

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Sonderheft

Microsoft Azure

Sichere Infrastrukturen für
Anwendungen und Clients





Quelle: wavebreakmediamicro - 123RF

Azure Monitor

Wolkenpuls

von Thomas Drilling

Azure Monitor als Überwachungsdienst unterstützt dabei, Performance und Verfügbarkeit der Azure-Dienste und -Anwendungen zu verbessern, Security-Audits zu steuern oder Kosten und Nutzung von Apps und Services zu kontrollieren. Microsoft positioniert den Dienst als Werkzeug für das Sammeln, Analysieren und Behandeln von Telemetriedaten aus der Azure-Wolke, anderen Clouds und lokalen Umgebungen.

Neulingen legt Azure Monitor einige Hürden in Form widersprüchlicher Bezeichnungen von Funktionen, Konzepten und Diensten in den Weg. Dies gilt insbesondere für ältere oder nicht von Microsoft stammende Quellen. Das liegt daran, dass Microsoft seit 2019 Azure Monitor für das Enterprise-Monitoring [1] adaptiert und dabei eine Reihe von älteren Diensten aus dem Azure-Monitor-Umfeld wie etwa die ehemals zentralisiert betriebene Operations-Manager-Suite in ein DevOps-getriebenes Modell überführt. Dieses soll alle ehemaligen Überwachungsdienste in Azure unter einem gemeinsamen Dach vereinen.

Die Umstellung ist zwar weitgehend abgeschlossen, hat aber den Effekt, dass sich eine Reihe von Funktionalitäten innerhalb der einzelnen Dienste zum Teil überlappen und es auch hinsichtlich der verfügbaren Monitoringagenten Überschneidungen gibt, sodass Sie nicht darum herumkommen, sich mit den Vor- und Nachteilen der einzelnen Agenten auseinandersetzen zu müssen.

Mit Azure Monitor verschiedene Ebenen überwachen

Bild 1 veranschaulicht den aktuellen Aufbau von Azure Monitor. Die linke Seite beschreibt mögliche Quellen von Überwachungsdaten. Diese können aus unterschiedlichen Hierarchie-Ebenen von der Anwendung bis hinunter zur Azure-Plattform stammen. Dabei sind die Ebenen Azure-Mandant, Azure-Subscription und Azure-Ressourcen spezifisch für Microsofts Clouddienst, während Gastsystem, Anwendungscode oder benutzerdefinierte Quellen auch beim Überwachen von virtuellen Computern, die lokal oder in anderen Clouds laufen, existieren können.

Die Überwachungsebene Anwendungscode liefert Daten zur Performance und zur Funktionalität Ihrer Applikation, einschließlich Leistungsnachverfolgungen, Anwendungsprotokolle und Benutzer-telemetrie. Die Mandantenebene zeigt Daten zum Betrieb von Azure-Diensten auf Mandantenebene, wie etwa zum Azure Active Directory. Die Abonnementebene hingegen bietet Informationen

zur Integrität und Verwaltung von ressourcenübergreifenden Diensten in einem Azure-Abonnement, wie beispielsweise Resource Manager und Service Health. Übrigens liefert Service Health, sobald Sie Azure Monitor im Azure-Portal gestartet haben, eine schnelle Übersicht zur Integrität und Verfügbarkeit sämtlicher Azure-Dienste.

Aktivitätsprotokolle bieten Sicht von außen

Darüber hinaus gibt es noch das Azure-Aktivitätsprotokoll. Dieses enthält Service-Health-Datensätze und zeigt jede Form von Konfigurationsänderungen, die Sie an den Ressourcen in Ihrem Azure-Abonnement vorgenommen haben. Es ist für alle Azure-Ressourcen verfügbar und stellt in Bezug auf den Azure Monitor eine externe Ansicht dar. Sie finden den Menüeintrag "Aktivitätsprotokoll" im Portal stets an zweiter Position bei jedem Azure-Service, können aber auch direkt im Azure-Portal nach "Aktivitätsprotokoll" suchen. Dann erhalten Sie die Aktivitätsprotokolle sämt-

licher Azure-Dienste, können dann aber mit dem Knopf "Filter hinzufügen" sehr komfortabel nach verschiedenen Entitäten wie "Ressourcetypen", "Ressourcen", "Vorgängen" oder "Ereignistypen" sowie "Schweregraden" suchen.

Aktivitätsprotokolle liefern also Daten zu den Vorgängen in einer Ressource von außen (Steuerebene), während zum Beispiel Diagnoseprotokolle von einer Ressource selbst stammen (Datenebene). Azure bewahrt Aktivitätsprotokolle übrigens 90 Tage lang auf und erlaubt Ihnen, nach beliebigen Datumsbereichen zu fragen. Mit dem Aktivitätsprotokoll können Sie also das "Was, Wer und Wann" für alle Schreibvorgänge (PUT, POST, DELETE) auf den Ressourcen in Ihrem Abonnement untersuchen. Dies gilt allerdings nicht für Lesevorgänge (GET).

Datentöpfe unterscheiden

Die von Azure Monitor gesammelten Daten landen stets in einem von zwei Datentöpfen, je nachdem, ob es sich um Metriken oder Protokolle handelt. Metriken sind numerische Werte, die einen Aspekt eines Systems zu einem bestimmten Zeitpunkt beschreiben. Sie sind in der Regel einfach strukturiert, dafür aber in der Lage, Szenarien nahezu in Echtzeit zu unterstützen.

Protokolle (Logs) hingegen enthalten verschiedene Arten von Daten. Diese sind in Datensätzen mit unterschiedlichen Eigenschaften für jeden Typ organisiert. Protokolle sind neben den bereits beschriebenen Activity-Logs zum Beispiel Diagnoseprotokolle oder Telemetriedaten aus anderen Überwachungslösungen. Zusätzlich zu den Leistungsdaten werden auch Telemetriedaten wie Ereignisse oder die Ablaufverfolgung als Protokolle gespeichert. Alle lassen sich später zur Analyse in Azure Monitor Log Analytics kombinieren.

So zeigen sich die drei grundsätzlichen Funktionsbereiche von Azure Monitor: Überwachen und Visualisieren von Metriken, Abfragen und Analysieren von Logs sowie Einrichten von Warnungen und Aktionen. Diese drei Punkte betrachten wir nun im Detail.

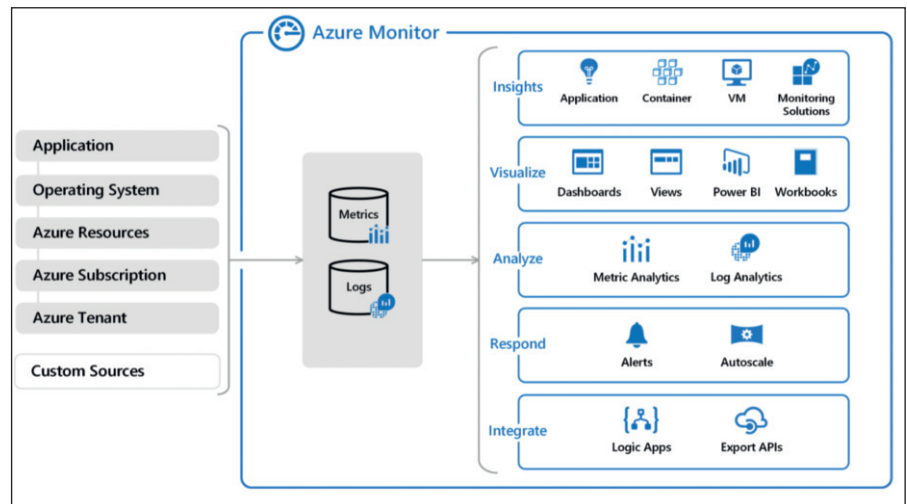


Bild 1: Die Funktionsbereiche von Azure Monitor im Überblick.

Visualisieren und analysieren

Sie können Azure Monitor nicht nur zum Sammeln (Quellen) und Speichern (Metrics und Logs) von Überwachungsdaten, sondern auch zur Visualisierung (Dashboards, Views und Power BI) und Analyse (Metric Analytics und Log Analytics) einsetzen. Log Analytics ist als Relikt aus der Operations-Manager-Suite deutlich mächtiger als etwa Metrics Analytics, wobei sich die verwendbaren Quellen bei beiden zwar prinzipiell unterscheiden, aufgrund der oben skizzierten Konsolidierungsmaßnahmen zum Teil aber auch überschneiden. Im Respond-Bereich der Übersichtsgrafik finden sich dann die erwähnten Alarme, die zum Beispiel bei "Virtual Machine Scale-sets" (das Azure Pendant zu AWS Auto-scaling Groups) Skalierungsereignisse auslösen können.

Eine Sonderstellung nimmt der Bereich "Insights" ein. Haben Sie die zugehörigen Agenten für VMs, Container oder Applikationen installiert [2], liefert Ihnen Azure Monitor dazu wertvolle Einblicke. Sämtliche Telemetrie-Datenströme sind in Azure Monitor integriert, sodass Sie im Azure-Portal leistungsstarke Analysen auf die Rohdaten anwenden können.

Application Insights richtet sich an Entwickler und unterstützt diese dabei, Leistung und Verwendung der von ihnen entwickelten Apps noch besser zu verstehen. Ermitteln lassen sich hier Anforderungsraten, Antwortzeiten, Fehlerraten oder Abhängigkeitsraten. Ferner können Sie benutzerdefinierte Ereignisse und Metriken

einrichten, die Sie selbst im Client- oder Servercode schreiben, um Geschäftsereignisse zu verfolgen. Zudem ist Application Insights auch mit vielen anderen Azure-Diensten wie Azure Kubernetes Service oder Azure App Services integriert.

Standardmetriken und mehr abfragen

Die Azure Monitor Metrics (Metrics Explorer) widmen sich klassischen Metriken. Sie wählen das Modul in Azure Monitor aus und bestimmen dann den gewünschten "Bereich" (zum Beispiel "Virtuelle Maschine"). Oder Sie navigieren im Azure-Portal zur gewünschten Ressource und klicken dort im Navigationsmenü auf der linken Seite im Abschnitt "Überwachung" auf den Eintrag "Metriken". Hier ist dann bei "Bereich" die gewählte virtuelle Maschine bereits eingetragen. Als "Metriknamespace" ist per Default nur "Host der virtuellen Maschine" verfügbar. Hier werden also standardmäßig Metriken auf Hostebene wie CPU-Auslastung, Datenträger- und Netzwerknutzung erfasst, ohne dass dazu zusätzliche Agenten erforderlich sind. Erst wenn Sie später die Diagnoseerweiterung für VMs aktivieren, können Sie weitere Erkenntnisse über die gewählte VM auf Gastebene sowie zusätzliche Protokolle und weitere Diagnosedaten erfassen.

Sie erhalten so ein selbst erstelltes Diagramm. Allerdings gehört die CPU-Auslastung ohnehin zu den Standarddiagrammen für VMs. Sie finden dieses und eine Reihe weiterer Übersichten auf Basis von Host-Metriken, wenn Sie auf der "Über-

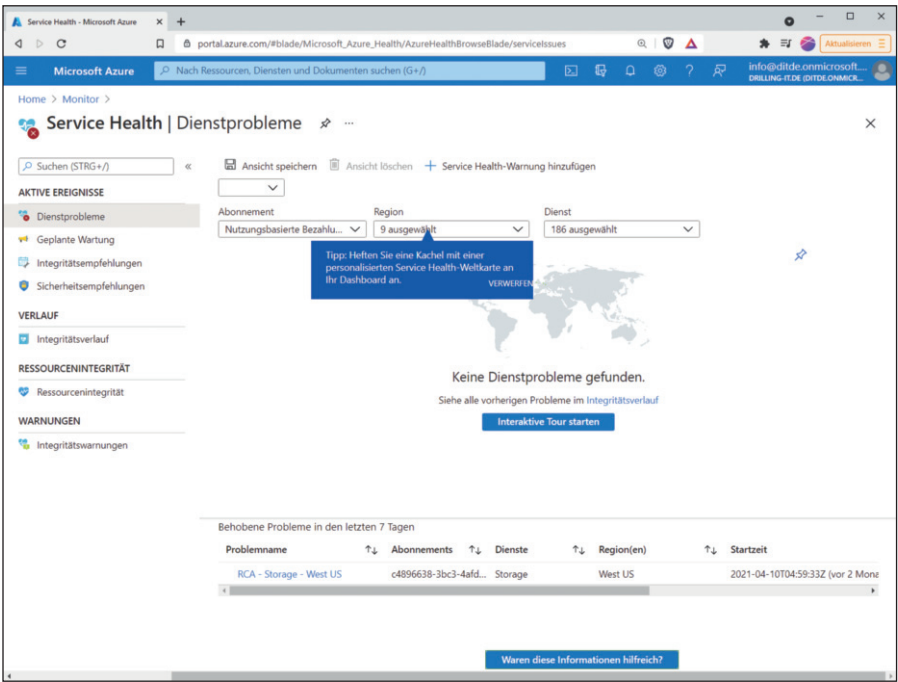


Bild 2: Azure Monitor liefert auch Einblicke in den Gesundheitszustand aller Azure-Dienste.

sicht"-Seite im Azure-Portal für virtuelle Maschinen auf den Tab "Überwachung" klicken. Hier können Sie in eines der Diagramme hineinklicken und dieses um eine weitere Metrik ergänzen. Sie sind aber auch in der Lage, neue Diagramme zu erstellen, nachdem Sie zunächst wieder den gewünschten "Scope" oder im VM-Menü "Überwachung / Metriken" gewählt haben. In letzterem Fall ist der Scope mit der VM

bereits gesetzt und Sie müssen dann nur noch den "Metriknamespace" (per Default geht nur "Host der virtuellen Maschine") und die gewünschte "Metrik" sowie die gewünschte "Aggregation" auswählen. Auch lassen sich mehrere Metriken in einem Diagramm zusammenfassen. Standardmetriken vom Hypervisor sind wichtig, aber nichts Besonderes. Um mehr

Einblicke in Ihre VM oder Anwendung zu erhalten, aktivieren Sie entweder den Gastsystem-Diagnose-Agenten und/oder den Log-Analytics-Agenten auf der VM. Beide überschneiden sich wie eingangs erwähnt bei der Datenerfassung, wohin sie die Daten speichern oder streamen und mit welchen Tools sich die Daten abfragen lassen (Azure Monitor Metrics oder Azure Monitor Logs).

Den Diagnose-Agenten aktivieren Sie entweder beim Neuerstellen einer VM im Tab "Verwaltung" mit Setzen des Häkchens bei "Diagnose des Gastbetriebssystems" oder installieren ihn bei bereits erstellten VMs im Menü "Überwachung / Diagnoseeinstellungen" mit einem Klick auf den Button "Überwachung auf Gastebene aktivieren". In beiden Fällen müssen Sie ein Speicherkonto angeben oder erstellen, das die erfassten Diagnosedaten zusätzlich zur Integration mit Azure Monitor Metrics ablegt. Die Gastsystem-Diagnose-Metriken werden übrigens alle 60 Sekunden abgefragt.

In Zukunft sieht Microsoft offenbar den Azure-Monitor-Agenten an prominenter Stelle. Der erfasst derzeit aber nur Ereignisprotokolle und Performancedaten, sendet diese dann aber sowohl an

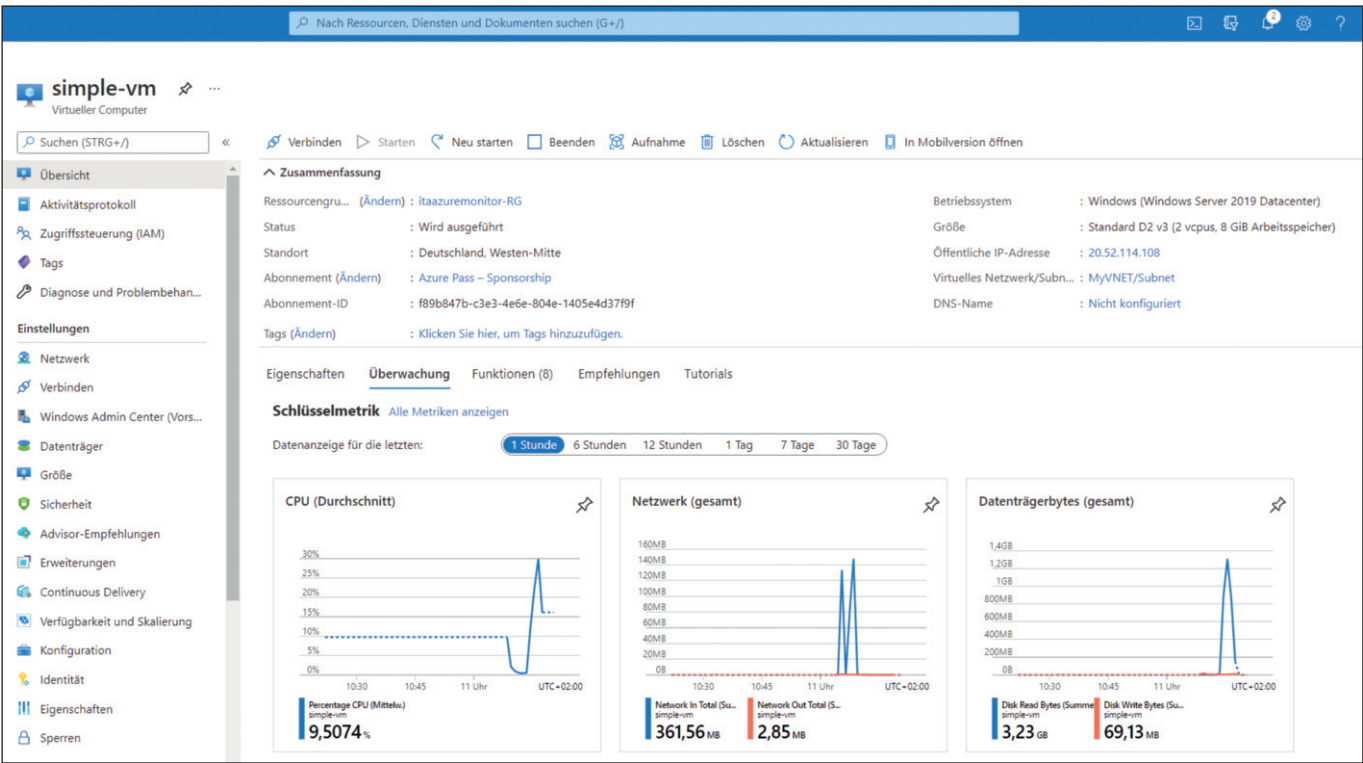


Bild 3: Für VMs und andere Dienste steht in Azure Monitor eine Reihe von Standarddiagrammen bereit.

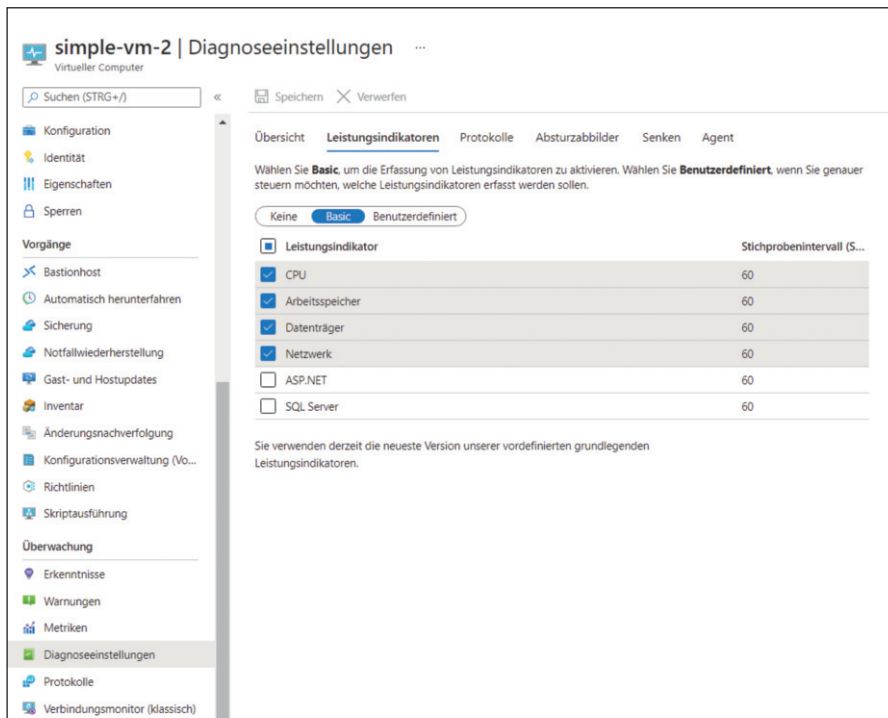


Bild 4: Der Diagnose-Agent sammelt die mit Abstand meisten Daten, steht aber nur für Azure-VMs zur Verfügung.

Azure Monitor Logs als auch Azure Monitor Metrics, sodass Sie diese mit dem Metrik Explorer und Log Analytics auswerten können. Derzeit sind aber der Log-Analytics-Agent und die Diagnoseerweiterung deutlich mächtiger, wobei Letztere die Daten zusätzlich in einem Speicherkonto ablegt und an Event Hub streamen kann.

Ist der Agent einmalig aktiviert, zeigt der gleiche Menüeintrag beispielsweise im Abschnitt "Übersicht", zu welchen Leistungsindikatoren genau er Daten sammelt (CPU, Arbeitsspeicher, Datenträger, Netzwerk) und welche Ereignisprotokolle er erfasst. Hier sind das "Anwendung" (Kritisch, Fehler, Warnung), "Sicherheit" (Überwachungsfehler) und "System" (Kritisch, Fehler, Warnung). Genauer sehen Sie das in den entsprechenden Tabs "Leistungsindikatoren", "Protokolle" oder "Absturzabbilder".

Über den Diagnose-Agenten haben Sie in Azure Monitor Metrics bei der Diagrammerstellung via "Metriknamespace" nun die Möglichkeit, zusätzlich zu "Host der virtuellen Maschine" auch die Optionen "Gast (klassisch)" oder "Neue Metriken für Gastarbeitsspeicher" auszuwählen, wobei Letzteres derzeit noch Pre-

view-Status hat. Sie können dann künftig Metriken direkt in den Azure-Monitor-Metrikspeicher schreiben, der bereits Standard-Plattformmetriken erfasst. So lässt sich damit auf dieselben Aktionen zugreifen, die für Standardmetriken verfügbar sind, wie Alarmierung in Quasi-Echtzeit, Diagrammerstellung, Routing, Zugriff über die REST-API und mehr. Solche Metriken sind dann jedoch nicht mehr kostenlos.

Wählen Sie "Gast (klassisch)" als Metriknamespace, müssen Sie zuvor den Ressourcenanbieter "Microsoft.Insights" registrieren. Damit können Sie problemlos Diagramme für Gastmetriken konfigurieren und die Auswahl an Metriken ist deutlich größer. Dies erledigen Sie wahlweise im Azure-Portal auf Abonnement-Ebene im Menü "Ressourcenanbieter" oder einfacher in der Cloud Shell via PowerShell-Modul:

```
Register-AzResourceProvider
-ProviderNamespace Microsoft.
Insights
```

Auswahl der geeigneten Agenten

Einblicke ins Gastsystem erhalten Sie aber nicht nur über den Diagnose-Agen-

ten, sondern wahlweise auch über den Log-Analytics-Agenten. Doch während die Diagnose-Erweiterung in Summe mehr Daten sammelt als der Log-Analytics-Agent, steht der Diagnose-Kollege nur für Azure-VMs zur Verfügung, während Sie den Log-Analytics-Agenten auch auf lokalen VMs, lokalen Computern oder VMs in AWS oder Google installieren können.

Bevor Sie sich also mit Azure Log Analytics befassen, sollten Sie sich eine Übersicht der verfügbaren Monitoringagenten für Windows und Linux verschaffen. Wegen der eingangs skizzierten Konsolidierung von Azure Monitor und Log Analytics verfügt Azure Monitor über mehrere Agenten, genau genommen vier verschiedene Windows-Agenten (Azure-Monitor-Agent, Diagnoseerweiterung, Log-Analytics-Agent und Dependency-Agent) und fünf verschiedene für Linux (Azure-Monitor-Agent, Diagnoseerweiterung, Log-Analytics-Agent, Telegraf-Agent, Dependency-Agent).

Sie unterscheiden sich hinsichtlich der unterstützten Umgebungen (Azure, lokal, Multi-Cloud/Azure-Arc), der gesammelten Daten, der Speicher- und Analyseplattform, in denen die Daten landen (Azure Monitor Metrics, Azure Monitor Logs, Speicherkonto oder Event Hub), und der Tools, mit denen sich die Daten abfragen lassen. Die Linux-Agenten unterscheiden sich von denen für Windows vor allem hinsichtlich der gesammelten Daten. Hier geht es fast ausnahmslos entweder um Leistungsdaten oder das Syslog. Da sich die verschiedenen Agenten bei den Eigenschaften zum Teil überschneiden, kann es schwierig sein, die richtige Wahl zu treffen – auch in Bezug auf die entstehenden Kosten. Microsoft schreibt [3] zu den verfügbaren Varianten: "Es kann vorkommen, dass spezifische Anforderungen für einen bestimmten Computer nicht vollständig durch einen einzelnen Agenten erfüllt werden können."

Azure Log Analytics nutzen

Den Log-Analytics-Agenten aktivieren Sie bei gewählter VM im Haupt-Navigationsmenü im Abschnitt "Überwachung" unter "Protokolle". Hier müssen

Sie auf den Knopf "Aktivieren" klicken. Die Abrechnung der in Log Analytics zu analysierenden Daten läuft dann über eine eigene Entität namens "Log Analytics Workspace". Mindestens einen Workspace müssen Sie entweder direkt beim Aktivieren des Agenten einschalten (die betreffende VM ist dann eine Quelle in diesem Log Analytics Workspace). Alternativ legen Sie vorher im Azure-Portal einen neuen "Log Analytics Arbeitsbereich" an und registrieren dort im Abschnitt "Arbeitsbereichdatenquellen / Virtuelle Computer" die gewünschte VM bei diesem Arbeitsbereich.

Weitere valide Datenquellen sind "System Center", "Azure Aktivitätsprotokoll" oder "Speicherkontoprotokolle". Wählen Sie einfach die gewünschte VM aus und klicken auf "Verbinden". VM und Log Analytics Workspace müssen sich übrigens nicht in der gleichen Region befinden. Ist mindestens eine Quelle eingerichtet, können Sie Log Analytics verwenden. Hierzu nutzen Sie wie zuvor beschrieben entweder von der VM ausgehend das Menü "Überwachung/ Protokolle" oder Sie öffnen im Azure Monitor den Abschnitt "Protokolle". Hier müssen Sie dann allerdings zunächst wieder den gewünschten Scope eingrenzen.

Eigene Abfragesprache an Bord

Azure Monitor Logs zielt mit seiner mächtigen Abfragesprache Kusto Query Language (KQL; gelegentlich auch "Azure Data Explorer" genannt) darauf ab, Informationen aus der Zusammenführung dieser unterschiedlichen Quellen und unterschiedlichen Datentypen zu gewinnen. Daher ergibt es in der Praxis wenig Sinn, den Log-Analytics-Agenten zum Beispiel auf einer oder wenigen VMs zu aktivieren. Die Abrechnung von Log Analytics erfolgt auf Basis der Menge an erfassten Daten, die in den Workspaces laufen, sowie der für die Datenaufbewahrungszeit getroffenen Einstellungen. Es kann übrigens bis zu zehn Minuten nach der Aktivierung der Quelle dauern, bis beispielsweise ein virtueller Computer konfiguriert ist und sich die Überwachungsdaten zeigen.

Kusto ist wie erwähnt sehr mächtig und eine systematische Einführung sprengt den Rahmen des Beitrags. Daher hier nur ein

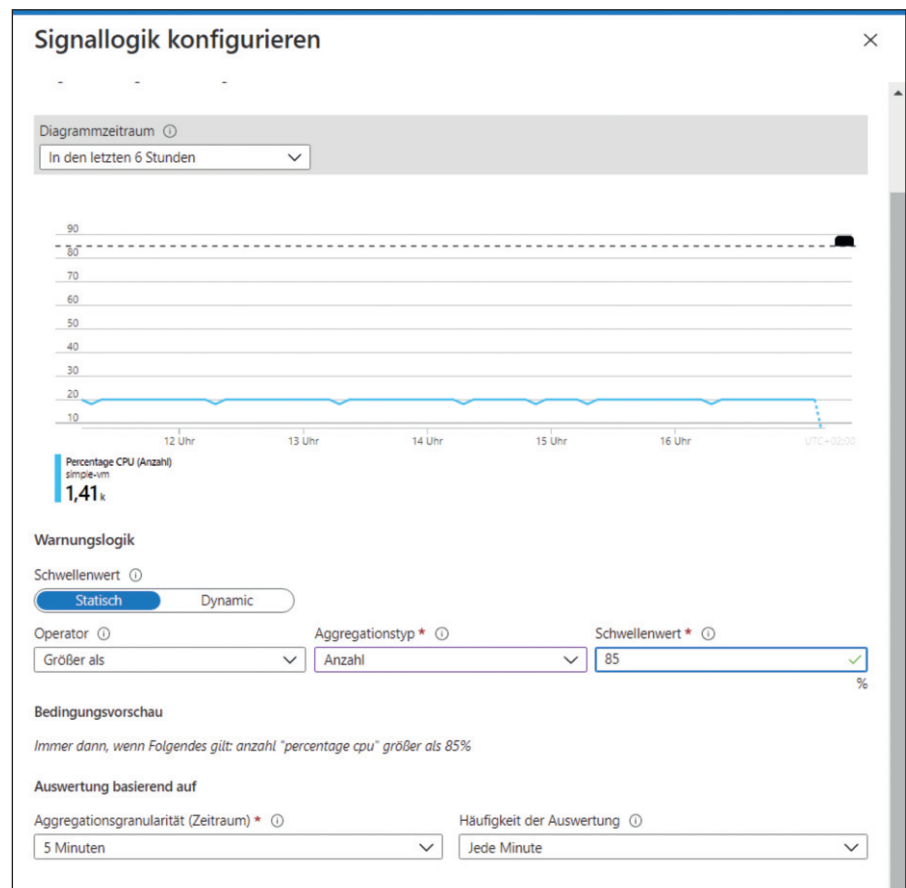


Bild 5: Das Erstellen einer Warnlogik am Beispiel der CPU-Auslastung einer VM.

Einstieg: Jede Kusto-Abfrage ist eine geschützte Anforderung zur Verarbeitung von Daten und zur Rückgabe der Ergebnisse, formuliert als unformatierter Text. Kusto verwendet ein Datenflussmodell, das einerseits Lesbarkeit und andererseits das Verfassen und die Automatisierung der Syntax vereinfachen soll. Die Abfrage verwendet Schema-Entitäten, die in einer SQL-ähnlichen Hierarchie organisiert sind wie Datenbanken, Tabellen und Spalten. Jede Abfrage besteht daher aus einer Folge von Anweisungen, getrennt durch ein Semikolon mit mindestens einer tabellarischen Ausdrucksanweisung [4], die Daten in einem tabellenähnlichen Raster aus Spalten und Zeilen erzeugt. Die tabellarischen Ausdrucksanweisungen der Abfrage liefern dann die Ergebnisse der Abfrage.

Sie müssen sich aber nicht beim ersten Aufruf von Log Analytics intensiv in Kusto einarbeiten, da Microsoft zum einen einen großen Fundus an Beispielabfragen mitliefert, die Sie als Basis verwenden können, und weil Sie Abfragen im Editor auch interaktiv zusammenbauen können, indem Sie im Menü auf die in den Daten-

banken und Tabellen organisierten Datenstrukturen zugreifen. Sobald Sie das beim ersten Start von Log Analytics angezeigte Beispielvideo gesehen oder übersprungen haben, öffnet Log Analytics ein Pop-up-Fenster mit Beispielabfragen. Jede davon können Sie mit dem gleichnamigen Knopf entweder "Ausführen" oder nur "In den Editor laden". Letzteres zeigt die Abfrage in Kusto-Syntax im Query-Editor.

Die folgende Abfrage liefert einen Report über den freien Festplattenspeicher über alle verbundenen Instanzen als Maximalwert über den angegebenen Zeitbereich (hier 24 Stunden):

```
// virtual machine free disk space
// Show the latest report of free
// disk space, per instance.
// To create an alert for this
// query, click '+ New alert rule'
Perf
| where ObjectName == "LogicalDisk"
or // the object name used in
// windows records
ObjectName == "Logical Disk" // the
// object name used in Linux records
```

```
| where CounterName == "Free
  Megabytes"
| summarize arg_max(TimeGenerated,
  *) by InstanceName // arg_max over
  TimeGenerated returns the latest
  record
| project TimeGenerated, Instance-
  Name, CounterValue, Computer,
  _ResourceId
```

Nach erfolgreicher Abfrage können Sie jederzeit wieder rechts oben auf den Knopf "Abfragen" klicken, um wieder zum Fenster mit den Musterabfragen zu gelangen. Nicht alle Beispiele erscheinen jedoch im Pop-up-Fenster, im Navigationsbereich links finden Sie bei markiertem Tab "Abfragen" eine vollständige Liste.

Fahren Sie mit der Maus ohne zu klicken über eine Abfrage aus der Liste, öffnet sich ebenfalls ein Fenster, von dem aus Sie die Abfrage entweder ausführen oder in den Editor laden. Sofern die Abfrage sinnvolle Daten liefert, zeigen sich diese nicht nur im Tab "Ergebnisse", sondern sind im Tab "Diagramm" auch grafisch aufbereitet verfügbar oder mit dem Button "Exportieren" oben rechts als CSV speicherbar.

Darüber hinaus lassen sich Kusto-Abfragen von Grund auf neu formulieren. Dazu wählen Sie im Navigationsmenü links statt "Abfragen" den Tab "Tabellen" und klicken dann einzelne Entitäten doppelt, die dadurch in das Editor-Fenster gelangen.

Mit Alarmen automatisieren

Alarmer und Warnregeln in Azure sind das Tor zur Automatisierung. So binden Sie Ihr vorhandenes Ticketsystem, sofern es mindestens Webhooks versteht, an Azure an. Dies erlaubt, dass eine Warnbedingung von außen das Anstoßen einer Aktion in Azure auslöst oder dass eine in Azure ausgelöste Alarmbedingung ein Ticket in Ihrem Ticketsystem erstellt. Alarmer können Sie auf Metriken, Ereignisse oder Protokollabfragen definieren.

Kehren wir dazu zu einer einfachen Host-basierten Metrik in Azure Monitor Metrics zurück. Werfen Sie einen Blick auf eines der Standarddiagramme wie "CPU Durchschnitt" für eine virtuelle Maschine und legen Sie mit einem Klick auf "Neue

Warnregel" eine ebensolche an. Als "Bereich" ist in diesem Fall die betreffende VM bereits eingetragen. Sie können das Erstellen von Warnregeln aber nicht nur aus jeder Ressource heraus, sondern auch aus Azure Monitor (Menü "Warnungen") anstoßen oder direkt im Azure-Portal nach "Warnungen" suchen.

Die vorgeschlagene "Bedingung" löschen Sie am besten gleich mit einem Klick auf den Mülleimer und erstellen mit dem Link "Bedingung hinzufügen" eine neue. In diesen Fall müssen Sie nur den Signaltyp aus der Liste auswählen. Achtung: Die verfügbaren 70 Signale für VMs verteilen sich auf vier Seiten. Durch diese navigieren Sie unten rechts oder bemühen einfach die Suche. Danach erstellen Sie die gewünschte Warnlogik mit den Parametern "Schwellenwert-Typ" (statisch oder dynamisch), "Operator", "Aggregationstyp" und "Schwellenwert" sowie der "Aggregationsgranularität" und der "Häufigkeit" der Auswertung.

Nach der Warnbedingung folgen die gewünschten Aktionen. Dazu müssen Sie, falls noch nicht vorher geschehen, mit dem gleichnamigen Link eine "Aktionsgruppe hinzufügen" oder eine solche, wenn noch nicht vorhanden, mit "Aktionsgruppe erstellen" anlegen. Diese bekommt wie jede Azure-Ressource zunächst im Tab " Grundeinstellungen" eine Ressourcengruppe, einen Namen und einen Anzeige-Namen.

Im Register "Benachrichtigungen" konfigurieren Sie dann eine Benachrichtigung. Diese sind immer Teil der Aktionsgruppe, gehören aber nicht zu den eigentlichen Aktionen. Als Benachrichtigungstypen stehen "E-Mail an Azure Resource Manager-Rolle" und "E-Mail/SMS-Nachricht/Push/Stimme" zur Verfügung. Der gewählte Typ braucht dann noch einen Namen und spezifische Konfigurationsoptionen.


Bei "E-Mail/SMS-Nachricht/Push/Stimme" sind das beispielsweise die Empfänger-E-Mail-Adresse oder SMS-Rufnummer. Erst dann geht es mit einem Klick auf "Weiter: Aktionen" im Tab "Aktionen" zu den möglichen Aktionen. Zur Wahl stehen an dieser Stelle "Automation Runbook", "Azure Function", "ITSM" (IT Service Manage-

ment), "Logik-App", "Sicherer Webhook" oder auch "Webhook".

Hier sind Ihrer Fantasie kaum Grenzen gesetzt: Sie können via ITSM, Webhook oder Secure Webhook ein Ticket in Ihrem Ticketsystem erzeugen und auch mehrere Aktionen kombinieren, wie zum Beispiel eine Azure Function oder Logic-App auslösen. Sie sind auch in der Lage, ein Azure Automation Runbook [5] zu triggern. Ist die Aktionsgruppe erstellt, benötigt die Warnregel nur noch einen Namen, ein zugeordnetes Abonnement, eine Ressourcengruppe und den gewünschten "Schweregrad" zwischen "0 (kritisch)" und "4 (ausführlich)". Jetzt erzeugen Sie die Policy mit einem Klick auf "Warnregel erstellen".

Fazit

Unser Beitrag hat die weitreichenden Möglichkeiten des Azure Monitor nur angerissen. Denn der komplette Funktionsumfang sprengt den Rahmen des Artikels. Zu erwähnen wären beispielsweise noch die Visualisierungsmöglichkeiten etwa in Form der Azure Dashboards oder weitere Analysewerkzeuge wie die Azure-Arbeits-mappen oder die Integration des Azure Monitor mit Power BI.

Dennoch sollten Sie einen Eindruck erlangt haben, wie mächtig Azure Monitor ist und welche Möglichkeiten sich beispielsweise aus den skizzierten Warnungen, den erfassbaren Metriken und der Integration in Ticketsysteme ergeben. Und auch in den Bereichen Security und Konfigurationsmanagement hat Azure Monitor einiges zu bieten. (In) 

Link-Codes

[1] Azure Monitor für das Enterprise-Monitoring
l8z31

[2] Application Insights
l8z32

[3] Übersicht über Azure-Monitor-Agenten
l8z33

[4] Anweisungen für tabellarische Ausdrücke
l8z34

[5] Azure-Automation-Runbook-Typen
l8z35