# Arbeitsbericht

# Syslog Monitoring



Abb¹: Ein Bild zum thema Network Monitoring

Name: Lena-Marie Kaufleitner, Felix Neumayer

Klasse: 4AHITS Fach: ITP2I

Datum: 14.10.2024

 $<sup>^1\</sup>mathrm{Ai}$  Genrated mit DALL:E

# Inhaltsverzeichnis

	0.1	Installation Laborumgebung	2			
	0.2	Netzkonfiguration	2			
	$0.2 \\ 0.3$	Internet testen	3			
	$0.3 \\ 0.4$	Application installing	3			
	0.1	0.4.1 W2K22-2	4			
		0.1.1 W21122 2	1			
1	Net	zkonfiguration	4			
	1.1	Internet testen	5			
	1.2	Application installing	5			
		1.2.1 DNS-Server Intern - Extern - Forwarder	8			
		1.2.2 Öffnen des DNS server Verwaltungsprogramms	8			
		1.2.3 überprüfen der aktuellen DNS einstellungen	8			
		1.2.4 Einrichten des DNS forwarders	8			
		1.2.5 Aufgabe 3: Installation Active Directory Service (inkl. DNS Service) auf W2K22-				
		2	9			
		1.2.6 DNS-Server Intern - Extern - Forwarder	12			
		1.2.7 Öffnen des DNS server Verwaltungsprogramms	12			
		1.2.8 überprüfen der aktuellen DNS einstellungen	12			
		1.2.9 Einrichten des DNS forwarders	12			
2	Net	zkonfiguration	14			
3	Inst	allation von Kiwi Syslog Server auf W2K22-1	14			
4	1 Inbetriebnahme des Cisco Routers 13					
5	5 Inbetriebnahme des Cisco Switches 16					
•	indetriedhamne des Cisco Switches 10					
6	5 Analyse der Syslog-Daten 10					
7	Faz	it	16			

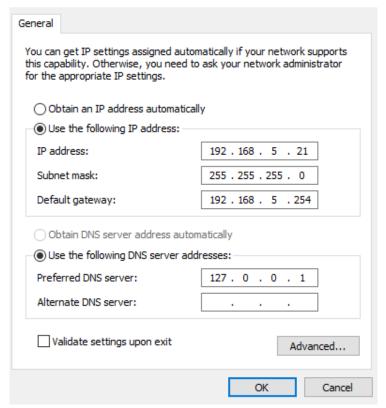
# 0.1 Installation Laborumgebung

#### 0.1.1 W2K22-1

Ich hatte windows VM's vom letzten jahr noch auf meinem eigenen laufwerk gespeichert, deshalb musste ich diese nur öffnen,und die Netzwerkkonfig machen.

## 0.2 Netzkonfiguration

Hostname: W2K22-1
 IP-Adresse: 192.168.5.22
 Gateway: 192.168.5.254
 Arbeitsgruppe: Workgroup



Abb<sup>2</sup>: Netzwerkconfiguration von W2K22-2

#### 0.3 Internet testen

```
Administrator Command Prompt

Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.at

Pinging google.at [142.251.208.99] with 32 bytes of data:
Reply from 142.251.208.99: bytes=32 time=23ms TTL=55
Reply from 142.251.208.99: bytes=32 time=23ms TTL=55
Reply from 142.251.208.99: bytes=32 time=21ms TTL=55
Reply from 142.251.208.99: bytes=32 time=22ms TTL=55
Ping statistics for 142.251.208.99:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 21ms, Maximum = 23ms, Average = 22ms

C:\Users\Administrator>
```

Abb<sup>3</sup>: Beweis der Internetfunktionalitaet.

## 0.4 Application installing

Abb<sup>4</sup>: Screenshot der installierten Applikationen.

<sup>&</sup>lt;sup>2</sup>Screenshot der Netzwerkconfig, Lena-Marie Kaufleitner(07.12.2023)

<sup>&</sup>lt;sup>3</sup>Screenshot der funktionstuechtigkeit der internetconnectivity, Lena-Marie Kaufleitner (07.12.2023)

<sup>&</sup>lt;sup>4</sup>Screenshot der installierten Applikationen, Lena-Marie Kaufleitner(07.12.2023)

### 0.4.1 W2K22-2

# 1 Netzkonfiguration

Hostname: W2K22-2
 IP-Adresse: 192.168.5.22
 Gateway: 192.168.5.254
 Arbeitsgruppe: Workgroup

Internet Protocol Version 4 (TCP/IPv4)	Properties	X		
General				
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.				
Obtain an IP address automatical	ly			
Use the following IP address:				
IP address:	192 . 168 . 5 . 22			
Subnet mask:	255 . 255 . 255 . 0			
Default gateway:	192 . 168 . 5 . 254			
Obtain DNS server address autom	natically			
Use the following DNS server addresses:				
Preferred DNS server:	192 . 168 . 5 . 21			
Alternate DNS server:	127 . 0 . 0 . 1			
☐ Validate settings upon exit	Advanced			
	OK Cance	!		

 ${\rm Abb^5}\colon {\rm Netzwerk configuration}$ von W2K22-2

<sup>&</sup>lt;sup>5</sup>Screenshot der Netzwerkconfig, Lena-Marie Kaufleitner(07.12.2023)

#### 1.1 Internet testen

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator.lab5>ping orf.at

Pinging orf.at [194.232.104.150] with 32 bytes of data:
Reply from 194.232.104.150: bytes=32 time=7ms TTL=53
Reply from 194.232.104.150: bytes=32 time=6ms TTL=53
Reply from 194.232.104.150: bytes=32 time=7ms TTL=53
Reply from 194.232.104.150: bytes=32 time=6ms TTL=53
Reply from 194.232.104.150: bytes=32 time=6ms TTL=53

Ping statistics for 194.232.104.150:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 7ms, Average = 6ms

C:\Users\Administrator.lab5>_
```

Abb<sup>6</sup>: Beweis der Internetfunktionalitaet.

### 1.2 Application installing

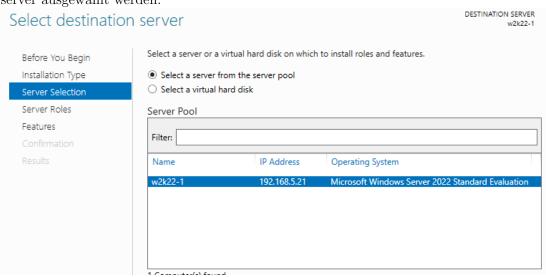
Abb<sup>7</sup>: Screenshot der installierten Applikationen.

Der vHost W2K22-1 muss zu einer der beiden Domänencontroller in der Windows Domäne werden. Dazu mussen auf diesem System weitere Windows Rollen hinzugefügt werden.

Als erstes muss ein neuer DNS server angegeben werden (192.168.5.21) anstatt des vorherigen cloudflare DNS servers.

Im server manager gibt es den Punkt ,, add roles and features". Dieser muss ausgewählt werden und schon geht es los.

Als erstes kommt man zu der Seite: ", select destination server". Hier muss einfach nur der W2K22-1 server ausgewählt werden.



Abb<sup>8</sup>:Screenshot des Konfigurationsschrittes: Select Destination Server

<sup>&</sup>lt;sup>6</sup>Screenshot der funktionstuechtigkeit der internetconnectivity, Lena-Marie Kaufleitner(07.12.2023)

<sup>&</sup>lt;sup>7</sup>Screenshot der installierten Applikationen, Lena-Marie Kaufleitner(07.12.2023)

 $<sup>^{8}</sup>$ Lena-Marie Kaufleitner (18.1.2024)

Als nächstes kommt man zu der Seite: ", select server role". Hier muss die Option ", Active Directory Domain Services" ausgewählt werden.

Select server roles				
Before You Begin Installation Type	Select one or more roles to install on the selected server.  Roles			
Server Selection Server Roles				
Features AD DS Confirmation Results	Active Directory Foliant Services  Active Directory Federation Services  Active Directory Lightweight Directory Services  Active Directory Rights Management Services  Device Health Attestation  DHCP Server  DNS Server  Fax Server  File and Storage Services (1 of 12 installed)  Host Guardian Service  Hyper-V  Network Policy and Access Services  Print and Document Services  Remote Access  Remote Access			

Abb<sup>9</sup>:Screenshot des Konfigurationsschrittes: Select Server role

Als nächstes kommt man zu der Seite: "Add Features that are required". Hier kann man einige tolle features hinzufügen die man gebrauchen könnte. Wir haben telnet noch extra aktiviert, da das ganz praktisch sein könnte.

Als nächsten schritt, muss man im server manager auf die kleine graue flagge oben links gehen. Dort sieht man(ziemlich versteckt) die Option: "Post-Deployment Configuration — Promote this server to a domain controller".

An diesem Punkt bekommt man die seite "Deployment Configuration" angezeigt. Dort wählt man den punkt " Add a new Forest" und gibt als Root domain name "lab5.local" an.

Die nächste seite ist die "Domain Controller Options" site. Dort muss man einige dinge konfigurieren.

Forest functional Level - Windows Server 2021

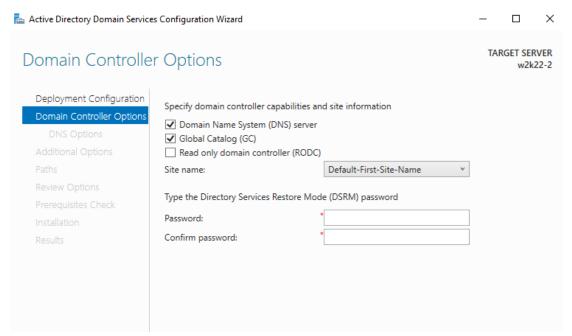
Domain functional Level - Windows Server 2021

Domain Name System (DNS) server bleibt bei default Einstellungen

Global Catalog (GC) bleibt bei default Einstellungen

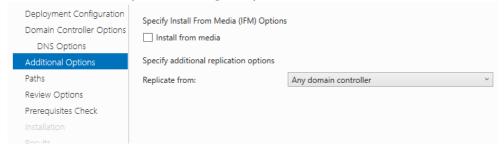
In den beiden Passwortfeldern unser default passwort "Win#Sys#admin10" eingeben.

<sup>&</sup>lt;sup>9</sup>Lena-Marie Kaufleitner(18.1.2024)



Abb<sup>10</sup>:Screenshot des Konfigurationsschrittes: Domain Controller Options

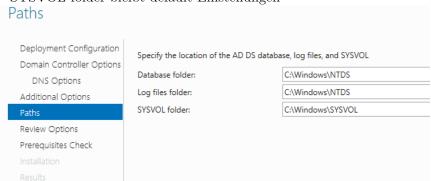
Im nächsten Schritt(Additional Options) NetBIOS Domain Name auf lab5 setzen.



Abb<sup>11</sup>:Screenshot des Konfigurationsschrittes: Additional Options

#### Im schritt Paths:

- Database folder bleibt default Einstellungen
- Log files folder bleibt default Einstellungen
- SYSVOL folder bleibt default Einstellungen



Abb<sup>12</sup>:Screenshot des Konfigurationsschrittes: Paths

 $<sup>^{10}</sup>$ Lena-Marie Kaufleitner (18.1.2024)

<sup>&</sup>lt;sup>11</sup>Lena-Marie Kaufleitner(18.1.2024)

<sup>&</sup>lt;sup>12</sup>Lena-Marie Kaufleitner (18.1.2024)

Nun den Installationsprozess starten und den server retstarten.

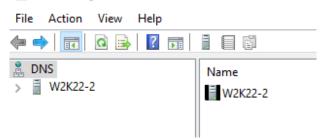
#### 1.2.1 DNS-Server Intern - Extern - Forwarder

### 1.2.2 Öffnen des DNS server Verwaltungsprogramms

Auf Tools im oberen Bereich klicken, und bei der Dopdownliste "DNS" auswaehlen.

#### 1.2.3 überprüfen der aktuellen DNS einstellungen

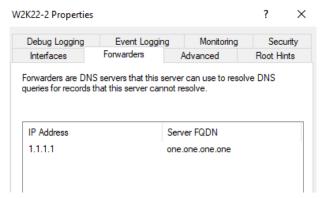
im DNS server, den Server (W2K22-1)erweitern um die vorhandenen Zonen und einstellungen zu sehen.  $$\stackrel{\bullet}{\mathbb{R}}$$  DNS Manager



Abb<sup>13</sup>:Screenshot des Schrittes: überprüfen der aktuellen DNS einstellungen

#### 1.2.4 Einrichten des DNS forwarders

- 1. Rechtsklicken auf den servernamen und eigenschaften waehlen.
- 2. Zum Tab forwarders wechseln.
- 3. Auf bearbeiten klicken.
- 4. IP adresse des externen DNS servers eingeben
- 5. Forwarder speichern



Abb<sup>14</sup>:Screenshot des Schrittes: Einrichten des DNS forwarders

 $<sup>^{13}</sup>$ Lena-Marie Kaufleitner (18.1.2024)

 $<sup>^{14}</sup>$ Lena-Marie Kaufleitner (18.1.2024)

Dieser Befehl hilft zu überprüfen, ob der DNS-Server Anfragen korrekt an Cloudflare weiterleitet und auflöst

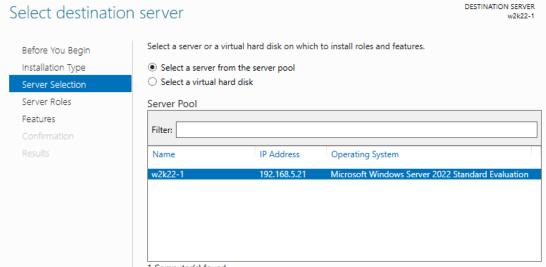
Abb<sup>15</sup>:Bestaetigung duch nslookup

# 1.2.5 Aufgabe 3: Installation Active Directory Service (inkl. DNS Service) auf W2K22-2

Der vHost W2K22-1 soll zu einem der beiden Domänencontroller in unserer Windows-Domäne werden. Dafür müssen wir auf diesem System zusätzliche Windows-Rollen hinzufügen. Als Erstes müssen wir den DNS-Server auf die IP-Adresse 192.168.5.21 ändern, anstatt des vorherigen Cloudflare DNS-Servers.

Als erstes Öffnet man den Server-Manager und wählt die Option Rollen und Features hinzufügenäus

Danach Wählt man auf der Seite ßelect destination serveëinfach unseren Server "W2K22-2" aus



Abb<sup>16</sup>:Screenshot des Konfigurationsschrittes: Select Destination Server (hatte keinen screenshot der W2K22-2)

Als nächstes kommt man zu der Seite: ", select server role". Hier muss die Option ", Active Directory Domain Services" ausgewählt werden.

<sup>&</sup>lt;sup>15</sup>Lena-Marie Kaufleitner(18.1.2024)

 $<sup>^{16}\</sup>mathrm{Lena\text{-}Marie\ Kaufleitner}(18.1.2024)$ 

Select server roles				
Before You Begin Installation Type Server Selection	Select one or more roles to install on the selected server.  Roles			
	Active Directory Certificate Services			
Server Roles	✓ Active Directory Domain Services  Active Directory Federation Services			
Features	Active Directory Federation Services  Active Directory Lightweight Directory Services			
AD DS	Active Directory Rights Management Services			
Confirmation	☐ Device Health Attestation ☐ DHCP Server			
Results	☐ DNS Server			
	Fax Server			
	▶ ■ File and Storage Services (1 of 12 installed)			
	Host Guardian Service			
	☐ Hyper-V			
	Network Policy and Access Services			
	Print and Document Services			
	Remote Access			

Abb<sup>17</sup>:Screenshot des Konfigurationsschrittes: Select Server role

Auf der Seite "Add Features that are required" kann man einige zusätzliche Features hinzufügen, die wir eventuell benötigen könnten. Wir haben auch Telnet aktiviert, falls das praktisch sein sollte.

Im nächsten Schritt gehe im Server-Manager zum kleinen grauen Menü oben links. Dort findest du die Option Post-Deployment Configuration – Promote this server to a domain controller".

An diesem Punkt wird man zur Seite "Deployment Configuration" weitergeleitet. Wählt die die Option "Add a domain controller to an existing domain" und geben Sie als Existing domain "lab5.local" ein.

Auf der Seite "Domain Controller Options" muss man einige Einstellungen vornehmen:

Forest functional Level - Windows Server 2021

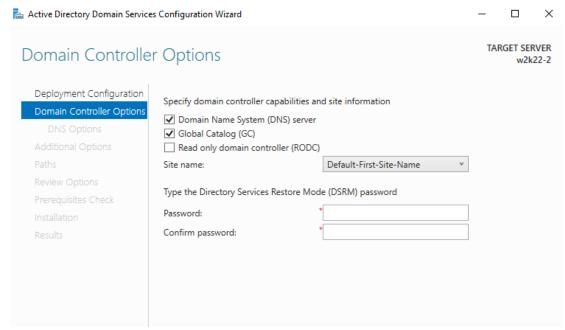
Domain functional Level - Windows Server 2021

Domain Name System (DNS) server bleibt bei default Einstellungen

Global Catalog (GC) bleibt bei default Einstellungen

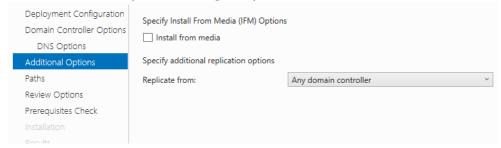
In den beiden Passwortfeldern unser default passwort "Win#Sys#admin10" eingeben.

<sup>&</sup>lt;sup>17</sup>Lena-Marie Kaufleitner(18.1.2024)



Abb<sup>18</sup>:Screenshot des Konfigurationsschrittes: Domain Controller Options

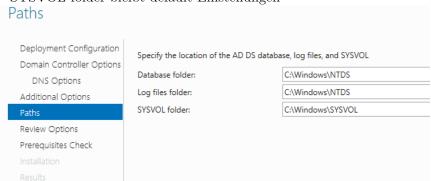
Im nächsten Schritt(Additional Options) NetBIOS Domain Name auf lab5 setzen.



Abb<sup>19</sup>:Screenshot des Konfigurationsschrittes: Additional Options

#### Im schritt Paths:

- Database folder bleibt default Einstellungen
- Log files folder bleibt default Einstellungen
- SYSVOL folder bleibt default Einstellungen



Abb<sup>20</sup>:Screenshot des Konfigurationsschrittes: Paths

 $<sup>^{18}</sup>$ Lena-Marie Kaufleitner (18.1.2024)

<sup>&</sup>lt;sup>19</sup>Lena-Marie Kaufleitner (18.1.2024)

<sup>&</sup>lt;sup>20</sup>Lena-Marie Kaufleitner (18.1.2024)

Nun den Installationsprozess starten und den server restarten.

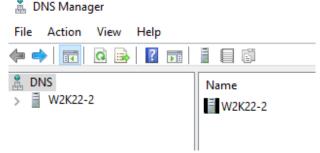
#### 1.2.6 DNS-Server Intern - Extern - Forwarder

## 1.2.7 Öffnen des DNS server Verwaltungsprogramms

Das DNS-Server-Verwaltungsprogramm wird geöffnet, indem oben auf "Tools" geklickt wird und in der Dropdown-Liste "DNS" ausgewählt wird.

#### 1.2.8 überprüfen der aktuellen DNS einstellungen

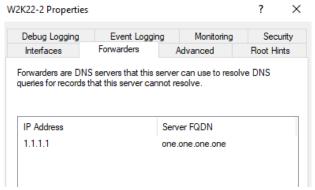
Die aktuellen DNS-Einstellungen werden im DNS-Server überprüft, indem der Server (W2K22-2) erweitert wird, um die vorhandenen Zonen und Einstellungen anzuzeigen



Abb<sup>21</sup>:Screenshot des Schrittes: überprüfen der aktuellen DNS einstellungen

#### 1.2.9 Einrichten des DNS forwarders

Der DNS-Forwarder wird eingerichtet, indem der Servername mit der rechten Maustaste angeklickt und Eigenschaftenäusgewählt wird. Dann wird zum Tab "Forwarders" gewechselt und auf "Bearbeiten" geklickt. Anschließend wird die IP-Adresse des externen DNS-Servers eingegeben und der Forwarder gespeichert.



Abb<sup>22</sup>:Screenshot des Schrittes: Einrichten des DNS forwarders

<sup>&</sup>lt;sup>21</sup>Lena-Marie Kaufleitner(18.1.2024)

 $<sup>^{22}\</sup>mathrm{Lena\text{-}Marie\ Kaufleitner}(18.1.2024)$ 

Dieser Befehl und auflöst	hilft zu überpr	üfen, ob der D	NS-Server An	fragen korrekt	an Cloudflare	weiterleitet
und aunost						

# 2 Netzkonfiguration

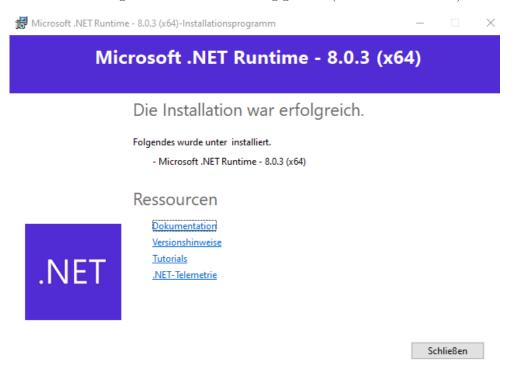
Die Netzwerkkonfiguration wurde wie folgt durchgeführt:

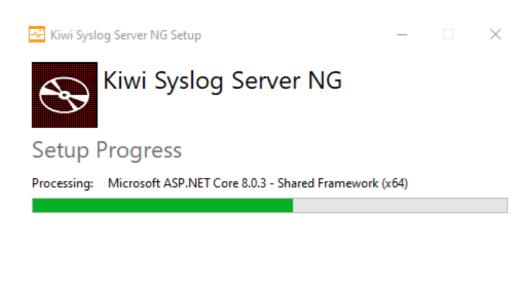
- Router und Switch wurden mit statischen IPs konfiguriert.
- Der Syslog-Server wurde auf Windows Server 2022 installiert.
- Das Logging wurde so eingerichtet, dass alle wichtigen Ereignisse erfasst werden.

# 3 Installation von Kiwi Syslog Server auf W2K22-1

Um den Kiwi Syslog Server zu nutzen, haben wir folgende Schritte durchgeführt:

- Registrierung eines SolarWinds-Accounts zur Nutzung der 14-tägigen Testlizenz.
- Download des Installers von der offiziellen SolarWinds-Website.
- Installation des Programms inklusive Abhängigkeiten (z.B. .NET Runtime).





### 4 Inbetriebnahme des Cisco Routers

Der Router wurde eingerichtet, um Syslog-Nachrichten an den Server zu senden. Die benötigten Konfigurationsbefehle lauten:

Cancel

logging enable
logging host <IP-Adresse>
logging trap debugging
service timestamps log datetime msec
write memory

Die Log-Level reichen von 0 bis 7, wobei für unser Experiment Level 7 (Debugging) gewählt wurde, um möglichst viele Informationen zu sammeln.

Level	Beschreibung
0	Emergencies
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging

Tabelle 1: Syslog Trap-Level

### 5 Inbetriebnahme des Cisco Switches

Die Konfiguration des Switches verlief analog zum Router. Die notwendigen Befehle lauten:

logging enable
logging host <IP-Adresse>
logging trap debugging
service timestamps log datetime msec
write memory

# 6 Analyse der Syslog-Daten

Nach erfolgreicher Einrichtung wurden die ersten Syslog-Nachrichten auf dem Dashboard sichtbar. Da jedoch nur zwei Geräte aktiv Logs sendeten, war die Datenmenge begrenzt. Ein zusätzlicher Datensatz wurde durch das Logging des HTL-Braunau-Netzwerks generiert. Aufgrund technischer Probleme mit der virtuellen Maschine und der Lizenzdauer konnten jedoch nur die letzten 30 Minuten der Vorwoche analysiert werden.

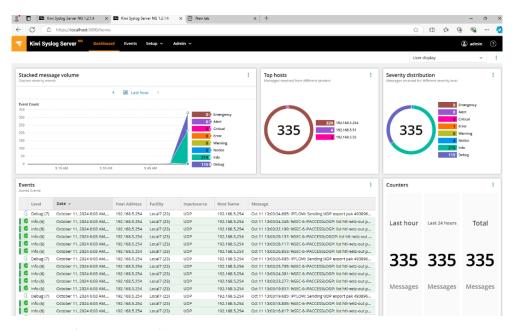


Abbildung 1: Syslog-Dashboard mit eingehenden Meldungen

### 7 Fazit

Das Experiment zeigte, dass ein zentralisierter Syslog-Server eine wertvolle Ressource zur Netzwerküberwachung darstellt. Dennoch sind einige Punkte zu beachten:

- Begrenzte Log-Daten durch geringe Anzahl an Netzwerkgeräten.
- Technische Einschränkungen durch Virtualisierung und Lizenzdauer.
- Erweiterung des Versuchs mit mehreren Geräten wäre sinnvoll.