Fehlerbehebung

Virtual Desktop Service

NetApp
February 20, 2023

Inhaltsverzeichnis

Fehlerbehebung

Fehlerbehebung bei fehlgeschlagenen VDS-Aktionen

Überblick

Ein Großteil der Protokollierung, die in VDS stattfindet, ist in der Web-UI aufgrund des schieren Volumens nicht zugänglich. Detailliertere Protokolle finden Sie am Endpunkt. Diese Protokolle werden im Folgenden beschrieben.

In VDS v5.4+ werden die Protokolle im folgenden Ordnerpfad gefunden:

```
 C:\programdata\cloudworkspace
In früheren VDS-Versionen können sie sich in den folgenden Pfaden
befinden:
```

```
C:\Program Files\CloudWorkspace\
C:\Program Files\CloudJumper\
C:\Program Files\IndependenceIT\
```

Der Dateityp variiert auch nach VDS-Version. Protokolldateien sind entweder .txt- oder .log-Dateien, die in Unterordnern des oben beschriebenen Pfads gefunden werden.

Automatisierungsprotokolle

CW VM Automation Service-Protokoll

```
 CwVmAutomationService.log
Der CW VM Automation Service ist ein Windows-Dienst, der für das
Management aller virtuellen Maschinen in der Bereitstellung verantwortlich
ist. Als Windows-Dienst wird er immer in einer Bereitstellung ausgeführt,
hat aber zwei Hauptbetriebsarten: Den geplanten Task-Modus und den
Ereignismodus.
```

Der geplante Task-Modus besteht aus Aktivitäten, die im Rahmen eines Zeitplans auf den VMs ausgeführt werden, einschließlich Erfassung von Sizing- und Performance-Daten, Neubooten von VMs, Einchecking-Status (ein oder aus) im Vergleich zu Regelsätzen, die durch die Funktionen „Workload Schedule“ und „Live Scaling“ generiert werden. Die Protokolle bezeichnen diese Aktionstypen in der 5. Spalte mit Namen wie „tägliche Aktionen“, „wöchentliche Aktionen“ und „tägliche Wartung“. Wenn Sie Fragen wie „Warum hat Server X Neustart letzte Nacht um 2:00 am“ oder „Warum ist dieser Server an, wenn ich denke, es sollte aus“ beheben, dann sind die geplanten Aufgaben für diese spezifischen VMs in der Regel der beste Ort, um zu schauen.

Der Ereignismodus wird aktiviert, wenn ein Benutzer oder ein anderer VDS-Dienst, wie z. B. der CW Automation Service, zur Fertigstellung einer Aufgabe auffordert. Beispiele für diese Art von Aktivität sind eine

Benutzeranfrage zum Erstellen eines neuen Servers oder CW Automation, in der die Größe und der Zustand der zu prüfenden Server angefordert werden, weil dem Arbeitsbereich weitere Benutzer hinzugefügt wurden. Diese Ereignisse haben in der Regel Protokolleinträge mit dem Ereignisnamen „Create Server“ und dem tatsächlichen Namen der VM direkt daneben (z. B. Server NXTS2 erstellen). Bei der Fehlerbehebung dieser Art von Ereignissen ist es normalerweise am besten, zum unteren Rand des Protokolls zu blättern und dann zur aufwärts Suche nach dem VM-Namen. Sie können dann weitere Zeilen nach oben scrollen, um zu sehen, wo der Prozess gestartet wurde.

CW Automation Service-Protokoll

```
 CWAutomationService.log
Das CW Automation Service-Protokoll ist der primäre Windows-Service zur
Verwaltung der Komponenten einer Workspace-Bereitstellung. Er führt die
Aufgaben aus, die für das Management von Benutzern, Applikationen,
Datengeräten und Richtlinien erforderlich sind. Darüber hinaus kann die IT
Aufgaben für den CW VM Automation Service erstellen, wenn die Größe,
Anzahl oder der Zustand der VMs in der Bereitstellung geändert werden
müssen.
```

Wie der CW VM Automation Service führt der CW Automation-Service sowohl geplante Aufgaben als auch ereignisgesteuerte Aufgaben aus, wobei letzterer der häufigere Typ ist. Das Protokoll für den CW Automation Service beginnt jede Zeile mit der Einheit und Aktion, die bearbeitet wird (z. B. Start Server NXTS1). Die Suche nach dem Entity-Namen am unteren Rand der Datei ist der schnellste Weg, um die spezifischen Protokollzeilen zu finden, die für die Aufgabe gelten.

CW Agent Service-Protokoll

```
 CwAgent.log
Der CW Agent Service führt alle Aufgaben aus, die lokal für eine bestimmte
VM liegen, einschließlich der Prüfung der Ressourcenebenen und der
Auslastung der VM, der Prüfung, ob die VM über ein gültiges Zertifikat für
den TLS-Datenverkehr verfügt, und prüft, ob der obligatorische Neustart-
Zeitraum erreicht ist. Neben der Überprüfung detaillierter Informationen
zu diesen Aufgaben kann dieses Protokoll auch verwendet werden, um auf
unerwartete VM-Neustarts oder unerwartete Netzwerk- oder
Ressourcenaktivitäten zu prüfen.
```

CWManagerX-Protokoll

```
 CWManagerX.log
CWManagerX ist ein Webservice, der die Kommunikationsverbindung zwischen
der lokalen Bereitstellung und der globalen VDS-Kontrollebene
bereitstellt. Aufgaben und Datenanfragen, die aus der VDS-Webanwendung
oder der VDS-API stammen, werden über diesen Webdienst an die lokale
Bereitstellung übermittelt. Von dort aus werden die Aufgaben und
Anforderungen an den entsprechenden Webservice (oben beschrieben) oder in
seltenen Fällen direkt an Active Directory weitergeleitet. Da es sich
dabei meist um eine Kommunikationsverbindung handelt, gibt es bei normaler
Kommunikation nicht viel Protokollierung, aber dieses Protokoll enthält
Fehler, wenn die Kommunikationsverbindung unterbrochen oder falsch
ausgeführt wird.
```

DC-Konfigurationsprotokoll

```
 DCConfig.log
Bei DC Config handelt es sich um eine Windows-Anwendung, die bestimmte
Konfigurationsparameter bereitstellt, die nicht in der VDS-
Webanwendungsoberfläche verfügbar sind. Im Protokoll DC Config werden die
Aktivitäten aufgeführt, die ausgeführt werden, wenn
Konfigurationsänderungen in DC Config vorgenommen werden.
```

CAVDCDeployment-Protokoll

```
 CAVDCDeployment.log
CW VDC Deployment ist eine Windows-Anwendung, die die für die Erstellung
einer Implementierung in Azure erforderlichen Aufgaben ausführt. Das
Protokoll verfolgt die Konfiguration der Windows-Services des Cloud
Workspace, der Standard-GPOs sowie Routing- und Ressourcenregeln.
```

Verschiedene Protokolle

```
CwVmAutomationService-Installing.log
CwAgent-Installing.log
```

Die verbleibenden Protokolle verfolgen die Installation der oben beschriebenen Windows-Dienste und -Anwendung. Da VDS-Dienste automatisch aktualisieren, wenn eine neue Version für diese spezifische Bereitstellung bestimmt ist, verfolgen diese Protokolle den Upgrade-Prozess, da der Service oder die Anwendung während des Upgrades normalerweise deaktiviert werden müssen. Wenn Sie feststellen, dass die Dienste ständig gestoppt werden, können diese Protokolle helfen festzustellen, ob ein Upgrade auf einen bestimmten Service die Ursache ist. In diesen Fällen würde es erwarten, dass ein Fehler in diesen Protokollen angezeigt wird, in denen erläutert wird, warum das Upgrade fehlgeschlagen ist.

Zugriff auf Protokolle und Überprüfung von Informationen

Bei angeforderten Aktionen wie Klonen eines Servers, Hinzufügen eines Benutzers oder Wiederherstellen eines Backups erhalten Sie Feedback in der VDS-UI.

+[]

1. VDS speichert ausführliche Protokolle und stellt einige von ihnen im Abschnitt „Aufgabenverlauf“ der Seite „Bereitstellungen“ im VDS bereit. Klicken Sie auf Ansicht, um Details zu den aufgeführten Aufgaben anzuzeigen.

   []

2. Manchmal enthält der Aufgabenverlauf nicht genügend Details, um die wahre Ursache zu identifizieren. Um den Bereich Task History nutzbar zu halten und nicht von allen protokollierten Ereignissen überfordert zu werden, wird hier nur eine Teilmenge an Aufgabeinformationen dargestellt. Für einen tieferen Einblick in die oben genannten Text-Log-Dateien können weitere Details bereitgestellt werden.

   a. Um auf dieses Protokoll zuzugreifen, navigieren Sie zum Abschnitt Bereitstellungen und klicken Sie auf das Zahnradsymbol neben der CWMGR1-VM, und klicken Sie dann auf Verbinden (oder stellen Sie im Fall des CwAgent-Protokolls eine Verbindung zur entsprechenden VM her).

   []

3. Bei der Verbindung zu einem Platform Sever (wie dem CWMGR1) werden Sie nicht automatisch beim Server angemeldet (im Gegensatz zur Verbindung mit einem Server im Mandanten). Sie müssen sich mit einem Level3 .tech-Konto anmelden.

   []

4. Navigieren Sie dann wie oben gezeigt zum Pfad und öffnen Sie die Protokolldatei.

   []

5. Diese Textdatei enthält ein Protokoll aller Ereignisse, das älteste der neuesten Ereignisse ist:

   []

6. Beim Öffnen eines Support-Cases mit NetApp VDS wird die Möglichkeit, die hier gefundenen Fehler bereitzustellen, DIE Beschleunigung der Problemlösung DEUTLICH beschleunigen.

Fehlerbehebung In Bezug Auf Die Qualität Der Internetverbindung

Symptome

Wenn Benutzerverbindungen getrennt werden müssen, muss eine Verbindung wiederhergestellt werden. Laggy Interface Antwort, allgemeine Performance-Probleme, die nicht scheinen, mit Ressource (RAM/CPU) Lasten zusammenhängen.

Ursache

Wenn Benutzer Performance-Probleme melden, Benutzerverbindungen fallen gelassen oder eine laggy Schnittstelle, die häufigste Ursache sind nicht Ressourcen überhaupt, sondern die Netzwerkverbindungen zwischen dem Kunden und dem Rechenzentrum. Diese Verbindungen laufen über ihren ISP, verschiedene

Internet-Backbone-Betreiber und schließlich in das Rechenzentrum. Dabei werden die Daten durch mehrere Zwischenstopps geleitet. Jeder dieser Hops kann zu Netzwerklatenz, verlorenen Paketen und Jitter führen, die alle zur wahrgenommenen Performance der Desktop Computing-Umgebung auf dem virtuellen Desktop beitragen können.

Tier 1-Triage und Fehlerbehebung enthalten grundlegende Schritte wie die Bestätigung von Ressourcen (RAM, CPU und HDD-Platz) ausreichend sind. Sobald der Vorgang abgeschlossen ist, ist das Testen der Netzwerkkonnektivität ein großer nächster Schritt bei der Fehlerbehebung. Auflösung

Primäre Option: Der NetApp VDS Windows-Client verfügt über integrierte Diagnosetools

Der Diagnosetest kann innerhalb des Virtual Desktop Client ausgeführt und an Ihre E-Mail gesendet werden.

1. Klicken Sie auf das Voreinstellung-Symbol (vier horizontale Linien in der oberen Menüleiste).
2. Klicken Sie Auf Hilfe
3. Klicken Sie Auf Netzwerk-Test
4. Geben Sie den Benutzernamen ein, bei dem die Probleme auftreten, und klicken Sie auf Ausführen
5. Geben Sie nach Abschluss Ihre E-Mail-Adresse ein, um einen E-Mail-Bericht zu erhalten
6. Lesen Sie den Bericht, um mögliche Verbindungsprobleme zu beheben

[]

[]

Sekundäre Option: Manuelle Analyse mit PingPlotter

Um zu bestätigen, dass die Netzwerkverbindung des Clients die Ursache ist, können Sie das kostenlose Dienstprogramm PingPlotter ausführen. Dieses Dienstprogramm sendet alle paar Sekunden einen Ping und berichtet über die Geschwindigkeit (Latenz) der Umrundung dieses Ping. Es notiert auch den Paketverlust (PL) Prozentsatz an jedem Hop entlang der Route. Wenn eine hohe Latenz und/oder ein hoher Paketverlust beobachtet wird, ist es ein guter Hinweis darauf, dass die Leistungsprobleme durch die Qualität der Internetverbindung am Hop verursacht werden, die diese Probleme zeigt.

1. Herunterladen und installieren "Ping-Plotter" (Verfügbar für MacOS, Windows und iOS).
2. Geben Sie das Gateway des Datacenters ein, in dem der Mandant bereitgestellt wird.
3. Lassen Sie es mehrere Minuten laufen. Idealerweise, während Performance-Probleme oder Distimmigungen auftreten.
4. Erfassen Sie die Daten mit „Bild speichern…“ Über das Menü Datei, wenn es für eine zusätzliche Fehlerbehebung benötigt wird.

Desktop-Hintergrund für Benutzersitzungen aktivieren

Überblick

Bei Remote-Sitzungen ist die Hintergrundanzeige standardmäßig deaktiviert, um die Leistung zu verbessern. Das Ergebnis ist ein schwarzes Hintergrundbild, das Benutzer oft anpassen möchten. Diese Einstellung kann mit einer einfachen GPO-Bearbeitung geändert werden

Wichtig:

1. Melden Sie sich bei einem Plattform-Server an (z. B. CWMGR1) Verwendung von Level3 .tech-Konto
2. Öffnen Sie Die Group Policy Management Console
3. Suchen Sie das GPO rdsh (gekennzeichnet als „Unternehmenscode“ rdsh (z. B. „Xyz1 rdsh“)) Klicken Sie mit der rechten Maustaste auf das GPO „xyz1 rdsh“, wählen Sie „Bearbeiten“
    a. In Azure AD-Domänendiensten wird das GPO „ADDC“ genannt „Computer > Cloud Workspace-Computer“.
4. Ändern Sie die Richtlinie: Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remote Desktop Session Host > Remote Session Environment > Remote Desktop Wallpaper entfernen. Setzen Sie diese Einstellung auf deaktiviert

[] [] []

Fehlerbehebung Beim Drucken Von Problemen

Fehler

Das Drucken auf dem lokalen Drucker über den Cloud-Desktop funktioniert nicht.

Remote Desktop Services mit ThinPrint

VDS umfasst optional ThinPrint für RDS-Implementierungen (Remote Desktop Services). Die Software und die Lizenzierung werden bei der ersten Implementierung automatisch konfiguriert. Wenn ThinPrint in Gebrauch ist, können die folgenden Abschnitte die Fehlerbehebung bei Problemen mit dem Drucken erleichtern.

Ursache

Es gibt verschiedene Methoden zur Verbindung mit dem Cloud-Desktop. Diese Methode unterscheidet sich in der Ausführung von Druckfunktionen und damit in der Gewissheit, welche Art von Zugriff für die Fehlersuche benötigt wird:

1. Verwenden des Access-Client von CloudJumper auf einem Windows-Gerät
    a. ThinPrint wird auf dem lokalen Gerät ausgeführt und leitet die Kommunikation zwischen dem Drucker und dem Cloud-Desktop weiter
2. Verwenden des HTML5-Browsers auf jedem Gerät
    a. Der Browser zeigt das gedruckte Dokument als PDF an, um lokal herunterzuladen und zu drucken
3. Verwenden eines manuell konfigurierten RDP-Clients (normalerweise) auf einem Mac oder Linux-Computer
    a. Lokale Drucker werden mit dem Cloud-Desktop freigegeben, indem sie „Lokale Ressourcen“ im RDP-Client manuell konfigurieren.

Auflösung

1. Versuchen Sie, ein Dokument vom lokalen Gerät zu drucken, um zu bestätigen, dass das lokale Gerät erfolgreich eine Verbindung zum Drucker herstellt.
2. Deinstallieren Sie ThinPrint, und installieren Sie es erneut, wenn Sie den Access Client auf einem Windows-Gerät verwenden. https://www.thinprint.com/en/resources-support/software/clientsandtools/

3. Notieren Sie sich den Zugriffstyp und die Ergebnisse der ersten beiden Schritte in einem neuen Fall mit CloudJumper Support.

Azure Virtual Desktop

VDS implementiert keine Drucklösung oder spezielle Druckkonfiguration für AVD-Umgebungen. Fragen zum Drucken sollten an Microsoft oder (wenn eine implementiert wurde) an den Hersteller der Drucktechnologie gerichtet werden.

Azure vCPU Kernquote

Aktuelle Quote Anzeigen

1. Melden Sie sich bei der Azure Konsole an, navigieren Sie zum Modul „Abonnements“ und klicken Sie auf „Quoten“. Wählen Sie dann im Dropdown-Menü Provider alle Provider aus, wählen Sie im Dropdown-Menü „Alle anzeigen“ aus und wählen Sie die Azure-Region aus, in der Ihr Cloud Workspace bereitgestellt wird.

   []

2. Dann werden Sie sehen, wie viel Sie verbrauchen gegen Wie viel Kontingent haben Sie verfügbar. In der nachstehenden Abbildung verbraucht CloudJumper 42 CPUs von den 350 CPUs, die für die BS-Produktfamilie von VMs verfügbar sind. Steigende Kontingente

   []

3. Wenn Sie Ihre Quote erhöhen möchten, klicken Sie auf Anfrage steigern und sagen Sie es, was Sie erhöhen möchten (99% der Zeit wird dies Compute/CPUs sein).

   []

4. Wählen Sie die Region aus, in der Ihr Cloud Workspace bereitgestellt wird, und die VM-Familie, für die Sie die Quote erhöhen möchten.

   []

5. Geben Sie Ihre Kontaktinformationen ein und klicken Sie auf Erstellen, um die Anfrage an Microsoft zu übermitteln. In der Regel erhöhen sie das sehr schnell.

Entsperren Von Benutzerkonten

Überblick

Das Entsperren eines gesperrten Kontos für einen Endbenutzer ist ein einfacher Prozess, der ein mittelmäßig häufiges Problem behebt, das Endbenutzer berichten.

Nach vier fehlgeschlagenen Anmeldeversuchen wird der Benutzer gesperrt. Die Dauer beträgt 30 Minuten, es sei denn, das Konto hat die Passwortkomplexität aktiviert, in diesem Fall kann die Sperrung nur manuell durchgeführt werden.

Das Benutzerkonto kann in der Liste der Benutzer auf der Seite Benutzer und Gruppen in den Arbeitsbereichen oder auf der Seite Benutzerdetails entsperrt werden.

Seite „Benutzer Und Gruppen“

[] []

Seite „Benutzerdetails“

[]

Fehlerbehebung Bei Der Leistung Von Virtuellen Maschinen

NetApp bietet Kunden Einblick in die Fehlerbehebung bei der Server-Performance für Benutzer/Applikationen. Alle Unternehmen nutzen Ressourcen anders, je nachdem, wie viele Endanwender sich gleichzeitig angemeldet haben: Nutzung von Applikationen, falls SQL Standard installiert ist oder nicht SQL Express usw. Es ist also wichtig, die Vorgänge zu überprüfen, wenn ein Benutzer Performance-Probleme meldet.

Überblick

Jede App ist anders, und selbst die gleiche Software, die von der gleichen Anzahl von Benutzern ausgeführt wird, kann verschiedene Ressourcenverbrauchsmuster haben. Aus diesem Grund hilft es, die Anwendungen zu verstehen, die Ihre Benutzer verwenden und was wirklich die Macht der App. Handelt es sich um CPU, RAM oder Storage? Diese Überlegungen helfen Ihnen bei der Fehlerbehebung.

Nach unserer Erfahrung haben sich diese als allgemein wahrhaftige Aussagen erwiesen, die Ihnen helfen, zu beginnen:

```
CPU: this is usually the culprit/limiting factor if the app in question is
home-grown and/or an Excel issue
RAM: this is usually the culprit/limiting factor if SQL Standard is used
Storage: this is usually a contributing factor if disk consumption is
greater than 90%.
```

Wenn SQL Express verwendet wird, ist es wahrscheinlich ein einschränkender Faktor – es begrenzt den RAM-Verbrauch auf 1 GB, die unter den erforderlichen Spezifikationen des Software-Anbieters sein kann.

In nächtlichen Ressourcenberichten

VDS sendet nächtliche Berichte mit Informationen über jede VM. Dieser Bericht enthält viele nützliche Informationen, darunter Empfehlungen, ob Ressourcen erhöht oder verringert werden sollen. Hier einige Auszüge:

Dieses Bild zeigt, ob Sie CPU/RAM auf VMs für einen bestimmten Arbeitsbereich erhöhen oder verringern sollten.[]

In der Abbildung unten sehen wir, dass es eine Spalte gibt, die zeigt, wie lange der Server seit dem Neustart des Servers vergangen ist.[]

In diesem Image sehen wir einen Vergleich zwischen Storage Provisioning und Verbraucht – Dies wird zu einem guten Thema, um kurz zu untersuchen auf den ersten oder sobald Sie bestätigt haben, dass CPU/RAM nicht das Problem sind.[]

Anzeige des CPU-/RAM-Ressourcenverbrauchs in Echtzeit

1. Melden Sie sich beim VDS an, klicken Sie dann auf das Organisationsmodul und wählen Sie die gewünschte Organisation aus.

   []

2. Sie können den Server finden, an dem der Benutzer angemeldet ist, indem Sie ihn im Abschnitt Benutzer suchen.

   []

3. Blättern Sie dann nach unten, bis Sie den Abschnitt „Server“ sehen. Suchen Sie den Server, auf dem der Benutzer, der das Problem meldet, angemeldet ist, und klicken Sie auf das Einstellrad, und stellen Sie dann eine Verbindung her.

   []

4. Wenn Sie eine Verbindung zum Server hergestellt haben, klicken Sie auf die Schaltfläche Start. Klicken Sie dann auf Task-Manager.

   []

5. Der Task-Manager gibt Ihnen einen umfassenden Einblick in das Geschehen, genau in diesem Moment. Dies ist der absolut beste Weg, um zu sehen, was Ihre Benutzer im Moment beeinflussen sie ein Problem an Sie melden.
6. Sie können die auf dem Server ausgeführten Prozesse überprüfen, ermitteln, welche Ursache das Problem hat und entweder mit dem Kunden kommunizieren oder die Prozesse vor Ort beenden.

   []

7. Sie können auch die Registerkarte Performance anzeigen, um zu zeigen, was passiert, live. Dies ist ein gewaltiger Schritt zur Fehlerbehebung: Die Endbenutzer müssen die Schritte wiederholen, die sie unternommen haben, um ein Performance-Problem zu verursachen, und dann sehen, was passiert. Ähnlich, wenn sie folgen allgemeinen Rat (schließen Sie überschüssigen Chrome-Browser-Tabs, wie Google Chrome Tabs sind eine gemeinsame Ressource Verbraucher) können Sie sehen Ressourcenverbrauch Rückgang.

   []

8. Auf der Registerkarte „Benutzer“ können Sie anzeigen, welcher Benutzer – falls überhaupt – die Ressourcen verbraucht, was zu einer Spitzenauslastung führt.

   []

9. Sie können jeden Endbenutzer erweitern, um zu sehen, welche spezifischen Prozesse sie laufen und wie viel jeder verbraucht.

   []

10. Eine weitere Option ist die Anzeige, welche Dienste ausgeführt werden.

    []

11. Kunden können den Ressourcenmonitor auch öffnen, um weitere Einzelheiten zu erfahren.

[]

Erwägen Storage-PerformAkne

Einer der häufigsten Ursachen für Performance-Probleme mit vms ist die unzureichende Performance von Festplatten. Standard- (und sogar SSD-Festplatten) sind nicht für die hohe I/O-Last ausgelegt, die für VDS Workloads erforderlich ist. Benutzer-Logins erfolgen in der Regel in Bündel und jeder erfordert erhebliche I/O, da Profile und Einstellungen geladen werden. Die hochperformanten Storage-Technologien von NetApp wie Azure NetApp Files, CVO und CVS eignen sich besonders gut für diesen Workload und sollten als Standardoption für VDS-Workloads angesehen werden.

Berücksichtigung des Storage-Verbrauchs

Microsoft gilt seit langem als Best Practice, beim Festplattenverbrauch jedes Laufwerks mindestens 90 % zu zulässt. Dies führt in ihren Augen zu einem Performance-Einbußen und kann zu weiteren Herausforderungen führen. Beispielsweise fehlt es an genügend Storage für Backups, sodass Benutzer nicht mehr arbeiten können.

RMM-Tools können Speicher-Monitoring-Services anbieten, einschließlich der Möglichkeit, Schwellenwerte und Warnmeldungen festzulegen. Wenn der Speicher zu einer Herausforderung für Sie wird, empfiehlt es sich, diese Art von Warnmeldungen mit Ihrem RMM-Anbieter zu aktivieren.

Zur tieferen Untersuchung installieren Sie Software, um den Laufwerkverbrauch zu überprüfen.

Aus Gesprächen mit Kunden haben sich WinDirStat oder TreeSize als bevorzugte Anwendungen für die Kontrolle des Antriebsverbrauchs erwiesen.

WinDirStat kann eine vollständige Festplatte über das Netzwerk untersuchen, wenn nicht genügend Speicherplatz vorhanden ist, um eine App lokal zu installieren/auszuführen oder die Anmeldung blockiert ist:

+[]

DNS leitet für Azure FÜGT & SSO über O365-Identität weiter

Überblick

Benutzer können nicht auf Firmen-Websites auf primären E-Mail-Domain zugreifen.

Zum Beispiel können NetApp Mitarbeiter in VDS-Arbeitsbereichen nicht auf netapp.com zugreifen, wenn ihr SSO-Konto user@netapp.com ist

Dedizierte VDS-Implementierungen nutzen die interne Domäne des Azure-Mandanten.

Auflösung

Um dies zu lösen, muss das Team des Unternehmens, das DNS verwaltet, eine DNS-Suchtzone für Ihre interne Domäne erstellen, damit sie die richtige externe IP-Adresse auflösen kann (um NetApp zu diesem Zweck NetApp Mitarbeiter innerhalb ihres virtuellen Desktops auf netapp.com durchsuchen zu können).

Schritt für Schritt

1. Installieren Sie die DNS-Server-Tools auf CWMGR1 – damit können Sie DNS verwalten.

[]

[]

[]

[]

[]

2. Nach der Installation können Sie zu Systemsteuerung → System und Sicherheit → Verwaltung Tools gehen und DNS öffnen.

   []

3. Wenn Sie nach dem DNS-Server gefragt werden, auf dem DNS ausgeführt wird, möchten Sie Ihren Domainnamen eingeben (in dem Beispiel, das wir verwendet haben, wäre dies *netapp.com*).

Fehlerbehebung Bei Applikationsproblemen

Überblick

Fehlerbehebung bei einem Anwendungsfehler ist eine gängige administrative Praxis, die nicht VDS selbst beinhaltet, aber wird stark unterstützt durch VDS und die Kontrolle, die es Administratoren bietet. Da NetApp VDS keine Fehlerbehebung für diese Probleme bei den Kunden übernimmt, können wir anhand unserer Erfahrungen Administratoren Ratschläge geben, nachdem wir einige grundlegende Informationen wie die folgenden ermittelt haben, um sich ausführlicher mit den Endbenutzern und/oder Drittanbietern zu beschäftigen.

- Name des Benutzers, der das Problem auftritt
- Name der Anwendung, mit der der Benutzer arbeitete
- Der Server, auf dem die Benutzersitzung war
- Schritte zur Reproduktion des Problems

Überprüfen Ihrer Tools

Monitoring

Nachdem Sie den Server identifiziert haben, den der Benutzer verwendet hat, überprüfen Sie Ihre Überwachungslösung, um zu überprüfen, ob der Ressourcenverbrauch (CPU und RAM) im normalen Bereich liegt. Sie können auch validieren, dass anwendungsspezifische Anforderungen (ein besonderer Service, der Probleme verursachen wird, wenn es nicht läuft) sind funktionsfähig. In solchen Situationen können erweiterte Einstellungen wie die Überwachung der oben/unten genannten Dienste ausgelöst worden sein.

Virenschutz

Als Administrator mit Zugriff auf die Server und auf Azure Active Directory können Sie die erkannten Daten und die festgelegten Richtlinien überprüfen. Sollte ein unvorhergesehener Vorfall vorhanden sein, kann es zu Auswirkungen auf Ihre Applikation kommen.

Weitere Tools

Einige Anwendungen erfordern zusätzliche Komponenten, wie z. B. ein Servicekonto, das unbestimmte Zeit angemeldet bleibt, oder ein VPN an eine physische Ausrüstung (z. B. eine Netzwerk-Appliance vor Ort oder ein Gerät der Fertigungsausrüstung oder Diagnoseprogramm). In diesen Fällen können anwendungsspezifische Fehler durch eine andere Ursache als die Installation der Anwendung oder die Konfiguration der Einstellungen verursacht werden.

Erweiterung des Zugriffs auf Dritte

Anwendungen und/oder deren Datenbanken werden häufig von dem Softwareanbieter (ISV) selbst oder einem Drittanbieter installiert, konfiguriert und unterstützt. In diesen Situationen möchten Sie den temporären Administratorzugriff auf folgende Schritte ausweiten: "Bereitstellen von zeitweiligen Zugangs zu Dritten"

Als Best Practice empfiehlt es sich, diese Konten von Dritten nach Abschluss des Upgrades oder Updates oder nach Behebung des Problems herunterzufahren.

In vielen Fällen erfordert ein Software-Wartungsvertrag mit dem ISV, um eine solche Fehlerbehebung durchzuführen. Falls dies nicht der Fall ist, kann Ihnen der ISV dieses Problem möglicherweise erst unterstützen, wenn er vorhanden ist.

> Möglicherweise besteht auch darin, dass das Problem der Fehlerbehebung auf die Hardware (Desktops, Laptops, Thin Clients usw.) zurückzuführen ist, mit der die Endbenutzer arbeiten. Ein Beispiel könnte sein, dass ein Upgrade des Laptops eines Benutzers könnte die Maschine in den Augen einer dünnen Client-Konfigurationsdatei sperren, was bedeutet, dass die Endbenutzer nicht auf die Tools zugreifen können, die ihnen erlauben, sich an ihrem virtuellen Desktop anzumelden. In diesem Fall kann ein Wartungsvertrag für Hardware erforderlich sein, bevor der Hersteller Ihnen behilflich sein wird.