



Monitoring Windows Server Infrastructure using Open Source products

Pablo Martin Zamora

HEPiX Spring 2023 Workshop

Agenda

- **Windows Server Infrastructure at CERN**
- **Project overview**
- **Icinga 2 at CERN**
 - Architecture
 - Checks
 - Notifications
 - Agent
 - Director
- **Summary**

Windows Server Infrastructure at CERN

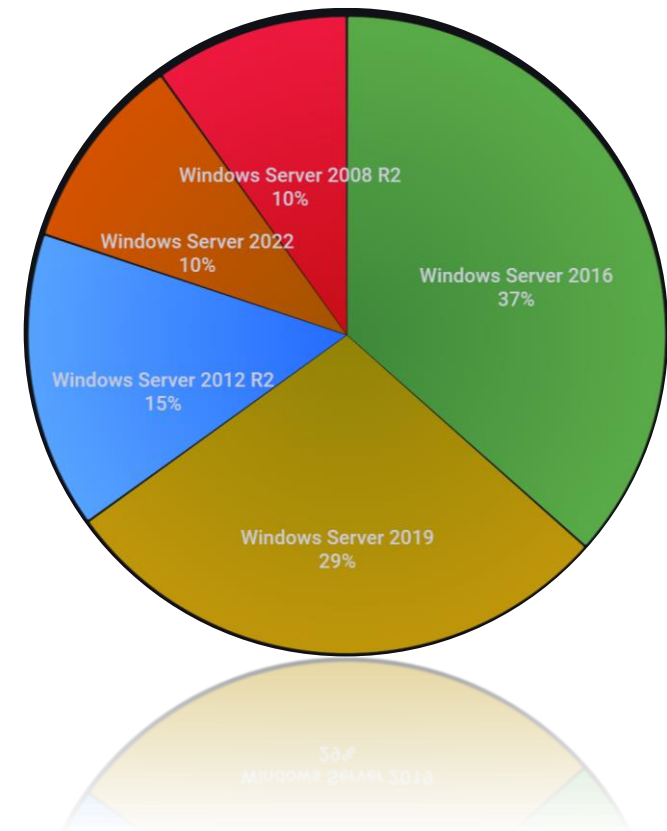
Windows Server Infrastructure:

- Part of the IT-CD-DPP section (Devices, Provisioning and Productivity)
- Actively manage the lifecycle of >500 Windows Servers in the organization
- WinInfra Activities: Day to day operations for Windows Servers running critical Services, +Security, +Configuration and +Monitoring.



Computer Management Framework

- Provide Windows Server expertise and support to >1600 Windows Servers throughout CERN.

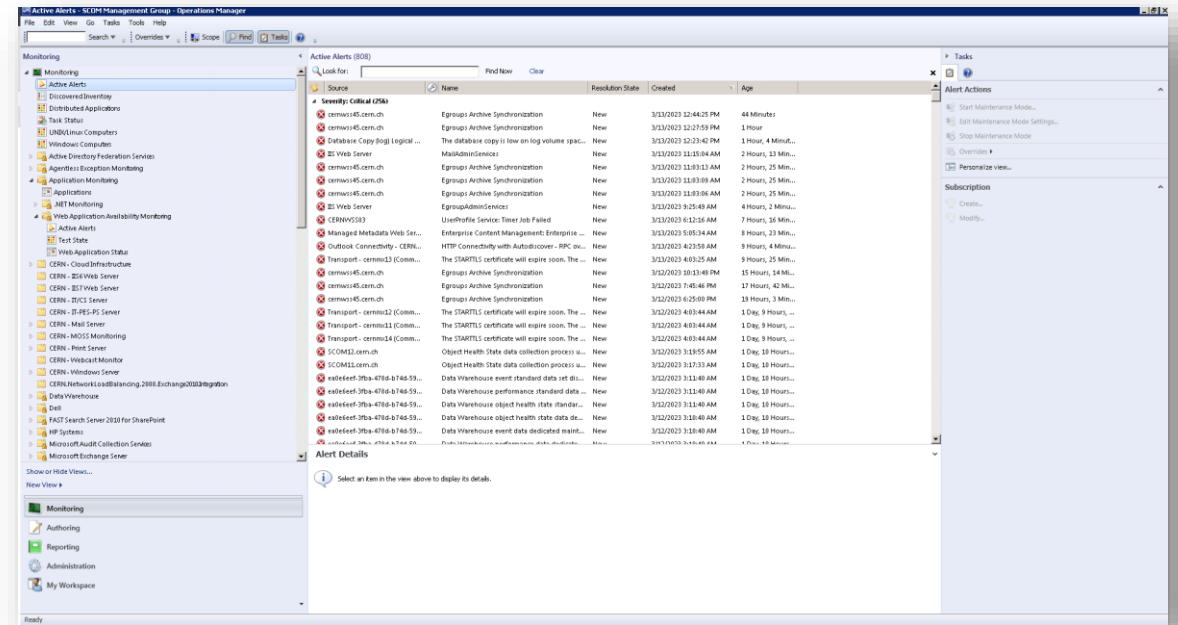


Project overview

Replace Microsoft System Center Operations Manager (SCOM) with an open-source lightweight and maintainable operations monitoring system.






- Powerful for on-premises infrastructure monitoring of Microsoft products, out-of-the-box integration with all standard Microsoft services. 👍
- Complex: requires deep product knowledge and person power to operate and maintain. 👎



Project overview



- **Icinga 2** 
 - [Scalable, extendable, modular](#)
 - [Powershell support](#) 
 - [Config. Mgmt. support](#)  puppet
 - Simple architecture
 - Management framework for notifications, hosts, services, historical data, dashboards, ...
- **Project scope**
 - Migrate:
 - Simple use cases (aliveness, port monitoring, notifications)
 - Complex functionality from SCOM (develop custom checks based on PowerShell)
 - Agent deployment and integrations
 - Thanks to Mike Kalliafas who worked on this project!
- **Used in day-to-day operations for WinInfra**
 - Interventions
 - Windows Patches
 - Hardware Events
 - Service status and availability
 - Icinga 2 maintenance:
 - Operate, extend functionality, update components, ...

Icinga 2

System Resources

Icinga accesses the local resources of your servers and monitors all aspects of the system.



Services and Processes



Utilization of Disks



Server Load



Utilization of Memory (RAM)



Specific OS Parameters



Logged in Users



Logfiles and Eventlog



Cronjobs and Scheduled Tasks



Uptime



Available Updates



Health of Applications



Containers



Anything else Icinga can access

Recommended Resources

For an easy start we recommend at least 2 GB of RAM, 2 or more cores, Ubuntu for the operating system, an Apache web server and MySQL as a database.

Install Icinga 2

You need Icinga 2 to collect the data to monitor your infrastructure. Follow the [Icinga 2 installation instructions](#) and learn how to run it and connect it to your database.

Install Icinga Web

Next you install Icinga Web. Use Icinga Web to display the monitoring information in a clean and fast web interface. In the [Icinga Web installation instructions](#) you learn how to kickstart it.

Basics are all set!

Here's how you can extend Icinga to use it to its full capacities:

Director

Manage your monitoring configuration through the web interface and automate it.

Install the [Icinga Director](#)

Modules

Extend Icinga with custom views, reports, business processes and more features.

View all [Icinga Modules](#)

Plugins

Search through thousands of plugins that you can use to monitor your entire infrastructure. Explore [Icinga Exchange](#)

[Exchange](#)

Your Icinga Stack

Your Icinga Stack is up and running! Plan your next big steps with Icinga – learn how to scale your setup in our [Distributed Monitoring](#) guide.

Images credit: <https://icinga.com/solutions/server-monitoring/>

Icinga 2: Architecture

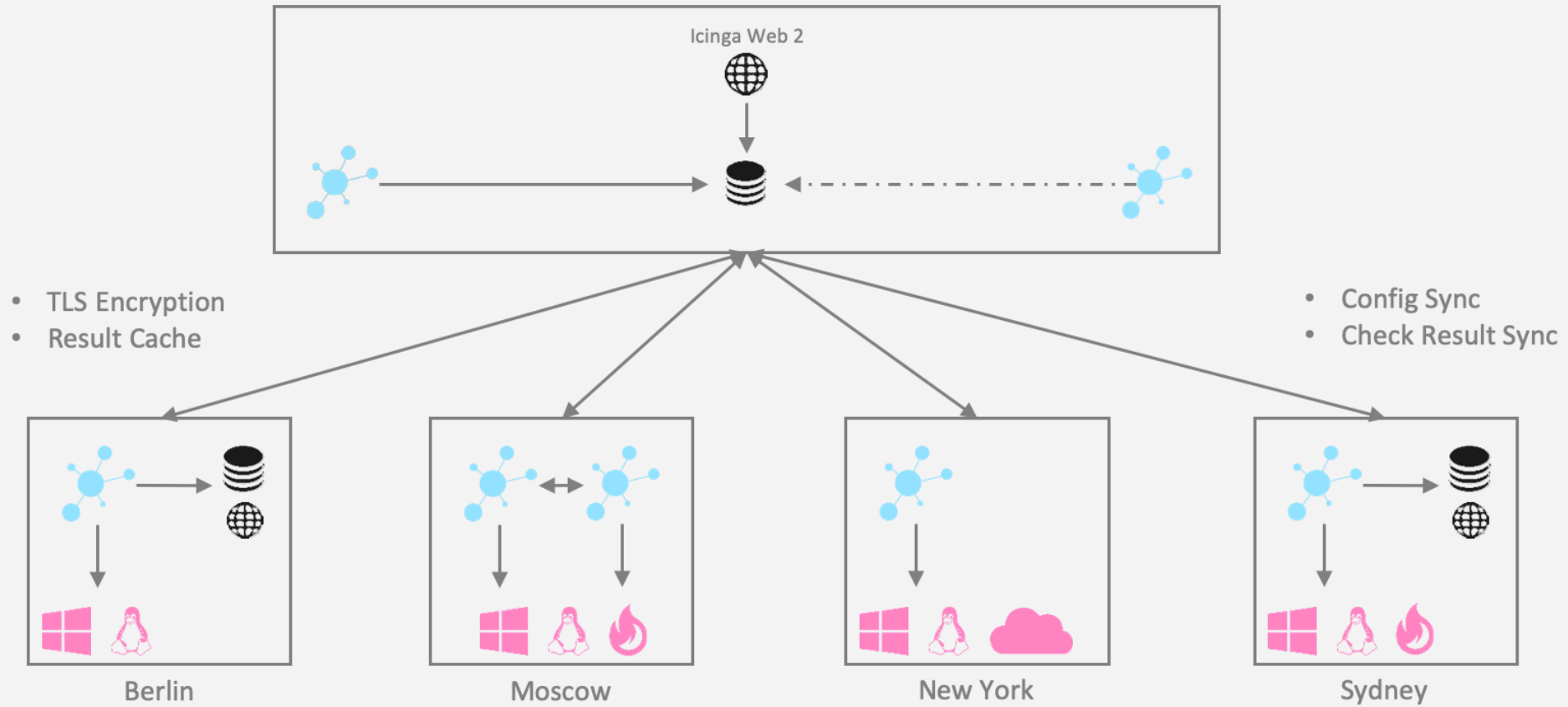
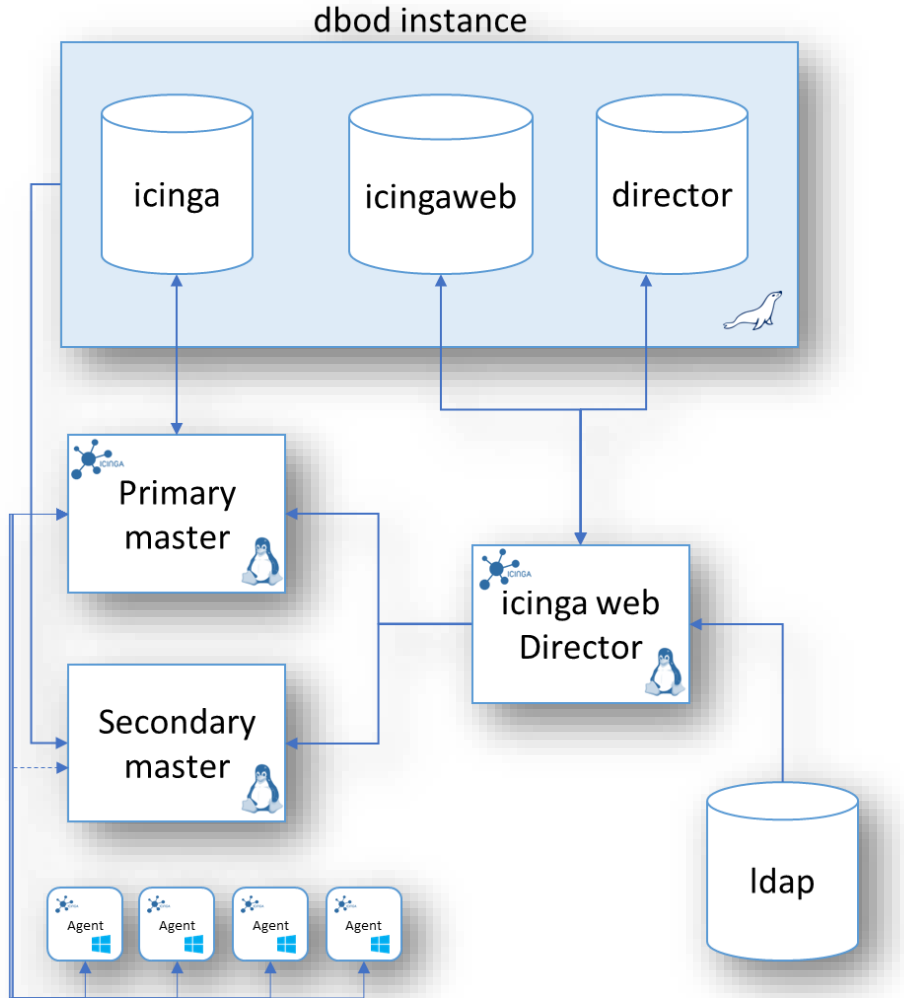


Image credit: <https://icinga.com/docs/icinga-2/latest/doc/01-about/>

Icinga 2: Architecture at CERN






- **2 x Icinga 2 Masters in HA*:**
 - 1 x primary (0513-R-0060)
 - 1 x secondary (0513 R-0050)
- **3 x MySQL Databases**
- **1 x Icinga 2 Apache Web server + 1 x Icinga 2 Director**
- **Objects sync from Idap source (users/groups)**
- **Supporting >500 hosts**

* HA (2nd master takes over if primary is down, max. time ~10min)

Icinga 2: Services Monitored at CERN

Icinga 2 Windows Infrastructure services:

- Active Directory 
- 35 x Windows Terminal Server Clusters
- Aras and SmarTeam (CAD PLM)
- MS SQL 
- CMF (Application deployment and configuration management)
- DFS (Distributed File System)
- Engineering License Servers
- Printing
- Authentication (ADFS, PKIs)
- Hyper-V 
- Web Services (IIS, Web AFS, Drupal, Notifications Service)
- Plus: Workers, Backup servers, WSUS, ...

Icinga 2: Services Monitored at CERN

| Service Group | Service States |
|----------------------------------------------------|-------------------|
| 76 Active Directory Lightweight Directory Services | 1 75 |
| 131 Active Directory services | 4 127 |
| 20 ARAS Services | 1 1 18 |
| 1 Authentication services | |
| 15 CMF services | 15 |
| 688 DFS Services | 13 675 |
| 28 HyperV services | 2 26 |
| 70 License Services | 70 |
| 1 Linux generic services | |
| 91 MSSQL Services | 2 89 |
| 46 Print Services | 46 |
| 32 SmarTeam Services | 32 |
| 549 Terminal services | 11 1 3 534 |
| 53 Web Services | 1 52 |
| 3714 Windows Generic Services | 32 221 11 19 3431 |
| 36 Wininfra services | 4 32 |
| 11 WSUS services | 2 9 |

Icinga 2: Check types

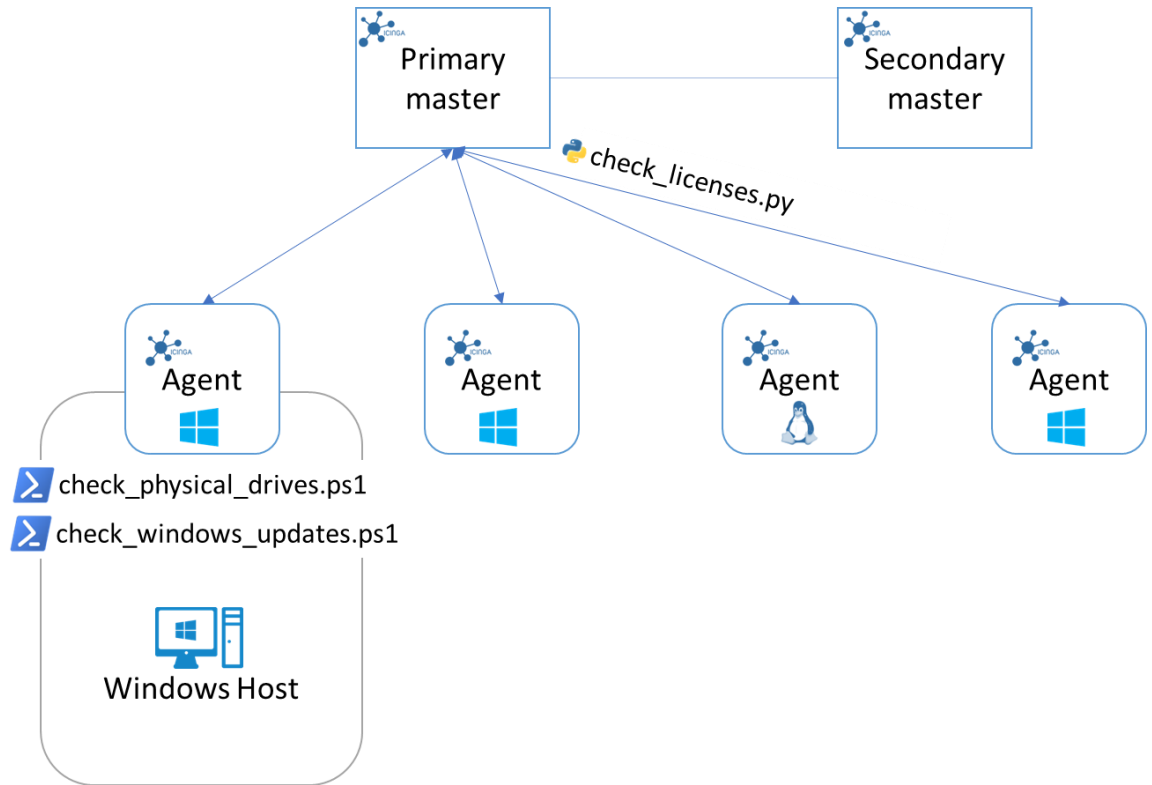
- ✓ **Remote checks:** Anything that can be queried from outside (port, URLs, certificates,...)
- ✓ **Agent-based:** queries runs in the Icinga 2 agent context

➤ check_ad_replication.ps1

```
# To be run in each DC, Failure count > 0, because when DCs are patching, it is very likely that they can
$replication = Get-ADReplicationFailure -Target $env:COMPUTERNAME
$status = $replication | Where-Object { $_.Failurecount -gt 0 }

# To check for errors in repadmin, if lines > 7 means that there are errors, we show the output in icinga2
$repadmin = repadmin /showrepl "$($env:COMPUTERNAME):389" /erroronly
$repadmin_lines = $repadmin | Measure-Object -Line | Select-Object Lines -ExpandProperty Lines

if (!$status -and $repadmin_lines -le 7 ){
  Write-Output "[OK] No AD Replication Failures on $env:COMPUTERNAME"
  Write-Output "| 'Replication fail'=0"
  exit(0)
}
else {
  Write-Output "[CRITICAL] AD Replication Failure with:" $($replication)
  Write-Output $($repadmin)
  Write-Output "| 'Replication fail'=1"
  exit(2)
}
```



* Requires at least PowerShell 4.0 (WS2012 R2 or later)

Icinga 2: Common checks



Common checks

- Processes and services
- CPU, Disk and Memory metrics
- Windows Updates (Security and Virus definitions)
- Server state:
 - Firewall
 - Puppet status
 - Scheduled tasks
 - File shares
 - Logged in users
- ...

The image displays several Icinga 2 check status cards for different servers and services. Each card shows the service name, status, and plugin output.

- Processes at cernm2p02:** OK since Feb 22. Plugin Output: [OK] The process m2pcmd is running. **Process metrics**
- cernts1624.cern.ch:** UP since 2022-12. Service: CPU Load. Plugin Output: LOAD OK 9.16244%. **CPU Load**
- cerntsbe205.cern.ch:** UP since Mar 2. Service: Disk Space (TS) !. Plugin Output: DISK CRITICAL - free space:C:\ 16330 MB (10%); **Disk Usage**
- xldap31.cern.ch:** UP since 2022-09. Service: Windows Updates !. Plugin Output: [WARNING] Windows Updates: 1 Warning 5 Ok [WARNING] Total Pending Updates (3c). [WARNING] Total Pending Updates: 3c is greater than threshold 1c. **Security Updates**
- cernprint-qa.cern.ch:** UP since 2022-10. Service: Printing UNC paths. Plugin Output: [OK] \\cernprint-qa.cern.ch, [OK] \\cernprinthp.cern.ch, [OK] \\cernprintcanon.cern.ch, [OK] \\cernprintoce.cern.ch, [OK] \\cernprintxerox.cern.ch. **Shares**

Icinga 2: Custom checks

The screenshot displays four Icinga 2 service monitoring cards:

- DNS records:** Service: DNS cerndc record !. Status: WARNING since 08:55. Plugin Output: [WARNING] CERND54 is not in AAAA cerndc. There are currently 4 host(s) in cerndc cerndc56.cern.ch. Hosts listed: cerndc53.cern.ch, cerndc52.cern.ch, cerndc51.cern.ch.
- Physical disks:** Service: Physical Drives. Status: OK since Feb 28. Plugin Output: Table of disk metrics for /dev/sda partitions 252:0 through 252:17.
- Loadbalancers:** Service: LBAAS status for cernts. Status: OK since Jan 16. Plugin Output: List of load balancer health checks for cerntsvac.cern.ch, cerntscryo.cern.ch, cerntscv.cern.ch, cerntse1.cern.ch, and cerntsice.cern.ch.
- Automated backup restores:** Service: SQL restores. Status: OK since 2022-12. Plugin Output: LAPS and Prod.

⚡ Custom checks

- AD operations (Replication, DNS records)
- Physical HW (Disks, Memory, Licensed USBs)
- Web services (IIS config availability)
- LBAAS status
- Software (version compliance, configuration)
- Backups (TSM, Windows System Backups, MS SQL Backup restores)
- URL availability
- Certificate expiration
- ...

Icinga 2: Checks

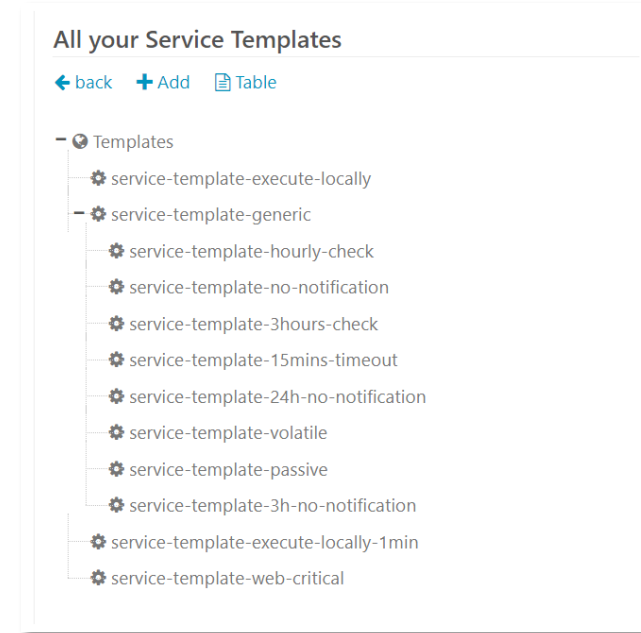


Rich granularity:

- Single host, host groups, service groups
 - Apply checks to certain hosts or groups only.
- Use templates, inheritance and dependencies to build services structure.
- Easy to tune, reduce noise and highlight valuable events.

Custom Dashboards:

- Shareable between Icinga users
- Allow for a quick overview of checks assigned to services or host groups







Icinga 2: Event handlers

Event handlers

- Actions executed after a check has reached a certain state.
- **Success CERN use case:**
 - IIS Hosted Web sites not available → recurrent every other week.
 - **Probable cause:** IIS Windows Server that loses access to the underlying storage hosting the website configuration files.
 - **Perform remediation logic** → Attempt to restart the web service and notify owners.

Monday, February 20, 2023

| | |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK 07:45:32 |  [OK] https://op-webtools.web.cern.ch/ (code 200) |
| CRITICAL 07:44:32 |  [2/5] [CRITICAL] Internal server error for https://op-webtools.web.cern.ch/ (code 500) |
| CRITICAL 07:43:32 |  [1/5] [CRITICAL] Internal server error for https://op-webtools.web.cern.ch/ (code 500) |
| OK 07:43:35 |  https://op-webtools.web.cern.ch/ (code 200) |

Icinga 2: Checks integrations

Integrations:

- REST API to ingest Icinga 2 data into other services.
- Historic of Icinga events in CERN Central monitoring.
- Service Availability for the IT Service catalog based on Icinga checks output.
 - Windows Service
 - DFS
 - Web hosting (IIS, AFS)



https://monit-grafana.cern.ch/goto/qi12Q_-4k?orgId=58

Icinga 2: Notifications



Granular:

- Per hosts, host groups or users
- Use templates and inheritance

Customizable

- Notify on defined states (warning, critical, recovered service,...)
- Add/Remove information in the notifications
- Define intervals, time periods, delays, silence.

Extendable

- Integration with CERN Mattermost and SMS notifications.

[PROBLEM] Last Boot on cerndc59.cern.ch is WARNING!

icinga@cern.ch
To: Pablo Martin Zamora

ICINGA2 REPORT

[Icinga2 Web](#)

Last Boot on cerndc59.cern.ch is **WARNING**

Group: *hostgroup-ad-servers*
When: 2023-03-17 11:18:53
Service: *Last Boot*
Host: *cerndc59.cern.ch*
IPv4: 188.184.51.235

Output

[WARNING] The server has been rebooted on 03/17/2023 11:14:52

Icinga BOT 3:28 AM
🔥 PROBLEM cernwds10.cern.ch is DOWN - Zone 'cernwds10.cern.ch' is not connected. Log lag: 22 hours, 31 minutes and 57 seconds

Icinga BOT 3:33 AM
✅ RECOVERY cernwds10.cern.ch is UP - Zone 'cernwds10.cern.ch' is connected. Log lag: less than 1 millisecond

Icinga BOT 3:42 AM
🔥 PROBLEM rdslic2012-01.cern.ch is DOWN - Zone 'rdslic2012-01.cern.ch' is not connected. Log lag: 28 days, 11 hours, 30 minutes and 19 seconds

Icinga BOT 3:47 AM
✅ RECOVERY rdslic2012-01.cern.ch is UP - Zone 'rdslic2012-01.cern.ch' is connected. Log lag: less than 1 millisecond

Icinga 2: Agent

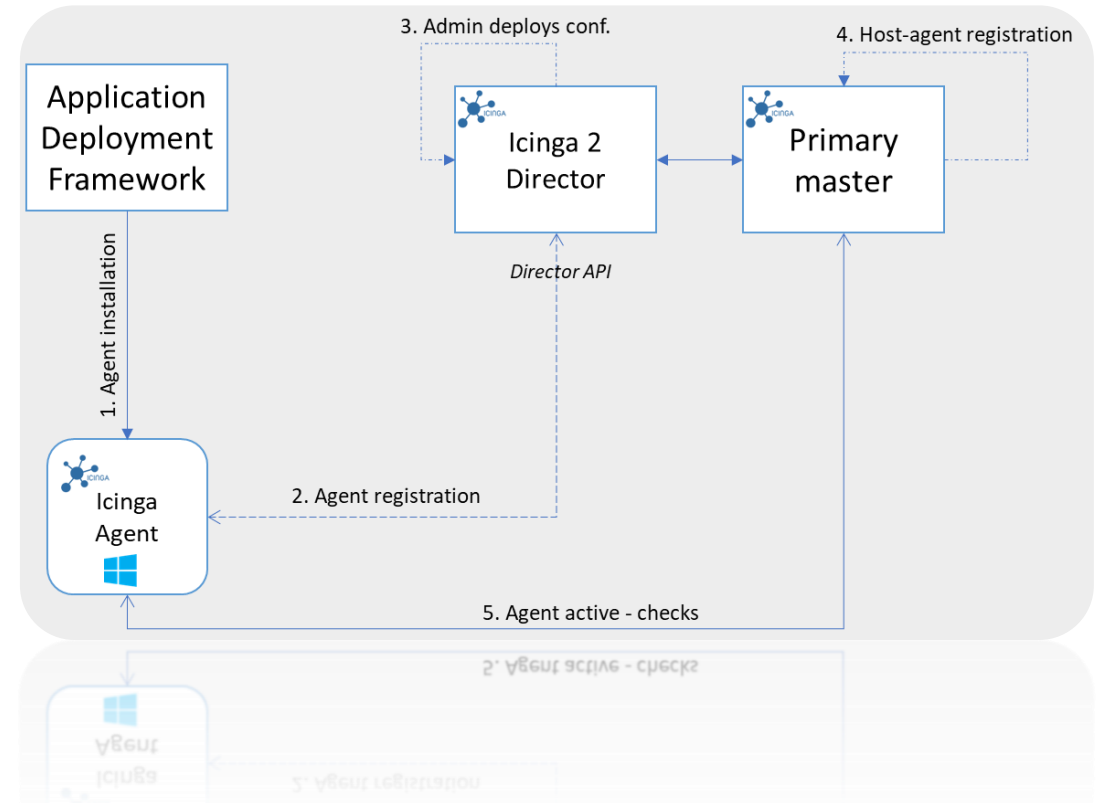
Orchestrate agent deployment in any framework:

 Windows:  Computer Management Framework

- PowerShell scripts that install pre-requisites (framework, plugins) and custom checks.
- Binary installation → Upgrade from previous versions

 Linux

- Puppet wrapper: <https://gitlab.cern.ch/ai/it-puppet-module-cernicinga2>



Icinga 2: Director



Director

- Icinga Web 2 module to deploy configurations.
- Alternative to plain text files and manual configuration.
- **Reduces the complexity**
 - Granular delegation of administration tasks
 - Manage hosts, services, thresholds and notifications.
- **Traceability**
 - Change tracking.
 - Allows re-deployment of old configurations at any time → config. version control
- **Enable automation, leverage data sources into Icinga 2:**
 - e.g., Import attributes from your Config. Management / Idap / SQL database
 - Run checks for hosts in a specific building, from a certain owner, belonging to a group, etc.

Summary



New incarnation of Windows Infrastructure Monitoring:



Based on open-source tools → Active Community



Easy to manage and maintain → Great PowerShell support



Rich API → Integrate with any tooling or other monitoring services.



Achievements:



Improved visibility into our services by aggregating workflows, emails and scripts into a single framework!



Admins access notifications and web monitoring everywhere.



Less time spent maintaining the infrastructure, focus on what really matters!

Thank you!

- **CERN Resources**

- CERN Linux Agent Installation: <https://gitlab.cern.ch/ai/it-puppet-module-cernicinga2>
- CERN Icinga 2 Puppet Configuration: <https://gitlab.cern.ch/ai/it-puppet-hostgroup-winmonit>
- CERN Windows Agent Installation: <https://gitlab.cern.ch/IT-DEP-CDA-AD/icinga2/icinga2-installation-scripts>
- CERN Icinga 2 PowerShell custom checks: <https://gitlab.cern.ch/IT-DEP-CDA-AD/icinga2/icinga2-custom-checks>

- **Icinga 2 Resources**

- Community: <https://community.icinga.com/>
- Demo: <https://icinga.com/demo/authentication/login>
- Repositories: <https://github.com/Icinga/>
- Puppet modules: <https://forge.puppet.com/modules/icinga/icinga2>



home.cern