Überblick

Fileservices des ZIM

Das Fileserviceangebot des ZIM wird auf Hardware der Firma NetApp, einem sog. Fabric-Metrocluster, betrieben
Dabei werden 2 Storagecontroller so miteinander verbunden, dass jeder der beiden den Dienst des jeweils anderen im Problemfall übernehmen kann.
Idealerweise wird ein solches System auf 2 Standorte verteilt, damit der Fileservice auch im Falle des Ausfalls eines kompletten Serverraumes weiterhin verfügbar ist.
In unserem Fall befinden sich beide Standorte, räumlich getrennt, auf dem Campus der HHU. Alle Hardwareteile, inkl. der Festplatten, sind daher mindestens doppelt vorhanden.
Der Zugriff auf Kundenseite erfolgt über sog. SVM's (Storage-Virtual-Machines). Dies sind virtuelle Fileserver, welche für gewöhnlich im selben Netzwerksegment beheimatet sind, wie die Arbeitsplatzrechner der Kunden.
Alle virtuellen Fileserver sind auf jeweils einem der beiden Storagecontroller "beheimatet" und werden auf den jeweils anderen gespiegelt.
Somit werden alle Daten die auf der "Heimatseite" geschrieben werden innerhalb weniger Millisekunden auf auch auf die andere Seite repliziert und sind dementsprechend immer auf beiden Controllern verfügbar.

Sicherheit

Die Authentisierung und Authorisierung geschieht gegen unser zentrales Active-Directory, dem Verzeichnisdienst von Microsoft.
In diesem Verzeichnisdienst liegen alle aktiven Uni-Kennungen von Bediensteten und Studierenden. Diesen können über Mitgliedschaften in Berechtigungsgruppen Zugriff auf Ressourcen, in diesem Fall Dateiablagen, gewährt werden.
Auf den Fileservern werden sog. ACL's (Access-Control-Lists) gepflegt, in denen steht, welche (Personen-) Gruppe(n) wie (lesend, lesend- und schreibend etc.) auf die Ordner und Dateien des Fileservers zugreifen dürfen.
Über diesen Mechanismus wird gewährleistet, dass nur Personen, welche bestimmte Berechtigungen erhalten haben, auch auf die entsprechenden Ressourcen Zugriff haben.
Die Schritte zur Authentisierung und Authorisierung finden über eine verschlüsselte Verbindung statt.
Die Datenübertragung des Fileservers selber wiederum, bei interner Verwendung über CIFS/SMB/NFS (im eigenen Institutsnetz), findet unverschlüsselt statt.
Auch die Dateien liegen unverschlüsselt (allerdings in 4-Kb kleine Blöcke zerteilt und randomisiert auf mehrere hundert Festplatten verteilt) auf unserem Fileserversystem.
Sollten Sie Anforderungen haben, bei denen eine Verschlüsselung unabdingbar ist, müssen Sie auf eine Containerverschlüsselung wie z.B. VeraCrypt zurück greifen.
Beim Zugriff von extern über unseren WebDAV Server ist auch die Kommunikation nach dem Schritt der Authentisierung und Authorisierung (über eine https Verbindung) verschlüsselt,
da dieser Zugriff für gewöhnlich über Netze erfolgt, welche nicht im Hoheitsgebiet der HHU liegen.

Snapshots & Backups

Das System sichert an mehreren Zeitpunkten pro Tag den Zustand des Dateisystems.
Diese sog. Snapshots dienen dazu, dass Kunden im Falle eines Falles einzelne Dateien oder auch ganze Ordnerstrukturen selbstständig widerherstellen können.
Dies funktioniert relativ fein granular. Snapshots werden täglich um 06:10, 08:10, 10:10, 12:10, 14:10, 16:10, 18:10, 20:10 und 22:10 Uhr gemacht.
Da hiervon immer die letzten 36 Stück aufbewahrt werden, können bis zu etwa 4 Tage alte Dateien in diesem Abstand wiederhergestellt werden.
Dazu kommen 8 Tages-Snapshots die jeweils um 00:10 Uhr gemacht werden und 4 Wochen-Snapshots die jeweils Sonntags um 00:15 gemacht werden.
Somit können insgesamt bis zu vier Wochen alte Dateien wiederhergestellt werden.