Distributed Monitoring

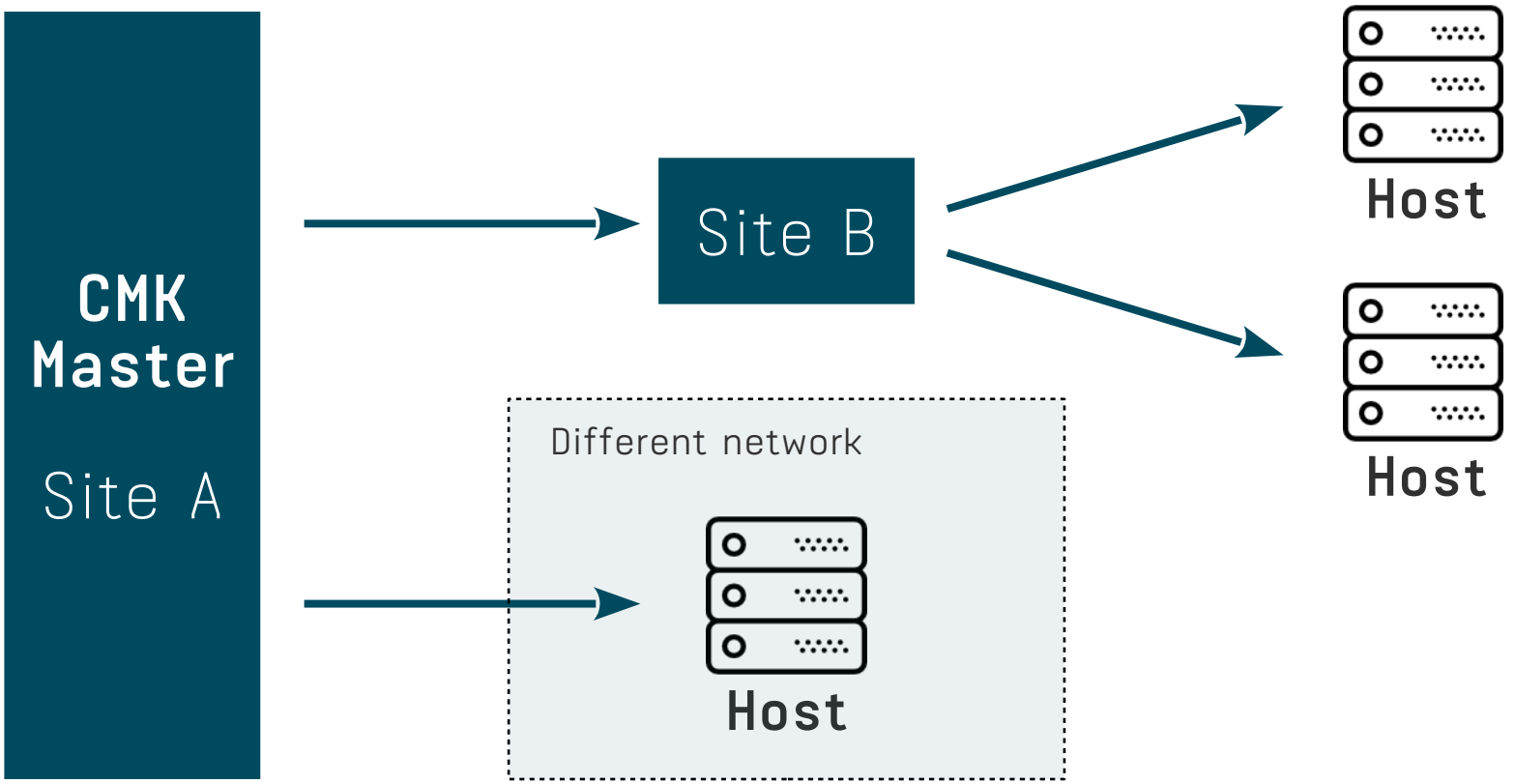
Which method suits my project?

04.05.2018, Marcel Arentz

Check_MK Conference #4

CONFERENCE
MUNICH 2018/5/2-4
#4

What's meant by Distributed Monitoring?



Accessing hosts vs. Accessing sites

When do I need Distributed Monitoring...

Geography

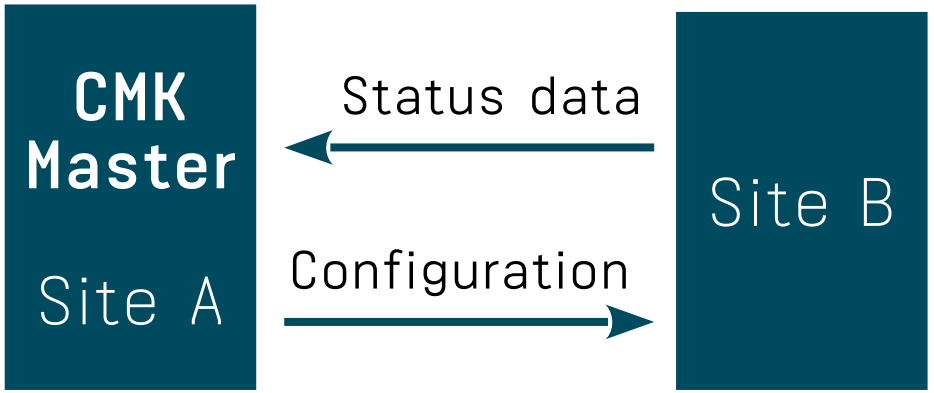
Organisation

Network

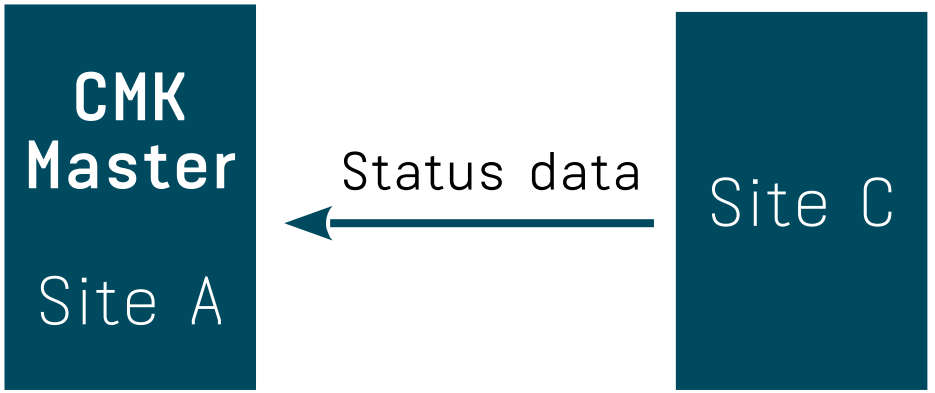
Performance

… and which concepts are on the table?

Central configuration

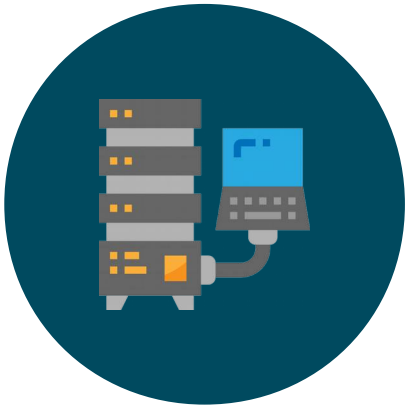


Decentral configuration



Available methods in Check_MK?

Direct host access



Livestatus

Business Intelligence

Livedump & CMCDump

Direct host access

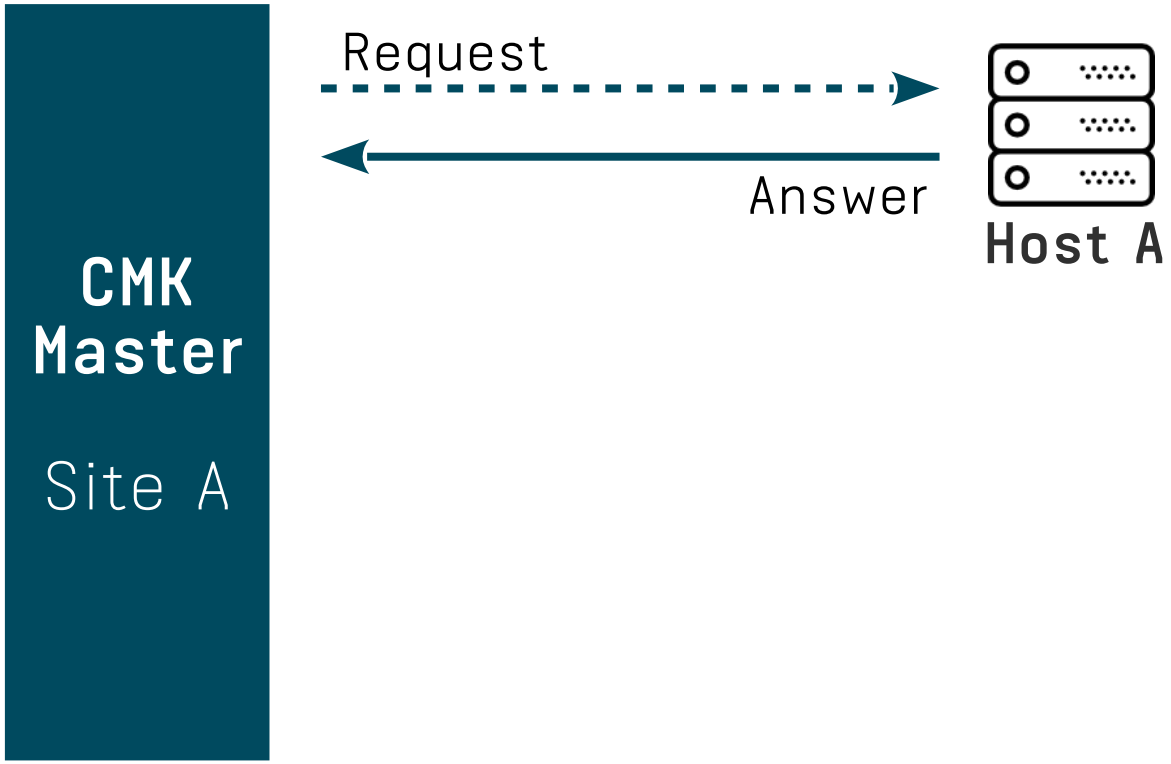
Livestatus

Business Intelligence

Livedump & CMCDump

How does it work …

Architecture



Comment

Access type

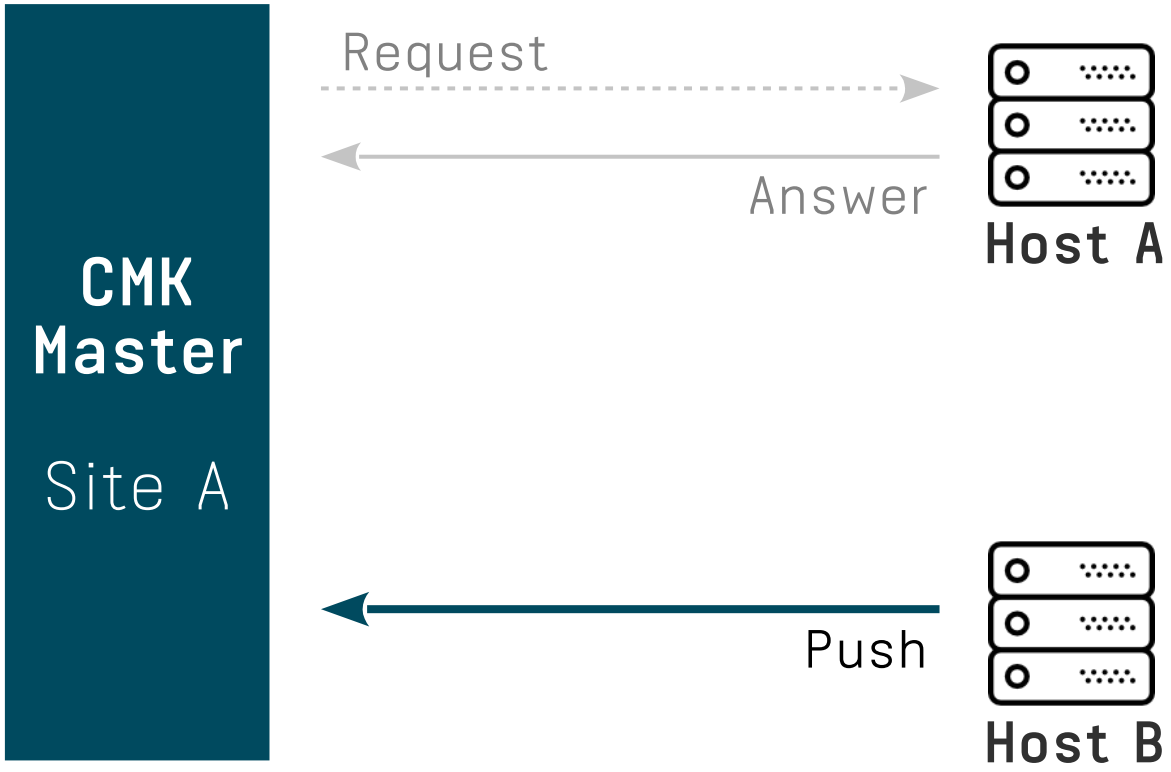
- Traditional access
- SSH

Request

Data transfer

… and which alternatives do I have?

Architecture



Comment

Access type

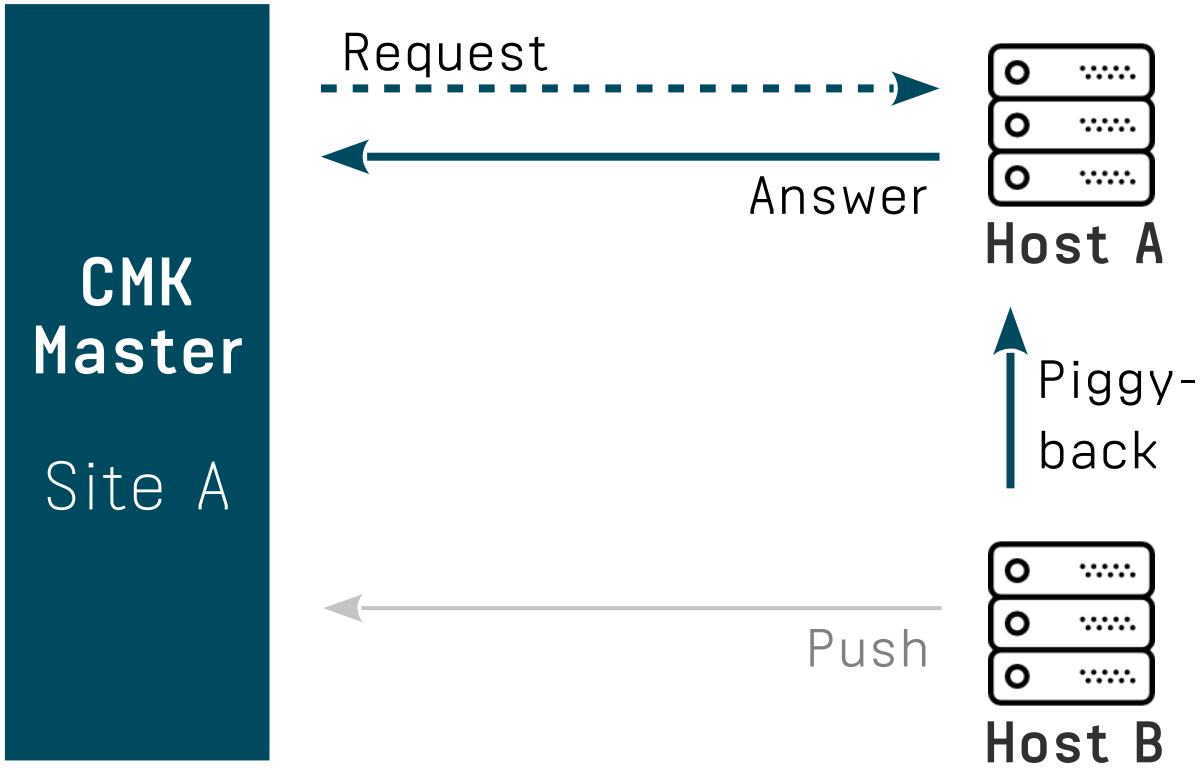
- Traditional access
- SSH
- Push

Request

Data transfer

… and which alternatives do I have?

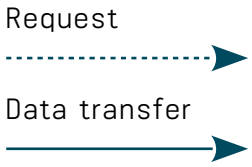
Architecture



Comment

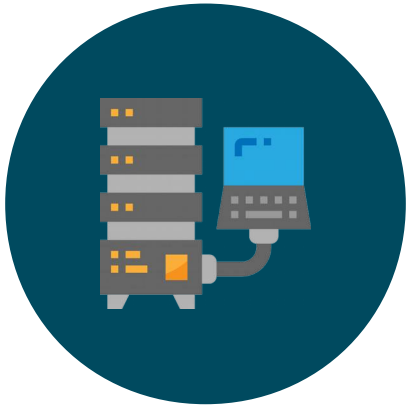
Access type

- Traditional access
- SSH
- Push
- Piggyback



Why not in all situations?

Limitations



- Network latency
- Dependency of connection
- Firewalls
- No native push
- Scalability

Direct host access

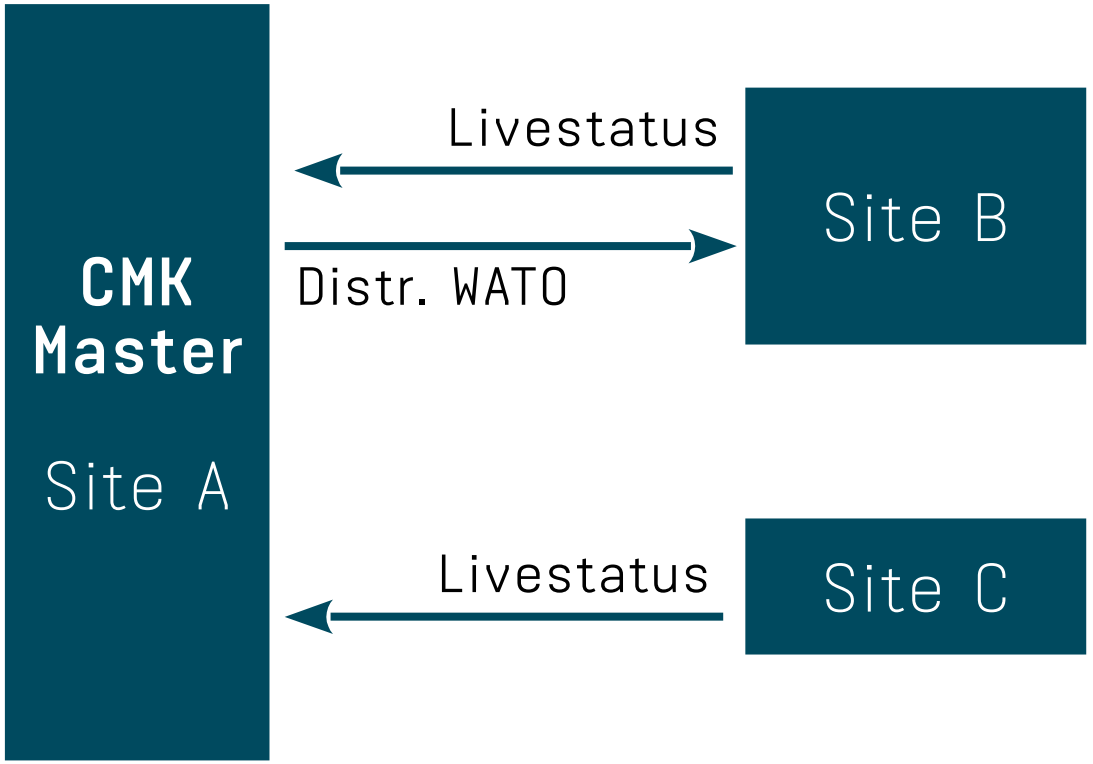
Livestatus

Business Intelligence

Livedump & CMCDump

How does it work ...

Architecture



Comment

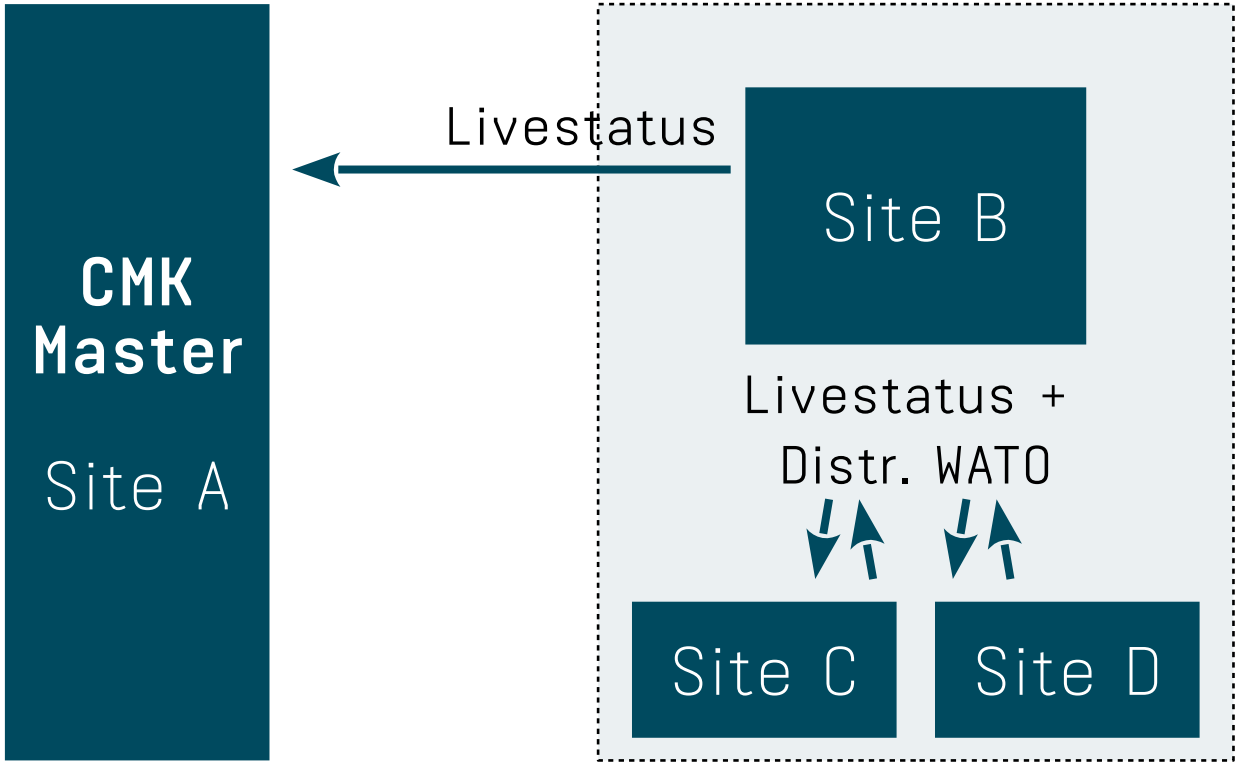
Access type

- Unix Socket
- TCP
- Livestatus Proxy

Data transfer

… and what about isolated sites?

Architecture



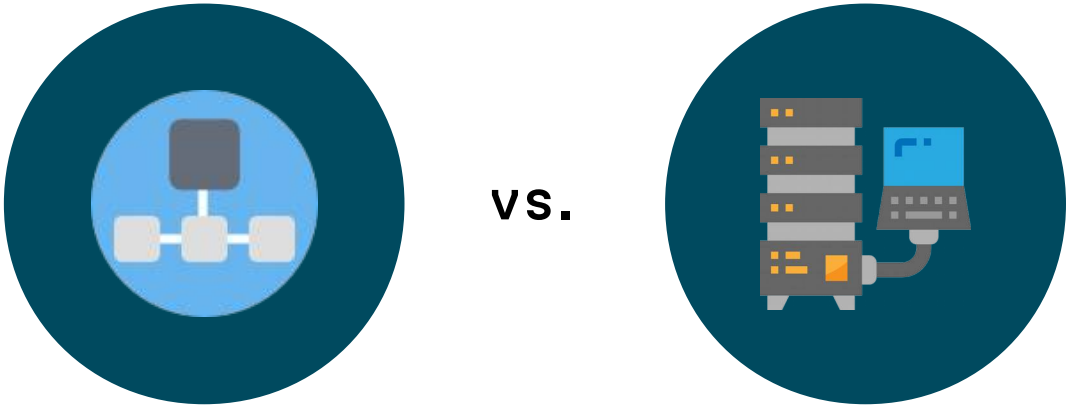
Comment

Access type

- Unix Socket
- TCP
- Livestatus Proxy
- Cascading Livestatus

When to use …

Livestatus vs. **Direct host access**



- Direct location monitoring
- High latency
- Unstable network connection
- Many hosts
- Limited network access

… and when not to use Livestatus

Limitations

- Scalable up to +/- 80 Sites
- Needs access to dedicated TCP-Port
- Agent Updater on Master only

Direct host access

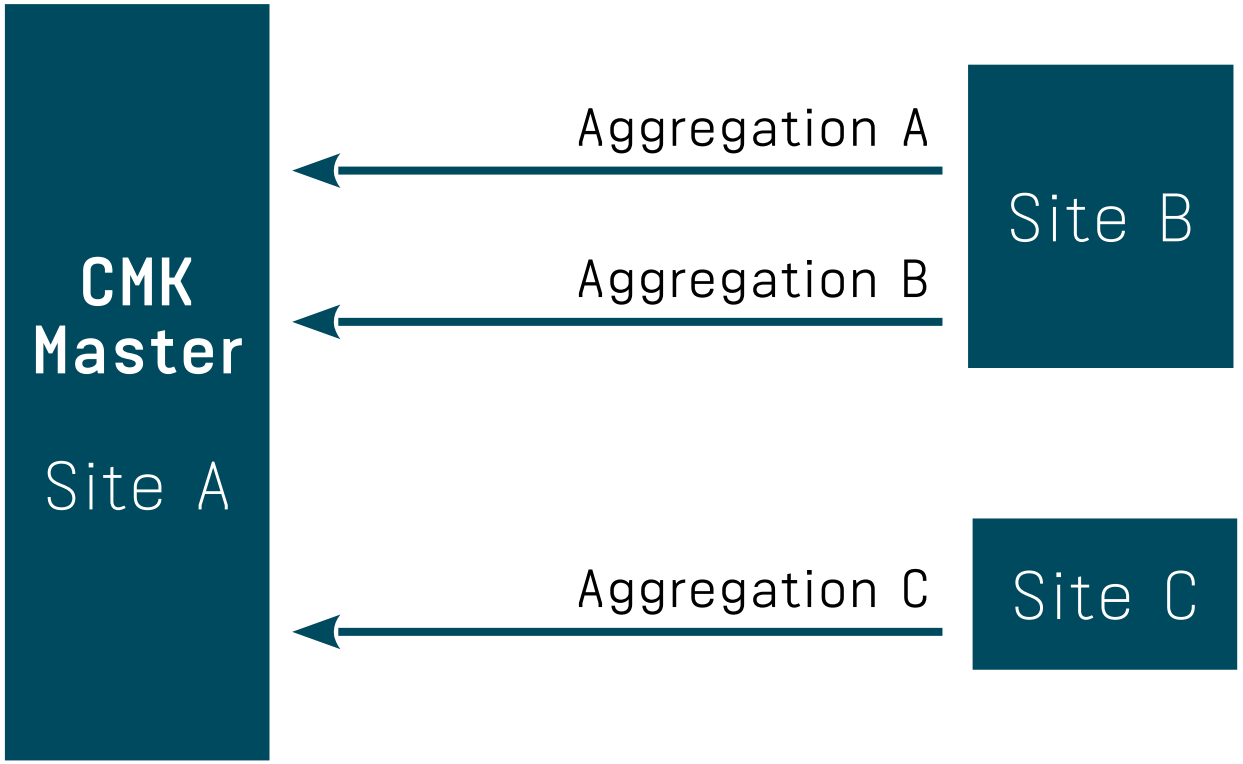
Livestatus

Business Intelligence

Livedump & CMCDump

Compress status data

Architecture



Comment

Access type

- Active check (HTTPS)

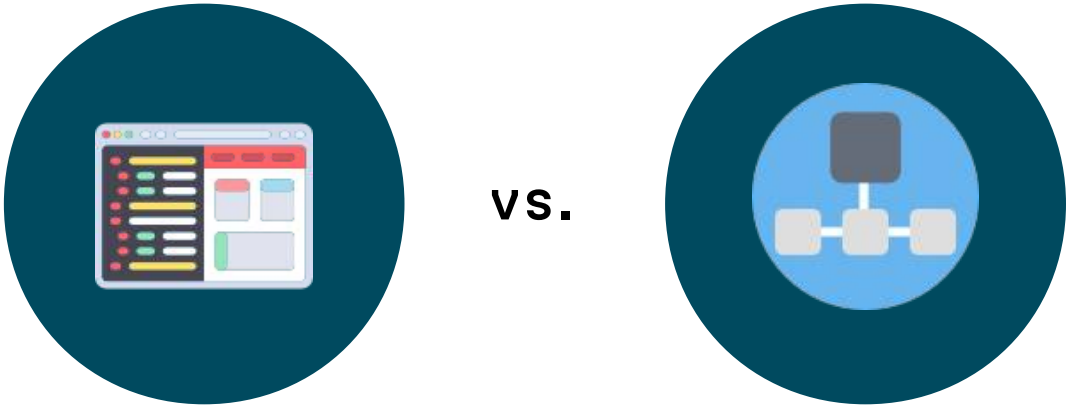
Options

- Multiple aggregation
- Individual config
- Link to group/site

Data transfer

Why Business Intelligence?

Business Intelligence **Livestatus**



vs.

- Large number of sites

How much does it cost me?

Limitations

- No config push
- Not all services in one view
- Complex configuration
- Every location needs a site

Direct host access

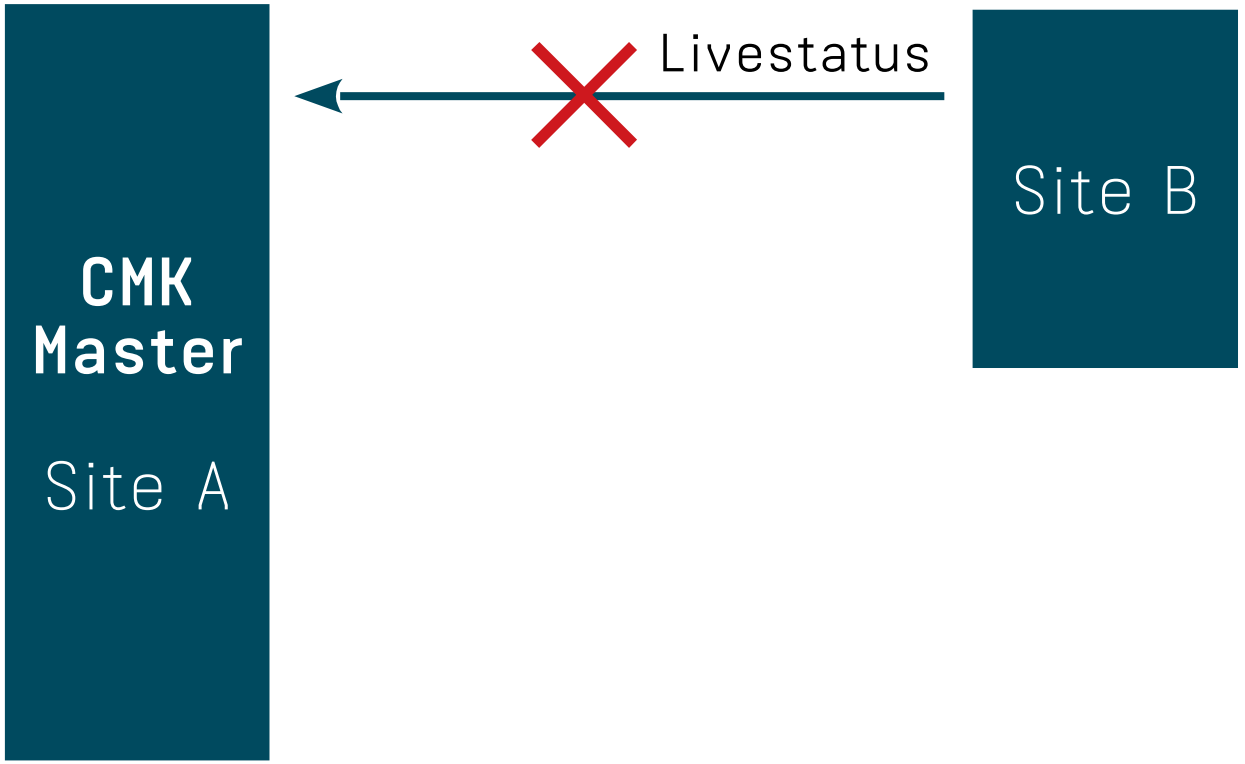
Livestatus

Business Intelligence

Livedump & CMCDump

No access is my problem …

Architecture

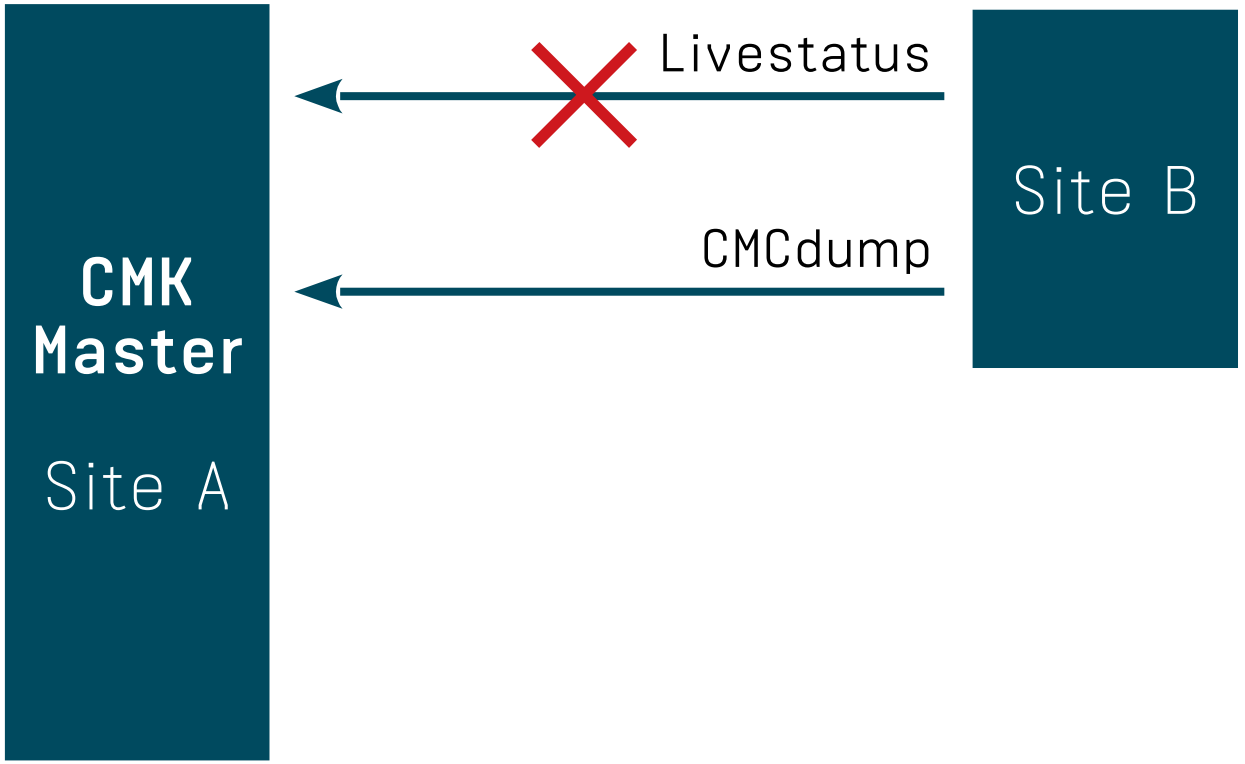


Comment

Data transfer

… and CMCDump my last option

Architecture



Comment

Access type

- SSH
- Email
- …

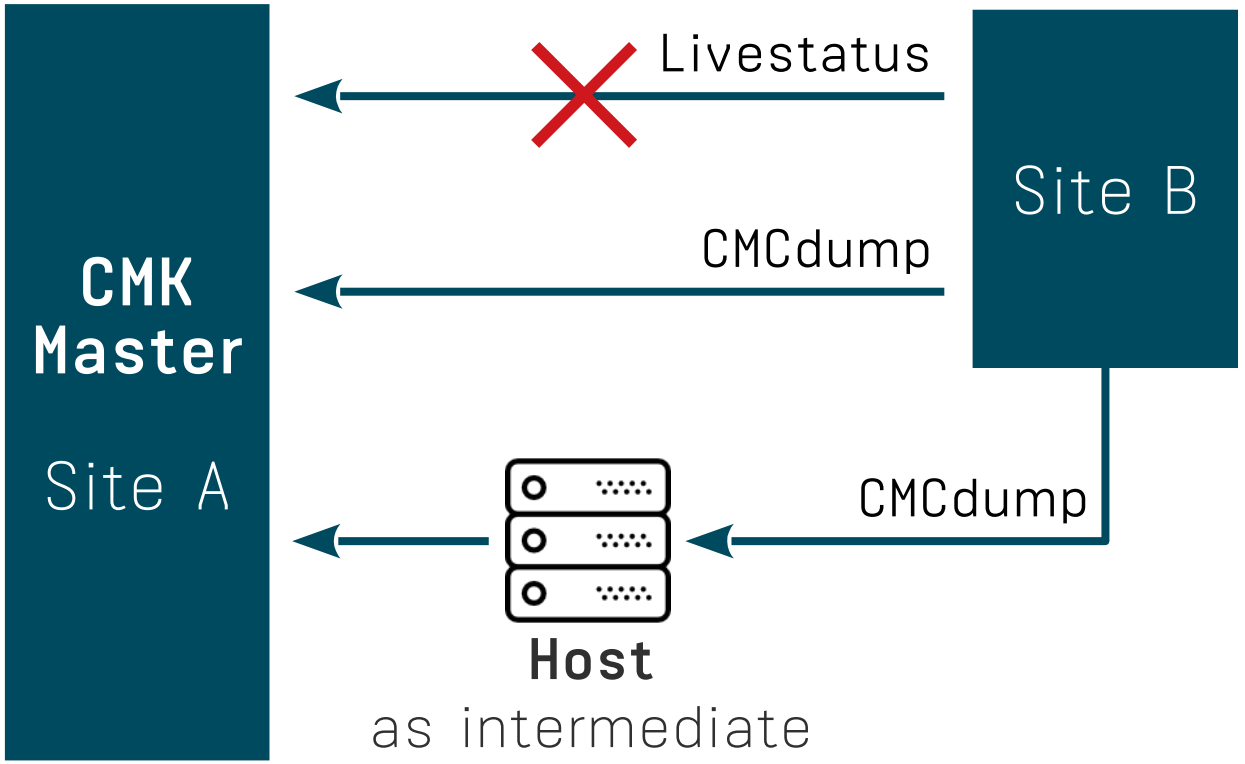
Dump types

- Status config
- Status data

Data transfer

With Intermediate if needed

Architecture



Comment

Access type

- SSH
- Email
- ...

Dump types

- Status config
- Status data

Data transfer

Why CMCDump?

To use if there is …

- … no access at all
- … no stable connection
- … very limited bandwidth

Limitations

- No Plug'n'Play
- No config push
- No live data
- Managing on Slave only

Direct host access

Livestatus

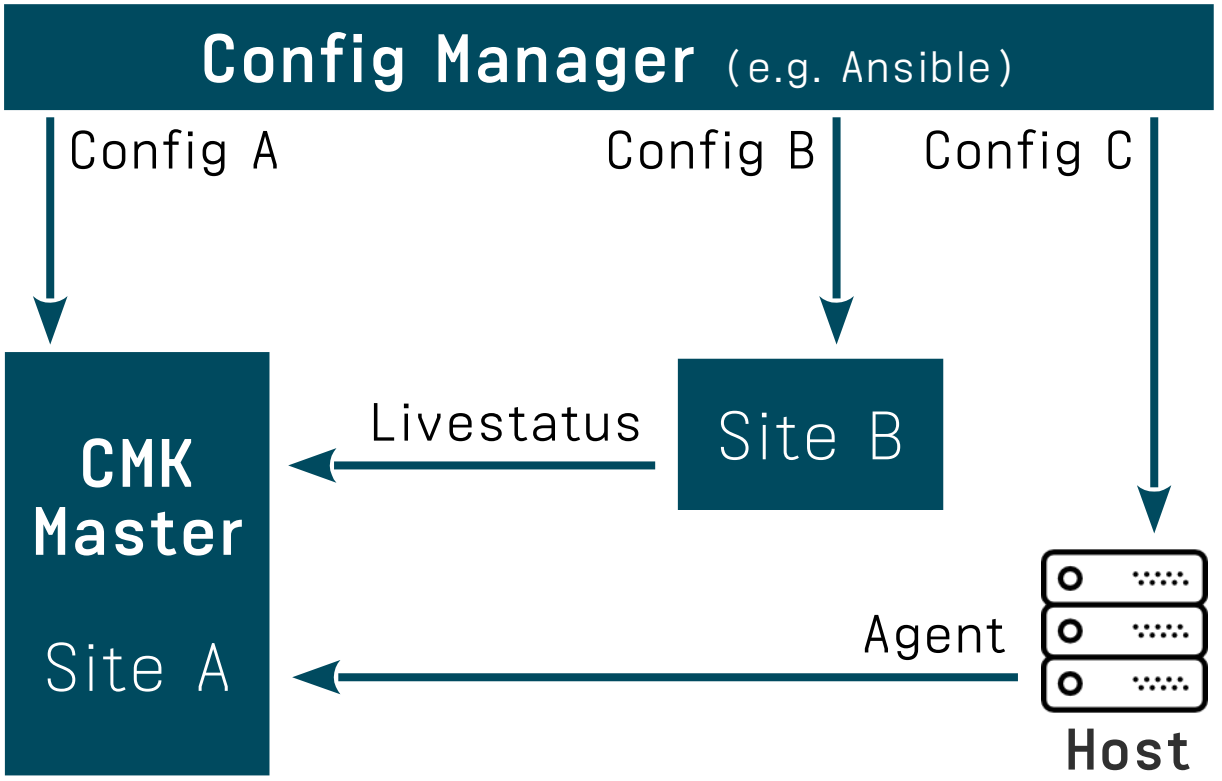
Business Intelligence

Livedump & CMCDump

Individual Configuration Mgt.

A first example

Architecture



Comment

Configuration...

- of agent
- of plugins
- of sites

Considerations

Pro

- Usage of existing methods
- Multilevel config push
- Possibility of automation
- Less self written scripts

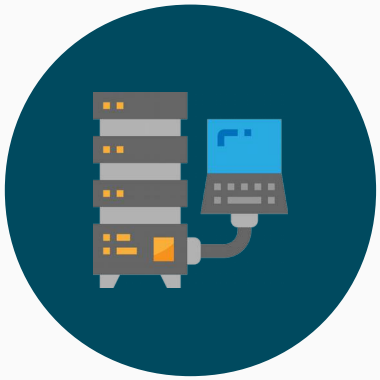
Con

- Higher complexity
- Error prone
- Expensive
  - Initial setup
  - Maintenance

Which method to choose first?

1

Direct host access



2

Livestatus

3

Business Intelligence

Livedump & CMCDump

Individual solutions

What aspects affect my decision?

Questions to ask

- Is independent monitoring important?
- Which method scales the best for me?
- Which functions do I need centralized?
- How autonomous are the teams?
- What are my security restrictions?
- What is my network structure?
- …

CHECK_MK

CONFERENCE

MUNICH 2018/5/2-4

#4