Whitepaper

Uptime Backup as a Service (BaaS) mit IBM Spectrum Protect

1. Funktionsweise

Uptime Backup as a Service (BaaS) basiert auf der IBM Spectrum Protect Software.
IBM Spectrum Protect ist eine plattform-übergreifende Lösung zur Datensicherung auf Speichersysteme und die Wiederherstellung dieser Daten.
Zentraler Bestandteil des Systems ist die Serverkomponente (IBM Spectrum Protect Server), welche Dienste zur Datensicherung anbietet und die Sicherungen auf den Speichersystemen verwaltet. Die Verwaltungsinformationen werden in einer zentralen Datenbank gespeichert.
Auf den Systemen, deren Daten gesichert werden sollen, werden Clientkomponenten installiert, welche für den Transport der Daten zur oder von der Serverkomponente sorgen und den Ablauf der Sicherung und Wiederherstellung steuern.

Die folgenden Funktionen von IBM Spectrum Protect können in Uptime Backup as a Service genutzt werden:

- Progressiv inkrementelle Sicherung des Systemzustandes und dessen Wiederherstellung für Windows-Systeme (IBM Spectrum Protect BA Client)
- Progressiv inkrementelle Sicherung von Dateisystemen bzw. Dateien und deren Wiederherstellung (IBM Spectrum Protect BA Client)
- Langzeitaufbewahrung von Dateien (Archive/Retrieve) (IBM Spectrum Protect BA Client)
- Vollständige, differentielle oder inkrementelle Sicherung und Wiederherstellung von Exchange und Domino Mailservern (IBM Spectrum Protect for Mail)
- Einzelne Postfächer vom Exchange Server wiederherstellen
- Vollständige, differentielle oder inkrementelle Sicherung und Wiederherstellung von Oracle (via RMAN) und MS SQL Datenbanken (via VSS oder VDI) (IBM Spectrum Protect for Databases)
- Schnappschuss-Technik (VSS) für die Sicherung von Microsoft SQL Server und Microsoft Exchange Server mit geringstmöglichem Einfluss auf den laufenden Betrieb (IBM Spectrum Protect for Databases, IBM Spectrum Protect for Mail)
- Sicherung von mySAP Systemen (IBM Spectrum Protect for ERP)
- Wiederherstellung
  - Einzelne Dateien
  - Gesamtes Dateisystem

2. Struktur

Uptime Backup as a Service unterliegt folgender Struktur:

- Uptime
  - IBM Spectrum Protect Server
    - Zeitplan
    - Aufbewahrungsregeln
  - Wiederverkäufer
    - Endkunde
      - Standort
        - Server
        - Knoten
          - Zuordnung zu Zeitplan (auf dem IBM Spectrum Protect Server)
          - Zuordnung zu Aufbe-wahrungsregeln (auf dem IBM Spectrum Protect Server)

3. Planung einer Datensicherung

Vorab müssen folgende Dinge festgelegt werden:

- Was soll gesichert werden?
- Wann soll gesichert werden?
- Wie häufig soll gesichert werden?
- Wie viele Versionen einer gesicherten Datei sollen aufbewahrt werden?
- Wie lange sollen die gesicherten Dateien aufbewahrt werden?

Sind diese Festlegungen getroffen und die Konfiguration erfolgt, läuft der Sicherungsvorgang in der Regel automatisch ab. Abweichend hiervon sind manuelle Sicherungen möglich, die direkt vom zu sichernden System aus gestartet werden. Die Vereinbarungen werden im Backup Recovery Agreement (BRA) festgehalten.

3.1. Generell zu berücksichtigen

Aus organisatorischen Gründen benötigt Uptime IT einen Zeitraum, in dem keine Sicherungen stattfinden. Dieser Zeitraum liegt jeden Morgen zwischen 06:00 Uhr und 08:00 Uhr. Es ist daher sicherzustellen, dass alle Sicherungen bis 6:00 Uhr abgeschlossen sind und die nächste Sicherung nicht vor 08:00 Uhr beginnt. Sicherungen, die in das Zeitfenster hineinlaufen, werden abgebrochen. Es wird eine entsprechende Fehlermeldung erzeugt.

3.2. System

Der Standardfall ist eine einmal tägliche progressiv inkrementelle Datensicherung des Systemzustandes.

3.3. Dateien bzw. Dateisysteme

Der Standardfall ist eine einmal tägliche progressiv inkrementelle Datensicherung der auf dem System vorhandenen Dateien.
Uptime IT bietet ein vorgefertigtes Sicherungsschema mit zugehörigen Templates zur Ausführung auf dem Client an, welches vom Wiederverkäufer angepasst werden kann.

3.4. Datenbanken

Der Standardfall ist eine wöchentliche Vollsicherung, eine tägliche differentielle Sicherung und eine stündliche Sicherung der Transaktionsprotokolle (nur tagsüber Mo. – Fr. und So. abends) der Datenbanken.
Uptime IT bietet ein vorgefertigtes Sicherungsschema mit zugehörigen Templates zur Ausführung auf dem Client an, welches vom Wiederverkäufer angepasst werden kann.
Je nach Datenbanksystem kann es abweichende Empfehlungen zur Sicherungsstrategie geben.

3.5. Mailserver

Der Standardfall ist eine wöchentliche Vollsicherung und eine stündliche inkrementelle Sicherung (nur tagsüber Mo. – Fr. und So. abends).
Uptime IT bietet ein vorgefertigtes Sicherungsschema mit zugehörigen Templates zur Ausführung auf dem Client an, welches vom Wiederverkäufer angepasst werden kann.
Je nach Mailserver kann es abweichende Empfehlungen zur Sicherungsstrategie geben.

4. Einrichtung einer Datensicherung

Um eine Datensicherung für ein System einzurichten sind folgende Schritte erforderlich:

1. Auf dem IBM Spectrum Protect Server werden die Aufbewahrungsregeln für die Dateien festgelegt. Dabei kann es mehrere Regelsätze (Management Classes) für unterschiedliche Dateiarten geben. (→ Wie viele Versionen einer gesicherten Datei sollen aufbewahrt werden? Wie lange sollen die gesicherten Dateien aufbewahrt werden?)
2. Auf dem IBM Spectrum Protect Server wird ein Knoten (Node) für das zu sichernde System angelegt und ein anfängliches Passwort festgelegt. Für jedes zu sichernde System können mehrere Knoten existieren, z.B. je einer für Dateisystem-, Mailserver- und Datenbanksicherung.
3. Auf dem IBM Spectrum Protect Server wird ein Zeitplan (Schedule) für die Sicherung eingerichtet. Dieser legt Zeitpunkt, Art und Häufigkeit der Sicherung fest. (→Wann soll gesichert werden? Wie häufig soll gesichert werden?)
4. Auf dem IBM Spectrum Protect Server wird der zuvor erstellte Zeitplan dem Client zugeordnet.
5. Auf dem zu sichernden System (Client) werden die notwendigen Clientkomponenten des IBM Spectrum Protect installiert.
6. Auf dem Client werden die von Uptime IT vorgefertigten Konfigurationsdateien und Scripts abgelegt.
7. Auf dem Client wird der Zugriff auf den IBM Spectrum Protect Server konfiguriert. Es werden die Netzwerkparameter und das anfängliche Passwort eingestellt.
8. Optional werden auf dem Client die Verzeichnisse oder Dateien angepasst, die in die Sicherung einbezogen bzw. von ihr ausgenommen werden sollen. (→ Was soll gesichert werden)
9. Optional werden auf dem Client die Zuordnungen von Verzeichnissen oder Dateien zu einem der zuvor auf dem IBM Spectrum Protect Server erstellten Aufbewahrungsregelsätze angepasst.
10. Auf dem Client wird der Zeitplanungsdienst (Scheduler Service) gestartet. Dies ist Voraussetzung für automatisierte Datensicherungen.

Die grün dargestellten Schritte führt der Wiederverkäufer aus. Die blau dargestellten Schritte führt Uptime IT aus.
Die dargestellten Schritte gelten für die Sicherung von Dateisystemen, Datenbanken und Mailservern gleichermaßen.

5. Ablauf einer Datensicherung

Eine automatische Datensicherung läuft in diesen Schritten ab:

1. In der Regel wird der Scheduler Service beim Starten des Client-Betriebssystems gestartet.
2. Der Scheduler Service auf dem Client verbindet sich mit dem IBM Spectrum Protect Server
3. Der Scheduler Service auf dem Client fragt in regelmäßigen Zeitabständen beim IBM Spectrum Protect Server seinen Zeitplan ab.
4. Ist der Zeitpunkt für die Sicherung erreicht, startet der Scheduler Service auf dem Client die Datensicherung.
5. Nur bei Sicherung von MS SQL Server: Vor der Sicherung von Datenbanken wird eine Konsistenzprüfung durchgeführt.
6. Ggf. wird der Systemzustand gesichert
7. Nur bei Sicherung von Dateisystemen: Während der Sicherung wird entschieden, welche Dateiinhalte an den IBM Spectrum Protect Server gesendet werden müssen:
    a. Die Datei befindet sich nicht in der Ausnahmeliste.
    b. Die Datei befindet sich in der Liste der einzubeziehenden Dateien.
    c. Die Datei ist neu oder die Datei hat sich seit der letzten Sicherung geändert (bei inkrementeller Sicherung).
    d. Der minimale Zeitabstand zwischen zwei Sicherungen (falls definiert) ist erreicht oder überschritten.

6. Aufbewahrung gesicherter Dateien

Für die gesicherten Dateien werden Aufbewahrungsregeln definiert, die je nach Typ der Datei (z.B. ausführbare Programmdateien, Konfigurationsdateien, Protokolldateien, von Benutzern erstellte Dokumente) folgende Details festlegen:

- Anzahl der aufzubewahrenden Versionen einer auf dem Client existierenden Datei. Die Anzahl kann zwischen 1 und unendlich liegen.
- Aufbewahrungsdauer für veraltete Versionen einer auf dem Client existierenden Datei. Die Dauer kann zwischen null und unendlich liegen.
- Anzahl der aufzubewahrenden Versionen einer auf dem Client inzwischen gelöschten Datei. Die Anzahl kann zwischen null und unendlich liegen.
- Aufbewahrungsdauer für auf dem Client inzwischen gelöschte Dateien. Die Dauer kann zwischen null und unendlich liegen.

Für die Verwendung auf dem Client gibt es durch Uptime IT vorgefertigte Regelsätze (Management Classes), die durch den Wiederverkäufer auf dem Client (z.B. je nach Art der zu sichernden Datei) ausgewählt werden können.

7. Wiederherstellungsszenarien

7.1. Systemwiederherstellung

7.1.1 Herstellung eines Sicherungssatzes

Um ein komplettes System wiederherzustellen ist es zweckmäßig, dieses von einem lokal angeschlossenen Datenträger zu tun, falls die Bandbreite zum IBM Spectrum Protect Server eine zu große Einschränkung für eine schnelle Wiederherstellung darstellt.
Zu diesem Zweck kann Uptime IT einen Sicherungssatz (Backup Set) für einen bestimmten Client herstellen. Dieser Sicherungssatz wird z.B. auf Festplatte(n) an den Wiederverkäufer oder Endkunden ausgeliefert. Mit diesem kann dann das System wiederhergestellt werden.

7.1.2 Startfähiges Windows-System

Ein noch startfähiges System kann auf einen früheren Zustand ohne Neuinstallation wiederhergestellt werden. Dazu werden die zuvor gesicherten Dateien und der Systemzustand ggf. über die grafische Bedienoberfläche direkt vom IBM Spectrum Protect Server oder aus einem Sicherungssatz wiederhergestellt. Die vom System geschützten Dateien werden zunächst an einem temporären Ort wiederhergestellt und beim dann folgenden Neustart an den Originalort verschoben. Hierzu ist während der Wiederherstellung zusätzlicher Speicherplatz im jeweiligen Dateisystem erforderlich.

7.1.3 Nicht mehr startfähiges Windows-System

Eine Wiederherstellung kann nur auf weitgehend identische Hardware erfolgen. Die Wiederherstellung erfolgt in zwei Schritten:

- Das Betriebssystem und der IBM Spectrum Protect Client werden installiert.
- Die Dateisysteme und der Systemzustand werden ggf. über die grafische Bedienoberfläche direkt vom IBM Spectrum Protect Server oder aus einem Sicherungssatz wiederhergestellt. Die vom System geschützten Dateien werden zunächst an einem temporären Ort wiederhergestellt und beim dann folgenden Neustart an den Originalort verschoben. Hierzu ist während der Wiederherstellung zusätzlicher Speicherplatz im jeweiligen Dateisystem erforderlich.

7.1.4 Linux-System

Die Wiederherstellung eines Linux-Systems erfolgt in folgenden Schritten:

- Ein Notfall-Betriebssystem wird auf dem wiederherzustellenden System gestartet und darauf der IBM Spectrum Protect Client installiert.
- Der Systemzustand wird wiederhergestellt.
- Die Festplattenaufteilung wird wiederhergestellt und die Dateisysteme angelegt.
- Die Dateisysteme werden direkt vom IBM Spectrum Protect Server oder aus einem Sicherungssatz wiederhergestellt.
- Die Boot-Konfiguration des Systems wird wiederhergestellt und das System wird neu gestartet.

7.2. Verlorene oder zerstörte Dateien

Sind Dateien oder ganze Verzeichnisse versehentlich gelöscht oder unbeabsichtigt verändert worden, können diese ggf. über eine grafische Bedienoberfläche am Originalort oder in ein beliebiges Verzeichnis direkt vom IBM Spectrum Protect Server wiederhergestellt werden. Die Wiederherstellung von Dateien eines zurückliegenden Zeitpunktes ist möglich, sofern die alten Versionen entsprechend den Aufbewahrungsregeln noch vorhanden sind.

7.3. Datenbank

Datenbanken können in ihrem zuletzt gesicherten Zustand oder weiter zurückliegenden Zeitpunkten am Originalort oder an anderer Stelle wiederhergestellt werden, sofern die alten Versionen entsprechend den Aufbewahrungsregeln noch vorhanden sind. Sollten einzelne Bestandteile (File Groups bzw. Tablespaces) einer Datenbank zerstört sein, können diese auch einzeln restauriert werden.
Im Falle einer vollständigen Wiederherstellung werden zunächst ggf. Betriebssystem und Software mit allen nicht-Datenbankdateien und danach die Datenbanken wiederhergestellt. Die genaue Prozedur hängt vom verwendeten Datenbanksystem ab.
Für Microsoft SQL Server steht eine grafische Bedienoberfläche zur Verfügung.
Data Protection für Oracle integriert den Oracle Recovery Manager (RMAN) mit dem IBM Spectrum Protect Server. Für die Wiederherstellung (und auch die Sicherung) von Oracle-Datenbanken wird RMAN verwendet.

7.4. Mailserver

Im Falle einer vollständigen Wiederherstellung werden zunächst ggf. Betriebssystem und Software mit allen Nicht-Datenbankdateien und danach die Datenbank des Mailservers wiederhergestellt. Die genaue Prozedur hängt vom verwendeten Mailserver ab.
Es steht eine grafische Bedienoberfläche zur Verfügung.

7.5. Microsoft Exchange

Die Datenbanken des Mailservers können in ihrem zuletzt gesicherten Zustand am Originalort oder an anderer Stelle wiederhergestellt werden.
Einzelne Postfächer können in ihrem zuletzt gesicherten Zustand oder weiter zurückliegenden Zeitpunkten am Originalort oder an anderer Stelle wiederhergestellt werden. Eine Filterfunktion erlaubt die Wiederherstellung von Elementen des Postfachs, die bestimmten Kriterien entsprechen.

7.6. Lotus Domino

Die Datenbanken des Mailservers können in ihrem zuletzt gesicherten Zustand oder weiter zurückliegenden Zeitpunkten am Originalort oder an anderer Stelle wiederhergestellt werden, sofern die alten Versionen entsprechend den Aufbewahrungsregeln noch vorhanden sind.
Um einzelne Dokumente zu restaurieren, muss zunächst die Datenbank an anderem Ort wiederhergestellt werden, um dann das einzelne Dokument in die Originaldatenbank zu kopieren.

8. Überwachung und Benachrichtigung

Jede geplante Datensicherung wird von Uptime IT darauf überwacht, ob der Sicherungsvorgang im geplanten Zeitfenster stattgefunden hat und ob es während der Sicherung Fehler gegeben hat.
Es wird täglich an den Auftraggeber eine Mail versendet, die die folgenden Informationen enthält:

- den Status der Sicherungen für jeden Knoten
- das insgesamt zu einem Knoten gesicherte Volumen (nicht das übertragene)

Uptime IT bemüht sich die Mails so zu versenden, dass sie zu Arbeitsbeginn des Auftraggebers vorliegt.
Wird eine definierte Sicherung erneut nicht durchgeführt, unabhängig von den Gründen, erhält der Auftraggeber bei jedem Auftreten eine entsprechende Benachrichtigung. Diese Benachrichtigungen sind vom Auftraggeber zu sichten, zu bewerten und bei Bedarf sind vom Auftraggeber Maßnahmen zu ergreifen oder einzuleiten, um ggf. mit Hilfe von Uptime IT die Sicherung wieder in Gang zu setzen oder anders dafür zu sorgen, dass die Meldungen unterbleiben.
Ist eine Datensicherung fehlgeschlagen gibt es auch keinen Recovery Point.
Uptime IT hat wiederholt festgestellt, dass nicht behobene Fehler zu einem Anstieg des gesicherten Datenvolumens führen können. Es liegt daher im natürlichen Interesse des Auftraggebers Fehler umgehend zu beheben, bzw. bei der Behebung mitzuwirken.
Uptime IT behält sich vor, Benachrichtigungen auszusetzen, wenn ein Fehler über einen Zeitraum von mind. 14 Tagen regelmäßig auftritt, aber nicht behoben werden kann, weil

- dieser nicht im Verantwortungsbereich von Uptime IT liegt,
- die Mitwirkung des Auftraggebers nicht erfolgt.

In diesen Fällen wird Uptime IT den Kunden auf das Ende der Benachrichtigungen aufmerksam machen.
Uptime IT übernimmt keine Haftung, für Folgen, die aus dieser Situation entstehen wie z.B. ein erhöhtes Datensicherungsvolumen. Dies gilt ausdrücklich auch wenn durch diese Situation Benachrichtigungen zu schwerwiegenderen, behebbaren Fehlern unterbunden wurden und/oder eine andere Fehlerbehebung nicht stattfinden kann. Das Datenvolumen für jeden Backup-Job wird täglich erfasst und gespeichert. Aus den gesammelten Daten wird monatlich eine Abrechnung erstellt.

9. Sicherheit

9.1. Passwörter

Um eine Verbindung vom Client zum IBM Spectrum Protect Server herzustellen wird (neben dem Knotennamen und der IBM Spectrum Protect Server-Adresse) ein Passwort benötigt. Dieses wird anfänglich bei der Bekanntmachung des Clients auf dem IBM Spectrum Protect Server festgelegt. Im laufenden Betrieb wird das Passwort automatisch in regelmäßigen Zeitabständen geändert. Es kann eine Mindestlänge für die verwendeten Passwörter vorgegeben werden.

9.2. Secure Socket Layer

Für jegliche Kommunikation (Sicherung, Wiederherstellung und Abfragen) zwischen Client und IBM Spectrum Protect Server wird eine mit SSL gesicherte Verbindung verwendet, um Abhören und Manipulation der Daten zu verhindern. Dabei authentifiziert sich der IBM Spectrum Protect Server mit seinem SSL-Zertifikat.

9.3. Verschlüsselung der gesicherten Daten

Eine Verschlüsselung der zu sichernden Daten mit AES 128 oder AES256 ist möglich. Dies kann auf bestimmte Daten beschränkt werden. Standardeinstellung ist AES128 für alle gesicherten Daten.

9.4. Clientseitige Schlüsselfestlegung

Für die Datenverschlüsselung kann ein clientseitiger Schlüssel festgelegt werden, der nur dort bekannt ist. Er wird beim Start der ersten Sicherung festgelegt und für weitere Sicherungen auf dem Client gespeichert.
Nachteil: Die clientseitige Schlüsselfestlegung ist nur bei der Sicherung von Dateien, nicht jedoch bei Datenbanken, Mailservern usw. möglich.
Vorteil: Der Schlüssel ist nur auf dem Client bekannt. Daher ist diese Verschlüsselung auch für sensible Daten geeignet.

9.5. Transparente Verschlüsselung

Bei Verwendung der transparenten Verschlüsselung generiert der Client bei jeder Sicherung einen Schlüssel, der auf dem IBM Spectrum Protect Server zusammen mit der Sicherung hinterlegt wird. Der Schlüssel wird im Falle einer Wiederherstellung zurück an den Client ausgeliefert, um die Daten zu entschlüsseln. Dies ist die Standardeinstellung.
Vorteil: Die transparente Verschlüsselung wird für alle Sicherungen, also Dateien, Datenbanken, Mailserver usw. unterstützt.
Nachteil: Der Schlüssel ist auf dem IBM Spectrum Protect Server hinterlegt. Dies ist bei sensiblen Daten unerwünscht. Das Problem kann durch eine Offline-Sicherung der Datenbank oder des Mailservers auf Dateiebene umgangen werden.

9.6. Unterstützte Sicherheitsmerkmale

	Sicherung von Dateien	Sicherung von Datenbanken, Mailservern usw.
Passwörter	Ja	Ja
Secure Socket Layer	Ja	Ja
Clientseitige Schlüsselfestlegung (Schlüssel nur auf Client bekannt)	Ja	Nein
Transparente Verschlüsselung (Schlüssel auf TSM Server hinterlegt)	Ja	Ja

10. Verringerung des Transfervolumens

Um Daten eines Clients zu sichern, der mit niedriger Bandbreite an den IBM Spectrum Protect Server angebunden ist, gibt es verschiedene Möglichkeiten zur Verringerung des Transfervolumens.

10.1. Clientseitige Kompression

Zu sichernde Daten werden standardmäßig clientseitig komprimiert, um das Transfer- und auch das Sicherungsvolumen zu verringern.

10.2. Sicherung von geänderten Dateibereichen

Die Sicherung von geänderten Dateibereichen (Subfile Backup) kann bei großen Dateien das Transfer- und auch das Sicherungsvolumen verringern. Bei der ersten Sicherung wird die Datei komplett gesichert. Bei nachfolgenden Sicherungen werden nur die Bereiche der Datei gesichert, die sich seit der letzten Sicherung verändert haben. Subfile Backup wird nur unter Windows unterstützt.

10.3. Clientseitige Deduplizierung

Bei der clientseitigen Deduplizierung werden identische Dateien oder auch Bereiche von Dateien nur einmal zum IBM Spectrum Protect Server gesendet, um so das Transfer- und auch das Sicherungsvolumen zu verringern.

11. Unterstützte Funktionen je Betriebssystem

	BA Client	DP f. Exchange (2008SP3 .. 2017)	DP f. Domino	DP f. SQL Server (2008SP3 .. 2017)	DP f. Oracle (11gR2,12c, 12cR2, 18c)	DP f. SAP DB2	DP f. SAP Oracle	DP f. SAP HANA
Windows (Server 2008 .. 2016)	iu	iu	i	iu	iu	i[64]	i[64]	-
Windows (Server 2019)	i	i	-	i	-	-	-	-
Windows (7 .. 10)	i	-	-	-	-	-	-	-
AIX 6.1, 7.1 7.2	I	-	i	-	i	i[64]	i[64]	-
HP-UX 11iV3	i	-	-	-	i	i[64]	i[64]	-
SUSE Linux Enterprise Server 11 oder 12	i	-	i	-	i	i[64]	i[64]	i[64]
SUSE Linux Enterprise Server 15	i	-	-	-	-	i[64]	i[64]	i[64]
Red Hat Enterprise Linux 5	i	-	i	-	i	-	-	-
Red Hat Enterprise Linux 6 und 7	i	-	i	-	i	i[64]	i[64]	i[64]
Debian GNU Linux 6, 7, 8	b	-	-	-	-	-	-	-
CentOS Linux 5, 6, 7	b	-	-	-	-	-	-	-
Mac OS X 10.8 .. 10.11	i	-	-	-	-	-	-	-
Sun Solaris 10 und 11	i	-	i	-	i	i[64]	i[64]	-

Legende:
iu = offiziell von IBM unterstützt und von Uptime IT getestet
i = offiziell von IBM unterstützt und von Uptime IT bisher nicht verwendet
b = bedingt von IBM unterstützt („Best Effort“ Support) und von Uptime IT bisher nicht verwendet
[64] = nur 64bit-Systeme unterstützt

Angaben ohne Gewähr, Details siehe die entsprechenden IBM-Dokumente.