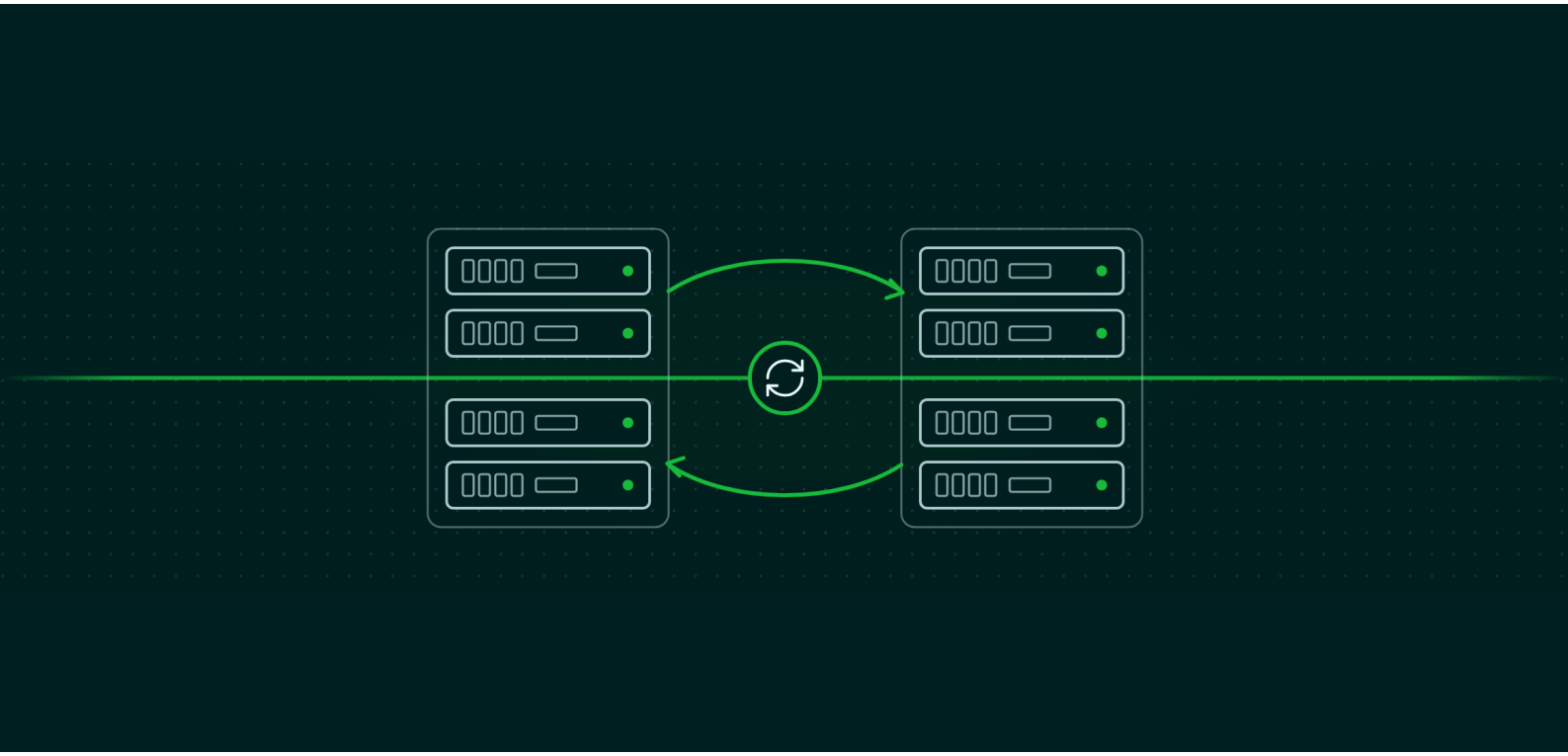
BUS4i

Whitepaper

Hochverfügbarkeit oder Disaster Recovery? IBM i nach Bedarf planen

Wie Sie aus RPO und RTO die passende Stufe der Business Continuity für Ihr IBM i ableiten.



BUS4i – eine Lösung der T.S.P. Ges. für Informationssysteme · Stand November 2026

Auf einen Blick

Wie Sie aus RPO und RTO die passende Stufe der Business Continuity für Ihr IBM i ableiten.

- RPO (wie viel Datenverlust ist tragbar) und RTO (wie lange darf der Betrieb stehen) legt die Geschäftsleitung je Anwendung fest. Erst danach lässt sich die Technik sinnvoll auswählen.
- Datensicherung, Echtzeit-Sicherung (DR) und Spiegelung auf ein zweites System (HA) unterscheiden sich vor allem darin, wie aktuell die Daten am Ziel sind und ob dort ein betriebsbereites System wartet.
- Die Journale von IBM i sind die Grundlage der meisten logischen Replikationsverfahren. Datenbankdateien allein reichen aber nicht: IFS, Programme, Benutzerprofile, Berechtigungen, Systemwerte und Spool-Dateien gehören ebenfalls dazu.
- Eine Absicherung gilt erst, wenn sie getestet ist: bei HA mit dem geplanten Rollentausch, bei DR mit der Wiederherstellung auf eine Testumgebung.
- Disaster Recovery und Hochverfügbarkeit schließen sich nicht aus. Viele Unternehmen beginnen mit DR und ergänzen später ein zweites System, sobald die Anforderungen wachsen.

Inhalt

1. RPO und RTO: Was ein Ausfall Ihr Unternehmen kosten darf
2. Drei Stufen: Datensicherung, Echtzeit-Sicherung, Spiegelung
3. Journale als Fundament: Was erfasst und gespiegelt werden muss
4. Umschalttests und Rollentausch: Nur ein geprüfter Plan zählt
5. Entscheiden nach Geschäftsanforderungen und der Weg von DR zu HA
6. Wie BUS4i unterstützt
7. Checkliste: Ist Ihre Business Continuity für IBM i geplant?

01

RPO und RTO: Was ein Ausfall Ihr Unternehmen kosten darf

Business Continuity bedeutet, dass der IT-Betrieb auch bei Störungen weiterläuft oder in planbarer Zeit wieder bereitsteht. Auf IBM i ist das System selbst meist zuverlässig. Ausfälle entstehen trotzdem: durch defekte Hardware, Brand oder Wasser im Rechenzentrum, einen Bedienfehler, eine fehlerhafte Programmänderung oder einen Angriff. Für die Planung ist die Ursache zweitrangig. Entscheidend sind zwei Kennzahlen.

Das Recovery Point Objective (RPO) gibt an, wie viel Datenverlust höchstens tragbar ist. Es wird als Zeitspanne vor dem Ausfall gemessen: Ein RPO von einem Tag bedeutet, dass im ungünstigsten Fall alle Buchungen seit der letzten Nachtsicherung fehlen und nacherfasst werden müssen. Das Recovery Time Objective (RTO) gibt an, wie lange der Betrieb höchstens stehen darf, bis die Anwendungen wieder nutzbar sind. Beide Werte sind Ziele, keine Messwerte. Ob eine Lösung sie erreicht, zeigt erst ein Test.

RPO und RTO sind Geschäftsentscheidungen. Die IT kann sagen, was technisch möglich ist und was es kostet. Wie viel ein Stillstand kostet, wissen aber die Fachbereiche: entgangene Aufträge, Personal ohne Arbeit, verspätete Lieferungen, Vertragsstrafen, Aufwand für das Nacherfassen. Deshalb sollte die Geschäftsleitung die Werte festlegen und schriftlich bestätigen.

Bewährt hat sich eine Einteilung nach Anwendungen statt nach Systemen. Ein ERP mit laufendem Auftragseingang, die Lagersteuerung im Schichtbetrieb oder die Fertigungssteuerung vertragen meist nur kurze Unterbrechungen. Ein Archiv, ein Berichtswesen oder eine Testumgebung können länger warten. Läuft alles auf einer Partition, bestimmt die anspruchsvollste Anwendung die Anforderung an das ganze System.

Ein praktischer Weg zu belastbaren Werten ist eine kurze Analyse der Geschäftsauswirkungen (Business Impact Analysis). Dafür sprechen IT und Fachbereiche je Prozess durch, was nach einer Stunde, nach einem Tag und nach einer Woche Stillstand passiert. Daraus ergeben sich Prioritäten für den Wiederanlauf und eine Grundlage, um die Kosten einer Lösung gegen die Kosten eines Ausfalls abzuwägen. Wichtig ist, die Werte regelmäßig zu überprüfen, denn neue Anwendungen, Schnittstellen oder Vertriebswege verändern die Abhängigkeit von IBM i.

- Welche Geschäftsprozesse hängen an IBM i, und welche davon stehen sofort still, wenn das System ausfällt?
- Welche Kosten entstehen je Stunde Stillstand, und ab wann werden sie kritisch?
- Können verlorene Daten nacherfasst werden, zum Beispiel aus Belegen oder aus vorgelagerten Systemen, und mit welchem Aufwand?
- Gibt es vertragliche oder gesetzliche Vorgaben zur Verfügbarkeit, etwa gegenüber Kunden oder aus NIS2, falls Ihr Unternehmen betroffen ist?

Kurz erklärt: RPO und RTO

RPO (Recovery Point Objective): der Zeitraum, aus dem Daten höchstens verloren gehen dürfen, also der Abstand zwischen dem letzten gesicherten Stand und dem Ausfall. RTO (Recovery Time Objective): die Zeit vom Ausfall, bis die Anwendungen wieder nutzbar sind. Ein kleines RPO verlangt eine häufige oder fortlaufende Übertragung, ein kleines RTO ein Zielsystem, das schnell bereitsteht.

02

Drei Stufen: Datensicherung, Echtzeit-Sicherung, Spiegelung

Zwischen „wir haben ein Band vom Vortag“ und „ein zweites System übernimmt“ liegen mehrere Stufen. Sie unterscheiden sich in zwei Punkten: wie aktuell die Daten am Sicherungsziel sind und ob dort ein betriebsbereites IBM i wartet. Das erste bestimmt das RPO, das zweite vor allem das RTO.

Die klassische Datensicherung erstellt in festen Abständen ein Abbild der Daten, meist nachts, auf Band, virtuelles Band oder Plattenspeicher. Sie ist unverzichtbar, weil sie ältere Stände aufbewahrt und vor logischen Fehlern schützt. Für die Verfügbarkeit hat sie aber Grenzen: Alles seit der letzten Sicherung ist im Ernstfall verloren, und vor dem Zurückspielen muss erst ein lauffähiges System bereitstehen.

Bei der Echtzeit-Sicherung, oft als Disaster Recovery (DR) bezeichnet, werden Änderungen fortlaufend an einen entfernten Ort übertragen, etwa auf einen Netzwerkspeicher (NAS), eine Linux-Partition oder in die Cloud. Das RPO sinkt damit deutlich, weil kaum noch Änderungen ungesichert sind. Ein zweites Power-System ist nicht nötig. Im Ernstfall muss aber zuerst eine IBM-i-Umgebung bereitgestellt werden, auf die die Daten dann zurückgespielt werden. Das RTO hängt also davon ab, wie schnell Ersatzhardware oder eine Cloud-Partition verfügbar ist.

Bei der Spiegelung auf ein zweites System, der Hochverfügbarkeit (High Availability, HA), überträgt eine Replikationssoftware alle Änderungen laufend auf ein zweites IBM-i-System, das betriebsbereit mitläuft. Fällt die Produktion aus, übernimmt das zweite System per Rollentausch. Damit sinken RPO und RTO. Dafür braucht es ein zweites System mit Lizenzen, Strom, Netz und Betreuung, idealerweise an einem anderen Standort.

Neben dieser logischen, softwarebasierten Replikation gibt es hardwarenahe Verfahren, die Daten auf Ebene des Speichersystems spiegeln, sowie Snapshots, also konsistente Abbilder eines Systems zu einem Zeitpunkt. Sie haben eigene Voraussetzungen an Speicher und Infrastruktur. Für die Planung gilt dieselbe Frage wie bei jeder Stufe: Welches RPO und welches RTO erreicht das Verfahren in Ihrer Umgebung, und wie aufwendig ist der Betrieb?

Unabhängig von der Stufe stellt sich die Frage nach dem Ort. Ein Sicherungsziel oder Zweitsystem im selben Raum schützt vor einem Hardwaredefekt, nicht aber vor Brand, Wasser oder einem Stromausfall im Gebäude. Ein zweiter Standort, ein Rechenzentrum eines Dienstleisters oder eine Cloud-Umgebung verteilen dieses Risiko. Je größer die Entfernung, desto wichtiger werden Bandbreite, Latenz und die Frage, ob synchron oder asynchron übertragen wird.

Stufe	Daten am Ziel	Im Ernstfall
Datensicherung	Stand der letzten Sicherung	System bereitstellen, Sicherung zurückspielen
Echtzeit-Sicherung (DR)	fortlaufend aktualisiert	IBM-i-Umgebung bereitstellen, Daten zurückspielen
Spiegelung (HA)	fortlaufend auf laufendem Zweitsystem	Rollentausch auf das Zweitsystem

Wichtig: Spiegelung ersetzt keine Sicherung

Replikation überträgt jede Änderung, auch versehentlich gelöschte oder unbrauchbar gemachte Daten. Wer HA oder DR einführt, behält deshalb eine Sicherung mit älteren Ständen oder eine Möglichkeit, auf einen früheren Zeitpunkt zurückzugehen. Die Stufen ergänzen sich, sie ersetzen sich nicht.

03

Journale als Fundament: Was erfasst und gespiegelt werden muss

Grundlage der logischen Replikation auf IBM i sind die Journale. Ein Journal protokolliert Änderungen an den zugeordneten Objekten, zum Beispiel jeden neuen, geänderten oder gelöschten Datensatz einer Datenbankdatei. Die Einträge landen in Journalempfängern, die nach und nach gefüllt und durch neue ersetzt werden. Eine Replikationssoftware liest diese Einträge und überträgt sie an das Ziel, wo sie in derselben Reihenfolge nachgefahren werden.

Das hat zwei Folgen für die Planung. Erstens wird nur repliziert, was journalisiert ist. Neue Dateien oder Bibliotheken müssen in die Journalisierung aufgenommen werden, sonst fehlen sie am Ziel, ohne dass es sofort auffällt. Zweitens wachsen die Journalempfänger stetig. Ohne geregelte Verwaltung belegen sie Plattenplatz, und alte Empfänger dürfen erst gelöscht werden, wenn sie übertragen und für eine eventuelle Wiederherstellung nicht mehr nötig sind.

IBM i bietet mit dem Remote Journal außerdem eine Funktion, mit der Journaleinträge auf Systemebene an ein anderes System gesendet werden. Ob synchron oder asynchron übertragen wird, ist eine Abwägung. Bei synchroner Übertragung gilt eine Änderung erst als abgeschlossen, wenn das Ziel sie bestätigt hat; das verkleinert das RPO, verlangt aber eine schnelle und stabile Verbindung. Asynchrone Übertragung belastet die Produktion weniger und eignet sich für größere Entfernungen, dafür kann im Ausfall ein kleiner Rest an Änderungen fehlen.

Ein lauffähiges System besteht aus mehr als Datenbankdateien. Für einen vollständigen Rollentausch oder Wiederanlauf müssen auch die übrigen Objekte am Ziel sein. Einige lassen sich direkt journalisieren, für andere erkennen Replikationslösungen Änderungen über eigene Mechanismen, häufig über das Sicherheitsprotokoll von IBM i (Audit-Journal QAUDJRN). Prüfen Sie bei jeder Lösung, welche der folgenden Bereiche sie abdeckt und wie.

Ebenso wichtig wie die Übertragung ist die Kontrolle. Eine Replikation kann unbemerkt ins Stocken geraten, etwa wenn ein Objekt gesperrt ist, die Verbindung unterbrochen wurde oder ein Eintrag am Ziel nicht nachgefahren werden kann. Achten Sie deshalb darauf, dass Rückstände und Fehler sichtbar werden, am besten über die Überwachung, die Sie ohnehin nutzen. Ein regelmäßiger Abgleich zwischen Quelle und Ziel zeigt, ob beide Seiten wirklich übereinstimmen.

- Datenbankdateien, Datenbereiche und Datenwarteschlangen: das Herz der Anwendungen, in der Regel über Journale erfasst.
- Programme, Serviceprogramme, Befehle und Anzeigedateien: ändern sich bei jedem Release der Anwendung und müssen am Ziel dieselbe Version haben.
- IFS (Integrated File System): Dateien wie PDF-Belege, Schnittstellendateien, Java-Anwendungen oder Konfigurationen; IFS-Objekte lassen sich journalisieren, müssen dafür

aber eingerichtet sein.

- Benutzerprofile, Kennwörter und Berechtigungen: ohne sie kann sich nach dem Rollentausch niemand anmelden oder die Rechte stimmen nicht.
- Spool-Dateien: Druckausgaben wie Lieferscheine oder Etiketten, die nach einem Ausfall nicht neu erzeugt werden können.
- Systemwerte, Jobbeschreibungen, Jobplanung und Netzkonfiguration: damit Batchläufe, Schnittstellen und Drucker am Ziel wie gewohnt arbeiten.

Kurz erklärt: Journal und Journalempfänger

Ein Journal ist auf IBM i das Änderungsprotokoll für zugeordnete Objekte. Die eigentlichen Einträge stehen in Journalempfängern. Ist ein Empfänger voll oder wird er gewechselt, beginnt ein neuer. Mit den Einträgen lassen sich Änderungen auf einem anderen System nachfahren (APYJRNCHG) oder bis zu einem bestimmten Zeitpunkt zurückverfolgen.

04

Umschalttests und Rollentausch: Nur ein geprüfter Plan zählt

Ein Zweitsystem oder eine Echtzeit-Sicherung ist nur so viel wert wie der letzte erfolgreiche Test. Erst im Test zeigt sich, ob wirklich alle Objekte am Ziel sind, ob die Anwendungen dort starten und wie lange die Umschaltung tatsächlich dauert. Ohne Test bleibt das RTO eine Annahme.

Bei Hochverfügbarkeit heißt der zentrale Test Rollentausch (Switchover). Dabei wird das Zweitsystem geplant zur Produktion, und das bisherige Produktionssystem übernimmt die Rolle des Ziels. Zu unterscheiden ist der geplante Rollentausch, etwa für Wartung oder einen Release-Wechsel, vom ungeplanten (Failover), wenn die Produktion ausfällt. Den geplanten Rollentausch können Sie üben, der ungeplante sollte nach demselben Ablauf funktionieren.

Ein geübter Rollentausch hat einen zweiten Nutzen: Er verkürzt geplante Unterbrechungen. Für Hardwarewartung, das Einspielen von PTFs oder einen Release-Wechsel kann der Betrieb vorübergehend auf das Zweitsystem wechseln, während am bisherigen Produktionssystem gearbeitet wird. Wer den Rollentausch so in den Alltag einbaut, testet ihn ganz nebenbei regelmäßig.

Bei Disaster Recovery ist der Test aufwendiger, weil zuerst eine IBM-i-Umgebung bereitstehen muss. Üblich ist die Wiederherstellung auf eine Testpartition, im eigenen Rechenzentrum oder in der Cloud. Dabei messen Sie, wie lange das Bereitstellen der Umgebung, das Zurückspielen und das Prüfen der Anwendungen dauern. Die Reihenfolge der Wiederherstellung beschreibt IBM im Handbuch „Recovering your system“; sie sollte in Ihrem Notfallhandbuch auf Ihre Umgebung übertragen sein.

Testen Sie regelmäßig und zusätzlich nach größeren Änderungen, zum Beispiel nach einem Release-Wechsel von IBM i oder der Anwendung, nach einem Hardwaretausch oder nach neuen Schnittstellen. Halten Sie jedes Ergebnis fest und vergleichen Sie es mit dem RTO. Abweichungen sind kein Scheitern, sondern der eigentliche Nutzen des Tests.

Das Ergebnis jedes Tests gehört in das Notfallhandbuch. Es beschreibt Schritt für Schritt, wer im Ernstfall entscheidet, wer welche Aufgabe übernimmt und wie die Fachbereiche informiert werden. Hinterlegen Sie es so, dass es auch dann erreichbar ist, wenn das Produktionssystem und die üblichen Ablagen nicht verfügbar sind. Ein Handbuch, das nur auf dem ausgefallenen System liegt, hilft im Ernstfall nicht.

- Starten alle Anwendungen auf dem Ziel, und sind die Daten konsistent?
- Können sich Benutzer mit ihren gewohnten Profilen und Rechten anmelden?
- Werden Netzadressen, Namensauflösung und Verbindungen der Clients und Schnittstellen umgestellt?

- Laufen Batchjobs, Jobplanung und Druckausgaben wie gewohnt?
- Wie lange hat jeder Schritt gedauert, und passt die Gesamtzeit zum RTO?
- Funktioniert der Weg zurück auf das ursprüngliche Produktionssystem?

Aus der Praxis

Ein Rollentausch betrifft nicht nur die IT. Planen Sie die Fachbereiche ein, die nach der Umschaltung prüfen, ob Aufträge, Bestände und Druckausgaben stimmen. Ein kurzer Prüfplan je Anwendung macht diesen Schritt schnell und wiederholbar.

05

Entscheiden nach Geschäftsanforderungen und der Weg von DR zu HA

Mit festgelegten RPO- und RTO-Werten wird die Auswahl nachvollziehbar. Die folgende Übersicht ordnet typische Anforderungen den Stufen zu. Sie ersetzt keine Einzelfallprüfung, zeigt aber, welche Fragen die Entscheidung tragen.

Neben RPO und RTO zählen weitere Punkte: Gibt es einen zweiten Standort oder eine Cloud-Umgebung für das Zweitsystem? Wer betreut ein zweites System im Alltag? Wie viel Bandbreite steht zwischen den Standorten zur Verfügung? Und wie oft stehen geplante Wartungen oder Release-Wechsel an, bei denen ein Rollentausch die Unterbrechung verkürzen würde? Gerade der letzte Punkt wird oft unterschätzt: Hochverfügbarkeit hilft nicht nur im Ausfall, sondern auch bei geplanten Arbeiten.

Beim Vergleich von Lösungen helfen dieselben Fragen wie in den vorigen Kapiteln: Welche Objekte werden erfasst und auf welchem Weg? Wie werden Rückstände und Fehler sichtbar? Lässt sich der Rollentausch oder die Wiederherstellung testen, ohne die Produktion zu stören? Welche Systemkombinationen, Hardwaregenerationen und IBM-i-Versionen werden unterstützt? Lassen Sie sich diese Punkte in einer Demo zeigen, bevor Sie entscheiden.

Disaster Recovery und Hochverfügbarkeit sind keine Entweder-oder-Entscheidung. Ein häufiger Weg beginnt mit der Echtzeit-Sicherung: Die Daten sind fortlaufend außer Haus, das RPO sinkt, und es ist noch kein zweites Power-System nötig. Wächst später die Bedeutung von IBM i für das Geschäft oder ändern sich die Vorgaben, kommt ein Zweitsystem hinzu und die Lösung wird zur Hochverfügbarkeit ausgebaut.

Damit dieser Schritt gelingt, lohnt es sich, schon bei der Auswahl der DR-Lösung darauf zu achten, ob sie sich zu HA erweitern lässt, ohne Journalisierung, Abläufe und Know-how neu aufzubauen. Auch die Datensicherung bleibt auf jeder Stufe bestehen, weil sie ältere Stände aufbewahrt.

Für die Entscheidung im Unternehmen hilft eine einfache Gegenüberstellung: auf der einen Seite die Kosten eines Ausfalls aus der Analyse der Geschäftsauswirkungen, auf der anderen Seite die Kosten jeder Stufe für Software, Hardware oder Cloud-Ressourcen, Leitungen und Betreuung. Legen Sie diese Gegenüberstellung der Geschäftsleitung vor, zusammen mit den RPO- und RTO-Werten, die jede Stufe in Ihrer Umgebung erreichen soll. So wird aus einer technischen Frage eine dokumentierte Geschäftsentscheidung, die sich später prüfen und anpassen lässt.

Anforderung	Geeignete Stufe	Voraussetzung
Datenverlust eines Tages tragbar, längerer Stillstand möglich	Datensicherung	Ersatzsystem oder Notfallvertrag
Kaum Datenverlust tragbar, Stillstand für Bereitstellung möglich	Echtzeit-Sicherung (DR)	Entfernter Speicher, Ersatzumgebung im Ernstfall
Kaum Datenverlust und nur kurzer Stillstand tragbar	Spiegelung (HA)	Zweites IBM-i-System, Netzverbindung
Wartung und Release-Wechsel mit kurzer Unterbrechung	Spiegelung (HA)	Zweitsystem, geübter Rollentausch
Heute DR, später höhere Anforderungen erwartet	DR mit Ausbaupfad zu HA	Lösung, die beide Stufen abdeckt

06

Wie BUS4i unterstützt

BUS4i ist die Softwarefamilie der T.S.P. Gesellschaft für Informationssysteme mbH (TSP) aus Karlsruhe, Softwarehersteller seit 1984, für Business Continuity auf IBM Power i. Zwei Module decken die beiden Stufen aus diesem Whitepaper ab: BUS4i DR für die Echtzeit-Sicherung und BUS4i HA für die Spiegelung auf ein zweites System.

BUS4i DR sichert alle Änderungen auf Ihrem IBM-i-System in Echtzeit auf ein entferntes Ziel: ein gängiges NAS-System, eine Linux-Partition oder die Cloud, zum Beispiel die IBM Cloud oder einen IBM-Partner als Managed Service Provider. Ein zweites Power-System ist dafür nicht nötig. Die Daten sind bei der Übertragung und bei der Speicherung verschlüsselt, einzelne gelöschte Daten lassen sich in Minuten wiederherstellen. Die Einrichtung dauert nur kurze Zeit, und ein späteres Upgrade auf BUS4i HA ist möglich.

BUS4i HA spiegelt Ihr IBM-i-System über die IBM-i-Journale in Echtzeit auf ein Sekundärsystem und schaltet bei einem Ausfall automatisch um. Gespiegelt werden alle Objekte, auch das IFS, Benutzerprofile und Spool-Dateien. Physische, virtuelle und Cloud-Systeme lassen sich beliebig kombinieren, mit Any-to-Any-, Dual- und Multi-Node-Replikation, synchron oder asynchron. Gemischte Hardware und unterschiedliche IBM-i-Versionen sind möglich, ebenso Live Partition Mobility und virtuelle Seriennummern. Der Bandbreitenbedarf ist gering.

Den Rollentausch können Sie mit BUS4i HA testen, ohne dass der Betrieb steht. Bedient wird BUS4i HA über eine grafische Oberfläche, für die Überwachung gibt es eine Nagios-Schnittstelle. BUS4i ist bereit für IBM i 7.6. Für die Verwaltung und Bereinigung der Journale gibt es zusätzlich BUS4i JOMA4i, das auch neben Replikationssoftware anderer Hersteller läuft.

BUS4i wird weltweit über Partner vertrieben. Sie bleiben bei Ihrem gewohnten IBM i Partner; meldet sich ein Unternehmen direkt bei uns, arbeiten wir mit diesem Partner zusammen. Die Support-Hotline steht allen Kunden rund um die Uhr zur Verfügung, auf Deutsch und Englisch. Eine Demo ist kostenfrei.

- BUS4i DR: Echtzeit-Sicherung auf NAS, Linux-Partition oder Cloud, ohne zweites Power-System, verschlüsselt, später erweiterbar zu HA.
- BUS4i HA: Echtzeit-Spiegelung über Journale auf ein Zweitsystem mit automatischer Umschaltung, inklusive IFS, Benutzerprofilen und Spool-Dateien.
- Rollentausch testbar, ohne dass der Betrieb steht.
- Vertrieb über Partner, Hotline rund um die Uhr für alle Kunden.

Checkliste: Ist Ihre Business Continuity für IBM i geplant?

- [ ] Sind RPO und RTO je Anwendung festgelegt und von der Geschäftsleitung bestätigt?
- [ ] Wissen Sie, was eine Stunde Stillstand Ihres IBM i kostet?
- [ ] Passt Ihre heutige Stufe (Datensicherung, DR oder HA) zu diesen Werten?
- [ ] Sind alle relevanten Dateien und Bibliotheken journalisiert, auch neu hinzugekommene?
- [ ] Werden Journalempfänger geregelt verwaltet und erst gelöscht, wenn sie nicht mehr gebraucht werden?
- [ ] Erfasst Ihre Lösung neben der Datenbank auch IFS, Programme, Benutzerprofile, Berechtigungen, Systemwerte und Spool-Dateien?
- [ ] Ist geklärt, wo Ihr IBM i im Ernstfall läuft und wie schnell diese Umgebung bereitsteht?
- [ ] Gibt es neben der Replikation eine Sicherung mit älteren Ständen?
- [ ] Wann haben Sie Rollentausch oder Wiederanlauf zuletzt getestet und die Dauer gemessen?
- [ ] Lässt sich Ihre DR-Lösung zu Hochverfügbarkeit ausbauen, wenn die Anforderungen wachsen?

Welche Stufe passt zu Ihrem IBM i?

Ob Echtzeit-Sicherung, Spiegelung oder der Weg von einem zum anderen: Die Antwort hängt von Ihren RPO- und RTO-Vorgaben und Ihrer Umgebung ab. Gern besprechen wir mit Ihnen und Ihrem IBM i Partner, welche Stufe zu Ihren Anforderungen passt. Vereinbaren Sie ein unverbindliches Erstgespräch oder eine kostenfreie Demo.

Gespräch vereinbaren

BUS4i – eine Lösung der T.S.P. Gesellschaft für Informationssysteme mbH, Karlsruhe
bus4i.de/kontakt · info@bus4i.de
bus4i.de/bus4i-ha/

BUS4i

Stand November 2026. Dieses Whitepaper gibt einen fachlichen Überblick und ersetzt keine individuelle Beratung. © T.S.P. Gesellschaft für Informationssysteme mbH