



Toolforge webservices are in the final stages of [migrating to the toolforge.org domain](#) .
Please help us clean up older documentation referring to tools.wmflabs.org!

Incident documentation/20181204-Toolforge-Kubernetes

[< Incident documentation](#)

Contents [\[hide\]](#)

- 1 [Summary](#)
- 2 [Timeline](#)
- 3 [Conclusions](#)
 - 3.1 [Toolforge configuration is spread between ops/puppet.git, Wikitech and Horizon](#)
 - 3.2 [Lack of knowledge \(and documentation\) about tools-checker-01](#)
 - 3.3 [Usage of "tools.eqiad.wmflabs" and "tools.wmflabs.org" interchangeably](#)
 - 3.4 [Mysterious networking issues](#)
 - 3.5 [Human error](#)
- 4 [Actionables](#)

Summary

The Toolforge Kubernetes cluster was partially unavailable from 20:03 until 22:35 following the removal of 2 floating IPs from the "tools-k8s-master-01" instance and the removal of the "k8s-master.tools.wmflabs.org" DNS entry. During this time, workloads continued to run but new pods could not be scheduled on the cluster.

Timeline

- 20:03 - Removed floating IPs 208.80.155.204 and 208.80.155.247 from tools-k8s-master-01 instance and deleted the k8s-master.tools.wmflabs.org DNS entry
- 20:25 - Received warning from Icinga for the "toolschecker: All k8s worker nodes are healthy on checker.tools.wmflabs.org" check
- 20:31 - Started to troubleshoot issue. Kubernetes nodes were up and only monitoring was failing, pointing to an issue with the monitoring.
- 20:52 - Proceeded to update toolschecker configuration to use internal name "tools-k8s-master-01.tools.eqiad.wmflabs" instead of "k8s-master.tools.wmflabs.org". Server went from timeout error to 504 error complaining that "Caught exception: hostname 'tools-k8s-master-01.tools.eqiad.wmflabs' doesn't match either of *.tools.wmflabs.org"
- 19:00 - Quick investigation didn't show the root cause for the error in toolschecker. Decided to roll back floating IP and DNS changes
- 19:03 - Unable to associate a floating IP back to tools-k8s-master-01 instance
- 19:07 - Reconfigured floating IP quota on `tools` project from zero to 60 so a new floating IP could be allocated (it complained that there were already 58 other floating IPs in use), even though the quota wouldn't allow that.
- 19:13 - Floating IP 208.80.155.244 was associated to tools-k8s-master-01 and DNS entry for "k8s-master.tools.wmflabs.org" was added back with the new IP
- 19:15 - "<http://checker.tools.wmflabs.org/k8s/nodes/ready>" was timing out
- 19:23 - Restarted "toolschecker_kubernetes_nodes_ready" on tools-checker-01 server. No changes.
- 19:30 - Noticed Kubernetes is now broken (timeout talking to API server). Confirmed API server is running and accepting connections on the internal address (10.68.17.142) but connections using the floating IP were failing
- 19:35 - Associated old floating IPs .204 and .247 again. No changes.
- 19:47 - Noticed connections attempts coming from tools-checker-01 were being replied by tools-k8s-master-01 but replies never arrived to tools-checker-01. Started to look like networking issue we faced a few weeks ago.
- 19:50 - Engaged networking team to check switch MAC table.

[Main page](#)
[Recent changes](#)
[Server admin log \(Prod\)](#)
[Server admin log \(RelEng\)](#)
[Deployments](#)
[SRE/Operations Help](#)
[Incident status](#)

[Cloud VPS & Toolforge](#)

[Cloud VPS documentation](#)

[Toolforge documentation](#)

[Request Cloud VPS project](#)

[Server admin log \(Cloud VPS\)](#)

[Tools](#)

[What links here](#)

[Related changes](#)

[Special pages](#)

[Permanent link](#)

[Page information](#)

[Cite this page](#)

[Print/export](#)

[Create a book](#)

[Download as PDF](#)

[Printable version](#)

- 19:57 - Cleared labvirt1009 eth1. No changes.
- 19:58 - Cleared labvirt1004 eth1. No changes.
- 20:18 - Removed all floating IPs from tools-k8s-master-01 and re-associated only 208.80.155.247. No changes.
- 20:24 - Confirmed pinging k8s-master.tools.wmflabs.org worked externally, from other labvirt's and cloud any instance on eqiad1-r region. It didn't work from any instance in the eqiad/main region so it was not isolated to tools-checker-01 only
- 20:25 - Cleared labnet1001 eth1. No changes.
- 20:35 - ICMP echo replies from tools-k8s-master-01 start to arrive on tools-checker-01. All communication is restored.

Conclusions

Toolforge configuration is spread between ops/puppet.git, Wikitech and Horizon

The initial research done on T164123 to find out why 2 floating IPs were being used when the Kubernetes master was not supposed to be accessible externally focused on the ops/puppet.git and ops/dns.git repositories only. Had it also included Wikitech/Horizon and checks on the servers themselves, it would have uncovered that "k8s-master.tools.wmflabs.org" was indeed in use.

There is a long-standing discussion about multiple Hieradata backends and how it adds to the confusion when looking for some value. There already is a task for this ([T211029](#)).

There's an argument to be made that the Toolforge [documentation](#) explicitly mentions k8s-master.tools.wmflabs.org as being used. However, one important value like what is the Kubernetes master address was expected to be defined in code. In any case, had the documentation been consulted before making the initial change, this problem could have been avoided.

Lack of knowledge (and documentation) about tools-checker-01

When monitoring failed, there was no documentation available about the services running on tools-checker-01. Troubleshooting focused on tracing where Icinga was connecting, which process was running on that port and what was it trying to do. This took a long time and involved finding an obscure configuration file hardcoded in toolschecker.py that was owned by a Toolforge tool that is being used as an infrastructure component apparently (`~tools.toolschecker/.kube/config`). The configuration file is not tracked in Puppet, there is no documentation about it and it was made immutable (`chattr +i`), which added to delays when fixing monitoring was the priority.

The alerts are mentioned [in our alerts documentation](#) but there is no explanation about how they work. There is also a page about the Toolforge nodes that says "TODO: fill me" about the checker nodes.

These kinds of little scripts with hardcoded settings seem very widespread in Toolforge. It's not clear what should be done about them since they power important infrastructure pieces like the port grabber, maintain-kubeusers and others. Until/if a solution can be reached to better organize all of this, one should be very careful making changes.

Usage of "tools.eqiad.wmflabs" and "tools.wmflabs.org" interchangeably

Quick Phabricator archeology shows that it was decided at some point to use "*.wmflabs.org" addresses for certain things. However, the internal names are used everywhere too. Added to this the fact we have split DNS, it adds to the confusion. Some could argue that the public "tools.wmflabs.org" domain should be used only for external-facing resources and the internal one "tools.wmflabs" for internal-facing resources. This is a common pattern in Toolforge and it would benefit from further simplification.

Mysterious networking issues

Although we faced similar networking issues in the past, we could not determine exactly where the issue was working this time. It could have been the switch but also the Nova network. We're migrating everything to the eqiad1-r region where we use Neutron networking instead of Nova. Without a specific action that fixed the issue and nothing in the logs that point to the root cause, it's hard to draw any conclusions.

Human error

As usual, there was a human error when it was decided that "k8s-master.tools.wmflabs.org" should be removed. That decision ignored the fact that we have split DNS resolution in Cloud VPS. ~~Had the engineer restricted~~

himself to only removing the floating IPs and not taking the extra step to remove the DNS entry, this issue would have been largely avoided (Split DNS resolution depends on the floating IP being associated to an instance so it knows to which instance IP it should point to when resolved internally. Removing all floating IPs was sufficient to break k8s-master.tools.wmflabs.org internally and thus the cluster would still be broken at some point). As the task was about the floating IPs themselves and not the DNS entry, concluding the DNS entry wasn't needed should have taken more careful analysis.

Actionables

- Improve documentation about Toolforge checker nodes ([T211199](#))
- Review *.tools.wmflabs.org usage in Toolforge ([T211200](#))
- Sort out only one ideal hiera mechanism for Cloud VPS ([T211029](#))
- Declutter errors in tools-k8s-master-01 ([T211202](#))

Category: [Incident documentation](#)

This page was last edited on 5 December 2018, at 15:37.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. See [Terms of Use](#) for details.

[Privacy policy](#) [About](#)
[Wikitech](#)

[Disclaimers](#) [Code of Conduct](#) [Developers](#) [Statistics](#) [Cookie statement](#) [Mobile view](#)

