Juniper Networks | Engineering Simplicity

E-Guide

WAN-Fehlerbehebung E-Guide für eine zügige Lösung

Eingabe

Einführung

Wide Area Networks (WANs) sind komplexe Clouds, die kritischen und nicht-kritischen Datenverkehr bewältigen.

Die meisten WANs nutzen Service Provider und verschiedene zugrunde liegende Transporttypen. In den vergangenen Jahren wurde für den Aufbau und die Erweiterung von WANs zu niedrigen Kosten vermehrt auf Dedicated Internet Access (DIA) Circuits gesetzt.

In einigen Fällen werden WANs vollständig als Overlay oder VPN auf diesen Internet-Circuits eingerichtet. Anstelle private Verbindungen zu nutzen, teilt der Datenverkehr dann einen Pfad mit einem lokalen Internet-Breakout.

Die Überwachung und Beobachtung des WANs (einschließlich seiner Komponenten) ist für die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit des Datenverkehrs des Geschäfts, von entscheidender Bedeutung.

Die meisten WANs basieren entweder direkt oder indirekt auf dynamischen Routing-Protokollen. Diese Protokolle erfassen Fehler in Grundelementen und der daraus folgenden pfadübergreifenden Erreichbarkeit.

Fehler sind zwar nicht unvermeidbar, sie treten aber dennoch mit hoher Wahrscheinlichkeit aufgrund verschiedentlichster Ursachen von Geräteproblemen, Überlastung, Kabelbrüchen bis hin zu Bedienfehlern ein.

Bei steigender Automatisierung und durchgehender Abstraktion finden wir bisweilen Datenlecks bezüglich der Logik oder der Routen, die die Gewährleistung unserer Services gefährden.

Dieser Leitfaden beschreibt praktische Schritte und Ansätze, die Ihnen helfen, wenn etwas schief läuft.

Wenn etwas schief läuft, können zur Wiederherstellung der Dienste verschiedene Ansätze verfolgt werden.

Das Ziel bleibt dabei jedoch immer gleich: Minimierung der MTTR und Maximierung der MTBF (mittlere Zeit zwischen Ausfällen).

Wie verteilt sich das Risiko auf Ihr WAN?

Wie lässt es sich klassifizieren?

Wie ist mit den unvermeidlichen Auswirkungen von Fehlern oder Überlastungen umzugehen?

Ansätze für die Fehlerbehebung

Das Internet (oder ein IP-Netzwerk) wird auch als eine „Reihe von Röhren" beschrieben. Man sollte es sich besser als eine Reihe an Sitzungen und Nachrichten, die unter Gruppen verwalteter und nicht verwalteter Geräte stattfinden, vorstellen.

Nachrichten müssen nicht unbedingt einen Status aufweisen, die Sitzungen speichern jedoch das Konzept eines „Status" ab. Diese Datenverkehrstypen erstellen und haben mehrere Abhängigkeiten.

Abhängigkeiten führen zu Risiken.

Bei der Fehlerbehebung wird aktiv sondiert und gesucht. Eines der effizientesten Verfahren zur Fehlerbehebung besteht, ähnlich wie bei einer binären Suche, in der kontinuierlichen Halbierung des Problembereichs. Während dieses Verfahrens wird kontinuierlich validiert, aber die Symptome, Problemberichte und die Überwachung stellen den zugrunde liegenden Problemstatus nicht immer korrekt dar.

Häufig muss der Netzwerksingenieur zur Ermittlung einer spezifischen Ursache zu direkten Maßnahmen korrelieren. Das Ziel besteht in der schnellstmöglichen Ursachenermittlung zur Bestimmung von Notfallmaßnahmen bzw. zur Eindämmung des Problems, um dann entsprechende Gegenmaßnahmen zur Vermeidung eines erneuten Auftretens auszuarbeiten.

Zur Fehlerbehebung kann „Top-Down" oder „Bottom-Up" gearbeitet werden; beide Verfahren können jedoch ineffizient oder unnötig aufwändig sein bzw. zu langsamen Ergebnissen führen. Ein „Middle-Out"-Verfahren kann bei anfänglich mehrdeutigen Bedingungen unter Umständen rascher Ergebnisse hervorbringen.

Wenn ein Netzwerkingenieur oder System ein Signal erhält, dass etwas schief läuft, ist normalerweise eine unabhängige bzw. sekundäre Verifizierung erforderlich. Das ist die Umsetzung des Prinzips „Vertrauen ist gut, aber Kontrolle ist besser", da selbst bei einer vertrauenswürdigen Alarmsignalquelle immer Zweifel eintreten, wenn eine konstenintensive Fehlerbehebung ausgeführt werden muss.

Für die meisten Validierungs- und Verifizierungsphasen ist eine Automatisierung von Vorteil: Sie reduzieren mühselige Aufgaben, beschleunigen das Erzielen von Ergebnissen und lassen den menschlichen Bedienern mehr Zeit für hochrangigere komplexe Interaktionen.

Benutzerüberwachung

Auch hier gilt: „Man kann nichts verwalten, was man nicht messen kann.“ Die Visibilität Ihrer Assets und Services ist zur Vermeidung ablenkenden Rauschens bei der Filterung der eingehenden Daten von grundlegender Bedeutung.

Eine ausgewogene Instrumentierung „aller Dinge” ist zum Erkennen des Status wichtig und ermöglicht, rasch umsetzbare Alarme zu priorisieren.

Optimale Nutzung von Benutzersitzungen

Den Benutzern sind ihre spezifischen Daten und Sitzungen wichtig. Sie bedienen komplexe Geräte und lassen Unmengen an Anwendungen laufen, bei denen sich Fehler unter Umständen nur schwer beheben lassen. Wenn Probleme auftreten, erhalten sie möglicherweise den Eindruck, dass das Netzwerk nicht funktioniert, aber es ist nicht ihre Aufgabe bzw. Verantwortungsbereich, zu ermitteln, wo genau die Ursache eines technischen Fehlers liegt.

Auch wenn Benutzer bisweilen Fehler ungenau melden, sind sowohl sie selbst als auch ihre Rechner als Indikator, wo die Fehlerursache liegen kann, äußerst nützlich. Ihre Sitzungen können Ihnen helfen, die Ursachen rasch zu ermitteln und sie können sogar dazu beitragen den tatsächlichen Zustand des WANs offenzulegen.

Aus Benutzersitzungen lassen sich Kontrollgruppen erstellen, um individuelle oder aggregierte Netzwerkprobleme zu identifizieren. Bis vor Kurzem war es noch teuer, sie zu verfolgen und zu instrumentieren.

Die herkömmliche manuelle Fehlerbehebung kann zwar auch weiterhin eingesetzt werden, aber unsere Toolbox bietet nun bessere Diagnostik für Szenarien, die bislang äußerst zeitraubend und ein diplomatisches Tretminenfeld waren.

Nun können wir echte Benutzerüberwachung im WAN bieten und eine automatische „Bottom-Up”-Fehlerbehebung ausführen. So können wir WAN-Probleme schneller diagnostizieren und klassifizieren, was wiederum zu schnelleren Lösungen und wiederhergestellten Services führt.

Netzwerküberwachung und Transparenz

Wenn wir die Ursache eines Problems kennen, sollte sich die Fehlersuche erübrigen. Stattdessen können wir den unerwünschten Status der relevanten Komponenten oder Elemente überwachen.

Je transparenter das gesamte Netzwerk ist, desto besser können wir den Systemstatus aus den Ergebnissen ableiten und desto schneller und feinmaschiger kann der Problembereich zur Ermittlung von Antworten partitioniert werden.

Protokolle, Signalübertragung, Datagramme und Pakete sind gut definiert und dürften die Regeln einhalten. Das Netzwerk selbst ist jedoch ein komplexes verteiltes System: Die Konfiguration eines Geräts meldet den Status eines anderen Geräts.

Bei der herkömmlichen Überwachung von Netzwerken konzentrierte man sich auf den Zustand von Netzwerkelementen. Dies ist zwar auch weiterhin äußerst wichtig, aber wir müssen nachweisen, dass die Sitzungsdaten eines spezifischen Benutzers zuverlässig von A nach B übermittelt werden können.

Das bedeutet, dass wir bessere Kardinaldaten benötigen und die Nachweislast obliegt weiterhin den Netzwerktechnikern, um nicht nur die Verfügbarkeit, sondern auch die Erreichbarkeit innerhalb des Pfads aus der Benutzerperspektive zu bestätigen.

Wenn ein System so komplex wird, dass die Abhängigkeiten und geteilten Status uns nicht mehr einfach eine Ursache finden lassen, müssen wir leider weiterhin Fehlersuche betreiben.

- Die Informationen von Systemen und Benutzern mögen zwar korrekt sein, können jedoch zu Bugs und Tendenzen führen.
- Die Erfassung zu großer Datenmengen kann uns überlasten. Hier hilft im Voraus zu wissen, wonach zu suchen ist, auch wenn sich damit die notwendige Verifizierung nicht erübrigt.
- Die Überwachung hilft bekannt problematische Status oder Schwellwerte im Auge zu behalten, obwohl wir zur Bestimmung der Ursache häufig weiter gehen müssen.

Die Suche nach einem vorübergehend unbekannten Fehler heißt implizit, dass wir bislang nicht in der Lage waren, dieses Problem zu instrumentieren oder zu überwachen. Dieses Abfragen und Suchen ist die Grundessenz der Fehlerbehebung.

Bei zunehmender Komplexität multiplizieren sich die Variablen, die sich auf den Datenverkehr ausüben können.

Der Nachweis, dass das Netzwerk korrekt funktioniert, wird zu einer nicht unerheblichen Aufgabe.

WAN-Fehlerbehebung

Ein WAN kann aus vielen Arten von Topologien, Protokollen, Anbietern und Elementen bestehen.

Hier finden Sie einige allgemeine High-Level Anleitungen und Hinweise, um Ihnen zu helfen, das Beste aus Ihren Bemühungen zu holen. Als Nächstes sollte das Ziel sein, Ihre eigenen individuell angepassten Verfahren zur Fehlerbehebung, Modellierung und Dokumentierung betrieblich so umzusetzen, dass sie einen besseren Wissensaustausch und eine rasche Automatisierung ermöglichen.

Allgemeine Empfehlungen

Verfeinern und definieren sie kontinuierlich die **Problemstellung.**

Klassifizieren Sie **Umfang und Auswirkung** entsprechend Ihrer geschäftlichen Anforderungen und der Einschätzung der Bedeutung.

Stufen Sie die Wiederherstellung der Funktionalität schnellstmöglich ein. Führen Sie eine Nachuntersuchung ohne Ursachenbestimmung durch, wenn die Ursache auch weiterhin nicht bekannt ist.

Bitten Sie stets um Einsicht **neuer Daten und um empirische Evidenz.**

Dokumentieren Sie kontinuierlich. Erfassen und teilen Sie alle Daten, Snippets, Zeitstempel und Meldungen (wenn zulässig).

Besuchen Sie kontinuierlich **erste Anfänge erneut**, um über ein Problem nachzusinnen.

Das Prinzip der Parsimonie trifft meist zu. Auch der Verlauf ist wichtig: **Was hat sich geändert?**

Konzentrieren Sie sich beim Partitionieren des Problembereichs sowohl **auf die Unterschiede** als auch auf die Gemeinsamkeiten.

Nur weil Sie es nicht sehen können, bedeutet das nicht, dass es nicht geschieht.

Je einfacher Ihre Einrichtung, desto leichter lassen sich Fehler beheben.

Voraussetzungen

Die Überwachung von Netzwerkelementen ist für die Zustandsprüfung auf Geräteebene aktiviert (einschließlich eventueller aggregierter virtueller Geräte).

Die Überwachung und Trendüberwachung auf Schnittstellenebene ist eingerichtet, einschließlich der korrekten Geschwindigkeiten, Schwellwerte und Puffer oder Warteschlangenstatistiken.

Die Fähigkeit, Routen von der Benutzerlokalisierung oder vom Standort zu verfolgen.

Für alle relevanten managed Netzwerkelemente einschließlich, wenn möglich, des Geräts des Benutzers, ist Zugriff auf die Routing- und Forwarding-Tabellen (RIBs und FIBs) verfügbar.

Zentrale Anmeldung oder Abfrage, vorzugsweise mit UTC-Zeitstempel in Millisekundengenauigkeit.

Annahmen

1. Das Benutzerendgerät gehört zu einer Gerätegruppe mit dem gleichen Problem (im Gegensatz zu vereinzelten Host-Vorfällen).
2. Benutzerendgeräte können Datenverkehr korrekt an andere Ziele weiterleiten (ohne über das WAN zu gehen).
3. Alle erfassten Daten (vereinzelt oder anderweitig) sind zwar nützlich, gelten aber als möglicherweise nicht korrekt bis sie in einem Aufzeichnungssystem unabhängig verifiziert oder geprüft sind.
4. Ein WAN-Problem kann konstant oder gelegentlich auftreten.
5. Das Problem liegt nach (1) und (2) im WAN und ist kein Client-seitiges Problem mit Host-Routing, Authentifizierung, Client-VPN usw.
6. Vollständiger IPv4-Stack (im Gegensatz zu einem Dual-Stack oder nur IPv6).
7. ICMP-Echo Request (Typ 8), Echo Reply (Typ 0) und Zeitüberschreitung (Typ 11) sind auf Netzwerkelementen auf dem Pfad von der Quelle bis zum Ziel Ende-zu-Ende-verschlüsselt.
8. Die Netzwerktechniker kennen sich mit dem Aufbau ihrer verwalteten Topologie aus. Die Dokumentation oder das dynamische Mapping ist hinsichtlich aller verwalteten Infrastukturknoten aktuell.
9. Die Netzwerküberwachung meldet keine bekannten oder relevanten Probleme, die sich auf das beschriebene Zeitfenster auswirken.

Auflösung und Erreichbarkeit

1. **Etablierung und Gewährleistung der Nutzung der aktuellen IP-Adresse der Quellschnittstelle des Client und des Remote-Services bzw.** des Ziels. Hierzu gehört das Prüfen, ob eine benannte Ressource verwendet wird und wie sie aus Client-Perspektive gemeistert wird.

2. **Von der Ursprungs-IP-Adresse des Standard-Gateways des Clients ein ICMP Echo (ping) an die Zieladresse senden** (das DF-Bit einstellen und eine Paketgröße wählen, die voraussichtlich die Ende-zu-Ende-Verschlüsselung übersteht). Bei Fehlschlagen...

3. **Die Route von der Ursprungs-IP-Adresse des Standard-Gateways des Clients zur Ziel-IP rückverfolgen** (ICMP verwenden, aber wenn zulässig die Nutzung von UDP oder TCP in Betracht ziehen). Wenn das nicht funktioniert oder zu erwarteten Knoten führt...

4. **Sicherstellen, dass die IP-Erreichbarkeit den erwarteten Pfad einschlägt** und die RIB des letzten bekannten „guten" Hops prüfen.

5. **Die relevanten Zugriffskontrolllisten (ACLs), Firewall-Vorgaben und maximalen Übertragungseinheiten (MTUs)** am letzten bekannten „guten" Hop sowie innerhalb des Pfads bei allen, die nur einen Hop entfernt sind, prüfen.

6. **Wenn die IP-Erreichbarkeit nachgewiesen ist, im Ursprungs-Subnet mit dem Testen der relevanten TCP oder UDP-Ports für den fraglichen Dienst beginnen.** Tools wie telnet, tcptraceroute, tcping, curl, hping3, nmap oder nc erfordern möglicherweise den Zugriff auf ein Allzweck-Computerendgerät, wenn dies auf dem Netzwerkgerät nicht verfügbar ist.

7. **Nahezu alle TCP-Dienste antworten auf ein SYN;** viele UDP-Dienste antworten eventuell nur wenn die Nachricht für den fraglichen Dienst korrekt aufgebaut ist.

8. **Unabhängig validieren, ob der Remote-Service am richtigen Port ist** (wenn möglich) und die Schritte von (1) aus Perspektive des remote Subnets wiederholen.

Wenn das Quellendgerät nicht auf Ausführung eines Tests unter voller Emulierung des Benutzers geprüft wird, muss die erste und nächste Layer 3-Schnittstelle verwendet werden (gewöhnlich der Standard-Gateway des Clients).

Netzwerkelemente verfügen gewöhnlich über ein kleines Tool-Set zur Fehlerbehebung in der Befehlszeile; diese sind jedoch nicht immer so flexibel wie die eines voll ausgestatteten Allzweck-Computerendgeräts mit installierbaren Paketen und Tools.

Ziehen Sie in Betracht, Ihre bekannten Services für die Echtzeitsensibilisierung auf Sitzungsebene um echte Benutzerüberwachung (RUM) zu erweitern.

Sitzungs- und anwendungsbewusst werden

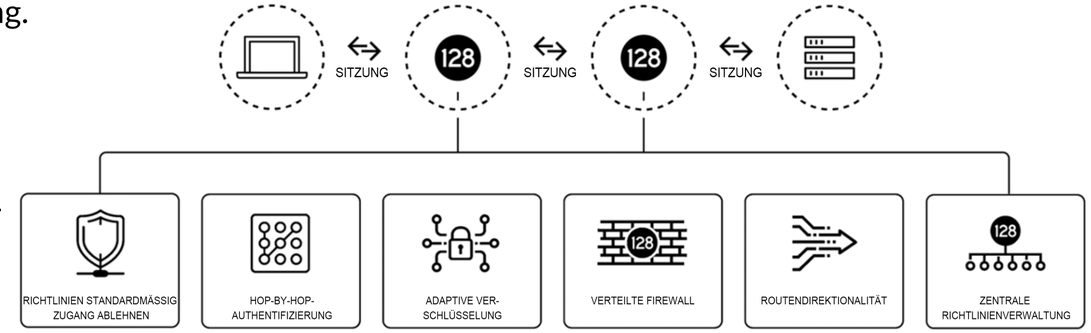
Die Fehlerbehebung setzt auf Situationsbewusstsein. Bislang haben Router ihre Weiterleitungsaufgaben ohne ein echtes Konzept des Sitzungs- bzw. Anwendungsstatus ausgeführt. Firewalls und Load Balancer verfolgen und nutzen Aspekte des Status, obwohl Sitzungsbewusstsein nicht im gesamten Netzwerk vorhanden ist. Wie wäre es, wenn eine neue Router-Generation sitzungs- und anwendungsbewusst werden könnte, um ein intelligenteres Routing und die Umsetzung von Richtlinien zu ermöglichen.

Junipers Session Smart™ Router (SSR) sind für Anwendungs- und Sitzungsbewusstsein gemacht.

Durch die kontinuierlichen Optimierungen der Benutzererfahrung werden die Supportkosten und MTTR um 30 bis 40 % dramatisch gesenkt. Dieses Sitzungs-basierte Netzwerkmodell bietet tunnelfreie Leisutngssteigerungen und eine einfache Skalierung.

Simplifizierte Zugangskontrollen und Hypersegmentierung, sprich SASE (Secure Access Service Edge), sind von Anfang an integriert.

In die Fabric wird unzertrennlich eine „Zero-Trust“-Sicherheit integriert, was das Risiko dramatisch senkt und das Vertrauen in die Integrität des Services steigert.



Sobald das Network Fabric um Intelligenz erweitert werden kann, folgen zahlreiche Vorteile wie zum Beispiel geringere Support-Kosten, eine bessere Visibilität und eine einfachere Fehlerbehebung.

Juniper Session Smart™

Junipers Software-basierte Session Smart™ Lösung lässt sich (über white-box/hypervisor) oder über die öffentliche Cloud rasch und leicht vor Ort bereitstellen.

Dieses Sitzungs-basierte Modell ermöglicht ein grenzenloses Fabric, das die Latenz um bis zu 60 % und die Kosten pro Bandbreite um 30 bis 50 % reduziert. Durch die flexiblen Bereitstellungsoptionen können Sie alles bereits Vorhandene nutzen und dabei von den Vorteilen eines intelligenteren und einfacheren WAN profitieren: zufriedenere Benutzer, bessere Leistung, weniger Arbeit mit der Fehlerbehebung und mehr Sicherheit.

Simplizität

Keine Tunnel, keine Overlays, ohne Hardware-zentriertes Netzwerk.

Agilität

Schnellere Bereitstellung, eine bessere Reaktionsfähigkeit, dynamische Optimierung.

Sicherheit

Zero-Trust-Modell: Authentifizierung + Verschlüsselung + Segmentierung.

Leistung

Weniger Betriebskosten, mehr Skalierbarkeit, dynamische Optimierung.

Einsparungen

Reduzierte Bandbreite und Konnektivitätskosten.

Discover Session Smart™ SD-WAN

Schauen Sie sich das Webinar an.

Nehmen Sie an einer unserer Live-Demos „Transformation Thursday“ teil, um das KI-gestützte SD-WAN in Aktion zu sehen.

Haben Sie noch weitere Fragen?
Weiteren Support und genaue Leitfäden für die Fehlerbehebung finden Sie in unserer Wissensdatenbank.

PN: 7400132-001-DE

Hauptsitz und Sitz des Vertriebs
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Telefon: +1 888 586 4737
oder +1 408 745 2000
Fax: +1 408 745 2100
www.juniper.net

Hauptniederlassung für die Regionen APAC und EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31 0207 125 700
Fax: +31 0207 125 701