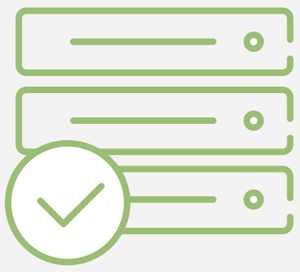
OPSERVE

Eindelijk zijn je servers in veilige handen



Installatie en configuratie

Beheer en monitoring

Veiligheid

www.opserve.nl

088 - 488 4444

contact@opserve.nl

OPSERVE

Waarom Opserve?

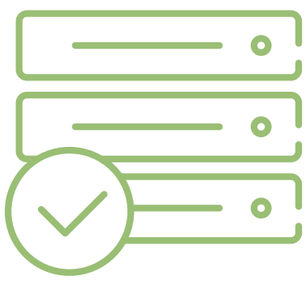
Een webbureau runnen is een hele onderneming. Als je dan ook de servers goed wilt managen, raakt je agenda nog voller. In de zoektocht naar hostingpartijen die begrijpen wat webbureaus nodig hebben bleven we met lege handen staan, dus zijn we zelf aan de slag gegaan. Wat bleek? Het is moeilijk, tijdrovend en heel intensief. Maar we slaagden in onze missie.

We hebben het installeren, configureren en beheren van software geautomatiseerd. Daarbij wordt een hele stack aan security maatregelen ingezet. Daarnaast handelen we proactief door servers te monitoren, updates uit te voeren en security news te volgen. Daardoor weten we waar de behoeften liggen en wanneer direct actie vereist is.

Wat kunnen we je bieden?

Installatie en configuratie

- Inrichten nieuwe servers
- Installatie en configuratie van extra software
- Server migraties
- Inrichten High Available clusters



Beheer en monitoring

- Overnemen beheer bestaande servers
- Actieve monitoring
- Optimalisaties
- Inregelen en controle van backups

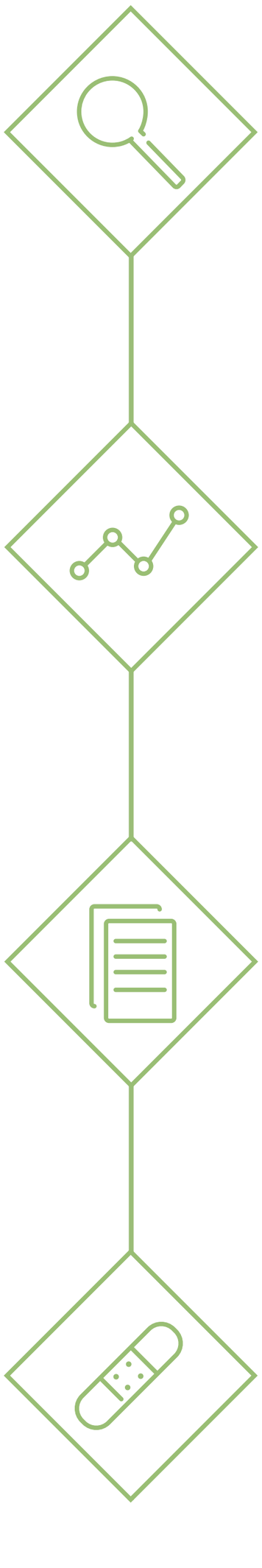
Veiligheid

- OS en software up to date brengen en houden
- Security hardening
- Incidentafhandeling
- Security audits

OPSERVE

Hoe we je helpen

Met een expert review, een gedegen plan en de juiste persoonlijke aanpak helpen we ook jou vooruit.



Expert review

Na de inventarisatie van je server. We beoordelen de aanwezige software en zorgen voor de juiste updates, controleren op security issues en brengen de server naar het gewenste veiligheidsniveau.

Server management

Het beheren van de servers bestaat uit vaste activiteiten. Dagelijks worden logs en backups gecontroleerd, iedere week voeren we beschikbare updates door en maandelijks voeren we een security audit uit.

Rapportage

Een keer per maand nemen we wat uitgebreider de tijd om de status van je server te bekijken. Op basis van informatie uit de monitoring, het dagelijks beheer en de ontwikkeling van het resourcegebruik stellen we een rapport voor je op.

Incidentafhandeling

Ondanks al onze preventieve maatregelen zijn incidenten niet uit te sluiten. Als er een incident optreedt, komen we direct in actie.

Expert review

We beginnen met een inventarisatie van je server. We beoordelen de aanwezige software en zorgen voor de juiste updates, controleren op security issues en brengen de server naar het gewenste veiligheidsniveau. We adviseren -indien nodig- aanpassingen en optimalisaties. Je server wordt ondergebracht in de monitoring, vanaf dat moment zien we continu hoe je server ervoor staat.

Basisactiviteiten intake

Onder de basisactiviteiten van het in beheer nemen van een bestaande server behoren:

- server inventarisatie
  - bepalen type OS en eventueel type virtualisatie
  - bepalen beschikbare hardware resources
  - inventarisatie van geïnstalleerde software
  - controleren of er handmatig geïnstalleerde software aanwezig is
  - controleren of er aangepaste configuratie is
  - controleren firewall, open en actieve poorten, insecure services
  - controle backup procedure
  - afstemmen eisen ten aanzien van firewall en users
- servers opnemen in monitoring- en alerting systemen van Opserve (Zabbix en Opsgenie)
- servers opnemen in het remote configuration management systeem (SaltStack) en centraal beheer instellen van configuratie van:
  - firewall (managed iptables of ConfigServer Firewall)
  - users
  - log controle (logwatch)
  - eventueel extra te installeren software
- OS en software in kaart en up-to-date brengen
  - updaten van alle componenten
  - servers opnemen in update notificatiesysteem
- reboot test: komen alle services automatisch op na een reboot
- security hardening
  - uitvoeren van een geautomatiseerde security audit
  - password based logins omzetten naar keybased logins
  - root toegang beperken
  - gebruikersrechten controleren en waar nodig beperken
  - brute force en anti-hack bescherming instellen (fail2ban, mod_security)
- inrichting lokale en remote backup

Rapportage

Na deze periode van circa 4 weken hebben we, mede vanuit de monitoringsystemen, voldoende informatie over het bezoekers patroon aan de websites/webapplicaties en het resourcegebruik van de servers. Met deze informatie stellen we een advies op over de servers:

- zijn er meer of minder hardware resources nodig?;
- volstaat eventuele virtualisatie, of is er bijvoorbeeld teveel overboeking?
- is er behoefte om webserver of database tuning uit te voeren?

Ook kunnen we optioneel advies geven ten aanzien van afzonderlijke websites:

- zou de website gebaat zijn met verhuizen een andere provider of locatie?
- zou inzet van een CDN nuttig zijn?
- zou inzet van externe DDoS protectie nuttig zijn?
- zou inzet van schaalbare infrastructuur nuttig zijn?

Als er uit de intake of de rapportage blijkt dat aanvullende wijzigingen geadviseerd worden, dan offreren we deze activiteiten of voeren we deze in overleg met de klant op nacalculatie uit.

OPSERVE

Server management

Het managen van de servers bestaat uit vaste activiteiten die op dagelijkse, wekelijkse en maandelijkse basis plaatsvinden. Daarnaast wordt er actief gehandeld bij incidenten. Een keer per maand nemen we wat uitgebreider de tijd om de status van je server te bekijken. Op basis van informatie uit de monitoring, het dagelijks beheer en de ontwikkeling van het resourcegebruik stellen we een rapport voor je op met conclusies van de afgelopen periode en adviezen voor de toekomst.

Dagelijks

Iedere dag worden deze controles uitgevoerd:

- controle log rapportages;
- controle gebande IP adressen, indien nodig instellen IP of URL whitelisting en doorgeven abuse melding;
- controle beschikbare updates, high risk/low impact updates direct doorvoeren;
- controle of backups zijn uitgevoerd.

Wekelijks

Op een vaste wekelijkse dag en tijdstip

- uitvoeren beschikbare updates, inclusief high impact updates (bijv. kernel, MySQL).

Maandelijks

Op een vaste dag in de maand:

- uitvoeren van een geautomatiseerde security audit;
- analyse ontwikkeling resourcegebruik;
- opstellen rapportage.

Afhandeling van incidenten

Ondanks al onze preventieve maatregelen zijn incidenten niet uit te sluiten. Als er een incident optreedt, leggen we ons werk opzij en komen we direct in actie. In nauwe samenwerking met jou, zodat we snel achter de oorzaak komen, het incident op kunnen lossen en verbeteringen voor de toekomst door kunnen voeren.

Een incident kan op verschillende manieren bekend worden:

- uit de monitoring- en notificatiesystemen;
- uit de dagelijkse controles;
- door een melding van de klant.

Als er een incident optreed dan verzorgen we een melding naar de klant. Op basis van de response van de klant kunnen we de volgende aanvullende activiteiten uitvoeren:

- (verdere) analyse van het incident;
- acties gericht op het verhelpen van het incident;
- tussentijdse updates aan de klant;
- alle benodigde communicatie met de hosting provider;
- een eindrapportage met analyse, uitgevoerde acties en verdere aanbevelingen.

OPSERVE

Additionele services

Naar aanleiding van de intake rapportage of op verzoek van de klant kunnen we bij zowel bestaande als nieuwe servers een aantal additionele activiteiten verzorgen, zoals bijvoorbeeld:

- Inrichten van nieuwe servers;
- Installeren of configureren van aanvullende software of panels;
- Upgrades naar nieuwe OS releases;
- Beheer van mailafhandeling en spamfiltering;
- Inrichting remote backup systemen
- DNS beheer;
- Migratie van websites of complete servers naar andere hostingproviders;
- Instellen SSL certificaten;
- Installeren en configureren van CMS security plugins;
- Verwijderen backdoors en hacks uit systemen;
- Instellen van applicatielog monitoring in SheepMonitor, NewRelic, Bugsnag of andere monitoring tools;
- Inrichten centrale ElasticSearch Logstash Kibana (ELK) logserver;
- Inrichten Malware scanning met bijvoorbeeld Wazuh;
- PageSpeed optimalisatie:
  - met behulp van Apache of Nginx modules (mod_pagespeed, mod_expires);
  - met behulp van Full Page Cache oplossingen (CMS geïntegreerd of extern);
  - advies over aanpassingen in de website.
- Inrichten van High Available en/of schaalbare infrastructuur;
- Inrichten software versiebeheer (bijv. Git via GitHub, Bitbucket of on premise);
- Inrichten Continuous Integration, Continuous Deployment;
- Geautomatiseerde functionele tests (van smoketest tot complete testsuite);
- Performance (load) tests;
- Penetration tests.

Service level

Opserve biedt 2 pakketten aan voor server management:

	Basis	Uitgebreid
Bereikbaarheid servicedesk	via webportal	via webportal
Telefonische bereikbaarheid voor melden incidenten	tussen 8:00 en 17:00, op werkdagen	tussen 7:00 en 24:00, 7 dagen per week
Ondersteuning tijden bij urgente incidenten	tussen 8:00 en 17:00 op werkdagen	tussen 7:00 en 24:00, 7 dagen per week
Ondersteuning tijden overige verzoeken	tussen 8:00 en 17:00 op werkdagen	tussen 8:00 en 17:00 op werkdagen
Prioriteit	Volgorde van binnenkomst	Voorrang
Eerste response tijdens kantooruren	Binnen 2 uur	Binnen 1 uur
Eerste response buiten kantooruren	n.v.t.	Binnen 1 uur
Actieve opvolging notificatie monitoring	tussen 8:00 en 17:00, op werkdagen	tussen 7:00 en 24:00, 7 dagen per week
Server updates	standaard wekelijks kritieke updates z.s.m.	standaard wekelijks kritieke updates z.s.m.
Controle logs en bans	dagelijks	dagelijks
Controle backups	actualiteit: dagelijks	actualiteit: dagelijks
Security audit (basis)	maandelijks	maandelijks
Security audit (uitgebreid)	optioneel	optioneel
Rapportage	maandelijks	maandelijks
Toegang tot monitoring	ja	ja
Maandelijkse kosten	€ 40 per server/VM	€ 65 per server/VM
Tarief afhandeling incidenten en additionele services tijdens kantooruren	€ 100 per uur	€ 100 per uur
Tarief afhandeling incidenten buiten kantooruren	n.v.t.	€ 145 per uur

OPSERVE

Enthousiast over ons?

We helpen je graag. Bel ons op 088 - 488 4444 of laat een terugbelverzoek achter via het formulier op onze website www.opserve.nl, dan bellen we je binnen twee werkdagen terug.