Universität Rostock

Traditio et Innovatio

Service- and Security Monitoring

Auswertung, Konsolidierung, Korrelierung und Visualisierung IT-Sicherheitskritischer Ereignisse

Martin Steinbach
Universität Rostock, Institut für Informatik

Seminar Sommersemester 2018
Auswertung und Visualisierung komplexer Daten

Struktur

Struktur

Struktur

Einführung
- Warum Überwachung?
- Überwachungsformen

Aktives Monitoring
- Was kann überwacht werden

Passives Monitoring
- Netzwerkanalyse
- Logkorrelation in Cloud-Umgebungen

DEMO
- (Icinga2: aktives Monitoring)
- ELK-Stack: passives Monitoring

Struktur

Einführung
- Warum Überwachung?
- Überwachungsformen

Aktives Monitoring
- Was kann überwacht werden

Passives Monitoring
- Netzwerkanalyse
- Logkorrelation in Cloud-Umgebungen

DEMO
- (Icinga2: aktives Monitoring)
- ELK-Stack: passives Monitoring

Warum Überwachung?

Servicemonitoring = Securitymonitoring?

Ziele der Informationssicherheit

- Vertraulichkeit
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit**

Betrachtungen

- Zeitliche Perspektive
- Schweregrad (severity)
- Quelle
- Ereigniskorrelation

Ziele der Informationssicherheit

- Vertraulichkeit
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit**

Betrachtungen

- Zeitliche Perspektive
- Schweregrad (severity)
- Quelle
- Ereigniskorrelation

Ziele der Informationssicherheit

- Vertraulichkeit
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit**

Betrachtungen

- Zeitliche Perspektive
- Schweregrad (severity)
- Quelle
- Ereigniskorrelation

Warum Überwachung?

Schaden identifizieren und vermeiden

- 90% aller Firmen: Opfer von Cyberattacken
- 80% derer mit finanziellen Einbußen
- Diebstahl geistigen Eigentums (zwischen 2011 und 2015 Verdopplung)

Servicemonitoring = Securitymonitoring?

Ja!?

Nur ein unmanipulierter Dienst, der erwiesenermaßen seine Aufgaben erfüllt, hält die Ziele der IT-Sicherheit ein.

Beweis durch Überwachung

- Unerwartetes Verhalten
- Erreichbarkeit
- Angriffserkennung
- Nachvollziebarkeit

Servicemonitoring = Securitymonitoring?

Ja!?

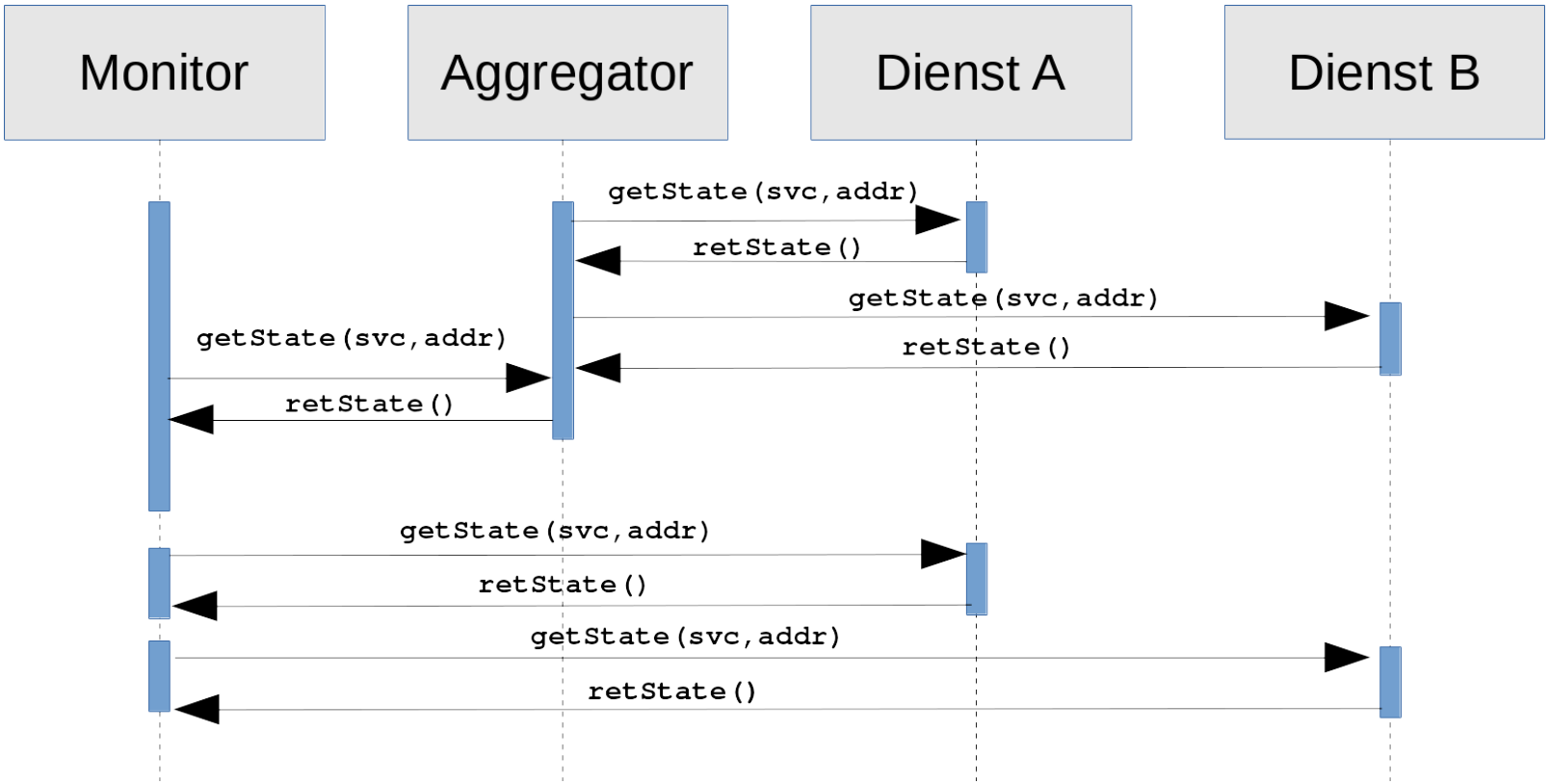
Nur ein unmanipulierter Dienst, der erwiesenermaßen seine Aufgaben erfüllt, hält die Ziele der IT-Sicherheit ein.

Beweis durch Überwachung

- Unerwartetes Verhalten
- Erreichbarkeit
- Angriffserkennung
- Nachvollziebarkeit

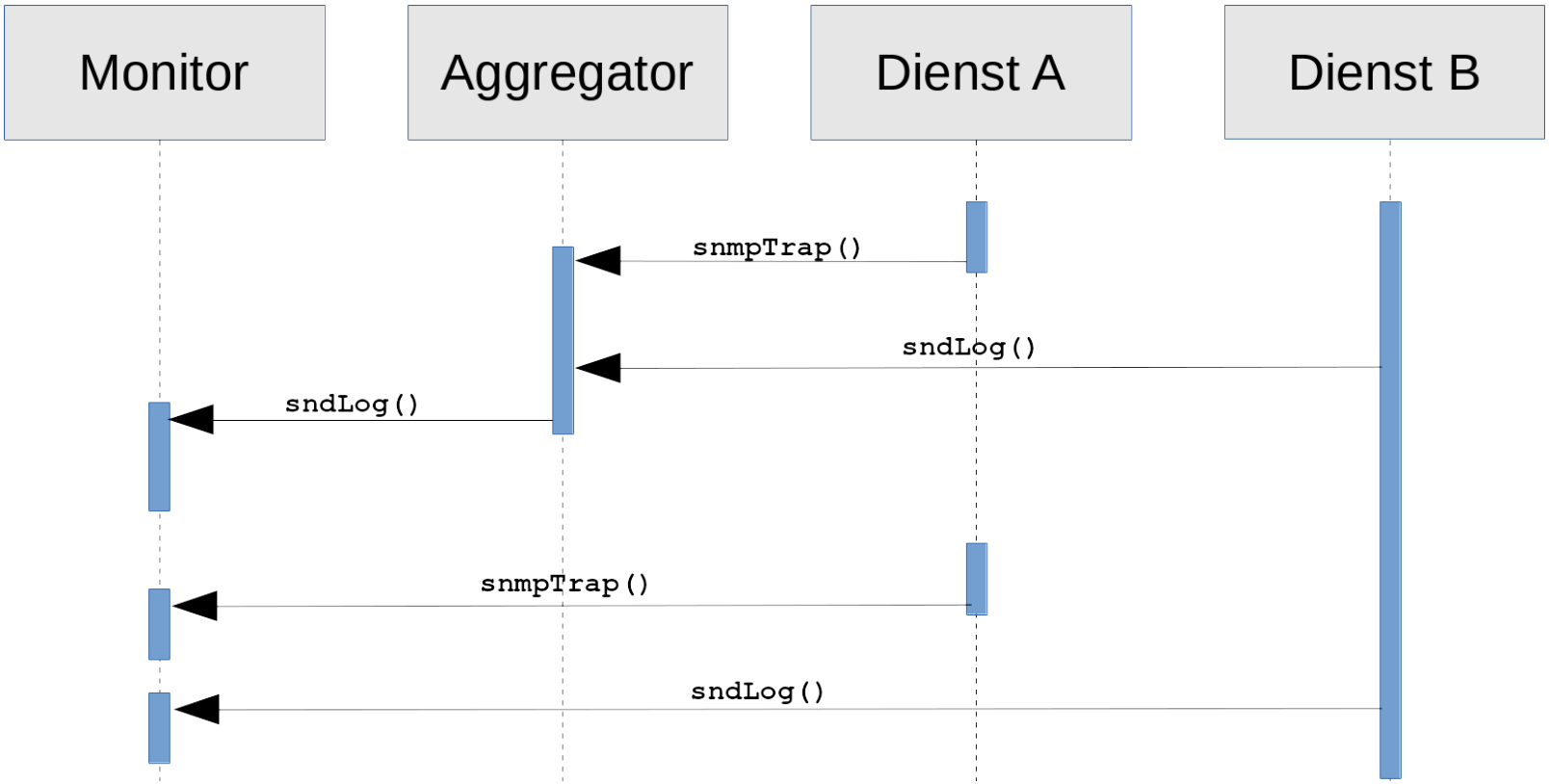
Aktive Überwachung

Beispiel Sequenzdiagramm



Passive Überwachung

Beispiel Sequenzdiagramm



Aktive Überwachung

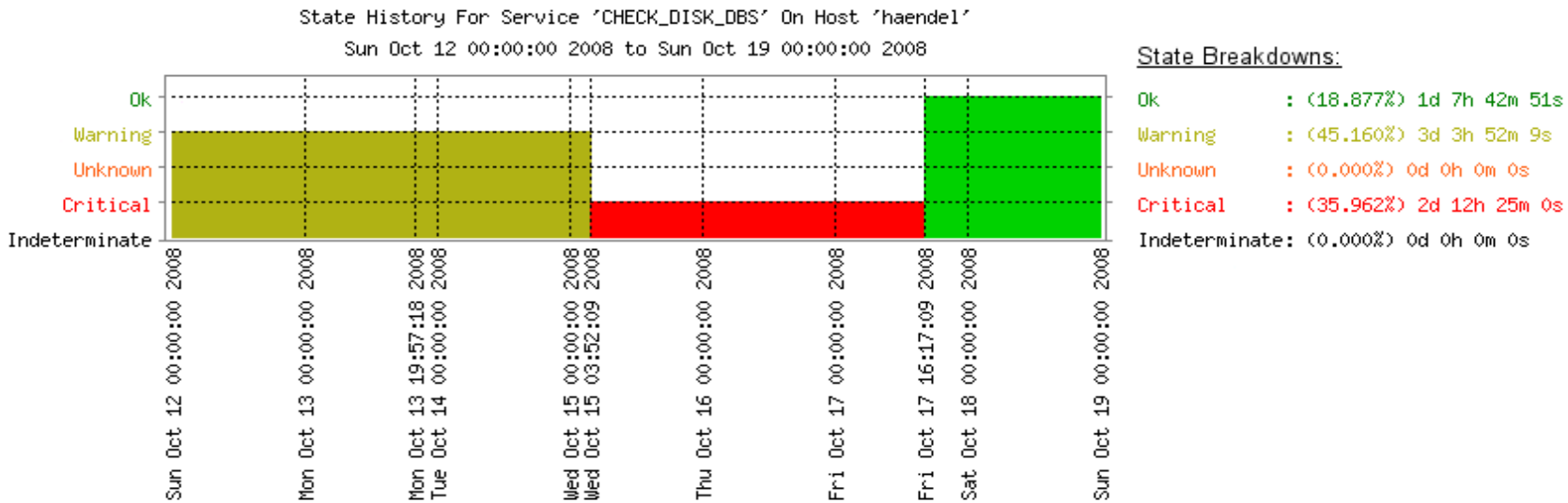
Was kann überwacht werden?

Jede Entität, deren Status deutlich zueinander abgrenzbar sind.

- Betriebsystemabhängig
  - Betriebsystemparameter
    - Auslastung
    - Speicher
    - Prozesse
    - Datendurchsatz
  - Updates
  - Sicherheitsauditierung

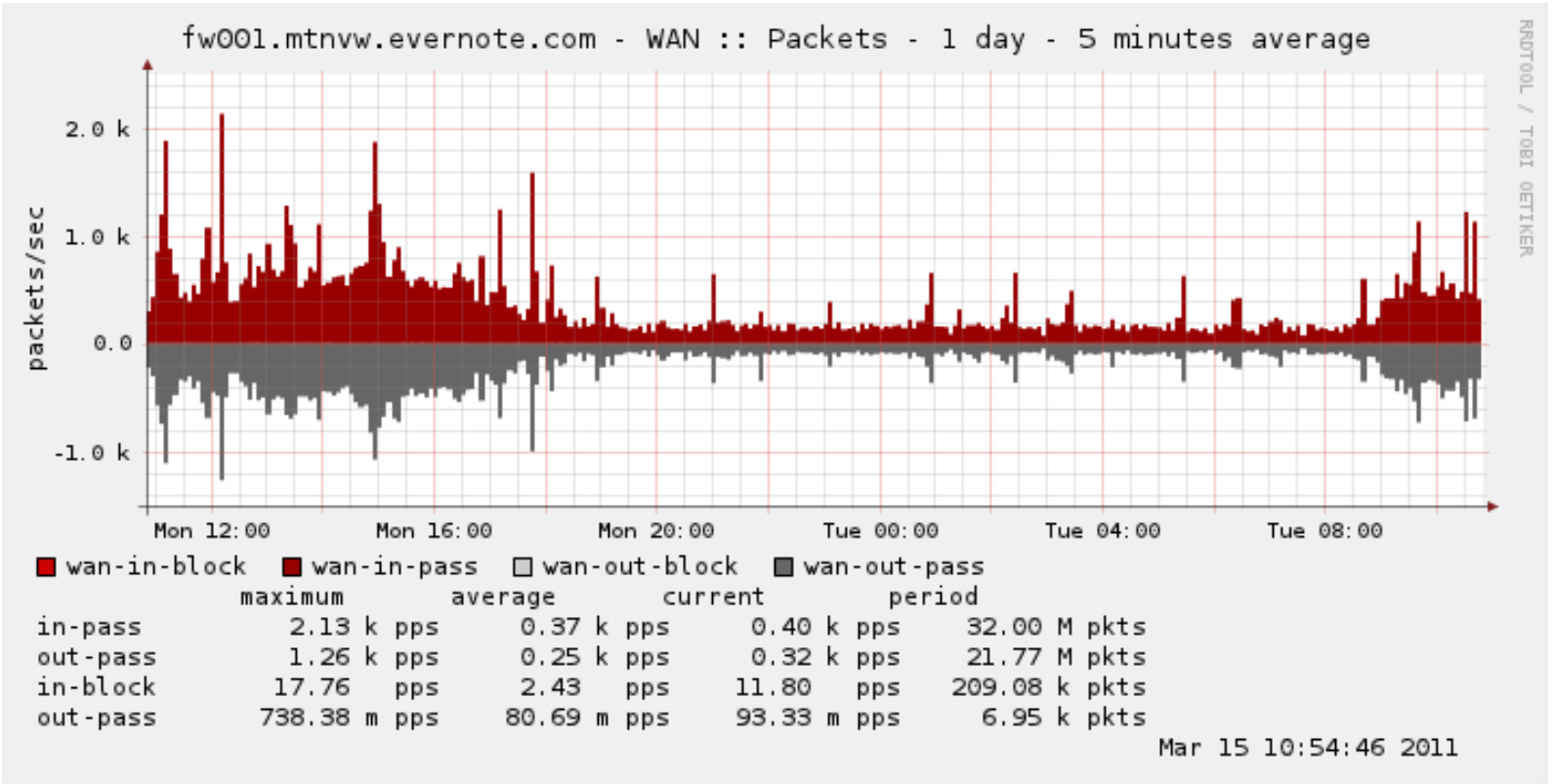
- Betriebsystemunabhängig
  - Netzwerkdienste
    - L3: ICMP{4,6}
    - L4: TCP, UDP - basierend
    - L4+: SNMP
  - Sensoren
  - Aktive Netzwerkkomponenten

Visualisierungen
Statusverlauf



Quelle: selbst erstellt
Erstellt mit: NagVis

Visualisierungen
packets/time



Quelle: https://redmine.pfsense.org/issues/1354
Erstellt mit: https://oss.oetiker.ch/rrdtool/

scanning detection systems

- Trafficanalyse zu ungenau
- Erstellung eines *fingerprints* kaum möglich

Verkehrskorrelation durch statistische Verfahren

- Scans werden zeitlich korreliert
- Scan-Traffic zuordnung zu Scan-Technik

cloud

- Stark steigende Systemanzahl (10K+)
- In wenigen Sekunden: virtuelles RZ
- Dynamisch wachsendes/sinkendes Logaufkommen
- Dynamische Kosten
- Proprietäre, inkompatible Monitoringsysteme [a]

[a] IETF-draft: *Syslog Extension for Cloud Using Syslog Structured Data*

Anforderungen Logkorrelation

- Manuell undurchführbar
- Skalierbar (n+1)
- Automatisch durchführbar
- Minimierung des Speicheraufwandes

cloud

- Stark steigende Systemanzahl (10K+)
- In wenigen Sekunden: virtuelles RZ
- Dynamisch wachsendes/sinkendes Logaufkommen
- Dynamische Kosten
- Proprietäre, inkompatible Monitoringsysteme [a]

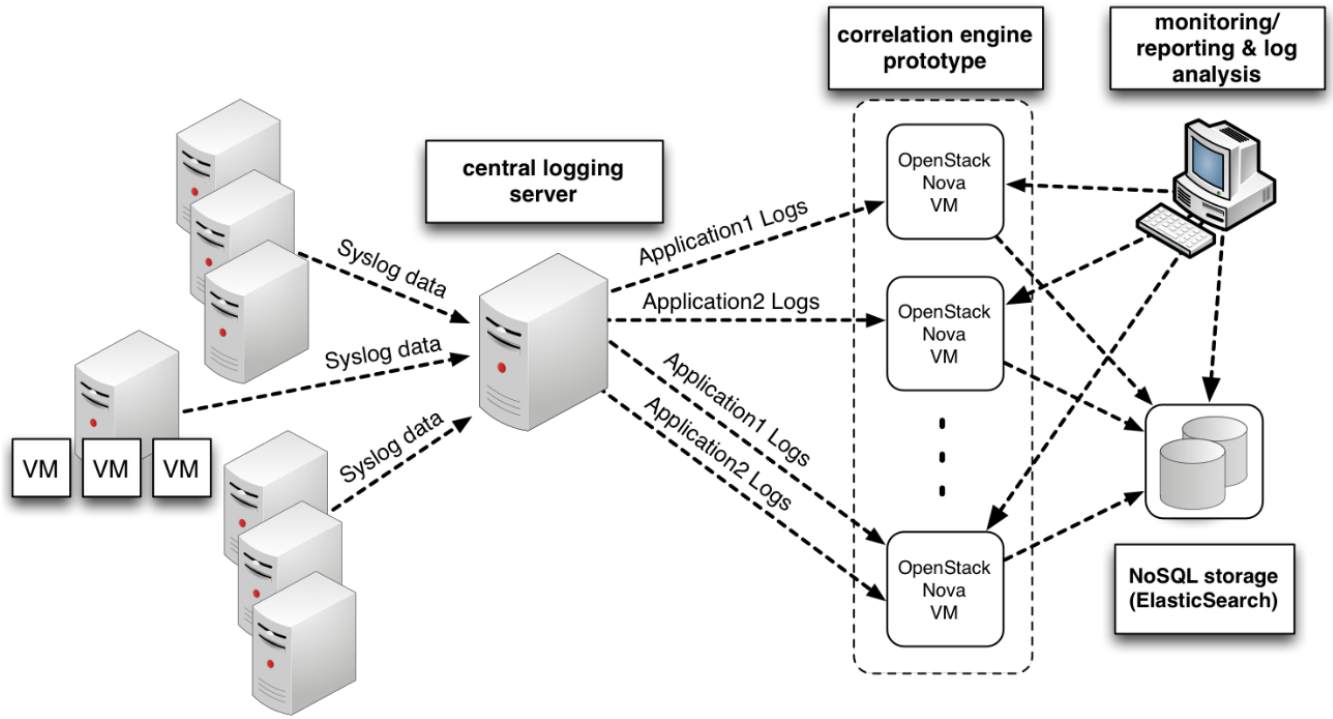
[a] IETF-draft: *Syslog Extension for Cloud Using Syslog Structured Data*

Anforderungen Logkorrelation

- Manuell undurchführbar
- Skalierbar (n+1)
- Automatisch durchführbar
- Minimierung des Speicheraufwandes

Prototyp JCorrelat

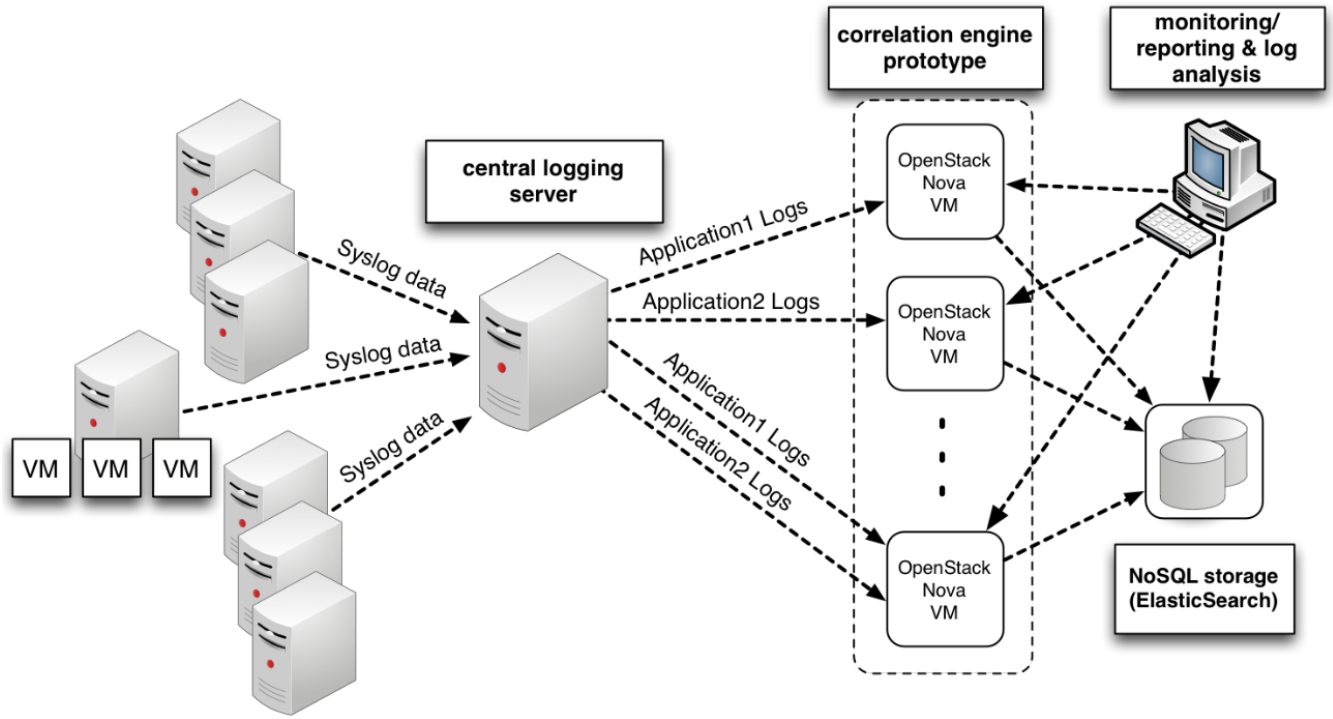
Schema



Quelle: D.Frisch ,C. Pape, S. Reissmann, and S. Rieger “Correlation and Consolidation of Distributed Logging Data in Enterprise Clouds” In International Journal on Advances in Internet Technology, vol 7 , 2013, pp. 39–51.

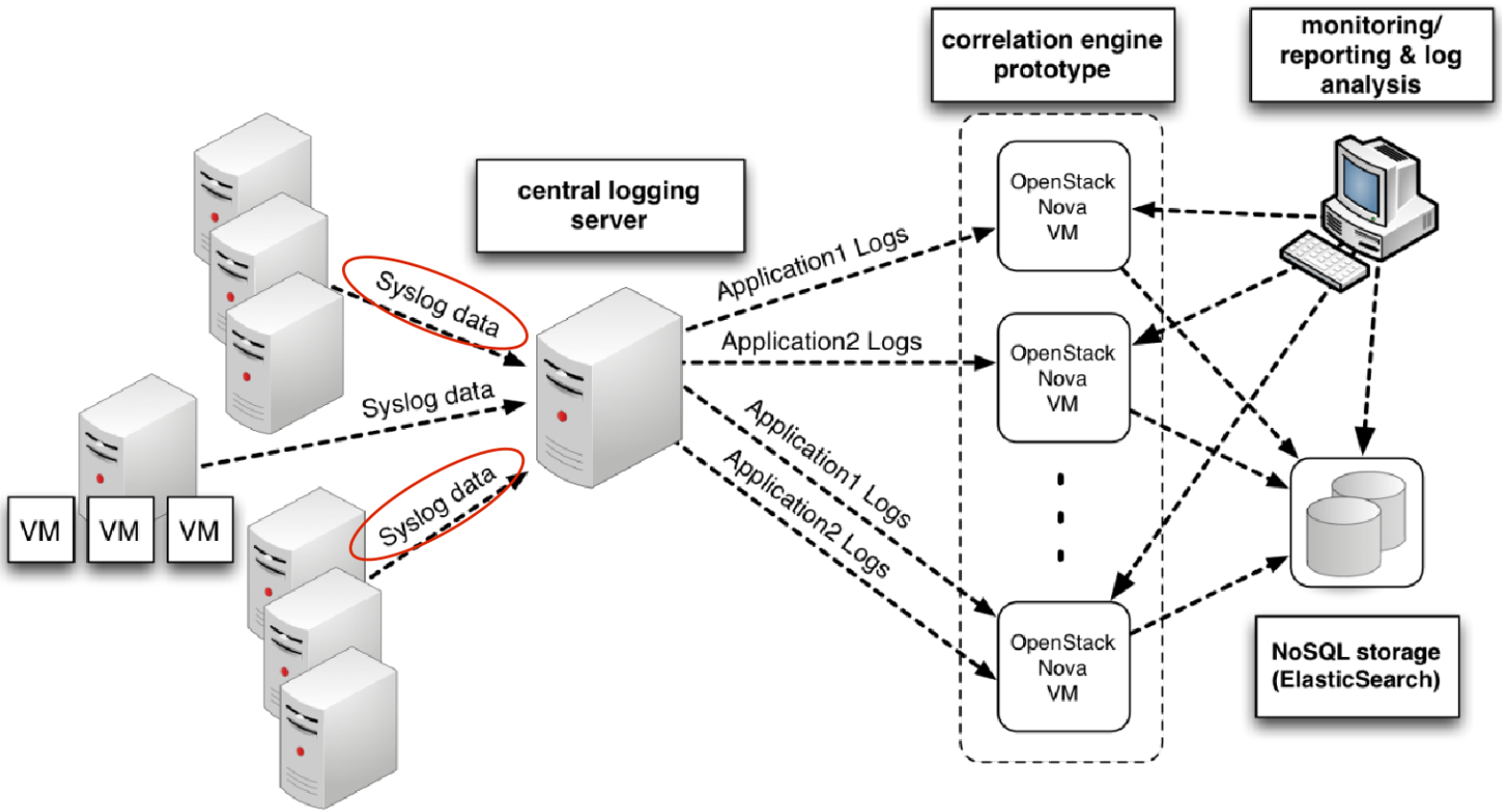
Prototyp JCorrelat

Schema



Quelle: D.Frisch ,C. Pape, S. Reissmann, and S. Rieger “Correlation and Consolidation of Distributed Logging Data in Enterprise Clouds” In International Journal on Advances in Internet Technology, vol 7 , 2013, pp. 39–51.

Syslog
Aufbau RFC 3164



Feld	Inhalt	Beispiel
PRI		
facility	*int* ∈ 0..23	<**3**4>
severity	*int* ∈ 0..7	<3**4**>
HEADER		
timestamp	mm dd hh:mm:ss	`Oct 11 22:14:15`
hostname	string	`mymachine`
MSG		
tag	string	`su:`
content	string	`'su root' failed ...`

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick
on /dev/pts/8
```

RFC5425 Implementiert durch syslog-ng und rsyslog

Feld	Inhalt	Beispiel
HEADER		
facility	*int* $\in$ 0..23	<**16**5>
severity	*int* $\in$ 0..7	<16**5**>
timestamp	RFC3339	2003-10-11T22:14:15.003Z
hostname	string	mymachine.example.com
MSG		
tag	string	su:
content	string	'su root' failed ...

```
<165> 2003-10-11T22:14:15.003Z mymachine.example.com
evntslog - ID47 [exampleSDID@32473 iut="3" eventSource=
"Application" eventID="1011"] BOMAn application
event log entry...
```

Einführung
- Warum Überwachung?
- Überwachungsformen

Aktives Monitoring
- Was kann überwacht werden

Passives Monitoring
- Netzwerkanalyse
- Logkorrelation in Cloud-Umgebungen

DEMO
- (Icinga2: aktives Monitoring)
- ELK-Stack: passives Monitoring

There Is No Largest Prime Number

There Is No Largest Prime Number