-CRG nicht erfolgreich. Nachdem alle Einheiten zurückgeschaltet wurden, sofern sie am ursprünglichen Primärknoten erfolgreich angehängt waren, ruft das Clustering das Exitprogramm auf dem Primärknoten mit dem Aktionscode für "Start" auf.

Wenn das Exitprogramm für eine Anwendungs-CRG nicht erfolgreich oder abnormal endet, versuchen die Cluster Resource Services, die Anwendung erneut zu starten, sofern die CRG aktiv ist. Das CRG-Exitprogramm wird mit dem Aktionscode für "Neustart" aufgerufen. Kann die Anwendung mit der angegebenen maximalen Anzahl von Versuchen nicht erneut gestartet werden, wird das CRG-Exitprogramm mit dem Aktionscode für "Failover" aufgerufen. Der Zähler für Neustart wird nur zurückgesetzt, wenn das Exitprogramm mit dem Aktionscode für "Start" aufgerufen wird, der das Ergebnis einer CRG-Starts, eines Failover oder Switchover sein kann.

Wenn die Clusterressourcengruppe gestartet wird, darf das auf dem Primärknoten aufgerufene Exitprogramm der Anwendungs-CRG die Steuerung so lange nicht an die Cluster Resource Services zurückgeben, bis die Anwendung selbst endet oder ein Fehler auftritt. Sobald eine Anwendungs-CRG aktiv ist und die Cluster Resource Services das Exitprogramm der Anwendungs-CRG über ein Ereignis informieren müssen, wird eine weitere Instanz des Exitprogramms in einem anderen Job gestartet. Es wird erwartet, dass ein anderer Aktionscode als "Start" oder "Neustart" zurückgegeben wird.

Beim Aufrufen eines CRG-Exitprogramms werden mehrere Parameter an das Exitprogramm übergeben, die das gerade verarbeitete Clusterereignis, den aktuellen Status der Clusterressourcen und den erwarteten Status der Clusterressourcen angeben.

Vollständige Informationen über CRG-Exitprogramme, einschließlich Angaben darüber, welche Informationen für die einzelnen Aktionscodes an das Exitprogramm übergeben werden, finden Sie unter Cluster Resource Group Exit Program in der Dokumentation über Cluster-APIs. In der Bibliothek QUSRTOOL wird Musterquellcode bereitgestellt, der als Basis zum Schreiben eines Exitprogramms verwendet werden kann. Siehe die Teildatei TCSTAPPEXT in der Datei QATTSYSC.

Hinweise für Anwendungs-CRGs

Eine Anwendungs-Clusterressourcengruppe (Anwendungs-CRG) verwaltet die Ausfallsicherheit von Anwendungen.

Übernahme der IP-Adressen von Anwendungs-CRGs verwalten:

Sie können die Übernahme der IP-Adressen von Anwendungs-CRGs mit Hilfe der Cluster Resource Services verwalten. Eine manuelle Verwaltung der Übernahme ist ebenfalls möglich.

Es gibt zwei Möglichkeiten, die einer Anwendungs-CRG zugeordnete IP-Übernahmeadresse zu verwalten. Die einfachste Möglichkeit, die standardmäßig verwendet wird, besteht darin, die IP-Übernahmeadresse von den Cluster Resource Services verwalten zu lassen. Bei dieser Methode werden die Cluster Resource Services angewiesen, die IP-Übernahmeadresse auf allen Knoten in der Wiederherstellungsdomäne zu erstellen, einschließlich der Knoten, die der Domäne nachträglich hinzugefügt werden. Bei Auswahl dieser Methode darf die IP-Übernahmeadresse derzeit auf keinem Knoten in der Wiederherstellungsdomäne definiert sein.

Die Alternative besteht darin, die IP-Übernahmeadressen selbst zu verwalten. Bei dieser Methode werden die Cluster Resource Services angewiesen, keine Schritte zur Konfiguration der IP-Übernahmeadresse zu ergreifen, da der Benutzer für die Konfiguration verantwortlich ist. Die IP-Übernahmeadresse muss vor dem Starten der Clusterressourcengruppe auf allen Knoten der Wiederherstellungsdomäne, ausgenommen Replikationsknoten, hinzugefügt werden. Bevor ein Knoten der Wiederherstellungsdomäne einer aktiven Clusterressourcengruppe hinzugefügt werden kann, muss die IP-Übernahmeadresse auf dem Knoten konfiguriert worden sein.

Zugehörige Konzepte

„Beispiel: Failoveraktionen für eine Anwendungs-CRG“ auf Seite 9

Dieses Beispiel zeigt, wie ein Failoverszenario funktioniert. Andere Failoverszenarios können sich anders verhalten.

Mehrere Teilnetze: Es ist möglich, die IP-Übernahmeadresse von Anwendungen so einzurichten, dass sie über mehrere Teilnetze hinweg funktioniert, obwohl sich die Knoten der Wiederherstellungsdomäne standardmäßig alle im selben Teilnetz befinden sollten. Wenn die Knoten der Wiederherstellungsdomäne über mehrere Teilnetze verteilt sind, muss für die Konfiguration der IP-Übernahmeadresse von Anwendungen die Switchover-Umgebung aktiviert werden.

Switchover von Anwendungen über mehrere Teilnetze aktivieren:

Im Allgemeinen müssen sich beim Clustering alle Clusterknoten der Wiederherstellungsdomäne einer Anwendungs-CRG im selben LAN befinden (dieselbe Teilnetzadressierung verwenden). Die Cluster Resource Services unterstützen beim Konfigurieren von Anwendungs-CRGs eine vom Benutzer konfigurierte IP-Übernahmeadresse.

| Das zugrunde liegende Netzwerkprotokoll, das beim Umschalten der konfigurierten IP-Übernahme-
| adresse von Anwendungen von einem Knoten in der Wiederherstellungsdomäne auf einen anderen ver-
| wendet wird, ist das Address Resolution Protocol (ARP). Es ist auch möglich, die Wiederherstellungs-
| domäne zu erweitern und Clusterknoten aufzunehmen, die sich in anderen LANs befinden, die durch
| kommerzielle Router voneinander getrennt sind. Diese Erweiterung wird durch die Verwendung virtuel-
| ler IP-Adressen und des Routing Information Protocol (RIP) in den Clusterknoten und die kommerziellen
| Router im Netzwerk erreicht.

Die folgenden manuell durchzuführenden Konfigurationsschritte sind erforderlich, um die Switchover-Umgebung einzurichten. **Diese Schritte müssen auf allen Knoten der Wiederherstellungsdomäne durchgeführt und für alle anderen Knoten im Cluster, die nachträglich in die Wiederherstellungsdomäne für die betreffende Anwendungs-CRG aufgenommen werden, wiederholt werden.**

1. Die von der Anwendungs-CRG zu verwendende IP-Übernahmeadresse auswählen.
 - Um Verwechslungen zu vermeiden, darf sich diese Adresse nicht mit anderen vorhandenen Adressen überschneiden, die von den Clusterknoten oder Routern verwendet werden. Wenn Sie beispielsweise 19.19.19.19 auswählen, muss sichergestellt sein, dass 19.0.0.0 (19.19.0.0) keine Leitwege sind, die den System-Routing-Tabellen bekannt sind.
 - Fügen Sie die Übernahmeschnittstelle (z. B. 19.19.19.19) hinzu. Erstellen Sie diese mit einer Leitungsbeschreibung mit der Angabe *VIRTUALIP, der Teilnetzmaske 255.255.255.255 (Hostleit-

weg), einer maximalen Übertragungseinheit von 1500 (jede beliebige Zahl im Bereich von 576-16388) und der Angabe *NO für automatisches Starten. Diese Übernahmeadresse (z. B. 19.19.19.19) muss als *VIRTUALIP-Adresse vorhanden sein, bevor Sie im nächsten Schritt als eine zugeordnete lokale Schnittstelle angegeben wird. Sie darf jedoch nicht aktiv sein.

2. Ordnen Sie die beabsichtigte IP-Übernahmeadresse einer oder beiden IP-Adressen zu, die Sie für die Clusterkommunikation vorgesehen haben, wenn Sie den Cluster erstellen oder dem Cluster einen Knoten hinzufügen.
 - Dies bedeutet, dass die Übernahmeadresse 19.19.19.19 als zugeordnete lokale Schnittstelle für die IP-Adresse des Clusterknotens angegeben wird. Dieser Vorgang muss für jede Clusteradresse auf jedem Clusterknoten wiederholt werden.

Anmerkung: Die Zuordnung der Clusteradressen muss beendet sein, um diese Änderung unter CFGTCP durchzuführen.

3. Erstellen Sie den Cluster und alle CRGs. Geben Sie für die Anwendungs-CRG im Feld 'IP-Übernahmeadresse konfigurieren' `QcstUserCfgsTakeoverIpAddr` ein. Starten Sie keine der Anwendungs-CRGs.
4. Geben Sie 'TCP/IP-Anwendungen konfigurieren' (Auswahl 20) unter CFGTCP ein, dann 'RouteD konfigurieren' (Auswahl 2) und 'RouteD-Attribute ändern' (Auswahl 1), und prüfen Sie, ob 'Bereitstellen' auf *YES gesetzt ist. Ist dies nicht der Fall, geben Sie *YES ein, und starten Sie (ggf. erneut) den Router-Dämon (RouteD) (RIP oder RIP-2) auf jedem Clusterknoten.
 - NETSTAT Auswahl 3 zeigt, dass der Router-Dämon (RouteD) einen lokalen Port verwendet, sofern er aktiv ist. Der Router-Dämon muss aktiv sein und Leitwege auf jedem Clusterknoten in der CRG-Wiederherstellungsdomäne bekannt machen (Bereitstellen = *YES).
5. Vergewissern Sie sich, dass alle kommerziellen Router im Netzwerk, die die LANs der Wiederherstellungsdomäne untereinander verbinden, Hostleitwege für das RIP akzeptieren und bekannt machen.
 - Dies ist nicht unbedingt die Standardeinstellung für Router. Das Protokoll ist abhängig vom Hersteller des Routers; die Einstellungen für RIP-Schnittstellen sollten so festgelegt sein, dass Hostleitwege gesendet und dynamische Hosts empfangen werden.
 - Dies gilt sowohl für die Router-zu-System-Schnittstellen, als auch für die Router-zu-Router-Schnittstellen.

Anmerkung: Verwenden Sie in dieser Konfiguration keine System i-Maschine als Router, sondern einen kommerziellen Router (IBM oder einen anderen Hersteller), der für Weiterleitungszwecke konzipiert ist. Die Weiterleitungsfunktionalität auf dem System i kann für diese Funktion nicht konfiguriert werden.

6. Aktivieren Sie die Übernahmeadresse auf einem der Clusterknoten manuell:
 - a. Warten Sie bis zu 5 Minuten, damit das RIP die Leitwege weitergeben kann.
 - b. Überprüfen Sie mit Ping die Übernahmeadresse auf allen Knoten in der CRG-Wiederherstellungsdomäne und allen ausgewählten Clients in den LANs, die diese Adresse verwenden werden.
 - c. Vergewissern Sie sich, dass die Übernahmeadresse wieder beendet wird.

(Beim Starten der CRGs wird die Adresse auf dem angegebenen Primärknoten vom Clustering gestartet.)

7. Starten Sie die Anwendungs-CRGs.
 - Die Übernahmeadresse wird vom Clustering auf dem angegebenen bevorzugten Knoten gestartet, und RIP macht die Leitwege in der Wiederherstellungsdomäne bekannt. RIP kann bis zu 5 Minuten brauchen, um Leitwege in der Domäne zu aktualisieren. Die RIP-Funktion ist unabhängig von der Funktion zum Starten der CRG.

Wichtig:

- Wenn die obige Prozedur nicht für alle Clusterknoten in der Wiederherstellungsdomäne der Anwendungs-CRG befolgt wird, wird beim Switchover eine "Blockierung" im Cluster eintreten.
- Obwohl normalerweise ein Failover auf Replikationsknoten nicht vorgesehen ist, ist es sinnvoll, diese Prozedur auf den Replikationsknoten für den Fall ausführen, dass sie zu einem späteren Zeitpunkt in Ausweichknoten geändert werden.
- Sollen mehrere virtuelle IP-Adressen verwendet werden, ist für jede eine separate Anwendungs-CRG und eine separate IP-Adresse, der sie zugeordnet wird, erforderlich. Diese Adresse kann eine andere logische IP-Adresse auf demselben physischen Adapter oder ein ganz anderer physischer Adapter sein. Außerdem ist darauf zu achten, dass Mehrdeutigkeiten in den Routing-Tabellen vermieden werden. Dies wird am besten auf die folgende Weise erreicht:
 - Fügen Sie jeder virtuellen IP-Adresse in der Routing-Tabelle eine *DFTRROUTE hinzu.
 - Verwenden Sie CFGTCP (Auswahl 2), um mehrere IP-Adressen anzugeben.
 - Geben Sie alle Parameter an, einschließlich des nächsten Hops (derselbe, über den auch der ausgewählte Router erreichbar ist). Für die bevorzugte Binderschnittstelle sollte die IP-Adresse des lokalen Systems angegeben werden, die der virtuellen IP-Adresse zugeordnet ist, die durch diesen Leitweg dargestellt wird.

Beispiel: Failoveraktionen für eine Anwendungs-CRG:

Dieses Beispiel zeigt, wie ein Failoverszenario funktioniert. Andere Failoverszenarios können sich anders verhalten.

Die folgende Situation tritt ein, wenn für eine Clusterressourcengruppe einer ausfallsicheren Anwendung ein Failover durchgeführt wird, weil entweder das Wiederholungslimit überschritten oder der Job abgebrochen wurde:

- Das CRG-Exitprogramm wird auf allen aktiven Knoten in der Wiederherstellungsdomäne für die CRG mit dem Aktionscode für "Failover" aufgerufen. Dies ist ein Hinweis darauf, dass die Cluster Resource Services Vorbereitungen treffen, um den Zugriffspunkt der Anwendung auf den ersten Ausweichknoten zu verschieben.
- Die Cluster Resource Services beenden die IP-Übernahmeverbindung auf dem Primärknoten.
- Die Cluster Resource Services starten die IP-Übernahmeadresse auf dem ersten Ausweichknoten (dem neuen Primärknoten).
- Die Cluster Resource Services übergeben einen Job, der das CRG-Exitprogramm nur auf dem neuen Primärknoten mit dem Aktionscode "Start" aufruft. Mit dieser Aktion wird die Anwendung erneut gestartet.

Zugehörige Konzepte

„Übernahme der IP-Adressen von Anwendungs-CRGs verwalten“ auf Seite 6

Sie können die Übernahme der IP-Adressen von Anwendungs-CRGs mit Hilfe der Cluster Resource Services verwalten. Eine manuelle Verwaltung der Übernahme ist ebenfalls möglich.

Beispiel: Anwendungsexitprogramm:

Dieses Codebeispiel enthält ein CRG-Exitprogramm für Anwendungen.

Sie finden dieses Codebeispiel in der Bibliothek QUSRTOOL.

Anmerkung: Durch die Verwendung der Codebeispiele erklären Sie sich mit den Bedingungen einverstanden, die im „Haftungsausschluss für Programmcode“ auf Seite 183 erläutert werden.

```

/*****/
/*                                           */
/* 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 QATTYSYC 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/qattsys/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 0x00000000000000000000

/*-----*/
/*
/* 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 setApp1CrgDataArea(char *);
#pragma argopt(setApp1CrgDataArea)
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 to be
/* 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 < count

```

```

        ) {
        nodeData++;
        iter++;
    }

    if (iter < 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 <= 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.
    /*
    /*
/*-----*/
    setApp1CrgDataArea(App1_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.
    /*
    /*
/*-----*/
    setApp1CrgDataArea(App1_Ended);
}
else

/*-----*/
    /*
    /* On backup or replicate nodes, mark the status of the application in
    /* the data area as not running.
    /*
    /*
/*-----*/
    setApp1CrgDataArea(App1_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) {
        setApp1CrgDataArea(App1_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.
/*
/*
/*-----*/
    setApp1CrgDataArea(App1_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;
/*
/*
/*
/*
/*-----*/
/*
/* 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.
/*
/*
/*-----*/
    setApp1CrgDataArea(App1_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.
/*
/*
/*-----*/

setApp1CrgDataArea(App1_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 setApp1CrgDataArea(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.
/*
/*
/*-----*/
        setApp1CrgDataArea(App1_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";

```

```

        case QcstMemberFailure:    break;
                                  str = "QcstMemberFailure";
        case QcstEndNode:         break;
                                  str = "QcstEndNode";
        case QcstRemoveNode:     break;
                                  str = "QcstRemoveNode";
        case QcstApplFailure:     break;
                                  str = "QcstApplFailure";
        case QcstResourceEnd:     break;
                                  str = "QcstResourceEnd";
        case QcstDltCluster:     break;
                                  str = "QcstDltCluster";
        case QcstRmvRcvyDmnNode: break;
                                  str = "QcstRmvRcvyDmnNode";
        case QcstDltCrg:         break;
                                  str = "QcstDltCrg";
        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 QcstCrgAcEndNode:    code = "QcstCrgAcEndNode";
                                   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";
    }
}

```

```

        case QcstCrgIndoubt:          break;
        case QcstCrgRestored:         str = "QcstCrgRestored";
        case QcstCrgAddnodePending:  str =
"QcstCrgAddnodePending";
        case QcstCrgDeletePending:   str = "QcstCrgDeletePending";
        case QcstCrgChangePending:   str = "QcstCrgChangePending";
        case QcstCrgEndCrgPending:   str = "QcstCrgEndCrgPending";
        case QcstCrgInitializePending: str =
"QcstCrgInitializePending";
        case QcstCrgRemovenodePending: str =
"QcstCrgRemovenodePending";
        case QcstCrgStartCrgPending: str =
"QcstCrgStartCrgPending";
        case QcstCrgSwitchOverPending: str =
"QcstCrgSwitchOverPending";
        case QcstCrgDeleteCmdPending: str =
"QcstCrgDeleteCmdPending";
        case QcstCrgAddDevEntPending: str =
"QcstCrgAddDevEntPending";
        case QcstCrgRmvDevEntPending: str =
"QcstCrgRmvDevEntPending";
        case QcstCrgChgDevEntPending: str =
"QcstCrgChgDevEntPending";
        case QcstCrgChgNodeStatusPending: str =
"QcstCrgChgNodeStatusPending";
        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<=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 */

```

Ausfallsichere Daten planen

Datenausfallsicherheit bedeutet, dass Daten für Benutzer oder Anwendungen verfügbar sind. Sie kann unter Verwendung der i5/OS-Clustertechnologie mit entweder umschaltbaren Platten (sog. Switched Disks), standortübergreifender Spiegelung oder Technologien für logische Replikation erreicht werden.

Für die von i5/OS unterstützten Implementierungen der Datenausfallsicherheit kann zwischen verschiedenen Technologien ausgewählt werden. Werden diese Technologien mit den i5/OS Cluster Resource Services kombiniert, kann so eine umfassende Hochverfügbarkeitslösung aufgebaut werden. Diese Technologien können wie folgt kategorisiert werden:

Unabhängige Plattenpools unter i5/OS

Diese Technologien basieren alle auf einer i5/OS-Implementierung unabhängiger Plattenpools. Bei einer Hochverfügbarkeitslösung mit unabhängigen Plattenpools müssen alle Daten, die ausfallsicher sein sollen, in einem unabhängigen Plattenpool gespeichert sein. In vielen Fällen bedeutet dies, dass die Daten auf unabhängige Plattenpools migriert werden müssen. In dieser Beschreibung wird vorausgesetzt, dass die Migration der Daten abgeschlossen ist.

Die folgenden von i5/OS unterstützten Technologien basieren auf unabhängigen Plattenpools:

- Umschaltbare Platten
- Geographische Spiegelung
- Metro Mirror
- Global Mirror

Logische Replikation

Logische Replikation ist eine journalbasierte Technologie, mit der Daten in Echtzeit auf ein anderes System repliziert werden. Technologien für logische Replikation kombinieren die i5/OS Cluster Resource Services und Journaling mit Anwendungen von IBM Business Partnern. Diese Lösungen setzen voraus, dass die Umgebung mit einer HA-Anwendung eines Business Partners konfiguriert und verwaltet wird. An

dieser Stelle werden keine spezifischen Voraussetzungen für die Lösungen von IBM Business Partnern genannt. Wenn Sie beabsichtigen, eine Lösung mit logischer Replikation zur Erreichung der Hochverfügbarkeit zu implementieren, informieren Sie sich über das Thema, oder wenden Sie sich an einen zuständigen Ansprechpartner.

Zugehörige Informationen

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

Welche Daten müssen ausfallsicher sein?

Dies sind die Kriterien für die Auswahl der Daten, die ausfallsicher gemacht werden sollten.

Die Entscheidung darüber, welche Daten ausfallsicher sein müssen, ist vergleichbar mit der Auswahl der Daten, die gesichert werden sollen, wenn Sie eine Sicherungs- und Wiederherstellungsstrategie für Ihre Systeme vorbereiten. Sie müssen die Daten in Ihrer Umgebung auswählen, die kritisch für die Aufrechterhaltung des Geschäftsbetriebs sind.

In einem Webunternehmen könnten dies Beispiele für kritische Daten sein:

- Die heutigen Aufträge
- Inventar
- Kundenstammdaten

Im Allgemeinen gilt, dass Informationen, die sich nicht häufig ändern oder die nicht täglich gebraucht werden, nicht ausfallsicher sein müssen.

Umschaltbare Platten planen

Eine Kopie der Daten befindet sich auf der umschaltbaren Hardware, die entweder eine Erweiterungseinheit (Tower) oder ein IOP in einer Umgebung mit logischen Partitionen sein kann.

Wenn der Primärknoten ausfällt, wird der Zugriff auf die Daten, die sich auf der umschaltbaren Hardware befinden, auf einen vorgesehenen Ausweichknoten umgeschaltet. Zusätzlich können in einer Umgebung mit standortübergreifender Spiegelung (Cross-site Mirroring = XSM) unabhängige Plattenpools eingesetzt werden. Damit besteht die Möglichkeit, eine Spiegelkopie des unabhängigen Plattenpools auf einem System zu erzeugen, das sich aus Gründen der Verfügbarkeit und oder als Schutzmaßnahme (optional) geographisch entfernt vom Ursprungsstandort befindet.

Eine sorgfältige Planung ist erforderlich, wenn die Vorteile umschaltbarer Ressourcen genutzt werden sollen, die sich auf umschaltbaren, unabhängigen Plattenpools befinden oder Bestandteil der standortübergreifenden Spiegelung (XSM) sind.

Sie sollten außerdem Ihre aktuelle Systemplattenkonfiguration daraufhin überprüfen, ob zusätzliche Platteneinheiten erforderlich sind. Neben der Systemplattenkonfiguration kann auch die Anzahl der Platteneinheiten, die der Anwendung zur Verfügung stehen, beträchtliche Auswirkungen auf ihre Leistung haben. Wird eine begrenzte Anzahl von Platteneinheiten mit zusätzlicher Workload belastet, kann dies zu längeren Plattenwartezeiten und letztlich auch längeren Antwortzeiten für die Anwendung führen. Dies ist besonders wichtig im Hinblick auf den temporären Speicher in einem System, das mit unabhängigen Plattenpools konfiguriert ist. Der gesamte temporäre Speicher wird in den Plattenpool SYSBAS geschrieben. Wenn Ihre Anwendung nur wenig temporären Speicher in Anspruch nimmt, kommen Sie auch mit weniger Plattenzugriffsarmen im Plattenpool SYSBAS aus. Sie müssen aber berücksichtigen, dass die Betriebssystem- und Basisfunktionen ebenfalls im Plattenpool SYSBAS ausgeführt werden.

Bevor Sie IBM Systems Director Navigator for i5/OS für Plattenverwaltungstasks einsetzen können, wie z. B. zur Erstellung eines unabhängigen Plattenpools, müssen Sie die richtigen Berechtigungen für die Dedicated Service Tools (DST) einrichten.

Zugehörige Tasks

Enabling and accessing disk units

| **Hardwarevoraussetzungen für umschaltbare Platten:**

| Für den Einsatz umschaltbarer Platten (sog. Switched Disks) ist spezielle Hardware erforderlich.

| Für den Einsatz umschaltbarer Platten benötigen Sie entweder

- | • eine oder mehrere Erweiterungseinheiten (Frames/Einheiten) an einem HSL-Loop (High-speed Link = Hochgeschwindigkeitsverbindung);
- | • einen oder mehrere IOPs auf einem gemeinsam genutzten Bus oder einen IOP, der einem E/A-Pool zugeordnet ist. In einer LPAR-Umgebung kann der IOP, der die unabhängigen, umschaltbaren Platten steuert, zwischen Systempartitionen umgeschaltet werden, ohne dass eine Erweiterungseinheit vorhanden ist. Der IOP muss sich auf dem Bus befinden, der von mehreren Partitionen gemeinsam genutzt wird, oder einem E/A-Pool zugeordnet sein. Alle IOAs auf dem IOP werden umgeschaltet.

| Zusätzlich zu diesen Hardwarevoraussetzungen für die umschaltbaren Platten ist bei der Installationsplanung Folgendes erforderlich:

- | • Für den Anschluss der Erweiterungseinheiten an die Systeme im Cluster müssen HSL-Kabel verwendet werden. Die Erweiterungseinheit muss sich im HSL-Loop physisch in der Nähe des alternativen Systems oder der Erweiterungseinheit befinden, die zum alternativem System gehört. Die Anzahl der Systeme (Clusterknoten) pro HSL-Loop ist auf zwei begrenzt, wobei jedes System mit mehreren HSL-Loops verbunden sein kann. Die Anzahl der Erweiterungseinheiten pro HSL-Loop ist auf vier begrenzt, wobei aber maximal drei Erweiterungseinheiten pro Loopsegment vorhanden sein können. In einem HSL-Loop mit zwei Systemen sind zwei Segmente vorhanden, die durch die beiden Systeme voneinander getrennt sind. Alle Erweiterungseinheiten in einem Loopsegment müssen sich in derselben Einheiten-Clusterressourcengruppe (Einheiten-CRG) befinden.
- | • Damit eine Erweiterungseinheit umgeschaltet werden kann, muss sie die Einheit in dem Loopsegment sein, die am weitesten vom Eignersystem entfernt ist. Anmerkung: Wenn Sie versuchen, eine Erweiterungseinheit umschaltbar zu machen und eine weitere Erweiterungseinheit vorhanden ist, die sich in größerer Entfernung vom Eignersystem befindet, aber nicht umschaltbar ist, tritt ein Fehler auf.
- | • Die umschaltbare Erweiterungseinheit muss per SPCN-Verkabelung mit der Systemeinheit verbunden sein, die zunächst als Primärknoten für die Einheiten-CRG fungiert. Der Primärknoten kann eine primäre oder sekundäre logische Partition innerhalb der Systemeinheit sein. Bei Verwendung logischer Partitionen müssen die Systembusse in der vorgesehenen Erweiterungseinheit der am Cluster beteiligten Partition gehören und von dieser dediziert zugeordnet werden.

| **Softwarevoraussetzungen für umschaltbare Platten:**

| Wenn Sie beabsichtigen, umschaltbare Platten für eine i5/OS-Hochverfügbarkeitslösung einzusetzen, müssen Sie dafür sorgen, dass die Softwaremindestvoraussetzungen erfüllt sind.

- | • Damit Sie die neuen und funktional erweiterten Funktionen und Features dieser Technologie nutzen können, wird empfohlen, den aktuellsten Versions- und Release-Level des Betriebssystems auf jedem System oder jeden logischen Partition zu installieren, die an der Hochverfügbarkeitslösung basierend auf dieser Technologie beteiligt ist.

| **Anmerkung:** Befinden sich mehrere Systeme im selben HSL-Loop, sollten Sie die Website zum Thema Hochverfügbarkeit besuchen, um sicherzustellen, dass Sie über kompatible Versionen von i5/OS verfügen.

- | • Eine der folgenden grafischen Oberflächen wird benötigt, um einige der Plattenverwaltungstasks auszuführen, die für die Implementierung der unabhängigen Plattenpools erforderlich sind.
 - | – IBM Systems Director Navigator for i5/OS
 - | – System i Navigator
- | • Sie müssen i5/OS Option 41 HA Switchable Resources installieren. Mithilfe von Option 41 können unabhängige Plattenpools zwischen Systemen umgeschaltet werden. Für das Umschalten dieser Plattenpools zwischen Systemen müssen die Systeme Mitglieder eines Clusters und die unabhängigen Plattenpools einer Einheiten-CRG in diesem Cluster zugeordnet sein. Option 41 wird zum Arbeiten mit

| HA-Managementschnittstellen benötigt, die als Teil des Lizenzprogramms IBM System i High Availability Solutions Manager (iHASM) bereitgestellt werden.

| **Zugehörige Informationen**

| High Availability and Clusters

| **Kommunikationsvoraussetzungen für umschaltbare Platten:**

| Für umschaltbare Platten ist mindestens eine TCP/IP-Kommunikationsschnittstelle zwischen den Systemen im Cluster erforderlich.

| Aus Redundanzgründen werden mindestens zwei separate Schnittstellen zwischen den Systemen empfohlen.

Standortübergreifende Spiegelung planen

Die standortübergreifende Spiegelung stellt mehrere Technologien für die Wiederherstellung nach einem Katastrophenfall und die Hochverfügbarkeit unter i5/OS zur Verfügung. Dazu gehören: geographische Spiegelung, Metro Mirror und Global Mirror.

Bei den Technologien für standortübergreifende Spiegelung wird die Wiederherstellung nach einem Katastrophenfall über separate Standorte implementiert, die normalerweise geographisch voneinander getrennt sind. Jede dieser Technologien zeichnet sich durch spezielle Kommunikations-, Hardware- und Softwarevoraussetzungen aus. Bevor Sie eine dieser Technologien implementieren, sollten Sie auch die Standorte planen. Ein Standort ist normalerweise der Produktions- oder Quellenstandort. An diesem Standort befinden sich die Produktionsdaten, die auf den fernen Standort gespiegelt oder kopiert werden. Am fernen Standort, der auch als Ausweich- oder Zielstandort bezeichnet wird, befindet sich die gespiegelte Kopie der Produktionsdaten. Wenn es am Produktionsstandort zu einem Komplettausfall kommt, setzt der Ausweichstandort Ihre Geschäftsprozesse mit den gespiegelten Daten fort. Vor der Konfiguration der standortübergreifenden Spiegelung sollten Sie folgende Hinweise hinsichtlich der Standortplanung berücksichtigen.

Produktions- und Ausweichstandort bestimmen

Überprüfen Sie die Hardware- und Softwareressourcen an jedem Standort daraufhin, ob alle Komponenten, die für eine Lösung mit standortübergreifender Spiegelung benötigt werden, vorhanden sind.

Entfernung zwischen Produktions- und Ausweichstandort bestimmen

Abhängig von der Kommunikationsbandbreite und anderen Faktoren kann sich die Entfernung zwischen den Standorten auf Leistung und Latenz der ausgewählten Spiegelungstechnologie auswirken. Einige Technologien der standortübergreifenden Spiegelung sind besser für Standorte geeignet, die weiter voneinander entfernt sind, während bei anderen Leistungseinbußen auftreten können.

Richtige Berechtigung für DST einrichten

Bevor Sie IBM Systems Director Navigator for i5/OS zur Ausführung von Plattenverwaltungstasks einsetzen können, müssen Sie die richtigen Berechtigungen für die Dedicated Service Tools (DST) einrichten.

Zugehörige Tasks

Enabling and accessing disk units

Geographische Spiegelung planen:

Geographische Spiegelung ist die Unterfunktion der standortübergreifenden Spiegelung. Diese Technologie unterstützt die Wiederherstellung nach einem Katastrophenfall und Hochverfügbarkeit in i5/OS-Umgebungen.

| *Hardwarevoraussetzungen für geographische Spiegelung:*

- | Wenn Sie geographische Spiegelung als Bestandteil einer i5/OS-Hochverfügbarkeitslösung planen, vergewissern Sie sich, dass die Hardwaremindestvoraussetzungen erfüllt sind.
- | • Alle Hardwarevoraussetzungen in Bezug auf unabhängige Plattenpools müssen erfüllt sein.
- | • Es werden mindestens zwei geographisch voneinander getrennte System i-Modelle benötigt.
- | • An jedem Standort werden mindestens zwei Plattensätze mit derselben Kapazität benötigt.
- | • Es sollte ein separater Speicherpool für Jobs unter Verwendung geographisch gespiegelter unabhängiger Plattenpools konfiguriert werden. Geographische Spiegelung des Hauptspeicherpools kann bei extremen Workloadbedingungen eine Blockierung des Systems zur Folge haben.
- | • Geographische Spiegelung wird ausgeführt, wenn der Plattenpool verfügbar ist. Der Systemwert für die Uhrzeit (QTIME) darf während der Ausführung der geographischen Spiegelung nicht geändert werden.
- | • Die Kommunikationsvoraussetzungen für unabhängige Plattenpools sind besonders kritisch, da sie sich auf den Durchsatz auswirken.

Zugehörige Konzepte

„Kommunikationsvoraussetzungen für geographische Spiegelung“

Wenn Sie eine i5/OS-Hochverfügbarkeitslösung mit geographischer Spiegelung implementieren, sollten Sie entsprechende Übertragungsleitungen einplanen, damit sich der Datenverkehr der geographischen Spiegelung nicht nachteilig auf die Systemleistung auswirkt.

Softwarevoraussetzungen für geographische Spiegelung:

Wenn Sie geographische Spiegelung als Bestandteil einer i5/OS-Hochverfügbarkeitslösung planen, ist die folgende Software erforderlich.

- Um die erweiterten Funktionen der geographischen Spiegelung nutzen zu können, muss IBM System i High Availability Solutions Manager (iHASM), Lizenzprogrammnummer 5761-HAS, installiert werden.
- Damit Sie die neuen und funktional erweiterten Funktionen und Features dieser Technologie nutzen können, wird empfohlen, den aktuellsten Versions- und Release-Level des Betriebssystems auf jedem System oder jeden logischen Partition zu installieren, die an der Hochverfügbarkeitslösung basierend auf dieser Technologie beteiligt ist.

Anmerkung: Befinden sich mehrere Systeme im selben HSL-Loop, sollten Sie die Website zum Thema Hochverfügbarkeit besuchen, um sicherzustellen, dass Sie über kompatible Versionen von i5/OS verfügen.

- Eine der folgenden grafischen Oberflächen wird benötigt, um einige der Plattenverwaltungstasks auszuführen, die für die Implementierung der unabhängigen Plattenpools erforderlich sind.
 - IBM Systems Director Navigator for i5/OS
 - System i Navigator
- Sie müssen i5/OS Option 41 HA Switchable Resources installieren. Mithilfe von Option 41 können unabhängige Plattenpools zwischen Systemen umgeschaltet werden. Für das Umschalten dieser Plattenpools zwischen Systemen müssen die Systeme Mitglieder eines Clusters und die unabhängigen Plattenpools einer Einheiten-CRG in diesem Cluster zugeordnet sein. Option 41 wird zum Arbeiten mit HA-Managementschnittstellen benötigt, die als Teil des Lizenzprogramms IBM System i High Availability Solutions Manager (iHASM) bereitgestellt werden.

Zugehörige Informationen

High Availability and Clusters

Kommunikationsvoraussetzungen für geographische Spiegelung:

- | Wenn Sie eine i5/OS-Hochverfügbarkeitslösung mit geographischer Spiegelung implementieren, sollten Sie entsprechende Übertragungsleitungen einplanen, damit sich der Datenverkehr der geographischen Spiegelung nicht nachteilig auf die Systemleistung auswirkt.

| Hier einige Empfehlungen:

| • Durch die geographische Spiegelung kann Datenverkehr mit großen Datenvolumen erzeugt werden. Wenn für die geographische Spiegelung dieselbe IP-Verbindung wie für eine andere Anwendung, z. B. für Clustering, verwendet wird, kann die geographische Spiegelung ausgesetzt werden, was zur Synchronisation führt. Ferner könnten die Clustering-Antworten nicht akzeptabel sein, was zu partitionierten Knoten führt. Für die geographische Spiegelung sollten dedizierte Übertragungsleitungen vorhanden sein. Ist keine eigene Übertragungsleitung für die geographische Spiegelung vorhanden, kommt es zu einer Konkurrenzsituation mit anderen Anwendungen, die ebenfalls diese Übertragungsleitung nutzen, was sich auf die Netzwerkleistung und den Durchsatz auswirken kann. Dazu gehören auch negative Auswirkungen auf die Heartbeatüberwachung im Cluster, wodurch Knoten im Cluster "partitioniert", d. h., vom Cluster getrennt werden können. Daher werden dedizierte Übertragungsleitungen sowohl für die geographische Spiegelung als auch für die Cluster empfohlen. Die geographische Spiegelung unterstützt bis zu vier Übertragungsleitungen.

| Bei der geographischen Spiegelung werden Änderungen zur Erzielung einer optimalen Leistung über mehrere Leitungen verteilt. Die Daten werden der Reihe nach über jede der konfigurierten Übertragungsleitungen gesendet, wobei der Vorgang von Leitung 1 bis 4 laufend wiederholt wird. Vier Übertragungsleitungen bieten die höchste Leistung, aber schon mit zwei Leitungen kann eine relative gute Leistung erzielt werden.

| Werden zwei oder mehr Übertragungsleitungen zwischen den Knoten für die geographische Spiegelung verwendet, sollten diese Leitungen in mehrere Teilnetze aufgeteilt werden, damit die Nutzung der Leitungen zwischen beiden Systemen ausgeglichen ist.

| • Ist Ihre Konfiguration so angelegt, dass mehrere Anwendungen und Services dieselbe Übertragungsleitung nutzen müssen, können einige dieser Probleme verringert werden, indem Servicequalität (Quality of Service = QoS) über die TCP/IP-Funktionen von i5/OS implementiert wird. Mit der i5/OS-Lösung für Servicequalität werden die Richtlinien zum Anfordern von Netzwerkpriorität und Bandbreite für TCP/IP-Anwendungen im gesamten Netzwerk realisiert.

| Werden zwei oder mehr Übertragungsleitungen zwischen den Knoten für die geographische Spiegelung verwendet, sollten diese Leitungen in mehrere Teilnetze aufgeteilt werden, damit die Nutzung der Leitungen zwischen beiden Systemen ausgeglichen ist.

| • Achten Sie darauf, dass der Durchsatz der Datenportverbindungen einheitlich ist. Dies bedeutet, dass Geschwindigkeit und Verbindungsart für alle Verbindungen zwischen Systempaaren übereinstimmen sollten. Ist der Durchsatz unterschiedlich, richtet sich die Leistung nach der langsamsten Verbindung.

| • Ziehen Sie die Konfiguration eines virtuellen privaten Netzes (VPN) für TCP/IP-Verbindungen in Erwägung, um folgende Vorteile nutzen zu können:

- | – Sicherheit bei der Datenübertragung durch Datenverschlüsselung
- | – Größere Zuverlässigkeit der Datenübertragung durch Senden umfangreicher Redundanzdaten

| **Zugehörige Konzepte**

| „Hardwarevoraussetzungen für geographische Spiegelung“ auf Seite 51

| Wenn Sie geographische Spiegelung als Bestandteil einer i5/OS-Hochverfügbarkeitslösung planen, vergewissern Sie sich, dass die Hardwaremindestvoraussetzungen erfüllt sind.

| **Zugehörige Verweise**

| Quality of Service (QoS)

Journalplanung für geographische Spiegelung:

Vor der Implementierung der Hochverfügbarkeit auf Basis der geographischen Spiegelung unter i5/OS sollten Sie die Journalverwaltung planen.

Durch die Journalverwaltung wird verhindert, dass bei einer abnormalen Beendigung des Systems Transaktionen verloren gehen. Bei der Aufzeichnung eines Objekts im Journal werden die an dem Objekt vorgenommenen Änderungen vom System erfasst. Unabhängig von der implementierten HA-Lösung wird Journaling als die beste Methode angesehen, um Datenverluste bei abnormalen Systemausfällen zu verhindern.

Zugehörige Informationen

Journal management

| *Planung einer Sicherheitsstrategie für geographische Spiegelung:*

| Vor der Implementierung der Hochverfügbarkeit auf Basis der geographischen Spiegelung sollten Sie eine Sicherheitsstrategie für diese Umgebung vorsehen und planen.

| Bevor Sie eine Hochverfügbarkeitslösung konfigurieren, sollten Sie Ihre aktuelle Sicherheitsstrategie überprüfen und gegebenenfalls Änderungen vornehmen. Bei der geographischen Spiegelung ist gleichzeitiger Zugriff auf die Spiegelkopie des unabhängigen Plattenpools nicht zulässig, was wiederum Auswirkungen auf ferne Sicherungen hat. Soll die durch geographische Spiegelung erzeugte gespiegelte Kopie auf Band gesichert werden, muss die Spiegelung auf dem Produktionssystem stillgelegt und die gespiegelte Kopie mit aktivierter Überwachung abgehängt werden. Durch die Überwachung können Änderungen auf dem Produktionssystem verfolgt und später mit der gespiegelten Kopie synchronisiert werden, wenn diese wieder im Onlinebetrieb ist. Anschließend muss die abgehängte Kopie des unabhängigen Plattenpools angehängt, die Sicherungsprozedur durchgeführt, der unabhängige Plattenpool ab- und wieder an den ursprünglichen Produktionshost angehängt werden. Bei diesem Prozess ist nur eine partielle Datenresynchronisation zwischen der Produktionskopie und den gespiegelten Kopien erforderlich.

| Ihr System ist ungeschützt, während die Sicherungen laufen und wenn die Synchronisation stattfindet. Es wird außerdem empfohlen, die Spiegelung mit aktivierter Überwachung auszusetzen, wodurch der Synchronisationsprozess beschleunigt wird. Synchronisation ist auch erforderlich, wenn permanente Übertragungsunterbrechungen auftreten, wie z. B. beim Verlust aller Kommunikationspfade zwischen dem Quellen- und dem Zielsystem während eines längeren Zeitraums. Es können auch redundante Kommunikationspfade verwendet werden, die dazu beitragen, dass einige der Risiken im Zusammenhang mit Kommunikationsfehlern vermieden werden.

| Es wird empfohlen, geographische Spiegelung noch mindestens für ein drittes System oder eine dritte logische Partition einzurichten, damit die Produktionskopie des unabhängigen Plattenpools auf ein anderes System am gleichen Standort, das ebenfalls geographische Spiegelung unterstützt, umgeschaltet werden kann.

Zugehörige Konzepte

| „Szenario: Sicherungen in einer Umgebung mit geographischer Spiegelung durchführen“ auf Seite 118
Dieses Szenario verschafft Ihnen einen Überblick über die Tasks, die bei Durchführung einer Sicherung über Remotezugriff für eine i5/OS-Hochverfügbarkeitslösung mit geographischer Spiegelung erforderlich sind.

| „Szenario: Umschaltbare Platte mit geographischer Spiegelung“ auf Seite 81
In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die umschaltbare Platten mit geographischer Spiegelung in einem aus drei Knoten bestehenden Cluster verwendet. Mit dieser Lösung ist sowohl eine Wiederherstellung nach einem Katastrophenfall als auch Hochverfügbarkeit sicherstellt.

| *Leistungsplanung für geographische Spiegelung:*

| Bei der Implementierung einer geographischen Spiegelung müssen Sie Ihre Umgebung so planen, dass potenzielle nachteilige Auswirkungen auf das Leistungsverhalten minimiert werden.

| Eine Vielzahl von Faktoren kann sich auf die Leistung einer geographischen Spiegelung auswirken. Die folgenden Faktoren sollten bei der allgemeinen Planung zur Erzielung einer maximalen Leistung in einer Umgebung mit geographischer Spiegelung berücksichtigt werden:

| Was muss bei der CPU beachtet werden?

| Geographische Spiegelung erhöht die CPU-Belastung, daher sollte ausreichend große CPU-Kapazität verfügbar sein. Unter Umständen sind weitere Prozessoren zur Erhöhung der CPU-Kapazität erforderlich.
| Allgemein gilt, dass die für die geographische Spiegelung eingesetzten Partitionen mehr als nur einen
| Prozessoranteil benötigen. In einer CPU-Minimalkonfiguration kann möglicherweise eine CPU-Mehrbelas-
| tung von 5 bis 20 % bei der geographischen Spiegelung festgestellt werden. Hat das gespiegelte System
| im Vergleich zum Produktionssystem weniger Prozessoren und finden viele Schreiboperationen statt,
| kann die CPU-Mehrbelastung deutlich bemerkbar sein und die Leistung beeinträchtigen.

| Was muss bei der Größe des Maschinenpools beachtet werden?

| Um bei der geographischen Spiegelung und besonders während der Synchronisation eine optimale Leis-
| tung zu erzielen, müssen Sie die Größe des Maschinenpools um mindestens den durch die folgende For-
| mel ermittelten Wert erhöhen:

- | • Die Größe des zusätzlich benötigten Maschinenpoolspeichers wird wie folgt berechnet: $300 \text{ MB} + 0,3$
| MB x die Anzahl der Plattenzugriffsarme (ARMs) im unabhängigen Plattenpool. Das folgende Beispiel
| zeigt den zusätzlich benötigten Maschinenpoolspeicher für unabhängige Plattenpools mit 90 Plattenzu-
| griffsarmen bzw. 180 Plattenzugriffsarmen:
 - | – $300 + (0,3 \times 90 \text{ ARMs}) = 327 \text{ MB}$ an zusätzlichem Maschinenpoolspeicher
 - | – $300 + (0,3 \times 180 \text{ ARMs}) = 354 \text{ MB}$ an zusätzlichem Maschinenpoolspeicher

| Der zusätzliche Maschinenpoolspeicher wird auf allen Knoten in der Clusterressourcengruppe (CRG)
| benötigt, damit die Zielknoten im Falle eines Switchover oder Failover über ausreichend großen Speicher
| verfügen. Wie immer gilt auch hier: je mehr Platteneinheiten sich in einem unabhängigen Plattenpool
| befinden, desto größer die Leistung, da mehr Vorgänge parallel stattfinden können.

| Um zu verhindern, dass die Leistungsanpassungsfunktion die Maschinenpoolgröße verringert, sollte eine
| der folgenden Maßnahmen durchgeführt werden:

- | 1. Setzen Sie die Mindestgröße des Maschinenpools mit dem Befehl WRKSHRPOOL (Mit gemeinsamen
| Speicherpools arbeiten) oder CHGSHRPOOL (Gemeinsame Speicherpools ändern) auf die berechnete
| Größe (die aktuelle Größe plus der anhand der Formel berechneten zusätzlichen Größe für geographi-
| sche Spiegelung).

| **Anmerkung:** Es wird empfohlen, diese Option im Befehl WRKSHRPOOL (Mit gemeinsamen
| Speicherpools arbeiten) anzugeben.

- | 2. Setzen Sie den Systemwert QPFRADJ (Automatische Leistungsanpassung) auf null. Dadurch wird ver-
| hindert, dass die Größe des Maschinenpools von der Leistungsanpassungsfunktion geändert wird.

| Was muss bei Platteneinheiten beachtet werden?

| Die Leistung der Platteneinheit und des IOA kann sich auf die Gesamtleistung der geographischen Spie-
| gelung auswirken. Dies gilt besonders dann, wenn das Plattensubsystem auf dem gespiegelten System
| langsamer ist als auf dem Quellensystem. Befindet sich die geographische Spiegelung in einem synchro-
| nen Modus, werden alle Schreiboperationen auf der Produktionskopie durch die Plattenschreib-
| operationen auf der gespiegelten Kopie verlangsamt. Somit kann ein langsames Plattensubsystem auf der
| Zielseite Auswirkungen auf die Leistung auf der Quellenseite haben. Diese Auswirkungen können mini-
| miert werden, indem die geographische Spiegelung im asynchronen Modus ausgeführt wird. Im asyn-
| chronen Modus wird die durch das Plattensubsystem auf der Zielseite verursachte Wartezeit verringert
| und eine Bestätigung an die Quellenseite gesendet, wenn sich die geänderte Hauptspeicherseite auf der
| Zielseite im Hauptspeicher befindet.

| Was muss beim Systemplattenpool beachtet werden?

| Neben der Systemplattenkonfiguration kann auch die Anzahl der Platteneinheiten, die der Anwendung zur Verfügung stehen, beträchtliche Auswirkungen auf ihre Leistung haben. Wird eine begrenzte Anzahl von Platteneinheiten mit zusätzlicher Workload belastet, kann dies zu längeren Plattenwartezeiten und letztlich auch längeren Antwortzeiten für die Anwendung führen. Dies ist besonders wichtig im Hinblick auf den temporären Speicher in einem System, das mit unabhängigen Plattenpools konfiguriert ist. Der gesamte temporäre Speicher wird in den Plattenpool SYSBAS geschrieben. Wenn Ihre Anwendung nur wenig temporären Speicher in Anspruch nimmt, kommen Sie auch mit weniger Plattenzugriffen im Plattenpool SYSBAS aus. Sie müssen ferner bedenken, dass die Betriebssystem- und Basisfunktionen ebenfalls im Plattenpool SYSBAS ausgeführt werden.

| Was muss bei der Netzwerkkonfiguration beachtet werden?

| Die Netzwerkverkabelung und Konfiguration können sich möglicherweise auf die Leistung der geographischen Spiegelung auswirken. Darüber hinaus muss bei der Netzwerkadressierung sichergestellt sein, dass sich jede Gruppe von Datenport-IP-Adressen in einem anderen Teilnetz befindet, und die Netzwerkverkabelung und Konfiguration sollte entsprechend eingerichtet sein.

Metro Mirror planen:

i5/OS-Hochverfügbarkeit unterstützt Metro Mirror. Diese Art der Spiegelung bietet Hochverfügbarkeit und Wiederherstellung nach einem Katastrophenfall. Damit einer Hochverfügbarkeitslösung, die diese Technologie einsetzt, effizient konfiguriert und verwaltet werden kann, ist eine sorgfältige Planung erforderlich.

Zugehörige Informationen

-  [Guidelines and recommendations for using Copy Services functions with DS6000](#)
-  [Guidelines and recommendations for using Copy Services functions with DS8000](#)

Hardwarevoraussetzungen für Metro Mirror:

Wenn Sie eine i5/OS-Hochverfügbarkeitslösung mit Metro-Mirror-Technologie konfigurieren und verwalten, sollten Sie sich vergewissern, dass die Hardwaremindestvoraussetzungen erfüllt sind.

Die folgenden Hardwaremindestvoraussetzungen werden empfohlen:

- Mindestens zwei System i-Modelle, die geographisch getrennt sind, wobei mindestens eine externe Speichereinheit IBM System Storage DS6000 oder DS8000 an jedes System angeschlossen ist. Die externen Speichereinheiten DS6000 und DS8000 werden an allen System i-Modellen unterstützt, die Glasfaserkabelanschluss für externe Speicher unterstützen.
- Einer der folgenden unterstützten Glasfaserkabeladapter ist erforderlich:
 - 2766 2 Gigabit Fibre Channel Disk Controller PCI
 - 2787 2 Gigabit Fibre Channel Disk Controller PCI-X
 - 5760 4 Gigabit Fibre Disk Controller PCI-X
- Zur Unterstützung einer externen IPL-Einheit auf der DS6000 oder DS8000 ist ein neuer IOP erforderlich:
 - Feature 2847 PCI-X IOP für SAN-Ladequelle
- Die Auswahl einer angemessenen Plattengröße für den Systemspeicher sollte vor der Konfiguration erfolgt sein. Sie benötigen einen Plattensatz für die Quelle und einen gleich großen Plattensatz für das Ziel sowie einen weiteren Plattensatz für jede konsistente Kopie.

Zugehörige Informationen

-  [iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5](#)

 [IBM System Storage DS6000 Information Center](#)

 [IBM System Storage DS8000 Information Center](#)

| *Softwarevoraussetzungen für Metro Mirror:*

| Bevor Sie eine i5/OS-Hochverfügbarkeitslösung mit Metro-Mirror-Technologie konfigurieren, sollten Sie sich vergewissern, dass die Softwaremindestvoraussetzungen erfüllt sind.

| Bei Metro Mirror bestehen folgende Softwaremindestvoraussetzungen:

- | • Auf jedem System i-Modell in der Hochverfügbarkeitslösung muss i5/OS V6R1 in Verbindung mit dem Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS, ausgeführt werden.

| **Anmerkung:** Bei früheren Releases können weiterhin die IBM Kopierservices für System i, ein Angebot der Lab Services, zum Arbeiten mit IBM System Storage-Lösungen verwendet werden. Wenn Global Mirror auf mehreren Plattformen eingesetzt wird oder auf mehreren System i-Partitionen implementiert werden soll, können Sie auch die IBM Kopierservices für System i verwenden.

- | • Das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS, muss auf jedem System installiert sein, das an der Hochverfügbarkeitslösung mit Metro Mirror beteiligt ist.
- | • Sie müssen i5/OS Option 41 HA Switchable Resources installieren. Option 41 ermöglicht das Umschalten der unabhängigen Plattenpools zwischen Systemen. Für das Umschalten dieser Plattenpools zwischen Systemen müssen die Systeme Mitglieder eines Clusters und die unabhängigen Plattenpools einer Einheiten-CRG in diesem Cluster zugeordnet sein. Option 41 wird zum Arbeiten mit HA-Managementschnittstellen benötigt, die als Teil des Lizenzprogramms IBM System i High Availability Solutions Manager (iHASM) bereitgestellt werden.
- | • Zur Speichersteuerung benötigt das Lizenzprogramm iHASM ferner eine Speicherbefehlszeilenschnittstelle (DSCLI). DSCLI ist eine Software, die für alle IBM System Storage-Lösungen erforderlich ist. Als Voraussetzung für die Verwaltung einer IBM System Storage-Lösung wie Flashcopy, Metro Mirror oder Global Mirror muss DSCLI auf jedem der Systeme oder Partitionen installiert sein, die an der Hochverfügbarkeitslösung mit diesen Speichersystemen beteiligt sind. Bei DSCLI bestehen folgende zusätzliche Softwarevoraussetzungen:
 - | – Java Version 1.4
 - | – Option 35 (CCA Cryptographic Service Provider) muss auf jedem System oder jeder Partition installiert sein
- | • Vergewissern Sie sich, dass die neuesten PTFs installiert sind.

| **Zugehörige Informationen**

|  [iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5](#)

|  [IBM System Storage DS6000 Information Center](#)

|  [IBM System Storage DS8000 Information Center](#)

| *Kommunikationsvoraussetzungen für Metro Mirror:*

| Bevor Sie eine i5/OS-Hochverfügbarkeitslösung mit Metro-Mirror-Technologie konfigurieren, sollten Sie sich vergewissern, dass die Kommunikationsmindestvoraussetzungen erfüllt sind.

| Für die Nutzung der Metro-Mirror-Technologie müssen Sie entweder bereits ein Speicherbereichsnetz (SAN = Storage Area Network) einsetzen oder den Einsatz eines SAN planen.

| Ein SAN ist eine dedizierte, zentral verwaltete, sichere Informationsinfrastruktur, die Any-to-Any-Verbindungen zwischen Systemen und Speichersystemen ermöglicht. SAN-Konnektivität ist die Voraussetzung für den Einsatz von IBM System Storage, wie beispielsweise der externen Speichereinheiten DS8000 und DS6000.

| Dies sind die Kommunikationsmindestvoraussetzungen für eine i5/OS-Hochverfügbarkeitslösung mit Metro Mirror:

- | • Einer der folgenden unterstützten Glasfaserkabeladapter ist erforderlich:
 - | – 2766 2 Gigabit Fibre Channel Disk Controller PCI
 - | – 2787 2 Gigabit Fibre Channel Disk Controller PCI-X
 - | – 5760 4 Gigabit Fibre Disk Controller PCI-X
- | • Das System i-Produkt unterstützt eine Vielzahl von SAN-Switches und -Directors. Eine vollständige Liste der unterstützten Switches und Directors finden Sie auf der Website zum Storage Area Network (SAN).
- | • Darüber hinaus wird die Nutzung von Multipath I/O empfohlen, um die Ausfallsicherheit und Leistung insgesamt zu verbessern. Mit Multipath I/O können mehrere Fibre-Channel-Einheiten (FC-Einheiten) für dieselben logischen Platteneinheiten innerhalb des Speichers konfiguriert werden. Bei einer ordnungsgemäßen Konfiguration bleibt die Verbindung zu den Platteneinheiten bestehen, selbst wenn einzelne Einheiten, E/A-Gehäuse oder auch HSL-Loops ausfallen. Multipath bietet außerdem Leistungsvorteile durch die Verteilung der Workload auf alle verfügbaren Verbindungen (Pfade). Jede Verbindung zu einer Multipath-Platteneinheit arbeitet unabhängig. Mehrere Verbindungen bieten erhöhte Ausfallsicherheit, da der Plattenspeicher auch dann weiterhin verwendet werden kann, wenn ein einzelner Pfad ausfällt.

Zugehörige Verweise

|  Website Storage area network (SAN)

Journalplanung für Metro Mirror:

Das Journaling hat eine wichtige Funktion bei der Verkürzung der Wiederanlaufzeit für alle Hochverfügbarkeitslösungen. Im Falle der auf IBM System Storage basierenden Technologien wie Metro Mirror ist es unerlässlich, dass Journaling verwendet wird, um Schreiboperationen auf externe Speichereinheiten zu erzwingen, da die Datenspiegelung außerhalb des System i-Speichers stattfindet.

Durch die Journalverwaltung wird verhindert, dass bei einer abnormalen Beendigung des Systems Transaktionen verloren gehen. Bei der Aufzeichnung eines Objekts im Journal werden die an dem Objekt vorgenommenen Änderungen vom System erfasst. Unabhängig von der implementierten HA-Lösung wird Journaling als die beste Methode angesehen, um Datenverluste bei abnormalen Systemausfällen zu verhindern.

Zugehörige Informationen

Journal management

Planung einer Sicherheitsstrategie für Metro Mirror:

Mit Metro Mirror kann die FlashCopy-Funktion zur Erstellung einer Kopie der Daten verwendet werden, die in externen IBM System Storage-Speichereinheiten gespeichert sind.

Mit FlashCopy-Operationen können Zeitpunktkopien (sog. Point-in-Time-Kopien) erstellt werden. Sobald die FlashCopy-Operation verarbeitet wurde, stehen sowohl der Quellen- als auch der Zieldatenträger zur Nutzung durch Anwendungen zur Verfügung. FlashCopy kann zusammen mit anderen IBM System Storage-Technologien wie Metro Mirror und Global Mirror eingesetzt werden, um konsistente Zeitpunktkopien der Daten an einem fernen Standort zu erstellen, die anschließend mit den Standardsicherungsprozeduren gesichert werden. Folgende Schritte sollten vor der Implementierung von FlashCopy ausgeführt werden:

- Die Quellen- und Zieldatenträger für FlashCopy-Beziehungen identifizieren. Sie sollten FlashCopy-Zieldatenträger in unterschiedlichen Ranks auswählen, um eine bessere Leistung zu erzielen.
- FlashCopy-Datenkonsistenz beachten. Es gibt Umgebungen, in denen Daten im Hauptspeichercache des Systems gespeichert und zu einem späteren Zeitpunkt auf die Platte geschrieben werden. Um diese Art von Neustartaktionen zu vermeiden, sollte sichergestellt werden, dass alle Daten, die auf dem FlashCopy-Quellendatenträger vorhanden sein sollten, auf die Platte geschrieben wurden, bevor die FlashCopy-Operation ausgeführt wird.
- Ein vorhandener Metro-Mirror-Quellendatenträger kann als FlashCopy-Zieldatenträger verwendet werden. Auf diese Weise kann eine Zeitpunktkopie auf dem Zieldatenträger in einem FlashCopy-Datenträgerpaar erstellt werden, und anschließend können diese Daten auf einen Metro-Mirror-Quellendatenträger an einem fernen Standort kopiert werden.

Leistungsplanung für Metro Mirror:

Folgende Leistungsaspekte sollten vor der Metro-Mirror-Konfiguration beachtet werden.

Beachten Sie die folgenden Voraussetzungen und Richtlinien, bevor Sie Metro Mirror verwenden:

- Der Quellen- und Zieldatenträger in einer Metro-Mirror-Beziehung müssen denselben Speichertyp haben.
- Die logischen Quellen- und Zieldatenträger müssen dieselbe Größe haben, oder der Zieldatenträger muss größer sein.
- In Metro-Mirror-Umgebungen sollten die Workload so verteilt werden, dass nicht alle Updates auf eine kleine Gruppe von Datenträgern in einer einzigen Zielspeichereinheit übertragen werden. Leistungsbeeinträchtigungen bei der Speichereinheit am Zielstandort wirken sich nachteilig auf die Leistung am Quellenstandort aus.
- Neben der Systemplattenkonfiguration kann auch die Anzahl der Platteneinheiten, die der Anwendung zur Verfügung stehen, beträchtliche Auswirkungen auf ihre Leistung haben. Wird eine begrenzte Anzahl von Platteneinheiten mit zusätzlicher Workload belastet, kann dies zu längeren Plattenwartenzeiten und letztlich auch längeren Antwortzeiten für die Anwendung führen. Dies ist besonders wichtig im Hinblick auf den temporären Speicher in einem System, das mit unabhängigen Plattenpools konfiguriert ist. Der gesamte temporäre Speicher wird in den Plattenpool SYSBAS geschrieben. Wenn Ihre Anwendung nur wenig temporären Speicher in Anspruch nimmt, kommen Sie auch mit weniger Plattenzugriffen im Plattenpool SYSBAS aus. Sie müssen ferner bedenken, dass die Betriebssystem- und Basisfunktionen ebenfalls im Plattenpool SYSBAS ausgeführt werden.

Zugehörige Informationen

 Guidelines and recommendations for using Copy Services functions with DS6000

 Guidelines and recommendations for using Copy Services functions with DS8000

| Global Mirror planen:

| i5/OS-Hochverfügbarkeit unterstützt Global Mirror. Diese Art der Spiegelung bietet Hochverfügbarkeit und Wiederherstellung nach einem Katastrophenfall in Umgebungen mit externen Speicherlösungen. Damit einer Hochverfügbarkeitslösung, die diese Technologie einsetzt, effizient konfiguriert und verwaltet werden kann, ist eine sorgfältige Planung erforderlich.

| Bei der IBM System Storage-Global-Mirror-Technologie müssen alle Benutzer eine einzige Global-Mirror-Verbindung gemeinsam nutzen. In einer i5/OS-Hochverfügbarkeitslösung mit Global Mirror darf nur eine einzige System i[™]-Partition in der Global-Mirror-Sitzung auf einem bestimmten System Storage-Server aktiv sein. Keine anderen System i-Partitionen oder -Server von anderen Plattformen dürfen Global Mirror zum selben Zeitpunkt nutzen. Wenn einer Global-Mirror-Sitzung mehr als ein Benutzer hinzugefügt wird, kann dies zu unvorhersehbaren Ergebnissen führen.

| Wenn Global Mirror auf mehreren Plattformen eingesetzt wird oder auf mehreren System i-Partitionen implementiert werden soll, können Sie auch die IBM Kopierservices für System i verwenden. Dieses Angebot ist bei Lab Services erhältlich.

| **Zugehörige Informationen**

|  [Guidelines and recommendations for using Copy Services functions with DS6000](#)

|  [Guidelines and recommendations for using Copy Services functions with DS8000](#)

| *Hardwarevoraussetzungen für Global Mirror:*

| Wenn Sie eine i5/OS-Hochverfügbarkeitslösung mit Global-Mirror-Technologie konfigurieren und verwalten, sollten Sie sich vergewissern, dass die Hardwaremindestvoraussetzungen erfüllt sind.

| Die folgenden Hardwaremindestvoraussetzungen müssen für Global Mirror erfüllt sein:

- | • Mindestens zwei System i-Modelle, die geographisch getrennt sind, wobei mindestens eine externe Speichereinheit IBM System Storage DS6000 oder DS8000 an jedes System angeschlossen ist. Die externen Speichereinheiten DS6000 und DS8000 werden an allen System i-Modellen unterstützt, die Glasfaserkabelanschluss für externe Speicher unterstützen.
- | • Einer der folgenden unterstützten Glasfaserkabeladapter ist erforderlich:
 - | – 2766 2 Gigabit Fibre Channel Disk Controller PCI
 - | – 2787 2 Gigabit Fibre Channel Disk Controller PCI-X
 - | – 5760 4 Gigabit Fibre Disk Controller PCI-X
- | • Zur Unterstützung einer externen IPL-Einheit auf der DS6000 oder DS8000 ist ein neuer IOP erforderlich:
 - | – Feature 2847 PCI-X IOP für SAN-Ladequelle
- | • Die Auswahl einer angemessenen Plattengröße für den Systemspeicher sollte vor der Konfiguration erfolgt sein. Sie benötigen einen Plattensatz für die Quelle und einen gleich großen Plattensatz für das Ziel sowie einen weiteren Plattensatz für jede konsistente Kopie.

| **Zugehörige Informationen**

|  [iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5](#)

|  [IBM System Storage DS6000 Information Center](#)

|  [IBM System Storage DS8000 Information Center](#)

| *Softwarevoraussetzungen für Global Mirror:*

| Bevor Sie eine i5/OS-Hochverfügbarkeitslösung mit Global-Mirror-Technologie konfigurieren, sollten Sie sich vergewissern, dass die Softwaremindestvoraussetzungen erfüllt sind.

| Bei Global Mirror bestehen folgende Softwaremindestvoraussetzungen:

- | • Auf jedem System i-Modell in der Hochverfügbarkeitslösung muss i5/OS V6R1 in Verbindung mit dem Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS, ausgeführt werden.

| **Anmerkung:** Bei früheren Releases können weiterhin die IBM Kopierservices für System i, ein Angebot der Lab Services, zum Arbeiten mit IBM System Storage-Lösungen verwendet werden. Wenn Global Mirror auf mehreren Plattformen eingesetzt wird oder auf mehreren System i-Partitionen implementiert werden soll, können Sie auch die IBM Kopierservices für System i verwenden.

- | • Das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS, muss auf jedem System installiert sein, das an der Hochverfügbarkeitslösung mit Global Mirror beteiligt ist.

- | • Zur Speichersteuerung benötigt das Lizenzprogramm iHASM ferner eine Speicherbefehlszeilenschnittstelle (DSCLI). DSCLI ist eine Software, die für alle IBM System Storage-Lösungen erforderlich ist. Als Voraussetzung für die Verwaltung einer IBM System Storage-Lösung wie Flashcopy, Metro Mirror oder Global Mirror muss DSCLI auf jedem der Systeme oder Partitionen installiert sein, die an der Hochverfügbarkeitslösung mit diesen Speichersystemen beteiligt sind. Bei DSCLI bestehen folgende zusätzliche Softwarevoraussetzungen:
- | – Java Version 1.4
- | – Option 35 (CCA Cryptographic Service Provider) muss auf jedem System oder jeder Partition installiert sein
- | • Vergewissern Sie sich, dass die neuesten PTFs installiert sind.

| **Zugehörige Informationen**

|  [iSeries™ and IBM TotalStorage: A Guide to Implementing External Disk on i5](#)

|  [IBM System Storage DS6000 Information Center](#)

|  [IBM System Storage DS8000 Information Center](#)

| *Kommunikationsvoraussetzungen für Global Mirror:*

| Bevor Sie eine i5/OS-Hochverfügbarkeitslösung mit Global-Mirror-Technologie konfigurieren, sollten Sie sich vergewissern, dass die Kommunikationsmindestvoraussetzungen erfüllt sind.

| Für die Nutzung der Global-Mirror-Technologie müssen Sie entweder bereits ein Speicherbereichsnetz (SAN = Storage Area Network) einsetzen oder den Einsatz eines SAN planen.

| Ein SAN ist eine dedizierte, zentral verwaltete, sichere Informationsinfrastruktur, die Any-to-Any-Verbindungen zwischen Systemen und Speichersystemen ermöglicht. SAN-Konnektivität ist die Voraussetzung für den Einsatz von IBM System Storage, wie beispielsweise der externen Speichereinheiten DS8000 und DS6000.

| Dies sind die Kommunikationsmindestvoraussetzungen für eine i5/OS-Hochverfügbarkeitslösung mit Global Mirror:

- | • Einer der folgenden unterstützten Glasfaserkabeladapter ist erforderlich:
 - | – 2766 2 Gigabit Fibre Channel Disk Controller PCI
 - | – 2787 2 Gigabit Fibre Channel Disk Controller PCI-X
 - | – 5760 4 Gigabit Fibre Disk Controller PCI-X
- | • Das System i-Produkt unterstützt eine Vielzahl von SAN-Switches und -Directors. Eine vollständige Liste der unterstützten Switches und Directors finden Sie auf der Website zum Storage Area Network (SAN).
- | • Darüber hinaus wird die Nutzung von Multipath I/O empfohlen, um die Ausfallsicherheit und Leistung insgesamt zu verbessern. Mit Multipath I/O können mehrere Fibre-Channel-Einheiten (FC-Einheiten) für dieselben logischen Platteneinheiten innerhalb des Speichers konfiguriert werden. Bei einer ordnungsgemäßen Konfiguration bleibt die Verbindung zu den Platteneinheiten bestehen, selbst wenn einzelne Einheiten, E/A-Gehäuse oder auch HSL-Loops ausfallen. Multipath bietet außerdem Leistungsvorteile durch die Verteilung der Workload auf alle verfügbaren Verbindungen (Pfade). Jede Verbindung zu einer Multipath-Platteneinheit arbeitet unabhängig. Mehrere Verbindungen bieten erhöhte Ausfallsicherheit, da der Plattenspeicher auch dann weiterhin verwendet werden kann, wenn ein einzelner Pfad ausfällt.

| **Zugehörige Verweise**

|  [Website Storage area network \(SAN\)](#)

| *Journalplanung für Global Mirror:*

| Das Journaling hat eine große Auswirkung auf die Wiederanlaufzeit für alle Hochverfügbarkeitslösungen.
| Im Falle der auf IBM System Storage basierenden Technologien wie Global Mirror ist es unerlässlich, dass
| Journaling verwendet wird, um Schreiboperationen auf externe Speichereinheiten zu erzwingen, da die
| Datenspiegelung außerhalb des System i-Speichers stattfindet.

| Durch die Journalverwaltung wird verhindert, dass bei einer abnormalen Beendigung des Systems Trans-
| aktionen verloren gehen. Bei der Aufzeichnung eines Objekts im Journal werden die an dem Objekt vor-
| genommenen Änderungen vom System erfasst. Unabhängig von der implementierten HA-Lösung wird
| Journaling als die beste Methode angesehen, um Datenverluste bei abnormalen Systemausfällen zu ver-
| hindern.

| **Zugehörige Informationen**

| Journal management

| *Planung einer Sicherheitsstrategie für Global Mirror:*

| Wenn die Hochverfügbarkeitslösung mit der Global-Mirror-Technologie kombiniert wird, können Sie mit
| FlashCopy Zeitpunktkopien Ihrer Daten erstellen.

| Mit FlashCopy-Operationen können Zeitpunktkopien (sog. Point-in-Time-Kopien) erstellt werden. Sobald
| die FlashCopy-Operation verarbeitet wurde, stehen sowohl der Quellen- als auch der Zieldatenträger zur
| Nutzung durch Anwendungen zur Verfügung. FlashCopy kann zusammen mit anderen IBM System Sto-
| rage-Technologien wie Metro Mirror und Global Mirror eingesetzt werden, um konsistente Zeitpunkt-
| kopien der Daten an einem fernen Standort zu erstellen, die anschließend mit den Standardsicherungs-
| prozeduren gesichert werden. Folgende Schritte sollten vor der Implementierung von FlashCopy
| ausgeführt werden:

- | • Die Quellen- und Zieldatenträger für FlashCopy-Beziehungen identifizieren. Sie sollten FlashCopy-Ziel-
| datenträger in unterschiedlichen Ranks auswählen, um eine bessere Leistung zu erzielen.
- | • FlashCopy-Datenkonsistenz beachten. Es gibt Umgebungen, in denen Daten im Hauptspeichercache
| des Systems gespeichert und zu einem späteren Zeitpunkt auf die Platte geschrieben werden. Um diese
| Art von Neustartaktionen zu vermeiden, sollte sichergestellt werden, dass alle Daten, die auf dem Flas-
| hCopy-Quellendatenträger vorhanden sein sollten, auf die Platte geschrieben wurden, bevor die Flash-
| Copy-Operation ausgeführt wird.

| *Leistungsplanung für Global Mirror:*

| Folgende Leistungsaspekte sollten vor der Global-Mirror-Konfiguration beachtet werden.

| Beachten Sie die folgenden Richtlinien zur Leistung, bevor Sie Global Mirror verwenden:

- | • Der Quellen- und Zieldatenträger in einer Metro-Mirror-Beziehung müssen denselben Speichertyp
| haben.
- | • Neben der Systemplattenkonfiguration kann auch die Anzahl der Platteneinheiten, die der Anwendung
| zur Verfügung stehen, beträchtliche Auswirkungen auf ihre Leistung haben. Wird eine begrenzte
| Anzahl von Platteneinheiten mit zusätzlicher Workload belastet, kann dies zu längeren Platten-
| wartezeiten und letztlich auch längeren Antwortzeiten für die Anwendung führen. Dies ist besonders
| wichtig im Hinblick auf den temporären Speicher in einem System, das mit unabhängigen Plattenpools
| konfiguriert ist. Der gesamte temporäre Speicher wird in den Plattenpool SYSBAS geschrieben. Wenn
| Ihre Anwendung nur wenig temporären Speicher in Anspruch nimmt, kommen Sie auch mit weniger
| Plattenzugriffsarmen im Plattenpool SYSBAS aus. Sie müssen ferner bedenken, dass die Betriebssystem-
| und Basisfunktionen ebenfalls im Plattenpool SYSBAS ausgeführt werden.

| **Zugehörige Informationen**



| Guidelines and recommendations for using Copy Services functions with DS6000



| Guidelines and recommendations for using Copy Services functions with DS8000

Logische Replikation planen

Mit der logischen Replikation werden mehrere Datenkopien verwaltet. Die Daten werden vom Primärknoten im Cluster auf die in der Wiederherstellungsdomäne angegebenen Ausweichknoten repliziert oder kopiert. Wenn der Primärknoten ausfällt, bleiben die Daten verfügbar, da ein angegebener Ausweichknoten die Funktion des primären Zugriffspunkts übernimmt.

Bei der *logischen Replikation* werden Kopien von Objekten in Echtzeit erstellt. Replikation ist der Prozess, bei dem Objekte von einem Knoten in einem Cluster auf einen oder mehrere andere Knoten im Cluster kopiert werden. Nach der logischen Replikation sind und bleiben die Objekte auf Ihren Systemen identisch. Änderungen an einem Objekt auf einem Knoten werden auf die übrigen Knoten im Cluster repliziert.

Sie müssen entscheiden, welche Softwaretechnologie für die logische Replikation verwendet werden soll. Folgende Lösungen stehen für die logische Replikation in Ihrem Cluster zur Verfügung:

- **Produkte von IBM Business Partnern**

Mit Datenreplikationssoftware von anerkannten IBM Business Partnern im Bereich Clustering können Sie Objekte über mehrere Knoten replizieren.

- **Eine kundenspezifische Replikationsanwendung**

Mit der IBM Journalverwaltung können die Aktivitäten der Objekte in Ihrem System aufgezeichnet werden. Sie können eine Anwendung schreiben, die die Vorteile der Journalverwaltung für die logische Replikation nutzt.

Zugehörige Informationen

Journal management

Systeme zur Verwendung für die logische Replikation auswählen:

Bei der Auswahl der Systeme, die für die logische Replikation verwendet werden sollen, müssen mehrere wichtige Aspekte beachtet werden.

Diese sind:

- Leistungskapazität
- Plattenkapazität
- Kritische Daten
- Katastrophenschutz

Wenn Ihr System ausfällt, müssen Sie wissen, welche Daten und Anwendungen auf dem primären System und auf dem Ausweichsystem ausgeführt werden. Die kritischen Daten sollten sich auf dem System befinden, das im Falle eines Systemausfalls die Workload am besten handhaben kann. Sie müssen verhindern, dass der Plattenspeicher knapp wird. Falls der Speicherplatz auf dem primären System knapp wird und das System ausfällt, ist es ziemlich wahrscheinlich, dass Ihr Ausweichsystem ebenfalls aufgrund von zu wenig Plattenspeicher ausfallen wird. Damit Ihr Rechenzentrum bei einer Katastrophe, z. B. Überflutung, Feuer oder Blitzschlag, nicht vollständig zerstört wird, sollte sich das replizierte System an einem fernen Standort befinden.

IBM Business Partner für Cluster-Middleware und verfügbare Clustering-Produkte:

Neben den IBM Management Solutions können Sie über einen Anbieter von HA-Lösungen ein Cluster-Middlewareprodukt beziehen, das die Technologie für logische Replikation verwendet.

- | IBM Business Partner für IBM Cluster-Middleware bieten Softwarelösungen für dedizierte Replikations- und Clusterverwaltungsfunktionen an. Die meisten Business Partner-Lösungen basieren auf der logischen Replikation. Bei der logischen Replikation wird eine Kopie von Änderungen auf Objekt- und Satzebene in Echtzeit erstellt. Replikation ist der Prozess, bei dem Objekte von einem Knoten in einem Cluster auf

- | einen oder mehrere andere Knoten im Cluster kopiert werden. Nach der Replikation sind und bleiben die
- | Objekte auf Ihren Systemen identisch. Änderungen an einem Objekt auf einem Knoten werden auf die
- | übrigen Knoten im Cluster repliziert.

Journalplanung für logische Replikation:

Bei der logischen Replikation sollte Journaling eingesetzt werden, damit die Daten der Produktionskopie durch erzwungene Schreiboperationen auf das Ausweichsystem übertragen werden.

Durch die Journalverwaltung wird verhindert, dass bei einer abnormalen Beendigung des Systems Transaktionen verloren gehen. Bei der Aufzeichnung eines Objekts im Journal werden die an dem Objekt vorgenommenen Änderungen vom System erfasst. Unabhängig von der implementierten HA-Lösung wird Journaling als die beste Methode angesehen, um Datenverluste bei abnormalen Systemausfällen zu verhindern.

In Umgebungen mit logischer Replikation ist Journaling die Basis der Lösung und aus diesem Grund bei der Implementierung einer Lösung basierend auf dieser Technologie unerlässlich. Bei der logischen Replikation kann die Echtzeitkopie, die auf das Ausweichsystem übertragen wird, abhängig von der Größe des replizierten Objekts unvollständig sein. Angenommen, ein Programm aktualisiert einen Datensatz in einer Datei, die im Journal aufgezeichnet wird. Im Rahmen derselben Operation wird auch ein Objekt aktualisiert, wie z. B. ein Benutzeradressbereich, der nicht im Journal aufgezeichnet wird. Die Sicherungskopie ist erst dann konsistent, wenn auch der Benutzeradressbereich vollständig auf das Ausweichsystem repliziert wurde. Wenn also das primäre System ausfällt und der Benutzeradressbereich noch nicht vollständig repliziert wurde, ist ein manueller Wiederherstellungsprozess erforderlich, um den Status des Benutzeradressbereichs mit der letzten gültigen Operation abzugleichen, bei der die Daten vollständig repliziert wurden.

Zugehörige Informationen

Journal management

Planung einer Sicherheitsstrategie für logische Replikation:

Wenn Sie die in einer Anwendung eines anderen Herstellers verwendete Technologie für logische Replikation einsetzen, sollten Sie Sicherungsoperationen in dieser Umgebung planen.

Bei der logischen Replikation werden Änderungen an Objekten, wie z. B. an den Dateien oder Programmen einer Produktionskopie, auf eine Sicherungskopie repliziert. Die Replikation findet nahezu in Echtzeit (simultan) statt. Wird das Objekt, z. B. eine Datei, im Journal aufgezeichnet, erfolgt die Replikation auf Datensatzebene. Ein wesentlicher Vorteil dieser Technologie besteht darin, dass in Echtzeit auf die Sicherungskopie zugegriffen werden kann, um Sicherungsoperationen auszuführen. Sie können die Sicherungskopie der Daten ohne Auswirkung auf die Produktionsversion der Daten fern sichern.

Leistungsplanung für logische Replikation:

Wenn Sie den Einsatz der Technologie für logische Replikation als Teil einer HA-Lösung planen, sollten Sie wissen, welche Auswirkungen diese Lösung auf die Leistung hat.

Bei der logischen Replikation ergeben sich potenzielle Auswirkungen auf die Leistung durch die Latenzzeit des Replikationsprozesses. Diese beziehen sich auf die Zeitverzögerung zwischen dem Zeitpunkt, zu dem die Änderungen auf dem Quellsystem durchgeführt werden, und dem Zeitpunkt, zu dem diese Änderungen auf dem Ausweichsystem verfügbar sind. Durch synchrones fernes Journaling kann diese Zeitverzögerung größtenteils minimiert werden. Unabhängig vom verwendeten Übertragungsverfahren müssen Sie das voraussichtliche Übertragungsvolumen berücksichtigen und die Übertragungsleitungen und -geschwindigkeiten korrekt planen, damit die Umgebung die Replikationsvolumen zu Spitzenzeiten steuern kann. In einer Umgebung mit einem hohen Volumen kann die Latenzzeit zu einem Problem auf der Zielseite führen, selbst wenn die Übertragungseinrichtungen korrekt geplant wurden.

Ausfallsichere Umgebung planen

Durch eine ausfallsichere Umgebung wird gewährleistet, dass die Objekte und Attribute für alle in der HA-Umgebung definierten Ressourcen konsistent bleiben. Sie müssen die Ressourcen identifizieren, die für eine einwandfreie Funktionsweise eine konsistente Umgebung benötigen, und eine Clusterverwaltungsdomäne erstellen, die sicherstellt, dass alle Ressourcenattribute in Ihrer HA-Umgebung konsistent bleiben.

Clusterverwaltungsdomäne planen

Eine Clusterverwaltungsdomäne muss geplant werden, um die Ressourcen, die zwischen den Knoten einer Clusterverwaltungsdomäne synchronisiert werden, verwalten zu können. Damit eine Anwendung auf jedem System in einer HA-Umgebung konsistent ausgeführt werden kann, müssen alle Ressourcen, die das Verhalten der Anwendung beeinflussen, sowie die Clusterknoten, auf denen die Anwendung ausgeführt wird oder wo sich die Anwendungsdaten befinden können, identifiziert werden.

Ein Clusteradministrator kann eine Clusterverwaltungsdomäne erstellen und überwachte Ressourcen, die zwischen den Knoten synchronisiert werden, hinzufügen. Der i5/OS-Cluster stellt eine Liste der Systemressourcen zur Verfügung, die als Einträge für überwachte Ressourcen (Monitored Resource Entries = MREs) dargestellt sind und von einer Clusterverwaltungsdomäne synchronisiert werden können.

Beim Entwurf einer Clusterverwaltungsdomäne sollten folgende Fragen beantwortet werden:

Welche Knoten werden in die Clusterverwaltungsdomäne aufgenommen?

Geben Sie an, welche Knoten in einem Cluster von der Clusterverwaltungsdomäne verwaltet werden sollen. Dabei sollten solche Clusterknoten ausgewählt werden, die Systeme darstellen, auf denen eine Anwendung ausgeführt werden kann oder die Anwendungsdaten gespeichert sind, und für deren Ausführung eine konsistente Betriebsumgebung erforderlich ist. Knoten können sich nicht in mehreren Clusterverwaltungsdomänen befinden. Angenommen, ein Cluster enthält vier Knoten (Knoten A, Knoten B, Knoten C und Knoten D). Die Knoten A und B können sich in einer Clusterverwaltungsdomäne befinden, und die Knoten C und D in einer anderen. Es ist jedoch nicht möglich, die Knoten B und C einer dritten Clusterverwaltungsdomäne zuzuordnen und sie gleichzeitig in ihrer ursprünglichen Clusterverwaltungsdomäne zu belassen.

Welche Namenskonventionen bestehen bei Clusterverwaltungsdomänen?

Abhängig von der Komplexität und Größe der Clusterumgebung können Sie eine Standardnamenskonvention für Peer-CRGs und Clusterverwaltungsdomänen einführen. Da bei der Erstellung einer Clusterverwaltungsdomäne auch eine Peer-CRG erstellt wird, ist es sinnvoll, für andere Peer-CRGs eine andere Namenskonvention zu wählen als für die Peer-CRGs, die Clusterverwaltungsdomänen darstellen. Zum Beispiel können Peer-CRGs, die Clusterverwaltungsdomänen darstellen, als *ADMDMN1*, *ADMDMN2* usw. bezeichnet werden, während die anderen Peer-CRGs *PEER1* usw. heißen. Mithilfe der API List Cluster Resource Group Information (Qcst-ListClusterResourceGroupIn) kann festgestellt werden, welche Peer-CRG als Clusterverwaltungsdomäne verwendet wird. Eine Peer-CRG, die eine Clusterverwaltungsdomäne darstellt, kann anhand ihrer Anwendungs-ID identifiziert werden, die QIBM.AdminDomain lautet.

Einträge für überwachte Ressourcen (MREs) planen

Überwachte Ressourcen sind i5/OS-Objekte, die in einer Clusterverwaltungsdomäne definiert werden können. Diese Ressourcen müssen auf allen Systemen einer HA-Umgebung konsistent bleiben, da Anwendungen andernfalls während einer Betriebsunterbrechung unter Umständen nicht wie erwartet ausgeführt werden. Sie sollten planen, welche unterstützten Ressourcen in Ihrer Umgebung überwacht werden sollen.

Sie müssen die Systemressourcen bestimmen, die synchronisiert werden müssen. Dabei können für jede Ressource Attribute ausgewählt werden, um sie für die Synchronisation anzupassen. Anwendungen, die auf mehreren Knoten ausgeführt werden, benötigen für eine ordnungsgemäße Ausführung unter Umständen bestimmte Umgebungsvariablen. Außerdem können für den Zugriff auf Daten, die über mehrere Knoten verteilt sind, verschiedene Benutzerprofile erforderlich sein. Bedenken Sie, welche Voraussetzun-

gen für die Ausführung Ihrer Anwendungen und die Daten erfüllt sein müssen, bevor Sie entscheiden, welche Ressourcen von einer Clusterverwaltungsdomäne verwaltet werden müssen.

Cluster planen

Vor der Implementierung einer HA-Lösung muss sichergestellt sein, dass alle Voraussetzungen für die Cluster erfüllt sind.

Hardwarevoraussetzungen für Cluster

Für die Implementierung einer HA-Lösung muss ein Cluster geplant und konfiguriert werden. In einem Cluster sind die Systeme und Ressourcen einer HA-Umgebung zusammengefasst.

Dies sind die Hardwaremindestvoraussetzungen für Cluster:

- Sie benötigen mindestens zwei System i-Modelle oder logische Partitionen. Ein Cluster kann bis zu 128 Systeme unterstützen. Jedes System i-Modell, auf dem i5/OS V4R4M0 oder ein späteres Release ausgeführt werden kann, ist für Clustering geeignet.
- Der Einsatz einer externen unterbrechungsfreien Stromversorgung (USV) oder einer ähnlichen Einheit zur Notstromversorgung wird empfohlen, um das System vor einem plötzlichen Spannungsverlust zu schützen, was zu einer Clusterpartition führt.
- Clustering verwendet die Multicast-Funktionalität des Internet Protocol (IP). Nicht alle physischen Medien sind für Multicasting geeignet.
- Wenn Sie beabsichtigen, Technologien für Datenausfallsicherheit einzusetzen, die unabhängige Plattenpools erfordern, müssen Sie Hardware einplanen, die die von Ihnen gewählte Technologie für Datenausfallsicherheit unterstützt. Sie können außerdem verschiedene Methoden zum Plattenschutz verwenden, um ein Failover zu verhindern, falls eine geschützte Platte ausfällt.

Zugehörige Konzepte

„Ausfallsichere Daten planen“ auf Seite 48

Datenausfallsicherheit bedeutet, dass Daten für Benutzer oder Anwendungen verfügbar sind. Sie kann unter Verwendung der i5/OS-Clustertechnologie mit entweder umschaltbaren Platten (sog. Switched Disks), standortübergreifender Spiegelung oder Technologien für logische Replikation erreicht werden.

Zugehörige Verweise

„Planungsprüfliste für Cluster“ auf Seite 73

Füllen Sie die Prüfliste für die Clusterkonfiguration aus, damit Ihre Umgebung ordnungsgemäß vorbereitet ist, bevor Sie mit der Clusterkonfiguration beginnen.

Zugehörige Informationen

Unterbrechungsfreie Stromversorgung (USV)

IP multicasting

Disk protection

Softwarevoraussetzungen für Cluster

Für den Einsatz des Clustering sind die korrekte Software und entsprechende Lizenzen erforderlich.

1. i5/OS V6R1 muss installiert sein.
2. Das Feature TCP/IP Connectivity Utilities muss installiert sein.
3. Falls der Einsatz von Technologien für Datenausfallsicherheit, wie umschaltbare Platten oder standortübergreifende Spiegelung geplant wird, bestehen zusätzliche Anforderungen.
4. Option 41 (High Availability Switchable Resources) ist erforderlich, wenn Sie die folgenden Schnittstellen verwenden möchten:
 - Grafische Oberfläche der System i Navigator-Clusterverwaltung

Anmerkung: Informationen zum Arbeiten mit der grafischen Oberfläche der System i Navigator-Clusterverwaltung finden Sie unter Clusters im i5/OS V5R4 Information Center.

- Das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM). Dieses Lizenzprogramm enthält die folgenden Schnittstellen, für die Option 41 erforderlich ist:
 - Grafische Oberfläche des High Availability Solutions Manager
 - Grafische Oberfläche der Cluster Resource Services
 - Befehle für IBM System i High Availability Solutions Manager (iHASM)
 - APIs für IBM System i High Availability Solutions Manager (iHASM)

Anmerkung:

5. Sie können auch das Produkt eines IBM Business Partners verwenden oder unter Verwendung von Cluster-APIs Ihre eigene HA-Managementanwendung schreiben.

Zugehörige Konzepte

„Umschaltbare Platten planen“ auf Seite 49

Eine Kopie der Daten befindet sich auf der umschaltbaren Hardware, die entweder eine Erweiterungseinheit (Tower) oder ein IOP in einer Umgebung mit logischen Partitionen sein kann.

„Standortübergreifende Spiegelung planen“ auf Seite 51

Die standortübergreifende Spiegelung stellt mehrere Technologien für die Wiederherstellung nach einem Katastrophenfall und die Hochverfügbarkeit unter i5/OS zur Verfügung. Dazu gehören: geographische Spiegelung, Metro Mirror und Global Mirror.

„Ausfallsichere Daten planen“ auf Seite 48

Datenausfallsicherheit bedeutet, dass Daten für Benutzer oder Anwendungen verfügbar sind. Sie kann unter Verwendung der i5/OS-Clustertechnologie mit entweder umschaltbaren Platten (sog. Switched Disks), standortübergreifender Spiegelung oder Technologien für logische Replikation erreicht werden.

Zugehörige Verweise

„Planungsprüfliste für Cluster“ auf Seite 73

Füllen Sie die Prüfliste für die Clusterkonfiguration aus, damit Ihre Umgebung ordnungsgemäß vorbereitet ist, bevor Sie mit der Clusterkonfiguration beginnen.

Zugehörige Informationen

Cluster-APIs

Kommunikationsvoraussetzungen für Cluster

Sie können für die Clusterumgebung jede Art von Kommunikationsmedium verwenden, sofern es das Internet Protocol (IP) unterstützt.

Die Cluster Resource Services verwenden für die Kommunikation zwischen den Knoten die Protokolle TCP/IP und UDP/IP. Lokale Netze (LANs), Weitverkehrsnetze (WANs), OptiConnect System Area Networks (SANs) oder beliebige Kombinationen dieser Konnektivitätsoptionen werden unterstützt. Ihre Auswahl sollte auf den folgenden Faktoren beruhen:

- Transaktionsvolumen
- Anforderungen an die Antwortzeit
- Entfernung zwischen den Knoten
- Kostenfaktor

Dieselben Faktoren kommen auch bei der Auswahl der Verbindungsmedien zum Tragen, die für die Verbindung zwischen dem primären und den Ausweichstandorten für die Ressourcen verwendet werden sollen. Bei der Planung des Clusters wird empfohlen, mindestens einen der Ausweichknoten an einem fernen Standort einzurichten, damit bei einem Komplettausfall des primären Standorts der ferne Standort übernehmen kann.

Zur Vermeidung von Leistungsproblemen durch unzureichende Kapazität müssen Sie die Kommunikationsmedien, die zur Übertragung der Datenvolumen von einem Knoten zum anderen verwendet werden, sorgfältig auswählen. Sie können zwischen physischen Medien wie Token-Ring, Ethernet,

asynchronem Übertragungsmodus (ATM), SPD OptiConnect, HSL OptiConnect oder Virtual OptiConnect (einer internen Hochgeschwindigkeitsverbindung zwischen logischen Partitionen) wählen.

HSL OptiConnect ist eine Technologie, die von OptiConnect für i5/OS (i5/OS Option 23 - i5/OS OptiConnect) zur Verfügung gestellt wird. Sie kann zur Realisierung von Hochverfügbarkeitslösungen eingesetzt werden. HSL OptiConnect ist ein System Area Network, das Punkt-zu-Punkt-Konnektivität im Hochgeschwindigkeitsbereich zwischen Clusterknoten durch Einsatz der HSL-Loop-Technologie bietet. Für HSL OptiConnect werden Standard-HSL-Kabel benötigt, aber keine zusätzliche Hardware.

Für umschaltbare Hardware, die auch als ausfallsichere Einheiten-CRG bezeichnet wird, benötigen Sie eine umschaltbare Platte (sog. Switched Disk) in Ihrer Umgebung. In einer Umgebung mit logischen Partitionen ist dies eine Gruppe von Platteneinheiten, die sich an dem Bus befindet, der von den logischen Partitionen gemeinsam benutzt wird, oder die an einen Ein-/Ausgabeprozessor angeschlossen ist, der einem E/A-Pool zugeordnet wurde. Bei einer Umgebung mit mehreren Systemen handelt es sich dabei um eine (oder auch mehrere) umschaltbare Erweiterungseinheiten, die auf dem HSL-Loop konfiguriert sind, der auch die Systeme in der Wiederherstellungsdomäne enthält. Die umschaltbare Erweiterungseinheit kann auch in einer LPAR-Umgebung eingesetzt werden.

Anmerkung: Werden 2810 LAN-Adapter nur mit TCP/IP ohne Systems Network Architecture (SNA) oder IPX verwendet, können Sie die Adapterleistung eines Systems mit OS/400 V4R5M0 erhöhen, indem Sie im Befehl WRKLIND (Mit Leitungsbeschreibungen arbeiten) für den Parameter "Nur für TCP/IP aktivieren" den Wert *YES für die betreffende Leitungsbeschreibung angeben. In OS/400 V5R1M0 und höheren Releases ist der Parameter "Nur für TCP/IP aktivieren" automatisch auf den Wert *YES gesetzt.

Zugehörige Konzepte

„Umschaltbare Platten planen“ auf Seite 49

Eine Kopie der Daten befindet sich auf der umschaltbaren Hardware, die entweder eine Erweiterungseinheit (Tower) oder ein IOP in einer Umgebung mit logischen Partitionen sein kann.

Zugehörige Verweise

„Planungsprüfliste für Cluster“ auf Seite 73

Füllen Sie die Prüfliste für die Clusterkonfiguration aus, damit Ihre Umgebung ordnungsgemäß vorbereitet ist, bevor Sie mit der Clusterkonfiguration beginnen.

Dediziertes Netzwerk für Cluster planen:

Bei normalen Operationen ist der Basiskommunikationsaustausch in einem Cluster minimal. Es wird jedoch empfohlen, redundante Kommunikationspfade für jeden Knoten in einem Cluster zu konfigurieren.

| Redundante Kommunikationspfade bedeuten, dass zwei Leitungen zwischen zwei Knoten in einem Cluster konfiguriert sind. Tritt auf dem ersten Kommunikationspfad ein Fehler auf, kann die Kommunikation über den zweiten Kommunikationspfad fortgesetzt werden, wodurch weitestgehend vermieden werden kann, dass einer oder mehrere Knoten des Clusters in eine Clusterpartition versetzt werden. Bei der Konfiguration der Pfade muss jedoch berücksichtigt werden, dass diese Übertragungsleitungen nach wie vor gefährdet sind, wenn beide Leitungen an denselben Adapter am System angeschlossen sind und dieser Adapter ausfällt. Allerdings ist eine Clusterpartition nicht immer vermeidbar. Kommt es auf dem System zu einem Spannungsverlust oder tritt ein Hardwarefehler auf, kann dies dazu führen, dass der Cluster partitioniert wird. Indem zwei Leitungen konfiguriert werden, kann eine Leitung dediziert für den Clusterdatenverkehr und die andere Leitung für den normalen Datenverkehr und zusätzlich als Ausweichleitung zugeordnet werden, falls die dedizierte Leitung für das Clustering ausfällt. Typische netzwerkbedingte Clusterpartitionierung lässt sich am besten vermeiden, indem redundante Kommunikationspfade zwischen allen Knoten eines Clusters konfiguriert werden.

Tipps für die Clusterkommunikation:

Die folgenden Tipps sollten Sie bei der Konfiguration der Kommunikationspfade beachten.

- Vergewissern Sie sich, dass die Bandbreite der Übertragungsleitungen für die Abwicklung der Nicht-Clusteraktivität sowie den Heartbeataustausch im Cluster ausreicht, und überwachen Sie die Übertragungsleitungen ständig auf erhöhte Aktivität.
- Um bestmögliche Zuverlässigkeit zu erreichen, sollte zwischen den Knoten auf jeden Fall zwei Kommunikationspfade konfiguriert werden.
- Überlasten Sie nicht die Leitung, die eine Fortsetzung der Kommunikation mit einem Knoten gewährleistet.
- Vermeiden Sie möglichst alle Single Points of Failure, wie z. B. zwei Übertragungsleitungen, die an denselben Adapter angeschlossen sind, oder die Verwendung desselben E/A-Prozessors oder derselben Erweiterungseinheit.
- Werden extrem hohe Datenvolumen über die Leitungen übertragen, sollten Sie in Erwägung ziehen, Datenreplikation und Heartbeatüberwachung über separate Netzwerke auszuführen.
- Die Infrastruktur der Clusterkommunikation verwendet die Multicastfunktionen von UDP (User Datagram Protocol) als bevorzugtes Protokoll zum Senden von Clusterverwaltungsinformationen zwischen Knoten in einem Cluster. Wenn Multicastfunktionen von den zugrunde liegenden physischen Medien unterstützt werden, sendet die Clusterkommunikation mit Hilfe der UDP-Multicastfunktionen Verwaltungsnachrichten von einem bestimmten Knoten an alle lokalen Clusterknoten, die dieselbe Teilnetzadresse unterstützen. Nachrichten an Knoten in fernen Netzwerken werden immer mit den Punkt-zu-Punkt-Funktionen von UDP gesendet. Die Clusterkommunikation ist nicht auf die Weiterleitungsfunktion für Multicastnachrichten angewiesen.
- Der Multicastverkehr, der die Übertragung von Clusterverwaltungsnachrichten unterstützt, ist von Natur aus oftmals schwankend. Je nach Anzahl der Knoten in einem LAN (das eine gemeinsame Teilnetzadresse unterstützt) und der Komplexität der Clusterverwaltungsstruktur, die vom Clusteradministrator gewählt wurde, können bei clusterbezogenen Multicastpaketen durchaus mehr als 40 Pakete pro Sekunde gesendet werden. Derartige Schwankungen können sich negativ auf ältere Netzwerkeinheiten auswirken. So könnte z. B. eine Überlastung der Einheiten im LAN auftreten, die als SNMP-Agenten (Simple Network Management Protocol) fungieren und jedes UDP-Multicastpaket auswerten müssen. Einige der älteren Netzwerkeinheiten verfügen nicht über eine ausreichende Bandbreite, um diese Art von Datenaustausch über das Netzwerk zu unterstützen. Sie sollten die Kapazität der Netzwerke für den UDP-Multicastverkehr überprüfen, um sicherzustellen, dass sich das Clustering nicht negativ auf die Leistung der Netzwerke auswirkt, oder diese Prüfung vom Netzwerkadministrator durchführen lassen.

Leistungsplanung für Cluster:

Da in Ihrer Kommunikationsumgebung unter Umständen erhebliche Leistungsschwankungen auftreten können, besteht die Möglichkeit, Variablen, die sich auf die Clusterkommunikation auswirken, entsprechend den Anforderungen Ihrer Umgebung anzupassen.

Der Standardwerte sollten normalerweise für die meisten üblichen Umgebungen geeignet sein. Wenn sich die Standardwerte für Ihre spezielle Umgebung nicht besonders gut eignen, können Sie die Clusterkommunikation entsprechend den Umgebungsanforderungen optimieren. Dazu stehen Basisoptimierungsoptionen und erweiterte Optimierungsoptionen zur Verfügung.

Basisoptimierung

Bei der Basisoptimierung können die Optimierungsparameter auf eine vordefinierte Gruppe von Werten für hohe, niedrige und normale Zeitlimits und Nachrichtenintervalle gesetzt werden. Wird die normale Stufe ausgewählt, werden für die Parameter für die Clusterübertragungsleistung und die Konfigurationsparameter die Standardwerte verwendet. Wird die niedrige Stufe ausgewählt, werden das Heartbeatintervall und die verschiedenen Zeitlimitwerte für Nachrichten erhöht. Mit weniger Heartbeats und höheren Zeitlimitwerten reagieren die Cluster langsamer auf Übertragungsfehler. Wird die hohe Stufe ausgewählt, werden das Heartbeatintervall und die verschiedenen Zeitlimitwerte für Nachrichten verringert. Mit häu-

figeren Heartbeats und niedrigeren Zeitlimitwerten reagieren die Cluster schneller auf Übertragungsfehler.

Erweiterte Optimierung

Bei der erweiterten Optimierung können einzelne Parameter über einen vordefinierten Wertebereich optimiert werden. Auf diese Weise kann eine differenziertere Optimierung vorgenommen werden, um den besonderen Anforderungen Ihrer Kommunikationsumgebung gerecht zu werden. Wenn eine erweiterte Optimierung gewünscht wird, wird empfohlen, Hilfe bei der IBM Benutzerunterstützung oder einer vergleichbaren Unterstützungsfunktion anzufordern. Unsachgemäße Einstellungen für einzelne Parameter können zu einer Leistungsverminderung führen.

Optimierbare Parameter für die Clusterkommunikation:

Über die API QcstChgClusterResourceServices (Change Cluster Resource Services) können einige Clustertopologieservices sowie Parameter für die Clusterkommunikationsleistung und Konfigurationsparameter für die vielen verschiedenen Anwendungs- und Netzbetriebsumgebungen, in denen Clustering verwendet wird, optimiert werden.

Über den Befehl CHGCLU (Cluster ändern) kann die Basisoptimierung ausgeführt werden, während die API QcstChgClusterResourceServices sowohl Basis- als auch erweiterte Optimierung unterstützt.

Mit der API QcstChgClusterResourceServices und dem Befehl CHGCLUCFG (Clusterkonfiguration ändern) können die Clusterleistung und -konfiguration optimiert werden. Die API und der Befehl unterstützen eine Basisoptimierung, mit der der Cluster an eine vordefinierte Gruppe von Werten für hohe, niedrige und normale Zeitlimits und Nachrichtenübertragungsintervalle angepasst wird. Wird eine erweiterte Optimierung gewünscht, die in der Regel von der IBM Benutzerunterstützung betreut wird, können einzelne Parameter mithilfe der API über einen vordefinierten Wertebereich optimiert werden. Unsachgemäße Änderungen einzelner Parameter können zu einer Leistungsverminderung führen.

Wann und wie müssen Clusterparameter optimiert werden?

Der Befehl CHGCLU und die API QcstChgClusterResourceServices bieten die Möglichkeit, die Clusterleistungs- und Konfigurationsparameter per Direktaufruf festzulegen, ohne dass Detailkenntnisse erforderlich sind. Die Basisoptimierung betrifft in erster Linie die Sensitivitätseinstellung für den Heartbeataustausch und die Zeitlimitwerte für Nachrichten. Die gültigen Werte, die von der Basisoptimierung unterstützt werden, lauten wie folgt:

1 (Hohe Zeitlimitwerte/Weniger Heartbeats)

Es werden Anpassungen bei der Clusterkommunikation vorgenommen, um die Heartbeathäufigkeit zu verringern und die verschiedenen Zeitlimitwerte für Nachrichten zu erhöhen. Mit weniger Heartbeats und höheren Zeitlimitwerten reagieren die Cluster langsamer (niedrigere Sensitivität) auf Übertragungsfehler.

2 (Standardwerte)

Für die Parameter für die Clusterübertragungsleistung und die Konfigurationsparameter werden die normalen Standardwerten verwendet. Diese Einstellung kann verwendet werden, um alle Parameter auf die ursprünglichen Standardwerte zurückzusetzen.

3 (Niedrige Zeitlimitwerte/Häufigere Heartbeats)

Es werden Anpassungen bei der Clusterkommunikation vorgenommen, um das Heartbeatintervall und die verschiedenen Zeitlimitwerte für Nachrichten zu verringern. Mit häufigeren Heartbeats und niedrigeren Zeitlimitwerten reagieren die Cluster schneller (höhere Sensitivität) auf Übertragungsfehler.

Die folgende Tabelle enthält Beispielantwortzeiten für einen Heartbeatfehler, der zu einer Knotenpartitionierung führt:

Anmerkung: Die Zeiten sind im Format Minuten:Sekunden angeben.

	1 (Niedrigere Sensitivität)			2 (Standardwert)			3 (Höhere Sensitivität)		
	Erkennung eines Heartbeat-problems	Analyse	Dauer	Erkennung eines Heartbeat-problems	Analyse	Dauer	Erkennung eines Heartbeat-problems	Analyse	Dauer
Einzelnes Teilnetz	00:24	01:02	01:26	00:12	00:30	00:42	00:04	00:14	00:18
Mehrere Teilnetze	00:24	08:30	08:54	00:12	04:14	04:26	00:04	02:02	02:06

Abhängig von der typischen Netzwerklast und den verwendeten physischen Medien kann ein Clusteradministrator entscheiden, ob er die Sensitivitätsebene für Heartbeats und Zeitlimitstufen für Nachrichten anpassen möchte. Werden Transportverbindungen mit hoher Geschwindigkeit und hoher Zuverlässigkeit wie beispielsweise bei OptiConnect eingesetzt und befinden sich alle Systeme im Cluster am selben OptiConnect-Bus, kann es sinnvoll sein, eine Umgebung mit höherer Sensitivität einzurichten, um sicherzustellen, dass Fehler schnell erkannt werden und ein schnelles Failover stattfindet. In diesem Fall wird Option 3 ausgewählt. Erfolgt der Transport über einen stark ausgelasteten 10-MBit/s-Ethernet-Bus und führten die Standardeinstellungen dazu, dass gelegentlich Partitionierungen aufgrund von Netzwerkspitzenbelastungen auftraten, sollte Option 1 gewählt werden, um die Sensitivität des Clustering in Bezug auf Spitzenbelastungen zu verringern.

Über die API Change Cluster Resource Services können außerdem bestimmte einzelne Parameter optimiert werden, wenn die jeweilige Netzwerkumgebung besondere Anforderungen stellt. Betrachten wir nochmals ein Cluster, in dem sich alle Knoten am selben OptiConnect-Bus befinden. Die Leistung von Clusternachrichten kann beträchtlich verbessert werden, indem der Parameter "Nachrichtenfragmentgröße" auf den Maximalwert von 32.500 Byte gesetzt wird, um eine bessere Übereinstimmung mit dem Wert für die maximale Übertragungseinheit (MTU = Maximum Transmission Unit) von OptiConnect zu erreichen, als dies mit dem Standardwert von 1.464 Byte möglich ist. Damit wird der Aufwand für die Fragmentierung und das erneute Zusammensetzen großer Nachrichten verringert. Der Vorteil ist natürlich abhängig von den Clusteranwendungen und der Nutzung der von den Anwendungen erzeugten Clusternachrichten. Weitere Parameter sind in der API-Dokumentation definiert und können entweder zur Leistungsoptimierung für die Clusternachrichtenübertragung oder zum Ändern der Sensitivität des Clusters in Bezug auf die Partitionierung verwendet werden.

Zugehörige Verweise

API QcstChgClusterResourceServices

Zugehörige Informationen

Cluster ändern (CHGCLU)

Einstellungen für Cluster Resource Services ändern:

Die Standardwerte für Nachrichtenzeitlimits und Wiederholungen sind so gesetzt, dass sie für die meisten Standardinstallationen geeignet sind. Diese Werte können jedoch geändert und an Ihre Kommunikationsumgebung angepasst werden.

Die Werte können wie folgt angepasst werden:

- Durch Auswahl einer allgemeinen Leistungsstufe, die Ihrer Umgebung entspricht.
- Durch Angabe von Werten für bestimmte Nachrichtenoptimierungsparameter, um eine spezifischere Anpassung zu erreichen.

Bei der ersten Methode wird die Nachrichtenübertragung an eine von drei Kommunikationsstufen angepasst. Die normale Stufe ist die Standardeinstellung und wird ausführlich bei der Heartbeatüberwachung beschrieben.

Die zweite Methode sollte normalerweise nur unter Beteiligung eines Experten durchgeführt werden.

Unter der API Change Cluster Resource Services (QcstChgClusterResourceServices) werden beide Methoden ausführlich beschrieben.

Zugehörige Verweise

API QcstChgClusterResourceServices

Zugehörige Informationen

Heartbeatüberwachung

Cluster mit verschiedenen Releases planen:

Wenn Sie ein Cluster erstellen, das Knoten mit verschiedenen Clusterversionen enthält, sind bei der Clustererstellung bestimmte Maßnahmen erforderlich.

Standardmäßig wird als aktuelle Clusterversion die potenzielle Clusterversion des ersten Knotens angenommen, der dem Cluster hinzugefügt wird. Diese Methode ist dann sinnvoll, wenn dieser Knoten den niedrigsten Versionsstand hat, der im Cluster vorkommen soll. Hat dieser Knoten aber einen höheren Versionsstand, können später keine Knoten mit einem niedrigeren Versionsstand mehr hinzugefügt werden. Alternativ kann bei der Clustererstellung auch der Wert für die Zielclusterversion verwendet werden, um als aktuelle Clusterversion einen Versionsstand anzugeben, der um eine Versionsstufe niedriger ist als die potenzielle Clusterversion des ersten Knotens, der hinzugefügt wird.

| **Anmerkung:** Wenn das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM)
| eingesetzt wird, muss auf allen Systemen im Cluster V6R1 installiert sein.

Angenommen, es soll ein Cluster mit zwei Knoten erstellt werden. Die Knoten für diesen Cluster sind:

Knoten-ID	Release	Potenzielle Clusterversion
Knoten A	V5R4	5
Knoten B	V6R1	6

Soll der Cluster ausgehend von Knoten B erstellt werden, muss erkennbar sein, dass es sich um einen Cluster mit verschiedenen Releases handelt. Durch die Angabe für die Zielclusterversion muss angezeigt werden, dass die Knoten im Cluster auf einem Versionsstand kommunizieren, der eine Versionsstufe unter der potenziellen Clusterversion des anfordernden Knotens liegt.

Leistungsplanung für Cluster

Zusätzlicher Verwaltungsaufwand entsteht bei einem Cluster nur dann, wenn Änderungen an einem Cluster vorgenommen werden.

Die einzigen Ressourcen, die für das Clustering erforderlich sind, sind diejenigen, die für die Heartbeatüberwachung, die Verwaltung der Clusterressourcengruppen und Clusterknoten sowie die Nachrichtenübertragung zwischen den Clusterressourcengruppen und Clusterknoten benötigt werden. Wenn die Clustering-Umgebung betriebsbereit ist, entsteht nur dann ein Mehraufwand, wenn Änderungen am Cluster vorgenommen werden.

In einer normalen Betriebsumgebung sollte die Clustering-Aktivität nur geringe Auswirkungen auf die Clustersysteme haben.

Planungsprüfliste für Cluster

Füllen Sie die Prüfliste für die Clusterkonfiguration aus, damit Ihre Umgebung ordnungsgemäß vorbereitet ist, bevor Sie mit der Clusterkonfiguration beginnen.

Table 1. TCP/IP-Konfigurationsprüfliste für Cluster

TCP/IP-Voraussetzungen	
—	Starten Sie TCP/IP mit dem Befehl STRTCP (TCP/IP starten) auf jedem Knoten, der in den Cluster aufgenommen werden soll.
—	Konfigurieren Sie die TCP-Loopback-Adresse (127.0.0.1), und prüfen Sie, ob sie den Status "Aktiv" hat. Prüfen Sie die TCP/IP-Loopback-Adresse auf jedem Knoten im Cluster mit dem Befehl WRKTCPSTS (Mit TCP/IP-Netzwerkstatus arbeiten).
—	Prüfen Sie, ob die auf einem bestimmten Knoten für das Clustering verwendeten IP-Adressen den Status "Aktiv" haben, indem Sie auf dem betreffenden Knoten den Befehl WRKTCPSTS (Mit TCP/IP-Netzwerkstatus arbeiten) eingeben.
—	<p>Prüfen Sie, ob INETD auf allen Knoten im Cluster aktiv ist, indem Sie entweder den Befehl STRTCPSVR *INETD verwenden oder über IBM Systems Director Navigator for i5/OS die folgenden Schritte durchführen:</p> <ol style="list-style-type: none"> 1. Geben Sie in einem Web-Browser <code>http://mysystem:2001</code> ein, wobei <code>mysystem</code> der Hostname des Systems ist. 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an. 3. Wählen Sie Netzwerk im IBM Systems Director Navigator for i5/OS. 4. Wählen Sie auf der Begrüßungsseite TCP/IP-Server aus. 5. Wählen Sie auf der Seite "TCP/IP-Server" TCP/IP-Server aus. Daraufhin wird eine Liste der verfügbaren TCP/IP-Server angezeigt. 6. Wählen Sie in der Liste INETD aus. 7. Wählen Sie im Menü Aktion auswählen den Eintrag Starten aus. Der Status des Servers wird in Gestartet geändert. <p>Der INETD-Server kann auch mit dem Befehl STRTCPSVR (TCP/IP-Server starten) unter Angabe des Parameters *INETD gestartet werden. Nach dem Starten des INETD-Servers sollte in der Liste der aktiven Jobs der Job QTOGINTD (Benutzer QTCP) auf dem Knoten angezeigt werden.</p>
—	Vergewissern Sie sich, dass das Benutzerprofil für INETD, das in <code>/QIBM/ProdData/OS400/INETD/inetd.config</code> angegeben ist, nur über die Mindestberechtigung verfügt. Hat dieses Benutzerprofil eine höhere Berechtigung, kann der Clusterknoten nicht gestartet werden. Standardmäßig ist QUSER als Benutzerprofil für INETD angegeben.
—	Prüfen Sie, ob sämtliche IP-Adressen im Cluster an jede andere IP-Adresse im Cluster Daten weiterleiten und UDP-Datagramme senden können. Verwenden Sie den Befehl PING mit einer lokalen IP-Adresse und den Befehl TRACEROUTE, indem Sie UDP-Nachrichten angeben.
—	Vergewissern Sie sich, dass die Ports 5550 und 5551 nicht von anderen Anwendungen verwendet werden. Diese Ports sind für IBM Clustering reserviert. Die Verwendung der Ports kann mit dem Befehl WRKTCPSTS (Mit TCP/IP-Netzwerkstatus arbeiten) angezeigt werden. Nach dem Starten von INETD ist Port 5550 geöffnet und für das Clustering empfangsbereit.

Table 2. Prüfliste für Clusterverwaltungsdomäne

Hinweise für Cluster Resource Services-Schnittstelle	
—	Installieren Sie das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS. Auf sämtlichen Clusterknoten, die in die HA-Lösung aufgenommen werden, müssen Lizenzberechtigungen vorhanden sein.
—	Installieren Sie Option 41 (i5/OS - HA Switchable Resources). Auf sämtlichen Clusterknoten, die in die Einheitendomäne aufgenommen werden, müssen Lizenzberechtigungen vorhanden sein.
—	Prüfen Sie mit dem Befehl STRHOSTSVR (Host-Server starten), ob alle Server gestartet wurden: STRHOSTSVR SERVER(*ALL)

Beabsichtigen Sie, umschaltbare Einheiten im Cluster einzusetzen, müssen folgende Voraussetzungen erfüllt sein:

Tabelle 3. Konfigurationsprüfliste für ausfallsichere Einheiten im Cluster

Voraussetzungen	
—	Installieren Sie das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS. Auf sämtlichen Clusterknoten, die in die HA-Lösung aufgenommen werden, müssen Lizenzberechtigungen vorhanden sein.
—	Prüfen Sie, ob Option 41 (HA Switchable Resources) installiert ist und auf allen Clusterknoten der Einheiten-domäne eine gültige Lizenzberechtigung vorhanden ist.
—	Für den Zugriff auf Plattenverwaltungsfunktionen müssen Sie den Service-Tools-Server (STS) mit DST-Zugriff und -Benutzerprofilen konfigurieren. Weitere Informationen finden Sie unter Enabling and accessing disk units.
—	Werden ausfallsichere Einheiten zwischen den logischen Partitionen eines Systems umgeschaltet und erfolgt die Verwaltung der logischen Partitionen nicht über die HMC, aktivieren Sie Virtual OptiConnect für die Partitionen. Dies geschieht mit der Anmeldung bei den DST (Dedicated Service Tools). Weitere Informationen finden Sie unter Virtual OptiConnect. Erfolgt die Verwaltung der Partitionen über die HMC, ändern Sie die Eigenschaften des Partitionsprofils auf der Registerkarte OptiConnect, um Virtual OptiConnect für jede Partition in der umschaltbaren Konfiguration zu aktivieren. Sie müssen das Partitionsprofil aktivieren, damit die Änderung übernommen wird.
—	Wird eine Erweiterungseinheit in einem HSL OptiConnect-Loop zwischen zwei Systemen umgeschaltet und hat eines der Systeme logische Partitionen, aktivieren Sie HSL OptiConnect für die Partitionen. Erfolgt die Verwaltung der logischen Partitionen nicht über die HMC, wird die Aktivierung mit der Anmeldung bei den DST (Dedicated Service Tools) vorgenommen. Erfolgt die Verwaltung der Partitionen über die HMC, ändern Sie die Eigenschaften des Partitionsprofils auf der Registerkarte OptiConnect, um HSL OptiConnect für jede Partition in der umschaltbaren Konfiguration zu aktivieren. Sie müssen das Partitionsprofil aktivieren, damit die Änderung übernommen wird.
—	Werden ausfallsichere Einheiten zwischen logischen Partitionen umgeschaltet und erfolgt die Verwaltung der logischen Partitionen nicht über die HMC, müssen Sie den Bus so konfigurieren, dass er von den Partitionen gemeinsam genutzt wird, oder Sie müssen einen E/A-Pool konfigurieren. Der Bus muss für eine einzige Partition als "Own bus shared" und für alle anderen Partitionen, die am Einheiten-Switching beteiligt sind, als "Use bus shared" konfiguriert werden. Erfolgt die Verwaltung der logischen Partitionen über die HMC, müssen Sie einen E/A-Pool konfigurieren, der den E/A-Prozessor, E/A-Adapter und alle zugeordneten Ressourcen umfasst, damit ein unabhängiger Plattenpool zwischen Partitionen umgeschaltet werden kann. Jede Partition muss Zugriff auf den E/A-Pool haben. Weitere Informationen finden Sie unter Hardware umschaltbar machen. Einzelheiten zu den Hardwarevoraussetzungen für umschaltbare Einheiten finden Sie unter Hardwarevoraussetzungen für umschaltbare Platten.
—	Wenn eine Erweiterungseinheit in einem HSL-Loop zwischen zwei Systemen umgeschaltet werden soll, muss die Erweiterungseinheit als umschaltbar konfiguriert werden. Weitere Informationen finden Sie unter Hardware umschaltbar machen.
—	Wenn eine Erweiterungseinheit einem vorhandenen HSL-Loop hinzugefügt wird, müssen alle Server in diesen Loop erneut gestartet werden.
—	Die maximale Übertragungseinheit (MTU) für die Kommunikationspfade muss größer sein als der für die Clusterkommunikation optimierbare Parameter "Nachrichtenfragmentgröße". Die MTU für eine Cluster-IP-Adresse kann mit dem Befehl WRKTCPS (Mit TCP/IP-Netzwerkstatus arbeiten) auf dem betreffenden Knoten geprüft werden. Außerdem muss die MTU in jedem Abschnitt auf dem gesamten Kommunikationspfad geprüft werden. Vermutlich ist es einfacher, den Parameter "Nachrichtenfragmentgröße" nach der Clustererstellung zu ändern, als die MTU für den Kommunikationspfad zu erhöhen. Weitere Informationen über die Nachrichtenfragmentgröße finden Sie unter Optimierbare Parameter für die Clusterkommunikation. Mit der API Retrieve Cluster Resource Services Information (QcstRetrieveCRSInfo) können die aktuellen Einstellungen der Optimierungsparameter angezeigt und mit der API Change Cluster Resource Services (QcstChgClusterResourceServices) können sie geändert werden.

Table 3. Konfigurationsprüfliste für ausfallsichere Einheiten im Cluster (Forts.)

Voraussetzungen	
—	Bei der geographischen Spiegelung müssen Sie sich vergewissern, dass beide Knoten verschiedenen Standortnamen zugeordnet sind.

Table 4. Prüfliste für Clustersicherheitskonfiguration

Sicherheitsanforderungen	
—	Wenn Sie einen fernen Knoten starten, setzen Sie das Netzwerkattribut ALWADDCLU (Hinzufügen zu Cluster zulassen) auf dem Zielknoten auf den passenden Wert. Abhängig von der Umgebung sollte dies *ANY oder *RQSAUT sein. Wird das Attribut auf *RQSAUT gesetzt, müssen die i5/OS-Optionen 34 (Digital Certificate Manager) und 35 (CCA Cryptographic Service Provider) installiert sein. Einzelheiten zur Angabe des Netzwerkattributs ALWADDCLU finden Sie unter Knoten aktivieren und einem Cluster hinzufügen.
—	Setzen Sie den Status des Benutzerprofils für INETD, das in /QIBM/ProdData/OS400/INETD/inetd.config angegeben ist, auf aktiviert (*ENABLED). Das Benutzerprofil darf nicht über die Sonderberechtigung *SECADM oder *ALLOBJ verfügen. Standardmäßig ist QUSER als Benutzerprofil für INETD angegeben.
—	Prüfen Sie, ob das Benutzerprofil, das die Cluster Resource Services-APIs aufruft, auf allen Knoten mit der Berechtigung *IOSYSCFG vorhanden ist.
—	Prüfen Sie, ob das Benutzerprofil für die Ausführung des Exitprogramms für eine Clusterressourcengruppe (CRG) auf allen Knoten der Wiederherstellungsdomäne vorhanden ist.

Table 5. Konfigurationsprüfliste für Clusterjobs

Hinweise für Jobs	
—	Von den Cluster Resource Services-APIs können Jobs zur Verarbeitung von Anforderungen übergeben werden. Die Jobs werden entweder unter dem Benutzerprofil ausgeführt, das bei der Erstellung einer Clusterressourcengruppe zur Ausführung des Exitprogramms angegeben wurde, oder unter dem Benutzerprofil, das die API angefordert hat (nur zum Anhängen von Einheiten in CRGs für ausfallsichere Einheiten). Vergewissern Sie sich, dass das Subsystem, das der Jobwarteschlange des Benutzerprofils zugeordnet ist, wie folgt konfiguriert ist: *NOMAX für die Anzahl der Jobs, die aus dieser Jobwarteschlange ausgeführt werden können.
—	Jobs werden an die Jobwarteschlange übergeben, die in der Jobbeschreibung angegeben ist, die in dem für eine CRG definierten Benutzerprofil hinterlegt ist. Die Standardjobbeschreibung sieht vor, dass die Jobs an die Jobwarteschlange QBATCH gesendet werden. Da diese Jobwarteschlange für viele Benutzerjobs verwendet wird, wird das Exitprogramm unter Umständen nicht rechtzeitig ausgeführt. Sie sollten eventuell eine eindeutige Jobbeschreibung mit einer eindeutigen Benutzerwarteschlange erstellen.
—	Exitprogrammjobs verwenden bei ihrer Ausführung Weiterleitungsdaten aus der Jobbeschreibung, um den Hauptspeicherpool und die Laufzeitattribute auszuwählen. Die Standardwerte sind so gesetzt, dass die Jobs in einem Pool zusammen mit anderen Stapeljobs ausgeführt werden, die die Ausführungspriorität 50 haben. Die für Exitprogrammjobs gewünschte Leistung kann damit nicht erreicht werden. Das Subsystem, von dem die Exitprogrammjobs eingeleitet werden (gemeint ist das Subsystem, das die eindeutige Jobwarteschlange verwendet) sollte die Exitprogrammjobs einem Pool zuordnen, der von anderen Jobs, die von diesem oder anderen Subsystemen eingeleitet werden, nicht benutzt wird. Ferner sollte den Exitprogrammjobs die Ausführungspriorität 15 zugeordnet werden, damit sie vor der Mehrzahl der anderen Benutzerjobs ausgeführt werden.
—	Setzen Sie den Systemwert QMLTHDACN auf 1 oder 2.

Zum Konfigurieren oder Verwalten des Clusters stehen mehrere Softwareschnittstellen zur Verfügung. Eine dieser Schnittstellen ist die Cluster Resource Services-Schnittstelle. Wenn Sie sich für die Cluster Resource Services entscheiden, müssen die folgenden Voraussetzungen erfüllt sein.

Tabelle 6. Konfigurationsprüfliste für Cluster Resource Services

Hinweise zur grafischen Oberfläche der Cluster Resource Services	
—	Installieren Sie das Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS. Auf sämtlichen Clusterknoten, die in die HA-Lösung aufgenommen werden, müssen Lizenzberechtigungen vorhanden sein.
—	Installieren Sie Option 41 (i5/OS - HA Switchable Resources). Auf sämtlichen Clusterknoten, die in die Einheitendomäne aufgenommen werden, müssen Lizenzberechtigungen vorhanden sein.
—	Prüfen Sie mit dem Befehl STRHOSTSVR (Host-Server starten), ob alle Server gestartet wurden: STRHOSTSVR SERVER(*ALL)

FlashCopy planen

Sie können FlashCopy verwenden, um das Fenster zum Durchführen von Sicherungen in i5/OS-Hochverfügbarkeitsumgebungen mit externen IBM Systems Storage-Speichereinheiten zu verkürzen. Bevor Sie FlashCopy einsetzen, sollten Sie sich vergewissern, dass die Mindestvoraussetzungen erfüllt sind.

Hardwarevoraussetzungen für FlashCopy

Wenn Sie FlashCopy in einer i5/OS-Hochverfügbarkeitslösung einsetzen möchten, sollten Sie sich vergewissern, dass die Hardwaremindestvoraussetzungen erfüllt sind.

Die folgenden Hardwaremindestvoraussetzungen müssen für FlashCopy erfüllt sein:

- Mindestens zwei System i-Modelle oder logische Partitionen, die geographisch getrennt sind, wobei mindestens eine externe Speichereinheit IBM System Storage DS6000 oder DS8000 an jedes System angeschlossen ist. Die externen Speichereinheiten DS6000 und DS8000 werden an allen System i-Modellen unterstützt, die Glasfaserkabelanschluss für externe Speicher unterstützen.
- Einer der folgenden unterstützten Glasfaserkabeladapter ist erforderlich:
 - 2766 2 Gigabit Fibre Channel Disk Controller PCI
 - 2787 2 Gigabit Fibre Channel Disk Controller PCI-X
 - 5760 4 Gigabit Fibre Disk Controller PCI-X
- Die Auswahl einer angemessenen Plattengröße für den Systemspeicher sollte vor der Konfiguration erfolgt sein. Sie benötigen einen Plattensatz für die Quelle und einen gleich großen Plattensatz für das Ziel sowie einen weiteren Plattensatz für jede konsistente Kopie.

Softwarevoraussetzungen für FlashCopy

Für den Einsatz von FlashCopy in einer i5/OS-Hochverfügbarkeitslösung müssen die folgenden Softwaremindestvoraussetzungen erfüllt sein.

Bei FlashCopy bestehen folgende Softwaremindestvoraussetzungen:

- Auf jedem System i-Modell in der Hochverfügbarkeitslösung muss i5/OS V6R1 in Verbindung mit dem Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM), 5761-HAS, ausgeführt werden.

Anmerkung: Bei früheren Releases können weiterhin die IBM Kopierservices für System i, ein Angebot der Lab Services, zum Arbeiten mit IBM System Storage-Lösungen verwendet werden. Wenn Global Mirror auf mehreren Plattformen eingesetzt wird oder auf mehreren System i-Partitionen implementiert werden soll, können Sie auch die IBM Kopierservices für System i verwenden.

- IBM System i High Availability Solutions Manager (iHASM) muss auf jedem System installiert sein.
- Vergewissern Sie sich, dass die neuesten PTFs installiert sind.

Kommunikationsvoraussetzungen für FlashCopy

Die folgenden Kommunikationsmindestvoraussetzungen müssen für FlashCopy erfüllt sein:

- Mindestens zwei System i-Modelle, die geographisch getrennt sind, wobei mindestens eine externe Speichereinheit IBM System Storage DS6000 oder DS8000 an jedes System angeschlossen ist. Die externen Speichereinheiten DS6000 und DS8000 werden an allen System i-Modellen unterstützt, die Glasfaserkabelanschluss für externe Speicher unterstützen.
- Einer der folgenden unterstützten Glasfaserkabeladapter ist erforderlich:
 - 2766 2 Gigabit Fibre Channel Disk Controller PCI
 - 2787 2 Gigabit Fibre Channel Disk Controller PCI-X
 - 5760 4 Gigabit Fibre Disk Controller PCI-X
- Zur Unterstützung einer externen IPL-Einheit auf der DS6000 oder DS8000 ist ein neuer IOP erforderlich:
 - Feature 2847 PCI-X IOP für SAN-Ladequelle
- Die Auswahl einer angemessenen Plattengröße für den Systemspeicher sollte vor der Konfiguration erfolgt sein. Sie benötigen einen Plattensatz für die Quelle und einen gleich großen Plattensatz für das Ziel sowie einen weiteren Plattensatz für jede konsistente Kopie.

Sicherheitsplanung für Hochverfügbarkeit

Vor der Konfiguration der Hochverfügbarkeitslösung sollten Sie die aktuellen Sicherheitsstrategien Ihres Unternehmens einer Prüfung unterziehen und alle erforderlichen Änderungen durchführen, um die Realisierung der Hochverfügbarkeit zu erleichtern.

Clusterweite Informationen verteilen

In diesem Abschnitt wird erläutert, wie sich Nutzung und Verwaltung clusterweiter Informationen auf die Sicherheit auswirken.

Über die API `QcstDistributeInformation` (Distribute Information) können Nachrichten von einem Knoten in einer CRG-Wiederherstellungsdomäne an andere Knoten dieser Wiederherstellungsdomäne gesendet werden. Diese Art der Nachrichtenübertragung kann sich bei der Exitprogrammverarbeitung als nützlich erweisen. Allerdings ist zu beachten, dass die Informationen nicht verschlüsselt werden. Daher sollten mit dieser Methode nur dann sicherheitskritische Informationen gesendet werden, wenn das Netzwerk sicher ist.

Nicht persistente Daten können unter Verwendung der Cluster-Hash-Tabellen-APIs von Clusterknoten gemeinsam genutzt und zwischen Clusterknoten repliziert werden. Diese Daten sind im flüchtigen (nicht permanenten) Speicher abgelegt. Das heißt, dass die Daten nur so lange aufbewahrt werden, wie der Clusterknoten in der Cluster-Hash-Tabelle enthalten ist. Diese APIs können nur auf einem Clusterknoten verwendet werden, der in der Cluster-Hash-Tabellen-Domäne definiert ist. Der Clusterknoten muss im Cluster aktiv sein.

Andere von der Clusternachrichtenübertragung verteilte Informationen sind ebenfalls nicht sicher. Dazu gehört auch die Clusternachrichtenübertragung der unteren Ebene. Wenn Änderungen an den Exitprogrammdateien vorgenommen werden, findet keine Verschlüsselung der Nachricht statt, die die Daten enthält.

Hinweise zur Verwendung von Clustern mit Firewalls

Wird Clustering in einem Netzwerk mit Firewalls eingesetzt, sind einige Einschränkungen und Anforderungen zu berücksichtigen.

Wird Clustering mit einer Firewall betrieben, müssen Sie jedem Knoten ermöglichen, abgehende Nachrichten an andere Clusterknoten zu senden und eingehende Nachrichten von diesen zu empfangen. Die Firewall muss für alle Clusteradressen auf allen Knoten durchlässig sein, damit diese miteinander kommunizieren können. Die IP-Pakete können mit verschiedenen Transportmethoden über das Netzwerk übertragen werden. Clustering verwendet ICMP Ping sowie UDP und TCP. Bei der Konfiguration der Firewall können Sie den Datenverkehr nach der Transportmethode filtern. Die Firewall muss ICMP-,

UDP- und TCP-Datenverkehr zulassen, damit das Clustering funktioniert. Der abgehende Datenverkehr kann über jeden beliebigen Port gesendet werden, der ankommende Datenverkehr wird auf den Ports 5550 und 5551 empfangen.

Benutzerprofile auf allen Knoten verwalten

Es gibt zwei Methoden zur Verwaltung von Benutzerprofilen auf allen Knoten in einem Cluster.

- | In einer Hochverfügbarkeitsumgebung wird ein Benutzerprofil als auf allen Systemen identisch angesehen, wenn der Profilname derselbe ist. Der Name ist die eindeutige Kennung im Cluster. Ein Benutzerprofil enthält außerdem eine Benutzernummer (UID) und eine Gruppennummer (GID). Um die bei einem Switchover stattfindende interne Verarbeitung zu reduzieren, wenn der unabhängige Plattenpool auf einem System gesperrt und für ein anderes System verfügbar gemacht wird, sollten die UID- und GID-Werte in der Wiederherstellungsdomäne für die Einheiten-CRG synchronisiert werden. Es gibt zwei Methoden zum Synchronisieren von Benutzerprofilen in einer Hochverfügbarkeitsumgebung.

Eine Methode besteht in der Erstellung einer Clusterverwaltungsdomäne, um gemeinsam genutzte Ressourcen auf allen Knoten eines Clusters überwachen zu können. Eine Clusterverwaltungsdomäne kann neben Benutzerprofilen auch andere Arten von Ressourcen überwachen und bietet somit eine einfache Möglichkeit zur Verwaltung der Ressourcen, die von allen Knoten gemeinsam genutzt werden. Änderungen an Benutzerprofilen werden automatisch an andere Knoten weitergegeben, wenn die Clusterverwaltungsdomäne aktiv ist. Ist die Clusterverwaltungsdomäne nicht aktiv, werden die Änderungen weitergegeben, nachdem sie wieder aktiviert wurde. Diese Methode wird empfohlen, da sie eine automatische Verwaltung der Benutzerprofile in einer Hochverfügbarkeitsumgebung bietet.

Bei der zweiten Methode verwenden die Administratoren Management Central in System i Navigator, um Funktionen für mehrere Systeme und Systemgruppe auszuführen. Diese Unterstützung umfasst einige allgemeine Benutzerverwaltungstasks, die üblicherweise von den Bediener ausgeführt werden und sich auf mehrere Systeme im Cluster beziehen. Über Management Central können Benutzerprofilfunktionen für Systemgruppen ausgeführt werden. Der Administrator kann bei der Erstellung eines Benutzerprofils einen Weitergabebefehl zur Ausführung auf den Zielsystemen angeben.

Wichtig:

- Ist beabsichtigt, Benutzerprofile mit Kennwortabgleich im Cluster zu verwenden, muss der Systemwert QRETSVRSEC (Server-Sicherheitsdaten sichern) auf 1 gesetzt werden.
- Wird QRETSVRSEC in 0 geändert, nachdem ein Eintrag für eine überwachte Ressource (MRE) für ein Benutzerprofil hinzugefügt wurde, und anschließend das Kennwort geändert (bei Kennwortüberwachung), dann wird der globale Status für den MRE auf "Inkonsistent" gesetzt. Der MRE wird als nicht verwendbar markiert. Alle nach dieser Änderung an dem Benutzerprofil vorgenommenen Änderungen werden nicht synchronisiert. Zur Behebung dieses Problems muss QRETSVRSEC auf 1 gesetzt, der MRE entfernt und dann wieder hinzugefügt werden.

Zugehörige Tasks

„Clusterverwaltungsdomäne erstellen“ auf Seite 106

- | Bei einer HA-Lösung bietet die Clusterverwaltungsdomäne den Mechanismus, der dafür sorgt, dass Ressourcen auf allen Systemen und Partitionen in einem Cluster synchronisiert bleiben.

Hochverfügbarkeitslösung konfigurieren

Bevor Sie eine Hochverfügbarkeitslösung in Ihrer i5/OS-Umgebung konfigurieren, vergewissern Sie sich, dass alle erforderlichen Planungsmaßnahmen abgeschlossen, die verfügbaren Ressourcen bekannt und die Ziele für Hochverfügbarkeit und Wiederherstellung nach einem Katastrophenfall definiert sind. Nutzen Sie die folgenden Konfigurationsszenarios für Hochverfügbarkeit und die den Hochverfügbarkeitstechnologien zugeordneten Tasks, um Ihre eigene HA-Lösung zu erstellen.

Szenarios: Hochverfügbarkeitslösungen konfigurieren

Die Konfigurationsszenarios umfassen Beispiele für unterschiedliche i5/OS-Hochverfügbarkeitsumgebungen sowie Anleitungen, die Sie Schritt für Schritt durch die Konfigurationstasks führen, die Sie bei der Implementierung einer HA-Lösung unterstützen, die Ihren Anforderungen an ein System und die Ausfallsicherheit des Systems gerecht wird.

Die Szenarios enthalten Beschreibungen zur Erreichung der Unternehmensziele in Bezug auf die Hochverfügbarkeit sowie grafische Darstellungen der Ressourcen in einer HA-Lösung. Jedes Lösungsbeispiel enthält detaillierte Anweisungen, die Sie Schritt für Schritt durch die Einrichtung und Überprüfung einer HA-Lösung führen. Da diese Informationen jedoch nicht alle möglichen Konfigurationen behandeln, können weitere Tests zur Überprüfung der Hochverfügbarkeit einer Lösung erforderlich sein.

Szenario: Zwischen logischen Partitionen umschaltbare Platte

In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die Plattenpools verwendet, die zwischen zwei logischen Partitionen umgeschaltet werden, die sich auf einem Einzelsystem befinden.

Übersicht

Die logische Partitionierung bewirkt, dass ein einzelnes i5/OS-System wie mindestens zwei unabhängige Systeme funktioniert. Diese Lösung bietet sich für Unternehmen an, in deren Umgebung bereits logische Partitionen konfiguriert sind.

Dieses Szenario liefert keine Beschreibung für die Konfiguration logischer Partitionen.

Zielsetzungen

Vorteile dieser Lösung:

- Kostengünstige Lösung, die vorhandene Systemressourcen nutzt.
- Verfügbarkeit für Unternehmensressourcen bei geplanten Betriebsunterbrechungen.
- Verfügbarkeit für Unternehmensressourcen bei einigen ungeplanten Betriebsunterbrechungen, z. B. dem Ausfall einer einzelnen logischen Partition.
- Durch Verwendung einer einzigen Datenkopie wird die Anzahl der erforderlichen Platteneinheiten auf ein Minimum beschränkt.
- Enthält aktuelle Daten, die nicht synchronisiert werden müssen.

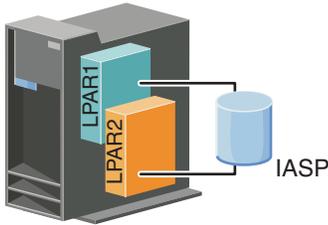
Nachteile dieser Lösung:

- Keinerlei Wiederherstellungsmöglichkeit nach Komplettausfall eines Standorts.
- Die Konfiguration einer logischen Partition ist Bedingung.
- Redundante Hardware in beiden Partitionen möglicherweise Bedingung.
- Es ist nur eine einzige logische Kopie der Daten im unabhängigen Plattenpool vorhanden. Dies kann sich als "Single Point of Failure" erweisen, obwohl die Daten dem RAID-Schutz unterliegen können.
- Es ist kein gleichzeitiger Zugriff auf den Plattenpool von beiden logischen Partitionen aus möglich.

| Details

| Die folgende Abbildung veranschaulicht die Umgebung für dieses Szenario:

|



|

| Konfigurationsschritte

| Führen Sie die folgenden Tasks aus, um die Hochverfügbarkeitstechnologien für dieses Szenario zu konfigurieren:

- | 1. Prüfliste für Cluster ausfüllen
- | 2. Cluster erstellen
- | 3. Knoten hinzufügen
- | 4. Knoten starten
- | 5. Knoten zu einer Einheitendomäne hinzufügen
- | 6. Clusterverwaltungsdomäne erstellen
- | 7. Clusterverwaltungsdomäne starten
- | 8. Unabhängigen Plattenpool erstellen
- | 9. Einträge für überwachte Ressourcen hinzufügen
- | 10. Hardware umschaltbar machen
- | 11. Einheiten-CRG erstellen
- | 12. Einheiten-CRG starten
- | 13. Plattenpool verfügbar machen
- | 14. Switchover ausführen, um die HA-Lösung zu testen

| Szenario: Zwischen Systemen umschaltbare Platte

| In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die Platten verwendet, die zwischen zwei Systemen umschaltbar sind, wodurch sie Hochverfügbarkeit für Daten, Anwendungen oder Einheiten bei geplanten oder ungeplanten Betriebsunterbrechungen sicherstellt.

| Übersicht

| Durch Anwendung der Technologie für umschaltbare Platten haben wir es hier mit einer einfachen HA-Lösung zu tun. Bei dieser Lösung bleibt eine einzige Datenkopie, die auf der umschaltbaren Platte gespeichert ist, immer aktuell, was die Synchronisation der Daten auf den Systemen überflüssig macht und die Gefahr von Datenverlusten während der Übertragung ausschließt.

| Zielsetzungen

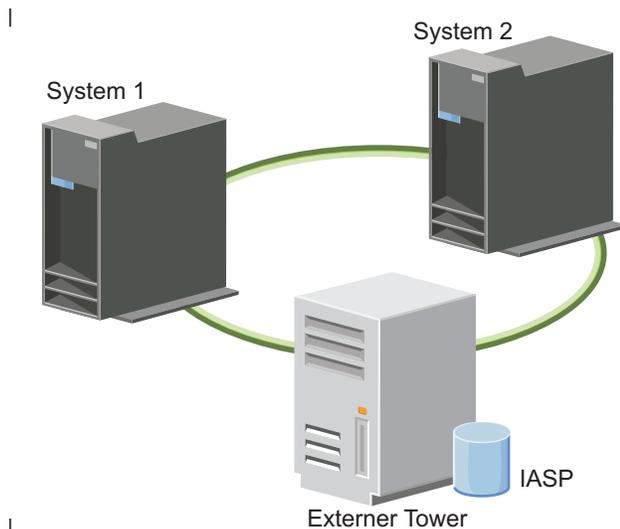
| Vorteile dieser Lösung:

- | • Stellt Verfügbarkeit für Unternehmensressourcen bei geplanten Betriebsunterbrechungen sicher.
- | • Stellt Verfügbarkeit für Unternehmensressourcen bei einigen ungeplanten Betriebsunterbrechungen sicher.
- | • Verwendet eine einzige Datenkopie, was die Anzahl der erforderlichen Platteneinheiten auf ein Minimum beschränkt.

- | • Führt zu minimalen Leistungseinbußen.
 - | • Daten bleiben aktuell und müssen nicht synchronisiert werden.
- | Nachteile dieser Lösung:
- | • Keinerlei Wiederherstellungsmöglichkeit nach Komplettausfall eines Standorts.
 - | • Es ist nur eine einzige logische Kopie der Daten im unabhängigen Plattenpool vorhanden. Dies kann sich als "Single Point of Failure" erweisen, obwohl die Daten dem RAID-Schutz unterliegen können.
 - | • Es ist kein gleichzeitiger Zugriff auf den Plattenpool von beiden Systemen aus möglich.

| **Details**

| Die folgende Abbildung veranschaulicht die Umgebung für dieses Szenario:



| **Konfigurationsschritte**

- | 1. Planungsprüfliste ausfüllen
- | 2. Cluster erstellen
- | 3. Knoten hinzufügen
- | 4. Knoten starten
- | 5. Knoten zu einer Einheitendomäne hinzufügen
- | 6. Clusterverwaltungsdomäne erstellen
- | 7. Clusterverwaltungsdomäne starten
- | 8. Unabhängigen Plattenpool erstellen
- | 9. Einträge für überwachte Ressourcen hinzufügen
- | 10. Hardware umschaltbar machen
- | 11. Einheiten-CRG erstellen
- | 12. Einheiten-CRG starten
- | 13. Plattenpool verfügbar machen
- | 14. Switchover ausführen, um die HA-Lösung zu testen

| **Szenario: Umschaltbare Platte mit geographischer Spiegelung**

| In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die umschaltbare Platten mit geographischer Spiegelung in einem aus drei Knoten bestehenden Cluster verwendet. Mit dieser Lösung ist sowohl eine Wiederherstellung nach einem Katastrophenfall als auch Hochverfügbarkeit sicherstellt.

Übersicht

Am Produktionsstandort (beispielsweise im Gewerbegebiet) werden unabhängige Plattenpools mit Hilfe umschaltbarer Platten zwischen zwei Knoten verschoben. Außerdem wird mit Hilfe der geographischen Spiegelung eine Kopie der unabhängigen Platte an einem zweiten Standort (beispielsweise in der Innenstadt) erstellt. Somit ermöglicht diese Lösung sowohl die Wiederherstellung nach einem Katastrophenfall als auch eine hohe Verfügbarkeit. Die Vorteile dieser Lösung entsprechen im Wesentlichen denen der Lösung mit umschaltbarer Platte, doch kommt hier noch der Vorteil der Wiederherstellungsmöglichkeit von Anwendungsdaten durch Duplizierung an einem anderen Standort hinzu. Der Produktionsstandort verfügt über einen unabhängigen Plattenpool, der zwischen logischen Partitionen umgeschaltet werden kann, um Hochverfügbarkeit mit kurzer Switchoverdauer für geplante Betriebsunterbrechungen, z. B. das Anlegen von Programmkorrekturen, bereitzustellen. Diese Lösung ermöglicht auch die Wiederherstellung nach einem Katastrophenfall mit standortübergreifender und geographischer Spiegelung.

Die geographische Spiegelung ist eine Unterfunktion der standortübergreifenden Spiegelung, bei der Daten auf eine Kopie des unabhängigen Plattenpools am fernen Standort gespiegelt werden. Die Daten werden vom unabhängigen Plattenpool am Produktionsstandort auf einen unabhängigen Plattenpool am Ausweichstandort gespiegelt. Diese Lösung stellt eine einfache und kostengünstigere Alternative zu Lösungen dar, die auf externen Speichereinheiten basieren, z. B. IBM System Storage Global Mirror und Metro Mirror. Die geographische Spiegelung bietet jedoch nicht das gesamte Spektrum an Leistungsoptionen, die von den Lösungen mit externen Speichereinheiten geboten werden.

Zielsetzungen

Vorteile dieser Lösung:

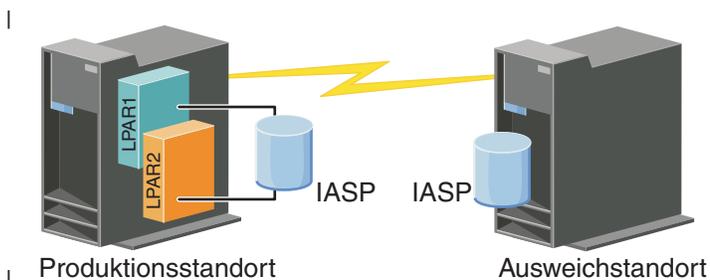
- Stellt Verfügbarkeit für Unternehmensressourcen bei geplanten Betriebsunterbrechungen sicher.
- Stellt Verfügbarkeit für Unternehmensressourcen bei einigen ungeplanten Betriebsunterbrechungen sicher.
- Stellt Verfügbarkeit für Unternehmensressourcen beim Komplettausfall eines Standorts sicher.
- Verwendet an jedem Standort eine einzige Datenkopie, was die Anzahl der erforderlichen Platteneinheiten auf ein Minimum beschränkt.
- Daten bleiben aktuell und müssen nicht synchronisiert werden.

Nachteile dieser Lösung:

- Es ist kein gleichzeitiger Zugriff auf den Plattenpool möglich. Die Spiegelkopie kann jedoch abgehängt werden, um eine zweite Kopie der Daten offline zu verarbeiten.
- Potenzielle Leistungseinbußen, da zur Unterstützung der geographischen Spiegelung eine höhere CPU-Belastung erforderlich ist.
- Die Verwendung redundanter Kommunikationspfade und adäquater Bandbreiten ist zu berücksichtigen.

Details

Die folgende Abbildung veranschaulicht diese Lösung:



| **Konfigurationsschritte**

- | 1. Planungsprüfliste für Cluster ausfüllen
- | 2. Cluster erstellen
- | 3. Knoten hinzufügen
- | 4. Knoten starten
- | 5. Knoten zu einer Einheitendomäne hinzufügen
- | 6. Einheiten-CRG erstellen
- | 7. Standortnamen definieren
- | 8. Clusterverwaltungsdomäne erstellen
- | 9. Clusterverwaltungsdomäne starten
- | 10. Unabhängigen Plattenpool erstellen
- | 11. Einträge für überwachte Ressourcen hinzufügen
- | 12. Hardware umschaltbar machen
- | 13. Geographische Spiegelung konfigurieren
- | 14. Plattenpool verfügbar machen
- | 15. Switchover ausführen, um die Konfiguration zu testen

| **Zugehörige Tasks**

- | „Geographische Spiegelung konfigurieren“ auf Seite 116
- | Die *geographische Spiegelung* ist eine Unterfunktion der standortübergreifenden Spiegelung. Bei der Konfiguration einer HA-Lösung unter Verwendung der geographischen Spiegelung müssen Sie eine Spiegelungssitzung zwischen dem Produktionssystem und dem Sicherungssystem konfigurieren.

| **Szenario: Standortübergreifende Spiegelung mit geographischer Spiegelung**

- | In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die geographische Spiegelung in einem Cluster mit zwei Knoten verwendet. Mit dieser Lösung ist sowohl eine Wiederherstellung nach einem Katastrophenfall als auch Hochverfügbarkeit sicherstellt.

| **Übersicht**

- | Die geographische Spiegelung ist eine Unterfunktion der standortübergreifenden Spiegelung, bei der Daten auf eine Kopie des unabhängigen Plattenpools am fernen Standort gespiegelt werden. Diese Lösung bietet eine Wiederherstellungsmöglichkeit für den Fall eines Komplettausfalls des Produktionssystems (System 1). In diesem Fall erfolgt ein Failover auf den Ausweichstandort (System 2), an dem der Betrieb dann mit der gespiegelten Kopie der Daten fortgesetzt werden kann. Diese Lösung stellt eine einfache und kostengünstigere Alternative zu Lösungen dar, die auf externen Speichereinheiten basieren, z. B. IBM System Storage Global Mirror und Metro Mirror. Die geographische Spiegelung beinhaltet jedoch nicht das gesamte Spektrum an Leistungsoptionen, die von den Lösungen mit externen Speichereinheiten geboten werden.

| **Zielsetzungen**

- | Vorteile dieser Lösung:

- | • Stellt Verfügbarkeit für Unternehmensressourcen bei geplanten Betriebsunterbrechungen sicher.
- | • Stellt Verfügbarkeit für Unternehmensressourcen bei einigen ungeplanten Betriebsunterbrechungen sicher.
- | • Stellt Verfügbarkeit für Unternehmensressourcen bei Störfällen sicher.
- | • Daten bleiben aktuell und müssen nicht synchronisiert werden.

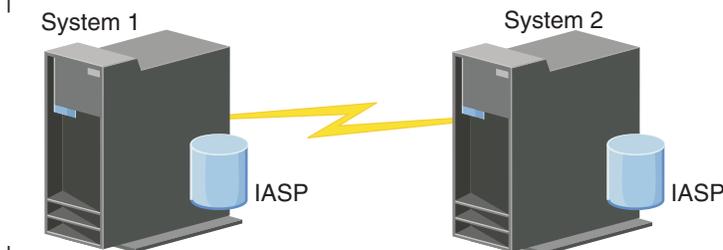
- | Nachteile dieser Lösung:

- | • Es ist kein gleichzeitiger Zugriff auf den Plattenpool möglich. Die Spiegelkopie kann jedoch abgehängt werden, um eine zweite Kopie der Daten offline zu verarbeiten.

- Potenzielle Leistungseinbußen, da zur Unterstützung der geographischen Spiegelung eine höhere CPU-Belastung erforderlich ist.
- Die Verwendung redundanter Kommunikationspfade und adäquater Bandbreiten ist zu berücksichtigen.

Details

Die folgende Abbildung veranschaulicht diese Lösung:



Konfigurationsschritte

1. Planungsprüfliste für Cluster ausfüllen
2. Cluster erstellen
3. Knoten hinzufügen
4. Knoten starten
5. Knoten zu einer Einheitendomäne hinzufügen
6. Clusterverwaltungsdomäne erstellen
7. Clusterverwaltungsdomäne starten
8. Unabhängigen Plattenpool erstellen
9. Einträge für überwachte Ressourcen hinzufügen
10. Hardware umschaltbar machen
11. Einheiten-CRG erstellen
12. Einheiten-CRG starten
13. Plattenpool verfügbar machen
14. Geographische Spiegelung konfigurieren
15. Switchover ausführen, um die Konfiguration zu testen

Szenario: Standortübergreifende Spiegelung mit Metro Mirror

In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die auf externem Speicher basiert und die Wiederherstellung nach einem Katastrophenfall sowie Hochverfügbarkeit für Speichersysteme sicherstellt, die geographisch nicht zu weit voneinander entfernt sind. Metro Mirror ist eine IBM System Storage-Lösung, mit der Daten synchron von der Speichereinheit am Produktionsstandort auf die Speichereinheit am Ausweichstandort kopiert werden. Auf diese Weise bleiben die Daten am Ausweichstandort konsistent.

Übersicht

Die standortübergreifende Spiegelung in Verbindung mit Metro Mirror ermöglicht hohe Verfügbarkeit und Wiederherstellung nach einem Katastrophenfall durch Verwendung externer Speichereinheiten in einem Ballungsraum. Der unabhängige Plattenpool wird zwischen den externen Speichereinheiten repliziert, um die Verfügbarkeit bei geplanten und ungeplanten Betriebsunterbrechungen zu gewährleisten. Wenn Metro Mirror eine Hostaktualisierung auf dem Produktionsdatenträger feststellt, wird die entsprechende Aktualisierung auf den Ausweichdatenträger übertragen. Metro Mirror unterstützt Entfernungen

| zwischen den Einheiten von bis zu 300 Kilometern. Verzögerungen bei den Antwortzeiten sind bei Metro Mirror proportional zur Entfernung zwischen den Datenträgern.

| Dieses Szenario umfasst die Konfiguration der nativen i5/OS-Hochverfügbarkeitstechnologie, enthält aber keine Installations- oder Konfigurationsanweisungen für die IBM System Storage-Einheiten der Reihe DS6000 oder DS8000. In diesem Szenario wird davon ausgegangen, dass vor der Konfiguration der i5/OS-Hochverfügbarkeitslösung bereits eine IBM System Storage-Lösung vorhanden ist. Informationen zur Installation und Konfiguration der Speichereinheit DS6000 finden Sie im IBM System Storage DS6000 Information Center. Informationen zur Installation und Konfiguration der Speichereinheit DS8000 finden Sie im IBM System Storage DS8000 Information Center.

| Zielsetzungen

| Vorteile dieser Lösung:

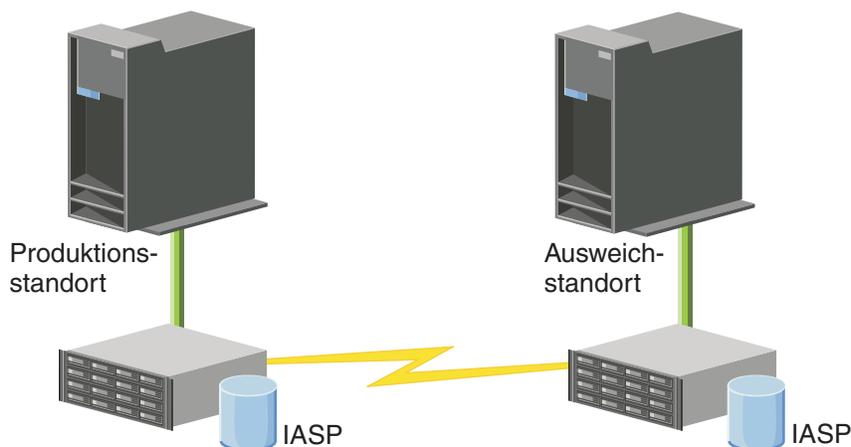
- | • Die gesamte Replikation wird von der externen Speichereinheit gesteuert, daher wird die CPU des Systems nicht belastet. Die Replikation wird in der Speichereinheit auch dann fortgesetzt, wenn es zu einem Systemausfall kommt.
- | • Verfügbarkeit der Unternehmensressourcen auch bei geplanten oder ungeplanten Betriebsunterbrechungen, wie z. B. bei Ausfällen bedingt durch Wartungsarbeiten, Softwareausfall oder PTF-Verarbeitung sowie Wiederherstellung nach einem Katastrophenfall.
- | • Die Ein-/Ausgabe bleibt konsistent und muss nicht synchronisiert werden.
- | • Kurze Wiederanlaufzeiten bei gleichzeitiger Nutzung des Journaling. Mithilfe des Journaling können Daten im Falle von ungeplanten Betriebsunterbrechungen oder Ausfällen schneller wiederhergestellt werden. Beim Journaling wird das Schreiben von Daten auf die Platte erzwungen, wenn die Spiegelung stattfindet. Wird kein Journaling verwendet, können die Daten im Hauptspeicher verloren gehen. Journaling stellt sicher, dass diese Transaktionen auf Datenebene wiederhergestellt werden und sorgt für kürzere Wiederanlaufzeiten.
- | • Möglichkeit zur Nutzung der FlashCopy-Funktion auf der Quellen- und Zielseite von Metro Mirror.

| Nachteile dieser Lösung:

- | • Erfordert externe Speicherhardware.
- | • Die Verwendung redundanter Kommunikationspfade und adäquater Bandbreiten ist zu berücksichtigen.
- | • Es ist kein gleichzeitiger Zugriff auf den Plattenpool möglich.

| Details

| Die folgende Abbildung veranschaulicht diese Lösung:



| **Konfigurationsschritte**

- | 1. Planungsprüfliste für Cluster ausfüllen
- | 2. Cluster erstellen
- | 3. Knoten hinzufügen
- | 4. Knoten starten
- | 5. Knoten zu einer Einheitendomäne hinzufügen
- | 6. Clusterverwaltungsdomäne erstellen
- | 7. Clusterverwaltungsdomäne starten
- | 8. Unabhängigen Plattenpool erstellen
- | 9. Einträge für überwachte Ressourcen hinzufügen
- | 10. Hardware umschaltbar machen
- | 11. Einheiten-CRG erstellen
- | 12. Einheiten-CRG starten
- | 13. Plattenpool verfügbar machen
- | 14. Metro-Mirror-Sitzung konfigurieren
- | 15. Switchover ausführen, um die Konfiguration zu testen

| **Szenario: Standortübergreifende Spiegelung mit Global Mirror**

| In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die auf externem Speicher basiert und die Wiederherstellung nach einem Katastrophenfall sowie Hochverfügbarkeit für Speichersysteme über große Entfernungen sicherstellt. Global Mirror ist eine IBM Systems Storage-Lösung, mit der Daten asynchron von der Speichereinheit am Produktionsstandort auf die Speichereinheit am Ausweichstandort kopiert werden. Auf diese Weise bleiben die Daten am Ausweichstandort konsistent.

| **Übersicht**

| Die Lösung mit standortübergreifender Spiegelung in Form von Global Mirror ermöglicht die Wiederherstellung durch Verwendung externer Speichereinheiten über große Entfernungen. Der unabhängige Plattenpool wird zwischen den externen Speichereinheiten repliziert, um die Verfügbarkeit bei geplanten und ungeplanten Betriebsunterbrechungen zu gewährleisten.

| Dieses Szenario umfasst die Konfiguration der nativen i5/OS-Hochverfügbarkeitstechnologie, enthält aber keine Installations- oder Konfigurationsanweisungen für die IBM System Storage-Einheiten der Reihe DS6000 oder DS8000. In diesem Szenario wird davon ausgegangen, dass vor der Konfiguration der i5/OS-Hochverfügbarkeitslösung bereits eine IBM System Storage-Lösung vorhanden ist. Informationen zur Installation und Konfiguration der Speichereinheit DS6000 finden Sie im IBM System Storage DS6000 Information Center. Informationen zur Installation und Konfiguration der Speichereinheit DS8000 finden Sie im IBM System Storage DS8000 Information Center.

| **Zielsetzungen**

| Vorteile dieser Lösung:

- | • Die gesamte Replikation wird von der externen Speichereinheit gesteuert, daher wird die CPU des Systems nicht belastet. Die Replikation wird in der Speichereinheit auch dann fortgesetzt, wenn es zu einem Systemausfall kommt.
- | • Verfügbarkeit der Unternehmensressourcen auch bei geplanten oder ungeplanten Betriebsunterbrechungen, wie z. B. bei Ausfällen bedingt durch Wartungsarbeiten, Softwareausfall oder PTF-Verarbeitung sowie Wiederherstellung nach einem Katastrophenfall.
- | • Kurze Wiederanlaufzeiten bei gleichzeitiger Nutzung des Journaling. Mithilfe des Journaling können Daten im Falle von ungeplanten Betriebsunterbrechungen oder Ausfällen schneller wiederhergestellt werden. Beim Journaling wird das Schreiben von Daten auf die Platte erzwungen, wenn die Spiege-

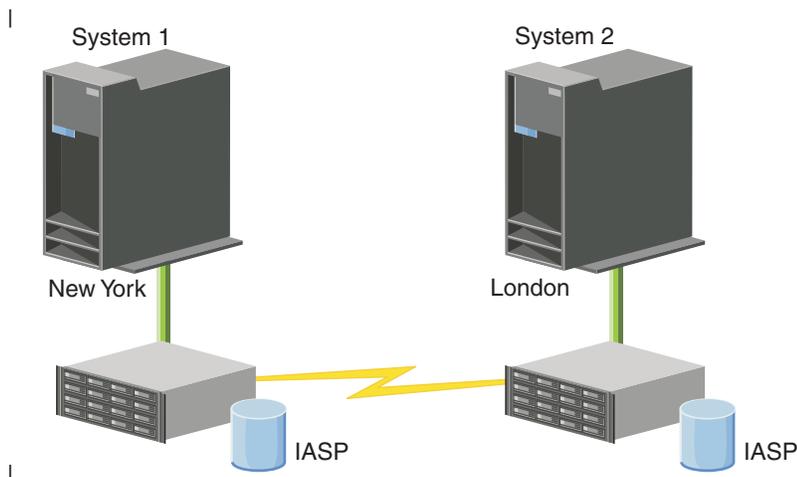
- | lung stattfindet. Wird kein Journaling verwendet, können die Daten im Hauptspeicher verloren gehen.
- | Journaling stellt sicher, dass diese Transaktionen auf Datenebene wiederhergestellt werden und sorgt für kürzere Wiederanlaufzeiten.
- | • Möglichkeit zur Nutzung der FlashCopy-Funktion auf der Quellen- und Zielseite von Global Mirror.

| Nachteile dieser Lösung:

- | • Erfordert externe Speicherhardware.
- | • Die Verwendung redundanter Kommunikationspfade und adäquater Bandbreiten ist zu berücksichtigen.
- | • Es ist kein gleichzeitiger Zugriff auf den Plattenpool möglich.
- | • Global Mirror darf nur auf einer System i-Partition auf einem bestimmten System Storage-Server konfiguriert sein. Keine anderen System i-Partitionen oder -Server von anderen Plattformen dürfen Global Mirror zum selben Zeitpunkt nutzen. Wenn einer Global-Mirror-Sitzung mehr als ein Benutzer hinzugefügt wird, kann dies zu unvorhersehbaren Ergebnissen führen.

| Details

| Die folgende Abbildung veranschaulicht diese Lösung:



| Konfigurationsschritte

- | 1. Planungsprüfliste für Cluster ausfüllen
- | 2. Cluster erstellen
- | 3. Knoten hinzufügen
- | 4. Knoten starten
- | 5. Knoten zu einer Einheitendomäne hinzufügen
- | 6. Clusterverwaltungsdomäne erstellen
- | 7. Clusterverwaltungsdomäne starten
- | 8. Unabhängigen Plattenpool erstellen
- | 9. Einträge für überwachte Ressourcen hinzufügen
- | 10. Hardware umschaltbar machen
- | 11. Einheiten-CRG erstellen
- | 12. Einheiten-CRG starten
- | 13. Plattenpool verfügbar machen
- | 14. Global-Mirror-Sitzung konfigurieren
- | 15. Switchover ausführen, um die Konfiguration zu testen

TCP/IP für hohe Verfügbarkeit konfigurieren

Da die Cluster Resource Services für die Kommunikation mit anderen Clusterknoten - die Systeme oder logische Partitionen innerhalb einer Hochverfügbarkeitsumgebung darstellen - ausschließlich IP benutzen, müssen alle Clusterknoten über IP erreichbar sein. D. h., Sie müssen über konfigurierte IP-Schnittstellen zur Verbindung der Knoten in Ihrem Cluster verfügen.

Die IP-Adressen werden entweder manuell vom Netzwerkadministrator in den TCP/IP-Routing-Tabellen der einzelnen Clusterknoten konfiguriert, oder sie werden durch Routing-Protokolle im Netzwerk generiert. Die TCP/IP-Routing-Tabelle dient als Leitfaden zum Auffinden der einzelnen Knoten in einem Cluster; daher muss jeder Knoten über eine eindeutige IP-Adresse verfügen.

Jedem Knoten können bis zu zwei IP-Adressen zugeordnet werden. Diese Adressen dürfen auf keinen Fall von anderen Netzwerkkommunikationsanwendungen geändert werden. Bei der Zuordnung der einzelnen Adressen sollten Sie beachten, welche Adresse welche Kommunikationsleitung verwendet. Wenn Sie eine bestimmte Art von Kommunikationsmedium bevorzugen, müssen Sie die erste IP-Adresse mit diesem bevorzugten Medium konfigurieren. Die erste IP-Adresse wird von der zuverlässigen Nachrichtenfunktion und der Heartbeatüberwachung bevorzugt behandelt. Sämtliche IP-Adressen auf einem Knoten müssen in der Lage sein, jede andere IP-Adresse in dem Cluster zu erreichen. Zwei Adressen gelten als gegenseitig erreichbar, wenn ein Ping-Befehl in beide Richtungen abgesetzt und ein UDP-Nachrichtentraceleitweg wechselseitig benutzt werden kann.

Anmerkung: Sie müssen sicher sein, dass die Loopback-Adresse (127.0.0.1) für das Clustering aktiv ist. Diese Adresse, über die beliebige Nachrichten an den lokalen Knoten zurückgesendet werden, ist normalerweise standardmäßig aktiv. Ist die Adresse jedoch versehentlich inaktiv geworden, muss sie erneut gestartet werden, damit die Clusternachrichtenfunktion wieder funktionieren kann.

TCP/IP-Konfigurationsattribute

Zur Aktivierung der Cluster Resource Services sind bestimmte Attributeinstellungen in der TCP/IP-Konfiguration des Netzwerks erforderlich.

Bevor ein Knoten einem Cluster hinzugefügt werden kann, müssen die Einstellungen für diese Attribute gesetzt werden.

- Geben Sie mit dem Befehl CHGTCPA (TCP/IP-Attribute ändern) für die IP-Datagrammweiterleitung den Wert *YES an, wenn Sie planen, ein System i-Produkt als Router für die Kommunikation mit anderen Netzwerken einzusetzen, und auf dem Server keine anderen Routing-Protokolle laufen.
- Setzen Sie den INETD-Server auf START. Weitere Informationen zum Starten des INETD-Servers finden Sie unter „INETD-Server starten“.
- Setzen Sie die UDP-Kontrollsumme (UDP = User Datagram Protocol) mit dem Befehl CHGTCPA (TCP/IP-Attribute ändern) auf *YES.
- Setzen Sie die MCAST-Weiterleitung auf *YES, wenn Sie die Token-Ring-Netzwerke über Brücken verbinden.
- Wenn Sie OptiConnect for i5/OS für die Kommunikation zwischen Clusterknoten verwenden, starten Sie das QSOC-Subsystem, indem Sie STRSBS(QSOC/QSOC) angeben.

INETD-Server starten

Zur Verarbeitung nach dem Zusammenführen von Partitionen oder zum Hinzufügen oder Starten eines Knotens muss zuerst der INETD-Server (INETD = Internet Daemon) gestartet werden.

Es wird empfohlen, den INETD-Server im Cluster ständig laufen zu lassen.

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Netzwerk** im IBM Systems Director Navigator for i5/OS aus.

4. Wählen Sie auf der Begrüßungsseite **TCP/IP-Server** aus.
5. Wählen Sie auf der Seite "TCP/IP-Server" **TCP/IP-Server** aus. Daraufhin wird eine Liste der verfügbaren TCP/IP-Server angezeigt.
6. Wählen Sie in der Liste **INETD** aus.
7. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Starten** aus. Der Status des Servers ändert sich in **Gestartet**.

Der INETD-Server kann auch mit dem Befehl STRTCPSVR (TCP/IP-Server starten) unter Angabe des Parameters *INETD gestartet werden. Nach dem Starten des INETD-Servers wird in der Liste der aktiven Jobs der Job QTOGINTD (Benutzer QTCP) auf dem Knoten angezeigt.

Zugehörige Verweise

TCP/IP-Server starten (STRTCPSVR)

Cluster konfigurieren

Für jede i5/OS-Implementierung mit hoher Verfügbarkeit muss ein Cluster zur Steuerung und Verwaltung ausfallsicherer Ressourcen konfiguriert werden. In Verbindung mit anderen Technologien für ausfallsichere Daten wie z. B. umschaltbare Platten, standortübergreifende Spiegelung oder logische Replikation, bietet die Clustertechnologie die Schlüsselinfrastruktur, die für HA-Lösungen benötigt wird.

Die Cluster Resource Services umfassen eine Reihe von integrierten Services, mit denen die Cluster-topologie gewartet, die Heartbeatüberwachung durchgeführt sowie Clusterkonfigurations- und Clusterressourcengruppen (CRGs) erstellt und verwaltet werden können. Die Cluster Resource Services stellen zuverlässige Messagingfunktionen zur Überwachung und Protokollierung der einzelnen Knoten bereit und sorgen dafür, dass alle Knoten ständig über den Zustand der Clusterressourcen informiert sind. Über die grafische Benutzeroberfläche der Cluster Resource Services, die zum Lieferumfang des IBM System i High Availability Solutions Manager (iHASM), Lizenzprogrammnummer, 5761-HAS, gehört, können Cluster innerhalb Ihrer HA-Lösung konfiguriert und verwaltet werden. Zudem stellt das Lizenzprogramm eine Reihe von CL-Befehlen bereit, die Ihnen die Möglichkeit geben, mit Clusterkonfigurationen zu arbeiten.

Ferner sind weitere Anwendungsprogrammierschnittstellen (APIs) und Einrichtungen verfügbar, die von Anwendungsprovidern und Kunden zur Verbesserung der Verfügbarkeit ihrer Anwendungen eingesetzt werden können.

Zusätzlich zu diesen IBM Technologien stellen Anbieter von Hochverfügbarkeitslösungen Anwendungen zur Verfügung, die Cluster mit logischer Replikationstechnologie verwenden.

Cluster erstellen

Zur Erstellung eines Clusters benötigen Sie mindestens einen Knoten, und Sie müssen Zugriff auf mindestens einen der Knoten verfügen, die Teil des Clusters sein werden.

Wenn Sie nur einen Knoten angeben, muss es sich dabei um das System handeln, auf das Sie derzeit zugreifen. Eine vollständige Liste der Voraussetzungen, die erfüllt werden müssen, um einen Cluster zu erstellen, finden Sie unter „Planungsprüfliste für Cluster“ auf Seite 73.

Wenn Sie planen, umschaltbare Einheiten in Ihrem Cluster zu verwenden oder Technologien für standortübergreifende Spiegelung zur Konfiguration einer HA-Lösung einzusetzen, müssen zusätzliche Voraussetzungen erfüllt sein. Verschiedene Beispiele zu HA-Lösungen, die diese Technologien einsetzen, finden Sie unter Szenarios: HA-Lösungen konfigurieren. Jedes Szenario umfasst in einzelne Schritte aufgeteilte Konfigurationstasks sowie eine Übersicht über die Art der Ausfallsicherheit, die diese Lösung bereitstellt. Sie können Ihre HA-Lösung anhand dieser Beispiele konfigurieren oder an Ihre individuellen Bedürfnisse anpassen.

Führen Sie die folgenden Schritte aus, um einen Cluster zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Begrüßungsseite **Neuer Cluster** aus.
- | 5. Folgen Sie den Anweisungen im Assistenten für neue Cluster, um den Cluster zu erstellen.

Nach der Erstellung des neuen Clusters wird auf der Begrüßungsseite der Cluster Resource Services oben der Name des Clusters angezeigt. Auf der Begrüßungsseite sind verschiedene Tasks für das Arbeiten mit Clustern aufgeführt.

Nach der Erstellung eines Clusters müssen Sie weitere Knoten hinzufügen und Clusterressourcengruppen (CRGs) erstellen.

Zugehörige Informationen

Cluster erstellen (CRTCLU)

API Create Cluster (QcstCreateCluster)

Knoten aktivieren und einem Cluster hinzufügen:

Bevor Sie einem Cluster einen Knoten hinzufügen können, müssen Sie zuerst einen Wert für das Netzwerkattribut `ALWADDCLU` (Hinzufügen zu Cluster zulassen) setzen.

Verwenden Sie hierzu den Befehl `CHGNETA` (Netzwerkattribute ändern) auf jedem beliebigen Server, auf dem Sie den Clusterknoten konfigurieren möchten. Mit dem Befehl `CHGNETA` werden die Netzwerkattribute eines Systems geändert. Über das Netzwerkattribut `ALWADDCLU` wird angegeben, ob dieses System von einem anderen System als Knoten in einem Cluster hinzugefügt werden kann.

Anmerkung: Sie müssen die Berechtigung `*IOSYSCFG` haben, um das Netzwerkattribut `ALWADDCLU` zu ändern.

Gültige Werte sind:

***SAME**

Der Wert wird nicht geändert. Das System wird mit dem Wert `*NONE` ausgeliefert.

***NONE**

Dieses System darf von keinem anderen System als Knoten in einem Cluster hinzugefügt werden.

***ANY** Andere Systeme können dieses System als Knoten in einem Cluster hinzufügen.

***RQSAUT**

Andere Systeme können dieses System als Knoten in einem Cluster hinzufügen, aber erst nachdem die Anforderung authentifiziert wurde.

Das Netzwerkattribut `ALWADDCLU` (Hinzufügen zu Cluster zulassen) wird überprüft, um festzustellen, ob der Knoten, der hinzugefügt wird, Teil des Clusters sein soll und ob die Clusteranfrage mittels digitaler X.509-Zertifikate validiert werden soll. Ein *digitales Zertifikat* ist eine Art persönlicher Ausweis, der elektronisch überprüft werden kann. Wenn eine Gültigkeitsprüfung erforderlich ist, müssen auf dem anfragenden Knoten und dem Knoten, der hinzugefügt werden soll, folgende Systemkomponenten installiert sein:

- i5/OS Option 34 (Digital Certificate Manager)
- i5/OS Option 35 (CCA Cryptographic Service Provider)

Wenn `*RQSAUT` für `ALWADDCLU` ausgewählt wurde, muss die Anerkennungsliste der Zertifizierungsinstanz für die i5/OS-Clustersicherheitsserveranwendung korrekt konfiguriert werden. Die Serveranwen-

dungs-ID ist QIBM_QCST_CLUSTER_SECURITY. Fügen Sie Zertifizierungsinstanzen zumindest für die Knoten hinzu, die Sie dem Cluster hinzufügen wollen.

Knoten hinzufügen:

Über die grafische Oberfläche der Cluster Resource Services können Sie bei der Ersterstellung eines Clusters zunächst einen einfachen, aus zwei Knoten bestehenden Cluster bilden. Der i5/OS-Hochverfügbarkeitslösung können dann weitere Knoten hinzugefügt werden.

Wenn Sie einen neuen Cluster als Teil der HA-Lösung erstellen, müssen Sie zusätzliche Knoten über einen aktiven Knoten im Cluster hinzufügen.

Führen Sie die folgenden Schritte aus, um einen Knoten zu einem vorhandenen Cluster hinzuzufügen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Klicken Sie auf der Registerkarte **Knoten** auf das Menü **Aktion auswählen**, und wählen Sie die Aktion **Knoten hinzufügen** aus. Die Seite "Knoten hinzufügen" wird angezeigt.
6. Geben Sie auf der Seite "Knoten hinzufügen" die Informationen für den neuen Knoten an. Klicken Sie dann auf **OK**, um den Knoten hinzuzufügen. Der neue Knoten erscheint in der Liste der Knoten. Ein Cluster kann bis 128 zu Knoten haben.

Knoten starten:

Durch Starten eines Clusterknotens werden das Clustering und die Cluster Resource Services auf einem Knoten in einer i5/OS-Hochverfügbarkeitsumgebung gestartet.

Ein Knoten kann sich selbst starten und kann wieder in den aktuellen Cluster aufgenommen werden, vorausgesetzt, er kann einen aktiven Knoten im Cluster finden.

Führen Sie die folgenden Schritte aus, um das Clustering auf einem Knoten zu starten:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Registerkarte **Knoten** den Knoten aus, den Sie starten möchten.
5. Klicken Sie im Menü **Aktion auswählen** auf **Starten**. Bei erfolgreichem Start der Cluster Resource Services auf dem angegebenen Knoten wird der Status des Knotens auf "Gestartet" gesetzt.

Knoten zu einer Einheitendomäne hinzufügen:

Eine Einheitendomäne ist eine Untergruppe von Knoten in einem Cluster, in dem Einheitenressourcen gemeinsam genutzt werden.

1. Bei Implementierung einer HA-Lösung, die Technologien auf der Basis unabhängiger Plattenpools nutzt, wie z. B. umschaltbare Platten oder standortübergreifende Spiegelung, müssen Sie den Knoten als Teil einer Einheitendomäne definieren. Nachdem Sie den Knoten einer Einheitendomäne hinzugefügt haben, können Sie eine Einheiten-CRG erstellen, die die Wiederherstellungsdomäne für den Cluster definiert.
2. Alle Knoten, die zu einer Wiederherstellungsdomäne für eine Einheiten-CRG gehören sollen, müssen sich in derselben Einheitendomäne befinden. Ein Clusterknoten darf nur einer Einheitendomäne angehören.

Zum Erstellen und Verwalten von Einheitendomänen müssen Sie i5/OS Option 41 (HA Switchable Resources) installiert haben. Sämtliche Clusterknoten in der Einheitendomäne müssen über eine gültige Lizenzberechtigung verfügen.

Führen Sie die folgenden Schritte aus, um einen Knoten zu einer Einheitendomäne hinzuzufügen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten**, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Wählen Sie auf der Registerkarte **Knoten** den Knoten aus, den Sie der Einheitendomäne hinzufügen möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus.
7. Geben Sie auf der Registerkarte **Clusterbildung** den Namen der Einheitendomäne an, der Sie den Knoten im Feld **Einheitendomäne** hinzufügen möchten.

Clusterressourcengruppe erstellen:

Clusterressourcengruppen (CRGs) verwalten HA-Ressourcen, wie z. B. Anwendungen, Daten und Einheiten. Jede CRG-Art verwaltet ihre spezielle Ressourcenart innerhalb einer HA-Umgebung.

Über die grafische Oberfläche der Cluster Resource Services können Sie unterschiedliche CRGs für die Verwaltung Ihrer HA-Ressourcen erstellen. Jede CRG-Art kann separat oder in Verbindung mit anderen CRGs eingesetzt werden. Angenommen, Sie verfügen über eine eigenständige Geschäftsanwendung, die unbedingt hohe Verfügbarkeit aufweisen muss. Nachdem Sie die Anwendung für Hochverfügbarkeit aktiviert haben, können Sie CRGs erstellen, die Sie bei der Verwaltung der Hochverfügbarkeit dieser Anwendung unterstützen.

Wenn lediglich die Anwendung, nicht aber die Daten bei einem Ausfall verfügbar sein müssen, können Sie eine Anwendungs-CRG erstellen. Wenn jedoch sowohl die Anwendung als auch die Daten verfügbar sein sollen, können Sie beide in einem unabhängigen Plattenpool speichern, der in einer Einheiten-CRG definiert wird. Bei einem Ausfall wird der gesamte unabhängige Plattenpool auf einen Ausweichknoten umgeschaltet, wodurch sowohl die Anwendung als auch deren Daten verfügbar gemacht werden.

Anwendungs-Clusterressourcengruppen erstellen:

Wenn Ihre HA-Lösung Anwendungen umfasst, die hochverfügbar sein müssen, können Sie eine Anwendungs-CRG erstellen, um Failover für diese Anwendung zu verwalten.

Geben Sie bei der Erstellung der Anwendungs-CRG an, dass eine aktive IP-Übernahmeadresse zulässig sein soll. Wenn Sie eine Anwendungs-CRG starten, die eine aktive IP-Übernahmeadresse zulässt, kann die CRG gestartet werden.

Führen Sie die folgenden Schritte aus, um eine Anwendungs-CRG zu erstellen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.

6. Wählen Sie **Neue Anwendungs-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Die Seite "Neue Anwendungs-Clusterressourcengruppe" wird angezeigt.
7. Geben Sie auf der Seite **Allgemein** die folgenden Informationen für die Anwendungs-CRG an:
- Geben Sie im Feld **Name** den Namen der CRG an. Der Name darf nicht länger als 10 Zeichen sein.
 - Geben Sie im Feld **IP-Übernahmeadresse** die IP-Adresse an, die der Anwendungs-CRG zugeordnet werden soll. Der Wert muss mit Trennzeichen angegeben werden und darf höchstens 15 Zeichen lang sein. Die IP-Übernahmeadresse erlaubt den Zugriff auf die Anwendung, ungeachtet des Systems, auf dem die Anwendung derzeit ausgeführt wird. Anhand der Angabe im Feld **IP-Übernahmeadresse konfigurieren** wird festgelegt, wer für die Erstellung der IP-Adresse verantwortlich ist, der Benutzer oder die Cluster Resource Services.
 - Geben Sie im Feld **Beschreibung** eine Beschreibung der Clusterressourcengruppe ein. Die Beschreibung darf nicht länger als 50 Zeichen sein.
 - Wählen Sie **Neustart zulassen** aus, und geben Sie eine Zahl für die Neustartversuche für eine Anwendungs-CRG an. Mit diesem Wert wird festgelegt, wie oft versucht werden darf, die Anwendung auf einem Knoten neu zu starten, bevor ein Failover auf den Ausweichknoten erfolgt.
 - Wählen Sie im Feld **IP-Übernahmeadresse konfigurieren** aus, ob die IP-Übernahmeadresse von den Cluster Resource Services oder einem Benutzer konfiguriert und verwaltet werden soll. Gültige Werte sind:

Cluster Resource Services

Wenn Sie diesen Wert angeben, darf die IP-Übernahmeadresse vor der Erstellung der Clusterressourcengruppe auf keinem Knoten der Wiederherstellungsdomäne vorhanden sein. Diese Adresse wird für Sie auf allen Wiederherstellungsdomänenknoten erstellt. Wenn die IP-Adresse bereits vorhanden ist, wird die Erstellung der Anwendungs-CRG fehlschlagen.

Benutzer

Wenn Sie diesen Wert angeben, müssen Sie die IP-Übernahmeadresse vor dem Starten der Clusterressourcengruppe auf allen in der Wiederherstellungsdomäne definierten Primär- und Ausweichknoten hinzufügen.

- Wählen Sie **Aktive IP-Übernahmeadresse zulassen** aus, um zuzulassen, dass eine IP-Übernahmeadresse aktiv ist, wenn sie einer Anwendungs-Clusterressourcengruppe zugeordnet wird. Dieses Feld ist nur gültig, wenn das Feld "IP-Übernahmeadresse konfigurieren" auf "Cluster Resource Services" gesetzt ist.
- Geben Sie im Feld **Benutzerwarteschlange für verteilte Informationen** den Namen der Benutzerwarteschlange an, die die verteilten Informationen empfangen soll. Der Name darf nicht länger als 10 Zeichen sein. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Benutzerwarteschlange für verteilte Informationen enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten. Der Name darf nicht länger als 10 Zeichen sein.

Anmerkung: Wenn Sie im Feld für die Benutzerwarteschlange für verteilte Informationen Leerzeichen eingeben, müssen Sie dies auch im Feld für den Bibliotheksnamen tun. Außerdem müssen Sie im Feld für die Failoverwartezeit und im Feld für die Failoverstandardaktion den Wert "0" eingeben.

- Geben Sie im Feld **Failovernachrichtenwarteschlange** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, wenn ein Failover für diese Clusterressourcengruppe durchgeführt wird. Wenn dieses Feld definiert ist, muss die angegebene Nachrichtenwarteschlange nach Beendigung des Exitprogramms auf allen Knoten der Wiederherstellungsdomäne vorhanden sein. Die Failovernachrichtenwarteschlange darf sich nicht in einem unabhängigen Plattenspeicherpool befinden. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten.
- Geben Sie im Feld **Failoverwartezeit** die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Clusternachrichtenwarteschlange erfolgen muss. Gültige Werte sind:

Nicht warten

Das Failover wird ohne Benutzereingriff ausgeführt.

Unbegrenzt warten

Es wird unbegrenzt auf die Beantwortung der Failoveranfragenachricht gewartet.

Anzahl Die Wartezeit (in Minuten) angeben, innerhalb der eine Antwort auf die Failoveranfragenachricht erfolgen muss. Wenn innerhalb des angegebenen Zeitraums keine Antwort eingeht, wird entsprechend dem im Feld "Failoverstandardaktion" angegebenen Wert fortgefahren.

- Geben Sie im Feld **Failoverstandardaktion** die Aktion an, die beim Clustering ausgeführt werden soll, wenn innerhalb der für das Failover festgelegten Wartezeit keine Antwort auf die Failovernachricht in der Clusternachrichtenwarteschlange eingegangen ist. Sie können in diesem Feld **Failover fortsetzen** oder **Failover abbrechen** angeben.

8. Auf der Seite **Exitprogramm** können Sie die Informationen für ein CRG-Exitprogramm angeben. Exitprogramme sind für alle CRG-Arten mit Ausnahme der Einheiten-CRGs erforderlich. Exitprogramme werden aufgerufen, nachdem ein clusterbezogenes Ereignis für eine Clusterressourcengruppe aufgetreten ist und diese darauf reagiert hat.
9. Auf der Seite **Wiederherstellungsdomäne** können Sie Knoten zur Wiederherstellungsdomäne hinzufügen und deren Rolle im Cluster angeben.

Daten-Clusterressourcengruppen erstellen:

Daten-Clusterressourcengruppen (CRGs) werden primär mit Anwendungen für logische Replikation eingesetzt, die von mehreren Anbietern zur Verfügung gestellt werden. Bei Implementierung einer HA-Lösung auf der Basis einer logischen Replikation können Sie eine Daten-CRG erstellen, die die Replikation von Daten zwischen Primär- und Ausweichknoten unterstützt.

Führen Sie die folgenden Schritte aus, um eine Daten-CRG zu erstellen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
6. Wählen Sie **Neue Daten-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Die Seite "Neue Daten-Clusterressourcengruppe" wird angezeigt.
7. Geben Sie auf der Seite **Allgemein** die folgenden Informationen in Bezug auf die Daten-CRG an:
 - Geben Sie im Feld **Name** den Namen der CRG an. Der Name darf nicht länger als 10 Zeichen sein.
 - Geben Sie im Feld **Beschreibung** eine Beschreibung der Clusterressourcengruppe ein. Die Beschreibung darf nicht länger als 50 Zeichen sein.
 - Geben Sie im Feld **Benutzerwarteschlange für verteilte Informationen** den Namen der Benutzerwarteschlange an, die die verteilten Informationen empfangen soll. Der Name darf nicht länger als 10 Zeichen sein. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Benutzerwarteschlange für verteilte Informationen enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten. Der Name darf nicht länger als 10 Zeichen sein.

Anmerkung: Wenn Sie im Feld für die Benutzerwarteschlange für verteilte Informationen Leerzeichen eingeben, müssen Sie dies auch im Feld für den Bibliotheksnamen tun. Außerdem müssen Sie im Feld für die Failoverwartezeit und im Feld für die Failoverstandardaktion den Wert "0" eingeben.

- Geben Sie im Feld **Failovernachrichtenwarteschlange** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, wenn ein Failover für diese Clusterressourcengruppe durchge-

führt wird. Wenn dieses Feld definiert ist, muss die angegebene Nachrichtenwarteschlange nach Beendigung des Exitprogramms auf allen Knoten der Wiederherstellungsdomäne vorhanden sein. Die Failovernachrichtwarteschlange darf sich nicht in einem unabhängigen Plattenspeicherpool befinden. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten.

- Geben Sie im Feld **Failoverwartezeit** die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Clusternachrichtwarteschlange erfolgen muss. Gültige Werte sind:

Nicht warten

Das Failover wird ohne Benutzereingriff ausgeführt.

Unbegrenzt warten

Es wird unbegrenzt auf die Beantwortung der Failoveranfragenachricht gewartet.

Anzahl Die Wartezeit (in Minuten) angeben, innerhalb der eine Antwort auf die Failoveranfragenachricht erfolgen muss. Wenn innerhalb des angegebenen Zeitraums keine Antwort eingeht, wird entsprechend dem im Feld "Failoverstandardaktion" angegebenen Wert fortgefahren.

8. Auf der Seite **Exitprogramm** können Sie die Informationen für ein CRG-Exitprogramm angeben. Exitprogramme sind für alle CRG-Arten mit Ausnahme der Einheiten-CRGs erforderlich. Exitprogramme werden aufgerufen, nachdem ein clusterbezogenes Ereignis für eine Clusterressourcengruppe aufgetreten ist und diese darauf reagiert hat.
9. Auf der Seite **Wiederherstellungsdomäne** können Sie Knoten zur Wiederherstellungsdomäne hinzufügen und deren Rolle im Cluster angeben.

Einheiten-Clusterressourcengruppen erstellen:

Eine Einheiten-Clusterressourcengruppe (CRG) besteht aus einem Pool von Hardwareressourcen, die als eine Entität umgeschaltet werden können. Zur Erstellung der umschaltbaren Einheiten in einer HA-Lösung müssen die Knoten, die diese Einheiten verwenden, Teil einer Einheiten-CRG sein.

Bevor Sie eine Einheiten-CRG erstellen, müssen alle Knoten, die eine umschaltbare Ressource gemeinsam benutzen werden, einer Einheitsdomäne hinzugefügt werden.

Führen Sie die folgenden Schritte aus, um eine Einheiten-CRG zu erstellen:

1. Geben Sie in einem Web-Browser <http://mysystem:2001> ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
6. Wählen Sie **Neue Einheiten-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Der Assistent **Neue Einheiten-Clusterressourcengruppe** wird angezeigt. Die Task **Neue Einheiten-Clusterressourcengruppe** ist nur verfügbar, wenn alle Knoten in der Wiederherstellungsdomäne gestartet wurden.
7. Folgen Sie den Anweisungen im Assistenten **Neue Einheiten-Clusterressourcengruppe**, um die neue Einheiten-CRG zu erstellen. Während der Assistent ausgeführt wird, können Sie eine neue Einheiten-CRG erstellen. Außerdem können Sie eine neuen unabhängigen Plattenpool erstellen oder einen vorhandenen zur Verwendung angeben.

Die Einheiten-CRG stellt sicher, dass die Informationen zu den Hardwareressourcen auf allen Knoten der Wiederherstellungsdomäne identisch bleiben und prüft, ob die Ressourcennamen identisch sind. Sie können eine Clusterverwaltungsdomäne konfigurieren, die dafür sorgt, dass die registrierten Attribute der Konfigurationsobjekte, die z. B. Ressourcennamen umfassen, innerhalb der Cluster-

| verwaltungsdomäne identisch bleiben. Wenn Sie standortübergreifende Spiegelung verwenden, sollten Sie an jedem Standort separate Einheiten-Clusterressourcengruppen für unabhängige Plattenpools und andere Typen umschaltbarer Einheiten erstellen.

| *Peer-Clusterressourcengruppen erstellen:*

| Erstellen Sie Peer-Clusterressourcengruppen (CRGs), um Knotenrollen in Lastverteilungsumgebungen zu definieren.

| Führen Sie die folgenden Schritte aus, um eine Peer-CRG zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
- | 6. Wählen Sie **Neue Peer-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Die Seite "Neue Peer-Clusterressourcengruppe" wird angezeigt.
- | 7. Geben Sie auf der Seite **Allgemein** die folgenden Informationen in Bezug auf die Peer-CRG an:
 - | • Geben Sie im Feld **Name** den Namen der CRG an. Der Name darf nicht länger als 10 Zeichen sein.
 - | • Geben Sie im Feld **Beschreibung** eine Beschreibung der Clusterressourcengruppe ein. Die Beschreibung darf nicht länger als 50 Zeichen sein.
 - | • Geben Sie die **Anwendungs-ID** für die Peer-Clusterressourcengruppen im Format `[Lieferantenname].[Anwendungsname]` an. Beispiel: `MeineFirma.MeineAnwendung`. Die Kennung darf nicht länger als 50 Zeichen sein.
- | 8. Auf der Seite **Exitprogramm** können Sie die Informationen für ein CRG-Exitprogramm angeben. Exitprogramme sind für alle CRG-Arten mit Ausnahme der Einheiten-CRGs erforderlich. Exitprogramme werden aufgerufen, nachdem ein clusterbezogenes Ereignis für eine Clusterressourcengruppe aufgetreten ist und diese darauf reagiert hat.
- | 9. Auf der Seite **Wiederherstellungsdomäne** können Sie Knoten zur Wiederherstellungsdomäne hinzufügen und deren Rolle im Cluster angeben.

Clusterressourcengruppe starten:

Durch Starten einer Clusterressourcengruppe wird das Clustering innerhalb Ihrer i5/OS-Hochverfügbarkeitsumgebung aktiviert.

Führen Sie die folgenden Tasks aus, um eine Clusterressourcengruppe zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Wählen Sie auf der Registerkarte **Clusterressourcengruppe** den Namen der CRG aus, die Sie starten möchten.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Starten** aus. In der Spalte Status ist zu sehen, dass die CRG gestartet wurde.

Zugehörige Informationen

CRG starten (STRCRG)

Nachrichtenantwarteschlangen angeben

Sie können entweder eine Clusternachrichtenantwarteschlange oder eine Failovernachrichtenantwarteschlange angeben. Mithilfe dieser Nachrichtenantwarteschlangen können Sie die Fehlerursachen in Ihrer i5/OS-Hochverfügbarkeitsumgebung feststellen.

Eine Clusternachrichtenantwarteschlange wird für Nachrichten auf Clusterebene verwendet und gibt eine Nachricht aus, die alle Clusterressourcengruppen (CRGs) bei einem Failover auf einen bestimmten Knoten steuert. Eine Failovernachrichtenantwarteschlange wird für Nachrichten auf CRG-Ebene verwendet und stellt jeweils eine Nachricht für jede CRG bereit, für die ein Failover durchgeführt wird.

Clusternachrichtenantwarteschlange angeben

Anmerkung: Wenn ein Cluster für die Verwendung einer Clusternachrichtenantwarteschlange konfiguriert werden soll, muss diese bei Ausführung des Assistenten zur Erstellung des Clusters angegeben werden.

Führen Sie die folgenden Schritte aus, um eine Clusternachrichtenantwarteschlange anzugeben:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Clustereigenschaften anzeigen**.
5. Klicken Sie auf der Seite "Clustereigenschaften" auf **Clusternachrichtenantwarteschlange**.
6. Geben Sie die folgenden Informationen an, um eine Clusternachrichtenantwarteschlange zu erstellen:
 - Geben Sie im Feld **Name** den Namen der Nachrichtenantwarteschlange an, die Nachrichten empfangen soll, die ein Failover auf Cluster- oder Knotenebene betreffen. Bei Failoveroperationen auf Knotenebene wird eine Nachricht gesendet, die das Failover aller Clusterressourcengruppen mit demselben neuen Primärknoten steuert. Wenn ein Failover für eine einzelne Clusterressourcengruppe durchgeführt wird, wird eine Nachricht gesendet, die das Failover dieser Clusterressourcengruppe steuert. Die Nachricht wird an den neuen Primärknoten gesendet. Ist dieses Feld definiert, muss die angegebene Nachrichtenantwarteschlange auf allen Knoten im Cluster vorhanden sein, wenn die Knoten gestartet werden. Die Nachrichtenantwarteschlange darf sich nicht in einem unabhängigen Plattenpool befinden.
 - Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenantwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht `*CURLIB`, `QTEMP`, `*LIBL`, `*USRLIBL`, `*ALL` oder `*ALLUSR` lauten.
 - Wählen Sie im Feld **Failoverwartezeit** entweder **Nicht warten** oder **Unbegrenzt warten** aus, oder geben Sie die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Clusternachrichtenantwarteschlange erfolgen muss.
 - Geben Sie im Feld **Failoverstandardaktion** die Aktion an, die von den Cluster Resource Services durchgeführt werden soll, wenn innerhalb der für das Failover festgelegten Wartezeit keine Antwort auf die Failovernachricht eingegangen ist. Sie können in diesem Feld **Failover fortsetzen** oder **Failover abbrechen** angeben.

Failovernachrichtenantwarteschlange angeben

Führen Sie die folgenden Schritte aus, um eine Failovernachrichtenantwarteschlange anzugeben:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.

4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Wählen Sie in der Liste der Clusterressourcengruppen die Clusterressourcengruppe aus, mit der Sie arbeiten möchten.
6. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**, und wählen Sie **Eigenschaften** aus.
7. Geben Sie auf der Seite "Allgemein" die folgenden Werte für die Failovernachrichtenwarteschlange an:
 - Geben Sie im Feld **Failovernachrichtenwarteschlange** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, wenn ein Failover für diese Clusterressourcengruppe durchgeführt wird. Wenn dieses Feld definiert ist, muss die angegebene Nachrichtenwarteschlange nach Beendigung des Exitprogramms auf allen Knoten der Wiederherstellungsdomäne vorhanden sein. Die Failovernachrichtenwarteschlange darf sich nicht in einem unabhängigen Plattenpool befinden.
 - Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten.
 - Geben Sie im Feld **Failoverwartezeit** die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Failovernachrichtenwarteschlange erfolgen muss. Sie können auch die Aktion angeben, die von den Cluster Resource Services durchgeführt werden soll, wenn innerhalb der für das Failover festgelegten Wartezeit keine Antwort auf die Failovernachricht eingegangen ist.

Switchover ausführen

Switchover werden zum Testen einer HA-Lösungsumgebung oder zur Handhabung geplanter Betriebsunterbrechungen für den Primärknoten, wie z. B. eine Sicherungsoperation oder eine geplante Systemwartung, durchgeführt.

Ein manuell durchgeführtes Switchover veranlasst den Primärknoten auf den Ausweichknoten umzuschalten. Die Wiederherstellungsdomäne der Clusterressourcengruppe definiert diese Rollen. Wenn ein Switchover stattfindet, ändern sich die Rollen der derzeit in der Wiederherstellungsdomäne definierten Rollen wie folgt:

- Dem aktuellen Primärknoten wird die Rolle des letzten aktiven Ausweichknotens zugewiesen.
- Dem aktuellen ersten Ausweichknoten wird die Rolle des Primärknotens zugewiesen.
- Alle folgenden Ausweichknoten rücken in der Reihenfolge um eine Position auf.

Ein Switchover ist nur für Anwendungs-, Daten- und Einheiten-CRGs mit dem Status "Aktiv" zulässig.

Anmerkung: Wenn Sie ein Switchover für eine Einheiten-CRG durchführen, sollten Sie Benutzerprofilnamen, Benutzer-ID (UID) und Gruppen-ID (GID) aus Leistungsaspekten synchronisieren. Die Clusterverwaltungsdomäne vereinfacht die Synchronisation der Benutzerprofile.

Führen Sie die folgenden Schritte aus, um ein Switchover für eine Ressource durchzuführen:

1. Geben Sie in einem Web-Browser <http://mysystem:2001> ein, wobei mysystem der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Wählen Sie eine Clusterressourcengruppe aus, für die Sie ein Switchover durchführen möchten. Sie können hierfür Anwendungs-, Daten- oder Einheiten-CRGs auswählen.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Switchover** aus.
7. Wählen Sie in der Bestätigungsanzeige **Ja** aus.

Die ausgewählte Clusterressourcengruppe wird jetzt auf den Ausweichknoten umgeschaltet. Die Spalte Status wird mit dem neuen Knotennamen aktualisiert.

Zugehörige Konzepte

Clusterverwaltungsdomäne

Zugehörige Tasks

„Clusterverwaltungsdomänen konfigurieren“ auf Seite 106

In einer HA-Umgebung muss die Anwendungs- und Betriebsumgebung für alle Knoten konsistent sein, die Teil der HA-Lösung sind. Die Clusterwaltungsdomäne ist die i5/OS-Implementierung der ausfallsicheren Umgebung, die dafür sorgt, dass die Betriebsumgebung für alle Knoten konsistent bleibt.

Zugehörige Informationen

CRG-Primärknoten ändern (CHGCRGPRI)

API Initiate Switchover (QcstInitiateSwitchOver)

Knoten konfigurieren

Knoten sind Systeme oder logische Partitionen, die Teil einer i5/OS-Hochverfügbarkeitslösung sind.

Die Knotenkonfiguration umfasst mehrere Tasks. Mit dem Assistenten "Cluster erstellen" können Sie einen einfachen, aus zwei Knoten bestehenden Cluster konfigurieren. Dem Cluster können Knoten bis zu einer Gesamtzahl von 128 Knoten hinzugefügt werden. Abhängig von den Technologien, auf der Ihre HA-Lösung basiert, sind möglicherweise weitere Knotenkonfigurationstasks erforderlich.

Knoten starten:

Durch Starten eines Clusterknotens werden das Clustering und die Cluster Resource Services auf einem Knoten in einer i5/OS-Hochverfügbarkeitsumgebung gestartet.

Ein Knoten kann sich selbst starten und kann wieder in den aktuellen Cluster aufgenommen werden, vorausgesetzt, er kann einen aktiven Knoten im Cluster finden.

Führen Sie die folgenden Schritte aus, um das Clustering auf einem Knoten zu starten:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Registerkarte **Knoten** den Knoten aus, den Sie starten möchten.
5. Klicken Sie im Menü **Aktion auswählen** auf **Starten**. Bei erfolgreichem Start der Cluster Resource Services auf dem angegebenen Knoten wird der Status des Knotens auf "Gestartet" gesetzt.

Zugehörige Informationen

Clusterknoten starten (STRCLUNOD)

API Start Cluster Node (QcstStartClusterNode)

Knoten aktivieren und einem Cluster hinzufügen:

Bevor Sie einem Cluster einen Knoten hinzufügen können, müssen Sie zuerst einen Wert für das Netzwerkattribut `ALWADDCLU` (Hinzufügen zu Cluster zulassen) setzen.

Verwenden Sie hierzu den Befehl `CHGNETA` (Netzwerkattribute ändern) auf jedem beliebigen Server, auf dem Sie den Clusterknoten konfigurieren möchten. Mit dem Befehl `CHGNETA` werden die Netzwerkattribute eines Systems geändert. Über das Netzwerkattribut `ALWADDCLU` wird angegeben, ob dieses System von einem anderen System als Knoten in einem Cluster hinzugefügt werden kann.

Anmerkung: Sie müssen die Berechtigung *IOSYSCFG haben, um das Netzwerkattribut ALWADDCLU zu ändern.

Gültige Werte sind:

***SAME**

Der Wert wird nicht geändert. Das System wird mit dem Wert *NONE ausgeliefert.

***NONE**

Dieses System darf von keinem anderen System als Knoten in einem Cluster hinzugefügt werden.

***ANY** Andere Systeme können dieses System als Knoten in einem Cluster hinzufügen.

***RQSAUT**

Andere Systeme können dieses System als Knoten in einem Cluster hinzufügen, aber erst nachdem die Anforderung authentifiziert wurde.

Das Netzwerkattribut ALWADDCLU (Hinzufügen zu Cluster zulassen) wird überprüft, um festzustellen, ob der Knoten, der hinzugefügt wird, Teil des Clusters sein soll und ob die Clusteranfrage mittels digitaler X.509-Zertifikate validiert werden soll. Ein *digitales Zertifikat* ist eine Art persönlicher Ausweis, der elektronisch überprüft werden kann. Wenn eine Gültigkeitsprüfung erforderlich ist, müssen auf dem anfragenden Knoten und dem Knoten, der hinzugefügt werden soll, folgende Systemkomponenten installiert sein:

- i5/OS Option 34 (Digital Certificate Manager)
- i5/OS Option 35 (CCA Cryptographic Service Provider)

Wenn *RQSAUT für ALWADDCLU ausgewählt wurde, muss die Anerkennungsliste der Zertifizierungsinstanz für die i5/OS-Clustersicherheitsserveranwendung korrekt konfiguriert werden. Die Serveranwendungs-ID ist QIBM_QCST_CLUSTER_SECURITY. Fügen Sie Zertifizierungsinstanzen zumindest für die Knoten hinzu, die Sie dem Cluster hinzufügen wollen.

Knoten hinzufügen:

Über die grafische Oberfläche der Cluster Resource Services können Sie bei der Ersterstellung eines Clusters zunächst einen einfachen, aus zwei Knoten bestehenden Cluster bilden. Der i5/OS-Hochverfügbarkeitslösung können dann weitere Knoten hinzugefügt werden.

Wenn Sie einen neuen Cluster als Teil der HA-Lösung erstellen, müssen Sie zusätzliche Knoten über einen aktiven Knoten im Cluster hinzufügen.

Führen Sie die folgenden Schritte aus, um einen Knoten zu einem vorhandenen Cluster hinzuzufügen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Klicken Sie auf der Registerkarte **Knoten** auf das Menü **Aktion auswählen**, und wählen Sie die Aktion **Knoten hinzufügen** aus. Die Seite "Knoten hinzufügen" wird angezeigt.
6. Geben Sie auf der Seite "Knoten hinzufügen" die Informationen für den neuen Knoten an. Klicken Sie dann auf **OK**, um den Knoten hinzuzufügen. Der neue Knoten erscheint in der Liste der Knoten. Ein Cluster kann bis 128 zu Knoten haben.

Zugehörige Informationen

Clusterknoteneintrag hinzufügen (ADDCLUNODE)

API Add Cluster Node Entry (QcstAddClusterNodeEntry)

Knoten zu einer Einheitendomäne hinzufügen:

Eine Einheitendomäne ist eine Untergruppe von Knoten in einem Cluster, in dem Einheitenressourcen gemeinsam genutzt werden.

- | Bei Implementierung einer HA-Lösung, die Technologien auf der Basis unabhängiger Plattenpools nutzt,
- | wie z. B. umschaltbare Platten oder standortübergreifende Spiegelung, müssen Sie den Knoten als Teil
- | einer Einheitendomäne definieren. Nachdem Sie den Knoten einer Einheitendomäne hinzugefügt haben,
- | können Sie eine Einheiten-CRG erstellen, die die Wiederherstellungsdomäne für den Cluster definiert.
- | Alle Knoten, die zu einer Wiederherstellungsdomäne für eine Einheiten-CRG gehören sollen, müssen sich
- | in derselben Einheitendomäne befinden. Ein Clusterknoten darf nur einer Einheitendomäne angehören.

Zum Erstellen und Verwalten von Einheitendomänen müssen Sie i5/OS Option 41 (HA Switchable Resources) installiert haben. Sämtliche Clusterknoten in der Einheitendomäne müssen über eine gültige Lizenzberechtigung verfügen.

Führen Sie die folgenden Schritte aus, um einen Knoten zu einer Einheitendomäne hinzuzufügen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten**, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
- | 5. Wählen Sie auf der Registerkarte **Knoten** den Knoten aus, den Sie der Einheitendomäne hinzufügen möchten.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus.
- | 7. Geben Sie auf der Registerkarte **Clusterbildung** den Namen der Einheitendomäne an, der Sie den Knoten im Feld **Einheitendomäne** hinzufügen möchten.

Zugehörige Informationen

Einheitendomäneneintrag hinzufügen (ADDDEVDMNE)

API Add Device Domain Entry (QcstAddDeviceDomainEntry)

Clusterressourcengruppen konfigurieren

Clusterressourcengruppen verwalten Ressourcen innerhalb einer i5/OS-Hochverfügbarkeitsumgebung. Verschiedene Tasks ermöglichen die Verwaltung der HA-Ressourcen mittels CRGs.

Clusterressourcengruppe starten:

Durch Starten einer Clusterressourcengruppe wird das Clustering innerhalb Ihrer i5/OS-Hochverfügbarkeitsumgebung aktiviert.

Führen Sie die folgenden Tasks aus, um eine Clusterressourcengruppe zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Wählen Sie auf der Registerkarte **Clusterressourcengruppe** den Namen der CRG aus, die Sie starten möchten.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Starten** aus. In der Spalte Status ist zu sehen, dass die CRG gestartet wurde.

Zugehörige Informationen

CRG starten (STRCRG)

API Create Cluster Resource Group (QcstCreateClusterResourceGroup)

| Clusterressourcengruppe erstellen:

| Clusterressourcengruppen (CRGs) verwalten HA-Ressourcen, wie z. B. Anwendungen, Daten und Einheiten. Jede CRG-Art verwaltet ihre spezielle Ressourcenart innerhalb einer HA-Umgebung.

| Über die grafische Oberfläche der Cluster Resource Services können Sie unterschiedliche CRGs für die Verwaltung Ihrer HA-Ressourcen erstellen. Jede CRG-Art kann separat oder in Verbindung mit anderen CRGs eingesetzt werden. Angenommen, Sie verfügen über eine eigenständige Geschäftsanwendung, die unbedingt hohe Verfügbarkeit aufweisen muss. Nachdem Sie die Anwendung für Hochverfügbarkeit aktiviert haben, können Sie CRGs erstellen, die Sie bei der Verwaltung der Hochverfügbarkeit dieser Anwendung unterstützen.

| Wenn lediglich die Anwendung, nicht aber die Daten bei einem Ausfall verfügbar sein müssen, können Sie eine Anwendungs-CRG erstellen. Wenn jedoch sowohl die Anwendung als auch die Daten verfügbar sein sollen, können Sie beide in einem unabhängigen Plattenpool speichern, der in einer Einheiten-CRG definiert wird. Bei einem Ausfall wird der gesamte unabhängige Plattenpool auf einen Ausweichknoten umgeschaltet, wodurch sowohl die Anwendung als auch deren Daten verfügbar gemacht werden.

| Anwendungs-Clusterressourcengruppen erstellen:

| Wenn Ihre HA-Lösung Anwendungen umfasst, die hochverfügbar sein müssen, können Sie eine Anwendungs-CRG erstellen, um Failover für diese Anwendung zu verwalten.

| Geben Sie bei der Erstellung der Anwendungs-CRG an, dass eine aktive IP-Übernahmeadresse zulässig sein soll. Wenn Sie eine Anwendungs-CRG starten, die eine aktive IP-Übernahmeadresse zulässt, kann die CRG gestartet werden.

| Führen Sie die folgenden Schritte aus, um eine Anwendungs-CRG zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
- | 6. Wählen Sie **Neue Anwendungs-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Die Seite "Neue Anwendungs-Clusterressourcengruppe" wird angezeigt.
- | 7. Geben Sie auf der Seite **Allgemein** die folgenden Informationen für die Anwendungs-CRG an:
 - | • Geben Sie im Feld **Name** den Namen der CRG an. Der Name darf nicht länger als 10 Zeichen sein.
 - | • Geben Sie im Feld **IP-Übernahmeadresse** die IP-Adresse an, die der Anwendungs-CRG zugeordnet werden soll. Der Wert muss mit Trennzeichen angegeben werden und darf höchstens 15 Zeichen lang sein. Die IP-Übernahmeadresse erlaubt den Zugriff auf die Anwendung, ungeachtet des Systems, auf dem die Anwendung derzeit ausgeführt wird. Anhand der Angabe im Feld **IP-Übernahmeadresse konfigurieren** wird festgelegt, wer für die Erstellung der IP-Adresse verantwortlich ist, der Benutzer oder die Cluster Resource Services.
 - | • Geben Sie im Feld **Beschreibung** eine Beschreibung der Clusterressourcengruppe ein. Die Beschreibung darf nicht länger als 50 Zeichen sein.

- Wählen Sie **Neustart zulassen** aus, und geben Sie eine Zahl für die Neustartversuche für eine Anwendungs-CRG an. Mit diesem Wert wird festgelegt, wie oft versucht werden darf, die Anwendung auf einem Knoten neu zu starten, bevor ein Failover auf den Ausweichknoten erfolgt.
- Wählen Sie im Feld **IP-Übernahmeadresse konfigurieren** aus, ob die IP-Übernahmeadresse von den Cluster Resource Services oder einem Benutzer konfiguriert und verwaltet werden soll. Gültige Werte sind:

Cluster Resource Services

Wenn Sie diesen Wert angeben, darf die IP-Übernahmeadresse vor der Erstellung der Clusterressourcengruppe auf keinem Knoten der Wiederherstellungsdomäne vorhanden sein. Diese Adresse wird für Sie auf allen Wiederherstellungsdomänenknoten erstellt. Wenn die IP-Adresse bereits vorhanden ist, wird die Erstellung der Anwendungs-CRG fehlschlagen.

Benutzer

Wenn Sie diesen Wert angeben, müssen Sie die IP-Übernahmeadresse vor dem Starten der Clusterressourcengruppe auf allen in der Wiederherstellungsdomäne definierten Primär- und Ausweichknoten hinzufügen.

- Wählen Sie **Aktive IP-Übernahmeadresse zulassen** aus, um zuzulassen, dass eine IP-Übernahmeadresse aktiv ist, wenn sie einer Anwendungs-Clusterressourcengruppe zugeordnet wird. Dieses Feld ist nur gültig, wenn das Feld "IP-Übernahmeadresse konfigurieren" auf "Cluster Resource Services" gesetzt ist.
- Geben Sie im Feld **Benutzerwarteschlange für verteilte Informationen** den Namen der Benutzerwarteschlange an, die die verteilten Informationen empfangen soll. Der Name darf nicht länger als 10 Zeichen sein. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Benutzerwarteschlange für verteilte Informationen enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten. Der Name darf nicht länger als 10 Zeichen sein.

Anmerkung: Wenn Sie im Feld für die Benutzerwarteschlange für verteilte Informationen Leerzeichen eingeben, müssen Sie dies auch im Feld für den Bibliotheksnamen tun. Außerdem müssen Sie im Feld für die Failoverwartezeit und im Feld für die Failoverstandardaktion den Wert "0" eingeben.

- Geben Sie im Feld **Failovernachrichtenwarteschlange** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, wenn ein Failover für diese Clusterressourcengruppe durchgeführt wird. Wenn dieses Feld definiert ist, muss die angegebene Nachrichtenwarteschlange nach Beendigung des Exitprogramms auf allen Knoten der Wiederherstellungsdomäne vorhanden sein. Die Failovernachrichtenwarteschlange darf sich nicht in einem unabhängigen Plattenspeicherpool befinden. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten.
- Geben Sie im Feld **Failoverwartezeit** die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Clusternachrichtenwarteschlange erfolgen muss. Gültige Werte sind:

Nicht warten

Das Failover wird ohne Benutzereingriff ausgeführt.

Unbegrenzt warten

Es wird unbegrenzt auf die Beantwortung der Failoveranfragenachricht gewartet.

Anzahl Die Wartezeit (in Minuten) angeben, innerhalb der eine Antwort auf die Failoveranfragenachricht erfolgen muss. Wenn innerhalb des angegebenen Zeitraums keine Antwort eingeht, wird entsprechend dem im Feld "Failoverstandardaktion" angegebenen Wert fortgefahren.

- Geben Sie im Feld **Failoverstandardaktion** die Aktion an, die beim Clustering ausgeführt werden soll, wenn innerhalb der für das Failover festgelegten Wartezeit keine Antwort auf die Failovernachricht in der Clusternachrichtenwarteschlange eingegangen ist. Sie können in diesem Feld **Failover fortsetzen** oder **Failover abbrechen** angeben.

| 8. Auf der Seite **Exitprogramm** können Sie die Informationen für ein CRG-Exitprogramm angeben. Exitprogramme sind für alle CRG-Arten mit Ausnahme der Einheiten-CRGs erforderlich. Exitprogramme werden aufgerufen, nachdem ein clusterbezogenes Ereignis für eine Clusterressourcengruppe aufgetreten ist und diese darauf reagiert hat.

| 9. Auf der Seite **Wiederherstellungsdomäne** können Sie Knoten zur Wiederherstellungsdomäne hinzufügen und deren Rolle im Cluster angeben.

| **Zugehörige Informationen**

| CRG erstellen (CRTCRG)

| API Create Cluster Resource Group (QcstCreateClusterResourceGroup)

| *Daten-Clusterressourcengruppen erstellen:*

| Daten-Clusterressourcengruppen (CRGs) werden primär mit Anwendungen für logische Replikation eingesetzt, die von mehreren Anbietern zur Verfügung gestellt werden. Bei Implementierung einer HA-Lösung auf der Basis einer logischen Replikation können Sie eine Daten-CRG erstellen, die die Replikation von Daten zwischen Primär- und Ausweichknoten unterstützt.

| Führen Sie die folgenden Schritte aus, um eine Daten-CRG zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
- | 6. Wählen Sie **Neue Daten-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Die Seite "Neue Daten-Clusterressourcengruppe" wird angezeigt.
- | 7. Geben Sie auf der Seite **Allgemein** die folgenden Informationen in Bezug auf die Daten-CRG an:
 - | • Geben Sie im Feld **Name** den Namen der CRG an. Der Name darf nicht länger als 10 Zeichen sein.
 - | • Geben Sie im Feld **Beschreibung** eine Beschreibung der Clusterressourcengruppe ein. Die Beschreibung darf nicht länger als 50 Zeichen sein.
 - | • Geben Sie im Feld **Benutzerwarteschlange für verteilte Informationen** den Namen der Benutzerwarteschlange an, die die verteilten Informationen empfangen soll. Der Name darf nicht länger als 10 Zeichen sein. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Benutzerwarteschlange für verteilte Informationen enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten. Der Name darf nicht länger als 10 Zeichen sein.

| **Anmerkung:** Wenn Sie im Feld für die Benutzerwarteschlange für verteilte Informationen Leerzeichen eingeben, müssen Sie dies auch im Feld für den Bibliotheksnamen tun. Außerdem müssen Sie im Feld für die Failoverwartezeit und im Feld für die Failoverstandardaktion den Wert "0" eingeben.

- | • Geben Sie im Feld **Failovernachrichtenwarteschlange** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, wenn ein Failover für diese Clusterressourcengruppe durchgeführt wird. Wenn dieses Feld definiert ist, muss die angegebene Nachrichtenwarteschlange nach Beendigung des Exitprogramms auf allen Knoten der Wiederherstellungsdomäne vorhanden sein. Die Failovernachrichtenwarteschlange darf sich nicht in einem unabhängigen Plattenspeicherpool befinden. Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten.
- | • Geben Sie im Feld **Failoverwartezeit** die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Clusternachrichtenwarteschlange erfolgen muss. Gültige Werte sind:

Nicht warten

Das Failover wird ohne Benutzereingriff ausgeführt.

Unbegrenzt warten

Es wird unbegrenzt auf die Beantwortung der Failoveranfragenachricht gewartet.

Anzahl Die Wartezeit (in Minuten) angeben, innerhalb der eine Antwort auf die Failoveranfragenachricht erfolgen muss. Wenn innerhalb des angegebenen Zeitraums keine Antwort eingeht, wird entsprechend dem im Feld "Failoverstandardaktion" angegebenen Wert fortgefahren.

8. Auf der Seite **Exitprogramm** können Sie die Informationen für ein CRG-Exitprogramm angeben. Exitprogramme sind für alle CRG-Arten mit Ausnahme der Einheiten-CRGs erforderlich. Exitprogramme werden aufgerufen, nachdem ein clusterbezogenes Ereignis für eine Clusterressourcengruppe aufgetreten ist und diese darauf reagiert hat.
9. Auf der Seite **Wiederherstellungsdomäne** können Sie Knoten zur Wiederherstellungsdomäne hinzufügen und deren Rolle im Cluster angeben.

Zugehörige Informationen

CRG erstellen (CRTCRG)

API Create Cluster Resource Group (QcstCreateClusterResourceGroup)

Einheiten-Clusterressourcengruppen erstellen:

Eine Einheiten-Clusterressourcengruppe (CRG) besteht aus einem Pool von Hardwareressourcen, die als eine Entität umgeschaltet werden können. Zur Erstellung der umschaltbaren Einheiten in einer HA-Lösung müssen die Knoten, die diese Einheiten verwenden, Teil einer Einheiten-CRG sein.

Bevor Sie eine Einheiten-CRG erstellen, müssen alle Knoten, die eine umschaltbare Ressource gemeinsam benutzen werden, einer Einheitsdomäne hinzugefügt werden.

Führen Sie die folgenden Schritte aus, um eine Einheiten-CRG zu erstellen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
6. Wählen Sie **Neue Einheiten-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Der Assistent **Neue Einheiten-Clusterressourcengruppe** wird angezeigt. Die Task **Neue Einheiten-Clusterressourcengruppe** ist nur verfügbar, wenn alle Knoten in der Wiederherstellungsdomäne gestartet wurden.
7. Folgen Sie den Anweisungen im Assistenten **Neue Einheiten-Clusterressourcengruppe**, um die neue Einheiten-CRG zu erstellen. Während der Assistent ausgeführt wird, können Sie eine neue Einheiten-CRG erstellen. Außerdem können Sie eine neuen unabhängigen Plattenpool erstellen oder einen vorhandenen zur Verwendung angeben.

Die Einheiten-CRG stellt sicher, dass die Informationen zu den Hardwareressourcen auf allen Knoten der Wiederherstellungsdomäne identisch bleiben und prüft, ob die Ressourcennamen identisch sind. Sie können eine Clusterverwaltungsdomäne konfigurieren, die dafür sorgt, dass die registrierten Attribute der Konfigurationsobjekte, die z. B. Ressourcennamen umfassen, innerhalb der Clusterverwaltungsdomäne identisch bleiben. Wenn Sie standortübergreifende Spiegelung verwenden, sollten Sie an jedem Standort separate Einheiten-Clusterressourcengruppen für unabhängige Plattenpools und andere Typen umschaltbarer Einheiten erstellen.

Zugehörige Informationen

| CRG erstellen (CRTCRG)
| API Create Cluster Resource Group (QcstCreateClusterResourceGroup)

| *Peer-Clusterressourcengruppen erstellen:*

| Erstellen Sie Peer-Clusterressourcengruppen (CRGs), um Knotenrollen in Lastverteilungsumgebungen zu definieren.

| Führen Sie die folgenden Schritte aus, um eine Peer-CRG zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**.
- | 6. Wählen Sie **Neue Peer-Clusterressourcengruppe** aus, und klicken Sie auf **Starten**. Die Seite "Neue Peer-Clusterressourcengruppe" wird angezeigt.
- | 7. Geben Sie auf der Seite **Allgemein** die folgenden Informationen in Bezug auf die Peer-CRG an:
 - | • Geben Sie im Feld **Name** den Namen der CRG an. Der Name darf nicht länger als 10 Zeichen sein.
 - | • Geben Sie im Feld **Beschreibung** eine Beschreibung der Clusterressourcengruppe ein. Die Beschreibung darf nicht länger als 50 Zeichen sein.
 - | • Geben Sie die **Anwendungs-ID** für die Peer-Clusterressourcengruppen im Format `[Lieferantenname-].[Anwendungsname]` an. Beispiel: `MeineFirma.MeineAnwendung`. Die Kennung darf nicht länger als 50 Zeichen sein.
- | 8. Auf der Seite **Exitprogramm** können Sie die Informationen für ein CRG-Exitprogramm angeben. Exitprogramme sind für alle CRG-Arten mit Ausnahme der Einheiten-CRGs erforderlich. Exitprogramme werden aufgerufen, nachdem ein clusterbezogenes Ereignis für eine Clusterressourcengruppe aufgetreten ist und diese darauf reagiert hat.
- | 9. Auf der Seite **Wiederherstellungsdomäne** können Sie Knoten zur Wiederherstellungsdomäne hinzufügen und deren Rolle im Cluster angeben.

| **Zugehörige Informationen**

| CRG erstellen (CRTCRG)
| API Create Cluster Resource Group (QcstCreateClusterResourceGroup)

| **Clusterverwaltungsdomänen konfigurieren**

| In einer HA-Umgebung muss die Anwendungs- und Betriebsumgebung für alle Knoten konsistent sein, die Teil der HA-Lösung sind. Die Clusterverwaltungsdomäne ist die i5/OS-Implementierung der ausfallsicheren Umgebung, die dafür sorgt, dass die Betriebsumgebung für alle Knoten konsistent bleibt.

| **Clusterverwaltungsdomäne erstellen:**

| Bei einer HA-Lösung bietet die Clusterverwaltungsdomäne den Mechanismus, der dafür sorgt, dass Ressourcen auf allen Systemen und Partitionen in einem Cluster synchronisiert bleiben.

| Zur Erstellung einer Clusterverwaltungsdomäne muss ein Benutzer über die Berechtigung `*IOSYSCFG` sowie über die Berechtigung zum Benutzerprofil `QCLUSTER` verfügen. Zur Verwaltung einer Clusterverwaltungsdomäne muss ein Benutzer für die CRG berechtigt sein, die die Clusterverwaltungsdomäne darstellt, für das Benutzerprofil `QCLUSTER` und die Cluster-CRG-Befehle.

| Führen Sie die folgenden Schritte aus, um eine Clusterverwaltungsdomäne zu erstellen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzulisten. Wenn keine Clusterverwaltungsdomänen konfiguriert wurden, ist die Liste leer.
5. Wählen Sie auf der Registerkarte **Verwaltungsdomänen** den Eintrag **Neue Verwaltungsdomäne** aus.
6. Geben Sie auf der Seite "Neue Verwaltungsdomäne" die folgenden Informationen zur Clusterverwaltungsdomänenengdomäne ein:
 - Geben Sie im Feld **Name** den Namen der Clusterverwaltungsdomäne ein. Der Name darf nicht länger als 10 Zeichen sein.
 - Im Feld **Cluster** wird der Name des Clusters angezeigt. Sie können den Wert in diesem Feld nicht ändern.
 - Geben Sie im Feld **Synchronisationsoption** das Synchronisationsverhalten an, das gewünscht wird, wenn ein Knoten mit einer Clusterverwaltungsdomäne verbunden wird. Das Feld wird nur aktiviert, wenn der Cluster Version 6 oder eine höhere Version hat. Gültige Werte sind:

Option Letzte Änderung (*LASTCHG) (Standardeinstellung)

Wählen Sie diese Option aus, wenn alle Änderungen an überwachten Ressourcen auf eine Clusterverwaltungsdomäne angewendet werden sollen. Die letzte (aktuellste) Änderung, die an einer überwachten Ressource vorgenommen wurde, wird auf allen aktiven Knoten auf die Ressource angewendet.

Option Aktive Domäne (*ACTDMN)

Wählen Sie diese Option aus, wenn Änderungen an überwachten Ressourcen nur auf aktiven Knoten zulässig sein sollen. Änderungen an überwachten Ressourcen auf inaktiven Knoten werden gelöscht, wenn der Knoten in die Domäne aufgenommen wird. Die Option Aktive Domäne gilt nicht für NWS-Speicherbereiche (*NWSSTG) oder NWS-Konfigurationen (*NWSCFG). Die Synchronisation dieser Ressourcen basiert immer auf der letzten vorgenommenen Änderung.

- Wählen Sie in der Liste **Knoten in der Verwaltungsdomäne** die Knoten aus, die Sie der Clusterverwaltungsdomäne hinzufügen möchten, und wählen Sie dann **Hinzufügen aus**.

Zugehörige Konzepte

„Benutzerprofile auf allen Knoten verwalten“ auf Seite 78

Es gibt zwei Methoden zur Verwaltung von Benutzerprofilen auf allen Knoten in einem Cluster.

Zugehörige Informationen

Clusterdomäne erstellen (CRTCAD)

API Create Cluster Administrative Domain (QcstCrtClusterAdminDomain)

Knoten zu einer Clusterverwaltungsdomäne hinzufügen:

In einer HA-Lösung können einer Clusterverwaltungsdomäne weitere Knoten hinzugefügt werden.

Bevor Sie einer Clusterverwaltungsdomäne einen Knoten hinzufügen, sollten Sie sich vergewissern, dass der Knoten auch Teil des Clusters ist, in dem sich die Clusterverwaltungsdomäne befindet. Ist dies nicht der Fall, können Sie den Knoten der Clusterverwaltungsdomäne nicht hinzufügen. Die Clusterverwaltungsdomäne muss zwar nicht aktiv sein, sollte es aber sein, um die Ressourcen konsistent zu halten.

Wenn Sie der Verwaltungsdomäne einen Knoten hinzufügen, werden die MREs aus der Domäne auf den hinzuzufügenden Knoten kopiert. Wenn die überwachte Ressource im neuen Knoten nicht vorhanden ist, wird sie von der Clusterverwaltungsdomäne erstellt. Ist die überwachte Ressource auf dem Knoten bereits vorhanden, wird sie mit dem Rest der Clusterverwaltungsdomäne synchronisiert, sofern die

| Domäne aktiv ist. D. h., die Attributwerte für jede überwachte Ressource auf dem Knoten, der hinzugefügt wird, werden geändert, um den globalen Werten der überwachten Ressourcen in der aktiven Domäne zu entsprechen.

| Führen Sie die folgenden Schritte aus, um einen Knoten zu einer Clusterverwaltungsdomäne hinzuzufügen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
- | 5. Wählen Sie auf der Seite "Verwaltungsdomänen" eine Clusterverwaltungsdomäne aus.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus.
- | 7. Wählen Sie auf der Seite **Eigenschaften** in der Liste **Knoten in der Verwaltungsdomäne** den Knoten aus, den Sie der Clusterverwaltungsdomäne hinzufügen möchten. Klicken Sie auf **Hinzufügen**.

| **Zugehörige Informationen**

| Knoteneintrag Domäne hinzufügen (ADDCADNODE)

| API Add Node To Recovery Domain (QcstAddNodeToRcvyDomain)

| **Clusterverwaltungsdomäne starten:**

| Clusterverwaltungsdomänen bieten eine ausfallsichere Umgebung für Ressourcen einer i5/OS-Hochverfügbarkeitslösung.

| Beim Starten der Clusterverwaltungsdomäne werden alle Änderungen, die während der Beendigung der Clusterverwaltungsdomäne an überwachten Ressourcen vorgenommen wurden, auf alle aktiven Knoten in der Clusterverwaltungsdomäne verteilt.

| Führen Sie die folgenden Schritte aus, um eine Clusterverwaltungsdomäne zu starten:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
- | 5. Wählen Sie auf der Seite "Verwaltungsdomänen" eine Clusterverwaltungsdomäne aus.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Starten** aus.

| In der Spalte Status wird angezeigt, dass die Clusterverwaltungsdomäne gestartet wurde.

| **Zugehörige Konzepte**

| „Synchronisation gespiegelter Ressourcen“

| Eine Synchronisation überwachter Ressourcen findet dann statt, wenn die überwachten Ressourcen auf den in der Clusterverwaltungsdomäne definierten Knoten geändert werden.

| **Zugehörige Informationen**

| Clusterdomäne starten (STRCAD)

| **Synchronisation gespiegelter Ressourcen:**

| Eine Synchronisation überwachter Ressourcen findet dann statt, wenn die überwachten Ressourcen auf den in der Clusterverwaltungsdomäne definierten Knoten geändert werden.

Während des Synchronisationsprozesses versucht die Clusterverwaltungsdomäne, jede Ressource zu ändern, deren Attributwerte nicht den globalen Werten entsprechen, es sei denn, es steht eine Änderung für die betreffende Ressource an. Alle anstehenden Änderungen werden an alle aktiven Knoten in der Domäne verteilt, und anschließend für jede betroffene Ressource auf jedem Knoten durchgeführt. Bei der Verteilung der anstehenden Änderungen wird der globale Wert geändert, und der globale Status jeder betroffenen Ressource wird, abhängig vom Ergebnis der Änderungsoperation für die Ressource auf den einzelnen Knoten, in *konsistent* oder *inkonsistent* geändert. Nachdem jede betroffene Ressource auf jedem Knoten in der Domäne erfolgreich geändert worden ist, ändert sich der globale Status für die betreffende Ressource in *konsistent*. Ist eine Änderungsoperation auf einem Knoten fehlgeschlagen, wird der globale Status auf *inkonsistent* gesetzt.

Wenn eine Ressource von mehreren Knoten geändert wird, während die Clusterverwaltungsdomäne inaktiv ist, werden beim Starten der Domäne alle Änderungen auf alle aktiven Knoten als Teil des Synchronisationsprozesses verteilt. Obwohl alle anstehenden Änderungen während der Aktivierung der Clusterverwaltungsdomäne verarbeitet werden, gibt es keine festgelegte Reihenfolge für die Verarbeitung der Änderungen. Werden Änderungen an einer einzigen Ressource von mehreren Clusterknoten aus vorgenommen, während die Clusterverwaltungsdomäne inaktiv ist, gibt es bei der Aktivierung keine festgelegte Reihenfolge für die Verarbeitung der Änderungen.

Wird ein Cluster in eine inaktive Clusterverwaltungsdomäne aufgenommen (d. h., der Knoten wird gestartet, während die Clusterverwaltungsdomäne beendet wird), werden die überwachten Ressourcen erst beim Starten der Clusterverwaltungsdomäne resynchronisiert.

Anmerkung: Die Clusterverwaltungsdomäne und das ihr zugeordnete Exitprogramm sind von IBM gelieferte Objekte. Sie sollten nicht über die API QcstChangeClusterResourceGroup oder dem Befehl CHGCRG (CRG ändern) geändert werden, da dies zu unvorhersehbaren Ergebnissen führen kann.

Nach Beendigung eines Clusterknotens, der Teil einer Clusterverwaltungsdomäne ist, können die überwachten Ressourcen auf dem inaktiven Knoten noch geändert werden. Die Änderungen werden dann beim erneuten Starten mit dem Rest der Clusterverwaltungsdomäne resynchronisiert. Während der Resynchronisationsverarbeitung führt die Clusterverwaltungsdomäne alle am inaktiven Knoten vorgenommenen Änderungen auf den übrigen aktiven Knoten in der Domäne aus, sofern keine Änderungen in der aktiven Domäne durchgeführt wurden, während der Knoten inaktiv war. Werden Änderungen an einer überwachten Ressource sowohl in der aktiven Domäne als auch auf dem inaktiven Knoten vorgenommen, werden die in der aktiven Domäne vorgenommenen Änderungen auch auf dem Knoten durchgeführt, der in den Cluster aufgenommen wird. Mit anderen Worten, die an überwachten Ressourcen vorgenommenen Änderungen gehen, unabhängig vom Status des Knotens, auf keinen Fall verloren. Durch Angabe der Synchronisationsoption kann das Synchronisationsverhalten gesteuert werden.

Wenn Sie einen Clusterknoten beenden möchten, der Teil einer Clusterverwaltungsdomäne ist, und nicht zulassen möchten, dass auf dem inaktiven Knoten vorgenommene Änderungen in der aktiven Domäne beim Starten des Knotens verteilt werden sollen, (z. B. wenn der Clusterknoten zum Testen beendet wird), müssen Sie den Knoten vor Beendigung des Clusterknotens aus der Peer-CRG der Verwaltungsdomäne entfernen.

Zugehörige Konzepte

KNT-Eintrag aus Domäne entfernen (RMVCADNODE)

Zugehörige Tasks

„Clusterverwaltungsdomäne starten“ auf Seite 108

Clusterverwaltungsdomänen bieten eine ausfallsichere Umgebung für Ressourcen einer i5/OS-Hochverfügbarkeitslösung.

Zugehörige Informationen

CRG-Knoteneintrag entfernen (RMVCRGNODE)

Einträge für überwachte Ressourcen hinzufügen:

| Sie können einer Clusterverwaltungsdomäne einen Eintrag für überwachte Ressourcen (MRE = Monitored Resource Entry) hinzufügen. Einträge für überwachte Ressourcen definieren kritische Ressourcen, damit Änderungen, die an diesen Ressourcen vorgenommen werden, innerhalb einer Hochverfügbarkeitsumgebung konsistent bleiben.

| Führen Sie die folgenden Schritte aus, um einen Eintrag für eine überwachte Ressource hinzuzufügen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
- | 4. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.
Hinweis: Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.
- | 5. Klicken Sie in der Liste der überwachten Ressourcenarten auf das Kontextsymbol neben der überwachten Ressourcenart, und wählen Sie **Eintrag für überwachte Ressourcen hinzufügen** aus. Die Seite "Eintrag für überwachte Ressource hinzufügen" wird angezeigt.
- | 6. Wählen Sie die Attribute aus, die für den Eintrag der überwachten Ressource überwacht werden sollen, und klicken Sie auf **OK**. Wenn das Eintragsobjekt sich in einer Bibliothek befindet, müssen Sie den Namen und die Bibliothek für das Objekt angeben. Der neue Eintrag für überwachte Ressource wird zur Liste der Ressourcen, die von der Clusterverwaltungsdomäne überwacht werden, hinzugefügt. Änderungen an der überwachten Ressource werden auf allen aktiven Knoten in der Clusterverwaltungsdomäne synchronisiert, wenn die Domäne aktiv ist. Standardmäßig werden alle Attribute überwacht, die einer überwachten Ressourcenart zugeordnet sind. Sie können jedoch eine Auswahl der zu überwachenden Attribute treffen.

Zugehörige Tasks

| „Zu überwachende Attribute auswählen“ auf Seite 144

| Nachdem Sie Einträge für überwachte Ressourcen hinzugefügt haben, können Sie die Attribute für die Ressource auswählen, die von der Clusterverwaltungsdomäne überwacht werden soll.

Zugehörige Informationen

| MRE-Eintrag Domäne hinzufügen (ADDCADMRE)

| API Add Monitored Resource Entry (QfpadAddMonitoredResourceEntry)

Umschaltbare Platten konfigurieren

Umschaltbare Platten sind unabhängige Plattenpools, die als Teil des i5/OS-Clusters konfiguriert wurden. Mithilfe umschaltbarer Platten können Daten und Anwendungen in einem unabhängigen Plattenpool gespeichert werden, um dann auf ein anderes System umgeschaltet zu werden.

Unabhängigen Plattenpool erstellen

Mithilfe des Assistenten für neue Plattenpools können Sie einen unabhängigen Plattenpool erstellen. Dieser Assistent unterstützt Sie bei der Erstellung eines neuen Plattenpools sowie beim Hinzufügen von Platteneinheiten zum Plattenpool.

Mit dem Assistenten für neue Plattenpools werden nicht konfigurierte Platteneinheiten in einer Paritätsgruppe zusammengefasst und der Einheitenparitätsschutz sowie die Komprimierung des Plattenspeichers gestartet. Beim Hinzufügen von Platteneinheiten sollten Sie darauf achten, dass Platteneinheiten, die sich in derselben Paritätsgruppe befinden, nicht über mehrere Plattenspeicherpools verteilt werden, da beim Ausfall einer Paritätsgruppe mehrere Plattenpools betroffen wären.

Führen Sie die folgenden Schritte aus, um mit dem Assistenten für neuen Plattenpool einen unabhängigen Plattenpool unter Verwendung des IBM Systems Director Navigator for i5/OS zu erstellen.

Hinweis: Wenn Sie mit Platten innerhalb des IBM Systems Director Navigator for i5/OS arbeiten möchten, müssen Sie über die entsprechende Kennwortkonfiguration für Dedicated Service Tools (DST) verfügen.

IBM Systems Director Navigator for i5/OS

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Platteneinheiten** aus.
5. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Neuer Plattenpool** aus.
6. Folgen Sie den Anweisungen des Assistenten, um Platteneinheiten einem neuen Plattenpool hinzuzufügen.
7. Drucken Sie die Plattenkonfiguration aus, damit Sie für den Fall einer Wiederherstellung verfügbar ist.
8. Notieren Sie den Namen des unabhängigen Plattenpools sowie die entsprechende Nummer.

System i Navigator

Führen Sie die folgenden Schritte aus, um mit dem System i Navigator einen unabhängigen Plattenpool zu erstellen:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das gewünschte System, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten**.
3. Klicken Sie mit der rechten Maustaste auf **Plattenpools**, und wählen Sie **Neuer Plattenpool** aus.
4. Folgen Sie den Anweisungen des Assistenten, um Platteneinheiten einem neuen Plattenpool hinzuzufügen.
5. Drucken Sie die Plattenkonfiguration aus, damit Sie für den Fall einer Wiederherstellung verfügbar ist.
6. Notieren Sie den Namen des unabhängigen Plattenpools sowie die entsprechende Nummer.

Anmerkung: Fügen Sie nach einem kompletten Neustart des System unabhängige Plattenpools hinzu. Wenn Sie den Assistenten für neuen Plattenpool im DST-Modus (DST - Dedicated Service Tools) einsetzen, müssen Sie nach dem kompletten Neustart des Systems eine Einheitenbeschreibung für den unabhängigen Plattenpool erstellen und zuordnen. Verwenden Sie hierzu den Befehl `CRTDEVASP` (Einheitenbeschreibung erstellen (ASP)). Vergeben Sie für die Einheitenbeschreibung und den Ressourcennamen denselben Namen wie für den unabhängigen Plattenpool. Prüfen Sie mit dem Befehl `WRKDEV` (Mit Einheitenbeschreibungen arbeiten), ob die Einheitenbeschreibung und der Name des unabhängigen Plattenpools übereinstimmen.

Spiegelschutz starten

Mit dem Assistenten zum Hinzufügen von Platteneinheiten und dem Assistenten für neue Plattenpools werden Sie durch den Prozess geführt, mit dem Sie Plattenpaare mit ähnlicher Kapazität einem geschützten Plattenpool hinzufügen. Sobald die Platten ordnungsgemäß konfiguriert sind, können Sie mit dem Spiegeln starten, um einen Spiegelschutz zu erhalten.

Der Spiegelschutz wirkt lokal auf einem System und unterscheidet sich von einer standortübergreifenden Spiegelung. Das System muss zuerst neu gestartet werden, damit Sie die Spiegelung auf auf einem unabhängigen, gesperrten Plattenpool starten können. Bei allen anderen Plattenpools müssen Sie Ihr System mit Dedicated Service Tools (DST) erneut starten, bevor Sie den Spiegelschutz starten können.

| Führen Sie die folgenden Schritte aus, um die Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS starten:

- | 1. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 2. Wählen Sie **Plattenpools** aus.
- | 3. Wählen Sie den Plattenpool aus, den Sie spiegeln möchten.
- | 4. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Spiegeln starten** aus.

| Führen Sie die folgenden Schritte aus, um die Spiegelung unter Verwendung des System i Navigator zu starten:

- | 1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
- | 2. Erweitern Sie den Eintrag für System i, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
- | 3. Klicken Sie mit der rechten Maustaste auf die zu spiegelnden Plattenpools, und wählen Sie **Spiegeln starten** aus.

| **Spiegelschutz stoppen**

| Wenn Sie den Spiegelschutz stoppen, bleibt eine Platteneinheit aus jedem spiegelgleichen Paar unformatiert. Bevor Sie jedoch den Spiegelschutz für einen Plattenpool stoppen können, muss in jedem spiegelgleichen Paar mindestens eine Platteneinheit vorhanden und aktiv sein.

| Sie können steuern, welche gespiegelte Platteneinheit in jedem Paar unformatiert bleibt, indem Sie die Platteneinheiten unterbrechen, deren Konfiguration zurückgenommen werden soll. Platteneinheiten, die nicht unterbrochen werden, werden automatisch ausgewählt.

| Das System muss zuerst neu gestartet werden, damit Sie die Spiegelung auf auf einem unabhängigen, gesperrten Plattenpool stoppen können. Bei allen anderen Plattenpools müssen Sie Ihr System mit Dedicated Service Tools (DST) neu starten, bevor Sie den Spiegelschutz stoppen können.

| Der Spiegelschutz ist lokal einem einzelnen System zugeordnet, und unterscheidet sich von einer standortübergreifenden Spiegelung.

| Führen Sie die folgenden Schritte aus, um den Spiegelschutz unter Verwendung des IBM Systems Director Navigator for i5/OS zu stoppen.

- | 1. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 2. Wählen Sie **Plattenpools** aus.
- | 3. Wählen Sie den Plattenpool aus, den Sie stoppen möchten.
- | 4. Wählen Sie im Menü **Select Actions** den Eintrag **Spiegeln stoppen** aus.

| Führen Sie die folgenden Schritte aus, um die Spiegelung unter Verwendung des System i Navigator zu stoppen:

- | 1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
- | 2. Erweitern Sie den Eintrag für System i, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
- | 3. Wählen Sie die Platteneinheit aus, für die Sie den Spiegelschutz stoppen möchten.
- | 4. Klicken Sie mit der rechten Maustaste auf einen ausgewählten Plattenpool, und wählen Sie **Spiegeln stoppen** aus.
- | 5. Klicken Sie im daraufhin angezeigten Dialogfenster auf **Spiegeln stoppen**.

| **Platteneinheit oder Plattenpool hinzufügen**

| Mit dem Assistenten zum Hinzufügen von Platteneinheiten können Sie einem bereits vorhandenen Plattenpool neue oder nicht konfigurierte Platteneinheiten hinzufügen.

| Mit den Assistenten für das Hinzufügen von Platteneinheiten und Plattenpools sparen Sie sehr viel Zeit, da Sie mehrere zeitaufwändige Konfigurationsfunktionen in einem effizienten Prozess zusammenfassen können. Durch die Assistenten erübrigen sich auch langwierige Überlegungen zur Konfiguration von Platteneinheiten, da sie die Funktionalität Ihres Systems kennen und nur gültige Auswahlmöglichkeiten anbieten. Ein Assistent listet z. B. die Option zum Starten der Komprimierung nur dann auf, wenn Ihr System auch über diese Funktionalität verfügt.

| Wenn Sie einem geschützten Plattenpool Platteneinheiten hinzufügen möchten, werden Sie vom Assistenten gezwungen, die Platteneinheiten unter Einheitenparitätsschutz ebenfalls einzubeziehen oder eine genügend große Anzahl an Platteneinheiten mit derselben Kapazität hinzuzufügen, bevor Sie den Spiegelschutz starten. Der Assistent bietet auch die Möglichkeit, durch Verteilung der Daten im Plattenpool einen Lastausgleich herbeizuführen oder die Plattenkomprimierung zu starten, sofern Ihre Systemkonfiguration diese Aktionen zulässt. Sie entscheiden, welche Optionen Sie auswählen möchten, damit die Operation den Gegebenheiten Ihres Systems entspricht.

| Führen Sie die folgenden Schritte aus, um eine Platteneinheit oder einen Plattenpool unter Verwendung des IBM Systems Director Navigator for i5/OS hinzuzufügen:

- | 1. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 2. Wählen Sie **Platteneinheiten** aus.
- | 3. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Platteneinheit hinzufügen** aus.
- | 4. Folgen Sie den Anweisungen des Assistenten, um Platteneinheiten einem Plattenpool hinzuzufügen.

| Führen Sie die folgenden Schritte aus, um eine Platteneinheit oder einen Plattenpool unter Verwendung des System i Navigator hinzuzufügen:

- | 1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
- | 2. Erweitern Sie den Eintrag für System i, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten**.
- | 3. Klicken Sie mit der rechten Maustaste auf **Alle Platteneinheiten**, und wählen Sie **Platteneinheit hinzufügen** aus.
- | 4. Folgen Sie den Anweisungen des Assistenten, um die Task zu beenden.

Aktuelle Konfiguration auswerten

Bevor Sie die Plattenkonfiguration Ihres Systems ändern, sollten Sie genau wissen, wo sich die vorhandenen Platteneinheiten in Bezug auf Plattenpools, IOAs und Frames befinden.

Aufgrund der grafischen Oberfläche des System i Navigator entfällt das Kompilieren der Informationen, da eine grafische Darstellung der Systemkonfiguration bereitgestellt wird. Über diese Grafikansicht können Sie jede Funktion ausführen, die auch über die Listenansicht für Platteneinheiten des System i Navigator ausgeführt werden kann, nur mit dem zusätzlichen Vorteil einer visuellen Darstellung. Wenn Sie mit der rechten Maustaste auf ein beliebiges Objekt in der Tabelle klicken (z. B. auf eine bestimmte Platteneinheit, eine Paritätsgruppe oder einen Frame), werden dieselben Optionen wie im Hauptfenster des System i Navigator angezeigt.

Sie können bestimmen, wie die Hardware in der grafischen Sicht für Platteneinheiten dargestellt wird. Sie können eine Sicht der Plattenpools anzeigen lassen und anschließend einen bestimmten Plattenpool in der Liste auswählen, für den nur die Frames mit den Platteneinheiten angezeigt werden sollen, aus denen sich der ausgewählte Plattenpool zusammensetzt. Wenn Sie "Alle Frames/Einheiten anzeigen" auswählen, werden alle Frames angezeigt, ungeachtet, ob sie Platteneinheiten im ausgewählten Plattenpool enthalten

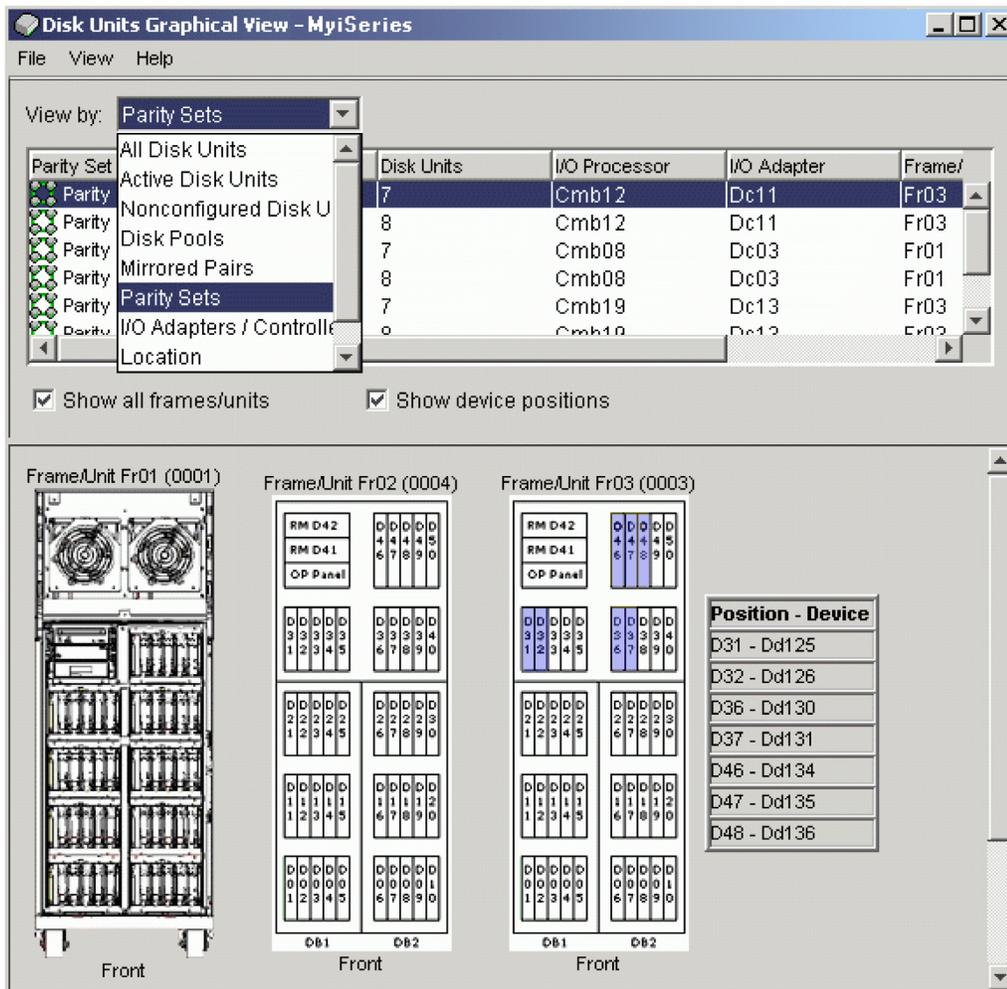
oder nicht. Eine weitere Option "Einheitenpositionen anzeigen" erlaubt Ihnen, Platteneinheitennamen den Einheitenpositionen zuzuordnen, an denen sie eingefügt werden.

Klicken Sie mit der rechten Maustaste auf eine beliebige, in der grafischen Sicht hervorgehobene blaue Platteneinheit, und wählen Sie eine Aktion aus, die für diese Einheit ausgeführt werden soll. Sie können beispielsweise die Auswahl "Komprimierung starten" oder "Komprimierung stoppen", "Platteneinheiten in eine Paritätsgruppe aufnehmen", "Platteneinheiten aus einer Paritätsgruppe ausschließen" oder "Platteneinheit umbenennen" treffen. Wenn die Platteneinheit mit Spiegelschutz ausgestattet ist, kann die Spiegelung vorübergehend unterbrochen oder wieder aufgenommen werden. Durch Klicken auf eine leere Platteneinheit mit der rechten Maustaste wird der Assistent zum Installieren von Platteneinheiten gestartet.

Führen Sie die folgenden Schritte aus, um die Grafiksicht zu aktivieren:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das gewünschte System, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten**.
3. Klicken Sie mit der rechten Maustaste auf **Alle Platteneinheiten**, und wählen Sie **Grafiksicht** aus.

Es folgt ein Beispiel für eine Grafiksicht im System i Navigator. Das Menü "Ansicht nach" enthält verschiedene Optionen zum Anzeigen der Platteneinheiten.



Plattenpool verfügbar machen

Damit auf Platteneinheiten im unabhängigen Plattenpool zugegriffen werden kann, müssen Sie den betreffenden Plattenpool zunächst verfügbar machen.

Damit auf Platteneinheiten in einem unabhängigen Plattenpool und auf die Objekte in der zugehörigen Datenbank zugegriffen werden kann, müssen Sie den betreffenden Plattenpool verfügbar machen (anhängen). Wenn Sie geographische Spiegelung verwenden, müssen Sie die Produktionskopie des Plattenpools zur Verfügung stellen. Die Spiegelkopie kann nur zur Verfügung gestellt werden, wenn Sie abgehängt ist. Bei einem Plattenpool mit geographischer Spiegelung muss die umschaltbare Hardwaregruppe gestartet sein, bevor versucht werden kann, den Plattenpool zur Verfügung zu stellen, es sein denn, die geographische Spiegelung wurde unterbrochen.

In einer Clusterumgebung mit mehreren Systemen kann der Plattenpool für den aktuellen Knoten oder einen anderen Knoten im Cluster verfügbar gemacht werden. Der unabhängiger Plattenpool kann jeweils nur für einen Knoten angehängt werden. Wenn Sie von einem anderen Knoten aus auf den unabhängigen Plattenpool zugreifen möchten, müssen Sie den unabhängigen Plattenpool auf den Ausweichclusterknoten umschalten. Der Abschnitt "Switchover durchführen" enthält Einzelheiten zum Umschalten einer Einheiten-CRG (im System i Navigator auch als umschaltbare Hardwaregruppe bezeichnet) zu einem Ausweichknoten.

Anmerkung: Wenn Sie einen primären oder sekundären Plattenpool verfügbar machen, werden alle Plattenpools in der Plattenpoolgruppe zur gleichen Zeit ebenfalls gleichzeitig verfügbar gemacht.

Wenn Sie einen Plattenpool verfügbar machen oder Änderungen der Plattenkonfiguration für einen unabhängigen Plattenpool durchführen, kann es so aussehen, als ob die Verarbeitung stoppen würde. Wenn Sie noch andere Einheitenbeschreibungsaktivitäten durchführen, werden die Aktionen zum Verfügbarmachen sowie die Konfigurationsänderungen in einen Wartestatus versetzt.

Treten in einem frühen Stadium der Verarbeitung, um einen geographisch gespiegelten Plattenpool verfügbar zu machen, Fehler auf, führt dies möglicherweise bei der nächsten derartigen Verarbeitung oder Wiederaufnahme zu einer vollständigen Synchronisation.

Führen Sie die folgenden Schritte aus, um einen unabhängige Plattenpool verfügbar zu machen:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das gewünschte System, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten**.
3. Erweitern Sie den Eintrag **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf den gesperrten Plattenpool, und wählen Sie **Verfügbar machen** aus. Sie können mehrere Plattenpools auswählen, um diese gleichzeitig verfügbar zu machen.
5. Klicken Sie im angezeigten Dialogfenster auf **Verfügbar machen**, um den Plattenpool verfügbar zu machen.

Sie können hierfür auch den Befehl VRYCFG (Konfiguration an-/abhängen) über die zeichenbasierte Schnittstelle verwenden.

Mit dem Befehl DSPASPSTS (ASP-Status anzeigen) lässt sich feststellen, welcher Schritt im Prozess gerade ausgeführt wird.

Standortübergreifende Spiegelung konfigurieren

Die standortübergreifende Spiegelung ist der Oberbegriff für verschiedene HA-Technologien. Diese mfassen die geographische Spiegelung, Metro Mirror und Global Mirror. Für jede dieser Technologien gibt es spezifische Konfigurationstasks.

Geographische Spiegelung konfigurieren

Die *geographische Spiegelung* ist eine Unterfunktion der standortübergreifenden Spiegelung. Bei der Konfiguration einer HA-Lösung unter Verwendung der geographischen Spiegelung müssen Sie eine Spiegelungssitzung zwischen dem Produktionssystem und dem Sicherungssystem konfigurieren.

Ein aktiver Cluster, Knoten und eine Clusterressourcengruppe sind die Voraussetzung für die Konfiguration der geographischen Spiegelung. Zur Durchführung der Konfiguration müssen die unabhängigen Plattenpools für die geographische Spiegelung abgehängt sein (d. h., sie dürfen nicht verfügbar sein). Unter dem Thema "Szenario: Standortübergreifende Spiegelung mit geographischer Spiegelung" finden Sie eine schrittweise Anleitung zur Einrichtung einer HA-Lösung auf der Basis der geographischen Spiegelung.

IBM Systems Director Navigator for i5/OS

Führen Sie die folgenden Schritte aus, um die geographische Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS zu konfigurieren.

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, den Sie als Produktionskopie (Quelle) verwenden möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Neue Sitzung** aus.
7. Folgen Sie den Anweisungen des Assistenten, um die Task zu beenden.

System i Navigator

Führen Sie die folgenden Schritte aus, um die geographische Spiegelung unter Verwendung des System i Navigator zu konfigurieren:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das System, das Sie als Produktionskopie verwenden möchten.
3. Erweitern Sie den Eintrag für **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf den Plattenpool, den Sie als Produktionskopie verwenden möchten, und wählen Sie **Sitzungen** → **Neu** aus.
5. Folgen Sie den Anweisungen des Assistenten, um die Task zu beenden.

Zugehörige Konzepte

„Szenario: Umschaltbare Platte mit geographischer Spiegelung“ auf Seite 81

In diesem Szenario wird eine i5/OS-Hochverfügbarkeitslösung vorgestellt, die umschaltbare Platten mit geographischer Spiegelung in einem aus drei Knoten bestehenden Cluster verwendet. Mit dieser Lösung ist sowohl eine Wiederherstellung nach einem Katastrophenfall als auch Hochverfügbarkeit sicherstellt.

Metro-Mirror-Sitzung konfigurieren

Für i5/OS-Hochverfügbarkeitslösungen mit IBM System Storage-Metro-Mirror-Technologie müssen Sie eine Sitzung zwischen der System i-Maschine und den externen IBM System Storage-Speichereinheiten, für die Metro Mirror konfiguriert wurde, herstellen. Unter i5/OS wird durch die Metro-Mirror-Sitzungen keine Spiegelung auf den externen Speichereinheiten eingerichtet, sondern es wird eine Beziehung zwischen den i5/OS-Systemen und der vorhandenen Metro-Mirror-Konfiguration auf externen Speichereinheiten hergestellt.

Bevor Sie eine Metro-Mirror-Sitzung unter i5/OS erstellen, sollten Sie Metro Mirror auf den externen IBM System Storage-Speichereinheiten konfiguriert haben. Informationen zur Verwendung von Metro Mirror auf IBM System Storage DS6000 finden Sie im IBM System Storage DS6000 Information Center. Informationen zur Verwendung von Metro Mirror auf IBM System Storage DS8000 finden Sie im IBM System Storage DS8000 Information Center.

Führen Sie die folgenden Schritte aus, um eine Metro-Mirror-Sitzung zu konfigurieren:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, den Sie als Produktionskopie (Quelle) verwenden möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Neue Sitzung** aus.
7. Folgen Sie den Anweisungen des Assistenten, um die Task zu beenden.

Zugehörige Informationen

ASP-Kopienbeschreibung hinzufügen (ADDASPCPYD)

ASP-Sitzung starten (STRASPSSN)

Global Mirror-Sitzung konfigurieren

Für HA-Lösungen unter i5/OS mit IBM System Storage-Global-Mirror-Technologie müssen Sie eine Sitzung zwischen der System i-Maschine und den externen IBM System Storage-Speichereinheiten, für die Global Mirror konfiguriert wurde, herstellen. Unter i5/OS wird durch die Global-Mirror-Sitzungen keine Spiegelung der externen Speichereinheiten eingerichtet, sondern es wird eine Beziehung zwischen den i5/OS-Systemen und der vorhandenen Global-Mirror-Konfiguration auf externen Speichereinheiten hergestellt.

Bei der IBM System Storage-Global-Mirror-Technologie müssen alle Benutzer eine einzige Global-Mirror-Verbindung gemeinsam nutzen. In einer i5/OS-Hochverfügbarkeitslösung mit Global Mirror darf nur eine System i-Partition für Global Mirror auf einem bestimmten System Storage-Server konfiguriert sein. Keine anderen System i-Partitionen oder -Server von anderen Plattformen dürfen Global Mirror zum selben Zeitpunkt nutzen. Wenn einer Global-Mirror-Sitzung mehr als ein Benutzer hinzugefügt wird, kann dies zu unvorhersehbaren Ergebnissen führen.

Bevor Sie eine Global-Mirror-Sitzung unter i5/OS erstellen, sollten Sie Global Mirror auf den externen IBM System Storage-Speichereinheiten konfiguriert haben. Informationen zur Verwendung von Global Mirror auf IBM System Storage DS6000 finden Sie im IBM System Storage DS6000 Information Center. Informationen zur Verwendung von Global Mirror auf IBM System Storage DS8000 finden Sie im IBM System Storage DS8000 Information Center.

Führen Sie die folgenden Schritte aus, um Global Mirror zu konfigurieren:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, den Sie als Produktionskopie (Quelle) verwenden möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Neue Sitzung** aus.
7. Folgen Sie den Anweisungen des Assistenten, um die Task zu beenden.

Zugehörige Informationen

ASP-Kopienbeschreibung hinzufügen (ADDASPCPYD)

Hochverfügbarkeit verwalten

Nachdem Sie eine i5/OS-Hochverfügbarkeitslösung konfiguriert haben, können Sie die Lösung über verschiedene HA-Schnittstellen verwalten.

Szenarios: HA-Lösungen verwalten

Als Systembediener oder Administrator einer HA-Lösung müssen Sie allgemeine Tasks, wie Sicherung und Systemwartung, in der HA-Umgebung ausführen.

Die folgenden Szenarios bieten Anweisungen zur Ausführung allgemeiner Schritte, wie Sicherungen und Upgrades, und enthalten Beispiele für die Verwaltung von HA-Ereignissen, wie Clusterpartitionen und Failover. Für jedes Szenario wurde eine eigene Modellumgebung ausgewählt. Die Anweisungen für die einzelnen Szenarios gelten speziell für die betreffende HA-Lösung und sind nur als Beispiel gedacht.

Szenarios: Sicherungen in einer HA-Umgebung ausführen

Abhängig von Ihrer HA-Lösung und Ihrer Sicherungsstrategie kommen für die Datensicherung unterschiedliche Methoden in Frage. Es gibt jedoch eine Reihe allgemeiner Tasks, die bei der Durchführung von Sicherungsoperationen auf Systemen in einer HA-Umgebung anfallen.

Bei mehreren HA-Lösungen besteht die Möglichkeit, Sicherungen der zweiten Datenkopie, die auf dem Sicherungssystem gespeichert ist, über Remotezugriff zu erstellen. Auf diese Weise bleibt Ihr Produktionssystem einsatzfähig, während das zweite System gesichert wird. Jedes der Szenarios zeigt Beispiele für die beiden HA-Lösungen, bei denen eine Sicherung über Remotezugriff auf dem Sicherungssystem durchgeführt wird.

Im ersten Szenario werden Sicherungen über Remotezugriff für eine HA-Lösung vorgenommen, die die Technologie für geographische Spiegelung einsetzt. Anhand des zweiten Szenarios wird gezeigt, wie FlashCopy in einer HA-Umgebung mit IBM System Storage-Lösungen, wie Metro Mirror oder Global Mirror, verwendet werden kann.

Szenario: Sicherungen in einer Umgebung mit geographischer Spiegelung durchführen:

Dieses Szenario verschafft Ihnen einen Überblick über die Tasks, die bei Durchführung einer Sicherung über Remotezugriff für eine i5/OS-Hochverfügbarkeitslösung mit geographischer Spiegelung erforderlich sind.

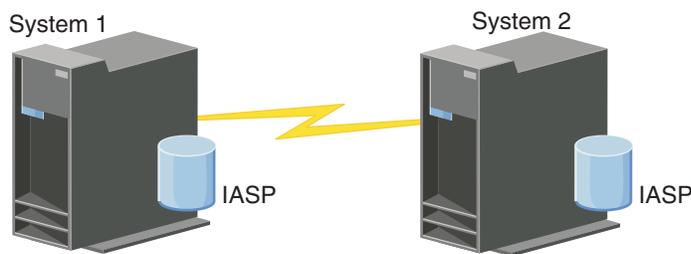
Übersicht

Im vorliegenden Beispiel führt ein Systemadministrator eine Sicherung der in unabhängigen Plattenpools gespeicherten Daten durch, die in einer HA-Lösung auf der Basis der Technologie für geographische Spiegelung eingesetzt werden. Der Administrator möchte vermeiden, dass das Produktionssystem offline geschaltet wird. Stattdessen plant er, die gespiegelte Kopie vorübergehend abzuhängen und anschließend eine Sicherung von der zweiten Kopie der in unabhängigen Plattenpools an einem fernen Standort abgelegten Daten durchzuführen.

Anmerkung: Durch Abhängen der gespiegelten Kopie wird im Prinzip die geographische Spiegelung beendet, bis die Kopie wieder an das Produktionssystem angehängt wird. Während die gespiegelte Kopie abgehängt ist, sind Hochverfügbarkeit und Wiederherstellung nicht aktiv. Wenn das System während dieses Prozesses ausfällt, gehen Daten verloren.

Details

Die folgende Abbildung veranschaulicht diese Umgebung:



Konfigurationsschritte

1. Unabhängigen Plattenpool stilllegen
2. „Spiegelkopie abhängen“ auf Seite 162
3. Plattenpool verfügbar machen
4. Unabhängigen Plattenpool sichern
5. „Unabhängigen Plattenpool wieder aufnehmen“ auf Seite 160
6. „Spiegelkopie wieder anhängen“ auf Seite 163

Szenario: FlashCopy ausführen:

Im vorliegenden Beispiel möchte ein Administrator eine Sicherung von der fernen Kopie der in externen Speichereinheiten am Sicherungsstandort gespeicherten Daten ausführen. Mit der FlashCopy-Funktion, die in IBM Storage Solutions bereitgestellt wird, kann der Administrator seine Sicherungszeit erheblich reduzieren.

Übersicht

Im vorliegenden Beispiel führt ein Systemadministrator eine Sicherung der auf externen IBM System Storage-Speichereinheiten gespeicherten Daten durch. Der Administrator möchte vermeiden, dass das Produktionssystem zur Durchführung der Sicherung offline geschaltet wird. Stattdessen plant der Administrator mit FlashCopy, eine zeitpunktgesteuerte Datenerfassung durchzuführen. Anhand dieser Daten erstellt der Administrator dann eine Datensicherung auf externen Medien. FlashCopy nimmt nur wenige Sekunden in Anspruch, wodurch die für den gesamten Sicherungsprozess erforderliche Zeit erheblich reduziert wird.

Obwohl im vorliegenden Beispiel FlashCopy für Sicherungsoperationen eingesetzt wird, bietet FlashCopy mehrere Nutzungsmöglichkeiten. FlashCopy kann beispielsweise beim Data-Warehousing eingesetzt werden, um die Abfrageworkloads auf Produktionssystemen zu reduzieren, oder zur Verdoppelung der Produktionsdaten, um eine Testumgebung zu erstellen.

Konfigurationsschritte

1. „Unabhängigen Plattenpool stilllegen“ auf Seite 160
2. „FlashCopy-Sitzung konfigurieren“ auf Seite 168
3. FlashCopy auf externen IBM System Storage-Speichereinheiten durchführen. Informationen zur Verwendung von FlashCopy auf IBM System Storage DS6000 finden Sie im IBM System Storage DS6000 Information Center. Informationen zur Verwendung von FlashCopy auf IBM System Storage DS8000 finden Sie im IBM System Storage DS8000 Information Center.
4. „Unabhängigen Plattenpool wieder aufnehmen“ auf Seite 160
5. Plattenpool verfügbar machen

6. Unabhängigen Plattenpool sichern

Szenarios: Betriebssystemupgrades in einer HA-Umgebung ausführen

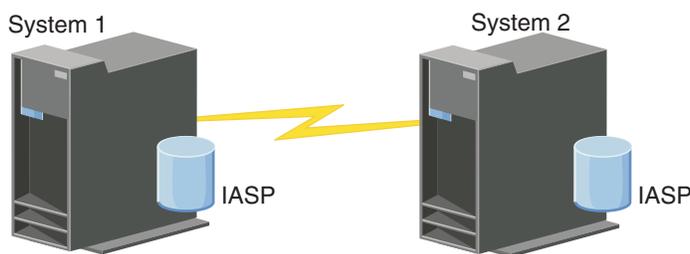
Im vorliegenden Beispiel führt ein Systemadministrator ein Betriebssystemupgrade für zwei i5/OS-Systeme in einer HA-Lösung durch, die auf der Technologie für geographische Spiegelung basieren.

Übersicht

Der Systemadministrator muss ein Betriebssystemupgrade für zwei Systeme in der HA-Umgebung durchführen. Im vorliegenden Beispiel gibt es zwei Knoten: System 1 und System 2. System 1 ist die Produktionskopie und System 2 die Spiegelkopie. Auf beiden Systemen ist i5/OS V5R4 installiert. Der unabhängige Plattenpool ist online, die geographische Spiegelung ist aktiv, und die Systeme sind synchronisiert. Der Systemadministrator möchte für beide Systeme ein Upgrade auf i5/OSV6R1 durchführen.

Details

Die folgende Abbildung veranschaulicht die Umgebung:



Konfigurationsschritte

1. Spiegelkopie abhängen (System 2).
2. CRG beenden (System 2).
3. Knoten stoppen (System 2).
4. Upgrade für System 2 auf das neue Release durchführen. Weitere Informationen finden Sie unter i5/OS und zugehörige Software installieren, löschen oder Upgrade durchführen.
5. IBM System i High Availability Solutions Manager (iHASM), Lizenzprogrammnummer, 5761-HAS, installieren.
6. Auf System 2 Testanwendungen und Plattenpool verfügbar machen. Durch Testen der Anwendungen wird sichergestellt, dass sie auf dem neuen Release wie erwartet funktionieren. Nach Beendigung der Anwendungstests können Sie das Upgrade anhand der folgenden Schritte zu Ende führen.
7. Plattenpool sperren (auf der abgehängten gespiegelten Kopie auf System 2)
8. Gespiegelte Kopie wieder anhängen. Hierdurch wird die Resynchronisation der gespiegelten Daten aufgebaut. Wenn die Resynchronisation abgeschlossen ist, können Sie mit dem Upgradeprozess fortfahren.
9. „Switchover ausführen“ auf Seite 98. Hierdurch wird die gespiegelte Kopie (System 2) zur neuen Produktionskopie, und die Produktionskopie (System 1) wird zur neuen gespiegelten Kopie.

Anmerkung: Die geographische Spiegelung wird unterbrochen, da von V6R1 auf V5R4 keine geographische Spiegelung durchgeführt werden kann. Sie können jedoch eine geographische Spiegelung problemlos von V5R4 auf V6R1 durchführen. Im vorliegenden Szenario wird die geographische Spiegelung nach Beendigung des Switchover unterbrochen. Da jetzt kein gültiges Sicherungssystem mehr vorhanden ist, bleiben die Daten für den Rest der Upgradeprozesses ungeschützt.

10. CRG beenden (System 1).

11. Knoten stoppen (System 1).
12. Upgrade für System 1 auf das neue Release durchführen. Weitere Informationen finden Sie unter i5/OS und zugehörige Software installieren, löschen oder Upgrade durchführen.
13. IBM System i High Availability Solutions Manager (iHASM), Lizenzprogrammnummer, 5761-HAS, installieren.
14. Knoten starten (System 1).
15. CRGs starten (System 1).
16. Spiegeln wieder aufnehmen
17. Switchover durchführen. Hierdurch wird die aktuelle gespiegelte Kopie (System 1) wieder zur Produktionskopie und die Produktionskopie (System 2) zur gespiegelten Kopie. Es handelt sich hierbei um die vor dem Upgrade bestehende Originalkonfiguration.

Beispiel: Betriebssystemupgrade durchführen:

In HA-Umgebungen müssen vor einem Betriebssystemupgrade bestimmte Aktionen durchgeführt werden.

Anhand der folgenden Beispiele können Sie herausfinden, welche Aktionen erforderlich sind, um ein Upgrade in Ihrer Clusterumgebung durchzuführen. Bevor Sie jedoch das Upgrade oder bestimmte Aktionen durchführen, sollten Sie zuerst die aktuelle Version Ihres Clusters herausfinden.

Beispiel 1: Auf dem Knoten, für den ein Upgrade durchgeführt werden soll, ist i5/OS V5R4 installiert. Auf allen anderen Knoten im Cluster ist i5/OS V5R4 oder eine höhere Version installiert. Die aktuelle Clusterversion ist 5.

Aktion: Führen Sie für den Knoten ein Upgrade auf i5/OS V6R1 durch. Starten Sie danach das Clustering auf dem aktualisierten Knoten.

Beispiel 2: Auf dem Knoten, für den ein Upgrade durchgeführt werden soll, ist i5/OS V5R4 installiert. Auf allen anderen Knoten im Cluster ist i5/OS V5R4 installiert. Die aktuelle Clusterversion ist 4.

Aktion: Ändern Sie die aktuelle Clusterversion in 5. Führen Sie für den Knoten ein Upgrade auf i5/OS V6R1 durch. Starten Sie danach das Clustering auf dem aktualisierten Knoten.

Beispiel 3: Auf dem Knoten, für den ein Upgrade durchgeführt werden soll, ist i5/OS V5R3 installiert. Auf allen anderen Knoten im Cluster ist i5/OS V5R4 installiert. Die aktuelle Clusterversion ist 4.

Aktion: Entfernen Sie den Knoten vor dem Upgrade aus dem Cluster. Ändern Sie die aktuelle Clusterversion in 5. Führen Sie für den Knoten ein Upgrade auf i5/OS V6R1 durch, und fügen Sie den Knoten wieder dem Cluster hinzu.

Beispiel 4: Auf dem Knoten, für den ein Upgrade durchgeführt werden soll, ist i5/OS V5R4 installiert. Zurzeit befinden sich nur Knoten mit i5/OS V5R3 und i5/OS V5R4 im Cluster. Die aktuelle Clusterversion ist 4. Es ist wichtiger, dass die Knoten die Version i5/OS V5R3 beibehalten, als ein Upgrade für einen Knoten von i5/OS V5R4 auf i5/OS V6R1 durchzuführen.

Aktionen:

1. Entfernen Sie den Knoten, für den ein Upgrade durchgeführt wird, aus dem Cluster.
2. Führen Sie für den Knoten ein Upgrade auf i5/OS V6R1 durch.
3. Führen Sie für die übrigen Knoten mit i5/OS V5R3 ein Upgrade auf mindestens i5/OS V5R4 durch.
4. Ändern Sie die Clusterversion in 5.
5. Fügen Sie den aktualisierten Knoten wieder dem Cluster hinzu.

Beispiel 5: Auf dem Knoten, für den ein Upgrade durchgeführt werden soll, ist i5/OS V5R4 installiert. Zurzeit befinden sich nur Knoten mit i5/OS V5R3 und i5/OS V5R4 im Cluster. Die aktuelle Clusterversion ist 4. Es ist wichtiger, dass für den Knoten mit i5/OS V5R4 ein Upgrade auf i5/OS V6R1 durchgeführt wird, als V5R3 auf den übrigen Knoten beizubehalten.

Aktionen:

1. Entfernen Sie alle Knoten mit i5/OS V5R3 aus dem Cluster.

2. Ändern Sie die Clusterversion in 5.
3. Führen Sie für den Knoten ein Upgrade auf i5/OS V6R1 durch.
4. Starten Sie den aktualisierten Knoten.
5. Die übrigen Knoten mit i5/OS V5R3 können nach dem Upgrade auf i5/OS V5R4 wieder dem Cluster „Knoten hinzufügen“ auf Seite 100 hinzugefügt werden.

Szenario 6: Auf dem Knoten, für den ein Upgrade durchgeführt werden soll, ist i5/OS V5R3 installiert. Mindestens ein weiterer Knoten im Cluster hat i5/OS V5R3. Die aktuelle Clusterversion ist 3 oder niedriger als 3.

Aktion: Führen Sie für alle Knoten ein Upgrade auf i5/OS V5R4 durch. Ändern Sie die Clusterversion in 4. Führen Sie für alle Knoten ein Upgrade auf i5/OS V6R1 durch.

In der folgenden Tabelle sind die Aktionen aufgeführt, die Sie bei einem Upgrade in einer Clusterumgebung durchführen müssen.

Tabelle 7. Upgrade für Knoten auf i5/OS V6R1 durchführen

Aktuelles Release des Knotens, für den ein Upgrade durchgeführt wird	Aktuelle Clusterversion	Aktionen
V5R4	5	<ol style="list-style-type: none"> 1. Upgrade für den Knoten auf i5/OS V6R1. 2. Den aktualisierten Knoten starten.
V5R4	4	<ol style="list-style-type: none"> 1. Clusterversion in 5 ändern. 2. Upgrade für den Knoten auf i5/OS V6R1. 3. Den aktualisierten Knoten starten. <p>Anmerkung: Wenn auf den anderen Knoten im Cluster i5/OS V5R3 installiert ist, finden Sie Einzelheiten unter Szenarios 4 und 5.</p>
V5R3	4 oder eine niedrigere Version.	<p>Option A</p> <ol style="list-style-type: none"> 1. Den Knoten aus dem Cluster entfernen, für den ein Upgrade erfolgt. 2. Clusterversion in 5 ändern. 3. Upgrade für den Knoten auf V6R1. 4. Knoten dem Cluster wieder hinzufügen. <p>Option B</p> <ol style="list-style-type: none"> 1. Upgrade aller Knoten auf V5R4. 2. Clusterversion in 5 ändern. 3. Upgrade aller Knoten auf V6R1.

Szenario: Einheit hochverfügbar machen

Hochverfügbarkeit kann nicht nur für unabhängige Plattenpools, sondern auch für andere unterstützte Einheiten bereitgestellt werden. Im vorliegenden Beispiel möchte der HA-Administrator Ethernet-Leitungen hochverfügbar machen.

Übersicht

Der Systemadministrator möchte Hochverfügbarkeit für Ethernet-Leitungen in einer HA-Lösung bereitstellen. Die aktuelle Konfiguration bietet Hochverfügbarkeit bei geplanten Betriebsunterbrechungen mit zwei Systemen, auf denen Technologie für umschaltbare Platten eingesetzt wird. Änderungen in der Betriebsumgebung der HA-Lösung werden bei diesem Ansatz mithilfe einer Clusterverwaltungsdomäne verwaltet und synchronisiert. Im Beispiel wird davon ausgegangen, dass die HA-Konfiguration und die Ethernet-Konfiguration vor Durchführung der Schritte erfolgreich durchgeführt wurden. Außerdem wird angenommen, dass die HA-Lösung aktiv ist und alle überwachten Ressourcen innerhalb der HA-Umgebung konsistent sind. Das Beispiel zeigt die Schritte zur Konfiguration der Hochverfügbarkeit von Ethernet-Leitungen.

Konfigurationsschritte

1. „Umschaltbare Einheiten erstellen“ auf Seite 133
2. „Einträge für überwachte Ressourcen hinzufügen“ auf Seite 109
3. „Zu überwachende Attribute auswählen“ auf Seite 144

Cluster verwalten

Zur Clustertechnologie, auf der die i5/OS-Hochverfügbarkeitslösung basiert gehören viele Tasks, die über die grafische Oberfläche der Cluster Resource Services ausgeführt werden können. Diese Tasks unterstützen Sie bei der Verwaltung und Wartung der Cluster.

Im Folgenden sind die Änderungen aufgeführt, die Sie nach der Konfiguration an einem Cluster vornehmen können:

Cluster-Tasks

- Knoten einem Cluster hinzufügen
- Knoten aus einem Cluster entfernen
- Clusterknoten starten
- Clusterknoten beenden
- Clusterversion eines Clusters auf den neuesten Stand bringen
- Cluster löschen
- Clusterknoten ändern

CRG-Tasks

- Neue CRGs erstellen
- Vorhandene CRGs löschen
- CRG starten
- Knoten einer CRG hinzufügen
- Knoten aus einer CRG entfernen
- CRG beenden
- Wiederherstellungsdomäne für eine CRG ändern
- Switchover durchführen
- Knoten einer Einheitendomäne hinzufügen
- Knoten aus einer Einheitendomäne entfernen

Clusterverwaltungsdomäne

- Clusterverwaltungsdomäne erstellen
- Überwachte Ressourcen hinzufügen
- Clusterverwaltungsdomäne löschen

Clusterversion eines Clusters ändern

Die Clusterversion definiert die Stufe, auf der alle Knoten im Cluster aktiv miteinander kommunizieren.

Die Clusterversionssteuerung ist eine Technik, die es dem Cluster ermöglicht, Systeme verschiedener Release-Level aufzunehmen und durch Festlegung der zu verwendenden Ebene des Übertragungsprotokolls uneingeschränkt interagieren zu lassen.

Zum Ändern der Clusterversion müssen alle Knoten im Cluster dieselbe potenzielle Version aufweisen. Die Clusterversion kann anschließend so geändert werden, dass sie der potenziellen Version entspricht. Dadurch wird die Verwendung der neuen Funktion ermöglicht. Die Versionsnummer kann nur um den Wert Eins erhöht werden. Die Versionsnummer kann nicht herabgesetzt werden, ohne dass der Cluster gelöscht und in einer niedrigeren Version erneut erstellt wird. Die aktuelle Clusterversion wird zuerst vom ersten Knoten festgelegt, der im Cluster definiert ist. Knoten, die danach dem Cluster hinzugefügt werden, müssen die aktuelle Clusterversion oder die nächsthöhere Version haben, andernfalls können sie dem Cluster nicht hinzugefügt werden.

- | Wenn für einen Knoten ein Upgrade auf ein neues Release durchgeführt wird, müssen Sie sicherstellen, dass der Knoten die entsprechende Clusterversion hat. Cluster können eine Versionsabweichung von nur einem Release unterstützen. Wenn alle Knoten in einem Cluster dasselbe Releasestand haben, sollten Sie statt einer Änderung der Clusterversion ein Upgrade auf das neue Release durchführen. Dadurch wird sichergestellt, dass alle Funktionen des neuen Release zur Verfügung stehen. Eine ausführliche Beschreibung der Aktionen, die bei einem Upgrade auf ein neues Release durchzuführen sind, finden Sie unter „Szenarios: Betriebssystemupgrades in einer HA-Umgebung ausführen“ auf Seite 120.

Führen Sie die folgenden Anweisungen aus, um die Clusterversion eines Knotens zu überprüfen und zu ändern.

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Clustereigenschaften anzeigen** aus.
- | 5. Klicken Sie auf der Seite "Clustereigenschaften" auf die Registerkarte **Allgemein**.
- | 6. Überprüfen Sie die Einstellung der Clusterversion oder ändern Sie die Version entsprechend.

Zugehörige Konzepte

Clusterversion

Zugehörige Informationen

Clusterversion ändern (CHGCLUVER)

API Adjust Cluster Version (QcstAdjustClusterVersion)

Cluster löschen

Beim Löschen eines Clusters werden alle Cluster Resource Services auf allen aktiven Clustern beendet und aus dem Cluster gelöscht.

- | Ein Cluster muss mindestens einen aktiven Knoten enthalten, um gelöscht werden zu können. Wenn Ihr Cluster umschaltbare Platten oder andere umschaltbare Einheiten enthält, müssen Sie zuerst jeden Knoten aus der Einheitendomäne entfernen, bevor Sie den Cluster löschen. Andernfalls besteht das Risiko, dass Sie die Platten nicht mehr einem anderen Cluster hinzufügen können.

Führen Sie die folgenden Schritte aus, um einen Cluster zu löschen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.

- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Klicken Sie auf der Seite **Cluster Resource Services** auf **Cluster löschen**.
- | 5. Das Bestätigungsfenster **Cluster löschen** wird angezeigt. Wählen Sie **Ja** aus, um den Cluster zu löschen. Nach der Erstellung des Clusters wird auf der Seite **Cluster Resource Services** die Task **Neuer Cluster** angezeigt:

Zugehörige Tasks

„Knoten aus einer Einheitendomäne entfernen“ auf Seite 130

Eine *Einheitendomäne* ist eine Untergruppe von Knoten in einem Cluster, die Einheitenressourcen gemeinsam nutzen.

Zugehörige Informationen

Cluster löschen (DLTCLU)

API Delete Cluster (QcstDeleteCluster)

| **Clusterkonfiguration anzeigen**

| Sie können einen Bericht mit detaillierten Informationen zur Clusterkonfiguration anzeigen. Dieser Bericht enthält Angaben zum Cluster, eine Liste mit der Knotenzugehörigkeit, Konfigurations- und Optimierungsparameter sowie eine Liste der Clusterressourcengruppen im Cluster.

| Führen Sie die folgenden Schritte aus, um eine Clusterkonfiguration anzuzeigen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Konfigurationsdaten anzeigen** aus. Daraufhin erscheint die Anzeige "Clusterkonfiguration und -eigenschaften". Sie können die Seite in einer Datei speichern oder ausdrucken.

Zugehörige Informationen

| Clusterinformationen anzeigen (DSPCLUINF)

Clusterkonfiguration sichern und wiederherstellen

Auch wenn Sie das Clustering auf Ihrem System einsetzen, sollten Sie trotzdem eine Strategie zum Sichern und Wiederherstellen entwickeln, um Ihre Daten zu schützen.

Wenn Sie das Clustering als Sicherungsstrategie nutzen wollen, d. h., wenn Sie möchten, dass ein System läuft, während das andere ausfällt, da es gesichert wird, sollte Ihr Cluster mindestens drei Systeme enthalten. Mit drei Systemen im Cluster können Sie bei einem Ausfall immer auf ein System umschalten.

Clusterressourcengruppen sichern und wiederherstellen

Eine Clusterressourcengruppe kann im aktiven oder im inaktiven Zustand des Clusters gesichert werden. Für die Wiederherstellung einer Clusterressourcengruppe gelten folgende Einschränkungen:

- Wenn der Cluster aktiv ist, die Clusterressourcengruppe aber vom Cluster nicht erkannt wird, kann die Clusterressourcengruppe nicht wiederhergestellt werden.
- Damit eine Clusterressourcengruppe wiederhergestellt werden kann, muss der Knoten für Cluster konfiguriert sein.

Eine Clusterressourcengruppe kann wiederhergestellt werden, wenn der Cluster aktiv ist, die Clusterressourcengruppe vom Cluster nicht erkannt wird, der Knoten sich in der Wiederherstellungsdomäne der Clusterressourcengruppe befindet und der Clustername mit dem in der Clusterressourcengruppe übereinstimmt. Eine Clusterressourcengruppe kann wiederhergestellt werden, wenn der Cluster konfiguriert, aber auf dem Knoten nicht aktiv ist, und sich der Knoten in der Wiederherstellungsdomäne der Clusterressourcengruppe befindet.

Vorbereitung auf einen Störfall

Im Falle einer Störung, muss der Cluster möglicherweise neu konfiguriert werden. Zur Vorbereitung auf ein solches Szenario wird empfohlen, die Clusterkonfigurationsdaten zu speichern und eine Druckausgabe der Angaben auf Papier aufzubewahren.

1. Setzen Sie nach einer Änderung der Clusterkonfiguration den Befehl SAVCFG (Konfiguration sichern) oder den Befehl SAVSYS (System sichern) ab, damit die wiederhergestellten internen Clusterinformationen auf dem aktuellen Stand und mit anderen Knoten im System konsistent sind. Im Abschnitt zum Sichern von Konfigurationsdaten finden Sie Details zur Durchführung einer SAVCFG- oder SAVSYS-Operation.
2. Drucken Sie die Clusterkonfigurationsdaten nach jeder Änderung aus. Rufen Sie dazu die Befehlsanzeige Clusterinformationen anzeigen (DSPCLUINF) auf. Bewahren Sie eine Kopie gemeinsam mit den Sicherungsbändern auf. Im Falle einer Störung, muss möglicherweise der gesamte Cluster neu konfiguriert werden.

Zugehörige Informationen

Konfigurationsdaten sichern

Konfiguration sichern (SAVCFG)

System sichern (SAVSYS)

Clusterinformationen anzeigen (DSPCLUINF)

| Clusterstatus überwachen

| Über die grafische Oberfläche der Cluster Resource Services wird der Clusterstatus überwacht sowie eine Nachricht angezeigt, wenn die in die HA-Lösung eingebundenen Knoten inkonsistent werden.

| Die grafische Oberfläche der Resource Services zeigt Warnung HAI0001W auf der Seite Knoten an, wenn der Cluster inkonsistent ist. Wenn eine solche Nachricht zur Inkonsistenz angezeigt wird, bedeutet dies, dass Informationen von diesem Knoten abgerufen werden, die mit anderen Knoten im Cluster nicht konsistent sind. Knoten werden inkonsistent, wenn Sie im Cluster inaktiv werden.

| Zum Abrufen konsistenter Informationen können Sie entweder auf die Clusterinformationen auf einem aktiven Knoten im Cluster zugreifen oder diesen Knoten starten und dann die Anforderung wiederholen.

| Führen Sie die folgenden Schritte aus, um den Clusterstatus zu überwachen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wenn der Knoten inkonsistent ist, wird auf der Seite "Knoten" die Nachricht HAI0001W angezeigt. Der lokale Clusterknoten ist nicht aktiv. Die Clusterinformationen sind möglicherweise nicht präzise, bevor der lokale Knoten gestartet wird.

| Zugehörige Tasks

| „Knoten starten“ auf Seite 99

| Durch Starten eines Clusterknotens werden das Clustering und die Cluster Resource Services auf einem Knoten in einer i5/OS-Hochverfügbarkeitsumgebung gestartet.

| Zugehörige Informationen

| Clusterinformationen anzeigen (DSPCLUINF)

| CRG-Informationen anzeigen (DSPCRGINF)

| API 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)

| **Nachrichtenwarteschlangen angeben**

| Sie können entweder eine Clusternachrichtenwarteschlange oder eine Failovernachrichtenwarteschlange angeben. Mithilfe dieser Nachrichtenwarteschlangen können Sie die Fehlerursachen in Ihrer i5/OS-Hochverfügbarkeitsumgebung feststellen.

| Eine Clusternachrichtenwarteschlange wird für Nachrichten auf Clusterebene verwendet und gibt eine Nachricht aus, die alle Clusterressourcengruppen (CRGs) bei einem Failover auf einen bestimmten Knoten steuert. Eine Failovernachrichtenwarteschlange wird für Nachrichten auf CRG-Ebene verwendet und stellt jeweils eine Nachricht für jede CRG bereit, für die ein Failover durchgeführt wird.

| **Clusternachrichtenwarteschlange angeben**

| **Anmerkung:** Wenn ein Cluster für die Verwendung einer Clusternachrichtenwarteschlange konfiguriert werden soll, muss diese bei Ausführung des Assistenten zur Erstellung des Clusters angegeben werden.

| Führen Sie die folgenden Schritte aus, um eine Clusternachrichtenwarteschlange anzugeben:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Clustereigenschaften anzeigen**.
- | 5. Klicken Sie auf der Seite "Clustereigenschaften" auf **Clusternachrichtenwarteschlange**.
- | 6. Geben Sie die folgenden Informationen an, um eine Clusternachrichtenwarteschlange zu erstellen:
 - | • Geben Sie im Feld **Name** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, die ein Failover auf Cluster- oder Knotenebene betreffen. Bei Failoveroperationen auf Knotenebene wird eine Nachricht gesendet, die das Failover aller Clusterressourcengruppen mit demselben neuen Primärknoten steuert. Wenn ein Failover für eine einzelne Clusterressourcengruppe durchgeführt wird, wird eine Nachricht gesendet, die das Failover dieser Clusterressourcengruppe steuert. Die Nachricht wird an den neuen Primärknoten gesendet. Ist dieses Feld definiert, muss die angegebene Nachrichtenwarteschlange auf allen Knoten im Cluster vorhanden sein, wenn die Knoten gestartet werden. Die Nachrichtenwarteschlange darf sich nicht in einem unabhängigen Plattenpool befinden.
 - | • Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht `*CURLIB`, `QTEMP`, `*LIBL`, `*USRLIBL`, `*ALL` oder `*ALLUSR` lauten.
 - | • Wählen Sie im Feld **Failoverwartezeit** entweder **Nicht warten** oder **Unbegrenzt warten** aus, oder geben Sie die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Clusternachrichtenwarteschlange erfolgen muss.
 - | • Geben Sie im Feld **Failoverstandardaktion** die Aktion an, die von den Cluster Resource Services durchgeführt werden soll, wenn innerhalb der für das Failover festgelegten Wartezeit keine Antwort auf die Failovernachricht eingegangen ist. Sie können in diesem Feld **Failover fortsetzen** oder **Failover abbrechen** angeben.

| **Failovernachrichtenwarteschlange angeben**

| Führen Sie die folgenden Schritte aus, um eine Failovernachrichtenwarteschlange anzugeben:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.

3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Wählen Sie in der Liste der Clusterressourcengruppen die Clusterressourcengruppe aus, mit der Sie arbeiten möchten.
6. Klicken Sie auf der Registerkarte "Clusterressourcengruppe" auf das Menü **Aktion auswählen**, und wählen Sie **Eigenschaften** aus.
7. Geben Sie auf der Seite "Allgemein" die folgenden Werte für die Failovernachrichtenwarteschlange an:
 - Geben Sie im Feld **Failovernachrichtenwarteschlange** den Namen der Nachrichtenwarteschlange an, die Nachrichten empfangen soll, wenn ein Failover für diese Clusterressourcengruppe durchgeführt wird. Wenn dieses Feld definiert ist, muss die angegebene Nachrichtenwarteschlange nach Beendigung des Exitprogramms auf allen Knoten der Wiederherstellungsdomäne vorhanden sein. Die Failovernachrichtenwarteschlange darf sich nicht in einem unabhängigen Plattenpool befinden.
 - Geben Sie im Feld **Bibliothek** den Namen der Bibliothek an, die die Nachrichtenwarteschlange für die Failovernachrichten enthält. Der Bibliotheksname darf nicht *CURLIB, QTEMP oder *LIBL lauten.
 - Geben Sie im Feld **Failoverwartezeit** die Wartezeit (in Minuten) an, innerhalb der eine Antwort auf die Failovernachricht in der Failovernachrichtenwarteschlange erfolgen muss. Sie können auch die Aktion angeben, die von den Cluster Resource Services durchgeführt werden soll, wenn innerhalb der für das Failover festgelegten Wartezeit keine Antwort auf die Failovernachricht eingegangen ist.

Prüfliste zur Aufhebung der Konfiguration

Verschiedene Clusterkomponenten müssen systematisch entfernt werden, um sicherzustellen, dass die Konfiguration des Clusters vollständig aufgehoben ist.

Tabelle 8. Prüfliste für Cluster zur Aufhebung der Konfiguration von unabhängigen Plattenpools.

Anforderungen für unabhängige Plattenpools	
—	Wenn Sie umschaltbare Plattenpools benutzen, sollten Sie den Tower auf den Knoten umschalten, der SPCN-Eigner (SPCN = System Power Control Network, Netz für Stromversorgungskontrolle des Systems) ist, bevor Sie die Konfiguration der Clusterressourcengruppe aufheben. Sie können die API QcstInitiateSwitchOver (Initiate Switchover) oder den Befehl CHGCRGPRI (CRG-Primärknoten ändern) verwenden, um die CRG wieder zurück an den SPCN-Eigner zu übertragen. Erst wenn dieser Schritt ausgeführt wurde, sind Sie in der Lage, den Tower für das System als persönlich zu markieren.
—	Wenn Sie einen Teil einer unabhängigen Plattenpoolgruppe oder den letzten unabhängigen Plattenpool in der Gruppe der umschaltbaren Einheiten entfernen möchten, müssen Sie zuerst die CRG beenden. Verwenden Sie hierzu den Befehl ENDCRG (CRG beenden).
—	Wenn Sie einen unabhängigen Plattenpool entfernen möchten, der Teil eines Clusters ist, wird empfohlen, dass Sie zuerst die Clusterressourcengruppe (CRG) löschen. Nähere Informationen finden Sie unter „Clusterressourcengruppe löschen“ auf Seite 133. Sie können das Konfigurationsobjekt des unabhängigen Plattenpools auch mit dem Befehl RMVCRGDEVE (CRG-Einheiteneintrag entfernen) aus der CRG entfernen.
—	Nachdem das Konfigurationsobjekt des unabhängigen Plattenpools aus der umschaltbaren Clustereinheit entfernt wurde, können Sie einen unabhängigen Plattenpool löschen.
—	Löschen Sie die Einheitenbeschreibung für einen unabhängigen Plattenpool, indem Sie die folgenden Tasks ausführen: <ol style="list-style-type: none"> 1. Geben Sie in der Befehlszeilenschnittstelle WRKDEVD DEVD(*ASP) ein, und drücken Sie die Eingabetaste. 2. Blättern Sie vor, bis die Einheitenbeschreibung für den unabhängigen Plattenpool, den Sie löschen möchten, angezeigt wird. 3. Wählen Sie Option 4 (Löschen) nach dem Namen der Einheitenbeschreibung aus, und drücken Sie die Eingabetaste.

Tabelle 9. Prüfliste für Cluster zur Aufhebung der Konfiguration von Clustern

Anforderungen für Clusterressourcengruppen	
—	<p>Führen Sie einen der folgenden Schritte aus, um die Clusterressourcengruppe zu löschen:</p> <ol style="list-style-type: none"> 1. Wenn auf dem Knoten das Clustering nicht aktiv ist, geben Sie DLTCRG CRG(CRGNAME) in der Befehlszeilenschnittstelle ein. CRGNAME ist der Name der CRG, die gelöscht werden soll. Drücken Sie die Eingabetaste. 2. Wenn auf dem Knoten das Clustering aktiv ist, geben Sie DLTCRGCLU CLUSTER(CLUSTERNAME) in der Befehlszeilenschnittstelle ein. CLUSTERNAME ist der Name des Clusters. CRGNAME ist der Name der CRG, die gelöscht werden soll. Drücken Sie die Eingabetaste.

Knoten verwalten

Systeme und logische Partitionen, die Teil einer HA-Umgebung unter i5/OS sind, werden als Knoten bezeichnet. Sie können mit Knoten verschiedene Verwaltungstasks ausführen:

Knoteneigenschaften anzeigen:

Über die grafische Oberfläche der Cluster Resource Services können die Eigenschaften für Knoten, die als Teil Ihrer HA-Umgebung konfiguriert wurden, angezeigt und verwaltet werden.

Führen Sie die folgenden Schritte aus, um die Knoteneigenschaften anzuzeigen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Klicken Sie auf der Registerkarte **Knoten** auf das Menü **Aktion auswählen**, und wählen Sie die **Eigenschaften** aus. Klicken Sie auf **Start**. Daraufhin erscheint die Anzeige "Knoteneigenschaften".
 - Auf der Seite "Allgemein" werden der Name und die System-IP-Adresse des Knotens angezeigt.
 - Auf der Seite "Clustering" werden die folgenden Informationen angezeigt:
 - Die Kommunikation zwischen den Knoten in einem Cluster erfolgt über die IP-Adressen der Clusterschnittstelle.
 - Die potenzielle Knotenversion gibt die Version und Modifikationsstufe an, auf der die Knoten im Cluster aktiv miteinander kommunizieren.
 - Die Einheitendomänen werden aufgelistet, die im ausgewählten Cluster konfiguriert sind. Wenn Sie eine Einheitendomäne in der Liste auswählen, werden die Knoten, die zur ausgewählten Einheitendomäne gehören, ebenfalls aufgelistet.

Knoten stoppen:

Durch Stoppen oder Beenden eines Knotens werden Clustering und Cluster Resource Services auf dem betreffenden Knoten gestoppt.

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Registerkarte **Knoten** den Knoten aus, den Sie stoppen möchten.
5. Klicken Sie im Menü **Aktion auswählen** auf **Stoppen**. Bei erfolgreichem Stoppen der Cluster Resource Services auf dem angegebenen Knoten wird der Status des Knotens auf "Gestoppt" gesetzt.

Zugehörige Informationen

Clusterknoten beenden (ENDCLUNOD)
API End Cluster Node (QcstEndClusterNode)

Knoten entfernen:

Wenn Sie ein Upgrade für einen bestimmten Knoten ausführen oder ein Knoten in der HA-Umgebung unter i5/OS nicht mehr benötigt wird, müssen Sie den Knoten aus dem Cluster entfernen.

Führen Sie die folgenden Schritte aus, um einen Knoten aus einem vorhandenen Cluster zu entfernen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Wählen Sie auf der Seite "Knoten" das Menü **Aktion auswählen** und abschließend den Eintrag **Entfernen** aus.
6. Klicken Sie in der Bestätigungsanzeige "Clusterknoten entfernen" auf **Ja**.

Zugehörige Tasks

„Geographische Spiegelung dekonfigurieren“ auf Seite 164

Wenn Sie die Funktion der geographischen Spiegelung nicht mehr für einen bestimmten Plattenpool oder ein Plattenpoolgruppe verwenden möchten, können Sie **Geographische Spiegelung dekonfigurieren** auswählen. Durch das Dekonfigurieren der geographischen Spiegelung wird die geographische Spiegelung vom System gestoppt und die Spiegelkopie der Plattenpools auf den Knoten am Standort der Spiegelkopie gelöscht.

Zugehörige Informationen

CRG-Knoteneintrag entfernen (RMVCLUNODE)

API Remove Cluster Node Entry (QcstRemoveClusterNodeEntry)

Knoten aus einer Einheitendomäne entfernen:

Eine *Einheitendomäne* ist eine Untergruppe von Knoten in einem Cluster, die Einheitenressourcen gemeinsam nutzen.

Wichtig:

Gehen Sie bitte mit äußerster Umsicht vor, wenn Sie einen Knoten aus einem Cluster entfernen. Wird ein Knoten aus einer Einheitendomäne entfernt und ist dieser Knoten zurzeit der primäre Eingangspunkt für unabhängige Plattenpools, dann werden diese unabhängigen Plattenpools mit dem Knoten entfernt. D. h., von den übrigen Knoten in der Einheitendomäne kann nicht mehr auf die unabhängigen Plattenpools zugegriffen werden.

Nachdem ein Knoten aus einer Einheitendomäne entfernt wurde, kann er nicht mehr in dieselbe Einheitendomäne eingefügt werden, wenn mindestens noch ein bereits vorhandener Clusterknoten zur selben Einheitendomäne gehört. Führen Sie die folgenden Schritte aus, um den Knoten der Einheitendomäne wieder hinzuzufügen:

1. Löschen Sie die unabhängigen Plattenpools, deren Eigner derzeit der Knoten ist, der der Domäne hinzugefügt werden soll.
2. Starten Sie das System erneut, indem Sie ein IPL auf dem Knoten durchführen.
3. Fügen Sie den Knoten der Einheitendomäne hinzu.
4. Erstellen Sie den unabhängigen Plattenpool, der in Schritt 1 gelöscht wurde, neu.

Führen Sie die folgenden Schritte aus, um einen Knoten aus einer Einheitendomäne zu entfernen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Wählen Sie auf der Registerkarte **Knoten** das Menü **Aktion auswählen** aus, und wählen Sie **Eigenschaften** aus. Klicken Sie auf **Start**. Die Seite "Knoteneigenschaften" wird angezeigt.
6. Löschen Sie auf der Registerkarte **Clustering** den Knotennamen im Feld **Einheitendomäne**, und klicken Sie dann auf **OK**.

Zugehörige Tasks

„Cluster löschen“ auf Seite 124

Beim Löschen eines Clusters werden alle Cluster Resource Services auf allen aktiven Clustern beendet und aus dem Cluster gelöscht.

Zugehörige Informationen

Einheitendomäneneintrag entfernen (RMVDEVDMNE)

API Remove Device Domain Entry (QcstRemoveDeviceDomainEntry)

Clusterressourcengruppen verwalten

Clusterressourcengruppen (CRGs) verwalten Ressourcen innerhalb einer ausfallsicheren HA-Umgebung unter i5/OS. Sie stellen eine Clustertechnologie dar, die das Umschalten von Ressourcen auf Sicherungssysteme für den Fall einer Betriebsunterbrechung definiert und steuert.

CRG-Status anzeigen:

In einer HA-Umgebung kann der CRG-Status überwacht werden. Anhand der Statusnachrichten können Sie die in der CRG vorgenommenen Änderungen validieren oder Probleme innerhalb der CRG feststellen.

Führen Sie die folgenden Schritte aus, um den CRG-Status anzuzeigen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Auf der Seite "Clusterressourcengruppe" wird der aktuelle Status einer CRG in der Spalte "Status" angezeigt.

Im Folgenden sehen Sie die für Clusterressourcengruppe möglichen Statuswerte:

Tabelle 10. Statuswerte für CRGs

Gültige Werte	Beschreibung
Gestartet	Die CRG wurde gestartet.
Gestoppt	Die CRG wurde gestoppt.
Unbestätigt	Die Informationen zu dieser CRG innerhalb der HA-Lösung sind möglicherweise ungenau. Dieser Status tritt ein, wenn das CRG-Exitprogramm mit der Aktion zum Rückgängigmachen einer Operation aufgerufen und nicht beendet werden kann.

Table 10. Statuswerte für CRGs (Forts.)

Gültige Werte	Beschreibung
Wiederhergestellt	Die CRG wurde auf ihrem Knoten wiederhergestellt und nicht auf andere Knoten im Cluster kopiert. Wenn das Clustering auf dem Knoten gestartet wird, wird die CRG mit anderen Knoten im Cluster synchronisiert, und ihr Status wird auf "Inaktiv" gesetzt.
Inaktiv	Cluster Resource Services für diese CRG sind auf dem Knoten nicht aktiv. Mögliche Ursachen: Knotenfehler, der Knoten wurde beendet, CRG-Job auf dem Knoten läuft möglicherweise nicht.
Löschen	Die CRG wird gerade aus dem Cluster gelöscht.
Wird geändert	Die CRG wird gerade geändert. Die CRG wird auf den vorherigen Status zurückgesetzt, wenn die Änderung durchgeführt wurde.
Wird gestoppt	Die CRG wird gerade gestoppt.
Wird hinzugefügt	Die CRG wird gerade dem Cluster hinzugefügt.
Wird gestartet	Die CRG wird gerade gestartet.
Wird umgeschaltet	Die CRG wird gerade auf einen anderen Knoten umgeschaltet.
Knoten wird hinzugefügt	Es wird gerade ein neuer Knoten dem Cluster hinzugefügt. Die CRG wird auf den vorherigen Status zurückgesetzt, wenn der Knoten erfolgreich hinzugefügt wurde.
Knoten wird entfernt	Ein Knoten wird gerade aus der CRG entfernt. Die CRG wird auf den vorherigen Status zurückgesetzt, wenn der Knoten erfolgreich entfernt wurde.
Knotenstatus wird geändert	Der Status eines Knotens in der Wiederherstellungsdomäne für eine Clusterressourcengruppe wird gerade geändert.

CRG stoppen:

Clusterressourcengruppen (CRGs) verwalten Ressourcen innerhalb einer ausfallsicheren HA-Umgebung unter i5/OS. Sie stellen eine Clustertechnologie dar, die das Umschalten ausfallsicherer Ressourcen auf Sicherungssysteme für den Fall einer Betriebsunterbrechung definiert und steuert.

Eine Clusterressourcengruppe wird z. B. gestoppt, um eine automatische Failoverfunktion in Ihrer HA-Umgebung zu beenden. Sie können hierzu ein IPL auf einem der in der Clusterressourcengruppe definierten Systeme durchführen.

Führen Sie die folgenden Schritte aus, um eine Clusterressourcengruppe zu stoppen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Wählen Sie auf der Seite "Clusterressourcengruppe" die Clusterressourcengruppe aus, die gestoppt werden soll.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Stoppen** und anschließend **Start** aus.

Zugehörige Informationen

- | CRG beenden (ENDCRG)
- | API End Cluster Resource Group (QcstEndClusterResourceGroup)

Clusterressourcengruppe löschen:

Über die grafische Oberfläche des Cluster Resource Service Manager kann Clusterressourcengruppe gelöscht werden.

Führen Sie die folgenden Schritte aus, um eine Clusterressourcengruppe zu löschen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Wählen Sie auf der Seite "Clusterressourcengruppe" die Clusterressourcengruppe aus, die gelöscht werden soll.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Löschen** aus, und klicken Sie anschließend auf **Start**.
7. Wählen Sie in der Bestätigungsanzeige "Clusterressourcengruppe löschen" **Ja** aus.

Zugehörige Informationen

CRG aus Cluster löschen (DLTCRGCLU)

API Delete Cluster Resource Group (QcstDeleteClusterResourceGroup)

Umschaltbare Einheiten erstellen:

Hochverfügbarkeit wird nicht nur bei unabhängigen Plattenpool, sondern auch für verschiedene andere Einheiten unterstützt. Einheiten wie Ethernet-Leitungen, optische Einheiten, Netzwerkserver usw. können jetzt auch in eine HA-Lösung einbezogen werden.

Eine Einheiten-Clusterressourcengruppe (CRG) enthält eine Liste mit umschaltbaren Einheiten. Jede Einheit in der Liste gibt einen umschaltbaren unabhängigen Plattenpool oder eine andere Art einer umschaltbaren Einheit an, z. B. Bandeneinheiten, Leitungsbeschreibungen, Steuereinheiten und Netzwerkserver. Bei einem Ausfall werden alle diese Einheiten auf den Ausweichknoten umgeschaltet. Sie können die Einheiten auch während des Switchover- oder Failoverprozesses anhängen.

Führen Sie die folgenden Schritte aus, um eine umschaltbare Einheit zu erstellen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
5. Klicken Sie auf der Seite "Clusterressourcengruppen" auf das Kontextsymbol neben der Einheiten-CRG, für die Sie eine vorhandene umschaltbare Einheit hinzufügen möchten, und wählen Sie dann **Vorhandene Einheit hinzufügen** aus dem Kontextmenü aus.
6. Klicken Sie in der Liste "Umschaltbare Einheit hinzufügen" auf **Hinzufügen**.
7. Geben Sie im Fenster "Umschaltbare Einheit hinzufügen" die Konfigurationsobjektart und den Objektnamen der umschaltbaren Einheit an. Klicken Sie dann auf **OK**, um die neue umschaltbare Einheit zur Liste hinzuzufügen. Wenn Sie beispielsweise eine umschaltbare Ethernet-Leitung hinzufügen möchten, wählen Sie Ethernet-Leitung in der Liste aus.

- | 8. Klicken Sie im Listenfenster auf **OK**, um die neue Einheit zur Einheiten-CRG hinzuzufügen.

Wiederherstellungsdomäne für eine Clusterressourcengruppe ändern:

Die Wiederherstellungsdomäne steuert Wiederherstellungsaktionen für eine Untergruppe von Knoten, die in einer Clusterressourcengruppe definiert sind.

- | Führen Sie die folgenden Schritte aus, um eine Wiederherstellungsdomäne für eine Einheiten-, Anwendungs- oder Daten-Clusterressourcengruppe zu ändern:
 - | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
 - | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
 - | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
 - | 4. Wählen Sie auf der Seite "Cluster Resource Services" die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
 - | 5. Wählen Sie auf der Seite "Clusterressourcengruppe" die CRG aus, die geändert werden soll.
 - | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** und anschließend **Start** aus.
 - | 7. Klicken Sie auf die Seite "Wiederherstellungsdomäne", um die bestehenden Werte für die Wiederherstellungsdomäne zu ändern. Auf dieser Seite können Sie die Rolle eines Knotens innerhalb der Wiederherstellungsdomäne ändern sowie einen Knoten zur Wiederherstellungsdomäne hinzufügen oder aus dieser entfernen. Bei Einheiten-Clusterressourcengruppen können der Standortname und die IP-Adresse des Datenports eines Knotens innerhalb der Wiederherstellungsdomäne ebenfalls geändert werden.

Zugehörige Informationen

CRG-Knoteneintrag hinzufügen (ADDCRGNODE)

CRG ändern (CHGCRG)

CRG-Knoteneintrag entfernen (RMVCRGNODE)

API Add a Node to Recovery Domain (QcstAddNodeToRcvyDomain)

API Change Cluster Resource Group (QcstChangeClusterResourceGroup)

API Remove Node from Recovery Domain (QcstRemoveNodeFromRcvyDomain)

- | *Standortnamen und IP-Adressen des Datenports erstellen:*

- | Wenn Sie die geographische Spiegelung verwenden, müssen die in der Wiederherstellungsdomäne der Einheiten-CRG definierten Knoten eine IP-Adresse des Datenports und einen Standortnamen haben.

- | Der Standortname ist einem Knoten in der Wiederherstellungsdomäne für eine Einheiten-Clusterressourcengruppe zugeordnet und gilt nur für die geographische Spiegelung. Bei der Konfiguration einer HA-Umgebung für die geographische Spiegelung muss jedem Knoten an verschiedenen Standorten ein anderer Standortname zugeordnet werden.

- | Führen Sie die folgenden Schritte aus, um die IP-Adresse des Datenports und die Standortnamen für einen Knoten in der Wiederherstellungsdomäne zu erstellen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Klicken Sie auf der Seite "Cluster Resource Services" auf die Task **Mit Clusterressourcengruppen arbeiten**, um eine Liste der im Cluster befindlichen Clusterressourcengruppen anzuzeigen.
- | 5. Klicken Sie auf der Registerkarte "Clusterressourcengruppen" auf das Kontextsymbol neben der Einheiten-Clusterressourcengruppe, und wählen Sie dann **Eigenschaften** aus.

- | 6. Wählen Sie auf der Seite Wiederherstellungsdomäne den Eintrag **Bearbeiten** aus.
- | 7. Möchten Sie eine vorhandene IP-Adresse des Datenports verwenden, wählen Sie sie aus der Liste aus, und klicken Sie auf **OK**. Klicken Sie auf **Hinzufügen**, um eine neue IP-Adresse des Datenports in die Liste aufzunehmen. Geben Sie im Fenster " IP-Adresse des Datenports" die IP-Adresse ein.
- | 8. In der Anzeige "Bearbeiten" können Sie den Standortnamen angeben.

Failover bei Ausfallereignissen verwalten

Normalerweise ist ein Failover das Ergebnis eines Knotenausfalls, aber es können auch noch andere Ursachen zu einem Failover führen. Verschiedene System- oder Benutzeraktionen können Failoversituationen verursachen.

Ein Problem kann sich unter Umständen nur auf eine einzige Clusterressourcengruppe (CRG) auswirken und für diese ein Failover auslösen, nicht jedoch für andere CRGs.

- | Innerhalb eines Clusters sind vier Kategorien an Ausfällen möglich. Einige dieser Ereignisse sind echte Failoversituationen, bei denen ein Ausfall am Knoten eintritt, während in anderen Fällen zuerst untersucht werden muss, wodurch der Fehler verursacht wurde, um dann die entsprechende Fehlerbehebungsmaßnahme einzuleiten. In den folgenden Tabellen werden die einzelnen Ausfallkategorien, die Arten der Ausfallereignisse, die in eine Kategorie fallen, sowie die entsprechenden Fehlerbehebungsmaßnahmen beschrieben.

Ausfälle der Kategorie 1: Durch Knotenausfall verursachtes Failover

- | Wenn ein Failover auf Knotenebene erfolgt, geschieht Folgendes:
 - | • Für jede Clusterressourcengruppe wird der Primärknoten als *inaktiv* markiert und als letzter Ausweichknoten definiert.
 - | • Der bis dahin erste Ausweichknoten wird zum Primärknoten.
- | Failover erfolgen in der nachstehenden Reihenfolge:
 - | 1. Alle Einheiten-CRGs
 - | 2. Alle Daten-CRGs
 - | 3. Alle Anwendungs-CRGs

Hinweise:

- | 1. Wenn bei einem Failover für eine Clusterressourcengruppe festgestellt wird, dass keiner der Ausweichknoten aktiv ist, wird der Status der Clusterressourcengruppe auf *Unbestätigt* gesetzt, und die CRG-Wiederherstellungsdomäne bleibt unverändert.
- | 2. Wenn alle Cluster Resource Services fehlschlagen, wird für alle von den Cluster Resource Services verwalteten Ressourcen (CRGs) ein Failover durchgeführt.

Tabelle 11. Ausfälle der Kategorie 1: Durch Knotenausfall verursachtes Failover

Failover bei Ausfallereignis
Befehl ENDTCP (*IMMED oder *CNTRLD mit Zeitlimit) wird ausgegeben.
Befehl ENDSYS (*IMMED oder *CNTRLD) wird ausgegeben.
Befehl PWRDWNYS (*IMMED oder *CNTRLD) wird ausgegeben.
Knopf für IPL (einleitendes Programmladen) wird gedrückt, während die Cluster Resource Services im System aktiv sind.
In der CRG-Wiederherstellungsdomäne wird "Clusterknoten beenden" (API oder Befehl) auf dem Primärknoten aufgerufen.
In der CRG-Wiederherstellungsdomäne wird "Clusterknoten entfernen" (API oder Befehl) auf dem Primärknoten aufgerufen.
Verzögertes Ausschalten der Partition über HMC oder Ausgabe der Konsoloption 7.

Tabelle 11. Ausfälle der Kategorie 1: Durch Knotenausfall verursachtes Failover (Forts.)

Failover bei Ausfallereignis
ENDSBS QSYSWRK(*IMMED oder *CNTRLD) wird ausgegeben.
Befehl zum Abbrechen des Jobs (*IMMED oder *CNTRLD mit Zeitlimit) wird durch den Job QCSTCTL ausgegeben.
Befehl zum Abbrechen des Jobs (*IMMED oder *CNTRLD mit Zeitlimit) wird durch den Job QCSTCRGM ausgegeben.

Ausfälle der Kategorie 2: Durch Knotenausfall verursachte Partitionierung

Die Ausfälle verursachen folgende Ereignisse:

- Der Status der Knoten, die nicht über Clusternachrichtenübertragung kommunizieren, wird auf "Partition" gesetzt. Weitere Informationen zu Partitionen finden Sie unter Clusterpartition.
- Alle Knoten in der Clusterpartition, die den Primärknoten nicht als Mitglied enthalten, führen zur Beendigung der Clusterressourcengruppe.

Hinweise:

1. Wenn der Primärknoten vollständig ausgefallen ist, der Ausfall aber lediglich als Partitionsproblem erkannt wurde, verlieren Sie alle Daten- und Anwendungsservices auf dem betreffenden Knoten, auf dem kein automatisches Failover gestartet wird.
2. Sie müssen den Knoten entweder als "Ausgefallen" deklarieren oder wieder aktivieren und das Clustering auf dem betreffenden Knoten neu starten. Weitere Informationen finden Sie unter Status partitionierter Knoten in "Ausgefallen" ändern.

Tabelle 12. Ausfälle der Kategorie 2: Durch Knotenausfall verursachte Partitionierung

Failover bei Ausfallereignis
CEC-Hardwareausfall (z. B. CPU) tritt ein.
Maschinenfehler bei Betriebssystemsoftware tritt ein.
Sofortiges Ausschalten über HMC oder Ausgabe der Konsoloption 8.
Neustart der Partition über HMC oder Ausgabe der Konsoloption 3.
Spannungsverlust bei CEC (Central Electronic Complex) tritt ein.

Ausfälle der Kategorie 3: Durch CRG-Fehler verursachtes Failover

Wenn ein Fehler in einer Clusterressourcengruppe ein Failover verursacht, geschieht Folgendes:

- Wenn nur eine einzige Clusterressourcengruppe von dem Ausfall betroffen ist, wird das Failover auf der Basis dieser einen Clusterressourcengruppe ausgeführt, da Clusterressourcengruppen unabhängig voneinander sind.
- Wenn mehrere Clusterressourcenjobs abgebrochen werden und mehrere Clusterressourcengruppen gleichzeitig davon betroffen sind, findet kein koordiniertes Failover zwischen den Clusterressourcengruppen statt.
- Der Primärknoten wird in jeder Clusterressourcengruppe als inaktiv markiert und als letzter Ausweichknoten innerhalb der CRG bestimmt.
- Der bis dahin erste Ausweichknoten wird zum neuen Primärknoten.
- Wenn kein aktiver Ausweichknoten vorhanden ist, wird der Status der Clusterressourcengruppe auf "Unbestätigt" gesetzt, und die Wiederherstellungsdomäne bleibt unverändert.

Tabelle 13. Ausfälle der Kategorie 3: Durch CRG-Fehler verursachtes Failover

Failover bei Ausfallereignis
Im CRG-Job ist ein Fehler aufgetreten, der zu seiner abnormalen Beendigung führt.
Fehler in Anwendungsexitprogramm einer Anwendungs-CRG.

Ausfälle der Kategorie 4: Durch Kommunikationsausfall verursachte Partitionierung

Diese Kategorie gleicht der Kategorie 2. Die folgenden Ereignisse treten ein:

- Die Knoten, die nicht über Clusternachrichtenübertragung kommunizieren, werden auf den Status "Partition" gesetzt. Weitere Informationen zu Partitionen finden Sie unter Clusterpartition.
- Alle Knoten sowie die Cluster Resource Services auf den Knoten sind immer noch aktiv, aber es können nicht alle Knoten miteinander kommunizieren.
- Der Cluster ist partitioniert, aber jeder Primärknoten einer Clusterressourcengruppe stellt noch Service bereit.

Die normale Wiederherstellung für den Status "Partition" besteht in der Behebung des Kommunikationsproblems, das die Clusterpartitionierung verursacht hat. Anschließend wird der Cluster den Status "Partition2" ohne weiteren Eingriff lösen.

Anmerkung: Wenn für die Clusterressourcengruppen ein Failover auf einen neuen Primärknoten erfolgen soll, muss sichergestellt werden, dass der alte Primärknoten auf keine der Ressourcen zugreift, bevor der Knoten als "Ausgefallen" markiert wird. Weitere Informationen finden Sie unter Status partitionierter Knoten in "Ausgefallen" ändern.

Tabelle 14. Ausfälle der Kategorie 4: Durch Kommunikationsausfall verursachte Partitionierung

Failover bei Ausfallereignis
Kommunikationsadapter-, Leitungs- oder Routerfehler bei Cluster-Heartbeat-IP-Adressleitungen tritt auf.
Der Befehl ENDTCPIFC wirkt sich auf alle Cluster-Heartbeat-IP-Adressen auf einem Clusterknoten aus.

Ausfallzeiten mit aktiven Clusterressourcengruppen

- Wenn die Clusterressourcengruppe aktiv ist und der ausgefallene Knoten *nicht* der Primärknoten ist, ergibt sich Folgendes:
 - Das Failover aktualisiert den Status des ausgefallenen Wiederherstellungsdomänenmitglieds in der Wiederherstellungsdomäne der Clusterressourcengruppe.
 - Wenn der ausgefallene Knoten ein Ausweichknoten ist, wird die Liste der Ausweichknoten erneut sortiert, so dass die Liste mit den aktiven Knoten beginnt.
- Wenn die Clusterressourcengruppe aktiv ist und das Mitglied in der Wiederherstellungsdomäne der Primärknoten ist, dann sind die vom System ausgeführten Aktionen davon abhängig, welche Art von Ausfall erfolgt ist.
 - Ausfälle der Kategorie 1: Durch Knotenausfall verursachtes Failover
 - Ausfälle der Kategorie 2: Durch Knotenausfall verursachte Partitionierung
 - Ausfälle der Kategorie 3: Durch CRG-Fehler verursachtes Failover
 - Ausfälle der Kategorie 4: Durch Kommunikationsausfall verursachte Partitionierung

Ausfallzeiten mit inaktiven Clusterressourcengruppen

Wenn Clusterressourcengruppen ausfallen, geschieht Folgendes:

- Der Status des ausgefallenen Knotens als Mitglied in der Wiederherstellungsdomäne der Clusterressourcengruppe wird entweder in "Inaktiv" oder "Partition" geändert.
- Die Knotenrollen ändern sich nicht, und die Ausweichknoten werden nicht automatisch neu sortiert.

- In einer inaktiven Clusterressourcengruppe werden die Ausweichknoten neu sortiert, wenn der Befehl STRCRG (CRG starten) abgesetzt oder die API QcstStartClusterResourceGroup (Start Cluster Resource Group) aufgerufen wird.

Anmerkung: Wenn der Primärknoten nicht aktiv ist, wird die API Start Cluster Resource Group fehlgeschlagen. Sie müssen den Befehl CHGCRG (CRG ändern) ausgeben oder die API QcstChangeClusterResourceGroup (Cluster Resource Group) aufrufen, um einen aktiven Knoten als Primärknoten zu bestimmen, und anschließend die API Start Cluster Resource Group erneut aufrufen.

Clusterverwaltungsdomänen verwalten

Nachdem eine Clusterverwaltungsdomäne erstellt und die entsprechenden Einträge für überwachte Ressourcen (MREs) hinzugefügt wurden, sollte der Clusteradministrator die Aktivitäten in der Clusterverwaltungsdomäne überwachen, um sicherzustellen, dass die überwachten Ressourcen konsistent bleiben. Eine Clusterverwaltungsdomäne kann über die grafische Oberfläche der Cluster Resource Services verwaltet und überwacht werden.

Die grafische Oberfläche bietet die Möglichkeit, die MREs zusammen mit dem globalen Status jeder Ressource aufzulisten. Durch Auswahl eines MREs können ausführliche Informationen dazu angezeigt werden. Diese Informationen umfassen den globalen Wert für jedes dem MRE zugeordnete Attribut sowie eine Angabe darüber, ob das Attribut mit der Domäne konsistent ist oder nicht. Wenn der globale Status einer überwachten Ressource inkonsistent ist, sollte der Administrator die erforderlichen Maßnahmen ergreifen, um festzustellen, weshalb die Ressource inkonsistent ist, das Problem beheben und die Ressource resynchronisieren.

Ist der inkonsistente Zustand der Ressource darauf zurückzuführen, dass ein Update auf einem oder mehreren Knoten fehlgeschlagen ist, können Sie die Fehlerursache eventuell anhand der für den MRE aufgezeichneten Information feststellen. Auf dem Knoten, auf dem der Fehler aufgetreten ist, wird eine Nachricht zur Ursache für die fehlgeschlagene Aktualisierung gemeinsam mit dem MRE aufgezeichnet. Auf anderen Knoten wird eine Informationsnachricht intern protokolliert, aus der hervorgeht, dass ein Fehler aufgetreten ist. Die Nachricht enthält auch eine Liste der Knoten, auf denen der Fehler aufgetreten ist. Diese Nachrichten stehen über die grafische Oberfläche der Cluster Resource Services oder nach Aufruf der API QfpadRtvMonitoredResourceInfo (Retrieve Monitored Resource Information) zur Verfügung. Fehlernachrichten werden auch im Jobprotokoll des Peer-CRG-Jobs aufgezeichnet.

Nachdem die Ursache der Inkonsistenz festgestellt wurde, kann die Ressource resynchronisiert werden, entweder durch eine Aktualisierung auf dem Knoten, auf dem der Fehler aufgetreten ist, oder durch Beendigung und Neustart der Verwaltungsdomäne. Der MRE für ein Benutzerprofil ist z. B. inkonsistent, wenn Sie die Benutzer-ID (UID) für das Benutzerprofil auf einem Knoten in der Verwaltungsdomäne geändert haben, die von Ihnen angegebene UID aber bereits von einem anderen Benutzerprofil auf einem der Knoten eingesetzt wurde. Wenn Sie die UID erneut in einen Wert ändern, der von keinem anderen Benutzerprofil innerhalb der Verwaltungsdomäne verwendet wird, führt die Clusterverwaltungsdomäne die Änderungen auf allen Knoten durch. Anschließend wird der globale Status für den Benutzerprofil-MRE auf konsistent gesetzt. Zur Resynchronisation des Benutzerprofil-MREs ist keine weitere Maßnahme erforderlich.

In einigen Fällen müssen Sie die Clusterverwaltungsdomänen-CRG beenden und erneut starten, damit die inkonsistenten Ressourcen resynchronisiert werden. Wenn Sie z. B. die UID für ein Benutzerprofil mit zugeordnetem MRE ändern, das in einem Job auf einem der anderen Clusterknoten in der Verwaltungsdomäne aktiv ist, wird der globale Wert für den dem Benutzerprofil zugeordneten MRE auf inkonsistent gesetzt, da die Änderungsoperation auf dem Knoten fehlgeschlagen ist, auf dem das Benutzerprofil in einem Job aktiv war. Sie müssen warten, bis der Job beendet ist, und anschließend die Clusterverwaltungsdomäne beenden, um den Fehler zu beheben. Wird die Verwaltungsdomäne wieder gestartet, werden die Ressourcen anhand der globalen Werte der einzelnen inkonsistenten Attribute in einen konsistenten Zustand versetzt.

Der globale Status einer überwachten Ressource wird immer auf "Ausgefallen" gesetzt, wenn die Ressource auf einem beliebigen Knoten in der Domäne gelöscht, umbenannt oder verschoben wird. In diesem Fall muss der MRE entfernt werden, da die Ressource nicht mehr von der Clusterverwaltungsdomäne synchronisiert wird.

Wird eine überwachte Ressource auf einem beliebigen System, das Teil einer Clusterverwaltungsdomäne ist, wiederhergestellt, dann wird die Ressource mit dem globalen Wert resynchronisiert, der in der Clusterverwaltungsdomäne bekannt war, als die Peer-CRG, die die Clusterverwaltungsdomäne darstellt, aktiv war.

Die folgenden Rückspeicherungsbefehle führen zu einer Resynchronisation von Systemobjekten: RSTLIB, RSTOBJ, RSTUSRPRF und RSTCFG. Außerdem führen die Befehle RSTSYSINF und UPDSYSINF zu einer Resynchronisation der Systemwerte und der Netzwerkattribute. Zur Resynchronisation der Systemumgebungsvariablen nach Ausführung des Befehls RSTSYSINF oder UPDSYSINF muss die Clusterressourcengruppe, die die Clusterverwaltungsdomäne darstellt, beendet und neu gestartet werden.

Wenn Sie überwachte Ressourcen mit dem vorherigen Zustand wiederherstellen möchten, sollten Sie den MRE entfernen, der die wiederherzustellende Ressource darstellt. Nach Wiederherstellung der Ressource fügen Sie den MRE für die Ressource aus dem System hinzu, auf dem die Wiederherstellungsoperation ausgeführt wurde. Die Clusterverwaltungsdomäne wird die überwachte Ressource mithilfe der Werte aus der wiederhergestellten Ressource synchronisieren.

Führen Sie die folgenden Schritte aus, um die Clusterverwaltungsdomäne zu überwachen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
4. Wählen Sie auf der Registerkarte **Verwaltungsdomänen** den Eintrag **Neue Verwaltungsdomäne** aus.
5. Geben Sie auf der Seite "Neue Verwaltungsdomäne" die Informationen zur Clusterverwaltungsdomänensdomäne ein.

Clusterverwaltungsdomäne stoppen:

Clusterverwaltungsdomänen bieten eine ausfallsichere Umgebung für Ressourcen einer i5/OS-Hochverfügbarkeitslösung. Unter Umständen müssen Sie eine Clusterverwaltungsdomäne stoppen, um die Synchronisation der überwachten Ressourcen vorübergehend zu beenden.

Eine Clusterverwaltungsdomäne wird inaktiv, wenn sie gestoppt wird. Während die Clusterverwaltungsdomäne inaktiv ist, werden alle überwachten Ressourcen als inkonsistent betrachtet, da die an ihnen vorgenommenen Änderungen nicht synchronisiert werden. Obwohl die Änderungen an überwachten Ressourcen weiterhin verfolgt werden, wird der globale Wert nicht geändert, und die Änderungen werden nicht in der restlichen Domäne repliziert. Beim Neustart der Clusterverwaltungsdomäne werden alle Änderungen, die während der Inaktivität der Clusterverwaltungsdomäne an überwachten Ressourcen vorgenommen wurden, auf alle aktiven Knoten verteilt.

Anmerkung: Die Clusterverwaltungsdomäne und das ihr zugeordnete Exitprogramm sind von IBM gelieferte Objekte. Sie sollten nicht über die API `QcstChangeClusterResourceGroup` oder mit dem Befehl `CHGCRG` geändert werden, da dies zu unvorhersehbaren Ergebnissen führen kann.

Führen Sie die folgenden Schritte aus, um eine Clusterverwaltungsdomäne zu stoppen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.

2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
4. Wählen Sie auf der Seite "Verwaltungsdomänen" eine Clusterverwaltungsdomäne aus.
5. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Stoppen** aus.
6. Klicken Sie in der Bestätigungsanzeige "Verwaltungsdomäne stoppen" auf **Ja**.

Zugehörige Informationen

Clusterdomäne beenden (ENDCAD)

Clusterverwaltungsdomäne löschen:

Eine Clusterverwaltungsdomäne kann über die grafische Oberfläche der Cluster Resource Services gelöscht werden. Durch Löschen einer Clusterverwaltungsdomäne wird die Synchronisation der überwachten Ressourcen, die in der Clusterverwaltungsdomäne definiert sind, beendet.

Führen Sie die folgenden Schritte aus, um eine Clusterverwaltungsdomäne zu löschen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
4. Wählen Sie auf der Seite "Verwaltungsdomänen" eine Clusterverwaltungsdomäne aus.
5. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Löschen** aus.
6. Klicken Sie in der Bestätigungsanzeige "Verwaltungsdomäne löschen" auf **Ja**.

Eigenschaften einer Clusterverwaltungsdomäne ändern:

Die Eigenschaften einer vorhandenen Clusterverwaltungsdomäne können über die grafische Oberfläche der Cluster Resource Services gelöscht werden. Über diese Eigenschaften wird die Synchronisation der überwachten Ressourceneinträge, die in der Clusterverwaltungsdomäne definiert sind, gesteuert.

Führen Sie die folgenden Schritte aus, um die Eigenschaften einer Clusterverwaltungsdomäne zu ändern:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
4. Wählen Sie auf der Seite "Verwaltungsdomänen" eine Clusterverwaltungsdomäne aus.
5. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus.
6. Auf der Seite "Eigenschaften" können Sie die folgenden Angaben zu einer Clusterverwaltungsdomäne ändern:
 - Geben Sie im Feld **Name** den Namen der Clusterverwaltungsdomäne ein. Der Name darf nicht länger als 10 Zeichen sein.
 - Geben Sie im Feld **Synchronisationsoption** das Synchronisationsverhalten an, das gewünscht wird, wenn ein Knoten mit einer Clusterverwaltungsdomäne verbunden wird. Das Feld wird nur aktiviert, wenn der Cluster Version 6 oder höher hat. Gültige Werte sind:

Option Letzte Änderung (*LASTCHG) (Standardeinstellung)

Wählen Sie diese Option aus, wenn alle Änderungen an überwachten Ressourcen auf eine Clusterverwaltungsdomäne angewendet werden sollen. Wenn ein Knoten in eine aktive Clusterverwaltungsdomäne aufgenommen wird, werden alle Änderungen, die an den überwachten Ressourcen auf dem aufzunehmenden Knoten vorgenommen wurden, während

der Knoten inaktiv war, auf die überwachten Ressourcen auf den anderen aktiven Knoten angewendet, es sei denn, an der Ressource in der aktiven Domäne wurde eine Änderung jüngerer Datums vorgenommen. Die aktuellste Änderung, die an einer überwachten Ressource vorgenommen wird, wird auf allen aktiven Knoten auf die Ressource angewendet.

Option Aktive Domäne (*ACTDMN)

Wählen Sie diese Option aus, wenn Änderungen an überwachten Ressourcen nur auf aktiven Knoten zulässig sein sollen. Änderungen an überwachten Ressourcen auf inaktiven Knoten werden gelöscht, wenn der Knoten in die Domäne aufgenommen wird. Die Option Aktive Domäne gilt nicht für NWS-Speicherbereiche (*NWSSTG) oder NWS-Konfigurationen (*NWSCFG). Die Synchronisation dieser Ressourcen basiert immer auf der letzten vorgenommenen Änderung.

- In der Liste **Knoten in der Verwaltungsdomäne** können Sie der Clusterverwaltungsdomäne durch Auswahl von **Hinzufügen** einen Knoten hinzufügen oder durch Auswahl von **Entfernen** einen Knoten aus der Domäne entfernen.

Einträge für überwachte Ressourcen verwalten:

Über die grafische Oberfläche der Cluster Resource Services können Sie Einträge für überwachte Ressourcen (MREs) in Ihrer Clusterverwaltungsdomäne verwalten. Über die Clusterverwaltungsdomäne wird sichergestellt, dass alle an diesen überwachten Ressourcen vorgenommenen Änderungen auf jedem Knoten innerhalb der HA-Umgebung konsistent sind.

Mit MRE-Status arbeiten:

Über die grafische Oberfläche der Cluster Resource Services werden Statusnachrichten zu Einträgen für überwachte Ressourcen (MREs) innerhalb einer Clusterverwaltungsdomäne bereitgestellt.

Sobald ein MRE einer Clusterverwaltungsdomäne hinzugefügt wurde, wird die Ressource auf allen Knoten der Verwaltungsdomäne auf Änderungen überwacht, um sicherzustellen, dass die Werte der Ressourcenattribute auf allen Knoten in der Clusterverwaltungsdomäne synchronisiert werden können. Das Synchronisationsverhalten wird von folgenden Faktoren bestimmt:

- Status des Clusters
- Status der Clusterverwaltungsdomäne
- Status des Knotens
- Bestimmten Aktionen auf der Ressource

Führen Sie die folgenden Schritte aus, um mit dem MRE-Status zu arbeiten:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
5. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.

Hinweis: Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.

6. Klicken Sie auf der Seite "Mit überwachten Ressourcenarten arbeiten" auf das Kontextsymbol neben der Ressourcenart, und wählen Sie **Attribute** aus.
7. Die Liste mit Einträgen für überwachte Ressourcen wird angezeigt. In der Spalte "Globaler Status" wird der aktuelle Status für dieses Attribut in der aktiven Clusterverwaltungsdomäne angezeigt.

Anhand dieser Werte wird der Status einer überwachten Ressource im Cluster bestimmt:

Globaler Wert

Der Wert, den jedes überwachte Ressourcenattribut auf allen Knoten der Verwaltungsdomäne haben sollte. Der globale Wert ist auf allen aktiven Knoten gleich und stellt die letzte in der Domäne synchronisierte Änderung dar.

Globaler Status

Der Status der Ressourcen in einer Clusterverwaltungsdomäne. Er gibt an, ob die Ressourcen vollständig synchronisiert sind. Gültige Werte für den globalen Status sind:

Konsistent

Die Werte für alle vom System überwachten Ressourcenattribute sind auf allen aktiven Knoten in der Clusterverwaltungsdomäne identisch. Dieser Status tritt in einer normalen Betriebsumgebung auf, in der Cluster, Clusterverwaltungsdomäne und alle Knoten im Cluster betriebsbereit und aktiv sind. In einer solchen Umgebung wird jede Änderung eines Werts für eine überwachte Ressource an alle übrigen Knoten in der Clusterverwaltungsdomäne weitergegeben. Die Verarbeitung erfolgt asynchron zur ursprünglichen Änderung, führt aber zu konsistenten Werten für die registrierte Ressource in der Verwaltungsdomäne. In dieser Situation ist der globale Status "Konsistent", die Änderung wird erfolgreich auf jedem Knoten durchgeführt, und der Wert der Ressource auf den einzelnen Knoten entspricht dem globalen Wert für die Ressource.

Inkonsistent

Die Werte für alle vom System überwachten Ressourcenattribute sind nicht auf allen aktiven Knoten in der Clusterverwaltungsdomäne identisch. Eine Nachricht wird aufgezeichnet, die beschreibt, weshalb der Status "Inkonsistent" ist. Wurde die überwachte Ressource beispielsweise geändert, während die Clusterverwaltungsdomäne inaktiv war, dann ist der Status der überwachten Ressource "Inkonsistent".

Anstehend

Die Werte der überwachten Attribute werden gerade innerhalb der Clusterverwaltungsdomäne synchronisiert.

Hinzugefügt

Der Eintrag für die überwachte Ressource wurde der Clusterverwaltungsdomäne hinzugefügt, aber noch nicht synchronisiert.

Beendet

Die überwachte Ressource hat einen unbekanntenen Status, da die Clusterverwaltungsdomäne beendet wurde und Änderungen an der Ressource nicht mehr verarbeitet werden. Bei Beendigung der Clusterverwaltungsdomäne wird der globale Status für alle MREs, die derzeit auf "Konsistent" gesetzt sind, auf "Beendet" gesetzt.

Ausgefallen

Die Ressource wird nicht mehr von der Clusterverwaltungsdomäne überwacht, und der MRE muss entfernt werden. Bestimmte Ressourcenaktionen werden nicht empfohlen, während eine Ressource von einer Clusterverwaltungsdomäne synchronisiert wird. Wenn es sich bei der von einem MRE repräsentierten Ressource um ein Systemobjekt handelt, darf dieses erst dann gelöscht, umbenannt oder in eine andere Bibliothek versetzt werden, nachdem der MRE entfernt wurde. Wird eine Ressource gelöscht, umbenannt oder in eine andere Bibliothek versetzt, lautet der globale Status für den MRE "Ausgefallen". Alle Änderungen, die anschließend auf irgendeinem Knoten an der Ressource vorgenommen werden, werden nicht an die übrigen Knoten in der Clusterverwaltungsdomäne weitergegeben.

Bei der Wiederherstellung einer überwachten Ressource auf einem Knoten innerhalb der Clusterverwaltungsdomäne werden die Werte der überwachten Ressource in die globalen Werte zurückgeändert, die von der Clusterverwaltungsdomäne synchronisiert wurden.

Einträge für überwachte Ressourcen entfernen:

Einträge für überwachte Ressourcen (MREs) sind Ressourcen, die derzeit innerhalb einer Hochverfügbarkeitsumgebung eingesetzt und auf Änderungen über eine Clusterverwaltungsdomäne überwacht werden. Wenn die MREs nicht mehr überwacht werden müssen, können Sie entfernt werden. Dies wird normalerweise über die grafische Oberfläche der Cluster Resource Services durchgeführt.

Führen Sie die folgenden Schritte aus, um einen Eintrag für eine überwachte Ressource zu entfernen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
5. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.

Hinweis: Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.

6. Klicken Sie in der Liste der überwachten Ressourcenarten auf das Kontextsymbol neben der überwachten Ressourcenart, und wählen Sie **Mit Einträgen für überwachte Ressourcen arbeiten** aus. Die Objektliste mit den Einträgen für überwachte Ressourcen wird angezeigt.
7. Klicken Sie auf das Kontextsymbol neben dem MRE-Objekt, das Sie entfernen möchten, und wählen Sie dann **Eintrag für überwachte Ressource entfernen** aus.
8. Klicken Sie in der Bestätigungsanzeige zum Entfernen des Eintrags auf **Ja**. Der Eintrag für die überwachte Ressource wird aus der Clusterverwaltungsdomäne entfernt.

Zugehörige Informationen

MRE aus Verwaltungsdomäne entfernen (RMVCADMRE)

API Remove Monitored Resource Entry (QfpadRmvMonitoredResourceEntry)

Überwachte Ressourcenarten auflisten:

Überwachte Ressourcenarten sind Systemobjekte, wie Benutzerprofile und Umgebungsvariablen, die von einer Clusterverwaltungsdomäne überwacht werden können. Sie können die überwachten Ressourcenarten, die derzeit in einer Clusterverwaltungsdomäne definiert sind, auflisten lassen.

Führen Sie die folgenden Schritte aus, um überwachte Ressourcenarten aufzulisten:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
5. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.

Hinweis: Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.

6. Führen Sie die erforderlichen Aktionen für ausgewählte überwachte Ressourcenarten aus.
 - Mit Attributen für überwachte Ressourcen arbeiten
 - Neuen Eintrag für überwachte Ressource hinzufügen

| *Einträge für überwachte Ressourcen auflisten:*

| Einträge für überwachte Ressourcen (MREs) sind Ressourcen, wie Benutzerprofile und Umgebungs-
| variablen, die von einer Clusterverwaltungsdomäne definiert wurden. Über die grafische Oberfläche der
| Cluster Resource Services können Einträge für überwachte Ressourcen (MREs) aufgelistet werden, die
| derzeit innerhalb einer Clusterverwaltungsdomäne definiert sind.

| Führen Sie die folgenden Schritte aus, um Einträge für überwachte Ressourcen aufzulisten:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
- | 5. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.
| **Hinweis:** Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.
- | 6. Klicken Sie in der Liste der überwachten Ressourcenarten auf das Kontextsymbol neben der überwachten Ressourcenart, und wählen Sie **Mit Einträgen für überwachte Ressourcen arbeiten** aus.
- | 7. Die Liste mit den registrierten Einträgen für überwachte Ressourcen wird angezeigt. Sie können die Einträge jetzt bearbeiten.

Zu überwachende Attribute auswählen:

Nachdem Sie Einträge für überwachte Ressourcen hinzugefügt haben, können Sie die Attribute für die Ressource auswählen, die von der Clusterverwaltungsdomäne überwacht werden soll.

Führen Sie die folgenden Schritte aus, um Attribute auszuwählen, die für einen MRE überwacht werden sollen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
5. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.
| **Hinweis:** Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.
6. Klicken Sie in der Liste der überwachten Ressourcenarten auf das Kontextsymbol neben der überwachten Ressourcenart, und wählen Sie **Mit Einträgen für überwachte Ressourcen arbeiten...** aus. Die Objektliste mit den Einträgen für überwachte Ressourcen wird angezeigt.
7. Klicken Sie auf das Kontextsymbol neben dem MRE-Objekt, das z. B. ein Benutzerprofil oder ein Systemwert sein kann, und wählen Sie dann **Mit Attributen arbeiten** aus. Die Liste mit den Attributen der Einträge für überwachte Ressourcen wird angezeigt.
8. Wählen Sie in der Attributliste der Einträge für überwachte Ressourcen die Attribute aus, die Sie überwachen möchten, und klicken Sie dann auf **Schließen**. Wenn Sie z. B. eine Ethernet-Leitungsbeschreibung auf Änderungen ihres Ressourcennamensattributs überwachen lassen möchten, wählen Sie den Ressourcennamen als Attribut aus.

Zugehörige Tasks

„Einträge für überwachte Ressourcen hinzufügen“ auf Seite 109

Sie können einer Clusterverwaltungsdomäne einen Eintrag für überwachte Ressourcen (MRE = Monitored Resource Entry) hinzufügen. Einträge für überwachte Ressourcen definieren kritische Ressourcen, damit Änderungen, die an diesen Ressourcen vorgenommen werden, innerhalb einer Hochverfügbarkeitsumgebung konsistent bleiben.

Attribute, die überwacht werden können:

Der Clusterverwaltungsdomäne kann ein Eintrag für eine überwachte Ressource für verschiedene Ressourcenarten hinzugefügt werden. Im Folgenden werden für jede Ressource die Attribute aufgelistet, die überwacht werden können.

Ressourcenarten

- Klassen (*CLS)
- | • Ethernet-Leitungsbeschreibungen (*ETHLIN)
- Beschreibungen für unabhängige Speicherpools (*ASPDEV)
- Jobbeschreibungen (*JOBDEV)
- Netzwerkattribut (*NETA)
- | • NWS-Konfiguration für Verbindungssicherheit (*NWSCFG)
- | • NWS-Konfiguration für ferne Systeme (*NWSCFG)
- | • NWS-Konfigurationen für Serviceprozessoren (*NWSCFG)
- | • NWS-Beschreibungen für iSCSI-Verbindungen (*NWSI)
- | • NWS-Beschreibungen für integrierte Netzwerksysteme (*NWSI)
- | • NWS-Speicherbereiche (*NWSSTG)
- | • Beschreibungen von NWSH-Einheiten (*NWSHDEV)
- | • Beschreibungen optischer Einheiten (*OPTDEV)
- | • Subsystembeschreibungen (*SBSDEV)
- Systemumgebungsvariablen (*ENVVVAR)
- Systemwerte (*SYSVAL)
- | • Beschreibungen von Bandeneinheiten (*TAPDEV)
- | • Token-Ring-Leitungsbeschreibungen (*TRNLIN)
- TCP/IP-Attribute (*TCPA)
- Benutzerprofile (*USRPRF)

Tabelle 15. Attribute, die für Klassen überwacht werden können

Attributname	Beschreibung
CPUTIME	Maximale CPU-Zeit
DFTWAIT	Standardwartezeit
MAXTHD	Maximale Anzahl Threads
MAXTMPSTG	Maximaler temporärer Speicher
RUNPTY	Ausführungspriorität
TEXT	Textbeschreibung
TIMESLICE	Zeitscheibe

Tabelle 16. Attribute, die für Ethernet-Leitungsbeschreibungen überwacht werden können

Attributname	Beschreibung
ASSOCPORT	Zugeordneter Portressourcenname
AUOCRTCTL	Steuereinheit automatisch erstellen
AUTODLTCTL	Steuereinheit automatisch löschen
CMNRCYLMT	Grenzwerte für Wiederherstellung
COSTBYTE	Relative Kosten pro Byte zum Senden / Empfangen von Daten über die Leitung
COSTCNN	Relative Kosten für Verbindung über die Leitung
DUPLEX	Duplex
GENTSTFRM	Testrahmen generieren
GRPADR	Gruppenadresse
LINESPEED	Übertragungsgeschwindigkeit
MAXFRAME	Maximale Rahmengröße
MAXCTL	Maximale Anzahl Steuereinheiten
MSGQ	Nachrichtwarteschlange
ONLINE	Online bei IPL
PRPDLY	Laufzeitverzögerung
RSRCNAME	Ressourcenname
SECURITY	Sicherheitsstufe der physischen Leitung
SSAP	Informationsliste für Source Service Access Point (SSAP)
TEXT	Textbeschreibung
USRDFN1	Benutzerdefiniert 1
USRDFN2	Benutzerdefiniert 2
USRDFN3	Benutzerdefiniert 3
VRYWAIT	Wartezeit beim Anhängen

Tabelle 17. Attribute, die für Beschreibungen unabhängiger Plattenpools überwacht werden können

Attributname	Beschreibung
MSGQ	Nachrichtwarteschlange
RDB	Relationale Datenbank
RSRCNAME	Ressourcenname
TEXT	Textbeschreibung

Tabelle 18. Attribute, die für Jobbeschreibungen überwacht werden können

Attributname	Beschreibung
ACGCDE	Berechnungscode
ALWMLTTHD	Mehrfach-Threads zulassen
DDMCNV	DDM-Dialog
DEVRCYACN	Aktion für Einheitenwiederherstellung.
ENDSEV	Bewertungsstufe für Beendigung
HOLD	In Jobwarteschlange anhalten

Tabelle 18. Attribute, die für Jobbeschreibungen überwacht werden können (Forts.)

Attributname	Beschreibung
INLASPGRP	ASP-Anfangsgruppe
INQMSGRPY	Antwort auf Anfragenachricht
JOBMSGQFL	Aktion bei voller Jobnachrichtenwarteschlange
JOBMSGQMX	Maximale Größe der Jobnachrichtenwarteschlange
JOBPTY	Jobpriorität (in JOBQ)
JOBQ	Jobwarteschlange
LOG	Nachrichtenprotokollierung
LOGCLPGM	CL-Programmbefehle protokollieren
OUTPTY	Ausgabepriorität (in OUTQ)
OUTQ	Ausgabewarteschlange
PRTDEV	Druckeinheit
PRTTXT	Text drucken
RQSDTA	Daten oder Befehl anfordern
RTGDTA	Leitwegdaten
SPLFACN	Aktion für Spool-Datei
SWS	Jobschalter
SYNTAX	CL-Syntaxprüfung
TEXT	Textbeschreibung
TSEPOOL	Zeitscheibenendepool
USER	Benutzer

Tabelle 19. Attribute, die für Netzwerkattribute überwacht werden können

Attributname	Beschreibung
ALWADDCLU	Hinzufügen zu Cluster zulassen
DDMACC	DDM/DRDA-Anforderungszugriff
NWSDOMAIN	Domäne des Netzwerkservers
PCSACC	Client-Anforderungszugriff
Hinweis: Jedes Netzwerkattribut wird als sein eigener Eintrag für überwachte Ressource betrachtet. Hierbei sind Ressourcenart und Attributname identisch.	

Tabelle 20. Attribute, die für NWS-Konfigurationen für Serviceprozessoren überwacht werden können

Attributname	Beschreibung
EID	Gehäuse-ID
ENBUNICAST	Unicast aktivieren
INZSP	Serviceprozessor initialisieren
SPAUT	Serviceprozessorberechtigung
SPCERTID	SP-Zertifikats-ID
SPINTNETA	Serviceprozessoradoresse
SPNAME	Serviceprozessorname
TEXT	Textbeschreibung

Tabelle 21. Attribute, die für die NWS-Konfiguration für ferne Systeme überwacht werden können

Attributname	Beschreibung
BOOTDEVID	Booteinheiten-ID
CHAPAUT	CHAP-Zielauthentifizierung
DELIVERY	Zustellungsmethode
DYNBOOTOPT	Dynamische Bootoptionen
INRCHAPAUT	CHAP-Initiatorauthentifizierung
RMTIFC	Ferne Schnittstellen
RMTSYSID	ID des fernen Systems
SPNWSCFG	Serviceprozessor-NWS-Konfiguration, die zum Verwalten des fernen Servers verwendet wird.
TEXT	Textbeschreibung

Tabelle 22. Attribute, die für die NWS-Konfiguration für Verbindungssicherheit überwacht werden können

Attributname	Beschreibung
IPSECRULE	IP-Sicherheitsregeln
TEXT	Textbeschreibung

Tabelle 23. Attribute, die für NWS-Beschreibungen für integrierte Netzwerkserver überwacht werden können

Attributname	Beschreibung
CFGFILE	Konfigurationsdatei
CODEPAGE	ASCII-Codepage, die den Zeichensatz darstellt, der von diesem Netzwerkserver eingesetzt wird
EVTLOG	Ereignisprotokoll
MSGQ	Nachrichtenwarteschlange
NWSSTGL	Speicherbereichsverbindungen
PRPDMNUSR	Domänenbenutzer weitergeben
RSRCNAME	Ressourcenname
RSTDDEVRSC	Eingeschränkte Einheitenressource
SHUTDTIMO	Zeitlimit bei Systemabschluss
SYNCTIME	Datum/Uhrzeit synchronisieren
TCPDMNNAME	Name der lokalen TCP/IP-Domäne
TCPHOSTNAM	Name des TCP/IP-Hosts
TCPPORTCFG	TCP/IP-Portkonfiguration
TCPNAMSVR	TCP/IP-Name-Server-System
TEXT	Textbeschreibung
VRYWAIT	Wartezeit beim Anhängen
WINDOWSNT	Windows-NWS-Beschreibung

Tabelle 24. Attribute, die für NWS-Beschreibungen für iSCSI-Verbindungen überwacht werden können

Attributname	Beschreibung
ACTTMR	Aktivierungszeitgeber
CFGFILE	Konfigurationsdatei

Tabelle 24. Attribute, die für NWS-Beschreibungen für iSCSI-Verbindungen überwacht werden können (Forts.)

Attributname	Beschreibung
CMNMSGQ	DFV-Nachrichtwarteschlange
CODEPAGE	ASCII-Codepage, die den Zeichensatz darstellt, der von diesem Netzwerkserver eingesetzt wird
DFTSECRULE	Standard-IP-Sicherheitsregel
DFTSTGPTH	Standardspeicherpfad
EVTLOG	Ereignisprotokoll
MLTPHGRP	Mehrfachpfadgruppe
MSGQ	Nachrichtwarteschlange
NWSCFG	NWS-Konfiguration
NWSSTGL	Speicherbereichsverbindungen
PRPDMNUSR	Domänenbenutzer weitergeben
RMVMEDPTH	Pfad der Wechseldatenträger
RSRCNAME	Ressourcenname
RSTDDEVRSC	Eingeschränkte Einheitenressource
SHUTDTIMO	Zeitlimit bei Systemabschluss
STGPTH	iSCSI-Speicherpfad des Netzwerkserver
SYNCTIME	Datum/Uhrzeit synchronisieren
TCPDMNNAME	Name der lokalen TCP/IP-Domäne
TCPHOSTNAM	Name des TCP/IP-Hosts
TCPNAMSVR	TCP/IP-Name-Server-System
TCPPORTCFG	TCP/IP-Portkonfiguration
TEXT	Textbeschreibung
VRTETHCTLP	Virtueller Ethernet-Steuerport
VRTETHPTH	Virtueller Ethernet-Pfad
VRYWAIT	Wartezeit beim Anhängen

Tabelle 25. Attribute, die für NWS-Speicherbereiche überwacht werden können

Attributname	Beschreibung
SIZE	Größe
TEXT	Textbeschreibung
TOTALFILES	Gesamtzahl Dateien

Tabelle 26. Attribute, die für Beschreibungen von NWSH-Einheiten überwacht werden können

Attributname	Beschreibung
CMNRCYLMT	Grenzwerte für Wiederherstellung
LCLIFC	Zugeordnete lokale Schnittstelle
MSGQ	Nachrichtwarteschlange
ONLINE	Online bei IPL
RSRCNAME	Ressourcenname
TEXT	Textbeschreibung

Tabelle 27. Attribute, die für Beschreibungen optischer Einheiten überwacht werden können

Attributname	Beschreibung
MSGQ	Nachrichtwarteschlange
ONLINE	Online bei IPL
RSRCNAME	Ressourcenname
TEXT	Textbeschreibung

Tabelle 28. Attribute, die für Subsystembeschreibungen überwacht werden können

Attributname	Beschreibung
AJE	Autostartjob-Eintrag
CMNE	Online bei IPL
JOBQE	Jobwarteschlange
MAXJOBS	Maximale Anzahl Jobs
PJE	Eintrag für vorab gestartete Jobs
RMTLOCNAME	Eintrag für fernen Standort (Name)
RTGE	Leitwegeintrag
SGNDSPF	Anmelde-Bildschirmdatei
SYSLIBL	Subsystembibliothek
TEXT	Textbeschreibung
WSNE	Datenstationseintrag (Name)
WSTE	Datenstationseintrag (Art)

Tabelle 29. Attribute, die für Systemumgebungsvariablen überwacht werden können

Jede Umgebungsvariable auf Systemebene (*SYS) kann überwacht werden. Attribut- und Ressourcenname sind mit dem Namen der Umgebungsvariablen identisch.
Hinweis: Jede Umgebungsvariable wird als ihr eigener Eintrag für überwachte Ressource betrachtet. Hierbei sind Ressourcenart und Attributname identisch.

Tabelle 30. Attribute, die für Systemwerte überwacht werden können

Attributname	Beschreibung
QACGLVL	Berechnungsebene
QACTJOBTP	Unterbrechung von Jobs zulassen
QALWOBJRST	Verhindert, dass ein Benutzer ein Objekt mit Systemstatus oder ein Objekt mit Berechtigungsübernahme wiederherstellt.
QALWUSRDMN	Benutzerdomänenobjekte zulassen
QASTLVL	Unterstützungsstufe
QATNPGM	Abrufprogramm
QAUDCTL	Protokollierungssteuerung
QAUDENDACN	Aktion bei Protokolljournalfehler
QAUDFRCLVL	Protokollierungsstufe erzwingen
QAUDLVL	Protokollierungsebene
QAUDLVL2	Erweiterung der Protokollierungsebene

Tabelle 30. Attribute, die für Systemwerte überwacht werden können (Forts.)

Attributname	Beschreibung
QAUTOCFG	Automatische Einheitenkonfiguration
QAUTORMT	Ferne Steuereinheiten und Einheiten
QAUTOVRT	Automatische Konfiguration von virtuellen Einheiten
QCCSID	Zeichensatz-ID
QCFGMSGQ	Nachrichtenwarteschlange für Leitungen, Steuereinheiten und Einheiten
QCHRID	Standardgrafikzeichensatz und -codepage zum Anzeigen oder Drucken von Daten
QCHRIDCTL	Steuerung für Zeichen-ID für den Job
QCMNRCYLMT	Automatische Wiederherstellung bei Kommunikationsfehler
QCNTYID	Landes- oder Regions-ID
QCRTAUT	Berechtigung für neue Objekte
QCRTOBJAUD	Prüfprotokollierung für neue Objekte
QCTLSBSD	Steuern des Subsystem oder Bibliothek
QCURSYM	Währungssymbol
QDATFMT	Datumsformat
QDATSEP	Datumstrennzeichen
QDBRCVYWT	Auf Datenbankwiederanlauf warten, bevor Neustart ausgeführt wird
QDECFMT	Dezimalformat
QDEVNAMING	Einheitennamenskonventionen
QDEVRCYACN	Aktion für Einheitenwiederherstellung
QDSCJOBIV	Zeit, bis unterbrochene Jobs enden
QDSPSGNINF	Steuert die angezeigten Anmeldeinformationen
QENDJOBLMT	Maximale Zeit für sofortige Beendigung
QFRCCVNRST	Umsetzung beim Zurückspeichern erzwingen
QHSTLOGSIZ	Größe der Systemprotokolldatei
QIGCCDEFNT	Name der codierten Schriftart
QIGCFNTSIZ	Größe der codierten Schriftart
QINACTITV	Zeitüberschreitungsintervall bei inaktivem Job
QINACTMSGQ	Aktion bei Zeitüberschreitung
QIPLTYPE	Art des durchzuführenden Neustarts
QJOBMSGQFL	Aktion bei voller Jobnachrichtenwarteschlange
QJOBMSGQMX	Maximale Größe der Jobnachrichtenwarteschlange
QJOBMSGQSZ	Anfangsgröße der Jobnachrichtenwarteschlange (in KB)
QJOBMSGQTL	Maximale Größe der Jobnachrichtenwarteschlange (in KB)
QJOBSPLA	Anfangsgröße des Spool-Steuerblocks für ein Job (in Byte)
QKBDBUF	Tastatureingabepuffer
QKBDTYPE	Landessprachliche Tastenbelegung

Tabelle 30. Attribute, die für Systemwerte überwacht werden können (Forts.)

Attributname	Beschreibung
QLANGID	Standardsprachen-ID
QLIBLCKLVL	Bibliotheken in der Bibliothekssuchliste eines Benutzerjobs sperren
QLMTDEVSSN	Einheitensitzungen begrenzen
QLMTSECOFR	Einheitenzugriff des Sicherheitsbeauftragten begrenzen
QLOCALE	Länderspezifische Angaben
QLOGOUTPUT	Druckausgabe für Jobprotokoll erzeugen
QMAXACTLVL	Maximaler Auslastungsgrad des Systems
QMAXJOB	Maximale Anzahl Jobs, die auf dem System zulässig sind
QMAXSGNACN	Die Systemantwort, wenn der durch den Systemwert QMAXSIGN vorgegebene Grenzwert erreicht ist
QMAXSIGN	Maximal zulässige Anzahl ungültiger Anmeldeversuche
QMAXSPLF	Maximale Anzahl Druckausgabedateien
QMLTTHDACN	Wenn eine Funktion in einem Job mit mehreren Threads nicht sicher für Threads ist
QPASTHRSVR	Verfügbare Datensichtgerätdurchgriffs-Serverjobs
QPRBFTR	Problemprotokollfilter
QPRBHLDTV	Mindestaufbewahrungsdauer
QPRTDEV	Standarddrucker
QPRTKEYFMT	Drucktastenformat
QPRTTXT	Bis zu 30 Zeichen, die am Listenende und auf Trennseiten gedruckt werden können
QPWDCHGBLK	Mindestzeit zwischen Kennwortänderungen
QPWDEXPITV	Intervall für Kennwortablauf
QPWDEXPWRN	Warnung vor Kennwortablauf
QPWDLMTACJ	Begrenzt die Verwendung aufeinanderfolgender Ziffern in einem Kennwort
QPWDLMTCHR	Begrenzt die Verwendung bestimmter Zeichen in einem Kennwort
QPWDLMTREP	Begrenzt die Verwendung sich wiederholender Zeichen in einem Kennwort
QPWDLVL	Kennwortstufe
QPWDMAXLEN	Maximale Anzahl Zeichen in einem Kennwort
QPWDMINLEN	Mindestanzahl Zeichen in einem Kennwort
QPWDPOSDIF	Steuert die Position der Zeichen in einem Kennwort
QPWDRQDDGT	Ziffer in einem neuen Kennwort anfordern
QPWDRQDDIF	Steuert, ob und wie sich das Kennwort von früheren Kennwörtern unterscheiden muss
QPWDRULES	Kennwortregeln
QPWDVLDPGM	Kennwortbestätigungsprogramm
QPWRDWNLMT	Maximale Zeit für sofortige Beendigung
QRCLSPLSTG	Automatische Bereinigung von nicht belegtem Druckausgabespeicher

Tabelle 30. Attribute, die für Systemwerte überwacht werden können (Forts.)

Attributname	Beschreibung
QRETSVRSEC	Server-Sicherheitsdaten sichern
QRMTSIGN	Ferne Anmeldung
QRMTSRVATR	Attribut für fernen Service
QSCANFS	Dateisysteme prüfen
QSCANFCTL	Prüfung steuern
QSCPFCONS	Konsolproblem tritt auf
QSECURITY	Systemsicherheitsstufe
QSETJOBATR	Jobattribute setzen
QSFWERLOG	Softwarefehlerprotokoll
QSHRMEMCTL	Nutzung von gemeinsam genutztem oder zugeordnetem Speicher mit Schreibfunktion zulassen
QSPCENV	Standardbenutzerumgebung
QSPLFACN	Aktion für Spool-Datei
QSRTSEQ	Sortierfolge
QSRVDMP	Serviceprotokoll für nicht überwachte Abbruchnachrichten
QSSLCSL	SSL-Chiffrierspezifikationsliste
QSSLCSLCTL	SSL-Chiffriersteuerung
QSSLPCL	SSL-Protokolle
QSTRUPPGM	Startprogramm festlegen
QSTSMMSG	Statusnachrichten anzeigen
QSYSLIBL	Systembibliotheksliste
QTIMSEP	Zeittrennzeichen
QTSEPOOL	Gibt an, ob interaktive Jobs bei Erreichen des Zeitscheibenenendes in einen anderen Hauptspeicherpool verschoben werden sollen
Hinweis: Jeder Systemwert wird als sein eigener Eintrag für überwachte Ressource betrachtet. Hierbei sind Ressourcenart und Attributname identisch.	

Tabelle 31. Attribute, die für Beschreibungen von Bandeinheiten überwacht werden können

Attributname	Beschreibung
ASSIGN	Einheit beim Anhängen zuordnen
MSGQ	Nachrichtenwarteschlange
ONLINE	Online bei IPL
RSRCNAME	Ressourcenname
TEXT	Textbeschreibung
UNLOAD	Einheit beim Abhängen entladen

Tabelle 32. Attribute, die für Token-Ring-Beschreibungen überwacht werden können

Attributname	Beschreibung
ACTLANMGR	LAN-Manager aktivieren
ADPTADR	Adresse des lokalen Adapters

Tabelle 32. Attribute, die für Token-Ring-Beschreibungen überwacht werden können (Forts.)

Attributname	Beschreibung
AUTOCTRL	Steuereinheit automatisch erstellen
AUTODLCTL	Steuereinheit automatisch löschen
CMNRCYLMT	Grenzwerte für Wiederherstellung
COSTBYTE	Relative Kosten pro Byte zum Senden / Empfangen von Daten über die Leitung
COSTCNN	Relative Kosten für Verbindung über die Leitung
DUPLEX	Duplex
ELYTKNRLS	Frühe Token-Freigabe
FCNADR	Funktionale Adresse
LINESPEED	Übertragungsgeschwindigkeit
LINKSPEED	Verbindungsgeschwindigkeit
LOGCFGCHG	Änderungen der Protokollkonfiguration
MAXCTL	Maximale Anzahl Steuereinheiten
MAXFRAME	Maximale Rahmengröße
MSGQ	Nachrichtenwarteschlange
ONLINE	Online bei IPL
PRPDLY	Laufzeitverzögerung
RSRCNAME	Ressourcenname
SECURITY	Sicherheitsstufe für Leitung
SSAP	Informationsliste für Source Service Access Point (SSAP)
TRNINFBCN	Token-Ring meldet Fehlersignal
TRNLOGLVL	Protokollstufe des TRLAN-Managers
TRNMGRMODE	TRLAN-Manager-Modus
TEXT	Textbeschreibung der Token-Ring-Leitung
USRDFN1	Benutzerdefiniert 1
USRDFN2	Benutzerdefiniert 2
USRDFN3	Benutzerdefiniert 3
VRYWAIT	Wartezeit beim Anhängen

Tabelle 33. Attribute, die für TCP/IP-Attribute überwacht werden können

Attributname	Beschreibung
ARPTIMO	Zeitlimitüberschreitung bei ARP-Cache
ECN	ECN aktivieren
IPDEADGATE	Inaktives IP-Gateway
IPDTGFWD	IP-Datagrammweiterleitung
IPPATHMTU	MTU-Pfaderkennung
IPQOSBCH	IP-QoS-Datagrammstapelverarbeitung
IPQOSENB	IP-QoS-Aktivierung
IPQOSTMR	IP-QoS-Zeitgeberauflösung
IPRSBTIMO	Zeitüberschreitung bei IP-Neuaufbau

Tabelle 33. Attribute, die für TCP/IP-Attribute überwacht werden können (Forts.)

Attributname	Beschreibung
IPSRCRTG	IP-Quellenweiterleitung
IP TTL	IP Time to Live (Hop-Limit)
LOGPCLERR	Protokollfehler protokollieren
NFC	Netzwerkdatei-Cache
TCP CLOTIMO	TCP-Wartezeitlimit
TCP CNNMSG	Nachricht bei TCP-Verbindungsende
TCP KEEPALV	TCP Keep Alive
TCP MINRTM	Mindestzeit vor TCP-Neuübertragung
TCP R1CNT	TCP R1-Übertragungswiederholungen
TCP R2CNT	TCP R2-Übertragungswiederholungen
TCP RCVBUF	TCP-Empfangspuffergröße
TCP SNDBUF	TCP-Sendepuffergröße
TCP URGPTR	TCP-Dringlichkeitszeiger
UD PCKS	UDP-Kontrollsumme
Hinweis: Jedes TCP/IP-Attribut wird als sein eigener Eintrag für überwachte Ressource betrachtet. Hierbei sind Ressourcenart und Attributname identisch.	

Tabelle 34. Attribute, die für Benutzerprofile überwacht werden können

Attributname	Beschreibung
ACGCDE	Berechnungscode
ASTLVL	Unterstützungsstufe
ATNPGM	Abrufprogramm
CCSID	ID des codierten Zeichensatzes
CHRIDCTL	Steuerung für Zeichen-ID
CNTRYID	Landes- oder Regions-ID
CURLIB	Aktuelle Bibliothek
DLVRY	Zustellungsmethode
DSPSGNINF	Anmeldeinformationen anzeigen
GID	Gruppennummer
GRPAUT	Gruppenberechtigung
GRPAUTYP	Art der Gruppenberechtigung
GRPPRF	Gruppenprofil
HOMEDIR	Ausgangsverzeichnis
INLMNU	Anfangsmenü
INLPGM	Aufzurufendes Startprogramm
JOB D	Jobbeschreibung
KBDBUF	Tastaturpufferung
LANGID	Sprachenkennung
LCLP WDMGT	Lokale Kennwortverwaltung
LMTCPB	Möglichkeiten einschränken

Tabelle 34. Attribute, die für Benutzerprofile überwacht werden können (Forts.)

Attributname	Beschreibung
LMTDEVSSN	Einheitensitzungen begrenzen
LOCALE	Länderspezifische Angaben
MAXSTG	Maximal zulässiger Speicher
MSGQ	Nachrichtenwarteschlange
OUTQ	Ausgabewarteschlange
OWNER	Eigner
PASSWORD	Benutzerkennwort
PRTDEV	Druckeinheit
PTYLMT	Höchste Planungspriorität
PWDEXP	Kennwort auf Abgelaufen setzen
PWDEXPITV	Intervall für Kennwortablauf
SETJOBATR	Jobattribute aus länderspezifischen Angaben
SEV	Bewertungscodefilter
SPCAUT	Sonderberechtigung
SPCENV	Sonderumgebung
SRTSEQ	Sortierfolge
STATUS	Status
SUPGRPPRF	Zusätzliche Gruppenprofile
TEXT	Textbeschreibung
UID	Benutzernummer
USRCLS	Benutzerklasse
USROPT	Benutzeroptionen

Nachrichten zu Einträgen für überwachte Ressourcen:

Über die grafische Oberfläche der Cluster Resource Services können Nachrichten zu Einträgen für überwachte Ressourcen angezeigt werden.

Führen Sie die folgenden Schritte aus, um Nachrichten zu Einträgen für überwachte Ressourcen anzuzeigen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Klicken Sie auf der Seite "Cluster Resource Services" auf **Mit Verwaltungsdomänen arbeiten**, um eine Liste der im Cluster befindlichen Clusterverwaltungsdomänen aufzurufen.
5. Klicken Sie auf der Seite "Verwaltungsdomänen" auf das Kontextsymbol neben der Clusterverwaltungsdomäne, und wählen Sie **Mit überwachten Ressourcenarten arbeiten** aus.

Hinweis: Die Aktion **Mit überwachten Ressourcenarten arbeiten** ist nur verfügbar, wenn der Knoten, den Sie verwalten möchten, zur Clusterverwaltungsdomäne gehört. Die aktuelle Liste der überwachten Ressourcenarten wird angezeigt.

6. Klicken Sie in der Liste der überwachten Ressourcenarten auf das Kontextsymbol neben der überwachten Ressourcenart, und wählen Sie **Mit Einträgen für überwachte Ressourcen arbeiten** aus. Die Objektliste mit den Einträgen für überwachte Ressourcen wird angezeigt.

7. Klicken Sie auf das Kontextsymbol neben dem MRE-Objekt, das z. B. ein Benutzerprofil oder ein Systemwert sein kann, und wählen Sie dann **Nachrichten anzeigen** aus.

Umschaltbare Platten verwalten

Umschaltbare Platten sind unabhängige Plattenpools, die als Teil eines Einheiten-CRGs konfiguriert wurden. Das Eigentumsrecht für Daten und Anwendungen, die in einer umschaltbaren Platte gespeichert sind, kann auf andere Systeme, die in der Einheiten-CRG definiert sind, übertragen werden. Die Technologie für umschaltbare Platten stellt Hochverfügbarkeit bei geplanten und ungeplanten Betriebsunterbrechungen zur Verfügung.

Plattenpools sperren

Sie können einen unabhängigen Plattenpool auswählen, um ihn zu sperren (abzuhängen). Es besteht kein Zugriff auf die Platteneinheiten oder Objekte im unabhängigen Plattenpool oder der zugehörigen Datenbank, bis der Plattenpool wieder verfügbar gemacht wird. Der Pool kann auf dem selben oder auf einem anderen System in der Wiederherstellungsdomäne der aktuellen Clusterressourcengruppe wieder verfügbar gemacht werden.

Wichtig: Erst nachdem ein unabhängiger Plattenpool gesperrt wurde, sind Jobreservierungen im Plattenpool möglich. Unter "Release job reservations on an independent disk" finden Sie weitere Informationen dazu, wie Sie herausfinden können, ob Jobs einen unabhängigen Plattenpool benutzen, und wie die Jobreservierungen freigegeben werden.

Wenn ein UDFS-Plattenpool unter Verwendung des System i Navigator gesperrt wird, werden eventuell Nachrichten generiert, auf die über die zeichenbasierte Schnittstelle geantwortet werden muss. System i Navigator zeigt nicht an, dass eine Nachricht ansteht.

Führen Sie die folgenden Schritte aus, um einen unabhängigen Plattenpool zu sperren:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für System i, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten**.
3. Erweitern Sie den Eintrag **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf den Plattenpool, den Sie sperren möchten, und wählen Sie **Sperren** aus.
5. Klicken Sie im angezeigten Dialogfenster auf **Sperren**, um den Plattenpool zu sperren.

Sie können hierfür auch den Befehl VRYCFG (Konfiguration an-/abhängen) über die zeichenbasierte Schnittstelle verwenden.

Mit dem Befehl DSPASPSTS (ASP-Status anzeigen) lässt sich feststellen, welcher Schritt im Prozess gerade ausgeführt wird.

Über die API QYASPCTLAA (Control API Access) können Sie die Prozesse einschränken, die Zugriff auf den ASP haben.

Wenn Sie den Zeitaufwand zum Sperren eines Plattenpools möglichst gering halten wollen, verwenden Sie die API QYASSDMO (Start DASD Management Operation).

Hardware umschaltbar machen

In einer i5/OS-Hochverfügbarkeitsumgebung müssen Sie eine externe Erweiterungseinheit umschaltbar machen.

Wenn Sie unabhängige Plattenpools in einer umschaltbaren Umgebung einsetzen, muss die zugehörige Hardware zum Umschalten berechtigt sein. Abhängig von Ihrer Umgebung können dazu Frames, Einhei-

ten oder IOPs sowie die zugeordneten Ressourcen gehören. Wählen Sie hierzu im Folgenden die Schritte aus, die sich auf Ihre umschaltbare Umgebung beziehen.

Frame oder Einheit umschaltbar machen

Ein unabhängiger Plattenpool kann Platteneinheiten in mehreren Erweiterungseinheiten enthalten. Bei Einsatz einer eigenständigen Erweiterungseinheit, die Platteneinheiten in einem unabhängigen Plattenpool enthält, müssen Sie der Erweiterungseinheit die Berechtigung erteilen, anderen Systemen Zugriff zu gewähren. Diesen Vorgang nennt man "eine Erweiterungseinheit umschaltbar machen". Wenn Sie nicht möchten, dass andere Systeme Zugriff auf die eigenständige Erweiterungseinheit erhalten sollen, müssen Sie die Erweiterungseinheit als private Einheit deklarieren.

Führen Sie die folgenden Schritte aus, um einen Frame oder eine Einheit umschaltbar zu machen.

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das gewünschte System, und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Nach Position**, und wählen Sie anschließend den Frame oder die Platteneinheit aus, die Sie umschaltbar machen wollen.
3. Klicken Sie mit der rechten Maustaste auf einen hervorgehobenen Frame oder eine hervorgehobene Platteneinheit, und wählen Sie **Umschaltbar machen** aus.
4. Folgen Sie den Anweisungen im daraufhin angezeigten Dialogfenster.

IOP umschaltbar machen

Ein IOP, der die umzuschaltenden Platteneinheiten steuert, darf nur umgeschaltet werden, wenn der Bus, der den IOP enthält, den Primärknoten (*owned shared*) gehört. Außerdem muss der Ausweichknoten den Bus ebenfalls benutzen (*use bus shared*). Weitere Informationen finden Sie unter "Dynamically switching IOPs between partitions".

Zur Ausführung dieser Task benötigen Sie ein Service-Tools-Benutzerprofil mit Verwaltungsberechtigung für die System-Partitions-Funktion der Dedicated Service Tools (DST). Weitere Informationen zu Berechtigungen für logische Partitionen finden Sie unter "Logical partition authority".

Führen Sie die folgenden Schritte aus, um das Eigentumsrecht an einem Bus unter Verwendung von Management Central zu ändern:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Wählen Sie die primäre Partition des Systems aus.
3. Erweitern Sie den Eintrag für **Konfiguration und Service**, und wählen Sie **Logische Partitionen** aus.
4. Klicken Sie mit der rechten Maustaste auf **Logische Partition**, und wählen Sie **Partitionen konfigurieren** aus.
5. Klicken Sie im Fenster "Logische Partitionen konfigurieren" mit der rechten Maustaste auf den Bus, für den Sie das Eigentumsrecht ändern möchten, und wählen Sie **Eigenschaften** aus.
6. Wählen Sie die Seite **Partitionen** aus.
7. Wählen Sie die Partition aus, die unter **Logische Eignerpartition** als Eigner des Busses angegeben ist, und wählen Sie anschließend die Art des Eigentumsrechts unter **Freigabe** aus. Wenn als Art des Eigentumsrechts eine gemeinsame Nutzung angegeben ist, dann werden alle Partitionen, die den Bus gemeinsam nutzen, in der Liste angezeigt. Klicken Sie auf Hilfe, wenn Sie weitere Informationen zu diesen Optionen benötigen.
8. Klicken Sie auf **OK**.

E/A-Pool mit Hardware Management Console umschaltbar machen

Wenn Sie die Hardware Management Console (HMC) zur Verwaltung Ihrer logischen Partitionen einsetzen, müssen Sie einen E/A-Pool erstellen, der IOP, IOA und alle angehängten Ressourcen umfasst, damit ein unabhängiger Plattenpool zwischen Partitionen umgeschaltet werden kann. Sie müssen jeder Partition, die über das Eigentumsrecht an dem unabhängigen Plattenpool verfügen soll, Zugriff gewähren, indem Sie den E/A-Pool in jedem Partitionsprofil zuordnen.

Führen Sie die folgenden Schritte aus, um einen E/A-Pool zu erstellen, der zwischen Partitionen umgeschaltet werden kann:

1. Öffnen Sie das Fenster "Merkmale des Profils für logische Partitionen", um die Profileigenschaften zu ändern und Ressourcen einem E/A-Pool zuzuordnen.
2. Klicken Sie auf die Registerkarte **Physische E/A**.
3. Erweitern Sie in der Spalte für das Profil der E/A-Einheiten den Eintrag für den Bus, der den IOP enthält, den Sie umschaltbar machen möchten.
4. Wählen Sie den IOP aus, den Sie einem E/A-Pool zuordnen möchten. Es muss sich um den gewünschten (*desired*) IOP handeln (keine Markierung in der Spalte **Erforderlich**).
5. Klicken Sie auf die Spalte für den E/A-Pool, und führen Sie den Cursor zur Zeile mit dem IOP, den Sie einem E/A-Pool zuordnen möchten. Geben Sie die Nummer für den E/A-Pool ein.
6. Wiederholen Sie diese Schritte für jeden IOA und jede Ressource unter der Steuerung des IOP, die Sie dem E/A-Pool hinzufügen möchten.
7. Klicken Sie auf **OK**.

E/A-Pool Partitionen zuordnen

Nachdem Sie die Ressourcen dem E/A-Pool hinzugefügt haben, führen Sie die folgenden Schritte aus, um den E/A-Pool jeder zusätzlichen Partition zuzuordnen, die über das Eigentumsrecht an dem unabhängigen Plattenpool in der umschaltbaren Umgebung verfügen soll.

1. Öffnen Sie das Fenster "Merkmale des Profils für logische Partitionen", um die Partitionsprofileigenschaften für jede zusätzliche Partition zu ändern, die Zugriff auf den unabhängigen Plattenpool benötigt.
2. Klicken Sie auf die Registerkarte **Physische E/A**.
3. Klicken Sie auf **Erweitert**.
4. Geben Sie im Fenster "E/A-Pools" im Feld **Hinzuzufügende E/A-Pools** die Nummer des E/A-Pools ein, dem Sie die Ressourcen zugeordnet haben, die gemeinsam mit dem unabhängigen Plattenpool umgeschaltet werden sollen.
5. Klicken Sie auf **Hinzufügen** → **OK**.

Damit die Änderungen wirksam werden, führen Sie die folgenden Schritte für jede Partition aus, deren Partitionsprofil geändert wurde:

1. Beenden Sie die Partition. Weitere Informationen finden Sie unter "Restarting and shutting down i5/OS in a logical partition".
2. Starten Sie die logische Partition durch Aktivierung des Partitionsprofils mit Änderungen.

Zugehörige Konzepte

Dynamically switching IOPs between partitions

Logical partition authority

I/O pool

Zugehörige Tasks

Changing partition profile properties

Activating the partition profile

Restarting and shutting down i5/OS™ in a logical partition.

Unabhängigen Plattenpool stilllegen

In einer i5/OS-Hochverfügbarkeitslösung dienen unabhängige Plattenpools zum Speichern ausfallsicherer Daten und Anwendungen. Bei bestimmten Systemfunktionen, wie z. B. beim Sichern, muss eine Änderung der Daten für den Zeitraum der Ausführung der Operation ausgesetzt werden.

Zur Verringerung des Zeitaufwands, der für die Stilllegung eines unabhängigen Plattenpools erforderlich ist, sollten Stapeljobwarteschlangen angehalten und einige Subsysteme beendet werden oder Durchbruchnachrichten an interaktive Benutzer gesendet werden, um sie aufzufordern, weitere Arbeiten zurückzustellen.

Führen Sie die folgenden Schritte aus, um einen unabhängigen Plattenpool stillzulegen:

Geben Sie einer Befehlszeilenschnittstelle den folgenden Befehl ein: CHGASPACT ASPDEV(Name) OPTION(*SUSPEND) SSPTIMO(30) SSPTIMOACN(*CONT), wobei *Name* für den Namen des unabhängigen Plattenpools steht, den Sie aussetzen möchten. Mit diesem Befehl geben Sie an, dass der unabhängige Plattenpool mit einem Zeitlimit von 30 Sekunden ausgesetzt und die Verarbeitung mit dem nächsten Schritt fortgesetzt werden soll, selbst wenn der Zeitlimitwert überschritten wurde.

Unabhängigen Plattenpool wieder aufnehmen

Nach der Stilllegung eines unabhängigen Plattenpools in einer i5/OS-Hochverfügbarkeitsumgebung zur Durchführung von Sicherungsoperationen müssen Sie den unabhängigen Plattenpool wieder aufnehmen, um sicherzustellen, dass die während der Stilllegung an den Daten vorgenommenen Änderungen aktualisiert werden.

Führen Sie die folgenden Schritte aus, um den unabhängigen Plattenpool wieder aufzunehmen:

Geben Sie einer Befehlszeilenschnittstelle den folgenden Befehl ein: CHGASPACT ASPDEV(name) OPTION(*RESUME), wobei *name* der Name des unabhängigen Plattenpools ist, der wieder aufgenommen werden soll.

Standortübergreifende Spiegelung verwalten

Drei standortübergreifende Spiegelungstechnologien können verwaltet werden: die geographische Spiegelung, Metro Mirror und Global Mirror. Diese standortübergreifenden Spiegelungstechnologien bieten Wiederherstellung nach einem Katastrophenfall, indem kritische Daten von Platteneinheiten am Produktionsstandort auf Platteneinheiten an einem Sicherungsstandort kopiert werden.

Geographische Spiegelung verwalten

Die folgenden Informationen unterstützen Sie bei der Verwaltung der geographischen Spiegelung. Die geographische Spiegelung ist eine Unterfunktion der standortübergreifenden Spiegelung, bei der Daten auf eine Kopie des unabhängigen Plattenpools in einer i5/OS-Umgebung gespiegelt werden.

Geographische Spiegelung aussetzen:

Wenn Sie die TCP-Kommunikation aus irgendeinem Grund beenden müssen, z. B. um das System in den Zustand des eingeschränkten Betriebs zu versetzen, sollten Sie zuerst die geographische Spiegelung aussetzen. Durch diese Aktion wird die Spiegelung zwischen Systemen in einer Hochverfügbarkeitslösung vorübergehend gestoppt.

Wenn die Spiegelung ausgesetzt ist, werden die in der Produktionskopie des unabhängigen Plattenpools vorgenommenen Änderungen nicht an die Spiegelkopie übertragen.

Anmerkung: Bei Wiederaufnahme der geographischen Spiegelung muss eine Synchronisation zwischen der Produktions- und der Spiegelkopie durchgeführt werden. Wurde die geographische Spiegelung ohne Verfolgung ausgesetzt, dann findet bei Wiederaufnahme eine vollständige Synchronisation statt. Diese kann einige Zeit in Anspruch nehmen.

| Geographische Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS aussetzen

Führen Sie die folgenden Schritte aus, um die geographische Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS auszusetzen:

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie **Plattenpools** aus.
- | 5. Wählen Sie die Produktionskopie des **Plattenpools** aus, den Sie aussetzen möchten.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
- | 7. Wählen Sie die Sitzung aus, die Sie aussetzen möchten.
- | 8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Aussetzen mit Verfolgung** oder **Aussetzen ohne Verfolgung** aus.

Geographische Spiegelung unter Verwendung von System i Navigator aussetzen

| Führen Sie die folgenden Schritte aus, um die Spiegelung unter Verwendung des System i Navigator auszusetzen:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das System, das Eigner der Produktionskopie des geographisch gespiegelten Plattenpools ist, den Sie aussetzen möchten.
3. Erweitern Sie den Eintrag für **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf die Produktionskopie des **Plattenpools**, den Sie aussetzen möchten, und wählen Sie **Geographische Spiegelung** → **Geographische Spiegelung aussetzen** aus.

Wenn Sie Das Aussetzen mit Verfolgung wählen, versucht das System die in den Plattenpools vorgenommenen Änderungen zu überwachen. Dadurch kann unter Umständen der Synchronisationsprozess verkürzt werden, da bei der Wiederaufnahme der geographischen Spiegelung lediglich eine Teilsynchronisation durchgeführt wird. Wenn kein Speicherplatz mehr für die Verfolgung vorhanden ist, muss bei der Wiederaufnahme der geographischen Spiegelung eine vollständige Synchronisation durchgeführt werden.

Anmerkung: Wenn die geographische Spiegelung ohne Verfolgung der Änderungen ausgesetzt wurde, muss bei Wiederaufnahme der Spiegelung eine vollständige Synchronisation zwischen der Produktions- und der Spiegelkopie durchgeführt werden. Wird die geographische Spiegelung jedoch mit Verfolgung der Änderungen ausgesetzt, ist bei der Wiederaufnahme nur eine Teilsynchronisation erforderlich. Eine vollständige Synchronisation kann sehr viel Zeit (eine bis mehrere Stunden) in Anspruch nehmen. Wie viel Zeit für die Synchronisation erforderlich ist, hängt auch von der Menge der zu synchronisierenden Daten, der Geschwindigkeit der TCP/IP-Verbindungen und der Anzahl der für die geographische Spiegelung belegten Leitungen ab.

Geographische Spiegelung wieder aufnehmen:

Wenn Sie die geographische Spiegelung aussetzen, müssen Sie sie später wieder aufnehmen, damit die Spiegelung zwischen der Produktionskopie und der Spiegelkopie der Daten erneut aktiviert werden kann.

Anmerkung: Gleichzeitig mit der Wiederaufnahme der geographischen Spiegelung werden die Produktions- und die Spiegelkopie synchronisiert. Diese Synchronisation kann einige Zeit in

Anspruch nehmen. Wenn ein Plattenpool gesperrt und dadurch die Synchronisation unterbrochen wird, wird diese bei Wiederaufnahme des Plattenpools an der Stelle fortgesetzt, an der sie unterbrochen wurde. Sobald die unterbrochene Synchronisation fortgesetzt wird, erscheint eine Nachricht (CPI0985D), die den Synchronisationsstatus mit 0 % angibt.

| **Geographische Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS wieder aufnehmen**

Führen Sie die folgenden Schritte aus, um die geographische Spiegelung mit IBM Systems Director Navigator for i5/OS wieder aufzunehmen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie die Produktionskopie des **Plattenpools** aus, den Sie wieder aufnehmen möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie wieder aufnehmen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Wiederaufnahme** aus.

| **Geographische Spiegelung unter Verwendung des System i Navigator wieder aufnehmen**

Führen Sie die folgenden Schritte aus, um die Spiegelung unter Verwendung des System i Navigator wieder aufzunehmen:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das System, das Eigner der Produktionskopie des Plattenpools ist, für den Sie die geographische Spiegelung wieder aufnehmen wollen.
3. Erweitern Sie den Eintrag für **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf den **Plattenpool**, für den Sie die Spiegelung wieder aufnehmen möchten, und wählen Sie **Geographische Spiegelung** → **Geographische Spiegelung wieder aufnehmen** aus.

Wenn Sie Zeit sparen möchten, sperren Sie den Plattenpool über die API QYASSDMO (Use the Start DASD Management Operation).

Spiegelkopie abhängen:

Wenn Sie die geographische Spiegelung einsetzen und auf die Spiegelkopie zugreifen wollen, um Sicherungsoperationen oder Data-Mining auszuführen oder Berichte zu erstellen, müssen Sie die Spiegelkopie von der Produktionskopie abhängen.

Durch Zugriff auf die Produktionskopie des Plattenpools wird die Spiegelkopie abgehängt.

Anmerkung: Wenn Sie die abgehängte Spiegelkopie wieder anhängen, ist eine vollständige Synchronisation zwischen der Produktionskopie und der Spiegelkopie erforderlich. Diese Synchronisation kann einige Zeit in Anspruch nehmen.

| **Spiegelkopie unter Verwendung des IBM Systems Director Navigator for i5/OS abhängen**

Führen Sie die folgenden Schritte aus, um die Spiegelkopie unter Verwendung des IBM Systems Director Navigator for i5/OS abzuhängen.

- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie **Plattenpools** aus.
- | 5. Wählen Sie die Produktionskopie des **Plattenpools** aus, den Sie abhängen möchten.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
- | 7. Wählen Sie die Sitzung aus, die Sie abhängen möchten.
- | 8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Abhängen mit Überwachung** oder **Abhängen ohne Überwachung** aus.

| **Spiegelkopie unter Verwendung des System i Navigator abhängen**

Es wird empfohlen, den unabhängigen Plattenpool zu sperren, um sicherzustellen, dass die Produktionskopie während des Vorgangs zum Abhängen nicht geändert wird.

| Führen Sie die folgenden Schritte aus, um die Spiegelkopie unter Verwendung des System i Navigator abzuhängen.

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das System, das Eigner der Produktionskopie des Plattenpools ist, aus dem Sie die Spiegelkopie abhängen möchten.
3. Erweitern Sie den Eintrag für **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf die Produktionskopie des **Plattenpools**, den Sie abhängen möchten, und wählen Sie **Geographische Spiegelung** → **Gespiegelte Kopie abhängen** aus.

Wenn Sie nicht auf **Geographische Spiegelung** → **Gespiegelte Kopie abhängen** klicken können, da die Einträge inaktiviert sind, bedeutet dies, dass die Spiegelkopie mit der Produktionskopie nicht synchron ist. Sie müssen zuerst die geographische Spiegelung wieder aufnehmen, der Plattenpool anhängen und die Produktionskopie sowie die Spiegelkopie synchronisieren, bevor die Spiegelkopie abgehängt werden kann.

Bevor Sie die abgehängte Spiegelkopie verfügbar machen, sollten Sie eine zweite eindeutige Einheitenbeschreibung für den unabhängigen Plattenpool erstellen, der ihn von der Produktionskopie unterscheidet. #Eine separate Einheitenbeschreibung für die Spiegelkopie verhindert, dass zwei Instanzen derselben Datenbank im Netzwerk existieren. Sie erleichtert auch die Arbeit außerhalb des System i Navigator. Verwenden Sie die Einheitenbeschreibung der Spiegelkopie, um die abgehängte Spiegelkopie verfügbar zu machen.

Spiegelkopie wieder anhängen:

Wenn Sie nach dem Abhängen der Spiegelkopie die Arbeit mit der abgehängten Spiegelkopie beendet haben, müssen Sie die Spiegelkopie wieder anhängen, um die geographische Spiegelung wieder aufzunehmen.

Durch Zugriff auf die Produktionskopie des Plattenpools wird die abgehängte Spiegelkopie wieder angehängt. Die abgehängte Spiegelkopie muss gesperrt sein, wenn Sie sie wieder an die Produktionskopie anhängen.

Anmerkung: Wenn Sie die abgehängte Spiegelkopie wieder anhängen, ist eine vollständige Synchronisation zwischen der Produktionskopie und der Spiegelkopie erforderlich. Diese Synchronisation kann einige Zeit in Anspruch nehmen.

- | **Spiegelkopie unter Verwendung des IBM Systems Director Navigator for i5/OS** wieder anhängen
- | Führen Sie die folgenden Schritte aus, um die Spiegelkopie unter Verwendung des IBM Systems Director Navigator for i5/OS wieder anzuhängen.
- | 1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
- | 2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
- | 3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
- | 4. Wählen Sie **Plattenpools** aus.
- | 5. Wählen Sie die Produktionskopie des **Plattenpools** aus, den Sie wieder anhängen möchten.
- | 6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
- | 7. Wählen Sie die Sitzung aus, die Sie wieder anhängen möchten.
- | 8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Anhängen** aus.

| Spiegelkopie unter Verwendung des System i Navigator wieder anhängen

| Führen Sie die folgenden Schritte aus, um die Spiegelkopie unter Verwendung des System i Navigator wieder anzuhängen.

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das System, das Eigner der Produktionskopie des Plattenpools ist, an den Sie die abgehängte Spiegelkopie wieder anhängen möchten.
3. Erweitern Sie den Eintrag für **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
4. Klicken Sie mit der rechten Maustaste auf die Produktionskopie des **Plattenpools**, den Sie wieder anhängen möchten, und wählen Sie **Geographische Spiegelung** sowie den Eintrag zum **Wiederanhängen der Spiegelkopie** aus.

Geographische Spiegelung dekonfigurieren:

Wenn Sie die Funktion der geographischen Spiegelung nicht mehr für einen bestimmten Plattenpool oder ein Plattenpoolgruppe verwenden möchten, können Sie **Geographische Spiegelung dekonfigurieren** auswählen. Durch das Dekonfigurieren der geographischen Spiegelung wird die geographische Spiegelung vom System gestoppt und die Spiegelkopie der Plattenpools auf den Knoten am Standort der Spiegelkopie gelöscht.

Zum Dekonfigurieren der geographischen Spiegelung muss sich der Plattenpool offline befinden.

Führen Sie die folgenden Schritte aus, um die geographische Spiegelung zu dekonfigurieren:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das gewünschte System und wählen Sie Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
3. Klicken Sie mit der rechten Maustaste auf die Produktionskopie des **Plattenpools**, den Sie dekonfigurieren möchten, und wählen Sie **Geographische Spiegelung** → **Geographische Spiegelung dekonfigurieren** aus.
4. Aktualisieren Sie die Clusterkonfiguration wie folgt:
 - a. Entfernen Sie die der Spiegelkopie zugeordneten Knoten aus der Wiederherstellungsdomäne der Einheiten-CRG.
 - b. Entfernen Sie den Standortnamen und die IP-Adressen der Datenports auf den im Cluster verbleibenden Knoten.

Zugehörige Tasks

„Knoten entfernen“ auf Seite 130

Wenn Sie ein Upgrade für einen bestimmten Knoten ausführen oder ein Knoten in der HA-Umgebung unter i5/OS nicht mehr benötigt wird, müssen Sie den Knoten aus dem Cluster entfernen.

Eigenschaften der geographischen Spiegelung ändern:

Sie können Informationen zur geographischen Spiegelung ändern, indem Sie die zugeordneten Kopiebeschreibungen bearbeiten.

Eigenschaften der geographischen Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS ändern

Führen Sie die folgenden Schritte aus, um die geographische Spiegelung unter Verwendung des IBM Systems Director Navigator for i5/OS zu bearbeiten:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus. Wählen Sie zum Ändern einer zugeordneten Kopiebeschreibung die betreffende Kopiebeschreibung aus, und klicken Sie dann auf **Bearbeiten**.

Eigenschaften der geographischen Spiegelung unter Verwendung des System i Navigator ändern

Führen Sie die folgenden Schritte aus, um die Eigenschaften der geographischen Spiegelung unter Verwendung des System i Navigator zu ändern:

1. Erweitern Sie den Eintrag für System i Navigator, und wählen Sie **Meine Verbindungen** (oder Ihre aktive Umgebung) aus.
2. Erweitern Sie den Eintrag für das System, das Eigner der Produktionskopie des geographisch gespiegelten Plattenpools ist, der der Sitzung für geographische Spiegelung zugeordnet ist. Wählen Sie zur Bearbeitung der Attribute des Plattenpools Folgendes aus: **Konfiguration und Service** → **Hardware** → **Platteneinheiten** → **Plattenpools**.
3. Klicken Sie mit der rechten Maustaste auf die Produktionskopie des **Plattenpools**, dessen Attribute Sie bearbeiten möchten, und wählen Sie **Sitzungen** → **Öffnen** aus.
4. Klicken Sie mit der rechten Maustaste auf die **Sitzung**, deren Attribute Sie bearbeiten möchten, und wählen Sie **Eigenschaften** aus. Wählen Sie zum Ändern einer zugeordneten Kopiebeschreibung die betreffende Kopiebeschreibung aus, und klicken Sie dann auf **Bearbeiten**.

Metro-Mirror-Sitzungen verwalten

In einer i5/OS -Hochverfügbarkeitsumgebung mit IBM System Storage-Metro-Mirror-Technologie müssen Sie eine Metro-Mirror-Sitzung zwischen den i5/OS-Systemen und den externen Platteneinheiten, für die Metro Mirror konfiguriert wurde, konfigurieren. Diese Sitzungen können über das System verwaltet werden.

Metro-Mirror-Sitzungen aussetzen:

Zur Durchführung von Wartungsarbeiten müssen Sie unter Umständen Metro-Mirror-Sitzungen aussetzen.

Führen Sie die folgenden Schritte aus, um eine Metro-Mirror-Sitzung auszusetzen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, den Sie aussetzen möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie aussetzen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Aussetzen** aus.

Metro-Mirror-Sitzungen wieder aufnehmen:

Nachdem Sie Routineoperationen, wie z. B. eine Systemwartung, ausgeführt haben, müssen Sie eine ausgesetzte Metro-Mirror-Sitzung wieder aufnehmen, um die Hochverfügbarkeit wieder zu aktivieren.

Führen Sie die folgenden Schritte aus, um eine Metro-Mirror-Sitzung wieder aufzunehmen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, der ausgesetzt wurde.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die ausgesetzt wurde.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Wiederaufnahme** aus.

Metro-Mirror-Sitzung löschen:

Eine Metro-Mirror-Sitzung, die nicht mehr für Hochverfügbarkeit und Wiederherstellung nach einem Katastrophenfall eingesetzt werden soll, kann gelöscht werden.

Führen Sie die folgenden Schritte aus, um eine Metro-Mirror-Sitzung zu löschen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der zu löschenden Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie löschen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Löschen** aus.

Metro-Mirror-Eigenschaften anzeigen:

Rufen Sie die Informationen zu einer Metro-Mirror-Sitzung auf, wenn Sie die zugeordneten Kopiebeschreibungen ändern möchten.

Führen Sie die folgenden Schritte aus, um die Metro-Mirror-Eigenschaften unter Verwendung des IBM Systems Director Navigator for i5/OS zu ändern.

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus. Wählen Sie zum Ändern einer zugeordneten Kopiebeschreibung die betreffende Kopiebeschreibung aus, und klicken Sie dann auf **Bearbeiten**.

Global Mirror verwalten

In einer i5/OS -Hochverfügbarkeitsumgebung mit IBM System Storage-Global-Mirror-Technologie müssen Sie eine Global-Mirror-Sitzung zwischen den i5/OS-Systemen und den externen Platteneinheiten, für die Global Mirror konfiguriert wurde, konfigurieren. Diese Sitzungen können über das System verwaltet werden.

Global-Mirror-Sitzungen aussetzen:

Zur Durchführung von Wartungsarbeiten im System müssen Sie unter Umständen Global-Mirror-Sitzungen aussetzen.

Führen Sie die folgenden Schritte aus, um eine Global-Mirror-Sitzung auszusetzen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, den Sie aussetzen möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie aussetzen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Aussetzen** aus.

Global-Mirror-Sitzungen wieder aufnehmen:

Nachdem Sie Routineoperationen, wie z. B. eine Systemwartung, ausgeführt haben, müssen Sie eine ausgesetzte Global-Mirror-Sitzung wieder aufnehmen, um die Hochverfügbarkeit wieder zu aktivieren.

Führen Sie die folgenden Schritte aus, um eine Global-Mirror-Sitzung wieder aufzunehmen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, der ausgesetzt wurde.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die ausgesetzt wurde.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Wiederaufnahme** aus.

Global-Mirror-Sitzungen löschen:

Eine Global-Mirror-Sitzung, die nicht mehr für Hochverfügbarkeit und Wiederherstellung nach einem Katastrophenfall eingesetzt werden soll, kann gelöscht werden.

Führen Sie die folgenden Schritte aus, um eine Global-Mirror-Sitzung zu löschen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der zu löschenden Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie löschen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Löschen** aus.

Eigenschaften der Global-Mirror-Sitzung ändern:

Rufen Sie die Informationen zu einer Global-Mirror-Sitzung auf, wenn Sie die zugeordneten Kopiebeschreibungen ändern möchten.

Führen Sie die folgenden Schritte aus, um die Global-Mirror-Eigenschaften unter Verwendung des IBM Systems Director Navigator for i5/OS zu ändern.

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus. Wählen Sie zum Ändern einer zugeordneten Kopiebeschreibung die betreffende Kopiebeschreibung aus, und klicken Sie dann auf **Bearbeiten**.

FlashCopy verwalten

FlashCopy ist eine IBM System Storage-Technologie, die es erlaubt, eine Zeitpunktkopie der externen Platteneinheiten zu erstellen. In i5/OS-Hochverfügbarkeitslösungen mit Metro- oder Global-Mirror-Spiegelung kann durch den Einsatz von FlashCopy das Fenster zum Durchführen von Sicherungen verkleinert werden, indem eine Datenkopie erstellt wird, die dann auf Speichermedien gesichert werden kann. Zur Verwendung von FlashCopy muss eine Sitzung zwischen dem System und den externen Speichereinheiten erstellt werden.

FlashCopy-Sitzung konfigurieren

Für i5/OS-Hochverfügbarkeitsumgebungen, die IBM System Storage-Technologie einsetzen, kann eine FlashCopy-Sitzung zur Erstellung einer Zeitpunktkopie der Daten konfiguriert werden.

Informationen zur Verwendung von FlashCopy auf IBM System Storage DS6000 finden Sie im IBM System Storage DS6000 Information Center. Informationen zur Verwendung von FlashCopy auf IBM System Storage DS8000 finden Sie im IBM System Storage DS8000 Information Center.

Führen Sie die folgenden Schritte aus, um eine FlashCopy-Sitzung zu konfigurieren:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool aus, den Sie als Quelle verwenden möchten.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Neue Sitzung** aus.
7. Folgen Sie den Anweisungen des Assistenten, um die Task durchzuführen.

FlashCopy aktualisieren

Eine FlashCopy-Sitzung kann bei Durchführung der Resynchronisation der FlashCopy-Datenträger auf den externen IBM System Storage-Speichereinheiten aktualisiert werden. Bei der Resynchronisation kann eine Kopie erstellt werden, ohne dass der gesamte Datenträger erneut kopiert werden muss. Dieser Prozess ist nur in einer persistenten Beziehung möglich, in der die Speichereinheit die Aktualisierungen auf dem Quellen- und dem Zieldatenträger ständig überwacht. Persistent bedeutet, dass die Beziehung zwischen dem Quellen- und dem Zieldatenträger auch nach Abschluss der Erstellung einer Hintergrundkopie bestehen bleibt. Die unter i5/OS erstellte FlashCopy-Sitzung bietet eine Möglichkeit, alle auf FlashCopy bezogenen Aktivitäten auf den IBM System Storage-Einheiten zu verwalten und zu überwachen.

Führen Sie die folgenden Schritte aus, um eine FlashCopy-Sitzung zu aktualisieren:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der zu aktualisierenden Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie aktualisieren möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag zum **Aktualisieren der FlashCopy** aus.

FlashCopy wieder anhängen

FlashCopy-Sitzung wieder anhängen

Führen Sie die folgenden Schritte aus, um eine FlashCopy-Sitzung wieder anzuhängen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der wieder anzuhängenden Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie wieder anhängen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag zum **Wiederanhängen der FlashCopy** aus.

FlashCopy abhängen

se können die Zieldatenträger für eine ausgewählte FlashCopy-Sitzung von der Quelle abhängen.

Führen Sie die folgenden Schritte aus, um Zieldatenträger für eine FlashCopy-Sitzung von der Quelle abzuhängen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der abzuhängenden Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, von der Sie Ziel- und Quellendatenträger abhängen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag zum **Abhängen der FlashCopy** aus.

FlashCopy löschen

eine FlashCopy-Sitzung löschen.

Führen Sie die folgenden Schritte aus, um eine FlashCopy-Sitzung zu löschen:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der zu löschenden Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus, die Sie löschen möchten.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Löschen** aus.

Daten von FlashCopy wiederherstellen

Nachdem eine FlashCopy auf den IBM System Storage-Einheiten erstellt wurde, können bei Ausfall der Datenquellenkopie die Daten vom Zieldatenträger wieder auf dem Quellendatenträger hergestellt werden. Hierzu müssen Sie die FlashCopy-Sitzung, die unter i5/OS erstellt wurde, umkehren. Durch Umkehren der Sitzung werden die Daten vom Zieldatenträger zurück auf den Quellendatenträger kopiert, wodurch die Quelle auf eine frühere Version gebracht wird.

Achtung: Durch Umkehren einer FlashCopy-Sitzung gehen die auf der Quellenkopie vorgenommenen Änderungen verloren, da die Daten vom Zieldatenträger auf die Quelle zurückkopiert werden. Dadurch wird die Quelle in den Stand zum Zeitpunkt der FlashCopy-Erstellung zurückversetzt.

Führen Sie die folgenden Schritte aus, um eine FlashCopy-Sitzung umzukehren:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den Plattenpool der Quellenkopie aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag zum **Öffnen der Sitzungen** aus.
7. Wählen Sie die Sitzung aus.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag zum **Umkehren der FlashCopy** aus.

FlashCopy-Eigenschaften ändern

Rufen Sie die Informationen zu einer FlashCopy-Sitzung auf, wenn Sie die zugeordneten Kopiebeschreibungen ändern möchten.

Führen Sie die folgenden Schritte aus, um eine FlashCopy-Sitzung zu ändern:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Konfiguration und Service** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie **Plattenpools** aus.
5. Wählen Sie den der Sitzung zugeordneten Plattenpool aus.
6. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Sitzungen** aus.
7. Wählen Sie die Sitzung aus.
8. Wählen Sie im Menü **Aktion auswählen** den Eintrag **Eigenschaften** aus. Wählen Sie zum Ändern einer zugeordneten Kopiebeschreibung die betreffende Kopiebeschreibung aus, und klicken Sie dann auf **Bearbeiten**.

Fehlerbehebung für HA-Lösung

Nach der Konfiguration der i5/OS-Hochverfügbarkeitslösung können unter Umständen Probleme mit unterschiedliche Technologien auftreten, wie z. B. bei Clustern und standortübergreifender Spiegelung.

Fehlerbehebung für Cluster durchführen

Hier finden Sie Lösungen zur Fehlerbehebung bei clusterspezifischen Problemen.

Zuweilen hat es den Anschein, dass ein Cluster nicht richtig funktioniert. Unter dem vorliegenden Thema finden Sie Informationen zu den Problemen, die bei Clustern auftreten können.

Feststellen, ob ein Clusterproblem besteht

Beginnen Sie hier mit der Diagnose Ihrer Clusterprobleme.

Zuweilen hat es den Anschein, dass ein Cluster nicht richtig funktioniert. Wenn Sie vermuten, dass ein Problem bestehen könnte, wird Sie die folgende Vorgehensweise dabei unterstützen, herauszufinden, ob ein Problem besteht, und gegebenenfalls, um welche Art von Problem es sich handelt.

- **Feststellen, ob das Clustering auf Ihrem System aktiv ist.**

Um festzustellen, ob die Cluster Resource Services aktiv sind, sollten Sie die beiden Jobs - QCSTCTL und QCSTCRGM - in der Liste der Systemjobs suchen. Wenn die Jobs aktiv sind, dann sind auch die Cluster Resource Services aktiv. Zum Anzeigen der Jobs können Sie die Ablaufsteuerungsfunktion von IBM Director Navigator for i5/OS oder von System i Navigator verwenden oder den Befehl WRKACTJOB (Mit aktiven Jobs arbeiten). Die Statusinformationen für den Cluster können auch mit dem Befehl DSPCLUINF (Clusterinformationen anzeigen) aufgerufen werden.

– Für die Cluster Resource Services können noch weitere Jobs aktiv sein. Clusterjobs geben Auskunft darüber, wie Cluster Resource Services-Jobs formatiert sind.

- **Ursache für Nachricht CPFBB26 feststellen.**

Nachricht : Die Cluster Resource Services sind nicht aktiv oder antworten nicht.

Ursache : Die Cluster Resource Services sind entweder nicht aktiv oder können auf diese Anforderung nicht antworten, da eine Ressource nicht verfügbar oder beschädigt ist.

Dieser Fehler kann bedeuten, dass entweder der CRG-Job oder der Cluster nicht aktiv ist. Verwenden Sie den Befehl DSPCLUINF (Clusterinformationen anzeigen), um herauszufinden, ob der Knoten aktiv ist. Ist dies nicht der Fall, starten Sie den Clusterknoten. Ist er aktiv, sollten Sie auch die Clusterressourcengruppe auf Probleme überprüfen.

Suchen Sie den CRG-Job in der Liste der Systemjobs. Zum Anzeigen der Jobs können Sie die Ablaufsteuerungsfunktion von IBM Director Navigator for i5/OS oder von System i Navigator verwenden oder den Befehl WRKACTJOB (mit aktiven Jobs arbeiten). Die Statusinformationen für die betreffende Clusterressourcengruppe können auch mit dem Befehl DSPCRGINF (CRG-Informationen anzeigen) auf-

gerufen werden, indem der Name der Clusterressourcengruppe im Befehl angegeben wird. Wenn der CRG-Job nicht aktiv ist, finden Sie anhand des CRG-Jobprotokolls die Ursache für die Beendigung des Jobs heraus. Sobald das Problem behoben ist, können Sie den CRG-Job mit dem Befehl CHGCLURCY (Clusterwiederherstellung ändern) erneut starten oder durch Beenden und erneutes Starten des Clusters auf dem betreffenden Knoten.

- **Nachrichten suchen, die auf ein Problem hinweisen.**

- Vergewissern Sie sich, dass Sie alle Nachrichten, die einem Clusterbefehl zugeordnet sind, prüfen können. Drücken Sie hierzu die Taste F10, um zwischen "Detaillierte Nachrichten einschließen" und "Detaillierte Nachrichten ausschließen" hin- und herzuschalten. Treffen Sie die Auswahl zum Einschließen aller detaillierten Nachrichten und prüfen Sie anhand dieser Nachrichten, ob weitere Maßnahmen erforderlich sind.
- Suchen Sie in QSYSOPR nach Anfragenachrichten, für die Antworten anstehen.
- Suchen Sie in QSYSOPR nach Fehlernachrichten, die auf ein Clusterproblem hinweisen. Normalerweise liegen diese Nachrichten im Bereich von CPFBB00 bis CPFBBFF.
- Rufen Sie das Systemprotokoll (CL-Befehl DSPLOG) auf, und suchen Sie nach Nachrichten, die auf ein Clusterproblem hinweisen. Normalerweise liegen diese Nachrichten im Bereich von CPFBB00 bis CPFBBFF.

- **Prüfen, ob Jobprotokolle für Clusterjobs auf schwerwiegende Fehler hinweisen.**

Für die Jobprotokolle ist normalerweise die Protokollstufe von (4 0 *SECLVL) gesetzt, damit Sie die erforderlichen Fehlernachrichten anzeigen können. Vergewissern Sie sich, dass die Protokollstufe für die Jobs und das Exitprogramm entsprechend gesetzt wurde. Wenn das Clustering nicht aktiv ist, können Sie aber auch die Spool-Dateien für die Clusterjobs und Exitprogrammjobs überprüfen.

- **Bei Verdacht auf eine Blockierung alle Aufrufstacks der Clusterjobs prüfen.**

Versuchen Sie herauszufinden, ob sich das Programm in einem DEQW-Status befindet. Ist dies der Fall, sollten Sie die Aufrufstacks der einzelnen Threads überprüfen, um zu sehen, ob sie getSpecialMsg enthalten.

- **VLIC-Protokolleinträge suchen.**

Der Hauptcode dieser Protokolleinträge ist 4800.

- **Verwenden Sie den Befehl NETSTAT, um festzustellen, ob Probleme in Ihrer Übertragungs-umgebung bestehen.**

Mit NETSTAT werden Statusinformationen zu den TCP/IP-Netzleitwegen, Schnittstellen, TCP-Verbindungen und UDP-Ports auf Ihrem System zurückgegeben.

- Verwenden Sie Netstat Auswahl 1 (Mit TCP/IP-Schnittstellenstatus arbeiten), um sicherzustellen, dass die für das Clustering ausgewählten IP-Adressen den Status 'Aktiv' aufweisen. Die LOOP-BACK-Adresse (127.0.0.1) muss ebenfalls aktiv sein.
- Verwenden Sie Netstat Auswahl 3 (Mit TCP/IP-Verbindungsstatus arbeiten), um die Portnummern (F14) anzuzeigen. Der lokale Port 5550 sollte den Status 'Empfangsbereit' haben. Dieser Port muss mit dem Befehl STRTCPSVR *INETD geöffnet werden, was durch das Vorhandensein des Jobs QTOGINTD (Benutzer QTCP) in der Liste der aktiven Jobs belegt ist. Wenn das Clustering auf einem Knoten gestartet wird, muss der lokale Port 5551 geöffnet sein und sich im Status '*UDP' befinden. Wenn das Clustering nicht gestartet ist, darf Port 5551 nicht geöffnet werden, da sonst das erfolgreiche Starten des Clustering auf dem betreffenden Knoten verhindert wird.
- Verwenden Sie den Pingbefehl. Wenn Sie versuchen, einen Clusterknoten zu starten, der nicht durch Pingbefehl erreicht werden kann, erhalten Sie einen internen Clusteringfehler (CPFBB46).

| **Wiederherstellungsinformationen für einen Cluster erfassen**

| Mit dem Befehl WRKCLU (Mit Cluster arbeiten) können Sie Informationen zu einem Cluster sammeln, um sich ein vollständiges Bild über den Cluster machen zu können. Diese Informationen sind bei der Fehlerbehebung nützlich.

| Der Befehl WRKCLU (Mit Cluster arbeiten) wird verwendet, um Clusterknoten und -objekte anzuzeigen und mit ihnen zu arbeiten. Bei Ausführung dieses Befehls wird die Anzeige "Mit Cluster arbeiten" ange-

| zeigt. Mit diesem Befehl können Knoten in einem Cluster und Clusterinformationen nicht nur angezeigt,
| sondern auch Daten über den Cluster aus den angezeigten Informationen erfasst werden.

| Führen Sie die folgenden Schritte aus, um Informationen zur Fehlerbehebung zu erfassen:

| 1. Geben Sie in einer zeichenbasierten Schnittstelle `WRKCLU OPTION(OPTION)` ein. Mithilfe der nachstehen-
| den Optionen können Sie angeben, mit welchen Clusterstatusinformationen Sie arbeiten möchten.

| ***SELECT**

| Menü "Mit Cluster arbeiten" anzeigen.

| ***CLUINF**

| Clusterinformationen anzeigen.

| ***CFG** Leistungs- und Konfigurationsparameter für den Cluster anzeigen.

| ***NODE**

| Anzeige "Mit Clusterknoten arbeiten" anzeigen, die eine Liste der Knoten im Cluster ist.

| ***DEVDMN**

| Anzeige "Mit Einheitendomänen arbeiten" anzeigen, die eine Liste der Einheitendomänen im
| Cluster darstellt.

| ***CRG** Anzeige "Mit Clusterressourcengruppen arbeiten" anzeigen, die eine Liste der Cluster-
| ressourcengruppen im Cluster darstellt.

| ***ADMMDN**

| Anzeige "Mit Verwaltungsdomänen arbeiten" anzeigen, die eine Liste der Verwaltungs-
| domänen im Cluster darstellt.

| ***SERVICE**

| Erfasst relevante Trace- und Debuginformationen für alle Cluster Resource Services-Jobs im
| Cluster. Diese Informationen werden in eine Datei geschrieben, wobei für jeden Cluster
| Resource Services-Job eine Teildatei verwendet wird. Diesen Befehl nur auf Anweisung des
| Servicegebers verwenden. Der Befehl zeigt eine Bedienerführung für den Befehl `DMPCLUTRC`
| (Speicherauszug von Cluster-Trace erstellen) an.

| **Allgemeine Clusterfehler**

Hier werden einige der häufigsten Probleme aufgelistet, die in einem Cluster auftreten können, sowie
Methoden zur Vermeidung von Clusterproblemen und deren Behebung.

Die folgenden allgemeinen Probleme sind einfach zu vermeiden und zu beheben.

Clusterknoten kann nicht gestartet oder erneut gestartet werden

Diese Situation wird üblicherweise durch Probleme in der Übertragungsumgebung verursacht. Zur Ver-
meidung dieser Situation sollten Sie sich vergewissern, dass die Netzattribute, einschließlich Loopback-
Adresse, `INETD`-Einstellungen, Attribut `ALWADDCLU` und IP-Adressen für die Clusterübertragung, kor-
rekt gesetzt wurden.

- Das Netzattribut `ALWADDCLU` muss auf dem Zielknoten korrekt gesetzt sein, wenn versucht wird,
einen fernen Knoten zu starten. Abhängig von der Umgebung sollte die Einstellung `*ANY` oder
`*RQSAUT` sein.
- Die für das Clustering ausgewählten IP-Adressen, die lokal und auf dem Zielknoten verwendet werden
sollen, müssen den Status *Aktiv* aufweisen.
- Die `LOOPBACK`-Adresse (127.0.0.1) muss ebenfalls lokal und auf dem Zielknoten aktiv sein.
- Die lokalen und fernen Knoten müssen in der Lage sein, den Pingbefehl über die IP-Adressen abzuset-
zen, die für das Clustering benutzt werden sollen, um sicherzustellen, dass die Weiterleitung im Netz-
werk aktiv ist.

- Auf dem Zielknoten muss INETD aktiv sein. Wenn INETD aktiv ist, muss Port 5550 auf dem Zielknoten im Status *Empfangsbereit* sein. Weitere Informationen zum Starten des INETD-Servers finden Sie unter INETD-Server.
- Bevor Sie versuchen, einen Knoten zu starten, darf Port 5551 nicht geöffnet werden, da sonst das erfolgreiche Starten des Clustering auf dem betreffenden Knoten verhindert wird.

Mehrere, aus jeweils einem Knoten bestehende Einzelcluster

Diese Situation kann eintreten, wenn der gestartete Knoten mit den restlichen Clusterknoten nicht kommunizieren kann. Prüfen Sie die Kommunikationspfade.

Langsame Reaktion vom Exitprogramm

Die Ursache für diese Situation ist normalerweise eine vom Exitprogramm benutzte falsche Einstellung für die Jobbeschreibung. Der Parameter MAXACT ist möglicherweise so niedrig eingestellt, dass zu einem gegebenen Zeitpunkt nur eine Instanz des Exitprogramms aktiv sein kann. Als Einstellung wird *NOMAX empfohlen.

Generelle Leistungsverminderung

Für dieses Symptom gibt es mehrere Ursachen.

- Die wahrscheinlichste Ursache ist hoher Datenverkehr über eine gemeinsam genutzte Datenübertragungsleitung.
- Eine weitere wahrscheinliche Ursache ist eine Inkonsistenz zwischen der Kommunikationsumgebung und den Anpassungsparametern für Clusternachrichten. Mit der API QcstRetrieveCRSInfo (Retrieve Cluster Resource Services) können die aktuellen Einstellungen der Optimierungsparameter angezeigt und mit der API QcstChgClusterResourceServices (Change Cluster Resource Services) können sie geändert werden. Eine Verminderung der Clusterleistung kann auch auftreten, wenn Standardeinstellungen für die Optimierungsparameter in Verbindung mit alter Adapterhardware verwendet werden. Die Adapterhardwaretypen, die als *alt* gelten, sind: 2617, 2618, 2619, 2626 und 2665. In diesem Fall sollte die Einstellung des Optimierungsparameters *Leistungsklasse* auf *Normal* gesetzt werden.
- Eine weitere häufige Ursache für diesen Zustand sind Probleme mit IP-Multicastgruppen. Wenn die primären Clusteradressen (eine primäre Clusteradresse ist die erste bei der Clustererstellung oder beim Hinzufügen eines Knotens für einen bestimmten Knoten eingegebene Adresse) für mehrere Knoten sich auf einem gemeinsamen LAN befinden, wird der Cluster die IP-Multicastfunktion verwenden. Mit dem NETSTAT-Befehl können Sie prüfen, ob die primären Clusteradressen die Multicast-Hostgruppe 226.5.5.5 haben. Verwenden Sie Auswahl 14 *Multicast-Gruppe anzeigen* zum Anzeigen der betreffenden Adresse. Wenn die Multicastgruppe nicht existiert, überprüfen Sie über die API QcstRetrieveCRSInfo (Retrieve Cluster Resource Services Information), ob die Standardeinstellung TRUE (WAHR) für den Clusteroptimierungsparameter *Multicast aktivieren* noch gesetzt ist.
- Wenn sich alle Knoten eines Clusters in einem lokalen LAN befinden oder über Weiterleitungsfunktionen verfügen, die in der Lage sind, MTU-Paketgrößen (MTU = Maximum Transmission Unit) von mehr als 1.464 Byte auf allen Netzleitwegen zu handhaben, kann die Geschwindigkeit zur Übertragung großer Volumen an Clusternachrichten (größer als 1.536 KB) erheblich verbessert werden, indem die Höhe des Werts für den Clusteroptimierungsparameter *Nachrichtenfragmentgröße* an die Leitweg-MTUs angepasst wird.

Funktionen des neuen Release können nicht genutzt werden.

Wenn Sie beim Versuch, eine Funktion des neuen Release zu verwenden, Fehlnachricht CPFBB70 erhalten, dann ist Ihre aktuelle Clusterversion noch auf die vorherige Version eingestellt. Sie müssen alle Clusterknoten mit dem neuen Release-Level aktualisieren und anschließend die aktuelle Clusterversion über die Schnittstelle zum Anpassen der Clusterversion auf den neuesten Stand bringen. Weitere Informationen finden Sie unter "Clusterversion eines Clusters auf den neuesten Stand bringen".

Einer Einheitendomäne kann kein Knoten hinzugefügt werden, oder es besteht keine Zugriff auf die Clusterverwaltungsschnittstelle des System i Navigator.

Für den Zugriff auf die Clusterverwaltungsschnittstelle des System i Navigator oder zur Verwendung von umschaltbaren Einheiten müssen Sie i5/OS Option 41, HA Switchable Resources, auf Ihrem System installiert haben. Für diese Option müssen Sie über eine gültige Lizenzberechtigung verfügen.

Das angelegte Cluster-PTF funktioniert nicht.

Vergewissern Sie sich, ob Sie nach dem Anlegen des PTF die folgenden Tasks ausgeführt haben:

1. Cluster beenden

2. Abmelden und anschließend wieder anmelden

Das alte Programm ist in der Aktivierungsgruppe so lange aktiv, bis die Aktivierungsgruppe zerstört ist. Der gesamte Clustercode (einschließlich APIS) wird in der Aktivierungsgruppe ausgeführt.

3. Cluster starten

Nach Anlegen der meisten Cluster-PTFs ist es erforderlich, das Clustering auf dem Knoten zu beenden und erneut zu starten, um das PTF zu aktivieren.

CEE0200 wird im Jobprotokoll des Exitprogramms angezeigt.

In dieser Nachricht ist das Ausgangsmodul QLEPM und die Ausgangsprozedur Q_LE_leBdyPeilog. Jedes Programm, das vom Exitprogramm aufgerufen wird, muss entweder in *CALLER oder einer benannte Aktivierungsgruppe ausgeführt werden. Sie müssen das Exitprogramm oder das fehlerhafte Programm ändern, um diesen Zustand zu korrigieren.

CPD000D gefolgt von CPF0001 wird im Jobprotokoll der Cluster Resource Services angezeigt.

Wenn Sie diese Fehlernachricht erhalten, vergewissern Sie sich, dass der Systemwert QMLTTHDACN entweder auf 1 oder 2 gesetzt ist.

Cluster ist anscheinend blockiert.

Prüfen Sie, ob Exitprogramme für Clusterressourcengruppe ausstehen. Verwenden Sie zur Überprüfung des Exitprogramms den Befehl WRKACTJOB (Mit aktiven Jobs arbeiten). Prüfen Sie anschließend, ob in der Spalte 'Funktion' PGM-QCSTCRGEXT angezeigt wird.

Partitionsfehler

Bestimmte Clusterbedingungen lassen sich ohne großen Aufwand korrigieren. Hier erfahren Sie, was zu tun ist, um den Cluster wiederherzustellen, wenn eine Clusterpartition aufgetreten ist. Unter diesem Thema erfahren Sie, wie Sie eine Clusterpartition vermeiden können, und zeigt Ihnen anhand eines Beispiels, wie Sie die Clusterpartitionen wieder zusammenfügen können.

In einem Cluster tritt immer dann eine Clusterpartition ein, wenn der Kontakt zwischen einem oder mehreren Knoten im Cluster verloren geht und ein Ausfall der verloren gegangenen Knoten nicht bestätigt werden kann. Dieser Zustand darf nicht mit einer Partition in einer logischen Partitions Umgebung (LPAR) verwechselt werden.

Wenn Sie Fehlernachricht CPFBB20 entweder im Systemprotokoll (QHST) oder im Jobprotokoll QCSTCTL erhalten, dann ist eine Clusterpartition aufgetreten, und Sie müssen herausfinden, wie Sie den Fehler beheben können. Das folgende Beispiel zeigt eine Clusterpartition, die sich auf einen Cluster mit vier Knoten bezieht: A, B, C und D. Das Beispiel zeigt einen Kommunikationsausfall zwischen den Clusterknoten B und C, der dazu führt, dass der Cluster in zwei Clusterpartitionen geteilt wird. Vor der Clusterpartition bestanden vier Clusterressourcengruppen, die beliebigen Typs sein konnten. Die Clusterressourcengruppen werden hier als CRG A, CRG B, CRG C und CRG D bezeichnet. Das Beispiel zeigt die

Wiederherstellungsdomäne jeder Clusterressourcengruppe.

Tabelle 35. Beispiel für eine Wiederherstellungsdomäne während einer Clusterpartition

Knoten A	Knoten B	x	Knoten C	Knoten D
CRG A (Ausweichknoten1)	CRG A (primär)			
	CRG B (primär)		CRG B (Ausweichknoten1)	
	CRG C (primär)		CRG C (Ausweichknoten1)	CRG C (Ausweichknoten2)
CRG D (Ausweichknoten2)	CRG D (primär)		CRG D (Ausweichknoten1)	
Partition 1			Partition 2	

Ein Cluster wird partitioniert, wenn die maximale Übertragungseinheit (MTU) an einem beliebigen Punkt im Kommunikationspfad kleiner ist als der für die Clusterkommunikation optimierbare Parameter "Nachrichtenfragmentgröße". Die MTU für eine Cluster-IP-Adresse kann mit dem Befehl WRKTCPS (Mit TCP/IP-Netzwerkstatus arbeiten) auf dem betreffenden Knoten geprüft werden. Zusätzlich muss die MTU in jedem Abschnitt des gesamten Kommunikationspfads geprüft werden. Ist die MTU kleiner als die Nachrichtenfragmentgröße, dann muss entweder die MTU für den Pfad erhöht werden oder ein kleinerer Wert für die Nachrichtenfragmentgröße angegeben werden. Mit der API QcstRetrieveCRSInfo (Retrieve Cluster Resource Services Information) können die aktuellen Einstellungen der Optimierungsparameter angezeigt und mit der API QcstChgClusterResourceServices (Change Cluster Resource Services) können sie geändert werden.

Wenn die Ursache für die Clusterpartition behoben ist, erkennt der Cluster die wiederhergestellte Kommunikationsverbindung und gibt Nachricht CPFBB21 entweder im Systemprotokoll (QHST) oder im Jobprotokoll QCSTCTL aus. Diese Nachricht teilt dem Bediener mit, dass der Cluster nach der Clusterpartition wiederhergestellt worden ist. Beachten Sie bitte, dass das Zusammenführen des Clusters nach der Korrektur einige Minuten dauern kann.

Primäre und sekundäre Clusterpartitionen festlegen:

Zum Festlegen der Aktionen für Clusterressourcengruppen, die innerhalb einer Clusterpartition ausgeführt werden können, müssen Sie wissen, ob es sich bei der Partition um eine primäre oder eine sekundäre Partition handelt. Bei Auftreten einer Partitionierung wird jeder im Cluster definierten Clusterressourcengruppe eine Partition entweder als primäre oder als sekundäre Partition zugeordnet.

Bei Sicherungsmodellen mit primärer Partition enthält die primäre Partition den Knoten, der aktuell die Rolle des primären Knotens hat. Alle anderen Partitionen sind sekundär. Die primäre Partition darf nicht für alle Clusterressourcengruppe gleich sein.

Bei einem Peer-Modell gelten die folgenden Partitionsregeln:

- Wenn die Wiederherstellungsdomänenknoten vollständig in einer Partition enthalten sind, dann ist diese Partition die primäre Partition.
- Wenn die Wiederherstellungsdomänenknoten sich über die Partition hinaus erstrecken, gibt es keine primäre Partition. Beide Partitionen sind dann sekundäre Partitionen.
- Wenn die Clusterressourcengruppe aktiv ist und eine bestimmte Partition keine Peerknoten enthält, wird die Clusterressourcengruppe in der betreffenden Partition beendet.
- In einer sekundären Partition sind betriebsrelevante Änderungen zulässig, sofern die für solche Änderungen geltenden Regeln eingehalten werden.
- In einer sekundären Partition sind keine Konfigurationsänderungen erlaubt.

Für die einzelnen CRG-APIs gelten folgende Einschränkungen:

Tabelle 36. Partitionseinschränkungen für CRG-API

CRG-API	Zulässig in primärer Partition	Zulässig in sekundären Partitionen
Add Node to Recovery Domain	X	
Add CRG Device Entry		
Change Cluster Resource Group	X	
Change CRG Device Entry	X	X
Create Cluster Resource Group		
Delete Cluster Resource Group	X	X
Distribute Information	X	X
End Cluster Resource Group ¹	X	
Initiate Switchover	X	
List Cluster Resource Groups	X	X
List Cluster Resource Group Information	X	X
Remove Node from Recovery Domain	X	
Remove CRG Device Entry	X	
Start Cluster Resource Group ¹	X	
Anmerkung:		
1. In allen Partitionen für Peer-CRGs zulässig, wirkt sich aber nur auf die Partition aus, auf der die API ausgeführt wird.		

Auf der Basis dieser Einschränkungen können Clusterressourcengruppen synchronisiert werden, wenn der Cluster nicht mehr partitioniert ist. Bei Wiederaufnahme eines Knotens aus dem partitionierten Status in den Cluster wird die Version der Clusterressourcengruppe in der primären Partition auf die Knoten aus einer sekundären Partition kopiert.

Wenn zwei sekundäre Partitionen für ein Peer-Model zusammengeführt werden, wird die Partition, die eine Clusterressourcengruppe mit dem Status 'Aktiv' enthält, als Gewinner bezeichnet. Haben beide Partitionen denselben Status für die Clusterressourcengruppe, wird die Partition, die den ersten in der CRG-Wiederherstellungsdomäne aufgelisteten Knoten enthält, als Gewinner bezeichnet. Die Version der Clusterressourcengruppe in der Gewinnerpartition wird auf die Knoten in einer anderen Partition kopiert.

Wenn eine Partition erkannt wird, können die APIs Add Cluster Node Entry, Adjust Cluster Version und Create Cluster in keiner der Partitionen ausgeführt werden. Die API Add Device Domain Entry kann nur dann ausgeführt werden, wenn kein Knoten in der Einheitendomäne partitioniert ist. Alle anderen APIs dürfen in jeder beliebigen Partition ausgeführt werden. Die von einer API ausgeführte Aktion ist jedoch nur in der Partition wirksam, in der die API ausgeführt wird.

Status partitionierter Knoten in "Ausgefallen" ändern:

Manchmal wird irrtümlicherweise eine Partitionsbedingung gemeldet, wenn tatsächlich ein Knoten ausgefallen ist. Dies kann vorkommen, wenn die Kommunikation zwischen den Cluster Resource Services und einem oder mehreren Knoten verloren geht, aber nicht erkannt werden kann, ob die Knoten noch betriebsbereit sind. Bei Eintreten dieser Situation gibt es eine einfache Methode, um anzuzeigen, dass der Knoten ausgefallen ist.

Achtung: Durch eine Mitteilung an die Cluster Resource Services, dass ein Knoten ausgefallen ist, wird die Wiederherstellung aus dem Partitionsstatus vereinfacht. Der Knotenstatus sollte jedoch nicht in 'Ausgefallen' geändert werden, wenn der Knoten noch aktiv ist und eine echte Partition stattgefunden hat. Dies könnte zur Folge haben, dass ein Knoten in mehreren Partitionen die primäre Rolle für eine Clusterressourcengruppe übernimmt. Wenn sich zwei Knoten als Primärknoten verhalten, können beispielsweise Dateien oder Datenbanken getrennt oder beschädigt werden, wenn mehrere unterschiedliche Knoten unabhängig voneinander Änderungen an den Kopien ihrer Dateien vornehmen. Außerdem lassen sich zwei Partitionen nicht wieder zusammenfügen, wenn in jeder Partition ein Knoten als Primärknoten zugeordnet wurde.

Wenn der Status eines Knotens in "Ausgefallen" geändert wird, werden die Rollen der Knoten in der Wiederherstellungsdomäne jeder Clusterressourcengruppe in der Partition möglicherweise neu verteilt. Der auf "Ausgefallen" gesetzte Knoten wird als letzter Ausweichknoten zugeordnet. Sind mehrere Knoten ausgefallen, deren Status geändert werden muss, wirkt sich die Reihenfolge, in der die Knoten geändert werden, auf die endgültige Anordnung der Ausweichknoten in der Wiederherstellungsdomäne aus. War der ausgefallene Knoten der Primärknoten einer Clusterressourcengruppe, dann wird der erste aktive Ausweichknoten erneut als neuer Primärknoten zugeordnet.

Wenn die Kommunikation zwischen den Cluster Resource Services und einem Knoten verloren gegangen ist, aber nicht festgestellt werden kann, ob der Knoten noch betriebsbereit ist, hat der Clusterknoten den Status **Keine Übertragung**. Unter Umständen müssen Sie den Status des Knotens von **Keine Übertragung** in **Ausgefallen** ändern. Anschließend müssen Sie den Knoten erneut starten.

Führen Sie die folgenden Schritte aus, um den Status eines Knotens von **Keine Übertragung** in **Fehlgeschlagen** zu ändern:

1. Geben Sie in einem Web-Browser `http://mysystem:2001` ein, wobei `mysystem` der Hostname des Systems ist.
2. Melden Sie sich mit Ihrem Benutzerprofil und Kennwort beim System an.
3. Wählen Sie **Cluster Resource Services** im IBM Systems Director Navigator for i5/OS-Fenster aus.
4. Wählen Sie auf der Seite **Cluster Resource Services** die Task **Mit Clusterknoten arbeiten** aus, um eine Liste der im Cluster befindlichen Knoten aufzurufen.
5. Klicken Sie im Menü **Aktion auswählen** auf **Status ändern**. Ändern Sie den Status auf dem Knoten in "Ausgefallen".

Zugehörige Informationen

Clusterknoten ändern (CHGCLUNODE)

API Change Cluster Node Entry (QcstChangeClusterNodeEntry)

Partitionierte Clusterverwaltungsdomänen:

Beim Arbeiten mit partitionierten Clusterverwaltungsdomänen sollten Sie Folgendes berücksichtigen.

In partitionierten Clusterverwaltungsdomänen werden Änderungen weiterhin unter den aktiven Knoten in jeder Partition synchronisiert. Wenn die Knoten wieder zusammengeführt werden, repliziert die Clusterverwaltungsdomäne alle in den einzelnen Partitionen vorgenommenen Änderungen, damit alle Ressourcen innerhalb der aktiven Domäne konsistent sind. Beachten Sie bitte Folgendes in Bezug auf die Verarbeitung beim Zusammenführen der Knoten für eine Clusterverwaltungsdomäne:

- Wenn alle Partitionen aktiv waren und Änderungen an derselben Ressource in verschiedenen Partitionen vorgenommen wurden, wird beim Zusammenführen die letzte Änderung an der Ressource auf allen Knoten durchgeführt. Der Zeitpunkt der letzten Änderung wird auf der Basis der Weltzeit (UTC) auf jedem Knoten, auf dem eine Änderung vorgenommen wurde, festgelegt.
- Wenn alle Ressourcen inaktiv waren, werden die globalen Werte für jede Ressource auf der Basis der zuletzt im aktiven Zustand einer Partition vorgenommenen Änderung aufgelöst. Die tatsächliche Durchführung der Änderungen auf überwachten Ressourcen erfolgt erst, wenn die Peer-CRG, die die Clusterverwaltungsdomäne darstellt, gestartet wird.

- Wenn vor der Zusammenführung einige Partitionen aktiv und einige inaktiv waren, werden die globalen Werte für die Änderungen, die in aktiven Partitionen vorgenommen wurden, auf die inaktiven Partitionen repliziert. Die inaktiven Partitionen werden anschließend gestartet, wodurch alle anstehenden Änderungen, die auf den Knoten in den inaktiven Partitionen vorgenommen wurden, auf die zusammengeführte Domäne repliziert werden.

Tipps zu Clusterpartitionen:

Verwenden Sie die folgenden Tipps für Ihre Clusterpartitionen.

1. Die Regeln zur Einschränkung des Betriebs innerhalb einer Partition dienen dazu, das Zusammenführen der Partitionen zu erleichtern. Ohne diese Einschränkungen wäre die Wiederherstellung des Cluster sehr arbeitsintensiv.
2. Wenn die Knoten in der Primärpartition zerstört wurden, ist unter Umständen eine besondere Verarbeitung in einer sekundären Partition erforderlich. Diese Situation entsteht am häufigsten durch den Verlust des Standorts, der die primäre Partition enthält. Gehen Sie bei der Wiederherstellung nach Partitionsfehlern anhand des Beispiels vor, das auf der Annahme basiert, dass Partition 1 zerstört wurde. In diesem Fall muss sich der primäre Knoten für Clusterressourcengruppen B, C und D in Partition 2 befinden. Die einfachste Methode zur Wiederherstellung besteht darin, den Status für Knoten A und Knoten B mit dem Befehl CHGCLUNODE (CST-Knoteneintrag ändern) auf "Ausgefallen" zu setzen. Weitere Informationen finden Sie unter "Status partitionierter Knoten in "Ausgefallen" ändern". Eine Wiederherstellung kann auch manuell erfolgen. Führen Sie hierzu die folgenden Schritte aus:

- a. Entfernen Sie die Knoten A und B aus dem Cluster in Partition 2. Partition 2 ist jetzt der Cluster.
- b. Richten Sie die erforderlichen logischen Replikationsumgebungen im neuen Cluster ein. API Start Cluster Resource Group API/CL-Befehl usw.

Da Knoten aus der Clusterdefinition in Partition 2 entfernt wurden, wird ein Versuch, Partition 1 und Partition 2 zusammenzuführen, fehlschlagen. Führen Sie die API Delete Cluster (QcstDeleteCluster) auf jedem Knoten in Partition 1 aus, um die Diskrepanz zu beheben. Fügen Sie dann die Knoten aus Partition 1 dem Cluster hinzu, und richten Sie alle CRG-Definitionen, Wiederherstellungsdomänen und die logische Replikation wieder ein. Diese Vorgehensweise ist sehr arbeitsintensiv und fehleranfällig. Es ist wichtig, dass die Prozedur nur im Falle eines Standortverlusts ausgeführt wird.

3. Die Verarbeitung der Operation zum Starten eines Knotens hängt vom Status des zu startenden Knotens ab:

Der Knoten ist entweder ausgefallen oder er wurde durch die Operation "Knoten beenden" beendet.

- a. Auf dem Knoten, der hinzugefügt werden soll, werden die Cluster Resource Services gestartet.
- b. Die Clusterdefinition wird von einem aktiven Knoten im Cluster auf den zu startenden Knoten kopiert.
- c. Jede Clusterressourcengruppe, zu deren Wiederherstellungsdomäne der zu startende Knoten gehört, wird von einem aktiven Knoten im Cluster auf den zu startenden Knoten kopiert. Es werden keine Clusterressourcengruppen vom zu startenden Knoten auf einen aktiven Knoten im Cluster kopiert.

Der Knoten ist ein partitionierter Knoten:

- a. Die Clusterdefinition eines aktiven Knotens wird mit der Clusterdefinition des zu startenden Knotens verglichen. Wenn die Definitionen identisch sind, wird der Startvorgang als Operation zum Zusammenführen fortgesetzt. Wenn die Definitionen voneinander abweichen, wird das Zusammenführen gestoppt, und der Benutzer muss manuell eingreifen.
- b. Wird der Vorgang zum Zusammenführen fortgesetzt, wird der Status des Knotens, der gestartet wird, in "Aktiv" geändert.
- c. Jede Clusterressourcengruppe, zu deren Wiederherstellungsdomäne der zu startende Knoten gehört, wird von der primären Partition der Clusterressourcengruppe in die sekundäre Partition der Clusterressourcengruppe kopiert. Clusterressourcengruppen können von dem zu startenden Knoten auf Knoten kopiert werden, die im Cluster bereits aktiv sind.

Wiederherstellung von Clustern

Lesen Sie, wie eine Wiederherstellung nach anderen möglichen Clusterausfällen ausgeführt wird.

Wiederherstellung nach Clusterjobfehlern:

Das Fehlschlagen eines Cluster Resource Services-Jobs deutet meistens auf ein anderes Problem hin.

Suchen Sie im Jobprotokoll, das den fehlgeschlagenen Job enthält nach Nachrichten, die die Fehlerursache beschreiben. Korrigieren Sie die Fehler.

Verwenden Sie den Befehl CHGCLURCY (Clusterwiederherstellung ändern), um einen CRG-Job, der beendet wurde, neu zu starten, ohne das Clustering auf dem Knoten beenden und neu starten zu müssen.

1. CHGCLURCY CLUSTER(EXAMPLE)CRG(CRG1)NODE(NODE1)ACTION(*STRCRGJOB) Mit diesem Befehl wird der CRG-Job, CRG1, auf dem Knoten NODE1 übergeben. Damit der CRG-Job auf NODE1 gestartet werden kann, muss das Clustering auf NODE1 aktiv sein.
2. Clustering auf dem Knoten erneut starten

Wenn Sie ein Clusterverwaltungsprodukt von einem IBM Business Partner verwenden, lesen Sie die mit dem Produkt gelieferte Dokumentation.

Zugehörige Informationen

Clusterwiederherstellung ändern (CHGCLURCY)

Beschädigtes Clusterobjekt wiederherstellen:

Obwohl es sehr unwahrscheinlich ist, dass ein Objekt beschädigt wird, kann es trotzdem vorkommen, dass Objekte der Cluster Resource Services beschädigt werden.

Vom System wird versucht, vorausgesetzt es befindet sich im Modus "Aktiv", eine Wiederherstellung von einem anderen Knoten im Cluster durchzuführen. Das System wird die folgenden Fehlerbehebungsmaßnahmen durchführen:

Bei einem beschädigten internen Objekt

1. Der beschädigte Knoten wird beendet.
2. Befindet sich mindestens ein weiterer aktiver Knoten im Cluster, wird sich der beschädigte Knoten automatisch neu starten, um wieder in den Cluster aufgenommen zu werden. Durch den Wiederaufnahmeprozess wird der Schaden behoben.

Bei einer beschädigten Clusterressourcengruppe

1. Auf dem Knoten mit der beschädigten Clusterressourcengruppe wird jede derzeit ausgeführte Operation fehlschlagen, die der beschädigten Clusterressourcengruppe zugeordnet ist. Das System versucht automatisch, die Clusterressourcengruppe von einem anderen aktiven Knoten wiederherzustellen.
2. Befindet sich mindestens ein aktives Mitglied in der Wiederherstellungsdomäne, dann funktioniert die Wiederherstellung der Clusterressourcengruppe. Andernfalls wird der Job beendet.

Wenn das System keine anderen aktiven Knoten identifizieren oder erreichen kann, müssen Sie diese Wiederherstellungsschritte ausführen.

Bei einem beschädigten internen Objekt

Sie erhalten einen internen Clusteringfehler (CPFBB46, CPFBB47 oder CPFBB48).

1. Beenden Sie das Clustering für den beschädigten Knoten.

2. Starten Sie das Clustering erneut für den beschädigten Knoten. Führen Sie diese Maßnahme von einem anderen aktiven Knoten im Cluster aus.
3. Wenn das Problem nach Ausführung der Schritte 1 und 2 nicht gelöst ist, entfernen Sie den beschädigten Knoten aus dem Cluster.
4. Nehmen Sie das System wieder in den Cluster und in die Wiederherstellungsdomäne für die entsprechenden Clusterressourcengruppen auf.

Bei einer beschädigten Clusterressourcengruppe

Sie erhalten einen Fehlerstatus, aus dem hervorgeht, dass ein Objekt beschädigt ist (CPF9804).

1. Beenden Sie das Clustering auf dem Knoten, der die beschädigte Clusterressourcengruppe enthält.
2. Löschen Sie die CRG mit dem Befehl DLTCRG.
3. Wenn sich kein weiterer aktiver Knoten im Cluster befindet, der ein CRG-Objekt enthält, führen Sie die Wiederherstellung von Datenträger durch.
4. Starten Sie das Clustering auf dem Knoten, der die beschädigte Clusterressourcengruppe enthält. Diese Maßnahme kann auf jedem beliebigen Knoten ausgeführt werden.
5. Beim Starten des Clustering führt das System eine Resynchronisation aller Clusterressourcengruppen aus. Möglicherweise müssen Sie die Clusterressourcengruppe neu erstellen, wenn kein anderer Knoten im Cluster die Clusterressourcengruppe enthält.

Clusterwiederherstellung nach Komplettausfall:

Verwenden Sie diese Informationen zusammen mit der Prüfliste unter dem Thema "Wiederherstellung des Systems", um das gesamte System nach einem Komplettausfall aufgrund eines unerwarteten Stromausfalls wiederherzustellen.

Szenario 1: Wiederherstellung auf dem selben System

1. Zur Vermeidung von Inkonsistenzen in den Angaben zur Einheitendomäne zwischen dem lizenzierten internen Code und und i5/OS wird empfohlen, dass Sie den lizenzierten internen Code unter Verwendung von Option 3 (Install Licensed Internal Code and Recover Configuration) installieren.

Anmerkung: Damit die Operation "Install Licensed Internal Code and Recover Configuration" erfolgreich durchgeführt werden kann, müssen Sie dieselben Platteneinheiten haben -- mit Ausnahme der IPL-Platteneinheit, wenn diese ausgefallen ist. Sie müssen auch dasselbe Release wiederherstellen

2. Folgen Sie nach der Installation des lizenzierten internen Codes bitte der Prozedur für Recovering Your Disk Configuration unter dem Thema *Wiederherstellung des Systems*. Mithilfe dieser Vorgehensweise können Sie vermeiden, dass Sie die Plattenpools erneut konfigurieren müssen.
3. Nach der Wiederherstellung Ihrer Systeminformationen können Sie das Clustering auf dem gerade wiederhergestellten Knoten neu zu starten. Zum Starten des Clustering muss der Knoten aktiv sein. Dadurch werden die aktuellen Konfigurationsinformationen auf dem wiederhergestellten Knoten repliziert.

Szenario 2: Wiederherstellung auf einem anderen System

Überprüfen Sie nach der Wiederherstellung der Systeminformationen das Jobprotokoll, um sicherzustellen, dass alle Objekte wiederhergestellt wurden. Führen Sie dann die folgenden Schritte aus, um die korrekte Konfiguration für die Clustereinheitendomäne zu erhalten.

1. Löschen Sie den Cluster auf dem gerade wiederhergestellten Knoten.
2. Führen Sie auf dem aktiven Knoten die folgenden Schritte aus:
 - a. Entfernen Sie den wiederhergestellten Knoten aus dem Cluster.
 - b. Fügen Sie den wiederhergestellten Knoten dem Cluster wieder hinzu.

- c. Fügen Sie den wiederhergestellten Knoten der Einheitendomäne hinzu.
- d. Erstellen Sie die Clusterressourcengruppe oder fügen Sie den Knoten der Wiederherstellungsdomäne hinzu.

Clusterwiederherstellung nach Katastrophenfall:

Nach einem Katastrophenfall, bei dem alle Knoten verloren gehen, muss der Cluster neu konfiguriert werden.

Zur Vorbereitung auf ein solches Szenario wird empfohlen, die Clusterkonfigurationsdaten zu speichern und eine Druckausgabe der Angaben auf Papier aufzubewahren.

Cluster von Sicherungsbändern wiederherstellen:

Während des normalen Systembetriebs sollten Sie keine Wiederherstellung von einem Sicherungsband durchführen.

Diese Art der Wiederherstellung ist nur erforderlich, wenn ein Katastrophenfall eintritt und alle Knoten in Ihrem Cluster verloren gegangen sind. Nach einem solchen Katastrophenfall führen Sie Ihre normalen Wiederherstellungsprozeduren durch, die Sie nach Erstellung Ihrer Sicherungs- und Wiederherstellungsstrategie etabliert haben.

Fehlerbehebung bei standortübergreifender Spiegelung

Type **your** text here.

- an interesting point
- another interesting point

Subheading

Here's a little section in a concept.

Example

Here's a little example section in a concept.

Nachrichten für geographische Spiegelung

Zur Lösung von Problemen mit der geographischen Spiegelung lesen Sie die Beschreibungen und Fehlerbehebungsmaßnahmen in den Nachrichten zur geographischen Spiegelung.

0x00010259

Beschreibung: Operation fehlgeschlagen, da die Spiegelkopie vom System nicht gefunden wurde.

Fehlerbehebung: Nicht alle Knoten in der Einheitendomäne haben reagiert.. Vergewissern Sie sich, dass das Clustering aktiv ist. Starten Sie gegebenenfalls Cluster auf dem Knoten. Nähere Informationen finden Sie unter „Knoten starten“ auf Seite 99. Anschließend die Anforderung wiederholen. Besteht das Problem weiterhin, die technische Unterstützung benachrichtigen.

0x0001025A

Beschreibung: Nicht alle Plattenpools in der Plattenpoolgruppe sind geographisch gespiegelt.

Fehlerbehebung: Wenn ein Plattenpool in einer Plattenpoolgruppe geographisch gespiegelt wird, müssen alle Plattenpools in der Plattenpoolgruppe ebenfalls geographisch gespiegelt werden. Führen Sie eine der folgenden Aktionen aus:

1. Konfigurieren Sie die geographische Spiegelung der Plattenpools, die nicht geographisch gespiegelt wurden.

2. Dekonfigurieren Sie die geographische Spiegelung der Plattenpools, die geographisch gespiegelt wurden.

0x00010265

Beschreibung: Die abgehängte gespiegelte Kopie ist verfügbar.

Fehlerbehebung: Sperren Sie die abgehängte Kopie, und wiederholen Sie anschließend die Operation zum Wiederanhängen.

0x00010380

Beschreibung: Eine Platteneinheit fehlt in der Konfiguration der Spiegelkopie.

Fehlerbehebung: Finden oder korrigieren Sie die fehlende Platteneinheit in der Spiegelkopie. Überprüfen Sie das Produktaktivitätenprotokoll auf dem Zielknoten. Fordern Sie den IOP-Cache-Speicher zurück.

0x00011210

Beschreibung: Der für die Plattenpoolgruppe vorgesehene sekundäre Plattenpool wurde nicht geographisch gespiegelt.

Fehlerbehebung: Wenn ein Plattenpool in einer Plattenpoolgruppe geographisch gespiegelt wird, müssen alle Plattenpools in der Plattenpoolgruppe ebenfalls geographisch gespiegelt werden. Für den vorgesehenen sekundären Plattenpool, der nicht geographisch gespiegelt wurde, müssen Sie entweder jetzt oder nach Abschluss dieser Operation die geographische Spiegelung konfigurieren.

0x00011211

Beschreibung: doppelte Spiegelkopien vorhanden.

Fehlerbehebung: Überprüfen Sie, ob lokal gespiegelte Platteneinheiten auf zwei Systemen, Enterprise Storage Server FlashCopy, oder Kopien unabhängiger Plattenpools mit einem alten Stand vorhanden sind. Weitere Informationen finden Sie im Aktivitätenprotokoll auf dem Knoten der Spiegelkopie. Löschen Sie die doppelt vorhandenen Exemplare, und wiederholen Sie die Anforderung. Besteht das Problem weiterhin, die i5/OS technische Unterstützung benachrichtigen, um nähere Informationen über die IBM Unterstützungsfunktion und Services zu erfahren.

Haftungsausschluss für Programmcode

IBM erteilt Ihnen eine nicht ausschließliche Copyrightlizenz für die Nutzung aller Programmcodebeispiele, aus denen Sie ähnliche Funktionen generieren können, die an Ihre spezifischen Anforderungen angepasst sind.

Vorbehaltlich einer gesetzlichen Gewährleistung, die nicht ausgeschlossen werden kann, geben IBM oder ihre Programmentwickler und Lieferanten keine ausdrückliche oder implizite Gewährleistung für die Marktfähigkeit, die Eignung für einen bestimmten Zweck oder die Freiheit von Rechten Dritter in Bezug auf das Programm oder die technische Unterstützung.

Auf keinen Fall sind IBM oder ihre Programmentwickler und Lieferanten in folgenden Fällen haftbar, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde:

1. Verlust oder Beschädigung von Daten;
2. direkte, unmittelbare, mittelbare oder sonstige Folgeschäden; oder
3. entgangener Gewinn, entgangene Geschäftsabschlüsse, Umsätze, Schädigung des guten Namens oder Verlust erwarteter Einsparungen.

Einige Rechtsordnungen erlauben nicht den Ausschluss oder die Begrenzung von Folgeschäden, so dass einige oder alle der obigen Einschränkungen und Ausschlüsse möglicherweise nicht anwendbar sind.

| **Lizenzprogramm IBM System i High Availability Solutions Manager (iHASM) installieren**

| Bevor Sie eine i5/OS-Hochverfügbarkeitslösung installieren können, müssen Sie IBM System i High Availability Solutions Manager (iHASM), Lizenzprogrammnummer, 5761-HAS, auf jedem System installieren, das Teil der Hochverfügbarkeitslösung sein soll.

| Vor der Installation des Lizenzprogramms iHASM sollten Sie die folgenden Installationsvoraussetzungen erfüllt haben:

- | 1. Installieren Sie V6R1 i5/OS, oder führen Sie ein Upgrade auf diese Version durch.
- | 2. Installieren Sie i5/OS Option 41 (HA Switchable Resources).

| Führen Sie die folgenden Schritte aus, um das Lizenzprogramm iHASM zu installieren:

- | 1. Geben Sie in einer Befehlszeile GO LICPGM ein.
- | 2. Treffen Sie in der Anzeige "Mit Lizenzprogrammen arbeiten" Auswahl 11 (Lizenzprogramme installieren).
- | 3. Wählen Sie Produkt 5761-HAS, Option *BASE aus, um iHASM für das System i-Produkt zu installieren. Drücken Sie die Eingabetaste.
- | 4. Wenn die Anzeige "Installationsauswahl" erscheint, geben Sie den angeforderten Namen der Installationseinheit ein. Drücken Sie die Eingabetaste, um die Installation zu starten.

Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellsprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Informationen zu Programmierschnittstellen

In der vorliegenden Veröffentlichung werden vorgesehene Programmierschnittstellen dokumentiert, mit deren Hilfe Kunden Programme für den Zugriff auf die Services von IBM i5/OS schreiben können.

Marken

Folgende Namen sind Marken der IBM Corporation in den USA und/oder anderen Ländern:

i5/OS
IBM
IBM (Logo)
System i
System i5
IBM Systems Storage
TotalStorage
FlashCopy

- | Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.
- | Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- | Java und alle auf Java basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.

IBM