SAYTEC

Juli 2023

sayFUSE HCI

Die symmetrische hyperkonvergente Infrastruktur

Whitepaper: Die ganzheitlich ausgelegte Infrastruktur

Inhaltsverzeichnis

1. SAYFUSE HCI-INFRASTRUKTUR

Die sayFUSE hyperkonvergente Infrastruktur (**sayFUSE HCI**) besteht mindestens aus drei sayFUSE All-in-One Infrastruktur Nodes (**sayFUSE HCI Node**), die die gesamte Server-Storage-Netzwerk Infrastruktur bereitstellen und eine **sayFUSE Backup** Appliance, die als Backup-Restore-Plattform für Archivierung, Datensicherung und Auslagerung sorgt, beinhaltet. Die integrierte **sayTRUST VPSC Zero Trust** Lösung ermöglicht eine hochsichere Kommunikation zwischen dem Client und der Infrastruktur.

Die sayFUSE HCI hyperkonvergenten Infrastruktur fasst CPU, RAM, Storage und Netzwerkressourcen zu einem einzigen softwaredefinierten System zusammen und kann über die Nodes hinweg verwaltet und gesteuert werden. Sie ist fehlertolerant gegenüber Komplettausfällen von einem oder mehreren Nodes und ermöglicht einen unterbrechungsfreien Betrieb. Zukünftige Erweiterungen können durch Ergänzung weiterer Nodes problemlos und ohne Migrationsaufwand durchgeführt werden.

Die einzelnen sayFUSE HCI Nodes sind in Bezug auf die Hard- und Software identisch. Jeder sayFUSE HCI Node enthält alle erforderlichen Hardware- und Softwarekomponenten, so dass in Zukunft keine zusätzlichen Lizenzen für Clustering, Computing, Storage, Kubernetes, Monitoring, Zero Trust, Personal Key Identifikation, Single Sign-on, Billing und Multi-Tendancy, … erforderlich sind. Bei einem Ausfall eines der Nodes, werden alle Computing, Storage, Networking Aufgaben des ausgefallenen Nodes von den anderen Nodes übernommen und eine störungsfreie Business Kontinuität ist gewährleistet.

Die Produkte sayFUSE HCI (All-in-One Node für hyperkonvergente Infrastruktur), sayFUSE Backup (All-in-on Appliance für Backup, Restore und Auslagerung) und sayTRUST VPSC (All-in-on Client Access Lösung für Zero Trust, SSO, PKI, …) können auch autark unabhängig voneinander betrieben werden und stellen für sich eine hochqualitative und sichere Lösung in ihrem jeweiligen Einsatzgebieten dar.

1.1. Beschreibung des ganzheitlichen Konzeptes

Die hyperkonvergente Infrastruktur besteht aus N sayFUSE HCI-Nodes und der sayFUSE Backup Appliance. Der Aufbau erfolgt idealerweise symmetrisch über zwei Brandabschnitte mit jeweils einer Backup Appliance in jedem Brandabschnitt. Die so aufgebaute HCI bildet eine zusammenhängende Storageplattform, Computing und Networking, dass als „**as a Service**“ verwendet wird und die Möglichkeit bietet, **komplett isolierte Infrastrukturen as a Service (IaaS)** für mehrere Standorte oder Mandanten bereitzustellen.

Das sayFUSE Backup sorgt **mit bis zu 12 TB/Stunde für Live-Backup** eine Hochgeschwindigkeitssicherung. Innerhalb der Backup Appliance können die Daten aus dem **Backup-Storage** in das integrierte **Backup Library System** migriert und ausgelagert werden. Jede Appliance enthält **sechs Backup Laufwerke** mit jeweils 24 TB Kapazität.

Die sayTRUST VPSC Zero Trust Client Access ermöglicht eine von Ort und Gerät unabhängige und sichere Kommunikation und eine hochsichere Arbeitsumgebung.

1.1.1. sayFUSE HCI-Infrastruktur

Die ganzheitliche Infrastruktur wird durch mehrere sayFUSE HCI-Nodes als hochsichere hyperkonvergente Infrastruktur gebildet. Sie bilden das zusammenhängende Storage, Computing und Networking Plattform, das als „as a Service“ verwendet wird und die Möglichkeit bietet, komplett isolierte Infrastrukturen as a Service (IaaS) für ein oder mehrere Standorte oder eine Vielzahl von Mandanten bereitzustellen.

Die sayFUSE HCI-Plattform bildet die Grundlage für echte Business Continuity, die beliebig skaliert werden kann. Sie reduziert die Komplexität der gesamten IT-Infrastruktur und minimiert den Hard- und Softwarebedarf. Der Installations-, Migrations- und Betriebsaufwand werden nachhaltig gesenkt.

Hardwareaustauschzyklen werden deutlich verlängert und die Stromkosten sowie CO_2-Emissionen deutlich gesenkt.

Das integrierte Hypervisor sorgt über die einzelnen Nodes hinweg für den Aufbau eines zusammenhängenden Storage, Computing und Networking und stellt alle Infrastrukturkomponenten als multimandantenfähigen Service bereit. Sie kann z.B. anderen Standorten oder Mandanten komplette Netzwerkinfrastrukturen bereitstellen, so dass in Zukunft vor Ort keine zusätzliche Investition für z.B. Server, Storage, Loadbalancer, … erforderlich wird.

Ein Standort oder Mandant erhält z.B. eine isolierte Infrastruktur als Service, die von der Hauptadministration bereitgestellt wird und vom jeweiligen Standort oder Mandanten verwaltet werden kann. Sie kann folgende Infrastrukturkomponenten als Service enthalten:

- Router,
- Loadbalancer,
- Firewall,
- Single Sign-on,
- Personal Key Identifikation,
- Zero Trust Zugang,
- VPN,
- NFS-, iSCSI-, S3-Storage,
- Server,
- Virtuelle Client-PC,
- Backup (mehrstufig mit Migration, Mediabruch und Auslagerung)

Dabei sind die einzelnen IaaS untereinander und gegenüber dem unsicheren Internet sowie gegenüber dem hausinternen Netzwerk isoliert und nicht sichtbar. Der Zugang der Anwender auf die einzelnen Anwendungen, Dienste, Netzwerke oder den eigenen virtuellen PC kann über die sayTRUST VPSC Zero Trust Technologie, nach Prüfung der Identität „**Personal Key Identifikation** (PKI)“ über ein **mehrstufiges Defence in Depth Sicherheitsverfahren** erfolgen.

1.1.2. VPSC (Virtual Private Secure Communication)

Die sayTRUST VPSC als Zero Trust Client Access Lösung, ermöglicht eine von Ort, Gerät und der Topologie unabhängige sichere Kommunikation und sorgt für eine hochsichere Arbeitsumgebung. sayTRUST VPSC bietet die höchste Stufe der Kommunikationssicherheit durch **Erfassen und Eliminieren der Schwachstellen zwischen dem Anwender und dem zu schützendem Netzwerk**. Die Nutzer können über die 8-stufige „Defence in Depth“ Zero Trust Technologie sowohl innerhalb des eigenen Netzwerkes als auch von fremden Standorten, Home-Office oder mobile Hotspots sicher arbeiten.

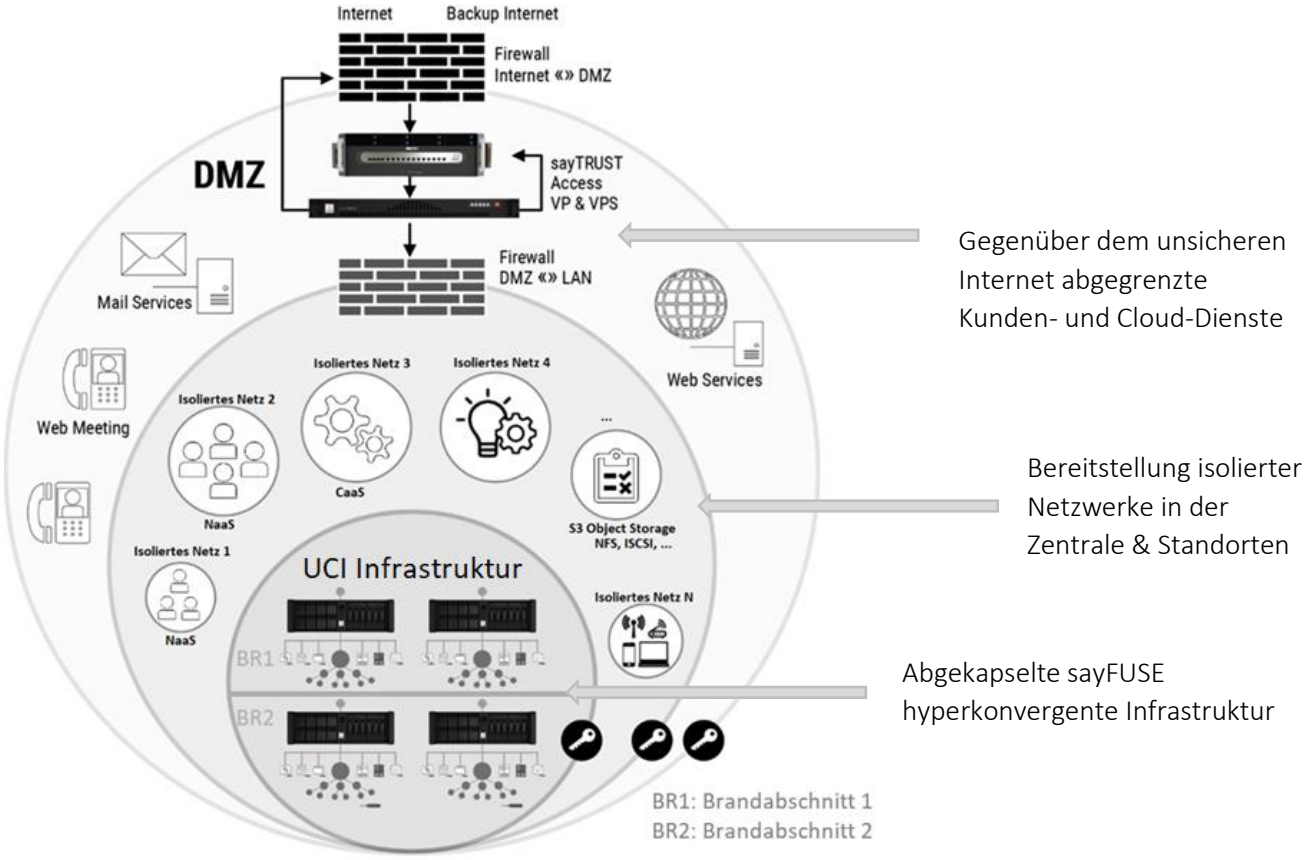
sayTRUST VPSC ermöglicht eine getunnelte Kommunikation für **lokale-, remote- und mobile Anwendungen**. Serverseitige erzeugte Anwenderzertifikate über die eigene „Certificate Authority“ **steuern das Erlauben, Blockieren und Isolieren** von Applikationen und Ressourcen. Die verschlüsselte Kommunikation beginnt nach der Identitätsprüfung des Anwenders und erfolgt **innerhalb der Applikationsebene verschlüsselt aus dem Arbeitsspeicher (RAM) der Client-PC**s, anstatt über Netzwerk-Netzwerk-Kopplung.

1.1.3. sayFUSE Backup

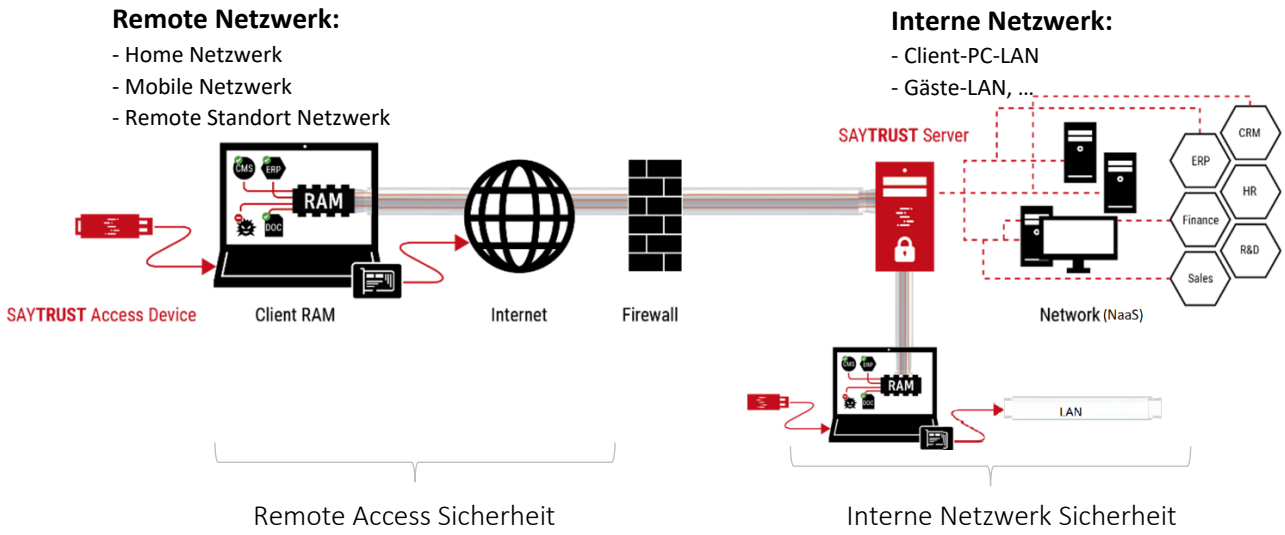
Die sayFUSE Backup Lösung bietet eine einzigartige **Hochgeschwindigkeitssicherung mit bis zu 12 TB/Stunde für Live-Backup und mit bis zu 18 TB/Stunde für Migrationsbackup**. Die Technologie beseitigt alle typischen Backup-Schwachstellen von Band- und Storage basierten Technologien. Sie **bündelt zudem alle sechs essenziellen Backup-Komponenten**. Backup-Server, Backup-Storage, Backup-Library, Backup-Laufwerke, Mediabruch und Auslagerung in einem Gerät. Es sorgt für hohe Backupqualität und stellt die Wiederherstellbarkeit der Daten und Systeme sicher. Innerhalb der Backup Appliance werden die Daten aus dem Backup-Storage in das integrierte Backup Library System migriert und ausgelagert.

Das Dreibein des sayFUSE HCI gewährleistet mit den eingebetteten Technologien eine ganzheitlich ausgelegte IT-Infrastruktur. Sie bringt maximale Sicherheit, Skalierbarkeit und hohe Kosteneinsparung.

1.2. Schematische Darstellung der sayFUSE hyperkonvergente Infrastruktur



1.3. Schematische Darstellung für Client-Access Zugriffssicherheit



Eine hochsichere Kommunikation setzt über die gesamte Kommunikationsstrecke das **Ineinandergreifen aller Sicherheitselemente an den Schnittstellen** voraus. Sie erkennt und beseitigt Schwachstellen, sowohl innerhalb des hausinternen Netzwerkes wie auch bei remote Access Zugriffen. Mit der sayTRUST VPSC Zero Trust Technologie wird durch **Erfassen und Eliminieren der Schwachstellen** in einer Kommunikation die höchste Stufe der Sicherheit erreicht.

2. EIGENSCHAFTEN DER IN SAYFUSE HCI ENTHALTENEN TECHNOLOGIEN

Dieses Kapitel stellt den Funktionsumfang und die Eigenschaften für die ganzheitlich ausgelegte IT-Infrastruktur dar. Der sayFUSE HCI Infrastruktur Bundle, der als hochsichere und ganzheitliche Infrastruktur Lösung bereitgestellt wird, sind drei elementare Technologien vereint.

- Hyperkonvergente Infrastruktur für den unterbrechungsfreien Geschäftsbetrieb, maximale Skalierbarkeit und hohe Flexibilität.
- Die Backup-Restore-Plattform für Datenarchivierung, Sicherung und Auslagerung.
- Personifizierte Zero Trust für Client-Access Zugriffssicherheit.

sayFUSE HCI-Infrastruktur bietet die höchstmögliche Verfügbarkeit von Daten und Systeme, Skalierbarkeit der IT-Infrastruktur und die höchste Sicherheitsstufe bei der Netzwerkkommunikation (Client-Access), sowohl innerhalb des Netzwerkes als auch bei Remotezugriffen. Ferner steht die Reduzierung der Komplexität des Gesamtsystems und Administrationsaufwandes im Vordergrund.

Beginnend mit drei Geräten als sayFUSE All-in-One Infrastruktur Appliance (Nodes) kann das Gesamtsystem durch weitere Geräte ohne Migrationsaufwand beliebig skaliert werden und eignet sich von mittelständischen Unternehmen bis hin zu Konzernen. Auch für staatliche Einrichtungen und Kommunen ist die Lösung einzigartig im Mehrwert.

Der Einsatz der sayFUSE HCI-Infrastruktur minimiert die gegenwärtigen und zukünftigen Hard- und Software Anforderungen (Kapitel 1. sayFUSE HCI-Infrastruktur). Bereits das kleinste Bundle enthält alle unten aufgelisteten Eigenschaften.

Im Folgenden werden die Eigenschaften entsprechen den Technologien gegliedert aufgelistet.

2.1. Leistungsumfang der sayFUSE hyperkonvergente Infrastruktur

2.1.1. allgemeine Eigenschaften des sayFUSE HCI-Systems

- Jedes Gerät in einer sayFUSE HCI-Infrastruktur ist eine **All-in-One Infrastruktur-Appliance** (Node). In jedem Node sind alle Hardware- und Software Komponenten enthalten.
- Die HCI – Infrastruktur besteht aus mehrere Nodes und eine sayFUSE Backup Appliance (Appliance) für die **Backup-Restore-Plattform**.
- Alle sayFUSE HCI Nodes beinhalten alle erforderlichen Hardwarekomponenten für Computing, Storage, Networking und die Softwarelizenzen für die hyperkonvergente Infrastruktur.
- Jede Appliance enthält alle erforderlichen Hardwarekomponenten für Computing, Backup-Storage, Backup Library System, Backup Storage-to-Disk mit Mediabruch und Auslagerung.
- Die Nodes sind identisch und alle Nodes sind in der Lage, bei einem Ausfall oder einer geplanten Wartung, automatisch die Rolle und die Aufgaben eines beliebigen Node aus dem Verbund zu übernehmen.
- Die Nodes, die das System bilden, kommunizieren über eine Ethernet-basierte Netzinfrastruktur miteinander. Eine andere Art von Netz oder Verbindung zwischen Servern oder zwischen Servern und Plattensystemen ist nicht erforderlich.
- Das System enthält Compute-, Software Based Storage (SDS)- und Software Based Networking (SDN) Komponenten, die das Cluster zwischen den Nodes bilden. Jede dieser Komponenten kann von einem einzigen Punkt aus in voller Kompatibilität zueinander verwaltet werden.

- Das System ist in der Lage weitere Nodes aufzunehmen und kann so linear ohne Migrationsaufwand skaliert werden.
- Das System bildet einen **Hochsicherheits-Cloud-Cluster**, der mit einem einzigen Node beginnt und durch Hinzufügen von Nodes wachsen kann. Es gibt keine Wachstumsgrenzen in Bezug auf Cluster oder die Anzahl der Nodes im Cluster.
- Der Server-Storage-Cluster ist so konzipiert, dass er den Ausfall von mindestens einem Node gleichzeitig toleriert. Auf Wunsch kann die Konfiguration angepasst werden, um einen Ausfall von zwei oder mehreren Nodes zu tolerieren.
- Die gesamte Verwaltung des Systems ist über eine webbasierte Schnittstelle, eine Befehlszeile und eine API-Schnittstelle möglich.
- Das System ist in der Lage CPU- und RAM-Ressourcen übermäßig zu beanspruchen. Der **Over-Commit-Multiplikator** kann vom Systemadministrator festgelegt werden.
- Bei allen virtuellen Datenträgern können nur so viele Daten auf den Datenträger geschrieben werden, wie verwendet werden (Thin Provisioning).
- Der Erstellungsprozess für virtuelle Maschinen kann mit vorgefertigten Hardware-Vorlagen schnell durchgeführt werden. Neue Maschinen können zu den Vorlagen hinzugefügt und die CPU- und RAM-Ressourcen festgelegt werden.
- Das System hat einen "Image Service". Durch diesen Image-Dienst, bei dem fertige Disk-Images oder ISO-Dateien kopiert werden, ist es möglich, eine virtuelle Maschine mit einem fertigen Disk-Image oder mit einer ISO-Installationsdatei zu erstellen.
- Im System können Sicherheitsrichtlinien erstellt werden, die auf virtuellen Maschinen oder Gruppen virtueller Maschinen zugewiesen werden können.
- Die Sicherheitsrichtlinien können die Festlegung von Zugriffsregeln von außen auf die virtuelle Maschine (eingehend) und von der virtuellen Maschine nach außen (ausgehend) ermöglichen, und diese Regeln können flexibel verändert werden.
- Vorgänge wie die Auflistung der virtuellen Maschinen mit einer Sicherheitsrichtlinie, die Zuweisung einer Richtlinie zu einer virtuellen Maschine und die Bearbeitung der Zugriffsregeln einer Richtlinie können über das Web-Panel durchgeführt werden.
- Warnmeldungen, Audit-Protokolle und detaillierte Leistungsdiagramme des Systems können über das Web-Panel überwacht werden.
- Das System ist in der Lage Fehler-, Warn- und Alarmmeldungen per E-Mail über das SMTP-Protokoll an die gewünschten Personen zu übermitteln.
- Das System ist multimandantenfähig und kann bei Bedarf einem Standort oder Mandanten eine vollständig eigenständige Implementierung und Administration für die eigene Verwaltung bieten. Die bereitgestellte IaaS kann alle Services wie S3-, iSCSI-, NFS-Storage, virtuelle Server und Client-PC, Routing, Loadbalancer, Zero Trust, VPN, … enthalten.
- Das System kann bei Bedarf oder wenn ein Standort keine Administration aufweist, über die Administration aus der Zentrale verwaltet werden.
- Auf den Servern können SSD- oder Festplatteneinheiten mit unterschiedlichen Zugriffsformaten wie NVMe, SAS, SATA parallel genutzt werden. Obwohl es selbstverständlich ist, die erforderliche Mindestanzahl dieser Einheiten festzulegen, gibt es keine Regel, die die gleichzeitige Verwendung verschiedener Festplattenkapazitäten und -formate in der gewünschten Kombination verhindert.
- Es gibt keine Begrenzung für die Anzahl der Disks, die auf einem Node installiert werden können.
- Eine software- oder hardwarebasierte RAID1-Struktur (Spiegelung) wird für das für Betriebssystem-Hypervisor zu verwendende M2 NVMe unterstützt.
- Jedes Node verfügt ein BMC-Modul für Remote-Management.

2.1.2. Spezifikationen des sayFUSE HCI-Disk-Teilsystems

Das Disk-Subsystem unterstützt die Definition verschiedener Tiers für Disk-Cluster mit:

- unterschiedlichen physikalischen Eigenschaften. Zum Beispiel NVMe-Tier, SSD-Tier, HDD-Tier, usw.
- Schreibvorgänge auf dem HDD-Tier können durch eine SSD- oder NVMe-Disk beschleunigt werden, die als Puffer (Cache) verwendet werden. Dieser Beschleunigungsprozess ist optional, wenn ein Disk Set erstellt wird. Ein Beschleunigungsprozess ist nicht für jedes Disk Set erforderlich.
- Auf Datenträger geschriebene Daten können auf Wunsch verschlüsselt werden. Der Verschlüsselungsprozess wird softwarebasiert vom System durchgeführt und es ist möglich, die Verschlüsselung auf dem Datenträger für jede Tier separat auszuwählen.
- Bei der Erstellung einer virtuellen Maschine ist es möglich, eine optionale Auswahl aus verschiedenen Schichten wie HDD, Accelerated HDD, SSD, NVMe zu treffen, z. B. kann der Betriebssystemdatenträger von der Accelerated HDD, der Datenaufzeichnungsdatenträger von der SSD und ein Datenträger, der für Backup und Archivierung verwendet werden soll, von der HDD-Schicht ausgewählt werden.
- Für jeden virtuellen Datenträger ist es möglich, neben der Schicht auch Redundanzoptionen anzugeben. Es ist möglich, zwischen echten Kopien (2 oder 3) oder platzsparenden Redundanzschemata mit Erasure-Coding-Algorithmen zu wählen.
- Durch Erasure-Coding wird die Wahl von Schemata wie (3+2, 5+2, …, 17+3) und der für die Redundanz benötigte zusätzliche Plattenplatz reduziert (Plattenplatzeffizienz). Außerdem wird der unterbrechungsfreie Betrieb, auch bei Verlust von 1 bis zu 3 Nodes zur gleichen Zeit ermöglicht.
- Das sayFUSE HCI-System kann so ausgelegt werden, dass es den gleichzeitigen Ausfall von mehreren Nodes tolerieren kann.
- Virtuelle Festplatten können hinzugefügt und entfernt werden und ihre Größe kann erhöht werden, ohne dass die virtuellen Maschinen heruntergefahren werden müssen.
- Für virtuelle Datenträger können Vorlagen für "Speicherrichtlinien" erstellt werden, die sowohl die Auswahl der Schicht als auch der Redundanz umfassen.

2.1.3. Spezifikation der Bedienfeld des sayFUSE UCI-Infrastruktur

- Das Bedienfeld des Systems ist isoliert, um Standort-Systemadministratoren und nicht Anwendern eine eigene Verwaltung zu ermöglichen.
- Vorgänge wie die Definition eines neuen Mandanten/Standortes auf dem Systembedienfeld, die Festlegung des Benutzernamens und des Passworts des Kunden und die Bestimmung der Ressourcennutzungsquoten des Kunden, können über die Webschnittstelle durchgeführt werden.
- Das Bedienfeld bietet die Möglichkeit, in die virtuellen Maschinen, Projekte und Netzwerke des Mandanten/Standorts einzugreifen. Der Betreiber in der Zentrale ist in der Lage, einem Standort bei Bedarf Managed Services frei zu schalten.

2.1.4. Das Bedienfeld der Standortadministration

- Für jeden Standort/Mandant, der die sayFUSE HCI-Infrastruktur nutzt, ist ein eigenes Zugangspanel vorhanden. Der jeweilige Standort/Mandant ist in der Lage, mit seinem eigenen Benutzernamen und Passwort auf dieses Panel zuzugreifen und seine eigenen täglichen Operationen durchzuführen.
- Durch den Zugriff auf dieses Panel ist der jeweilige Standort/Mandant in der Lage, Vorgänge wie das Erstellen und Löschen virtueller Maschinen, den Zugriff auf die Konsole und das Ein- und Ausschalten der eigenen Maschinen durchzuführen.
- Der Standort/Mandant ist in der Lage, verschiedene Betriebszonen und Projekte auf seinem Panel zu erstellen und verschiedenen Benutzern die Durchführung von Operationen in verschiedenen Zonen

zu ermöglichen. Der Standort ist in der Lage, zu bestimmen, welcher Benutzer Operationen an welchem Projekt durchführen kann.

- Die Ressourcennutzung des Standorts/Mandanten kann auf der Grundlage von CPU, RAM, Festplatten-speicher, Festplattenzugriffshäufigkeit (IOPS) und Anzahl der Lastverteiler begrenzt werden. Diese **Begrenzung wird vom Systemadministrator vorgenommen** und es wird sichergestellt, dass der Standort diese Grenzen nicht überschreitet.
- Der Standort ist in der Lage, den **Nutzungsstatus seiner eigenen Ressourcen** über das Zugangspanel einzusehen.
- Der Standort ist in der Lage virtuelle Netze, die zu seinem System gehören zu erstellen und den IP-Adressbereich, den diese virtuellen Netze haben werden, zu bestimmen.
- Der Standort ist in der Lage, einen **virtuellen Router** zu definieren, der das Routing zwischen den von ihm erstellten virtuellen Netzen durchführt und ist in der Lage, die notwendigen Routen für diesen Router zu erstellen.
- Der Standort ist in der Lage, den DHCP-Dienst in seiner virtuellen Netzstruktur zu aktivieren. Der vom DHCP-Dienst zu verwendende IP-Adressenpool wird vom Standort festgelegt.
- Die vom **Standort geschaffenen virtuellen Netze sind von der physischen Netzstruktur unabhängig**. Das System weist in sich selbst eine **SDN-Struktur** (Software-definiertes Networking) auf.
- Die virtuellen Netze sind durch Verwendung von Technologien wie **VxLAN (Virtual Extensible LAN) und Geneve Technologie von der physischen Netzstruktur unabhängig.**
- Der Standort ist in der Lage, eine virtuelle Maschine in dem offenen gemeinsamen Netz (Internet) zu erstellen oder virtuelle Netze einzurichten und über einen virtuellen Router mit Hilfe von NAT auf das offene Internet zuzugreifen.
- Der Standort ist in der Lage, der im virtuellen Netzwerk erstellten virtuellen Maschine eine IP-Adresse zuzuweisen, um den Zugriff von außen (z.B. aus dem Internet) zu ermöglichen. Diese Adresse wird als **Floating-IP-Adresse** definiert und ihre Anzahl kann für den Kunden/Standort begrenzt werden.
- Mit Genehmigung des Standort-Systemadministrators ist der Standort in der Lage, seine eigenen Images virtueller Maschinen in das System zu importieren, um sie für die Erstellung virtueller Maschinen zu verwenden.
- Es existiert eine "**Regulierungsfunktion"** für eine nicht genutzte virtuelle Maschine. Die ausgelagerte Maschine bleibt in einem nicht-operativen Zustand, wird bei der Ressourcennutzung des HCI-Benutzers nicht mitgezählt und wird nicht in die Quotennutzung einbezogen. Wenn die ausgelagerte virtuelle Maschine aus dem Regal genommen und zum Leben erweckt wird, wird sie erneut als Nutzung innerhalb des Kontingents gewertet.
- Der Standort ist in der Lage, ein **IPSec-basiertes, verschlüsseltes VPN** einzurichten, um die virtuellen Netzwerke innerhalb seiner eigenen Struktur mit einer anderen Rechenzentrumskonfiguration außerhalb der Cloud-Struktur zu verbinden. Diese VPN-Definition ist ein integraler Bestandteil des Systems und erfordert keine zusätzliche Software oder Installation.
- Der Systemadministrator ist in der Lage, die Anzahl der VPN-Definitionen, die der Standort/Mandant vornehmen kann, zu begrenzen.
- Der Standort/Mandant ist in der Lage, einen eigenen sayTRUST VPSC Zero Trust in seinem SDN zu implementieren und zu verwalten. Die Lizenzen für das **sayTRUST Zero Trust Serverbetriebssystem** sind für jeden Standort/Mandant enthalten.
- Der Standort ist in der Lage für seine Nutzer mit seinem sayTRUST VPSC Zero Trust auch **PKI-Personal Key Identifikation, SSO (Single Sign-on), Applikation- und Desktop-Publishing** auszurollen.
- Der Systemadministrator ist in der Lage für den SDN des Standorts das **Backup und Restore** frei zu schalten und zu verwalten.

2.1.5. Leistungsumfang des Backup Restore Plattforms

- Die sayFUSE Backup Restore Plattform ist eine All-In-One Backup Appliance und arbeitet vollständig autark. Sie benötigt keine weitere Hardware und Software für Mediahandling.
- Das Backup System enthält Backup-/Dedup Backup Storage für den gesamten Sicherungsdatenbestand und sechs Backup-Laufwerke, die autark oder als Pool arbeiten.
- Die Backuplaufwerke schalten sich mit dem Job vor dem Backup ein, nach Abschluss der Sicherung wieder aus und ermöglichen den Mediabruch und die Auslagerung der.
- Jedes Backup-Laufwerk lässt sich unabhängig konfigurieren, steuern und überwachen.
- Jedes Backup-Laufwerk kann für parallele Sicherungen und Rücksicherungen konfiguriert werden.
- In den 6 Backup-Laufwerken des Backup Systems können wahlweise Backup Medien für die Auslagerung mit einer Kapazität von 1 TB bis zu 24 TB verwendet werden.
- Die integrierten Backup-Laufwerke können die Verwendung von einheitlichen und unterschiedlichen Medienkapazitäten verwalten.
- Das All-In-One Backup-System ermöglicht Backup-to-Dedup, Backup-to-Disk, Migration-Storage-to-Disk, Medienbruch und Auslagerung.
- Das Backup-System ist standardmäßig mit zwei 2x50 Gbit/s und 2x10 Gbit/s Ethernet Anschlüssen für die Sicherung und Rücksicherung ausgestattet. Erweiterung mit weiteren 2x100 Gbit/s Anschlüssen sind möglich.
- Das System enthält ein BMC-Modul für Remote-Management.
- Die Kontrollsoftware (Media-Handling) der Backup-Laufwerke und Backup-Medien ist im Backup-System integriert.
- In das Backup-System ist ein Ersatz-Backup-Laufwerk integriert, so dass Laufwerk- und Medienfehler aufgefangen werden. Bei Auftreten solcher Fehler wird die Sicherung auf das Ersatz-Backup-Laufwerk geschrieben.
- Sowohl die Backup-Laufwerke als auch die Sicherungsmedien sind eineindeutig konfigurierbar und werden von der Kontrollsoftware gesteuert.
- Die Backup-Laufwerke und Backup-Medien lassen sich eindeutig über Backup Jobs steuern.
- Backuplaufwerke werden mit dem Job eingeschaltet und nach der Ausführung des Jobs wieder abschalten. So wird der Energieverbrauch signifikant reduziert und die Lebensdauer der Medien deutlich erhöht und Missbrauch signifikant reduziert.
- Der Standort ist in der Lage seine eigene Datensicherung inklusive Medienbruch und Auslagerung zu verwalten.
- Zum Schutz vor Fremdzugriffen befinden sich die Backup-Medien hinter abschließbaren Klappen.
- Die Tages-, Wochen-, Monats-, Jahressicherungen sind konfigurierbar und werden vollautomatisch durchgeführt.
- Die Backup-Medien können im laufenden Betrieb ausgewechselt und zur Auslagerung entnommen werden.
- Im Standardlieferumfang des Backup-Systems ist eine Auslagerung der Datensicherung bis zu 144/288 TB (native/ compressed) enthalten. Die Kapazität lässt sich bei Bedarf erweitern.
- Für die Backup-Library-System sind keine Reinigungskartuschen erforderlich.
- Das Backup-Library-System hat keine mechanischen Verschleißteile und weist keine Start-Stopp-Verhalten für die Backup-Medien auf.
- Die Backup-Medien sind elektromagnetisch abgekapselt.

- Die Backup-Medien können für die Auslagerung verschlüsselt werden.
- Das Backup-System ermöglicht die Duplikation der Backups vor der Auslagerung.
- Das Backup-System unterstützt Dedup-Backup um Netzwerklast und Zeitfenster zu reduzieren. Das Backupsystem ermöglicht ein Life-Backup mit einer Geschwindigkeit bis zu 12 TB in der Stunde.

2.1.6. Leistungsumfang der sayTRUST VPSC Zero Trust

- Die sayTRUST VPSC (Virtual Private Secure Communication) ist eine **personifizierte Zero-TRUST Multi Faktor Kommunikationslösung** für die Kommunikation der Anwender von einem beliebigen Standort und einem beliebige Clientrechner über die **Defence-Depth-Technologie**.
- Die sayTRUST Technologie ermöglicht eine sichere Verbindung über Mehr-Stufen-Authentifizierung und ohne aufwändige, starre und zeitintensive Installation und Konfiguration auf dem jeweiligen Anwender-PC.
- Die Kommunikation zwischen dem Client-Rechner und dem Remote-Netzwerk erfolgt ohne **Netzwerk-Netzwerk-Kopplung.**
- Der Client Rechner hat keine Informationen über das Remote-Netzwerk.
- Der Zugriff auf Anwendungen und Ressourcen erfolgt Zertifikatbasiert nach eindeutiger Identifizierung (PKI) des Nutzers entsprechend seiner Berechtigungen.
- Eine Lizenz für das Server Betriebssystem ist für die sayTRUST VPSC-Technologie für jeden Standort/Mandanten enthalten.
- Im sayTRUST VPSC Server Betriebssystem ist eine eigene integrierte, unabhängige Certificate Autority (CA) enthalten und eine PKI wird unterstützt.
- sayTRUST VPSC erzeugt und verwaltet eigene Certificate-Authority basierende, unabhängige, fälschungssichere und geschützte Zertifikate.
- Die Identitätsprüfung des Anwenders erfolgt vor Nutzung am Client-Rechner.
- Die Konfiguration der Anwenderzertifikate ist mit S-LDAP und manuell möglich.
- sayTRUST VPSC ermöglicht eine getunnelte Kommunikation für **lokale- sowie remote- und mobile Anwendungen**, die sich auf dem User Token befinden können.
- Serverseitige erzeugte Anwenderzertifikate **steuern das Erlauben, Blockieren und Isolieren** von **remote und/oder lokalen und oder mobilen Applikationen und Ressourcen**.
- Die verschlüsselte Kommunikation erfolgt **innerhalb der Applikationsebene aus dem Arbeitsspeicher (RAM) der Client-PC**s, anstatt über Netzwerk-Netzwerk-Kopplung der Netzwerkkarte.
- Die verschlüsselte Kommunikation erfolgt über eine **mehrstufige Defence-in-Depth Kommunikationssicherheit**.
- Während der Verbindung des Anwenders über den Remote Clientrechner, Fremdrechner aus dem Heim- oder Fremdnetzwerk ist **keine Möglichkeit für das Scannen des Remotenetzwerkes** gegeben.
- Der Anwenderrechner ist sogar während der VPSC-Kommunikation mit den Remotenetzwerk von diesem entkoppelt. Es gibt **keine Möglichkeit über den Anwenderrechner Rückschlüsse auf das zu schützende Netzwerk zu ziehen**.
- Es ist eine zentrale Administration zum Erstellen und Ausrollen der **Berechtigungen für Applikationen, Geräte, Netzwerkressourcen und der Verzeichnisse** vorhanden.
- Es ist ein **zentrales Verteilungssystem** für das Ausrollen der Anwenderzugänge unabhängig vom Standort und PC für die Erstimplementierung enthalten und darüber können auch automatisch spätere Anpassungen, Updates und Änderungen ausgerollt werden.

- Es ist möglich **Shares** aus dem zu schützenden Netzwerk dem Client-PC bereitzustellen, **ohne das der Client-PC und das Netzwerk gekoppelt werden** und ohne Verwendung von virtuellen Netzwerkkarten.
- Die Technologie ermöglicht die Bereitstellung von Netzwerkshares **mit oder ohne Laufwerkszuordnung** und unter Verschleierung der Netzwerkinformationen.
- Die sayTRUST Technologie ermöglicht die Nutzung als **Internal Network Protection** (INP) um die interne Netzwerksicherheit maximal zu erhöhen.
- Der **Zugriff auf Anwendungen und Ressourcen erfolgt zertifikatbasiert** und nach eindeutiger Identifizierung (PKI) des Nutzers und seiner Berechtigungen. Der Anwender kann ausschließlich mit den zugewiesenen Ressourcen arbeiten.
- Als Anwender-Token sind AES versschlüsselte USB-Tokens und Clientsoftware oder App für mobile Geräte vorhanden.
- Als sayTRUST Anwender-Token sind Ausführungen für die AES verschlüsselte Tokens mit PIN-Pad, biometrische Flashdisk oder Mikroprozessor basierende vorhanden.
- Die Tokens weisen AES256 Bit Verschlüsslung auf.
- sayTRUST Technologie ermöglicht eine parallele Nutzung von unterschiedlichen sayTRUST Client-Tokend, wie:
    - Client-Software
    - Mobile App
    - Secure SSD (AES256)
    - Secure USB-Token mit 3-Faktor Authentifizierung (**AES 256 Bit Microprozessor basierend** + Zertifikat + Passwort + Biometrie)
    - Secure USB-Stick mit 3-Faktor Authentifizierung (**AES 256 Bit Flashdisk basierend** + Zertifikat + Passwort + Biometrie)
    - Secure USB Stick (**AES 256 Bit**, Flash disk basierend + Zertifikat + Passwort + **PIN Pad**).

2.1.7. Funktionsumfang der Virtual Private Secure Communication (VPSC)

- Anwender-Computer erkennt den mikroprozessorbasierten sayTRUST Access Stick erst nach biometrischer Identifikation des Anwenders (**PKI**) oder PIN.
- Die 8-stufige Defence-in-Depth Zugangssicherheit (**DiD**) beginnt vor der Nutzung am Client-PC. Die Prüfung der Anwender erfolgt vor der Nutzung am Client-PC. Ausschließlich nach einer eindeutigen Identifizierung des Anwenders kann der sayTRUST Token verwendet werden.
- Die Kommunikationssicherheit beginnt im Ursprung **aus dem verschlüsselten RAM** des Client-PCs durch Perfect-Forward Secrecy (PFS).
- Verbindungsaufbau ohne Installation von jedem beliebigen Rechner mittels Remote Access Device.
- Passwortmanager für Single Sign-on (SSO) ist integriert.
- Filetransfer für unterbrechungsunabhängigen **File Transfer und Synchronisation** ist enthalten. Dadurch wird ein Kopier-/Synchronisationsvorgang auch nach einem Verbindungsabbruch wieder an der letzten Stelle aufgenommen.
- **Portable App Verwaltung** für mobile Anwendungen wie Mail-, Telefonclient oder Office Anwendungen ist integriert.
- In der sayTRUST Technologie ist ein Applikationsgateway für **Anwendungsfarmen und/oder virtuelle Anwendungen** für Citrix-, Microsoft-, Linux- und Webapplikationen **ohne Portfreigabe** nach außen oder Installation von Receivern am Anwender-PC integriert.
- Secure Wake on LAN (**sWo**L) auch über mehrere Gateways und Netzwerke ist integriert.

- Im System ist ein Encryption-Tool (**ET**) für Anwender zur Erstellung von persönlichen verschlüsselten Containern innerhalb des AES verschlüsselten Micro-/Flashchips integriert.
- Browserfunktion für eine Unabhängigkeit von installierten Web-Browsern ist integriert.
- Prüfung von Berechtigungen von Anwendern beginnt vor Beginn des Tunnelaufbaus.

2.1.8. Merkmale des Client Tokens

- **Beginn der Policy Überwachung vor dem Tunnel**
- Keine Abhängigkeit vom Client-PC
- **Keine Netzwerk-Netzwerk Kopplung** mit dem Remotenetzwerk
- **Verbindung auf der Applikationsebene**
- **Verbindung aus dem Arbeitsspeicher** (RAM) des Client-PCs heraus
- **Keine verbleibenden Spuren** auf dem Client Rechner und Keine verbleibenden Spuren der Verbindungsstrecke.
- **Das Client Gerät hat und kennt keine Netzwerkinformationen** vom zu schützenden Remote-Netzwerk
- **Kommunikation nur für nicht manipulierte Zertifikate** möglich
- **Remote PC wird nicht Mitglied des Netzwerkes** und kennt diese nicht
- **Tunnelaufbau für Applikationen aus dem Arbeitsspeicher** des Clientrechners
- **Keine Verbindungen für nicht autorisierte Anwendungen**
- **Gezieltes Blockieren** der Kommunikation für unerwünschte Anwendungen
- Für die Kommunikation wird im Prozessspeicher - **in Abhängigkeit des Client-Zertifikats nach Diffie-Hellman** ein neuer, bis dahin niemandem bekannter Schlüssel generiert und zusätzlich verschlüsselt
- **Keine Installation einer virtuellen Netzwerkkarte** auf dem Endgerät
- **Keine Installation einer Clientsoftware** (optional, wenn Token nicht gewünscht)
- **Schutz vor „Man-in-the-Middle-Angriff“**