

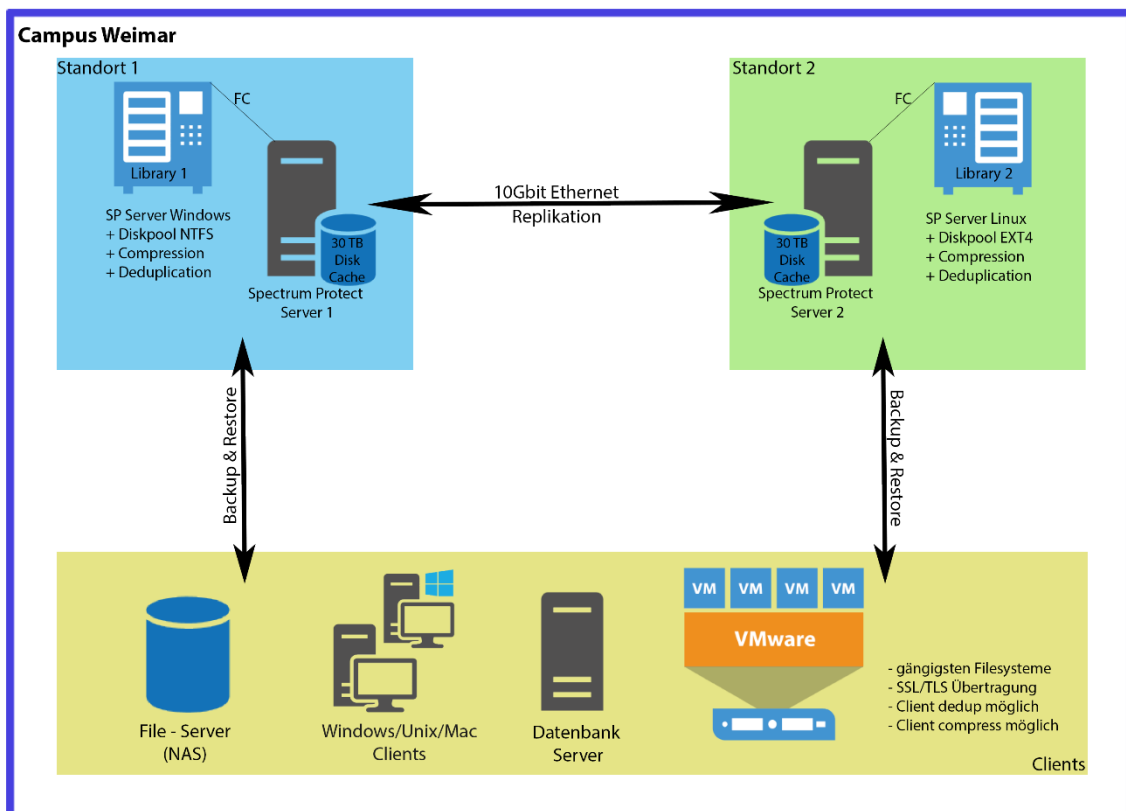
Backup- und Restorekonzept für die Bauhaus Universität Weimar und Hochschule für Musik FRANZ LISZT

Stand: Februar 2018

Mit Backup bezeichnen wir im Folgenden das Kopieren elektronisch gespeicherter Daten an einen anderen Ort und auf andere Medien. Unter Restore verstehen wir, dass diese Daten bei Bedarf, Verlust oder ungewollter Veränderung, in mehreren Versionen wiederhergestellt werden können.

Als Daten werden hier sowohl einfache Dateien, Verzeichnisse, wie auch Datenbanken und virtuelle Maschinen betrachtet.

1. Infrastruktur zur Datensicherung



Zur Datensicherung wird die professionelle Enterprise-Backup Lösung IBM Spectrum Protect eingesetzt. Es existieren zwei unabhängige, auf circa zwei Kilometer räumlich getrennte Backup-Zentren, die jeweils mit einem

physischen Backupserver und einem eigenen Bandroboter ausgestattet sind. Jedes Datum ist auf jedem Backupserver mindestens einmal gesichert.

Dies erfolgt durch eine gegenseitige Replikation neuer Daten. Die Sicherungen und Replikationsprozesse erfolgen täglich. Bei allen Kommunikationsprozessen wird eine SSL/TLS basierende Datenverschlüsselung genutzt. Teilweise werden Daten dedupliziert und komprimiert übertragen und gespeichert.

Mit der Softwarelösung IBM Spectrum Protect werden alle Daten initial nur einmal gesichert, alle geänderten bzw. neu angelegte Daten werden der Sicherung hinzugefügt (Incremental-Forever). Hierdurch wird die Belastung der Infrastruktur, d.h. des Datennetzes und der Server, erheblich reduziert.

2. Datensicherung und Wiederherstellung

2.1. Backup der Daten des Uni zentralen Fileservice

Für jede neu erzeugte bzw. geänderte Datei werden Sicherungskopien erstellt.

Zum einen erfolgen täglich Snapshots der gesamten Home- & Projekt-Daten auf dem Uni zentralen Fileserver, sowie eine Spiegelung zu einem zweiten Standort.

Es erfolgt täglich eine inkrementelle Sicherung der Projekt Daten zum Backupserver. Die Home Daten werden wöchentlich zum Backupserver gesichert.

2.2. Backup Uni zentraler virtueller Maschinen (VM)

Es werden grundsätzlich alle produktiven VMs für zentrale Aufgaben der Universität gesichert. Jede VM wird täglich ohne separate Client Software über die virtuelle Infrastruktur gesichert. Es werden immer nur die Datenblöcke gesichert welche sich zum letzten Backup basierten Snapshot geändert haben (ChangeBlockTracking). Die Datenübertragung und Speicherung erfolgt für alle VMs dedupliziert.

Bei VMs mit mehr als 150 GB Festplattenkapazität wird eine 2- stufige Datensicherung mittels Backup-Client vorgenommen.

2.3. Datensicherung dezentraler Server

Das SCC kann die Sicherung der dezentralen Server der Universität auf Antrag übernehmen.

Diese Art der Sicherung erfordert die Installation einer Client-Software. Die Festlegung der zu sichernden Datenbereiche und Backup-Regeln obliegt dem Serverbetreiber.

2.4. Archivierung/Langzeitspeicherung von Daten

Das SCC bietet die Offline-Langzeitspeicherung von Daten für die gesamte Universität an.

Unter Archivierung wird hier die langfristige Speicherung von Daten auf externen Medien (Magnetbänder) verstanden, wobei die Ursprungsdaten auf den lokalen oder zentralen Speicher der Universität in der Regel gelöscht werden.

2.5. Besonderheiten

Server mit Datenbanksystemen und vergleichbare Systeme sind explizit zu melden, da dort ggf. andere und individuelle Sicherungseinstellungen vorgenommen werden müssen. Zusätzliche Software-Lizenzen für Sonderlösungen sind vom Nutzer zu finanzieren.

2.6. Datenwiederherstellung

Die Wiederherstellung von Fileservice Daten ist mehrstufig gegliedert. Benutzer können auf die Snapshots ihrer Daten selbstständig zugreifen. Für Wiederherstellung von Daten aus dem Backup ist ein Ticket an die SCC-Hotline zu stellen.

Für die Wiederherstellungsanforderung von VMs ist ebenfalls ein Ticket an die SCC-Hotline zu stellen. Für die Wiederherstellung von Daten dezentraler Server sowie der separat gespeicherten Datenbereiche von VMs sind die Serververantwortlichen zuständig.

3. Kontrolle der Datensicherung

Die tägliche Kontrolle der Datensicherung liegt in Verantwortung des Server-/Infrastrukturbetreibers.

Eine Unterstützung durch die Arbeitsgruppe Storage/Backup wird bei Installation und Betrieb gewährleistet.

Anhang A: Weitere Informationen zur Umsetzung

Stand: Februar 2018

zu 2.1. Backup der Daten des Uni zentralen Fileservice

Es erfolgt viermal täglich, 7 – 12 – 17 – 22 Uhr, ein Snapshot des gesamten Datenraums, diese Snapshots werden 28 Tage aufgehoben.

Ergänzend dazu erfolgt eine tägliche inkrementelle Sicherung der Projekt Daten und eine wöchentliche inkrementelle Datensicherung der Home Daten. Diese werden für zwei Monate aufbewahrt. Die letzte bzw. gelöschte Version wird 1 Jahr vorgehalten.

zu 2.2. Backup Uni zentraler virtueller Maschinen (VM)

Die automatische Sicherung findet täglich im Zeitraum von 00:00 Uhr bis circa 6:00 Uhr statt. Der Aufbewahrungszeitraum der Sicherungen beträgt 30 Tage.

Bei VMs mit mehr als 150 GB Festplattenkapazität wird eine 2- stufige Datensicherung vorgenommen. Gemäß der Richtlinie „Betrieb der virtuellen Infrastruktur am SCC“ werden diese Systeme in System- und Datenbereich aufgeteilt. Die Sicherung der Systemplatte erfolgt erstmalig FULL, anschließend fortlaufend inkrementell (Incremental-Forever). Die Datenfestplatte ist separat mittels Backup-Client aus der VM heraus zu sichern. Dazu ist die erforderliche Clientsoftware zu installieren.

Testsysteme werden nicht in das automatische Backup einbezogen. Im Bedarfsfall ist hier ein Backup Antrag mittels der Serverdatenbank zu stellen.

zu 2.3. Datensicherung dezentraler Server

Als Standard gelten folgende Regeln:

- Es erfolgt ein täglicher inkrementeller Backup aller Daten der ausgewählten Dateisysteme.
- Die automatische Datensicherung findet im Zeitraum von 20:00 Uhr bis circa 5:00 Uhr des nächsten Tages statt.
- Die Aufbewahrungsfristen für unterschiedliche Versionen einer Datei sind 30 Tage, die letzte bzw. gelöschte Version wird ein Jahr aufbewahrt.

Abweichende Regeln sind auf Wunsch mit der Arbeitsgruppe Storage/Backup zu vereinbaren.

zu 2.4. Archivierung/Langzeitspeicherung von Daten
Archivdaten werden standardmäßig 10 Jahre aufbewahrt.

Daten, wie bspw. digitalisierte Medien, können unbegrenzt aufbewahrt werden. In diesen Fall ist ein spezieller Antrag erforderlich.

Diese Funktionalität kann von allen Servern genutzt werden, auf welchem die Backup Client-Software installiert ist.

Servicelevel

Der Backupdienst hat die Service-Klasse Bronze. Die Servicelevel sind in der aktuellen Fassung des Dokuments „Information und Kommunikations – Strukturkonzept“ beschrieben.

Ergänzende Dokumente

- Ordnung für die Nutzung der IT-Infrastruktur
- IT-Sicherheitsordnung
- IuK-Strukturkonzept der Bauhaus-Universität Weimar

- Fileservicekonzept für die Bauhaus Universität-Weimar
- Konzept „Betrieb der virtuellen Infrastruktur am SCC“
- Wiederherstellen von Dateien mit Nutzung der VSS Funktion in Windows (zu Absatz 2.1)
- Kurzbeschreibung Prozess Sichern von Daten an der Bauhaus Universität Weimar (in arbeit)
- Kurzbeschreibung Prozess Archivierung von Daten an der Bauhaus Universität Weimar (in arbeit)
- Backupantrag dezentraler Server
- Archivierungsantrag für Daten mit unbegrenzter Aufbewahrungsfrist
- Benutzung der SCC-Serverdatenbank