CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

01 Routing

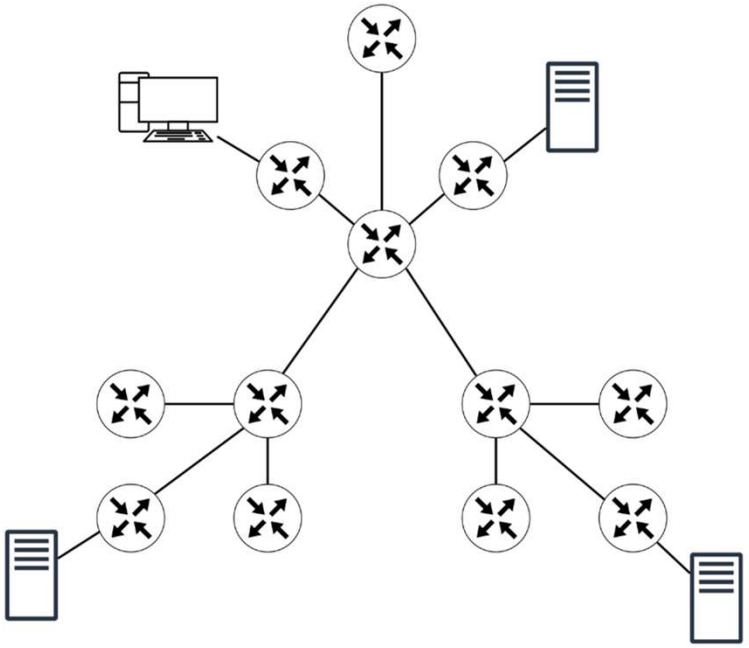
02 Netzwerk-Troubleshooting

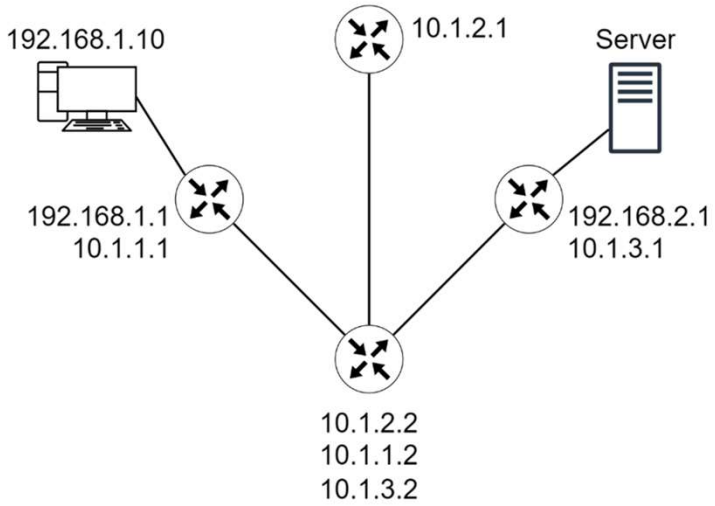
01 Routing

Router

- Router leiten Verkehr an Computer, andere Router und schließlich an den Zielcomputer weiter.
- Im einfachsten Fall senden Clientcomputer die gesamte Kommunikation über einen einzelnen Router, der als Standardgateway bezeichnet wird.
- Wenn mehrere Router in einem Subnetz vorhanden sind muss komplexeres Routing konfiguriert werden.

Router




192.168.1.10
10.1.2.1
Server
192.168.1.1
10.1.1.1
192.168.2.1
10.1.3.1
10.1.2.2
10.1.1.2
10.1.3.2

Statisches und Dynamisches Routen

- Eine statische Route wird manuell vom Administrator konfiguriert.
- Eine dynamische wird mit Hilfe spezieller Routingprotokolle ermittelt.
- Dynamisches Routing wird durch dynamische Konfiguration mit Hilfe von Routing-Tabellen umgesetzt.
    - Routing Information Protocol (RIP)
    - Open Shortest Path First (OSPF)
    - Interior Gateway Routing Protocol (IGRP)
    - Border Gateway Protocol (BGP)

Distance Vector und Link-State

Distance Vector	Link-State
Betrachtet die Netztopologie aus Sicht der Nachbarn	Erhält eine umfassende Information der gesamten Netztopologie
Addiert distanz Vektoren von Router zu Router	Berechnet den kürzesten direkten Pfad zu anderen Routern
Regelmäßige, periodische Updates; Mit langsamer Konvergenz	Ereigniss gesteuerte Updates; Schnelle Konvergenz
Leitet Kopien der Routing-Tabellen an benachbarte Router weiter	Leitet Link-State Routing Updates an andere Router weiter

RIP - Routing Information Protocol

- Ein dynamisches Protokoll, das Distanz-Vektor-Routing-Algorithmen verwendet, um zu bestimmen, welche Route die Datenpakete nehmen sollen.
- Das Protokoll berechnet den Pfad oder die Schnittstelle über die das Paket weitergeleitet werden soll, sowie die Anzahl der Hops zum Ziel.

OSPF - Open Shortest Path First

- Arbeitet mit SPF-Algorithmus (Shortest Path First) und resultierendem SPF-Baum.
- Regelmäßige Updates (Link-State-Aktualisierungen) durch Flooding.
- Feststellen der Erreichbarkeit von Nachbarn mittels Hello-Protokoll.
- Schnelle Reaktion auf Netzänderung: Der SPF-Algorithmus berechnet mit den LSA-Informationen die optimalen Pfade neu und aktualisiert die Routingtabelle (lokal).
- Die Routingtabelle enthält Pfad samt Kosten und Interfaces zu jedem bekannten Netz, um den optimalen Pfad für die Pakete zu bestimmen.

AS - Autonome Systeme

- Ein autonomes System (kurz AS) ist, laut klassischer Definition, eine Menge von Routern (die mehrere Netzwerke verbinden) mit einem gemeinsamen inneren Gateway-Protokoll (IGP) und gemeinsamen Metriken, die bestimmen, wie Pakete innerhalb eines AS vermittelt werden, unter einer einzigen technischen Verwaltung.
- Allerdings ist es nicht mehr unüblich, in einem AS mehrere IGP und mehrere Sätze von Metriken zu verwalten. Ein autonomes System ist dann ein System, das sich anderen autonomen Systemen so präsentiert, als hätte es nur einen einzigen inneren Routing-Plan, um ein beständiges Bild davon abzugeben, welche Ziele (z. B. andere Netzwerke) durch dieses System erreicht werden können.
- Autonome Systeme sind untereinander verbunden und bilden so das Internet.

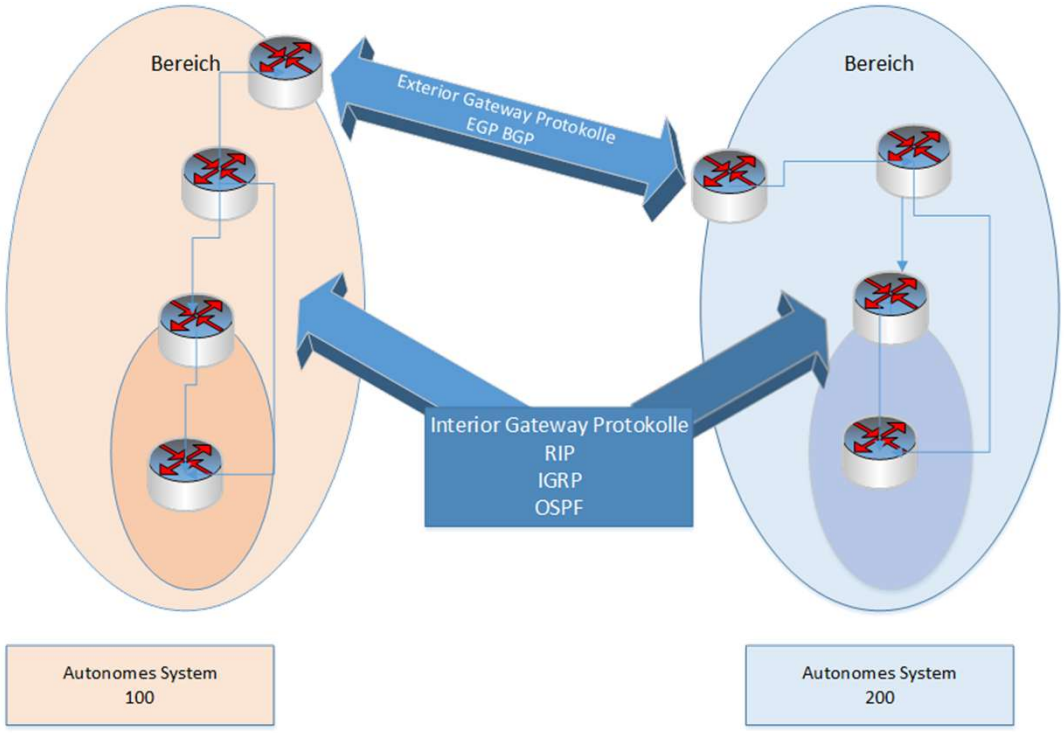
IGRP – Interior Gateway Routing Protocol

- In den 1980er Jahren von Cisco entwickelt
- proprietäres Distance-Vector-Routing Protocol
- innerhalb eines autonomen Systems
- weiterentwickelt zu EIRGP

BGP – Border Gateway Protocol

- Im Internet eingesetzte Routingprotokoll
- verbindet autonome Systeme (AS) miteinander.
- auch als Exterior Gateway Protokoll

Routing Protokolle



Routing Beispiel

NAT - Network Address Translation

- Beim NAT (Network Address Translation) werden die Adressen eines privaten Netzes über ein Koppelelement (Router) in öffentlich registrierte IP-Adressen „umgewandelt“.
- IP Masquerading, PAT (Port and Address Translation), bildet alle Adressen eines privaten Netzwerkes auf eine einzelne öffentliche IP-Adresse ab.

Was sollte ich auf jeden Fall behalten

- **Routing** - bezeichnet die Wegfindung von Daten einer Quelle zu einem definierten Ziel. Ein IP-Router übernimmt dabei die Aufgabe des Routings
- **AS** - ein System, das sich anderen autonomen Systemen so präsentiert, als hätte es nur einen einzigen inneren Routing-Plan, um ein beständiges Bild davon abzugeben, welche Ziele (z. B. andere Netzwerke) durch dieses System erreicht werden können.
- **Internes Routing** - mit Protokolle wie RIP, OSPF oder IGRP
- **BGP** - das verbreitetste Protokoll zum Routing zwischen AS
- **NAT (Network Address Translation)** - zur “Umwandlung” von Adressen eines privaten Netzes über ein Koppelelement (Router) in öffentlich registrierte IP-Adressen
- **PAT (Port and Address Translation)** - bildet alle Adressen eines privaten Netzwerkes auf eine einzelne öffentliche IP-Adresse ab.

02 Netzwerk-Trouble-shooting

Tools

Windows integriert

- Grafisch
    - Netzwerkproblembehandlung

Powershell

- Get-NetIPConfiguration
- Get-/New-NetIPAddress
- Get-/Set-NetIPInterface
- Set-DNSClientServerAddress
- Get-DNSClientCache
- Clear-DNSClientCache
- Get-NetRoute
- Test-Connection

Tools

Eingabeaufforderung

- Ipconfig
- Ping
- Tracert / pathping
- Netstat
- Nslookup
- Nbtstat
- Arp
- netsh
- route

Tools - ipconfig

-all - Zeigt detaillierte Informationen über alle Netzwerkadapter
-release - Gibt eine automatisch zugeteilte IP-Adresse wieder frei
-renew - Erneuert alle automatisch zugeteilten IP-Adressen / sucht nach DHCP im Netz
-flushdns - für Fehlersuche in DNS-Verbindung / löscht DNS-Cache
-registerdns
-displaydns

Tools - ping

-t - andauerndes pingen
-a - Für umgekehrte Namensauflösung an der Ziel-IP-Adresse
-n - Anzahl der zu sendenden Echo-Anforderungen (Default-Wert ist 4)
-l - Gibt die Länge des Datenfeldes in Bytes an (Default-Wert ist 32)
-i - Wert des TTL (Time To Live = Lebensdauer des Paketes) in Hop Counts
-4 - nutzt IPv4

Tools - tracert

-d - tracert löst die IP-Adressen von Zwischenroutern nicht in Namen auf
-h - Gibt Anzahl der maximalen Hops an
-w - Wartezeit in Millisekunden, zum Empfangen der ICMP-Nachricht

Tools - netstat

-a - Zeigt alle aktiven TCP-Verbindungen und offene TCP- und UDP-Ports
-b - Ist wie -a, plus welche ausführbare Datei daran beteiligt ist
-e - Zeigt Ethernet-Statistiken an
-o - Zeigt aktive TCP-Verbindungen mit der Prozess-ID (PID) für jede Verbindung
-r - Zeigt den Inhalt der IP-Routingtabelle an

Tools - nbtstat

-c - <cache> Zeigt den Inhalt des NetBIOS-Namen-Zwischenspeichers an
-n - <names> Zeigt die NetBIOS-Namentabelle des lokalen Computers an
-r - <resolved> Zeigt an, wie der NetBIOS-Namen aufgelöst wurde

1. Überwachung und Alarme

- Die erste Voraussetzung für die Behandlung und Lösung von Netzwerkproblemen ist ein System, das einen zeitnahen Alarm auslöst, wenn ein Problem auftritt.
- Mit einer stets aktiven (Netzwerk-)Monitoring-Software sind automatisierte Ermittlungen und zielgerichtete Workflows möglich. Die verbundenen Komponenten werden schnell angezeigt, wenn eine Störung oder Abweichung vorliegt.

2. Untersuchung

- Der Administrator muss den Umfang des Problems ermitteln.
- Wenn sich das Problem auf einen Client oder eine Gruppe von Clients bezieht, muss ein Test der Leistung oder Antwortzeit von Applikationen durchgeführt werden. um auf diesem Wege festzustellen, ob es sich um ein Problem mit dem drahtgebundenen Netzwerk oder WLAN handelt.

3. Isolierung

- Wenn das Problem auf ein einziges Netzwerksegment, einen Switch, Router oder Server oder eine Applikation identifiziert wurde, können der Pfad, Geräte und Ports ggf. isoliert.
- Der gesamte Pfad muss analysiert werden. Dazu sind Datenverkehrsstatistiken für jede Strecke einzusehen, um zu bestimmen, ob das Problem durch ein fehlerhaftes Gerät, Verbindungsmedien, Störungen oder eine Datenverkehrsüberlastung verursacht wird.

4. Ursachenanalyse und Problemlösung

- Wenn die Ursache des Problems zweifelsfrei feststeht, kann eine Lösung entwickelt, implementiert und geprüft werden. Wenn sich das Problem nicht auf das Netzwerk bezieht und nicht mit der Serverantwortzeit zusammenhängt oder durch überlastete Ressourcen zustande kommt, sind detailliertere Informationen durch die Erfassung und Analyse von Daten-Paketen erforderlich.

Tipps zur Fehlersuche

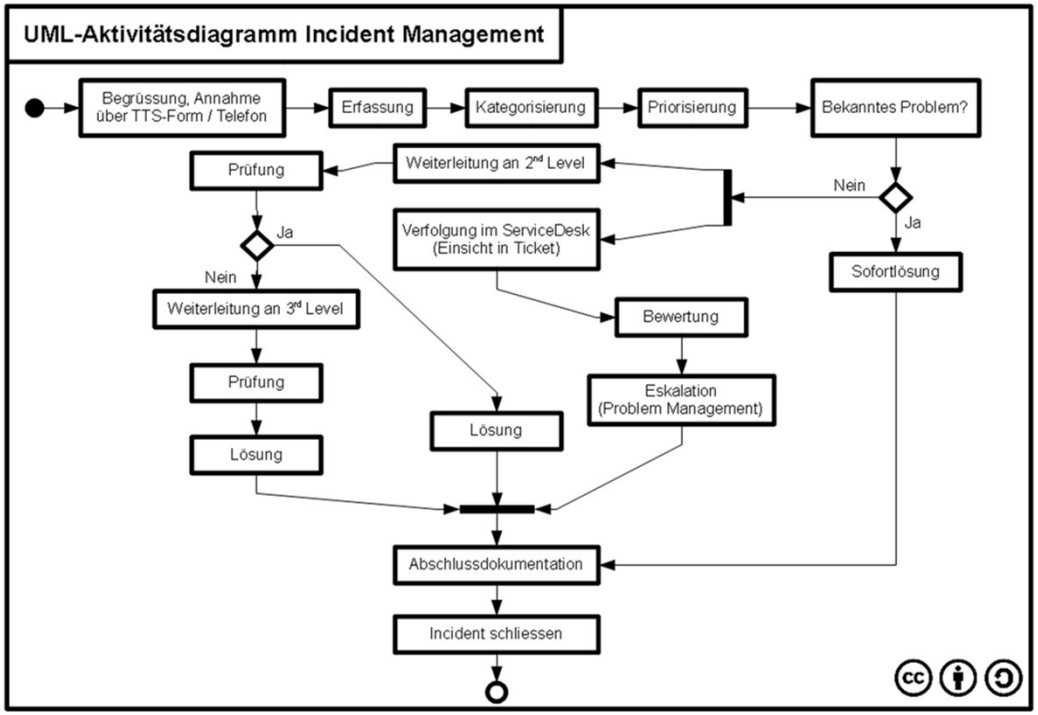
Der 4 Schritte Plan

1. Ermitteln der Änderungen
2. Ausschließen möglicher Ursachen (Was ist es nicht?)
3. Ermitteln und Bewerten einer Lösung
4. Testen einer Lösung

Tipps zur Fehlersuche

- Sichtprüfung
- Ipconfig
- Ping
- Tracert / Pathping
- Namensauflösung (nslookup, nbtstat)
- netstat

Incident Management



Was sollte ich auf jeden Fall behalten

- **ipconfig** - Er zeigt die verwendeten IP-Adressen und weitere Netzwerk-Informationen eines Computers an, die sich alternativ auch per Benutzeroberfläche ermitteln lassen.
- **ping** - ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist.
- **tracert/pathping** - ermittelt, über welche Router und Internet-Knoten IP-Datenpakete bis zum abgefragten Rechner gelangen.
- **netstat** - ein Kommandozeilenprogramm, das Protokollstatistiken und aktuelle Rechnernetzverbindungen anzeigt.

Was sollte ich auf jeden Fall behalten

- **nslookup** - ein Befehl um IP-Adressen oder Domains eines bestimmten Computers mittels DNS herauszufinden.
- **nbtstat** - Zeigt Protokollstatistik und aktuelle TCP/IP-Verbindungen an, die NBT (NetBIOS über TCP/IP) verwenden.
- **ARP** - Ändert und zeigt die Übersetzungstabellen für IP-Adressen/physische Adressen an, die von ARP (Address Resolution-Protokoll) verwendet werden.

DANKE!

Gibt es noch Fragen?

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm