IBM

eserver

iSeries

Planung einer Sicherungs- und Wiederherstellungsstrategie

Version 5 Release 3

IBM

@server

iSeries

Planung einer Sicherungs- und Wiederherstellungsstrategie

Version 5 Release 3

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen", auf Seite 19 gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. 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.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

| **Sechste Ausgabe (August 2005)**

| Diese Ausgabe bezieht sich auf Version 5, Release 3, Modifikation 2 von IBM Operating System/400 (5722–SS1) und
| auf alle nachfolgenden Releases und Modifikationen, sofern in neuen Ausgaben nicht anders angegeben. Diese Version läuft nicht auf CISC-Modellen und nicht auf allen RISC-Modellen (RISC - reduced instruction set computer).

| Diese Veröffentlichung ist eine Übersetzung des Handbuchs
| *IBM @server iSeries Planning a backup and recovery strategy,*
| herausgegeben von International Business Machines Corporation, USA

| 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
| Mai 2005

Inhaltsverzeichnis

Planung einer Sicherungs- und Wiederherstellungsstrategie

Computer sind im Allgemeinen sehr zuverlässig, ganz besonders gilt dies für den iSeries-Server. Sie können Ihr System monate- oder sogar jahrelang einsetzen, ohne dass Störungen auftreten, die zum Datenverlust auf Ihrem System führen. In demselben Maße wie die Häufigkeit von Problemen abgenommen hat, haben die potenziellen Auswirkungen von Problemen jedoch ein kritisches Maß angenommen. Unternehmen sind immer mehr von Computern und den darauf gespeicherten Informationen abhängig. Unter Umständen gibt es keine Sicherungen Ihrer auf dem Computer gespeicherten Daten.

Die Datensicherung auf Ihrem System ist zeitaufwendig und erfordert Disziplin. Warum also sollten Sie eine Datensicherung durchführen? Warum Zeit für die Planung und Bewertung der Datensicherung aufwenden?

Die Antwort ist einfach: Weil sonst unter Umständen Probleme auf Sie zukommen. Sie werden irgendwann auf Sicherungskopien Ihrer Daten zurückgreifen **müssen**, da bei jedem System früher oder später, aus welchen Gründen auch immer, die gesamten Daten oder Teile davon zurückgespeichert werden müssen.

Der Zeitrahmen für die Sicherung und Wiederherstellung stellt eine Übersicht der oberen Ebene über die Ereignisse bereit, die während des Sicherungs- und Wiederherstellungsprozesses auftreten.

Sobald Sie den Zeitrahmen für die Sicherung und Wiederherstellung studiert haben, können Sie mit dem Planen Ihrer Strategie beginnen. Führen Sie folgende Schritte aus:
1. Zu sichernde Daten und Häufigkeit der Sicherungen festlegen
2. Sicherungsfenster bestimmen
3. Verfügbarkeitsoptionen auswählen
4. Strategie testen

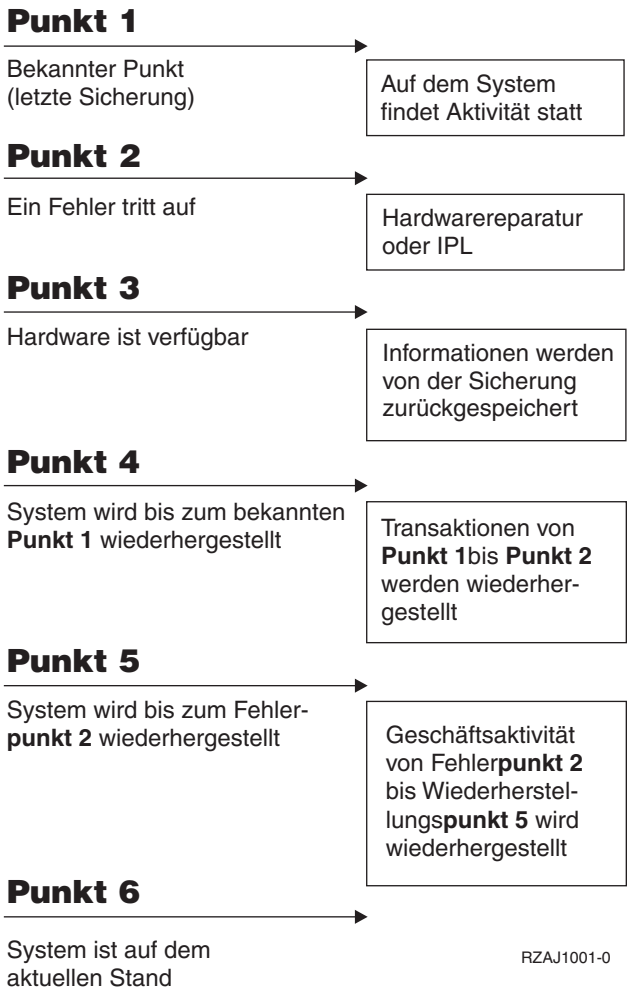
Die Schablone für den Plan zur Wiederherstellung nach einem Katastrophenfall kann als Planungsressource hilfreich sein.

Dieses Thema enthält Informationen zum Planen einer Strategie und zu den Auswahlen, die Sie beim Konfigurieren Ihres Systems hinsichtlich der Sicherung, Wiederherstellung und Verfügbarkeit treffen müssen. Informationen darüber, wie die einzelnen Tasks tatsächlich ausgeführt werden, siehe Thema Sicherung und Wiederherstellung  und Backup your server. Das Thema Availability roadmap for your iSeries server enthält Informationen über allgemeine Arten von Fehlern, die auftreten können.

Zeitrahmen für Sicherung und Wiederherstellung

Der Zeitrahmen für die Sicherung und Wiederherstellung beginnt, wenn Sie Informationen sichern, und endet, wenn Ihr System nach einem Ausfall vollständig wiederhergestellt wurde. Berücksichtigen Sie diesen Zeitrahmen, wenn Sie die nachfolgenden Informationen lesen und Entscheidungen treffen. Ihre Strategie für die Sicherung und Verfügbarkeit legt Folgendes fest:
- Ob Sie jeden Schritt im Diagramm erfolgreich ausführen können
- Wie lange Sie für die Ausführung jedes Schritts benötigen

Verwenden Sie beim Lesen das Diagramm, um spezifische Beispiele zu entwickeln. Was wäre, wenn der bekannte Punkt (1) ein Sonntagabend und der Fehlerpunkt (2) ein Donnerstag Nachmittag ist? Wie lange dauert es, zum bekannten Punkt zurückzukehren? Wie lange dauert es, zum aktuellen Punkt (6) zu gelangen? Ist dies mit der von Ihnen geplanten Sicherungsstrategie überhaupt möglich?



Imagebeschreibung

Die Beschreibung für das Zeitrahmenimage lautet wie folgt:

1. Punkt 1: Bekannter Punkt (letzte Sicherung). Auf dem System findet Aktivität statt.
2. Punkt 2: Ein Fehler tritt auf. Hardware muss repariert werden oder es wird ein IPL durchgeführt.
3. Punkt 3: Hardware ist verfügbar. Die Daten werden von der Sicherung zurückgespeichert.
4. Punkt 4: Das System wird beim bekannten Punkt 1 wiederhergestellt. Transaktionen von Punkt 1 bis Punkt 2 werden wiederhergestellt.
5. Punkt 5: Das System wird beim Fehlerpunkt 2 wiederhergestellt. Geschäftsaktivität von Fehlerpunkt 2 bis Wiederherstellungspunkt 5 wird wiederhergestellt.
6. Punkt 6: Das System ist auf dem aktuellen Stand.

Zu sichernde Daten und Häufigkeit der Sicherungen festlegen

Sie sollten alle Daten in Ihrem System so oft wie möglich sichern. Wenn Sie nicht regelmäßig alle Daten sichern, können Sie bei einem Standortverlust oder bei bestimmten Arten von Plattenfehlern unter Umständen keine Wiederherstellung durchführen. Wenn Sie die geeigneten Teile Ihres iSeries-Servers sichern, können Sie bis zu Punkt 4, der bei Zeitrahmen für Sicherung und Wiederherstellung gezeigt wird, wiederherstellen (letzte Sicherung). Teile des Systems, die häufigen Änderungen unterliegen, sollten Sie täglich sichern. Alle anderen Teile sollten wöchentlich gesichert werden.

Teile des Systems, die häufigen Änderungen unterliegen

Die nachfolgende Tabelle zeigt die Teile des Systems, die sich oft ändern und deshalb täglich gesichert werden sollten:

Tabelle 1. Täglich zu sichernde Daten: Teile des Systems, die sich oft ändern

Beschreibung des Systembestandteils	Von IBM geliefert?	Wann Änderungen auftreten
Sicherheitsinformationen (Benutzerprofile, persönliche Berechtigungen, Berechtigungslisten)	Einige	Regelmäßig: Wenn neue Benutzer und Objekte hinzugefügt werden oder Berechtigungen sich ändern[1]
Konfigurationsobjekte in QSYS	Nein	Regelmäßig: Wenn Einheitenbeschreibungen hinzugefügt oder geändert werden oder wenn Sie die Funktion Hardware Service Manager verwenden, um Konfigurationsdaten zu aktualisieren[1]
Von IBM gelieferte Bibliotheken, die Benutzerdaten enthalten (QGPL, QUSRSYS)	Ja	Regelmäßig
Benutzerbibliotheken, die Benutzerdaten und Programme enthalten	Nein	Regelmäßig
Ordner und Dokumente	Einige	Regelmäßig, wenn Sie diese Objekte verwenden
Verteilungsoperationen	Nein	Regelmäßig, wenn Sie die Verteilungsfunktion verwenden
Benutzerverzeichnisse	Nein	Regelmäßig

[1] Diese Objekte ändern sich unter Umständen auch dann, wenn Sie lizenzierte Programme aktualisieren.

Teile des Systems, die sich nicht oft ändern

Die nachfolgende Tabelle zeigt die Teile des Systems, die sich nicht oft ändern und deshalb auf wöchentlicher Basis gesichert werden können:

Tabelle 2. Wöchentlich zu sichernde Daten: Teile des Systems, die sich nicht oft ändern

Beschreibung des Systembestandteils	Von IBM geliefert?	Wann Änderungen auftreten
lizenzierter interner Code	Ja	PTFs oder ein neues Release des Betriebssystems
Betriebssystemobjekte in der Bibliothek QSYS	Ja	PTFs oder ein neues Release des Betriebssystems
Optionale Bibliotheken von Betriebssystem IBM OS/400 (QHLPSYS, QUSRTOOL)	Ja	PTFs oder ein neues Release des Betriebssystems
Lizenzprogrammbibliotheken (QRPG, QCBL, Qxxxx)	Ja	Änderungen an Lizenzprogrammen
Lizenzprogrammordner (Qxxxxxxx)	Ja	Änderungen an Lizenzprogrammen
Lizenzprogrammverzeichnisse (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Ja	Änderungen an Lizenzprogrammen

Sicherungsfenster bestimmen

In der Praxis hängt es von der Größe Ihres Sicherungsfensters ab, wann und wie Sie Sicherungsprozeduren ausführen und welche Daten Sie sichern. Unter dem **Sicherungsfenster** versteht man die Zeitspanne, in der Ihr System nicht für Benutzer zur Verfügung steht, da Sie Sicherungsoperationen ausführen. Zur Vereinfachung der Wiederherstellung müssen Sie zu dem Zeitpunkt sichern, wenn sich das System an einem bekannten Punkt befindet und sich die Daten nicht ändern.

Beim Erstellen einer Sicherungsstrategie müssen Sie die Systemverfügbarkeit für die Benutzer (d. h. welches Sicherungsfenster für die Benutzer akzeptabel ist) gegen den Wert der Daten, die unter Umständen verloren gehen, und den Zeitaufwand für die Wiederherstellung abwägen.

Wenn Ihr System so essenziell für Ihr Unternehmen ist, dass Sie über kein akzeptables Sicherungsfenster verfügen, können Sie sich wahrscheinlich auch keinen unvorhergesehenen Systemausfall leisten. In diesem Fall sollten Sie ernsthaft alle Verfügbarkeitsoptionen des iSeries-Servers, einschließlich Cluster, einer Bewertung unterziehen. Das Thema Availability roadmap for your iSeries server enthält weitere Informationen über Verfügbarkeitsoptionen.

Wählen Sie abhängig von der Größe Ihres Sicherungsfensters eine der nachfolgend beschriebenen Sicherungsstrategien aus. Bewerten Sie dann Ihre Entscheidung im Hinblick darauf, welche Möglichkeiten Ihnen die Sicherungsstrategie für eine Wiederherstellung bietet, nochmals neu.

- Einfache Sicherungsstrategie
  ;> Ihnen steht täglich ein ausgedehntes Sicherungsfenster mit acht bis zwöf Stunden zur Verfügung, in dem keine Systemaktivität stattfindet (einschließlich Stapelbetrieb).
- Mittlere Sicherungsstrategie
  ;> Ihnen steht täglich ein enger bemessenes Sicherungsfenster (vier bis sechs Stunden) zur Verfügung, in dem keine Systemaktivität stattfindet.
- Komplexe Sicherungsstrategie
  ;>Sie verfügen nur über ein enges Sicherungsfenster, so dass das System, abgesehen von wenigen Ausnahmen, ständig für interaktive Tätigkeiten oder für den Stapelbetrieb verwendet wird.

Einfache Sicherungsstrategie

Die einfachste Sicherungsstrategie besteht darin, alle Daten jede Nacht (oder außerhalb der Betriebszeiten) zu sichern. Dazu können Sie mit Option 21 (Gesamtes System) im Menü SICHERN arbeiten. Sie können Option 21 so terminieren, dass die Sicherung ohne Bedienereingriff (nichtüberwacht) zu einem bestimmten Zeitpunkt ausgeführt wird.

Sie können diese Methode auch für die Sicherung Ihres gesamten Systems nach einem Upgrade auf ein neues Release oder nach dem Installieren von vorläufigen Programmkorrekturen (PTFs) verwenden.

Möglicherweise stellen Sie fest, dass Ihnen nicht genügend Zeit zur Verfügung steht bzw. nicht genügend Bandeinheiten vorhanden sind, um Option 21 ohne einen Bediener auszuführen. In diese Fall können Sie dennoch eine einfache Strategie verfolgen:

Täglich	Alle Daten sichern, die sich oft ändern.
Wöchentlich	Alle Daten sichern, die sich nicht oft ändern.

Option 23 (Alle Benutzerdaten) im Menü SICHERN sichert die Daten, die regelmäßig geändert werden. Option 23 kann so terminiert werden, dass sie nichtüberwacht ausgeführt wird. Dazu müssen allerdings genügend Online-Sicherungsdatenträger zur Verfügung stehen.

Wenn Ihr System an Wochenenden längere Zeit nicht benutzt wird, könnte Ihre Sicherungsstrategie wie folgt aussehen:

Freitagnacht	Menü SICHERN, Option 21
Montagnacht	Menü SICHERN, Option 23
Dienstagnacht	Menü SICHERN, Option 23
Mittwochnacht	Menü SICHERN, Option 23
Donnerstagnacht	Menü SICHERN, Option 23
Freitagnacht	Menü SICHERN, Option 21

Mittlere Sicherungsstrategie

Möglicherweise stellen Sie fest, dass Ihr Sicherungsfenster nicht groß genug ist, um eine einfache Sicherungsstrategie zu verfolgen. Gründe dafür können umfangreiche Stapeljobs sein, die nachts ausgeführt werden müssen. Oder Sie haben sehr große Dateien, für deren Sicherung viel Zeit benötigt wird. Wenn dies der Fall ist, müssen Sie unter Umständen eine mittlere Sicherungsstrategie entwickeln, d. h. für die Sicherung und Wiederherstellung muss ein Mittelweg gewählt werden.

Beim Entwickeln einer mittleren Sicherungsstrategie sollten Sie nach folgendem Prinzip vorgehen: Je öfter Daten geändert werden, desto öfter sollten sie gesichert werden. Sie müssen bei der Auswertung der Häufigkeit von Datenänderungen mehr ins Detail gehen als bei einer einfachen Strategie.

Für eine mittlere Sicherungsstrategie stehen mehrere Methoden zur Verfügung. Sie können eine davon verwenden oder eine Kombination aus verschiedenen Methoden.

- Geänderte Objekte sichern
- Objekte aufzeichnen und die Journalempfänger sichern

Geänderte Objekte sichern

Sie können mit mehreren Befehlen arbeiten, um nur die Informationen zu sichern, die seit der letzten Sicherungsoperation bzw. seit einem bestimmten Datum und einer bestimmten Uhrzeit geändert wurden.

Mit dem Befehl SAVCHGOBJ (Save Changed Objects - Geänderte Objekte sichern) können Sie nur die Objekte sichern, die seit der letzten Sicherung einer Bibliothek oder einer Gruppe von Bibliotheken geändert wurden. Dies kann besonders dann hilfreich sein, wenn sich Programme und Datendateien in derselben Bibliothek befinden. In der Regel werden Datendateien häufig und Programme seltener geändert. Der Befehl SAVCHGOBJ erlaubt es Ihnen, lediglich die Dateien zu sichern, die geändert wurden.

Der Befehl SAVDLO (Save Document Library Object - Dokumentbibliotheksobjekt sichern) ermöglicht es, nur Dokumente und Ordner zu sichern, die sich geändert haben. Analog können Sie mit dem Befehl SAV (Save- Sichern) Objekte in Verzeichnissen sichern, die sich seit einem bestimmten Zeitpunkt geändert haben.

Sie könnten sich auch für das Sichern von geänderten Objekten entscheiden, wenn die Stapelauslastung in manchen Nächten größer als gewöhnlich ist. Beispiel:

Tag	Stapelauslastung	Sicherungsoperation
Freitagnacht	Gering	Menü SICHERN, Option 21
Montagnacht	Groß	Nur Änderungen sichern [1]
Dienstagnacht	Gering	Menü SICHERN, Option 23
Mittwochnacht	Groß	Nur Änderungen sichern [1]
Donnerstagnacht	Groß	Nur Änderungen sichern [1]
Freitagnacht	Gering	Menü SICHERN, Option 21

[1] Verwenden Sie eine Kombination aus den Befehlen SAVCHGOBJ, SAVDLO und SAV.

Objekte aufzeichnen und Journalempfänger sichern

Wenn die Sicherungsoperationen für Datenbankdateien zu lange dauern, da die Dateien umfangreich sind, hilft es Ihnen nicht, geänderte Objekte zu sichern. Wenn Sie eine Teildatei mit 100 000 Sätzen haben und sich auch nur ein einziger Satz darin ändert, sichert der Befehl SAVCHGOBJ die gesamte Teildatei. In diesem Fall stellt das Aufzeichnen Ihrer Datenbankdateien und das regelmäßige Sichern der Journalempfänger unter Umständen eine bessere Lösung dar, selbst wenn sich die Wiederherstellung komplexer gestaltet.

Ein ähnliches Prinzip gilt bei IFS-Objekten und -Datenbereichen (IFS - Integrated File System). Wenn Ihre Sicherungsoperationen für IFS-Objekte und -Datenbereiche zu lange dauern, können Sie die Objekte aufzeichnen und die Sicherungsoperationen effizienter gestalten. Das Sichern von Journalempfänger ist unter Umständen die bessere Option.

Beim Aufzeichnen von Objekten schreibt das System eine Kopie jeder Objektänderung in einen Journalempfänger. Wenn Sie einen Journalempfänger sichern, werden lediglich die geänderten Teile des Objekts gesichert, nicht das gesamte Objekt.

Wenn Sie Objekte aufzeichnen und die Stapelauslastung variiert, könnte Ihre Sicherungsstrategie wie folgt aussehen:

Tag	Stapelauslastung	Sicherungsoperation
Freitagnacht	Gering	Menü SICHERN, Option 21
Montagnacht	Groß	Journalempfänger sichern
Dienstagnacht	Gering	Menü SICHERN, Option 23
Mittwochnacht	Groß	Journalempfänger sichern
Donnerstagnacht	Groß	Journalempfänger sichern
Freitagnacht	Gering	Menü SICHERN, Option 21

Anmerkungen:

1. Um sich den Schutz, den die Aufzeichnung bietet, zunutze zu machen, sollten Sie die Journalempfänger regelmäßig abhängen und sichern. Wie oft sie gesichert werden sollten, hängt von der Anzahl der aufgezeichneten Änderungen ab. Vielleicht ist es in Ihrem Fall angebracht, Journalempfänger mehrmals am Tag zu sichern. Wie Sie Journalempfänger sichern, hängt davon ab, ob sie sich in einer separaten Bibliothek befinden. Sie könnten den Befehl SAVLIB (Save Library - Bibliothek sichern) oder den Befehl SAVOBJ (Save Object - Objekt sichern) verwenden.
2. Neue Objekte müssen gesichert werden, bevor Journaleinträge für ein Objekt angelegt werden können. Wenn Ihre Anwendungen regelmäßig neue Objekte hinzufügen, sollten Sie in Erwägung ziehen, mit dem Befehl SAVCHGOBJ zu arbeiten, entweder allein oder in Kombination mit der Journalführung.

Das Thema Journal management enthält weitere Erläuterungen zur Journalführung.

Komplexe Sicherungsstrategie

Steht nur ein sehr enges Sicherungsfenster zur Verfügung, muss für die Sicherung und Wiederherstellung eine komplexe Strategie verfolgt werden. Sie können dieselben Tools und Methoden verwenden, die im Zusammenhang mit der mittleren Sicherungsstrategie oben beschrieben wurden, aber auf einer höheren Detaillierungsebene. Beispielsweise müssen Sie unter Umständen bestimmte kritische Dateien zu bestimmten Tageszeiten oder an bestimmten Wochentagen sichern. Außerdem ist es sinnvoll, die Verwendung eines Tools wie beispielsweise IBM Backup Recovery and Media Services for iSeries (BRMS) in Betracht zu ziehen.

Bei einer komplexen Sicherungsstrategie ist es oft erforderlich, das System zu sichern, während es aktiv ist. Der Parameter SAVACT (save active - Sicherung im aktiven Zustand) wird bei folgenden Befehlen unterstützt:

- SAVLIB (Bibliothek sichern)
- SAVOBJ (Objekt sichern)
- SAVCHGOBJ (Geänderte Objekte sichern)
- SAVDLO (Dokumentbibliotheksobjekt sichern)
- SAV (Sichern)

Wenn Sie mit der Unterstützung für die Sicherung im aktiven Zustand arbeiten, können Sie den Zeitraum, in dem die Dateien nicht zur Verfügung stehen, signifikant reduzieren. Wenn das System für alle

Objekte, die gerade gesichert werden, einen Prüfpunkt erstellt hat, stehen die Objekte zwecks weitere Verwendung zur Verfügung. Die Unterstützung für die Sicherung im aktiven Zustand kann in Kombination mit der Journalführung und der COMMIT-Steuerung verwendet werden, um die Wiederherstellungsprozedur zu vereinfachen. Wenn Sie beim Parameter SAVACT die Werte *LIB oder *SYNCLIB verwenden, sollten Sie mit der Journalführung arbeiten, um die Wiederherstellung zu vereinfachen. Wenn Sie beim Parameter SAVACT den Wert *SYSDFN angeben, müssen Sie auch mit COMMIT-Steuerung arbeiten, wenn die zu sichernde Bibliothek zusammengehörige Datenbankobjekte enthält. Wenn Sie die Unterstützung für die Sicherung im aktiven Zustand wählen, müssen Sie unbedingt mit dem Prozedere vertraut sein und überwachen, wie gut Prüfpunkte auf Ihrem System erstellt werden.

Sie können den Zeitraum, in dem Dateien nicht zur Verfügung stehen ebenfalls reduzieren, indem Sie Sicherungsoperationen auf mehreren Einheiten gleichzeitig ausführen oder indem Sie **gleichzeitig ablaufende Sicherungsoperationen** ausführen. Sie können beispielsweise Bibliotheken auf einer Einheit sichern, Ordner auf einer anderen Einheit und Verzeichnisse wiederum auf einer dritten Einheit. Oder Sie können unterschiedliche Bibliothekengruppen oder Objektgruppen auf verschiedenen Einheiten sichern.

Bei Verwendung von V4R4 oder höheren Releases können Sie außerdem mehrere Einheiten gleichzeitig verwenden, indem Sie eine **parallele Sicherungsoperation** ausführen. Um eine parallele Sicherungsoperation ausführen zu können, benötigen Sie Backup Recovery and Media Services oder eine Anwendung, mit der Sie Datenträgerdefinitionsobjekte erstellen können.

Weitere Informationen zur Unterstützung für die Sicherung im aktiven Zustand, zu gleichzeitig ablaufenden Sicherungsoperationen und zu parallelen Sicherungsoperationen siehe Thema Backup your server. Das Thema Commitment Control enthält ausführlichere Informationen zur COMMIT-Steuerung. Das Thema Journal management enthält mehr Einzelheiten zur Journalführung.

Verfügbarkeitsoptionen auswählen

Verfügbarkeitsoptionen sind kein Ersatz für eine gute Sicherungsstrategie, sondern eine Ergänzung. Verfügbarkeitsoptionen können die Dauer einer Wiederherstellung nach einem Fehler signifikant verkürzen. In manchen Fällen können Verfügbarkeitsoptionen sogar verhindern, dass Sie eine Wiederherstellung durchführen müssen.

Um die Kosten für den Einsatz von Verfügbarkeitsoptionen zu rechtfertigen, sollten Sie Folgendes berücksichtigen:
- Den Wert, den Ihr System bereitstellt.
- Die Kosten eines terminierten oder nicht terminierten Ausfalls.
- Ihre Verfügbarkeitsanforderungen.

Mit folgenden Verfügbarkeitsoptionen können Sie Ihre Sicherungsstrategie ergänzen:
- Durch Journalverwaltung können Änderungen an Objekten, die seit der letzten vollständigen Sicherung vorgenommen wurden, wiederhergestellt werden.
- Mit dem Zugriffspfadschutz können Sie die Reihenfolge, in der Sätze in einer Datenbankdatei bearbeitet werden, erneut erstellen.
- Plattenpools beschränken die Datenmenge, die wiederhergestellt werden muss, auf die Daten im Plattenpool der fehlgeschlagenen Einheit.
- Der Einheitenparitätsschutz ermöglicht Ihnen, die verloren gegangenen Daten wiederherzustellen; der Systembetrieb kann fortgesetzt werden, während die Daten wiederhergestellt werden.
- Der Spiegelschutz hilft, die Daten verfügbar zu halten, da Sie über zwei Kopien der Daten auf zwei separaten Platteneinheiten verfügen.
- Beim Clustering können einige oder alle Daten auf zwei Systemen verwaltet werden; das sekundäre System kann kritische Anwendungen übernehmen, wenn im primären System ein Fehler auftritt.

Das Thema Availability roadmap for your iSeries server enthält Informationen, anhand derer Sie eine Verfügbarkeitslösung auf Ihrem iSeries-Server implementieren können.

Strategie testen

Wenn für Ihre Anforderungen eine mittlere Sicherungsstrategie oder eine komplexe Sicherungsstrategie benötigt wird, muss auch regelmäßig eine Überprüfung durchgeführt werden. Dabei ist Folgendes zu bedenken:

- Sichern Sie **alles** von Zeit zu Zeit?
- Was müssen Sie tun, um eine Wiederherstellung zum bekannten Punkt (4) innerhalb des Zeitrahmens für die Sicherung und Wiederherstellung durchzuführen?
- Verwenden Sie Optionen wie beispielsweise die Journalführung oder das Sichern von geänderten Objekten, um die Wiederherstellung beim Fehlerpunkt (5) zu unterstützen? Sind Sie mit der Vorgehensweise bei der Wiederherstellung unter Verwendung dieser Optionen vertraut?
- Haben Sie neue Anwendungen hinzugefügt? Werden die neuen Bibliotheken, Ordner und Verzeichnisse gesichert?
- Sind die von IBM gelieferten Bibliotheken, die Benutzerdaten enthalten (zum Beispiel QGPL und QUSRSYS), Teil der Sicherung?

  Anmerkung: Bei Thema Special values for the SAVLIB command sind alle von IBM gelieferten Bibliotheken, die Benutzerdaten enthalten, aufgelistet.
- Haben Sie die Wiederherstellung getestet?

Der beste Weg, Ihre Strategie zu testen, besteht darin, einen Testlauf für eine Wiederherstellung durchzuführen. Wenn Sie eine Wiederherstellung auf Ihrem eigenen System ausführen, kann dies riskant sein. Wenn Sie nämlich nicht alle Daten erfolgreich gesichert haben, gehen bei der versuchten Wiederherstellung möglicherweise Daten verloren.

Eine ganze Reihe von Unternehmen bieten Tests für Wiederherstellungen als Dienstleistung an. IBM Continuity and Recovery Services  ist ein solches Unternehmen, das Ihnen bei Wiederherstellungstests behilflich sein kann.

Plan zur Wiederherstellung nach einem Katastrophenfall — Schablone

Der Zweck eines Plans zur Wiederherstellung nach einem Katastrophenfall ist es, sicherzustellen, dass auf einen Notfall oder auf eine andere Ausnahmesituation, die Informationssysteme beeinträchtigt, reagiert werden kann und die Auswirkungen auf den Geschäftsbetrieb dabei so gering wie möglich gehalten werden. Dieses Thema stellt Richtlinien bereit, welche Informationen und Prozeduren für die Wiederherstellung nach einem Katastrophenfall erforderlich sind. Wenn Sie die in diesem Thema beschriebenen Informationen schriftlich fixiert haben, sollten Sie das Dokument an einem sicheren und zugänglichen Ort außerhalb des Unternehmens aufbewahren.

Nachfolgend steht eine Schablone, die Sie beim Erstellen eines Plans zur Wiederherstellung bei Notfällen verwenden können. Sie können diese Schablone hier anzeigen; zum Drucken müssen Sie die Schablone herunterladen und die PDF-Datei für dieses Thema drucken.

Plan zur Wiederherstellung bei Notfällen

Abschnitt 1. Hauptziele eines Wiederherstellungsplans

Dieser Plan hat die folgenden Hauptziele:

- Unterbrechungen des normalen Geschäftsbetriebs so gering wie möglich halten.
- Das Ausmaß von Unterbrechungen und Beschädigungen begrenzen.
- Die wirtschaftlichen Auswirkungen einer Unterbrechung so gering wie möglich halten.
- Im Voraus alternative Betriebsmöglichkeiten einrichten.
- Das Personal mit den Maßnahmen, die im Notfall zu ergreifen sind, vertraut machen.
- Eine problemlose und schnelle Wiederherstellung des Service ermöglichen.

Abschnitt 2. Personal

Datenverarbeitungspersonal			
Name	**Position**	**Adresse**	**Telefon**

Anmerkung: Hängen Sie an diesen Abschnitt des Plans eine Kopie Ihres Organisationsdiagramms an.

Abschnitt 3. Anwendungsprofil

Verwenden Sie den Befehl DSPSFWRSC (Display Software Resources - Softwareressourcen anzeigen) zum Ausfüllen dieser Tabelle.

Anwendungsprofil				
Anwendungsname	**Kritisch? Ja/Nein**	**Anlagevermögen? Ja/Nein**	**Hersteller**	**Kommentare**

Legende für Kommentare:

1. Tägliche Ausführung_____.
2. Wöchentliche Ausführung am _____.
3. Monatliche Ausführung am _____.

Abschnitt 4. Hardwareprofil

Verwenden Sie den Befehl WRKHDWPRD (Work with Hardware Products - Mit Hardwareprodukten arbeiten) zum Ausfüllen dieser Tabelle. Diese Liste sollte Folgendes beinhalten:
- Verarbeitungseinheiten
- Platteneinheiten
- Modelle
- Workstation-Controller
- Personal Computer
- Ersatz-Workstations
- Telefone
- Heizung/Klimaanlage
- Systemdrucker
- Band- und Disketteneinheiten
- Controller
- E/A-Prozessoren
- Allgemeine Datenübertragung
- Ersatzbildschirme
- Gehäuserahmen
- Luftfeuchtigkeitsregler

Hardwareprofil					
Hersteller	**Beschreibung**	**Modell**	**Seriennummer**	**Gekauft oder geleast**	**Kosten**
Anmerkung: Diese Liste sollte alle _____ Monate überprüft werden.					

Zubehör (verschiedenes)		
Beschreibung	**Menge**	**Kommentare**
Anmerkung: Diese Liste sollte Folgendes beinhalten: • Bänder • PC-Software (beispielsweise DOS) • Akten oder Dokumentation • Bänder im Sicherheitsraum • Disketten • Emulationspakete • Programmiersprachensoftware (wie COBOL und RPG) • Druckerzubehör (wie Papier und Formulare)		

Abschnitt 5. Sicherungsprozeduren für Informationsservices

- iSeries Server
  - Journalempfänger werden täglich um _____ Uhr und um _____ Uhr geändert.
  - Geänderte Objekte in folgenden Bibliotheken und Verzeichnissen werden täglich um _____ Uhr gesichert:
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____

    Mit dieser Prozedur werden auch die Journale und Journalempfänger gesichert.
  - Am _____ (Tag) um _____ (Uhrzeit) wird eine vollständige Sicherung des Systems ausgeführt.
  - Alle Sicherungsdatenträger werden außerhalb des Unternehmens in einem Sicherheitsraum in _____ (Standort) aufbewahrt.
- Personal Computer
  - Es wird empfohlen, die Daten auf allen Personal Computern zu sichern. Kopien der PC-Dateien sollten unmittelbar vor der vollständigen Sicherung des Systems am _____ (Datum) um _____ (Uhrzeit) auf den Server hochgeladen werden. Das System wird dann mit der normalen Systemsicherungsprozedur gesichert. Auf diese Weise wird eine zuverlässigere Sicherung von PC-bezogenen Systemen erreicht, bei denen durch einen lokalen Notfall Daten wichtiger PC-Systeme gelöscht werden könnten.

Abschnitt 6. Prozeduren zur Wiederherstellung nach einem Katastrophenfall

Bei jedem Plan für die Wiederherstellung nach einem Katastrophenfall sollten die drei folgenden Bereiche abgedeckt sein:

Katalog der Notfallmaßnahmen
Aufzeichnen der entsprechenden Notfallmaßnahmen bei Feuer, Naturkatastrophen usw. zum Schutz der Mitarbeiter und zur Schadensbegrenzung.

Sicherungsprozeduren
Sicherstellen, dass die wichtigsten Datenverarbeitungsfunktionen nach der Unterbrechung ausgeführt werden können.

Wiederherstellungsprozeduren
Erleichtern einer schnellen Wiederherstellung des Datenverarbeitungssystems nach einem Notfall.

Prüfliste für die im Notfall auszuführenden Maßnahmen

1. Starten des Plans
   a. Geschäftsleitung benachrichtigen
   b. Die für die Wiederherstellung nach einem Katastrophenfall geschulten Mitarbeiter benachrichtigen und einsetzen
   c. Ausmaß des Notfalls feststellen
   d. Abhängig vom Ausmaß des Notfalls den korrekten Plan zur Wiederherstellung der Anwendungen auswählen (siehe Abschnitt 7. Wiederherstellungsplan—mobiler Standort)
   e. Fortgang überwachen
   f. Den Ausweichstandort informieren und einen Zeitplan festlegen

g. Alle weiteren betroffenen Mitarbeiter informieren—sowohl die Benutzer als auch die Mitarbeiter in der Datenverarbeitung
h. Lieferanten informieren—sowohl für Hardware als auch für Software
i. Benutzer über die Serviceunterbrechung unterrichten

2. Prüfliste (Folgeliste)
   a. Liste der Teams und der Aufgaben jedes Teams erstellen
   b. Erforderliches Kapital besorgen und, falls erforderlich, Transportmöglichkeiten zum/vom Ausweichstandort einrichten
   c. Falls erforderlich, Unterkünfte einrichten
   d. Verpflegungseinrichtungen nach Bedarf organisieren
   e. Liste aller Mitarbeiter mit Telefonnummern erstellen
   f. Plan für die Mitwirkung der Benutzer erstellen
   g. Empfang und Versand von Post sicherstellen
   h. Bürobedarf bereitstellen
   i. Nach Bedarf Geräte mieten oder erwerben
   j. Feststellen, welche Anwendungen ausgeführt werden müssen und in welcher Reihenfolge
   k. Anzahl der erforderlichen Datenstationen feststellen
   l. Feststellen, welche Offline-Geräte für jede Anwendung erforderlich sind
   m. Prüfen, ob alle für die Anwendung erforderlichen Formulare vorhanden sind
   n. Alle für den Ausweichstandort bestimmten Daten prüfen, bevor der Heimatstandort verlassen wird, und das Hardwareprofil am Heimatstandort lassen.
   o. Die Hauptlieferanten bestimmen, die bei den durch den Notfall entstandenen Problemen eventuell helfen können
   p. Den Transport zusätzlich benötigter Ausrüstung zum Ausweichstandort planen
   q. Streckenpläne/Stadtplan zum Ausweichstandort bereithalten
   r. Prüfen, ob bei Bedarf zusätzliche Magnetbänder vorhanden sind
   s. System- und betriebsbezogene Dokumentation sowie Kopie(n) der Wiederherstellungsprozeduren mitnehmen
   t. Sicherstellen, dass alle betroffenen Mitarbeiter ihre Aufgaben kennen
   u. Versicherungsgesellschaften benachrichtigen

Startprozeduren für die Wiederherstellung nach einem Notfall

1. Den Wiederherstellungsservice _____ über den Notfall und die ausgewählten Wiederherstellungsprozeduren informieren.

   Anmerkung: Die garantierte Durchführungszeit läuft ab dem Zeitpunkt, zu dem _____ über die ausgewählten Wiederherstellungsprozeduren informiert wird.
   a. Telefonnummern für den Notfall

      _____ oder _____

   Diese Telefonnummern sind Montag bis Freitag von _____ Uhr bis _____ Uhr erreichbar.
2. Telefonnummer für den Noftfall: _____

   Diese Telefonnummer ist für Notfälle außerhalb der Geschäftszeiten sowie an Wochenenden und Feiertagen bestimmt. Diese Nummer bitte nur benutzen, um einen eingetretenen Notfall mitzuteilen.

3. _____ eine Adresse zur Anlieferung von Geräten (falls erforderlich), eine Kontaktadresse und eine alternative Kontaktadresse zur Koordinierung von Services und Telefonnummern, die 24 Stunden am Tag erreichbar sind, mitteilen.
4. Die Stromversorgungs- und Telefonunternehmen unterrichten und die erforderlichen Serviceverbindungen planen.
5. _____ sofort informieren, wenn zugehörige Pläne geändert werden.

Abschnitt 7. Wiederherstellungsplan–Mobiler Standort

1. _____ über die Art des Notfalls unterrichten und darüber informieren, dass der Wiederherstellungsplan für einen mobilen Standort benutzt werden soll.
2. Innerhalb von 48 Stunden die telefonische Benachrichtigung von _____ schriftlich bestätigen.
3. Sicherstellen, dass alle erforderlichen Sicherungsdatenträger zum Laden des Ausweichsystems zur Verfügung stehen.
4. Die Ausweichgeräte schriftlich bestellen.
5. _____ über die bevorstehende Ankunft des Transporters mit dem mobilen Rechenzentrum und über den Abstellort des Transporters informieren (auf der _____ Seite von _____). (Siehe Plan für den mobilen Standort in diesem Abschnitt.)
6. Abhängig von den Fernsprecherfordernissen das Telefonunternehmen (_____) über mögliche Änderungen der Notleitungen informieren.
7. Mit dem Einrichten der Strom- und Fernsprechverbindungen bei _____ beginnen.
   a. Strom- und Fernsprechleitungen sollten für den Anschluss vorbereitet sein, wenn der Transporter mit dem mobilen Rechenzentrum eintrifft.
   b. An der Stelle, an der die Telefonleitungen in das Gebäude führen (_____), die aktuelle Verbindung mit den Verwaltungs-Controllern (_____) unterbrechen. Diese Leitungen werden zu Leitungen umgeleitet, die zum mobilen Rechenzentrum führen. Sie werden mit Modems im mobilen Rechenzentrum verbunden.

      Die Leitungen, die zur Zeit von _____ nach _____ führen, würden dann an das mobile Rechenzentrum über Modems angeschlossen.
   c. Möglicherweise erfordert dies, dass _____ Leitungen bei _____ in einen geschützteren Bereich für den Fall eines Notfalls umleitet.
8. Nach Ankunft des Transporters die Stromversorgung herstellen und die notwendigen Prüfungen durchführen.
9. Verbindung zu den Übertragungsleitungen herstellen und die notwendigen Prüfungen durchführen.
10. Mit dem Laden des Systems von Sicherungen beginnen (siehe Abschnitt 9. Das gesamte System zurückspeichern).
11. Den normalen Betrieb so bald wie möglich wieder aufnehmen:
    a. Tägliche Jobs
    b. Tägliche Sicherungen
    c. Wöchentliche Sicherungen
12. Einen Zeitplan für die Sicherung des Systems erstellen, um das Zurückspeichern in das Basissystem am Ausgangsstandort vorzubereiten, nachdem es wieder verfügbar ist. (Die normalen Systemsicherungsprozeduren verwenden.)
13. Das mobile Rechenzentrum sichern und die Schlüssel nach Bedarf verteilen.
14. Ein Wartungsprotokoll für die Geräte des mobilen Rechenzentrums führen.

Plan für den Aufbau des mobilen Rechenzentrums

Den Plan für den Aufbau des mobilen Rechenzentrums hier beifügen.

Plan für einen Notfall im Kommunikationsbereich

Hier den Plan für einen Notfall im Kommunikationsbereich einschließlich der Schaltbilder beifügen.

Kundennetzschaltplan

Hier den Kundennetzschaltplan beifügen.

Abschnitt 8. Wiederherstellungsplan–Ersatzstandort

Der Wiederherstellungsservice für Notfälle stellt einen alternativen Standort (Ersatzstandort) zur Verfügung. An diesem Standort ist ein Ausweichsystem vorhanden, das vorübergehend benutzt werden kann, während der Ausgangsstandort wiederhergestellt wird.

1. _____ über die Art des Notfalls unterrichten und mitteilen, dass der Wunsch besteht, einen Ersatzstandort einzurichten.
2. Anfordern, dass die DFV-Modems so schnell wie möglich an _____ gesendet werden (evtl. auf dem Luftweg). (Informationen zu den DFV-Verbindungen für den Ersatzstandort bei _____ erfragen.)
3. Innerhalb von 48 Stunden die telefonische Benachrichtigung von _____ schriftlich bestätigen.
4. Mit den erforderlichen Reisevorbereitungen für das Einsatzteam beginnen.
5. Sicherstellen, dass alle erforderlichen Bänder zur Verfügung stehen und transportfertig verpackt sind, damit sie für die Wiederherstellung auf dem Ausweichsystem verwendet werden können.
6. Das Ausweichsystem schriftlich bestellen.
7. Anhand der Prüfliste vor der Abfahrt an den Ersatzstandort prüfen, ob das gesamte erforderliche Material dabei ist.
8. Prüfen, ob dem Wiederherstellungsteam die erforderlichen Informationen vorliegen, um mit dem Wiederherstellen des ursprünglichen Standorts zu beginnen. (Siehe Abschnitt 12. Wiederherstellen des zerstörten Standorts.)
9. Reisekosten decken (Vorschuss).
10. Nach Ankunft am Ersatzstandort Kontakt mit dem Heimatstandort aufnehmen, um die Übertragungsverbindung einzurichten.
11. Prüfen, ob das an den Ersatzstandort gebrachte Material vollständig ist.
12. Mit dem Laden des Systems von den Sicherungsbändern beginnen.
13. Den normalen Betrieb so bald wie möglich wieder aufnehmen:
    a. Tägliche Jobs
    b. Tägliche Sicherungen
    c. Wöchentliche Sicherungen
14. Einen Zeitplan für die Sicherung des Ersatzstandortsystems ausarbeiten, um in das System am Ausgangsstandort zurückspeichern zu können.

Systemkonfiguration für den Ersatzstandort

Hier die Systemkonfiguration für den Ersatzstandort beifügen.

Abschnitt 9. Das gesamte System zurückspeichern

Um das System so wiederherzustellen, wie es vor dem Notfall benutzt wurde, die im Handbuch *Sicherung und Wiederherstellung*, SC42-2053-07 beschriebenen Prozeduren für die Wiederherstellung nach einem vollständigen Systemausfall ausführen.

Erste Schritte: Holen Sie folgende Bänder, Geräte und Unterlagen aus dem Sicherheitsraum vor Ort oder aus dem Aufbewahrungsort außerhalb des Unternehmens:

- Wenn Sie von der alternativen Installationseinheit installieren, sind sowohl die Banddatenträger als auch die CD-ROM mit dem lizenzierten internen Code erforderlich.
- Alle Bänder der letzten vollständigen Sicherung
- Die Bänder, auf die zuletzt die Sicherheitsdaten gesichert wurden (SAVSECDTA oder SAVSYS)
- Die neuesten Bänder mit der gesicherten Konfiguration, falls erforderlich
- Alle Bänder mit Journalen und Journalempfängern, die nach der letzten täglichen Sicherung gesichert wurden
- Alle Bänder der letzten täglichen Sicherung
- PTF-Liste, die mit den Sicherungsbändern der letzten vollständigen Sicherung und/oder der letzten wöchentlichen Sicherung aufbewahrt wird
- Liste der Bänder der letzten vollständigen Sicherung
- Liste der Bänder der letzten wöchentlichen Sicherung
- Liste der Bänder der täglichen Sicherungen
- Systemprotokoll der letzten vollständigen Sicherung
- Systemprotokoll der letzten wöchentlichen Sicherung
- Systemprotokoll der täglichen Sicherungen
- Das Handbuch *Softwareinstallation*
- Das Handbuch *Sicherung und Wiederherstellung*
- Telefonverzeichnis
- Modemhandbuch
- Toolkit

Abschnitt 10. Wiederherstellungsprozess

Das Management-Team muss das Ausmaß des Schadens beurteilen und mit dem Aufbau eines neuen Rechenzentrums beginnen.

Wenn der ursprüngliche Standort wiederhergestellt oder ersetzt werden muss, sollten unter anderem folgende Faktoren berücksichtigt werden:

- Wie hoch ist die geplante Verfügbarkeit aller benötigten Computereinheiten?
- Ist es günstiger, die Computersysteme durch neue Geräte zu ersetzen?
- Wie lange werden die Reparaturen oder der Aufbau des Rechenzentrums voraussichtlich dauern?
- Gibt es einen Alternativstandort, der eher zu Datenverarbeitungszwecken aufgerüstet werden könnte?

Wenn die Entscheidung getroffen wurde, das Rechenzentrum wiederaufzubauen, bei Abschnitt 12 fortfahren. Wiederherstellen des zerstörten Standorts.

Abschnitt 11. Plan zur Wiederherstellung bei Notfällen testen

Für eine erfolgreiche Planung für den Notfall ist es wichtig, den Plan regelmäßig zu testen und zu bewerten. Die Datenverarbeitung ist naturgemäß einem ständigen Wandel unterworfen, der Veränderungen bei der Ausrüstung, bei den Programmen und bei der Dokumentation mit sich bringt. Daher ist es besonders wichtig, den Plan als ein sich änderndes Dokument zu betrachten. Gehen Sie beim Test anhand der Prüflisten vor und entscheiden Sie, welche Bereiche getestet werden sollten.

Tabelle 3. Ausführen eines Wiederherstellungstests

Bereich	Ja	Nein	Zutreffend	Nicht zutreffend	Kommentare
Zweck des Tests bestimmen. Welche Teile des Plans werden beurteilt?					
Testziele beschreiben. Wie wird das Erreichen der Ziele gemessen?					
Den Management-Verantwortlichen den Test und seine Ziele erklären. Einverständnis einholen und Unterstützung zusichern lassen.					
Den Test und die ungefähre Dauer der Ausführung durch die Management-Verantwortlichen bekannt geben lassen.					
Testergebnisse am Ende der Testperiode sammeln.					
Ergebnisse auswerten. War die Wiederherstellung erfolgreich? Gründe?					
Folgerungen aus den Testergebnissen ableiten. Bedeutet die erfolgreiche Wiederherstellung in einem einfachen Fall auch, dass alle kritischen Jobs in einer akzeptablen Zeit erfolgreich wiederhergestellt werden können?					
Empfehlungen für Verbesserungen ausarbeiten. Antworten und Reaktionen bis zu einem bestimmten Zeitpunkt anfordern.					
Andere Bereiche über die Ergebnisse informieren. Dabei auch Benutzer und Sicherheitsprüfer informieren.					
Den Plan zur Wiederherstellung bei Notfällen bei Bedarf ändern.					

Tabelle 4. Zu testende Bereiche

Bereich	Ja	Nein	Zutreffend	Nicht zutreffend	Kommentare
Wiederherstellung der einzelnen Anwendungssysteme mit Dateien und Dokumentation, die an einem anderen Standort außerhalb des Unternehmens aufbewahrt werden.					
Erneutes Laden der Systembänder und Durchführen eines IPL mit Dateien und Dokumentation, die an einem Standort außerhalb des Unternehmens aufbewahrt werden.					
Kann die Verarbeitung auf einem anderen Computer stattfinden?					
Kann das Management die Priorität von Systemen bestimmen, falls nur eingeschränkte Verarbeitungsmöglichkeiten vorliegen?					
Kann die Wiederherstellung und Verarbeitung auch ohne die eigentlich dafür vorgesehenen Mitarbeiter erfolgreich durchgeführt werden?					
Enthält der Plan klare Aussagen über Zuständigkeiten und Befehlswege.					
Effizienz der Sicherheitsmaßnahmen und Prozeduren zur Sicherheitsumgehung während der Wiederherstellung.					

Tabelle 4. Zu testende Bereiche (Forts.)

Bereich	Ja	Nein	Zutreffend	Nicht zutreffend	Kommentare
Ist eine Notfallevakuierung möglich und werden grundlegende Erste-Hilfe-Erfordernisse erfüllt?					
Kommen Benutzer von Echtzeitsystemen mit dem temporären Fehlen von Onlineinformationen zurecht?					
Können Benutzer tägliche Operationen ohne Anwendungen oder Jobs, die als nicht kritisch eingestuft werden, fortsetzen?					
Kann rasch Kontakt zu wichtigen Personen oder deren Stellvertretern aufgenommen werden?					
Kann die Dateneingabe bei kritischen Systemen über alternative Standorte und andere Eingabemedien erfolgen?					
Sind Peripheriegeräte wie Drucker und Scanner verfügbar und einsatzbereit?					
Ist Zusatzausrüstung verfügbar (beispielsweise Klimaanlage und Luftfeuchtigkeitsregler)?					
Verfügbarkeit von Hilfeleistungen bei Zubehör, Transport und Leitungen.					
Verteilung der am Wiederherstellungsstandort erstellten Ausgabe.					
Verfügbarkeit von wichtigen Formularen und Papier.					
Kann der Plan an weniger gravierende Notfälle angepasst werden?					

Abschnitt 12. Wiederherstellen des zerstörten Standorts

- Grundriss des Rechenzentrums
- Die aktuellen Hardwareerfordernisse und mögliche Alternativen feststellen. (Siehe Abschnitt 4. Hardwareprofil.)
- Grundfläche des Rechenzentrums, Elektrizitätsbedarf und Sicherheitsanforderungen.
  - Grundfläche (m²) _____
  - Elektrizitätsbedarf _____
  - Sicherheitsanforderungen: Abschließbare Räume, vorzugsweise Kombinationsschloss an einer Tür.
  - Raumaufteilung
  - Detektoren für überhöhte Temperatur, Wasser, Rauch, Feuer und Erschütterungen
  - Doppelboden

Lieferanten

Grundriss

Hier eine Kopie des möglichen Grundrisses beifügen.

Abschnitt 13. Aufzeichnung von Planänderungen

Halten Sie den Plan immer auf dem neuesten Stand. Fertigen Sie Unterlagen über Änderungen an der Konfiguration, an Anwendungen, Sicherungszeiten und -prozeduren an. Sie können beispielsweise eine Liste der aktuellen lokalen Hardware durch Eingabe des folgenden Befehls drucken:

```
| DSPHDWRSC OUTPUT(*PRINT)
```

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 Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices 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 Europe
| Director of Licensing
| 92066 Paris La Defense Cedex
| 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 dienen lediglich als Benutzerinformationen 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 Ver-
| pflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, 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 49XA
| 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 im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

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 der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

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 Lizenzprogrammes 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.

Marken

Folgende Namen sind in gewissen Ländern (oder Regionen) Marken der International Business Machines Corporation:

AS/400
IBM eServer
iSeries
Operating System/400
OS/400

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

Vertragsbedingungen zum Herunterladen und Drucken von Veröffentlichungen

Die Genehmigung für die Verwendung der zum Herunterladen ausgewählten Veröffentlichungen unterliegt den folgenden Vertragsbedingungen, denen Sie zustimmen müssen.

Persönlicher Bedarf: Sie können diese Veröffentlichungen für den persönlichen, nicht gewerblichen Bedarf nutzen, sofern Sie alle Eigentumshinweise beachten. Ohne die ausdrückliche Zustimmung von IBM dürfen diese Veröffentlichungen weder ganz noch teilweise verteilt, angezeigt oder abgeändert werden.

Gewerbliche Nutzung: Diese Veröffentlichungen dürfen ausschließlich innerhalb Ihres Unternehmens reproduziert, verteilt und angezeigt werden, unter der Voraussetzung, dass alle Eigentumshinweise beachtet werden. Ohne die ausdrückliche Zustimmung von IBM dürfen diese Veröffentlichungen außerhalb Ihres Unternehmens weder ganz noch teilweise reproduziert, verteilt, angezeigt oder abgeändert werden.

Mit den Veröffentlichungen oder in ihnen enthaltenen Daten, Softwareprodukten oder anderem geistigen Eigentum werden weder veröffentlicht noch stillschweigend keine anderen Genehmigungen, Lizenzen oder Rechte erteilt, sofern diese in der vorliegenden Genehmigung nicht ausdrücklich angegeben sind.

IBM behält sich das Recht vor, die hiermit erteilten Genehmigungen nach eigenem Ermessen zu widerrufen, wenn die Verwendung der Veröffentlichungen die Interessen von IBM verletzt oder (wie von IBM festgelegt) die vorstehenden Anweisungen nicht ordnungsgemäß befolgt werden.

Diese Informationen dürfen nur in vollständiger Übereinstimmung mit allen geltenden Gesetzen und Regelungen, einschließlich der in den USA geltenden Exportgesetze und -regelungen, heruntergeladen, exportiert oder erneut exportiert werden. IBM ÜBERNIMMT KEINE HAFTUNG FÜR DEN INHALT DIESER VERÖFFENTLICHUNGEN. IBM ÜBERNIMMT IN BEZUG AUF DIE VERÖFFENTLICHUNG KEINE GEWÄHRLEISTUNG, SEIEN SIE VERÖFFENTLICHT ODER STILLSCHWEIGEND GÜLTIG, EINSCHLIESSLICH, ABER NICHT BEGRENZT AUF DIE IMPLIZIERTE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK.

Durch das Herunterladen oder Drucken einer Veröffentlichung von dieser Site stimmen Sie den vorstehenden Vertragsbedingungen zu.

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 die IBM und ihre Programmlieferanten 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 die IBM oder ihre Programmlieferanten in folgenden Fällen haftbar, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde:

1. Verlust oder Beschädigung von Daten;
2. 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.