



# sayTRUST<sup>®</sup> Access

## Cluster-Lösung mit sayTRUST<sup>®</sup> Access

Whitepaper

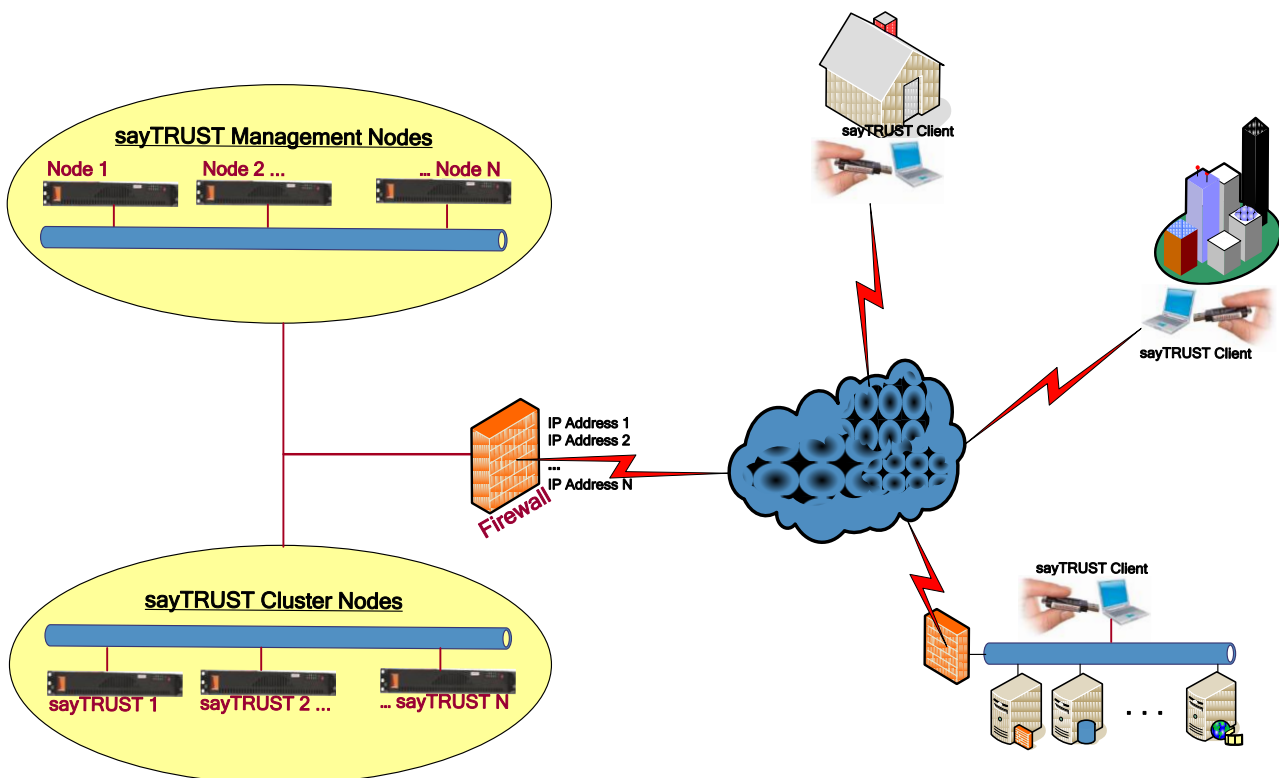
Oktober 2010



## sayTRUST® Access Cluster

Die sayTRUST Access Lösung ist eine hochsichere Remote-Access-Lösung für die Anbindung von mobilen Anwendern und Heimarbeitsplätzen. Die über Drei-Faktor-Authentifizierung verfügenden Access Clients greifen getunnelt auf die entfernten Ressourcen zu. Dabei entsteht zwischen dem Client und dem entfernten Netzwerk keine direkte Netz-zu-Netz bzw. Host-zu-Netzverbindung, es werden nur die einzelnen Anwendungen getunnelt.

In Umgebungen, in denen keine Ausfälle toleriert werden, empfiehlt sich der Aufbau eines sayTRUST Cluster Systems. Für den Aufbau eines sayTRUST Clusters sind mindestens zwei sayTRUST Server Nodes und mindestens ein sayTRUST Management Node erforderlich. Der Cluster kann bis zu 48 sayTRUST Server Nodes und mehrere Management Nodes enthalten.

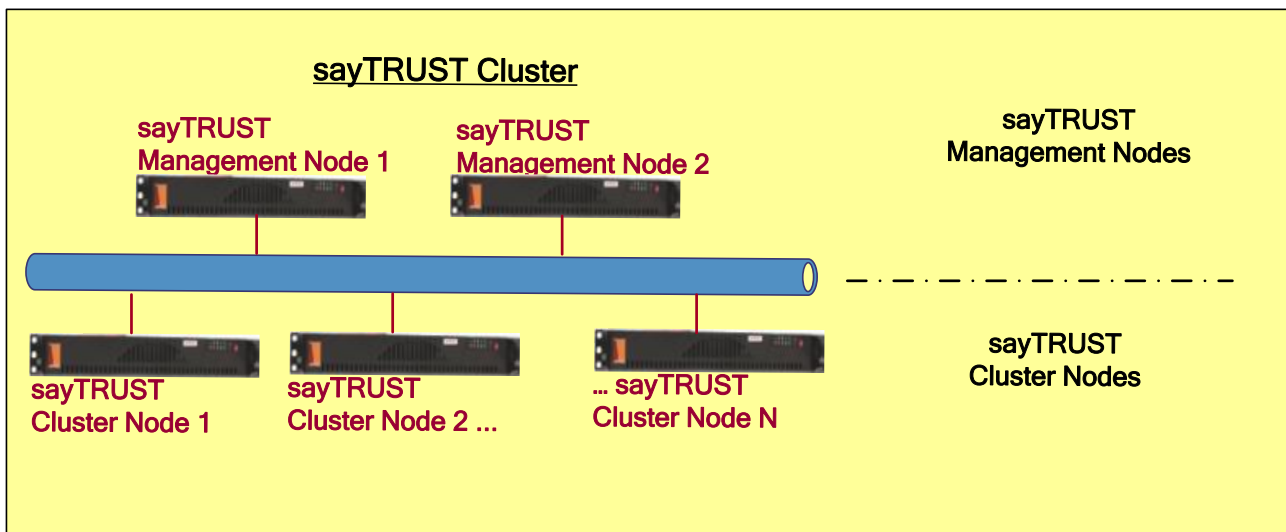


### Funktionsweise des sayTRUST Clusters

Der sayTRUST Cluster besteht aus **sayTRUST Management Nodes** und **sayTRUST Clustern Nodes**. Die Verwaltung der Zertifikate, Gruppen und Userinstellungen sowie die Netzwerkeinstellungen übernehmen die sayTRUST Cluster Nodes. Die sayTRUST Management Nodes sorgen dafür, dass auf allen sayTRUST Cluster Nodes die gleichen Informationen bzgl. der Zertifikate und Gruppen etc. vorhanden sind. In einem sayTRUST Cluster ist mindestens ein Management Node erforderlich. Empfohlen wird wegen der Ausfallsicherheit mindestens zwei sayTRUST Management Nodes zu verwenden.

Die sayTRUST Cluster Nodes ersetzen den klassischen sayTRUST Server um neben der Ausfallsicherheit auch eine Lastenverteilung zu erzeugen.

## sayTRUST® Access Cluster



Auf den einzelnen sayTRUST Cluster Nodes ändert sich seitens der Konfiguration nur die verwendete Lizenz (sayTRUST Cluster Node Lizenz). Mit Eingabe der Lizenz wird dem sayTRUST Cluster Node eine eindeutige Cluster-ID zugewiesen. Anhand dieser ID kann der sayTRUST Management Node die Datensynchronisation vornehmen.

Die sayTRUST Management Nodes müssen lediglich mit IP-Adressen und den Node-IDs der sayTRUST Cluster Nodes und der sayTRUST Management Node Lizenz ausgestattet werden. Die anschließende Datensynchronisation erfolgt automatisch.

Um einen effektiven Lastenausgleich zu erzielen sind entsprechend der Anzahl der sayTRUST Nodes offizielle IP Adressen und/oder entsprechende Anzahl von DNS-Einträgen erforderlich. Diese werden bei der Konfiguration des sayTRUST Clusters in die Client-Konfiguration übertragen. Der Client ist dann dazu in der Lage einen Lastenausgleich durch das Round-Robin-Verfahren herbeizuführen. Alternativ kann der Client auch für einen zufälligen sayTRUST Cluster Node aus einer vorgegebenen Liste konfiguriert werden.

Alternativ ist es möglich das Round-Robin-Verfahren über einen DNS-Eintrag abwickeln zu lassen. In diesem Falle wird dem sayTRUST Client nur ein Verbindungseintrag mitgeteilt. Das eigentliche Round-Robin geschieht durch den DNS-Server.

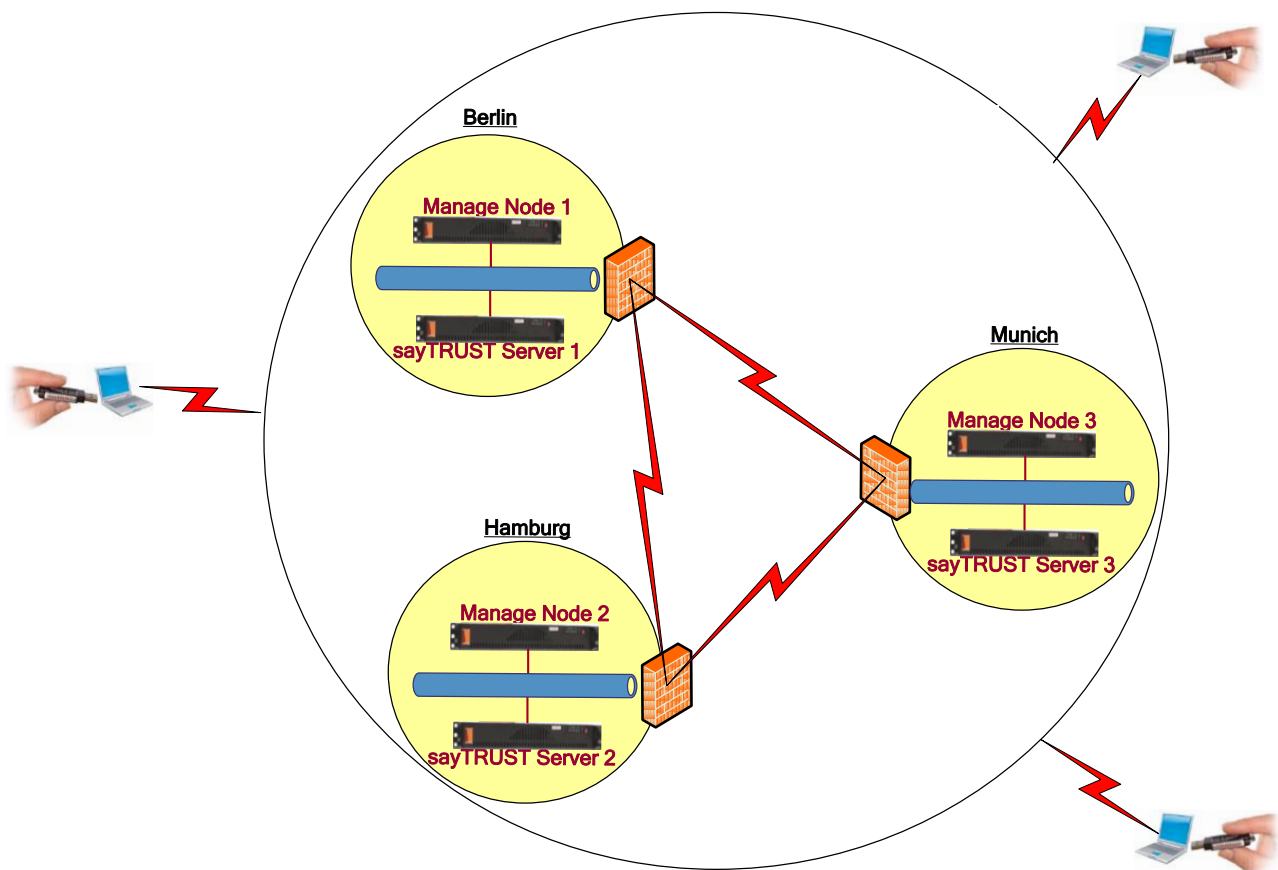
Eine dritte Möglichkeit wäre, den Round-Robin portbasierend ablaufen zu lassen. In diesem Falle würde nur eine externe IP Adresse benötigt. Der Nachteil dieses Ansatzes ist, dass die gewählten Ports möglicherweise von der Firewall clientseitig gesperrt sind und deshalb keine Verbindung zustande kommt.

Um die Ausfallsicherheit zu erhöhen ist es möglich, die sayTRUST Cluster Nodes und sayTRUST Management Nodes räumlich getrennt aufzustellen. Die einzige Voraussetzung ist, dass jeder sayTRUST Management Node alle anderen sayTRUST Management Nodes und jeder sayTRUST Management Node alle sayTRUST Cluster Nodes erreichen kann.

Um einen Cluster über mehrere Standorte zu verbinden ist eine ausreichend große Netzanbindung erforderlich. Ebenso sollten die Daten nur über ein VPN/MPLS Netz ausgetauscht werden, da die Kommunikation zwischen sayTRUST Cluster und sayTRUST Management Nodes unverschlüsselt abläuft.

## sayTRUST® Access Cluster

Beispiel einer Standortvernetzung mit getrennten sayTRUST Management und Cluster Nodes:



In diesem Beispiel steht der sayTRUST Cluster verteilt über drei Standorte. Die Standorte sind untereinander mit VPN verbunden.

Mit diesem Aufbau werden nun alle Änderungen an allen Standorten gleichzeitig aktiv. Wenn also jemand am Standort „München“ einen Benutzer hinzufügt, ist es sofort möglich sich auch am Standort „Hamburg“ damit anzumelden.

Diese Art der Verteilung hat den Vorteil dass die mobilen Benutzer auf die Server von Berlin und Hamburg zugreifen können (sofern die sayTRUST Policy dies erlaubt), selbst wenn der Zugangspunkt München nicht erreichbar sein sollte.