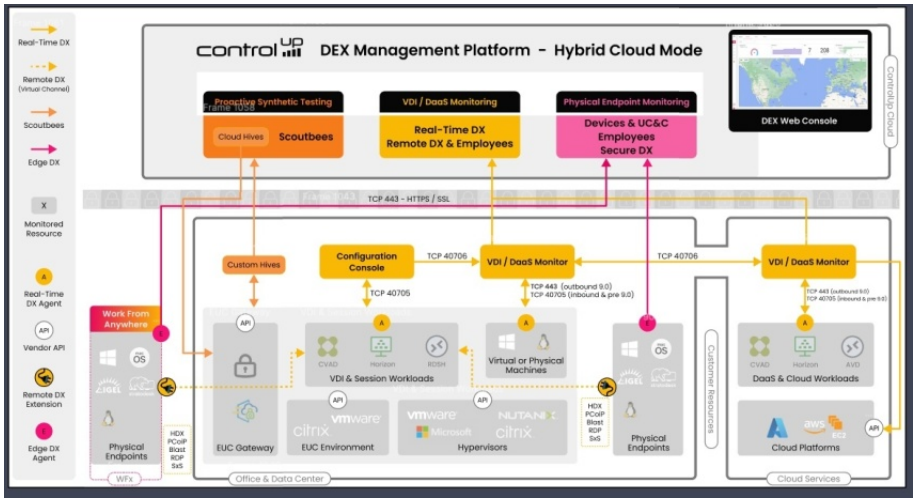
Im Test: Real-Time-Überwachung mit den DEX-Management-Produkten von ControlUp

Viel mehr als Monitoring, viel mehr als VDI

Dr. Götz Güttich

ControlUp bietet eine leistungsfähige Lösungs-Suite zum Überwachen von IT-Umgebungen. Die Produkte eignen sich sowohl zum Monitoring virtueller und physischer Desktops, als auch zum Sicherstellen eines hohen Security-Niveaus der überwachten Desktop-Systeme. Wir haben uns im Testlabor angesehen, wie sich die Suite in der Praxis verhält und was man bei ihrem Betrieb beachten muss.

Die DEX-Management-Suite arbeitet mit einem zentralen Web-Interface und Agenten für die jeweils zu überwachenden Systeme, wie beispielsweise Thin Clients oder Rechner unter Linux, macOS und Windows. Im Betrieb nehmen die Agenten nach der Installation Verbindung zum ControlUp-System auf und übertragen die während des Monitorings gewonnenen Daten dorthin, wo sie anschließend über das Web-Interface eingesehen und genutzt werden können.



Insgesamt besteht das ControlUp-System aus drei unterschiedlichen Komponenten. Bei "ControlUp Real-Time DX" handelt es sich um eine Lösung, die sich darauf konzentriert, die virtuellen Desktops und Anwendungen beziehungsweise die End-User-Computing-Umgebungen (EUC) der Nutzer vollständig zu überwachen. Die dabei gewonnenen Daten stehen dann in Echtzeit bereit und diverse Dashboards helfen den Administratoren dabei, einen umfassenden Überblick zu erhalten und auftretende Probleme zu erkennen beziehungsweise proaktiv anzugehen und so die System-Health sicherzustellen. Die Leistungsdaten werden vom System bis zu ein Jahr lang gespeichert, um Muster und Trends erkennen und die zukünftige Leistungsentwicklung in der gesamten Umgebung vorhersagen zu können. Abgesehen davon stellt das System auch automatisierte Aktionen zur Verfügung, um das Trouble-Shooting zu beschleunigen und die Ressourcen zu maximieren. Zu den unterstützten Plattformen gehören Citrix, VMware Horizon und Microsoft Azure Virtual Desktop.

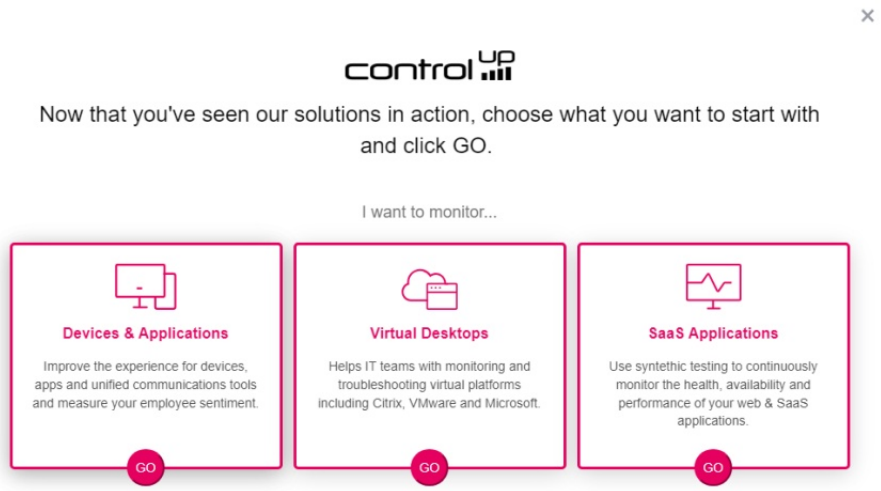
"ControlUp Edge DX" übernimmt die Aufgabe, physikalische Desktops unter Linux, macOS und Windows im Auge zu behalten. Die Lösung lässt sich in wenigen Minuten in Betrieb nehmen, da es ausreicht, die bereits erwähnten Agenten von der zentralen Webseite herunterzuladen und anschließend auf die Zielsysteme zu verteilen. Auch hier werden die Daten in Echtzeit erhoben und es stehen diverse informative Dashboards zur Verfügung. Darüber hinaus gibt es Alarmmeldungen, wenn die Endanwender Probleme bekommen und historische Daten ermöglichen umfassende Analysen. Da die Agenten auch eine Remote-Control-Option umfassen, haben die IT-Verantwortlichen jederzeit die Möglichkeit, sich – wenn die Anwender dies genehmigen – mit den Endpoints zu verbinden und

helfend einzugreifen. Eine Funktion zur Mitarbeiterbefragung hilft zudem dabei, das Zufriedenheitsniveau in Erfahrung zu bringen und auf einem hohen Level zu halten. Last but not least stellt die Lösung auch noch spezielle Überwachungsfunktionen für die Collaboration-Tools "Microsoft Teams" und "Zoom" bereit, um Probleme zu diagnostizieren und die virtuellen Meetings produktiv und zuverlässig zu gestalten.

Die letzte Komponente nennt sich "ControlUp Secure DX" und dient dazu, das Vulnerability-Management der überwachten Plattform zu übernehmen. Sie hilft beim Vermeiden von anfälligen Konfigurationen und minimiert die Gefahren, die mit dem Einsatz von Risiko-Applikationen verbunden sind. Die Lösung kombiniert ein Real-Time-Scanning-Feature mit Funktionen zur Priorisierung von Gefahren und zur Beseitigung von Verwundbarkeiten beziehungsweise Problemen bei der Herstellung der Compliance der Umgebungen. Das funktioniert beispielsweise durch das Patchen von Schwachstellen und das Beseitigen von Fehlkonfigurationen. Auch hier gibt es wieder intuitive, kontextuelle Dashboards und Automatisierungsfunktionen. Außerdem erkennt die Lösung veraltete Anwendungen und nimmt ein intelligentes Risiko- und Sicherheits-Scoring vor.

Der Test

Im Test installierten wir die ControlUp-Agenten auf diversen Testsystemen in unserem Netz, die unter Linux, macOS und Windows liefen. Darüber hinaus verwendeten wir die Lösung in Zusammenarbeit mit unserer virtuellen Desktop-Umgebung unter Microsoft Azure, um das EUC-Monitoring unter die Lupe zu nehmen. Anschließend machten wir uns mit dem Funktionsumfang des Produkts und der im täglichen Betrieb anfallenden Arbeit vertraut. Um auch eine Umgebung mit in den Test aufzunehmen, auf der etwas mehr Aktivität herrschte als in unserem Testlab, stellte uns der Hersteller zudem einen Zugriff auf seine Demo-Installation zur Verfügung, bei der wir die Monitoring-Möglichkeiten tiefgehender nutzen konnten. Zum Schluss analysierten wir unsere Ergebnisse.



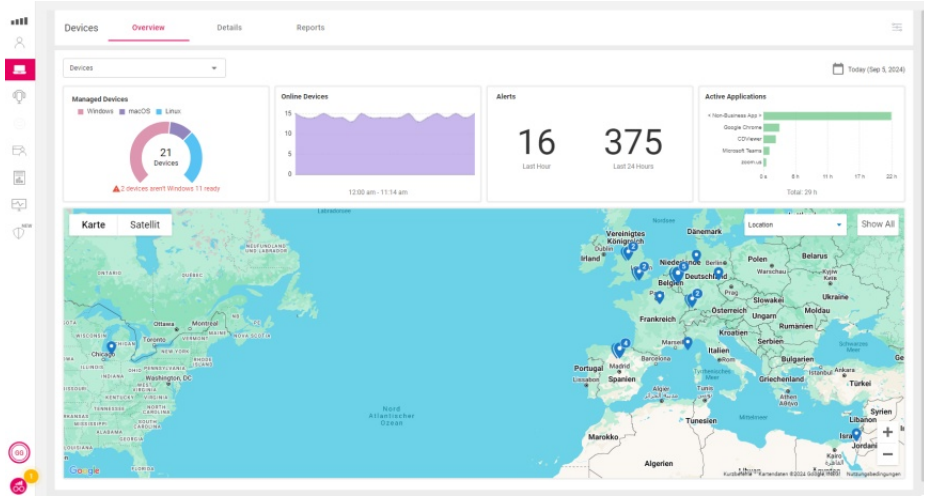
Nach dem Anlagen des Tenants hilft das System den Administratoren bei der Einrichtung der Monitoring-Funktionen

Die Installation der Agenten

Um unseren Test zu beginnen, erstellten wir zunächst einmal unter https://app.controlup.com einen neuen Tenant. Dabei besteht die Option, ein Konto mit Google, Microsoft Azure oder E-Mail und Passwort anzulegen. Wir entschieden uns hier für die letztgenannte Möglichkeit. Im nächsten Schritt fragt das System, in welcher Region der Tenant aktiv sein soll. Hierbei stehen Kanada, USA oder EU zur Auswahl, wir entschieden uns natürlich für die EU. Jetzt mussten wir unserer neuen Organisation noch einen Namen geben, hierbei fiel uns auf, dass das System keinen "_" im Organisationsnamen akzeptiert. Zum Schluss war es noch erforderlich, eine Handynummer anzugeben, die ControlUp für die Multifaktorauthentifizierung (MFA) nutzen konnte, danach wurde der Tenant angelegt, was ein paar Minuten dauerte.

Als der Tenant online ging, hatten wir Gelegenheit, uns zunächst diverse kurze Einführungsvideos anzusehen, die uns darüber informierten, wie die Überwachung von Endgeräten, Unified-Communications, VDI- und DaaS-Umgebungen und Ähnlichem abläuft. Danach ging es daran, Agenten für virtuelle Desktops (wie gesagt, unter Citrix, VMware Horizon oder Microsoft Azure) oder für physikalische Desktops (Linux, macOS, Windows und

Thin Clients) herunterzuladen. In dieser Phase fingen wir mit den physikalischen Desktops an und installierten den Agenten auf diversen Systemen unter Windows 10, Windows 11 und Windows Server 2019. Dazu kamen ein Macbook Pro unter macOS Sonoma 14.5 und zwei Linux-Systeme unter Ubuntu 24.04 und Raspberry Pi OS (Debian Linux 12 (Bookworm) in der 32-Bit-Version). Bei Linux ist zu beachten, dass der Agent in drei verschiedenen Varianten zur Verfügung steht. Ein Agent für 64-Bit-Linux-Systeme auf Intel-kompatiblen Systemen und zwei Agenten für ARM-Systeme, jeweils einer für 32 und einer für 64 Bit.



Die Übersichtsseite mit Informationen über die physikalischen Geräte

Für die Installation benötigen die Agenten die Angabe des Tenant Namens und des Device Registration Codes. Beide Informationen stehen im Web-Interface zur Verfügung und das System liefert den Administratoren auch gleich Kommandozeilenbefehle mit, die die Installation auf den verschiedenen Betriebssystemen anstoßen und dabei die genannten Informationen mit übergeben. Die Installation läuft also extrem einfach ab und sollte niemanden vor irgendwelche Probleme stellen. Sie ist auf der Webseite auch sehr gut dokumentiert. Unterstützt werden übrigens die Betriebssysteme Windows 7 beziehungsweise Windows Server 2012 R2 und neuer, macOS 11 und neuer sowie Linux-Systeme wie Fedora 39 sowie Ubuntu 20.04 und neuer. Nach der Installation des Agenten (zum Testzeitpunkt war unter Windows die Version 2.14.0.311 aktuell) melden sich die betroffenen Systeme direkt beim Web-Interface und beginnen damit, Daten zu übertragen. Sollen auch die Benutzeraktivitäten und die Unified Communications überwacht werden, so müssen die zuständigen Mitarbeiter die entsprechenden Funktionen über das Web-Interface aktivieren. Auch die dafür erforderlichen Schritte sind gut dokumentiert, bei der Benutzerüberwachung reicht ein Eintrag im Web-Interface, bei den Unified Communications (im Test überwachten wir Microsoft Teams), ist es etwas komplizierter.

Um Teams zu überwachen, müssen die Administratoren sich bei Microsoft Azure anmelden und nach “Microsoft Entry ID” wechseln. Danach ist es erforderlich, eine neue App-Registrierung vorzunehmen, ein neues Client-Secret sowie eine neue Permission festzulegen und eine Administrator-Zustimmung zum Datenaustausch mit ControlUp zu erteilen. Danach können die Verantwortlichen unter “Configuration/Settings” im ControlUp-Web-Interface in die UC&C-Sektion wechseln und auf „Configuration“ klicken. Dort tragen sie dann das Secret und vergleichbare Informationen ein und stellen die Verbindung her. All das wurde – wie gesagt – unter Get Started with UC&C (controlup.com) sehr gut dokumentiert und sollte für IT-affine Benutzer keine Probleme mit sich bringen.

Die Einrichtung der weiteren Überwachungsfunktionen

Um die Funktionen zum Überwachen der VDI-Installationen und der virtuellen Umgebungen in Betrieb zu nehmen, sind diverse zusätzliche Schritte erforderlich. Das dazu benötigte Modul verwendet einen on-premises laufenden Monitor-Server. Deswegen mussten wir im Test zunächst einmal diesen Server installieren.

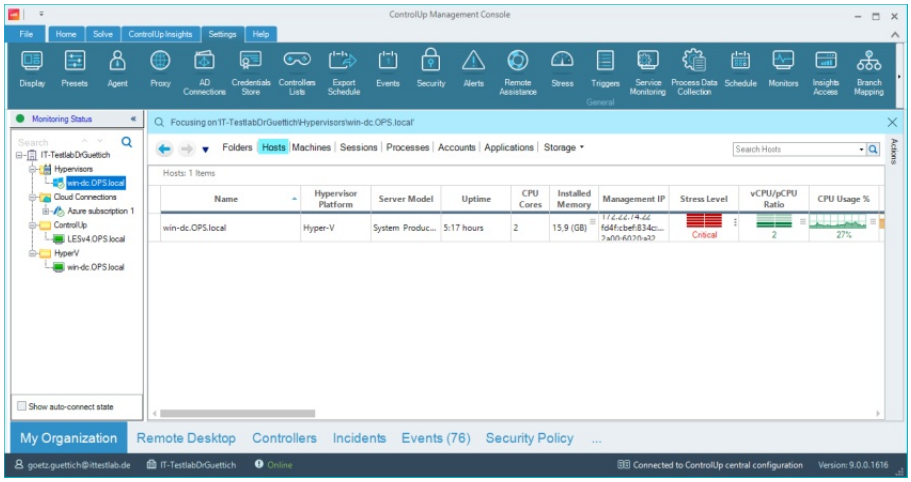
Zu diesem Zweck luden wir uns über einen Link im Web-Interface von ControlUp die Konsole von ControlUp Real-Time DX herunter. Diese kommt als EXE-Datei und kann ohne weitere Schritte direkt auf dem Zielsystem ausgeführt werden. Früher kam sie zum Einsatz, um das System zu konfigurieren und zu überwachen, da das Monitoring heute über das Web-Portal abläuft, wird sie nur noch für einige Konfigurationsarbeiten benötigt. Nachdem wir die Konsole auf unserem Zielsystem – einem Server unter Windows Server 2019 – gestartet hatten, konnten wir sie mit unserer ControlUp-Installation ver-

binden. Dazu mussten wir die E-Mail-Adresse unseres Kontos angeben und erhielten dann an diese Adresse einen Passcode, den wir in der Konsole eintragen mussten. Nachdem die Verbindung stand, konnte es daran gehen, der Konsole die zu überwachenden Systeme hinzuzufügen. Die Computer lassen sich dabei entweder über das Active Directory, über ihre IP-Adresse oder über eine Textdatei bestimmen. Im Test verwendeten wir das Active Directory. Sobald der betroffene Rechner im Ordner erscheint, können die IT-Verantwortlichen einen Rechtsklick auf den Eintrag durchführen und den Befehl "Agent Control / Upgrade/Install Remote Agent" ausführen. Das System spielt den Agenten dann auf dem Ziel-Computer ein.

Zunächst einmal installierten wir die Lösung auf dem genannten Windows- Server- 2019- System, auf dem später der Monitor-Server laufen sollte. Er nahm dort unverzüglich nach der Installation seiner Arbeit auf. Jetzt konnte es daran gehen, den Monitor-Server selbst zu installieren. Damit dieser funktioniert, muss auf dem Zielsystem die Dotnet-Laufzeitumgebung 4.8 vorhanden sein. Für die Installation wechselten wir in der Icon-Leiste auf "Add Monitor", wählten unser Zielsystem aus und starteten die Installation. Im letzten Schritt gingen wir nun nach "Solve / User Permissions" und ließen dort unter den "Security Policies / Use Web Application" den Zugriff auf die Web-Anwendung zu. Kurz darauf meldete uns die Konsole mit einem grünen Punkt vor "Monitor Status" dass der Dienst seine Arbeit aufgenommen hatte. Die Installation geht auch hier schnell von der Hand und sollte in wenigen Minuten abgeschlossen sein.

Das Einbinden von Hyper-V

Nachdem der Monitoring-Server lief, konnten wir unter "My Organization" unseren Hyper-V-Hypervisor zu unserer Überwachungsumgebung hinzufügen. Dazu installierten wir zunächst einmal den Agenten auf unserem Windows-Server mit der Hyper-V-Rolle. Nachdem dieser die Arbeit aufgenommen hatte, wechselten wir nach "Add Hypervisor" und wählten dort "Hyper-V" aus. Danach erschien das betroffene System in der Liste und wir



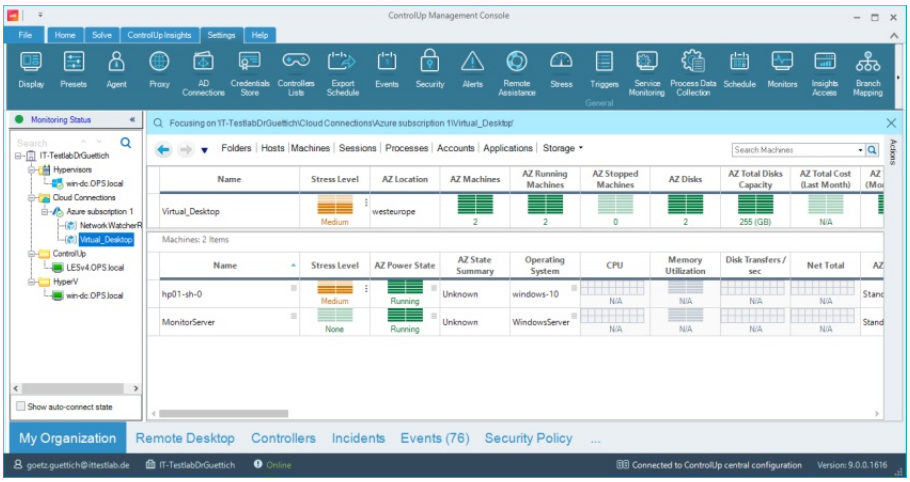
Nach dem Aufbau der Verbindung erschien unser Hyper-V-System in der lokalen Verwaltungskonsole

spielten auf ihm die Hyper-V-Monitoring-Funktionen ein. Kurz darauf tauschte der Hypervisor in unserer Übersicht auf und wir konnten seine Daten einsehen. Abgesehen vom Microsoft-Hypervisor unterstützt ControlUp auch das Monitoring von Nutanix AHV, VMware und Xen Server.

Das Einbinden der virtuellen Desktops

Zum Schluss wollten wir noch unsere Azure-Virtual-Desktop-Umgebung (AVD) zu unserer ControlUp-Installation hinzufügen. Dazu erstellten wir zunächst in Entra ID eine Enterprise-App namens "ControlUp" und fügten dieser dann im Azure-Portal unter "Subscriptions / Access Control (IAM) / Roles / Reader / Assignments" die Reader-Rolle hinzu. Danach wechselten wir nach "Microsoft Entra ID / Manage / Enterprise Applications / ControlUp" und kopierten dort die Application- und die Object-ID. Zum Schluss riefen wir "Identity / App Registrations / ControlUp" auf und erzeugten ein neues Client Secret. Hier kopierten wir anschließend die Secret-ID, den Value und die Tenant-ID. Jetzt konnten wir die ControlUp-Konsole aufrufen und dort auf "Add Cloud Connection" gehen. Hier wählten wir "Microsoft Azure" und gaben die Tenant-ID und die Application-ID als Credentials an. Anschließend testeten wir die Verbindung und richteten sie ein. Danach hatten wir Zugriff auf das Azure-API und konnten die von diesem gelieferten Daten wie Zahl der Maschinen, Zahl der Ressource-Gruppen, den Namen der Azure Subscription und so weiter überwachen. Um Zugriff auf maschinenspezifische Daten wie die jeweilige CPU-Last den Netzdurchsatz und Vergleichbares zu erhalten, mussten wir noch einen zusätzlichen Monitoring-

Service auf einer VM in der Cloud einrichten. Dieser wird über eine Organization-ID, die sich in der Web-Konsole unter "API Key Management" findet und einen API-Key, der sich an gleicher Stelle in der Web-Konsole anlegen lässt, mit der ControlUp-Installation verbunden. Zum Schluss ist es noch erforderlich, auf den zu überwachenden Desktops den VDI-Agenten zu installieren und diesen über Agenten-Authentifizierungs- und Agenten-Registrierungs-Strings, die sich in der On-Premises-ControlUp-Console finden, an die Installation anzubinden. Danach stehen in ControlUp alle Daten zur Verfügung. Wenn eine Citrix-Umgebung eingebunden werden soll, so ist das Vorgehen ähnlich. Die zuständigen Mitarbeiter müssen zunächst einmal ein paar Snap-Ins der Citrix-Virtual-Desktops-Powershell-SDK installieren und in der Citrix-Umgebung diverse Rechte setzen. Danach können sie in der ControlUp-Konsole den Befehl „Add EUC Environment" aufrufen und dort als „Solution / Platform" „Citrix Virtual Apps and Desktops" selektieren. Dann müssen sie den Namen oder die IP-Adresse des Brokers und den für die Kommunikation mit dem API verwendeten Port, die Credentials sowie den zu verwendenden Monitoring-Service angeben. Es würde den Rahmen dieses Beitrags sprengen, die erforderlichen Schritte nochmals im Detail zu besprechen, insbesondere da sie in der Dokumentation unter Add CVAD Integration – Connecting to your Virtual Infrastructure (controlup.com) genau erklärt werden. Es reicht zu sagen, dass die zuständigen Mitarbeiter die Credentials vor ihrer Verwendung in der ControlUp-Konsole zu den "Shared Credentials" hinzufügen müssen, bevor sie sie auswählen können.



Die lokale Konsole nach dem Verbindungsaufbau zu unserer Azure-Installation

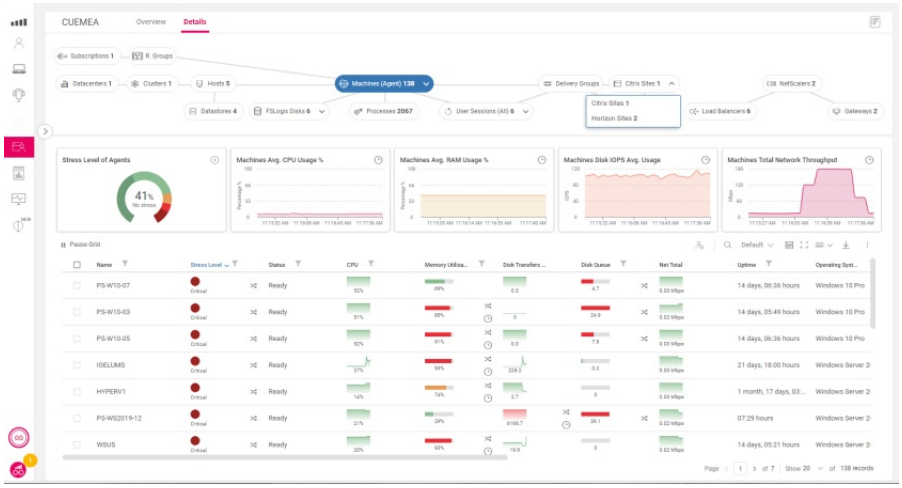
Die Arbeit im laufenden Betrieb

Schauen wir uns jetzt einmal an, wie die Arbeit mit ControlUp im laufenden Betrieb abläuft. Loggt sich ein Mitarbeiter beim Web-Interface der Lösung ein, so landet er auf einer Übersicht, die die vorhandenen Mitarbeiter mit ihren Geräten, Anwendungen und Problemen anzeigt. Die Daten der Endpoints werden also gesammelt und anschließend aus Mitarbeitersicht dargestellt. Das System informiert die IT-Verantwortlichen auf diese Weise darüber, auf welchen Maschinen die Mitarbeiter eingeloggt sind, welche Anwendungen sie benutzen und so weiter.

Wechselt der Administrator auf die Devices-Übersicht, so erhält er eine Karte mit der Position der Geräte und diverse Grafiken mit der Zahl der Online-Devices, den aktiven Anwendungen, den Alarmmeldungen und den verwalteten Geräten mit ihren Betriebssystemen. Eine Detailübersicht stellt die Devices in Listenform dar. Hier können sich die Verantwortlichen unter anderem über die Namen der Geräte informieren und sehen, welche gerade aktiv sind beziehungsweise wie lange die letzte Verbindungsaufnahme zurückliegt. Abgesehen davon bringen sie auch in Erfahrung welches Betriebssystem installiert wurde, wo sich die Komponenten befinden, wie viel Speicherplatz auf ihnen zur Verfügung steht und wie der Status in Bezug auf die Prozessor- und Netzwerklast aussieht.

Darüber hinaus lassen sich auch Geräte oder Gerätegruppen auswählen. Danach sind diverse Aktionen möglich, wie das Schicken einer Nachricht, das Ausführen einer Remote Shell sowie das Fernsteuern und Spiegeln des Systems. Man kann auch Benutzer ausloggen und Systeme ausschalten. Das funktioniert über alle Betriebssysteme hinweg gleich, es ist also nicht erforderlich, auf den Clients separate Fernsteuerungslösungen einzurichten. Abgesehen davon ist das System auch dazu in der Lage, Reports zu Anwendungen und Prozessen, zur Windows-Leistung und zur Sicherheit, zu Top Usern sowie zu fehlenden Patches und Ähnlichem zu erzeugen. Insgesamt wurden 36 Reports vorkonfiguriert, es besteht aber

auch die Option, eigene Reports zu definieren. Wechselt ein Anwender auf einen Geräteeintrag, so öffnet sich eine Performance-Übersicht. Diese enthält diverse Gerätedetails, zum Beispiel neben Informationen zu Betriebssystem und Hardware auch Daten über die Netzwerkverbindung, die Agentenversion, die letzte Kommunikation und so weiter. Abgesehen davon stehen auch diverse Grafiken zur Verfügung. Die erste gibt Aufschluss über den Device Score, also den generellen Zustand des Geräts. Er setzt sich zusammen aus CPU-Last, freiem Arbeitsspeicher, Netzwerklatenz, Anwendungs-Crashes, CPU-Queue-Ereignissen und Delays bei der Benutzereingabe. Je höher der Device Score, desto besser lässt es sich mit dem betroffenen Gerät arbeiten.



In der Detailübersicht der End-User-Computing-Umgebungen können die IT-Verantwortlichen einfach per Klick zwischen den Sites (hier Citrix und Horizon) wechseln

Weitere Grafiken visualisieren die Prozessorauslastung, die Länge der CPU Queues, die Speicherauslastung, die Netzwerknutzung, die Netzwerklatenz, die Stärke des WiFi-Signals (falls vorhanden) und die Zahl der aktiven Sitzungen. Die zuständigen Mitarbeiter können sich hier also auch über die zugrundeliegenden Details informieren.

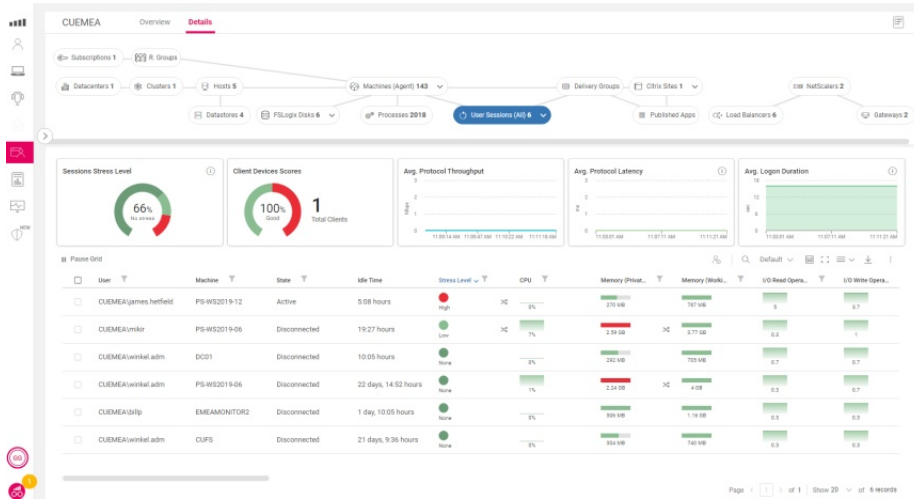
Es besteht die Möglichkeit, bei allen Grafiken einen Durchschnittswert zum Vergleich darüber zu legen und fährt der Anwender mit der Maus über die Grafiken, so zeigt das System Rohdaten zu den jeweiligen Zeitpunkten an. Klickt er auf die Grafiken, so wechselt ControlUp bei allen Grafiken in eine Zoom-Ansicht, die den betroffenen Zeitpunkt im Detail zeigt und Aufschluss dahingehend ermöglicht, was konkret auf dem System los war. Bei hoher Prozessorlast zeigt es beispielsweise an, welcher Prozess zu diesem Zeitpunkt am meisten CPU benötigt hat und wie gleichzeitig die CPU-Queue-Length und die Netzwerklast waren. Auf diese Weise lassen sich Zusammenhänge schnell erkennen und Probleme identifizieren. Neben der beschriebenen Performance-Übersicht gibt es bei den Gerätedetails auch noch Reiter zu den aktiven Prozessen, den installierten Anwendungen, den fehlenden Patches, den Device Events, den gestoppten Prozessen, den Diensten, den Sitzungen, den Top-Apps nach CPU- und Speichernutzung, dem Windows-Event-Log und den Power-Events.

Highlight zum Abschluss: das Überwachen von EUC-Umgebungen

Eines der Highlights des Produkts ist definitiv das Monitoring von EUC-Umgebungen. Wechselt der Administrator auf den dazugehörigen Eintrag, so landet er zunächst wieder auf einer Übersichtsseite die Aufschluss gibt über die laufenden Hosts, die Zahl der Maschinen, den freien Speicherplatz im Datastore, die aktiven Anwendersitzungen, die durchschnittliche Logon-Dauer und die Zahl der laufenden Prozesse. Dazu kommen noch grafische Darstellungen der Resources Health, des Sessions Stress Level und des Processes Stress Level. Übersichten über die Top-5-Prozesse nach CPU-Last, Arbeitsspeichernutzung und Disk-Nutzung fehlen ebenfalls nicht. Abgerundet wird die Übersichtsseite durch die Top-5-Benutzersitzungen nach Prozessornutzung, die fünf langsamsten Logons und diverse Session-spezifische Grafiken. Zu letzteren gehören unter anderem die durchschnittliche Logon-Dauer, der durchschnittliche Protokolldurchsatz, die durchschnittliche Prozessor- und Speichernutzung der Maschinen sowie die Speicher-, Prozessor- und Netzwerknutzung der physikalischen Cluster.

Rufen die IT-Verantwortlichen die Detailübersicht auf, so bietet diese am oberen Bildschirmrand eine grafische Darstellung der Umgebung mit ihren Metriken und dem Stress-Level. Diese umfasst etwa Azure-Subscriptions und darin vorhandene Gruppen, Maschinen, auf denen der dazu-

gehörige Agent aktiv ist, sowie Hosts, Datastores, logische Disks, Prozesse, Benutzersitzungen, Host-Pools, Anwendungsgruppen und AVD Workspaces (Azure Virtual Desktops). Klicken die Verantwortlichen hier auf einen Eintrag, so landen sie auf einer Übersichtsseite mit den wichtigsten dazugehörigen Daten. Unter der genannten Detail-



Der Überblick über die User-Sessions in End-User-Computing-Umgebungen

übersicht befinden sich wieder einige Grafiken, die den Stress-Level der Agenten, die durchschnittliche CPU- und Speichernutzung der Maschinen sowie deren durchschnittliche Disk-IOPS-Nutzung und den Netzwerkdurchsatz visualisieren.

Darunter findet sich eine Liste der Maschinen, wieder mit CPU- und Speichernutzung, Betriebssystem sowie Netzwerkdurchsatz. Wechselt der Administrator auf einen Maschineneintrag, so erhält er unter anderem Daten über die Zahl der Prozesse und die Top-5-Prozesse nach Prozessor-, Arbeitsspeicher- und Disk-Nutzung. Abgesehen davon steht auch eine Auflistung der aktiven Prozesse mit PID sowie CPU-, Speicher- und Disk-Usage zur Verfügung. Das System lässt also keine Wünsche offen.

Die Arbeit mit einer Citrix-Umgebung

Über die Detailübersicht am oberen Bildschirmrand besteht die Möglichkeit, nahtlos zwischen den angebundenen Umgebungen zu wechseln. Im Test riefen wir zu diesem Zeitpunkt einmal eine verbundene Citrix-EUC-Installation auf. Hier gibt es dann die Möglichkeit, Virtual Desktop Agents (VDAs), Delivery Groups und Broker, die in der Umgebung vorhanden sind, einzusehen. Konkret finden sich die VDAs und Broker in der Maschinenübersicht, es gibt aber auch jeweils eine Informationsseite mit den laufenden Sitzungen, den aktiven Prozessen und den veröffentlichten Anwendungen. Zu den angezeigten Daten gehören auch tiefergehende Details, beispielsweise in Bezug auf die Verfügbarkeit einzelner Desktops oder auf die Server, die zum Start einzelner Sitzungen zum Einsatz kamen.

Zusammenfassung und Fazit

Die DEX-Management-Produkte von ControlUp lassen sich relativ einfach in bestehende Netzwerke integrieren und bringen einen riesigen Funktionsumfang mit. Neben den bereits beschriebenen Features sind die Lösungen unter anderem auch dazu in der Lage, automatisierte Tests (Proactive Synthetic Testing) durchzuführen. Dabei simuliert das System beispielsweise die Arbeit eines Anwenders auf einem Server und führt Anmeldungen auf Websites sowie Suchen durch. Es kann sogar auf einzelne Einträge klicken. Auf diese Weise lassen sich Schwierigkeiten entdecken, bevor sie für die Anwender aktuell werden. Es stehen – wie bereits angesprochen – auch automatisierte Maßnahmen zur Verfügung. Dazu müssen die IT-Mitarbeiter über die lokale ControlUp-Konsole Trigger definieren und Maßnahmen angeben, die das System durchführt, wenn die definierten Trigger-Werte erreicht werden. ControlUp hat in diesem Zusammenhang bereits eine große Zahl an Triggern vordefiniert, es lassen sich aber auch eigene anlegen, die auf unterschiedliche Ereignisse reagieren können, wie beispielsweise erreichte Stress-Level, Windows-Events, Anwender-Logins, beendete Prozesse und Ähnliches. Das hilft beim schnellen Reagieren auf auftretende Schwierigkeiten. Im Test ergaben sich bei der Arbeit mit den Triggern keinerlei Probleme.

DEX ist ein Werkzeug zum Optimieren der Benutzererfahrung. Die IT-Verantwortlichen sind mit ihm dazu in der Lage, Schwierigkeiten vorzubeugen und Probleme schnell zu finden und zu lösen. Trotz des großen Funktionsumfangs gestaltet sich die Nutzung recht einfach. Die Einarbeitungszeit dürfte sich für die IT-Abteilungen in Grenzen halten. Deswegen verleihen wir dem überzeugenden Produkt die Auszeichnung „IT-Testlab tested and recommended“.