Service Level Agreement

Beschrijving van diensten LINFOSYS datacenter

Versie 1.1

Auteur:

Linfosys B.V.

Tijvoortsebaan 9a

5051 HJ Goirle

Inhoudsopgave

1. Afbakening en Terminologie

1.1 Afbakening

- Linfosys is verantwoordelijk voor de beschikbaarheid van de diensten geleverd vanuit het eigen datacenter.
- Linfosys is niet verantwoordelijk voor verstoring van dienstverlening buiten het eigen datacenter.
- De klant maakt verantwoord gebruik van de ter beschikking gestelde hostingruimte en volgt aanwijzingen voor verantwoord gebruik van Linfosys snel en adequaat op.

1.2 Terminologie

- Kantoortijden: Maandag tot en met vrijdag, 07:30u tot 18:00u, Nederlandse tijd, met uitzondering van officiële feestdagen.
- Service-uren: Maandag tot en met zondag, 00:00u tot 24:00u, Nederlandse tijd. Met uitzondering van 4 uur per week voor back-up en onderhoud (tijdschema tussen 22:00u tot 06:00u).
- Klant: De persoon of organisatie die de overeenkomst met Linfosys is aangegaan.
- Klant contact: De persoon of organisatie die voor de klant het aanspreekpunt is.
- Techneut: Gekwalificeerd technisch medewerker van Linfosys, die zelfstandig verstoringen kan verhelpen en toegang heeft tot het datacentrum.
- Retentie: uitdrukking van tijd waarin data terug gezet kan worden.
- Overmacht: Elke van de wil van partijen onafhankelijke c.q. onvoorzienbare omstandigheid, waardoor nakoming van de overeenkomst redelijkerwijs door de andere partij niet meer kan worden verlangd.
- Restitutie-eenheid: Bij downtime wordt gerekend in restitutie-eenheden (onder bepaalde condities).
- VLAN: Een virtueel gescheiden netwerk wat over dezelfde hardware communiceert als andere VLANs zonder dat de data bij elkaar kan komen.
- Storingsmelding: Er kan 24 uur per dag, 7 dagen per week een melding van een storing worden gedaan aan de dienstdoende techneut van Linfosys, middels de door Linfosys daarvoor ter beschikking gestelde tool.
- DDoS (aanval): Een aanval vanuit een groot aantal locaties/computers (botnet) met als doel een computernetwerk of dienst onbereikbaar te maken voor de gebruikers.
- Hacker: Iemand die inbreekt in computer systemen/websites.
- PKI: Een techniek om met digitale certificaten veilig en vertrouwd over het internet (of ander publiek netwerk) tussen servers te kunnen communiceren.
- SSL: Een techniek om met digitale certificaten veilig en vertrouwd met websites op het internet te kunnen communiceren.
- Fallback scenario: Een stappenplan om terug te kunnen keren naar de oude situatie wanneer er zich onvoorziene problemen voordoen tijdens onderhoud.
- Loadbalancer / loadbalancing: Het verdelen van belasting (load) over meerdere (identieke) servers.

- Netblock: Een set van IP adressen toegewezen aan een internet dienstverlener (provider).
- Ping: Een methode om te controleren of een IP adres/server bereikbaar is. Er wordt een klein pakketje naar de server gestuurd waar deze op dient te antwoorden.
- Traceroute: Een methode om te zien via welk route pakketten over het internet bij de ontvanger aankomen. Eventuele problemen met tussenliggende routers (knooppunten) kunnen zo in kaart gebracht worden.
- Anonymous FTP: Op een FTP server kunnen inloggen zonder een geldig account te hebben. Een gebruikersnaam en wachtwoord opgeven is dan niet nodig.

2. Beschikbaarheid

2.1 Downtime

Er is sprake van downtime als er meer dan 5 seconden geen verbinding gemaakt kan worden met minimaal één Cloud dienst server binnen het datacenter. Waarbij er wel een ping of traceroute reactie komt van de betreffende servers.

Er is geen sprake van downtime bij:
- Overmacht, zoals het uitvallen van stroom of netwerkverbindingen, DDoS aanvallen of andere hackeractiviteiten.
- Aangekondigd en afgesproken onderhoud.
- Spoedonderhoud noodzakelijk voor veiligheid en stabiliteit.

Tijdens service-uren
- 0,1% downtime per maand tijdens service-uren betekent dat de SLA niet gehaald is. Downtime wordt per maand berekend.

2.2 Aanspraak

De klant komt in aanmerking voor restitutie voor downtime mits deze aannemelijk maakt dat Linfosys de prestatieafspraken niet heeft gehaald. Bij verschil van mening zal de klant screenshots aanleveren die aantonen dat (a) het netblock van Linfosys bereikbaar is, en (b) het platform van Linfosys geheel of gedeeltelijk onbereikbaar is. Eindklant en partner hebben het recht om de overeenkomst per direct te beëindigen wanneer Linfosys een lagere beschikbaarheid heeft dan 99,9% uptime gedurende een maand.
Indien de gestelde eisen niet worden gehaald, vergoedt Linfosys 100% van de maandsom. De totale restitutie in een maand kan nooit meer zijn dan de maandsom voor het betreffende pakket waarbij de SLA is afgesloten.

3. Incidentmelding en response

- Indien de klant een storing ontdekt die downtime veroorzaakt, meldt deze dat aan Linfosys.
- Tijdens kantooruren: per e-mail en kantoortelefoon (tenzij de storing al op de site vermeld is).
- Buiten kantooruren: door een e-mail naar support@linfosys.nl
- Linfosys geeft tijdens kantooruren binnen 1 uur terugkoppeling aan de incidentmelder.
- Tijdens service -uren ontvangt de dienstdoende technicus meldingen van het monitoringsysteem.

4. Beveiliging

4.1 Dataveiligheid

- De bestanden staan altijd op een Fouttolerant systeem. Een dergelijk systeem zorgt er voor dat het uitvallen van een harde schijf geen dataverlies oplevert.
- In het datacentrum is noodstroomvoorziening aanwezig.
- De netwerkapparatuur en kabels zijn redundant uitgevoerd.
- Elke 24 uur wordt een kopie van de back-up van de database en files opgeslagen in een secundair datacenter.

4.2 Back-up

Alle Cloud diensten van Linfosys hebben het volgende back-up schema:

- Tot 7 dagen terug: 1 per dag (7 back-ups).
- Tot 30 dagen terug: 1 per week (3 back-ups).

Bestanden welke opgeslagen worden via Online Werkplekken en Online back-up hebben een retentie tijd van 365 dagen.

5. Privacy

- Het datacenter is alleen toegankelijk voor geautoriseerde medewerkers van Linfosys.
- De back-ups zijn alleen toegankelijk voor geautoriseerde medewerkers van Linfosys en de technisch beheerder van het hostingpakket.
- Medewerkers van Linfosys hebben een geheimhoudingsplicht met betrekking tot alle informatie en welke is opgeslagen in ons datacenter.
- Afgeschreven harde schijven worden na gebruik vernietigd door een daarvoor gecertificeerd bedrijf.

6. Beveiliging en onderhoud

Linfosys verplicht zich preventieve activiteiten te ondernemen die de kans op beveiligingsincidenten verkleinen.

6.1 Preventieve activiteiten

Linfosys voert verschillende preventieve activiteiten uit, waaronder, maar niet beperkt tot: scannen op slecht beveiligde software, scannen op verdachte activiteiten, periodiek updaten van softwarecomponenten.

6.2 Updaten software

Linfosys voert bij het uitkomen van nieuwe versies van software een risico analyse uit van de risico's, data integriteit en continuïteit voor het datacenter. Onderhoud wordt buiten kantoor-uren gedaan. Onderhoudswerkzaamheden leveren maximaal 16 uur per maand downtime op buiten kantoor-uren, deze tellen niet mee als downtime. Voor ieder onderhoud wordt van tevoren een fallback scenario uitgewerkt.

6.3 Onderhoud

Onderhoud gebeurt buiten kantoor-uren, tenzij de ingeschatte impact voor klanten minimaal of nihil is, dan kan onderhoud tijdens kantoor-uren plaatsvinden.

6.4 Spoedonderhoud

Linfosys moet ten behoeve van de stabiliteit van het gehele datacenter mogelijk spoedonderhoud uitvoeren, bijvoorbeeld in geval van publicatie van urgente veiligheidsproblemen. Vermindering van dienstverlening of downtime als gevolg van dit spoedonderhoud vallen niet onder de gemeten downtime.

Spoedonderhoud wordt indien mogelijk buiten kantoor-uren gedaan, maar indien noodzakelijk ook tijdens productie-uren. Spoedonderhoud zal altijd worden toegelicht via e-mail.

6.5 Groot onderhoud

Implementatie van software met significante functionaliteitswijzigingen, wordt van te voren aangekondigd via e-mail. Indien mogelijk en wenselijk wordt de nieuwe software middels een testplatform aangeboden. Belangrijke versiewijzigingen worden minimaal 30 dagen van tevoren aangekondigd.

6.6 Beveiliging: Technische maatregelen

- Alle administratieve handelingen worden uitgevoerd over versleutelde (SSL) verbindingen.
- Alle beheer handelingen worden uitgevoerd over een eigen VLAN (management VLAN).
- Back-ups worden gedaan over een eigen VLAN (storage VLAN).
- Authenticatie tussen servers onderling gebeurt op basis van PKI.
- Klantwachtwoorden worden door ons opgeslagen in een eigen password systeem welke enkel intern gebruikt kan worden.
- Onze database servers zijn niet rechtstreeks gekoppeld aan het internet en worden beschermd door een NextGen Firewall.
- Iedere bij ons gehoste site draait met afzonderlijke proces en eigendomsrechten. Hierdoor zijn de applicaties en data van onze klanten strikt gescheiden. Mocht een hacker er in slagen in te breken op de applicatie van een individuele klant, dan geeft dit geen risico voor onze overige klanten.

7. Beveiliging: Procedurele maatregelen

- Wij houden nauwgezet publicaties van beveiligingslekken in de gaten. Op basis van een interne richtlijn wordt de kans op exploitatie, impact van misbruik en functionele impact van de oplossing ingeschat. Zijn zowel impact van misbruik als kans op exploitatie hoog, dan wordt het lek direct gedicht. Is dit niet het geval en heeft de implementatie van een fix mogelijk functionele consequenties voor de toepassingen van onze klanten, dan wordt de implementatie gepland voor het volgende onderhoudsvenster en wordt een aankondiging rondgestuurd naar onze klanten.
- Onze systeemwachtwoorden veranderen iedere zes maanden of na afscheid van technische medewerkers.
- Voor iedere mutatie van site, e-mail en klantgegevens en domeineigendom vereisen we authenticatie met behulp van een wachtwoord of een schriftelijk en ondertekend bewijs van goedkeuring. Hier zijn we bijzonder streng in, aangezien dit de enige manier is om social engineering (manipulatie van onze medewerkers teneinde een wachtwoord te bemachtigen) te voorkomen.
- Wij scannen proactief op verouderde software. Hierdoor kunnen we onze klanten waarschuwen indien zij lekke (verouderde) applicaties hebben geïnstalleerd die mogelijk kunnen worden misbruikt voor het versturen van spam of het verhullen van de identiteit van een hacker.

7.1 Praktische maatregelen

Linfosys heeft ook een aantal praktische maatregelen ingevoerd om de beveiliging aan te scherpen.

- Anonymous FTP is uitgeschakeld. Vanwege de reputatie van FTP services op beveiligingsgebied, hebben we ervoor gekozen om preventief de FTP services op een geïsoleerd cluster onder te brengen. Daarnaast is alleen toegang met wachtwoordauthenticatie toegestaan (wachtwoorden worden m.b.v. MD5 hashes opgeslagen). Een extra maatregel is het aanbieden van versleutelde FTP (TLS) verbindingen, zodat files en inlogcodes niet kunnen worden afgeluisterd ("gesniffed")
- Op alle servers zijn overbodige diensten uitgeschakeld. Daarnaast wordt aan de rand van ons netwerk al het inkomende en uitgaande verkeer gefilterd door een redundante firewall. Alleen noodzakelijk verkeer (web, mail, ftp) wordt doorgelaten naar bepaalde servers.
- Administratieve databases zijn volledig afgeschermd van de buitenwereld.
- Klantspecifieke databases zijn op verzoek te benaderen van buiten het Linfosys netwerk.

8. Monitoring en support

8.1 Monitoring

Alle servers en applicaties worden gemeten op generieke en specifieke eigenschappen. Generieke eigenschappen zijn basiseigenschappen van elke server. Specifieke eigenschappen zijn afhankelijk van de functie van de server (DBserver, Webserver, Terminal Server, Exchange Server etc.)

Algemeen: CPU, RAM, Diskruimte, Ping, Processen
Specifiek: IIS, MySQL, SQL, Exchange

Metingen worden elke 5 minuten gedaan. Verstoringen van diensten worden primair direct doorgestuurd naar tenminste 1 technicus en na 15 minuten naar tenminste 2 technici. Buiten productie-uren wordt het uitvallen van een server gemeld aan tenminste 1 technicus en na 15 minuten naar tenminste 2.

Het monitoringsysteem zelf wordt gemonitord vanuit een secundair datacentrum en daarnaast door een externe provider. In het datacentrum wordt actief gecontroleerd op stroomvoorziening en temperatuur.
Het datacentrum is uitgerust met brandblusapparaten.

8.2 Support

De klant heeft recht op telefonische en e-mail support tijdens kantooruren. Klant specifieke applicaties hebben een eigen SLA.

9. Communicatie

9.1 Definities incidenten

- Klein incident:downtime verwacht 0-30 minuten, voor alle klanten.
- Groot incident: downtime verwacht 30+ minuten, of mogelijk dataverlies, voor ????

9.2 Follow-up klein incident

Melden op site www.Linfosysnoc.nl.

- Tijdens kantooruren binnen 1 uur een notificatie (wie, wat).
- Buiten kantooruren binnen 4 uur een notificatie (wie, wat).

9.3 Follow-up groot incident

- Melden op site www.Linfosysnoc.nl.
  - Tijdens kantooruren binnen 1 uur een notificatie (wie, wat).
  - Buiten kantooruren binnen 4 uur een notificatie (wie, wat).
- Planning en alternatieven worden binnen 2 uur tijdens kantooruren, en binnen 6 uur buiten kantooruren op www.Linfosys.nl vermeld.