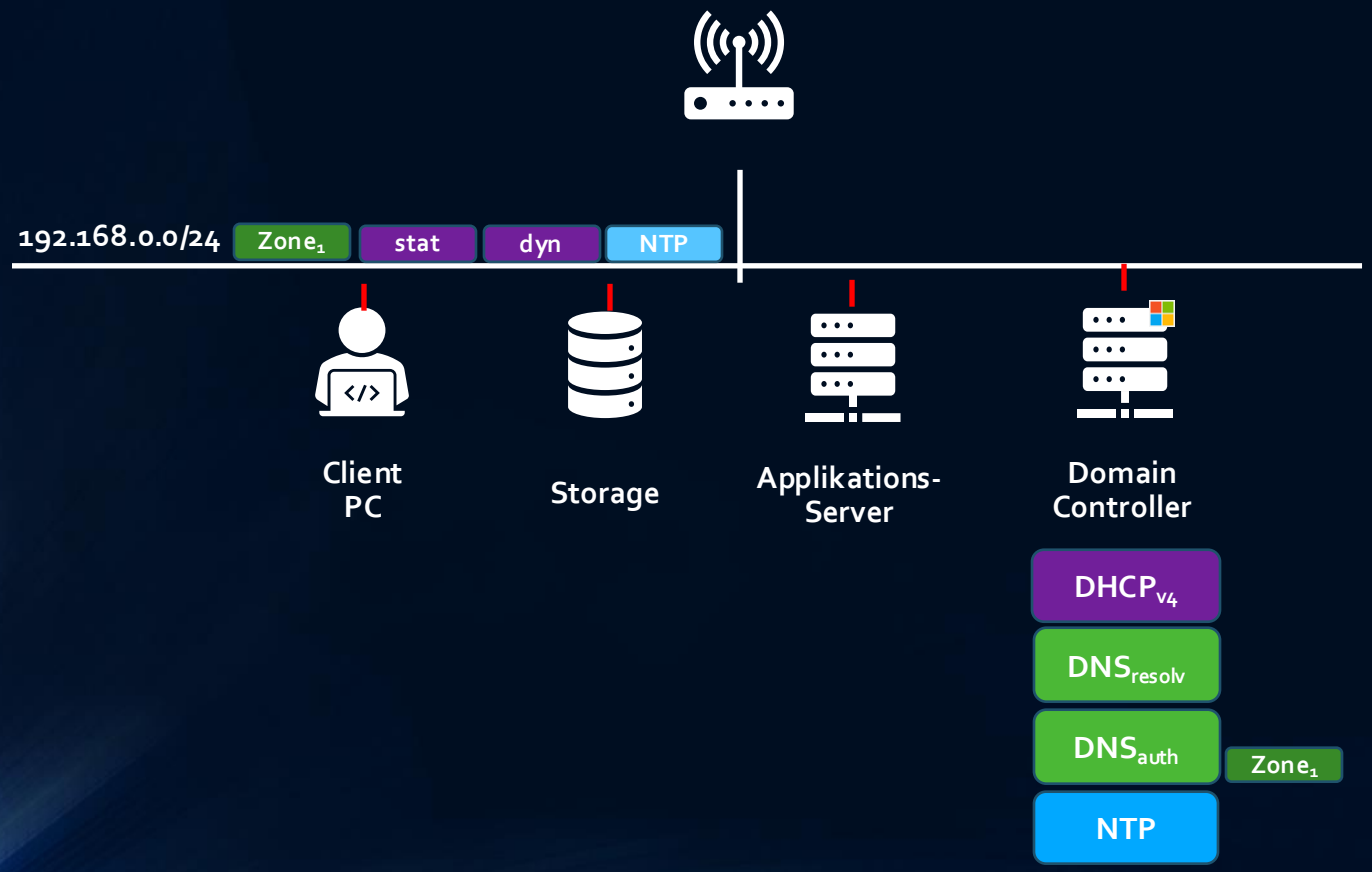
Von der IP-Adresse zur Netzwerkplanung

JÖRG BACKSCHUES - DDI USER GROUP – HAMBURG 11/2024

Über was reden wir?

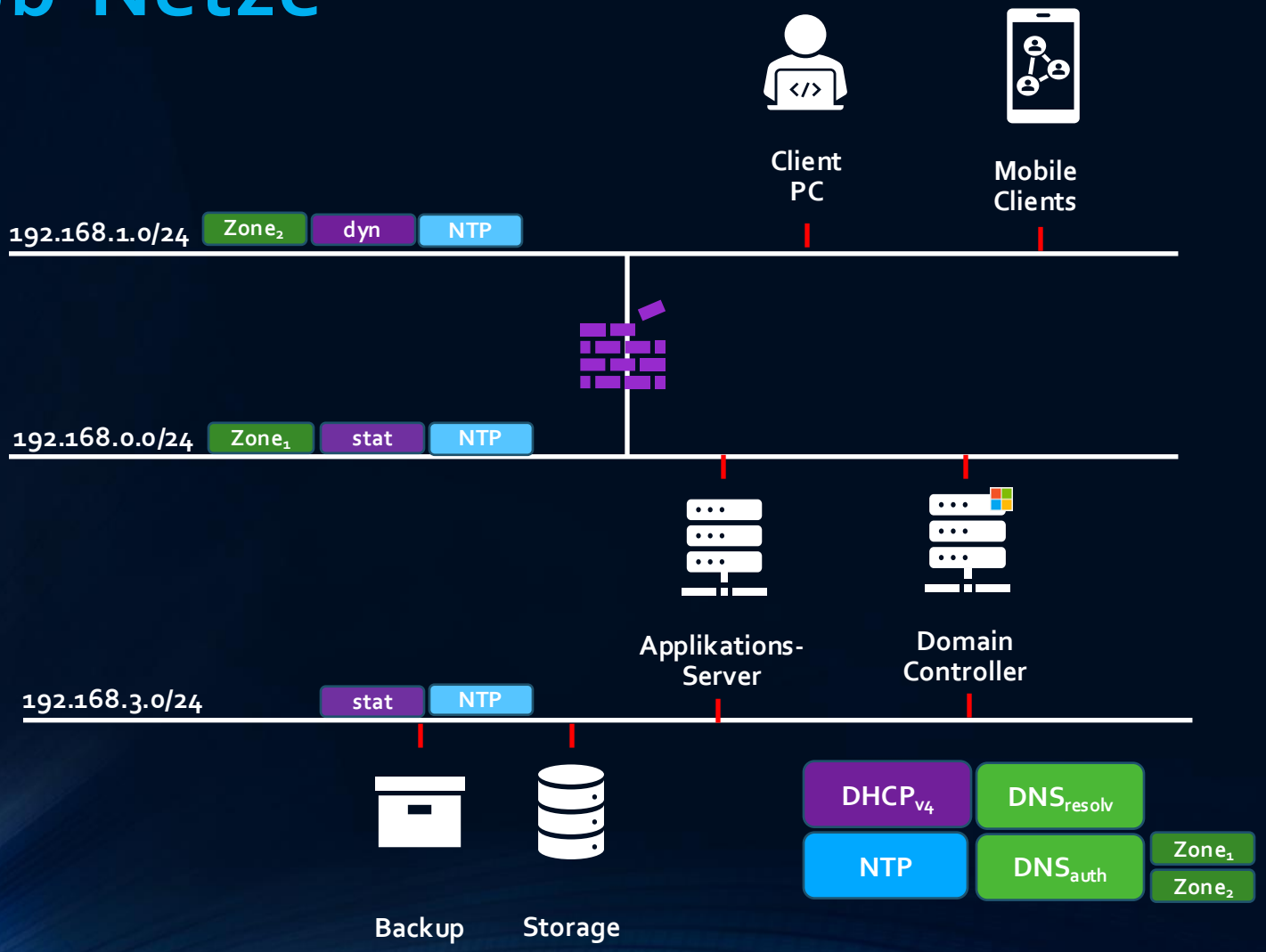
- **Netzwerk-Planung**
  - Netzwerk-Segmentierung (Sub-Netze, VLANs)
  - Routing (NAT)
  - Hosts, VMs, Container, Applikationen
- **DDI (DNS, DHCP, IP-Management)**
  - DHCPv4/DHCPv6+RA vs. statische Zuweisungen
  - authoritative / recursive DNS-Server, Zonen, Views
  - IP-Adressen & Namenskonventionen
- **„Add-ons“**
  - Network-Access Control (NAC) / RADIUS / 802.1x
  - Zeit-Service NTP bzw. NTS

Am Anfang: allles ganz einfach



- Keine Segmentierung
- kein VLANs
- DDI & NTP Services auf Microsoft DC zentralisiert

Sub-Netze



- Einführung von Sub-Netze, VLAN, Firewalls
- statische & dynamische IP-Adressen Verwaltung
- DDI & NTP Services auf Microsoft DC zentralisiert

Fragen, die sich stellen

- **In welchem Sub-Netz benötige ich**
  - Klassifizierung Sub-Netzten: Server vs. Client vs. IoT
  - Dynamische vs. statische IP-Adressen?
  - Dual Stack Aufbau aus IPv4 und IPv6 Adressen
  - authoritative / rekursive DNS-Server, DNS-Zonen Views
- **Welche Systeme verwende ich für DDI & NTP?**
  - wünschenswert: Separate DDI-Instanzen (DHCP, DNS, NTP) in jedem Sub-Netz
  - Separierung der „AD"-Netzwerke hinsichtlich DNS & DHCP
  - zentraler rekursiver DNS-Server für externe Zonen
  - Firewalls als DNS-Forwarder & NTP-Server ?
- **Security**
  - Absicherung durch NAC (RADIUS / 802.1x)

Sub-Netze aus DDI-Sicht betrachtet

- **192.168.0.0/24 "Server & Applikationen"**
  - statische IP-Adressen
  - Namesauflösung von internen, „AD-" und externen DNS-Zonen
  - NTP
- **192.168.1.0/24"Windows Clients"**
  - NAC /RADIUS / 802.x
  - dynamicche IP-Adressen: DHCPv4 / DHCPv6+RA
  - Namesauflösung von internen, „AD"- und externen DNS-Zonen
  - NTP
- **192.168.2.0/24"Backup & Storage"**
  - statische IP-Adressen
  - Namesauflösung von internen Zonen
  - NTP

Transition: Sub-Netze & IP-Adressen

- 1. Sub-Netz "Server & Applikationen"
  - IPv4: 10.128.128.0/24, IPv6: 2001:db8::80:80:/64
  - Sub-Domain: apps.example.com
  - VLAN: 128
- 2. Sub-Netz „Clients"
  - IPv4: 10.128.64.0/24, IPv6: 2001:db8::80:40:/64
  - Sub-Domain: clients.example.com
  - VLAN 64
- 3. Sub-Netz" Storage & Backup"
  - IPv4: 10.128.192.0/24, IPv6: 2001:db8::80:c0:/64
  - Sub-Domain: backup.example.com
  - VLAN 192

IP-Adressen und Namen

- IPv4
  - 10.64.128.0/24,
  - 10.<Standort>.<Sub-Netz>.<Host>

- IPv6
  - 2001:db8::40:80:/64
  - 2001:db8::<Standort>:<Sub-Netz>/64(<Host>)

IP-Adressen und Namen

- **Hostnamen & FQDN**
  - de-cgn01-host001.app.example.com
  - host001.de-cgn01.app.example.com

Design-Regeln aus DDI-Sicht

- immer Dual-Stack IPv4 & IPv6 planen
- IPv6 Stack nie unkonfiguriert lassen, IPv6 ist hexadezimal.
- Sub-Netze nicht numerisch sequentiell aufteilen.
- DDI-Services an den Anfang eines Sub-Netzes stellen.
- Immer Forward & Reverse DNS-Namesauflösung umsetzten.
- Zentralen DNS-Resolver aufbauen, Caching forcieren.
- DNS-Queries kontrollieren (DNS_{53}, DoT, DoH, DoQ)

Design-Regeln aus DDI-Sicht

- NTP-Instanzen in allen Sub-Netzen
- möglichst auf NTS umstellen
- Durchgängige Verwendung von NAC-Authentifizierung im „öffentlichen" Raum (WiFi, Büros, Außengelände, …),
- IoT Geräte: lieber eine schwache Authentifizierung im NAC als gar keine

Netzwerk-Anbindung am Beispiel eines Web-Servers

- **1. Management Netzwerk-Interface**
  - Access Administrative Ebene (SSH, RDP, …)
  - Service Binding: SSH/RDP, DNS-Namensauflösung externe (Internet-Zugriff) & interne Zonen
  - NTP
- **2. Applikations-Netzwerk-Interface**
  - Web-Service (HTTP/HTTPS)
  - Service Bindung: Applikation
- **3. Subnetz" Storage & Backup"**
  - Service Binding iSCSI & Restfull API

Design-Regeln aus DDI-Sicht

- DDI-Instanzen aus unterschiedlichen Security Kontexten nicht „kurzschließen“.
- „Backend“ Sub-Netze für Storage & Managmenet aus unterschiedlichen Security Kontexten nicht „kurzschließen“.
- Appikation-aware Sub-Netze mit dedizieren DDI-Instanzen aufbauen.

Vielen Dank!

OFFEN FÜR FRAGEN & DISKUSSION

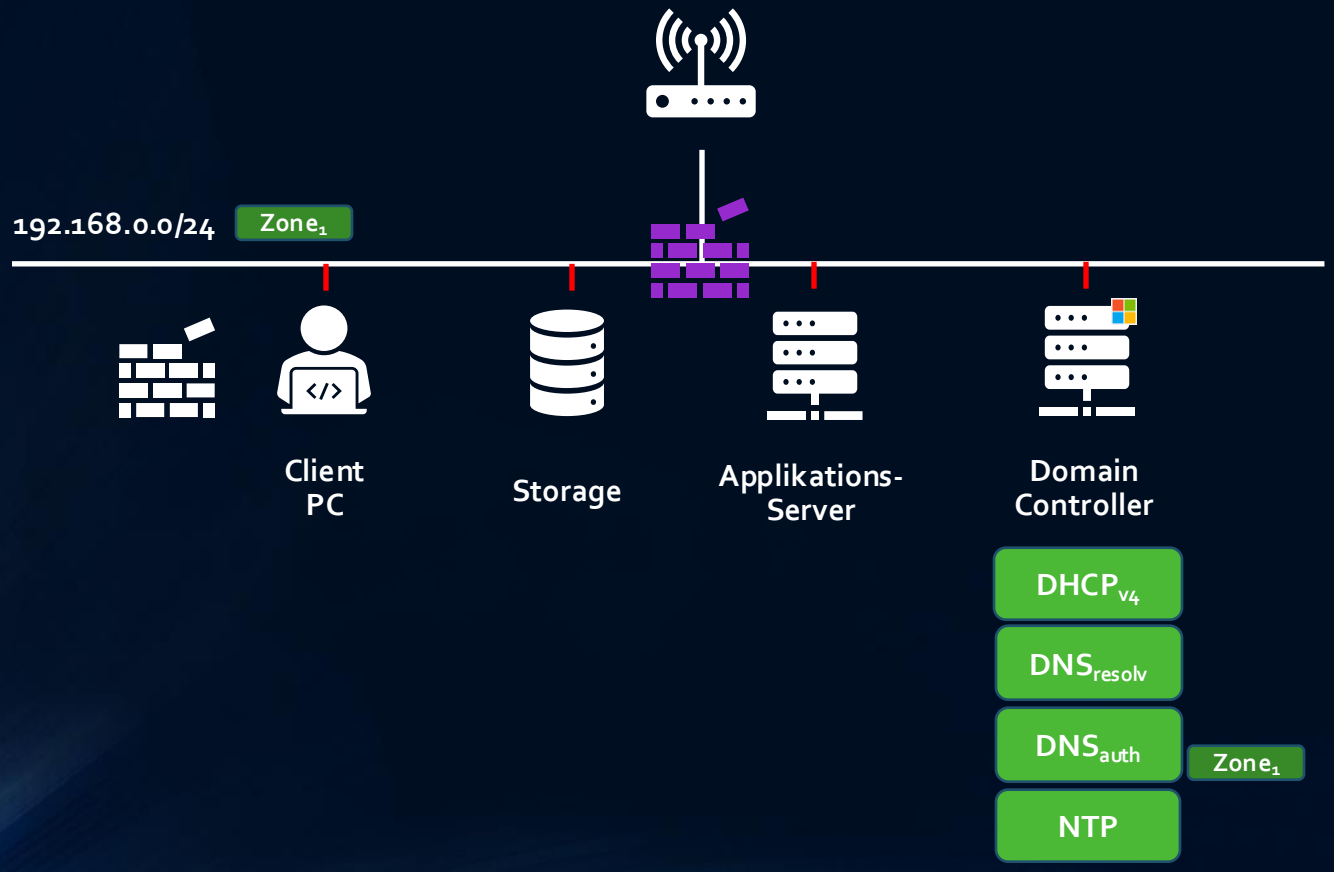
NAC

DHCP$_{v6}$

RA$_{v6}$

Am Anfang

Resolver/
Caching/
Recursive



Mobile Clients

Backup

- 1x Subnet
- kein VLAN
- DDI & NTP auf DC