08 | 26 Sonderdruck für Giritech

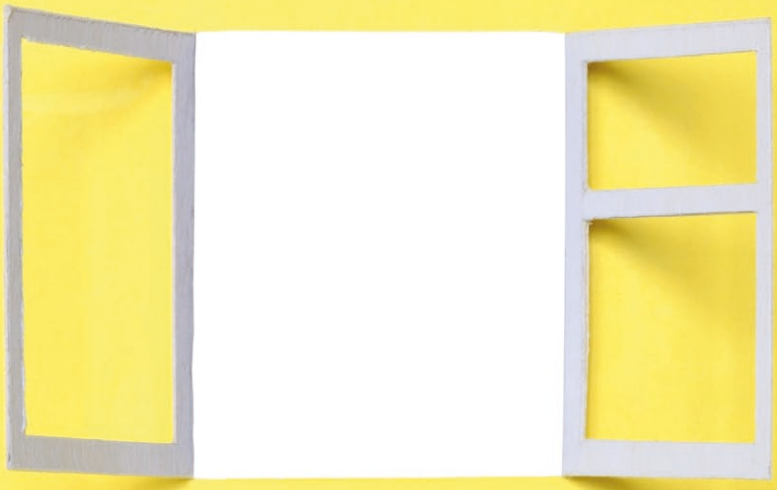
IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Cybele Software Thinfinity Workspace 8.5

www.it-administrator.de

Cybele Software
Thinfinity Workspace 8.5

Ein Fenster öffnet sich



Quelle: kvkirillov – 123RF

von Dr. Christian Knermann

Wie fügen sich Legacy-Anwendungen in eine moderne Netzwerkarchitektur? Cybele Software beantwortet diese Frage mit Thinfinity Workspace. Die Plattform veröffentlicht Windows-Desktops und -Anwendungen sowie weitere Ressourcen weitgehend clientlos im Browser. IT-Administrator hat Thinfinity ausprobiert und war vom breiten Funktionsumfang sehr angetan.

Die Anforderungen an die Netzwerksicherheit unterliegen einem stetigen Wandel – Unternehmen betreiben ihre IT-Infrastruktur längst nicht mehr ausschließlich innerhalb eines klar abgegrenzten internen Netzwerks mit Perimeterfirewall als Schutz gegenüber dem Internet. Hybride Betriebsmodelle, bei denen Ressourcen sowohl on-premises als auch in einer oder mehreren Public Clouds bereitstehen, werden zur Regel. Der Paradigmenwechsel hin zu Zero Trust Network Access (ZTNA) adressiert genau diesen Wandel. Doch während Administratoren ihre Infrastrukturen auf Netzwerkebene ZTNA-tauglich machen und Entwickler ihre Applikationen auf moderne Webarchitekturen umstellen, bleibt eine praktische Herausforderung bestehen.

In vielen Unternehmen bilden klassische Windows-Applikationen, Remotedesktopdienste oder eine Virtual Desktop Infrastructure (VDI) nach wie vor wichtige Säulen des Arbeitsalltags – oft als klassische Client-/Serveranwendungen mit Abhängigkeiten zu einem lokalen Microsoft Active Directory (AD), Datenbanken und Dateidiensten. Hinzu kommen historisch gewachsene Webanwendungen, Linux-Systeme sowie Hostsysteme und Mainframes. Solche Legacy-Anwendungen lassen sich nicht ohne Weiteres in eine Cloud migrieren oder durch einen modernen SaaS-Dienst ersetzen. All diese Ressourcen sicher über öffentliche Netze bereitzustellen erfordert eine Plattform, die Zugriffe über unsichere Netze mit einem modernen Sicherheitsmodell verbindet. Genau hier setzt Cybele Thinfinity Workspace an.

Sicherer Zugriff auf Legacy-Anwendungen

Das US-amerikanische Unternehmen Cybele Software entwickelt seit vielen Jahren Technologien für den sicheren Fernzugriff auf Anwendungen und Desktops. Im Mittelpunkt steht Thinfinity Workspace als universelle Access-Plattform, die sich als Alternative zu etablierten Produkten wie Citrix Virtual Apps and Desktops, Omnissa Horizon (ehemals VMware Horizon), Nutanix oder Microsoft Azure Virtual Desktop und Nerdio positioniert. Verglichen mit diesen oft hochkomplexen Plattformen zielt Thinfinity Workspace auf eine schlankere Bereitstellung ab, die weitgehend ohne dedizierte Clientsoftware auf den Endgeräten auskommt und dennoch eine vollwertige Applikationsbereitstellung auf Basis von Remotedesktopdiensten und VDI ermöglicht.

Daneben bietet Cybele mit Thinfinity VirtualUI eine Entwicklungsplattform an, die es erlaubt, native Windows-Desktopapplikationen mit minimalem Codeaufwand in webbasierte Anwendungen zu transformieren. Entwickler integrieren dazu eine proprietäre DLL in eine bestehende Anwendung, die anschließend in HTML5-kompatiblen Browsern läuft. Für Softwarehersteller und Unternehmen mit eigenentwickelten Windows-Applikationen eröffnet das einen Modernisierungspfad ohne vollständige Neuentwicklung.

Thinfinity VNC ist ein proprietäres Remoteprotokoll mit gegenüber herkömmlichen VNC-Implementierungen optimierter Performance und erweiterten Sicherheitsfunktionen. Es ermöglicht VNC-Sitzungen im HTML5-fähigen Browser, ohne Plug-ins oder Clientinstallationen vorauszusetzen. Für die Integration von Hostsystemen hält Cybele mit z/Scope einen klassischen Terminal-Emulator bereit, der den Zugriff auf IBM Mainframes der z- und i-Serie sowie weitere UNIX-Systeme abdeckt.

Ergänzend adressiert TN Bridge die Konnektivität zu IBM S/390- und AS/400-Systemen. Beide Produkte integrieren sich als Multi-Terminal-Verbindungen direkt in Thinfinity Workspace und erweitern den Funktionsumfang der Plattform um den Zugang zu klassischen Hostumgebungen, die in vielen Branchen nach wie vor eine wichtige Rolle spielen. Im Fokus

dieses Tests stand jedoch der Zugriff auf klassische Windows-Anwendungen über Thinfinity Workspace.

In der DACH-Region übernimmt die Giritech GmbH mit Sitz in Eriskirch am Bodensee exklusiv den Vertrieb von Thinfinity Workspace einschließlich Implementierungsunterstützung. Giritech bietet dabei ein vereinfachtes Lizenzmodell auf Basis gleichzeitiger Benutzer (Concurrent User) an, das bei zehn gleichzeitigen Benutzern startet und in Staffeln bis über 10.000 User skaliert. Die Lizenzierung erfolgt als Subscription mit Laufzeiten von zwölf oder 36 Monaten; Kunden können ihr Lizenzvolumen während der Laufzeit jederzeit in Schritten von mindestens fünf Lizenzen erweitern oder zu Beginn einer neuen Mietperiode reduzieren. Die Subscription umfasst sowohl die Serverkomponenten als auch die Softwarewartung.

Durchdachte Architektur mit Sicherheitskonzept

Die Architektur von Thinfinity Workspace folgt einem modularen Ansatz mit mehreren Rollen, die Administratoren entweder gemeinsam auf einem einzigen Server installieren oder auf verschiedene Maschinen, Standorte und Netzsegmente verteilen können. Im Kern besteht die Infrastruktur aus einem Gateway, einem Primary Broker, optional einem oder mehreren Secondary Brokern sowie den ebenfalls optionalen Agenten (Bild 1).

Das Gateway ist der nach außen exponierte Zugangspunkt. Es findet typischerweise in einer DMZ seinen Platz und ist die einzige Komponente, die eine öffentliche IP-Adresse benötigt. Clientverbindungen nimmt es ausschließlich über HTTPS mit TLS 1.3, standardmäßig auf TCP-Port 443, entgegen. Damit entfällt für externe Zugriffe die Notwendigkeit, in den jeweiligen Remotenetzen Ports freizugeben.

Das Gateway arbeitet als Reverse-Proxy und speichert weder Benutzerdaten noch Sitzungsstatus. Es terminiert die TLS-Verbindungen der Clients und leitet die Sitzungen an den zuständigen Broker weiter. Auch die interne Kommunikation mit den übrigen Komponenten erfolgt ausschließlich verschlüsselt über TLS 1.3. Wer Hochverfügbarkeit und Lastverteilung benötigt, stellt mehrere Gateway-Instanzen hinter einem Loadbalancer bereit.

IdP-Integration ohne Lücken

Der Primary Broker bildet das operative Herzstück der Plattform: Er übernimmt Benutzerauthentifizierung, Sitzungsverwaltung, Umsetzung von Zugriffsrichtlinien und Koordination der Verbindungen zu den Backend-Zielsystemen. Standardmäßig bringt er eine eingebettete Delphi Absolute Database mit, alternativ lässt sich ein separater SQL-Server einbinden. Für die Authentifizierung unterstützt der Primary Broker Active Directory sowie weitere Identity Provider über OAuth 2.0, SAML 2.0, LDAP, RADIUS und Web-Authn – letzteres in Verbindung mit Passkeys oder FIDO2-Token.

Secondary Broker erweitern die Architektur um logisch oder geografisch separierte Standorte und Umgebungen, on-premises wie in der Cloud. Sie residieren typischerweise in den Zielnetzen, in denen sich die eigentlichen Ressourcen befinden – Remotedesktopdienste, VDI-Hosts oder einzelne physische Systeme. Da Secondary Broker ausschließlich ausgehende WebSocket-Verbindungen zum Gateway aufbauen, müssen Administratoren in den Zielnetzen keine eingehenden Ports öffnen. Mehrere Secondary Broker lassen sich zu einem Pool zusammenfassen, um Hochverfügbarkeit und Lastverteilung zu gewährleisten.

Agenten verkörpern eine weitere Bereitstellungsform: Dabei installieren Administratoren eine schlanke Thinfinity-Komponente direkt auf Zielsystemen. Jeder Agent meldet sich mit einer eindeutigen Agent-ID und kommuniziert wie ein Secondary Broker ausschließlich über ausgehende HTTPS-Verbindungen mit dem Gateway. Auch Agenten lassen sich zu Pools zusammenfassen – typischerweise mit einem Poolnamen, der im Golden Image hinterlegt ist, das als Vorlage für Desktopinstanzen innerhalb einer VDI dient.

Multicloud-Anbindung mit breiter Plattformunterstützung

Der Cloud Manager ist ein integriertes Modul von Thinfinity Workspace, das auf Basis eines solchen Images virtuelle Desktops bedarfsgerecht provisionieren, starten und stoppen sowie Benutzer dynamisch oder statisch zuweisen kann. Er unterstützt eine breite Palette an Plattformen – on-premises wie in Public Clouds: VMware vSphere, Microsoft Hyper-V, Proxmox, Oracle KVM sowie Microsoft Azure, Amazon Web Services, Google Cloud Platform, IONOS Cloud, Oracle Cloud und Verge.IO. Darauf kommen wir weiter unten noch zurück.

Für die Evaluierung oder kleinere Produktivumgebungen fasst ein All-in-one-Setup alle Rollen auf einem einzigen Windows-Server zusammen. In größeren Umgebungen empfiehlt der Hersteller, Gateway und Broker min-

Cybele Software Thinfinity Workspace 8.5

Produkt
Software für den Remotezugriff auf Windows-, Linux- und Webapplikationen.

Hersteller
Cybele Software
www.giritech.de/cybele/thinfinity.html

Preise
Die Mindestmenge von zehn gleichzeitigen Benutzern bei einer Mietnutzungsdauer von zwölf Monaten startet bei 9,90 Euro pro Benutzer und Monat. 100 bis 499 gleichzeitige Benutzer kosten 6,97 Euro pro Benutzer und Monat bei einer Mietnutzungsdauer von zwölf Monaten oder 5,57 Euro bei einer Mietnutzungsdauer von 36 Monaten.

Systemvoraussetzungen
- Hardware: Quadcore-Prozessor (Intel oder AMD, x86_64) mit 2 GHz oder mehr, 8 GByte RAM oder mehr, 50 GByte freier Massenspeicher (SSD).
- Betriebssysteme für die Serverkomponenten: Microsoft Windows (x64) von 8 bis 11 oder Server 2012 bis 2025.
- Client: HTML5-fähiger Browser plattformunabhängig, alternativ Desktopclient für Microsoft Windows.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

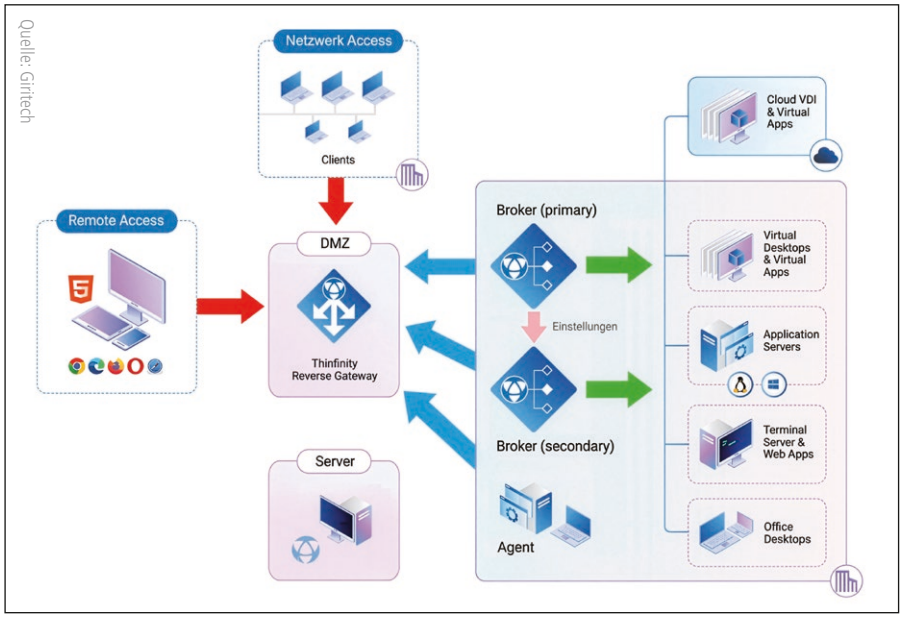


Bild 1: Thinfinity Gateway, Broker und Agenten bilden eine nahezu beliebig skalierbare Plattform.

destens auf separate Maschinen zu verteilen. Die Dokumentation beschreibt darüber hinaus Referenzarchitekturen für Hochverfügbarkeit und Lastverteilung, Multi-Tenant-Umgebungen mit mehreren Kunden und Domains sowie IT-/OT-Szenarien, in denen etwa sicherer Fernzugriff auf Anlagensteuerungen gefragt ist. In unserer Testumgebung haben wir uns für ein All-in-one-Setup entschieden, um Remotedesktopdienste und virtuelle Desktops unter Windows nach extern zu publizieren.

All-in-one-Setup schnell erledigt

Für unseren Test hatten wir einen Windows Server 2022 vorbereitet sowie mehrere Remotedesktop-Sitzungshosts (RDSH) und virtuelle Desktops, auf die wir von extern zugreifen wollten. Die Installation war in wenigen Minuten abgeschlossen – es genügte, die Nutzungsbedingungen zu akzeptieren und den Installationspfad zu bestätigen. Nach Abschluss der Setup-Routine bot diese direkt an, den Thinfinity Configuration Manager zu starten. Dabei handelt es sich um eine Windows-Applikation, die je nach gewählter Rolle die grundlegende Konfiguration des Servers in unterschiedlichem Umfang steuert.

Die weitergehende Konfiguration übernimmt das Webfrontend, dessen Funktionsumfang ebenfalls von Rolle und Berechtigungen des angemeldeten Benutzers abhängt. Nicht privilegierte Benutzer erreichen darüber die für sie freigegebenen Ressourcen; Administratoren verwalten und veröffentlichen Ressourcen, vergeben Berechtigungen und pflegen die zugehörigen Richtlinien. Auch der Cloud Manager ist ins Webfrontend integriert.

Im Thinfinity Configuration Manager wählten wir zunächst die Rolle "All-in-one", die sämtliche Komponenten auf einem Server zusammenfasst. Im nächsten Schritt bot der Assistent an, eine neue Testseriennummer abzurufen oder eine vorhandene Seriennummer online beziehungsweise offline zu aktivieren. Wir entschieden uns für die Onlineaktivierung der Testlizenz, die wir zuvor von Giritech erhalten hatten. Anschließend präsentierte der Configuration Manager seine Konfiguration aufgeteilt auf mehrere Registerkarten.

Im Bereich "General" war zunächst nur der unverschlüsselte Zugriff auf das Webfrontend über HTTP und den benutzerdefinierten TCP-Port 9443 vorgesehen. Wir ergänzten den HTTPS-Zugriff über TCP-Port 443, wofür wir vorab ein Zertifikat erstellt und im Zertifikatspeicher des Servers hinterlegt hatten. Zu empfehlen ist hier ein Zertifikat einer öffentlich anerkannten Zertifizierungsstelle, da alle Clients diesem vertrauen müssen, um reibungslos zugreifen zu können. Zusätzlich hatten wir eine Portweiterleitung von extern auf unseren Server eingerichtet.

Besondere Aufmerksamkeit verdient der Parameter "Network ID" auf der Registerkarte "Broker". Sein Wert muss auf allen Thinfinity-Komponenten einer Infrastruktur – also auf allen Gateways, Brokern und Agenten – identisch sein, damit diese sich gegenseitig erkennen. Umgekehrt dürfen im selben Netzsegment durchaus mehrere unterschiedliche IDs existieren; Komponenten mit abweichender ID gehören dann zu separaten Infrastrukturen und sind füreinander unsichtbar. Bei verteilten Rollen kommt diesem Parameter damit eine besondere Bedeutung zu.

Da Thinfinity Workspace die Anmeldung über das lokale AD bereits standardmäßig unterstützt, mussten wir im Configuration Manager lediglich dem Adminis-tratorkonto die Berechtigungen für alle Bereiche des Webfrontends erteilen und uns dann der weiteren Konfiguration widmen.

Multifaktor-Unterstützung mit kleinen Abstrichen

Im Frontend navigierten wir über das Benutzericon oben rechts zu den Einstellungen und dort zum Bereich "Configuration / Authentication". Unter "Authentication Methods" war der "Windows Logon" bereits aktiviert. Über die Schaltfläche "+ Add" lassen sich optional weitere Methoden konfigurieren, darunter Passkeys, RADIUS und SAML. Zudem fanden wir vorkonfigurierte OAuth-2.0-Provider – neben Google, Azure und Okta auch Facebook, LinkedIn und Dropbox. Für solche Anbieter erlaubt Thinfinity Workspace im Bereich "Identity Mappings" eine Abbildung auf interne Benutzerkonten, um den Zugriff auf Ressourcen zu steuern. Wir blieben bei der direkten AD-Anmeldung, wollten diese aber durch Multifaktor-Authentifizierung (MFA) absichern.

Dafür stehen im Bereich "Two-Factor Authentication" drei Optionen bereit: eine integrierte Methode für Time-based One-time Passwords (TOTP), die Integration mit Cisco Duo oder RADIUS MFA. Letztere bedient der Distributor mit dem optionalen Giritech Authenticator (siehe Abschnitt "MFA für Fortgeschrittene").

Im Rahmen unseres Tests nutzten wir die integrierte MFA, die Apps wie Google Authenticator oder Microsoft Authenticator unterstützt und grundlegende Anforderungen erfüllt. Konfigurierbar sind die TOTP-Länge mit sechs, sieben oder acht Stellen sowie der Hash-Algorithmus: SHA-1, SHA-256 oder SHA-512. Der gewählte SHA-Algorithmus bildet die kryptografische Grundlage, die aus dem geteilten Geheimnis und dem Zeitwert einen nicht vorhersagbaren, nicht umkehrbaren Hash erzeugt, der als Basis für den einmaligen Code dient. Zusätzlich lässt sich das MFA-Verfahren für einzelne Benutzer zurücksetzen.

Nach der Konfiguration und der Zuordnung zum Windows-Logon forderte das Webfrontend beim nächsten Login zur MFA-Einrichtung auf und präsentierte den üblichen QR-Code, allerdings ohne den zugehörigen alphanumerischen String. Wer einen alternativen TOTP-Generator ohne QR-Code-Scanner verwenden möchte, etwa einen Passwort-Safe, muss den QR-Code auf anderem Weg auslesen. Mit eingerichteter MFA wandten wir uns den Remoteverbindungen zu und navigierten in den Bereich "Configuration / Access Profiles".

MFA für Fortgeschrittene

Für Szenarien, die umfassendere Kontrolle über den zweiten Faktor und mehr Benutzerkomfort erfordern, bietet der Distributor den Giritech Authenticator als optionale Linux-Appliance im OVA-Format für VMware vSphere an. Bei der Integration mit anderen Hypervisoren unterstützt Giritech auf Anfrage. Unter der Haube steckt eine gehärtete Ubuntu-VM, deren Benutzerverwaltung vollständig isoliert innerhalb der Appliance läuft. Die Kommunikation mit dem Thinfinity-Server beschränkt sich auf TCP-Port 1840 für RADIUS sowie einen Administratorzugang per XRDP auf TCP-Port 3389.

Der Giritech Authenticator unterstützt verschiedene Nutzungsstrategien: klassische TOTP-Apps auf Smartphones, Hardware-Token, ein Recycling bestehender TOTP-Secrets aus anderen Systemen wie Office 365 über das optionale MySecret-Plug-in, On-Demand-Zugänge für externe Dienstleister über ein TAN-Plug-in sowie klassische TAN-Listen mit zehn Einmalpasscodes. Für die Benutzerverwaltung stehen Shell-Skripte bereit, mit denen sich Benutzer einzeln oder per Batch-Import anlegen, testen und löschen lassen. Ein integriertes Self-Service-Portal gibt Anwendern Zugriff auf ihren QR-Code und das Secret im Klartext zur Einrichtung; Administratoren erhalten über eine separate Ansicht den Überblick über alle Benutzer.

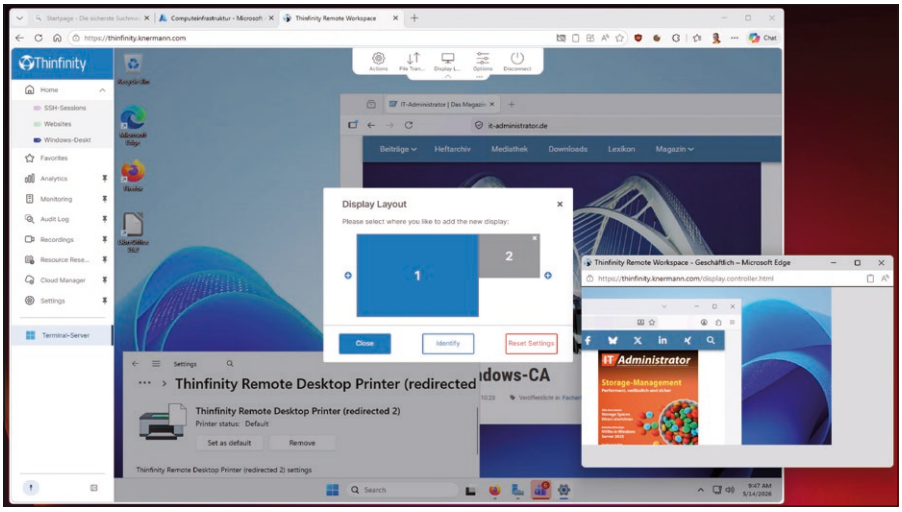


Bild 2: Der HTML5-Client bildet mehrere Displays ab und reicht Drucker sowie weitere Peripherie durch.

Flexible Zugriffsprofile

Access Profiles definieren, welche Ressourcen welchen Benutzern oder Gruppen zur Verfügung stehen. Sie legen Verbindungstyp, Protokoll, Zieladresse, Authentifizierungsmethode und Zugriffsberechtigungen fest. Nach der Anmeldung am Webfrontend sehen Benutzer ausschließlich die für sie freigegebenen Ressourcen in einer Kachelansicht. Zur logischen Gruppierung dienen Labels, die unter einer Kachel ein oder mehrere Profile zusammenfassen und Berechtigungen auf untergeordnete Labels sowie die enthaltenen Profile vererben können. Umgekehrt lassen sich einem Profil mehrere Labels gleichzeitig zuweisen.

Über die Schaltfläche "+ Add" oben rechts konfigurierten wir zunächst einige Labels und legten dann erste Profile an. Thinfinity unterscheidet die vier Verbindungstypen "Desktop", "Application", "Web Folder" und "Terminal". Der Typ "Desktop" kennt dabei drei Untertypen: Remote Desktop Connection (RDC) für den vermutlich häufigsten Anwendungsfall – die Bereitstellung eines Desktops über Microsofts Remote Desktop Protocol (RDP) –, VNC sowie das hauseigene Zusatzprodukt Thinfinity VNC.

Beim Typ "Application" stehen wahlweise eine Remote App (eine einzelne per RDP veröffentlichte Applikation), eine Web App oder eine VirtualUI App zur Wahl. Letztere stellt angepasste Windows-Anwendungen als Webapplikation bereit, ohne einen vollständigen Remotedesktop vorauszusetzen. Darüber hinaus unterscheidet Thinfinity einen einfachen "Web Link" – einen direkt erreichbaren URL – vom "Web Application Gateway", bei dem Thinfinity als Reverse-Proxy mit optionaler Linkersetzung eine interne Webseite nach außen durchreicht.

"Web Folder" ermöglicht den Browserzugriff auf interne Dateiablagen per WebDAV. Der Verbindungstyp "Terminal" schließlich realisiert wahlweise SSH- und Telnet-Verbindungen oder bindet über den Untertyp "Multi Terminal" Hostsysteme an.

HTML5-Client mit vielen Optionen

Ein RDC-Profil startet eine Sitzung auf dem Thinfinity-Server selbst oder typischerweise auf einem vom Server erreichbaren weiteren System. Als Ziel lässt sich im Profil eine IP-Adresse oder ein

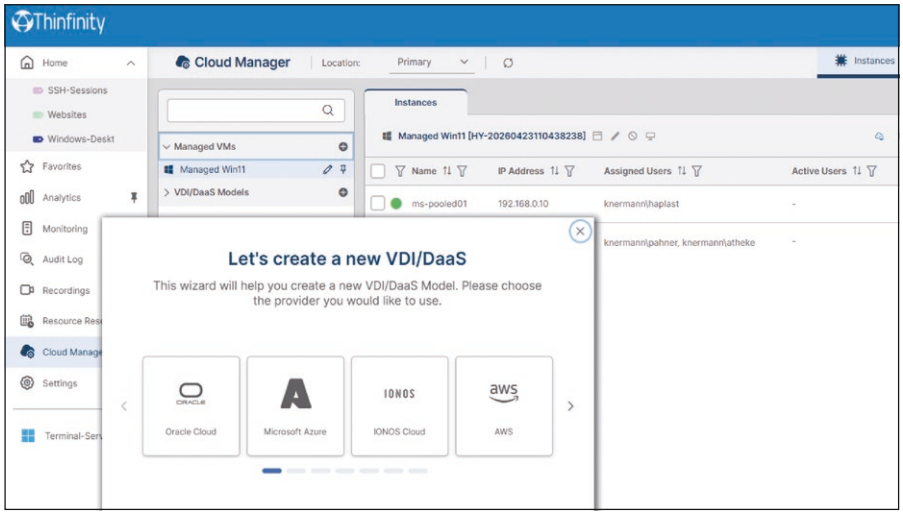


Bild 3: Der Cloud Manager steuert vorhandene Zielsysteme und orchestriert VDI in verschiedenen Clouds.

Hostname, eine Agent-ID, ein Agentpool oder eine im Cloud Manager verwaltete Ressource angeben. Wir konfigurierten zunächst einen unserer RDSH direkt über seinen Namen. Neben der Bezeichnung, unter der die Verbindung im Webfrontend erscheint, erlaubt der Parameter "Virtual Path" den Start des Profils über einen direkten Link.

Für die Authentifizierung stehen drei Varianten zur Verfügung: SSO mit dem am Frontend angemeldeten Benutzerkonto, eine separate Authentifizierung oder fest im Profil hinterlegte Anmeldedaten. Letzteres erlaubt es etwa, externen Technikern Zugriff auf ein System zu gewähren, ohne ihnen dessen Zugangsdaten preiszugeben.

Bei den weiteren Einstellungen zu Bildschirmen und Ressourcen überraschte uns die Vielfalt der Optionen – insbesondere in Verbindung mit dem HTML5-Client. Konfigurierbar sind neben der Farbtiefe auch die Auflösungssteuerung: Diese kann sich am Browserfenster oder am physischen Bildschirm orientieren oder aus fest vorgegebenen Seitenverhältnissen von 640×480 bis 1920×1200 Pixel wählen. Der HTML5-Client passt die Auflösung dynamisch an und beherrscht Multi-Monitor-Betrieb – unabhängig von der tatsächlichen Anzahl physischer Monitore. Weitere virtuelle Bildschirme starten in separaten Browserfenstern, die sich dynamisch verschieben und skalieren lassen (Bild 2).

Über eine ausklappbare Werkzeugleiste lassen sich Anzahl und Position der virtuellen Bildschirme im laufenden Betrieb anpassen. Der Browser bietet damit eine Flexibilität, die wir bislang nur von nativen Client anderer Produkte kannten. Ein Wermutstropfen bleibt: Bei benutzerdefinierter Skalierung des lokalen Monitors – etwa 125 statt 100 Prozent auf einem großen Bildschirm – renderte Thinfinity die entfernte Sitzung nicht in nativer Auflösung, was zu einer leicht unscharfen Darstellung führte. Dasselbe galt für die High-DPI-Displays zweier Notebooks aus unserem Testparcours. Abhilfe schaffte erst der native Desktopclient, der jedoch ausschließlich für Microsoft Windows verfügbar ist.

Bidirektionaler Datenaustausch

Die Zwischenablage reicht der HTML5-Client zwischen lokalem Rechner und dem entfernten Ziel durch – wahlweise direkt oder über eine zwischengeschaltete virtuelle Disk, die Cybele als ThinDisk bezeichnet. Diese erreichten wir über die Option "File Transfer / File Manager" in der Werkzeugleiste einer laufenden Sitzung, wo wir in einem separaten Browser-Tab Daten mit der ThinDisk austauschen konnten. Darüber hinaus erzeugt Thinfinity ein virtuelles Druckerobjekt in der entfernten Sitzung, das Druckaufträge über den Browser an den lokalen Computer umleitet, wo sie auf einem der vorhandenen Drucker ausgegeben werden können.

Der HTML5-Client beherrscht zudem bidirektionales Audio, reicht das Mikrofon des Clients in die Remotesitzung durch und ebenso eine Webcam. Letzteres funktionierte in unserem Test nicht auf allen Geräten gleichermaßen: Die Kamera eines MacBooks erschien wie erwartet in der entfernten Sitzung, während das Querformat der integrierten Kamera eines älteren Microsoft Surface auf ein quadratisches Format gestaucht wurde. Auch hier schaffte der native Desktopclient Abhilfe, der in der Profilkonfiguration zusätzliche Optionen bietet. Er reicht neben Kamera und Mikrofon auch Disks, COM-Ports, Smartcards und WebAuthn-Geräte, weitere USB-Geräte sowie Standortdaten in eine Sitzung durch.

Pools einfach konfiguriert

Im nächsten Schritt fassten wir mehrere Server zwecks Lastverteilung zu einem Pool zusammen. Dazu wechselten wir zunächst in den Configuration Manager auf dem Primary Broker und fügten dort auf der Registerkarte "Broker" einen Pool hinzu. Thinfinity unterscheidet dabei die Strategien "Breadth-First" und "Depth-First": Erstere verteilt Sitzungen gleichmäßig über alle Poolmitglieder, Letztere füllt zunächst einen Host bis zum definierten Maximum, bevor weitere Hosts herangezogen werden.

Anschließend installierten wir das Thinfinity-Paket auf unseren Hosts und wählten jeweils die Rolle "Secondary Broker". Im Configuration Manager trugen wir den Poolnamen, die Network ID unserer Infrastruktur sowie den FQDN des Gateways ein. Im Webfrontend konnten wir daraufhin im Bereich "Monitoring" unter der Registerkarte "Brokers" nachvollziehen, dass sich unsere RDSH unter dem Poolnamen als betriebsbereit meldeten.

Nachdem wir das Profil von der dedizierten Adresse eines einzelnen Hosts auf den Poolnamen umgestellt hatten, verteilte Thinfinity unsere Sitzungen wie erwartet dynamisch über die verfügbaren Hosts.

Leistungsfähiges VDI-Management

Noch flexibler gestaltete sich die Integration von Ressourcen über den Cloud Manager, den wir ebenfalls über das Be-

nutzericon oben rechts erreichten. Den Einstieg bildete die Hinterlegung von Zugangsdaten für die jeweilige Plattform – im Fall unseres lokalen Hyper-V-Hosts schlicht Benutzername und Passwort. Danach standen zwei Wege offen: die Einbindung bereits vorhandener VMs oder die Erstellung eines neuen VDI-Modells.

Im ersten Fall wählten wir VMs aus, die wir zuvor auf dem Hyper-V-Host erstellt und ins AD aufgenommen hatten, wiesen ihnen Benutzer zu und erzeugten direkt aus dem Cloud Manager heraus ein Zugriffsprofil. Bei diesen "Managed VMs" lassen sich zwar mehrere Benutzer für eine Maschine berechtigen, aber nicht einem Benutzer mehrere Maschinen zuweisen. Managed VMs eignen sich damit vor allem für den Fernzugriff auf dedizierte Arbeitsplätze oder bestimmte PCs wie Anlagensteuerungen und erfordern keine zusätzliche Software auf den Zielsystemen.

Eine dynamische Zuweisung an einen Pool gleichartiger Desktop-VMs realisieren die "VDI/DaaS Models" (Bild 3). Ein solches Modell definiert alle Parameter einer zu erstellenden VM und liefert damit die Blaupause für die Provisionierung – wobei die verfügbaren Optionen je nach Plattform variieren. Für die großen Hyperscaler bringt der Cloud Manager vorgefertigte Modelle mit, die Standardarbeitsplätze, höhere Rechenleistung oder GPU-beschleunigte Grafik adressieren. Optional lässt sich hier auch Terraform einbinden.

Im Fall von On-Premises-Hypervisoren setzt Thinfinity auf vorbereitete Golden Images mit vorinstalliertem Agenten, wobei der Funktionsumfang von der jeweiligen Plattform abhängt. Unter Proxmox dienen Snapshots als Basis; die Onlinedokumentation weist auf damit verbundene Einschränkungen hin: Sysprep ist nicht möglich, sodass Administratoren nach der Provisionierung weitere skriptbasierte oder manuelle Schritte einplanen müssen.

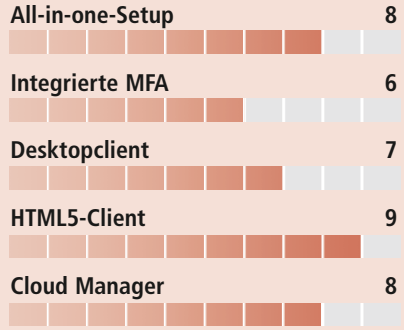
In Verbindung mit Hyper-V und vSphere greift der Cloud Manager dagegen auf per Sysprep generalisierte Images zurück. Auf dieser Basis stehen mehrere Bereitstellungsstrategien zur Wahl: bedarfsgesteuert bei Benutzerzugriff, zeitplangesteuert oder als Kombination beider Ansätze. Der Cloud Manager kann Maschinen bei Bedarf starten, stoppen und auch wieder entsorgen. Profile regeln dabei detailliert die Zugriffsberechtigungen und ob Benutzer per SSO zugreifen oder sich erneut authentifizieren müssen. Das Modul "Resource Reservation" steuert ergänzend zeitlich begrenzten Zugriff mit Genehmigungsworkflows; mit "Analytics", "Monitoring" und "Audit Logs" behalten Administratoren den Überblick und können Sitzungen für Compliance-, Sicherheits- und Schulungszwecke spiegeln sowie aufzeichnen.

Fazit

Thinfinity Workspace überzeugt als umfangreiche Plattform für den sicheren Fernzugriff auf heterogene Ressourcen. Die Architektur mit ausschließlich ausgehenden Verbindungen aus den Zielnetzwerken, dem zustandslosen Gateway in der DMZ und durchgängiger TLS-Verschlüsselung entspricht den Anforderungen moderner Sicherheitsarchitekturen. Die integrierte MFA genügt einfachen Szenarien; der optionale Giritech Authenticator deckt darüber hinaus auch komplexere Anforderungen an den zweiten Faktor ab.

Administratoren mit besonderen Ansprüchen an hohe Bildschirmauflösungen, High-DPI-Displays oder spezielle Clienthardware sollten prüfen, ob der HTML5-Client ihre Anforderungen vollständig erfüllt – und im Hinterkopf behalten, dass der Desktopclient ausschließlich Windows unterstützt. Jenseits solcher Spezialfälle liegen die Stärken klar auf der Hand: die clientlose Architektur über den HTML5-Client, die flexible Skalierbarkeit vom All-in-one-Setup bis zur hochverfügbaren Multi-Gateway-Umgebung sowie die Breite der unterstützten Zugriffsprotokolle von RDP über VNC und SSH bis zur Host-Terminal-Emulation und WebDAV. Der Cloud Manager rundet das Portfolio um ein leistungsfähiges VDI-Management ab – on-premises wie in der Cloud. *(dr)*

So urteilt IT-Administrator



Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Thinfinity | Workspace

Clientloser Zero Trust Network Access

Schluss mit...

- hohen Lizenzgebühren
- mangelhafter Sicherheit
- kostenintensiver Hardware
- unzureichender Usability

Bild: KI-generiert

Informationen und Testanforderung auf

giritech.de/thinfinity

Giritech GmbH
Cybele Distribution D/A/CH
Mariabrunnstrasse 123
88097 Eriskirch (Germany)

Tel. +49 7541 9700-0
Fax +49 7541 9700-90
Mail: info@giritech.de
Web: www.giritech.de

CYBELE software

GIRITECH®
WORK SMART, WORK SECURELY. ANYWHERE.