KRONOS®

Technisch Document

Kronos Workforce Central in de Cloud

INLEIDING

Kronos® oplossingen voor personeelsmanagement bieden de volledige automatisering en hoogwaardige informatie die nodig zijn om uw arbeidskosten te beheersen, uw compliance risico te beperken en de productiviteit van uw personeel te verbeteren. Maar uw Kronos-oplossing kan alleen van blijvende waarde zijn als deze beschikbaar is en correct beheerd wordt. Daarom kiezen meer en meer klanten ervoor om Kronos in de Cloud te gebruiken voor hun oplossingen voor personeelsmanagement.

We kunnen uw oplossing voor personeelsmanagement in onze private cloud beheren, waar gebruikers op elk moment en waar dan ook via internet toegang hebben tot de applicatie(s). U hebt 24 uur per dag, 7 dagen per week toegang tot uw oplossing zonder aanschaf van extra hardware, besturingssystemen of RDBMS-licenties. U kunt eveneens gerust zijn, wetende dat ervaren technische consultants van Kronos uw applicaties en werknemersgegevens beheren. Het is de ideale keuze voor organisaties die hun doelen voor personeelsmanagement willen bereiken zonder hun budgetten voor bedrijfskapitaal te overschrijden of hun IT-personeel te veel te belasten.

Kronos biedt uitgebreid onderhoud en ondersteuning voor uw oplossing voor personeelsmanagement, waaronder volledige ondersteuning van de IT-infrastructuur inclusief de server hardware, besturingssystemen en databasesystemen die nodig zijn om uw Kronos applicatie(s) in de Kronos Cloud draaien:

- Serverbeveiliging en -beheer
- Installatie van Service Packs
- Installatie van updates m.b.t. wetgeving
- Installatie van softwareversies
- Dagelijkse back-up van systeem en data
- Gegarandeerde service level agreement (SLA) van 99,75 procent

Bij de evaluatie van Cloud diensten van verkopers moet u ervan uit kunnen gaan dat uw applicatie(s) en database onderhouden worden in een data center van wereldklasse, ontworpen voor meerdere niveaus van beveiliging en redundantie en met een gegarandeerde maximale beschikbaarheid van uw oplossing voor personeelsmanagement. Met dit document willen we de infrastructuur, diensten, processen en het beleid achter de Kronos Cloud beschrijven, met inbegrip van:

- Specificaties van het data center betreffende fysieke infrastructuur, netwerkconnectiviteit, datacommunicaties, beveiliging en meer
- Back-up van het systeem en recovery proces
- Veiligheidsbeleid en controlemaatregelen
- Change control
- Integratie met klantgegevens en applicatieomgeving
- Beleid en beheer m.b.t. service level agreement
- Certificeringen en accreditaties
- Technische ondersteuning

CLOUDAANBOD – KRONOS® WORKFORCE CENTRAL®

Het onderstaande is van toepassing op single-tenant applicaties in de Kronos Cloud.

Cloudaanbod	
Omgevingen: Een standaard productie- en een ontwikkelings-(niet-productie-) omgeving.	Inbegrepen; meer niet-productieomgevingen zijn beschikbaar tegen meerprijs
Herstel van de omgeving: Eenmaal per week herstel van productie naar een niet-productieomgeving.	Inbegrepen; voor frequenter herstel of extra omgevingen moet een vergoeding voor time & material worden betaald
Connectiviteit met de dienst: Gebruikers van de klant roepen de applicatie op via een beveiligde verbinding via internet. Samenwerking met IT-personeel van de klant kan vereist zijn om toegang mogelijk te maken. Kronos assisteert bij de controle van de connectiviteit met de site, maar is niet verantwoordelijk voor de internetverbinding of ISP-relaties van de klant. Kronos-gerelateerd internetverkeer kan niet worden gefilterd door proxy- of caching-apparaten op het netwerk van de klant. Exclusions moeten worden toegevoegd voor de volledig gekwalificeerde domeinnamen en openbare IP-adressen die aan de omgevingen worden toegewezen.	Inbegrepen
Terminal geïnitieerde verbinding: In de communicatiemodus waarbij de terminal de verbinding initieert, start de Kronos-terminal alle communicatie met de server in Kronos Cloud via internet. Voor deze modus moet de klant poort 443 openen voor uitgaand verkeer. Alle Kronos 4500™-terminals verzonden na februari 2008 met firmwareversie 3.0 of hoger en alle InTouch™-terminals kunnen deze communicatiewijze gebruiken. Hieronder vallen onderdeelnummers 8602800-500 tot en met 8602800-899 van de terminal. In gevallen waar vertaling van het netwerkadres voor terminals vereist is, is de klant verantwoordelijk voor het toepassen van de vertalingen op zijn netwerk.	Inbegrepen
Toegang op afstand tot niet-webapplicaties: Toegang op afstand tot niet-webapplicaties (bijv., Kronos Workforce Integration Manager™) met gebruik van een hulpmiddel voor toegang op afstand zoals een Citrix®-ontvanger. Een aantal Kronos-applicaties vereisen het gebruik van deze accounts voor toegang op afstand.	Twee (2) gebruikers met naam inbegrepen
SFTP accounts: Geleverd aan de klant om bestanden naar de Kronos Cloud op te laden en bestanden uit de Kronos Cloud te downloaden voor bepaalde integratiepunten (bijv. input-/outputmappen voor Kronos Workforce Integration Manager). Deze locatie is niet ontworpen voor opslag op lange termijn en bestanden kunnen 30 dagen na aanmaak worden verwijderd.	Twee (2) logins inbegrepen
Beheer van besturingssysteem en databasesoftware: bevat toepassing van kritische beveiligingspatches, servicepakketten en hot fixes; onderhoud van servers.	Inbegrepen
Serveronderhoud: Reparatie en vervanging van defecte of falende hardware en de installatie van upgrades van hardware.	Inbegrepen
Updates van applicaties: Service Packs voor de applicatie, updates m.b.t. wetgeving (indien van toepassing), point releases en upgrades.	Inbegrepen
Back-up: Van de klantgegevens wordt dagelijks een back-up gemaakt. Gegevens van de database worden via versleutelde verbindingen gekopieerd naar een tweede Kronos Cloud-data center. Gedurende de eerste 28 dagen worden back-ups op rotatiebasis bewaard. Alle historische werknemers- en configuratiegegevens worden in de roterende back-ups opgeslagen.	Inbegrepen

WORKFORCE CENTRAL UPGRADEDIENSTEN

Bevat diensten voor Kronos voor het uitvoeren van taken om point releases en upgrades toe te passen op Kronos-applicaties van klanten in de Kronos Cloud. De diensten zijn beperkt tot het toepassen van de updates op de applicaties.

In de tabel hieronder zijn de inbegrepen upgradetaken weergegeven.

Projectcoördinatie: projectmanager voor coördinatie van het upgradeproject • Tot acht wekelijkse statusgesprekken van 30 minuten (één per week) • Kronos resources coördineren • Uitnodigingen voor vergaderingen verzenden • Tijdlijn voor het project en verwachte betrokkenheid van de klant bij de start van het project leveren • Initieel projectschema leveren en voortgang communiceren tijdens wekelijkse statusgesprekken • Communicatieplan en lijst met contactpersonen leveren	Inbegrepen
Planningsfase	
Inleidend gesprek tussen klant en Kronos – maximaal een uur.	Inbegrepen
Beoordeling van technische geschiktheid en architectuur – Kronos Cloud-omgeving	Inbegrepen
Assessment fase	
Evaluatie van de upgrade van de interface.	Inbegrepen
Evaluatie van nieuwe functies of wijzigingen in de configuratie.	Niet inbegrepen
Evaluatie van aangepaste rapporten en bijbehorende ontwikkelingsactiviteiten.	Niet inbegrepen
Upgrade/bouwfase van de oplossing	
Eén (1) herstel van productiedatabase naar pre-productieomgeving met als doel het testen van de upgrade. Voor extra herstel, indien gewenst, wordt een vergoeding voor extra time & material berekend.	Inbegrepen
Upgrade van niet-productie- en productieomgeving naar nieuwe point release of versie.	Inbegrepen
Upgrade van Workforce Integration Manager-interfaces vanwege productwijzigingen als onderdeel van de technische upgrade beschreven in de productdocumentatie. Voor Workforce Central 8 bestaat dit onder andere uit XML export/importen en database-views zoals beschreven in de “Workforce Central Import User Guide” en de “Workforce Central Data View Reference Guide.”	Inbegrepen
Upgrade van niet-WIM-interfaces in niet-productieomgeving en productieomgeving.	Niet inbegrepen
Upgrade van aangepaste rapporten. Dit bestaat onder andere uit een upgrade van Workforce Integration Manager-interfaces, die batchfunctionaliteit voor tabelimport gebruiken, direct naar databasetabellen lezen/schrijven of wijzigingen vereisen vanwege nieuwe/gewijzigde eisen van de klant.	Niet inbegrepen
Upgrade van interfaces en rapporten aangemaakt of geleverd door de klant.	Niet inbegrepen
Update van firmware van de terminal beheerd door Kronos.	Niet inbegrepen
Configuratie van nieuwe features of functies of wijzigingen van bestaande configuratie.	Beschikbaar voor aankoop
Test- en certificeringsfase	
Systeemtest van geüpgrade omgevingen door test of een gebruiker zich kan aanmelden.	Inbegrepen
Testen van gebruikersacceptatie van geüpgrade omgevingen, interfaces, aangepaste rapporten, nieuwe features, etc.	Niet inbegrepen
Ontwikkeling van klant specifieke testcases.	Niet inbegrepen
Aftekenen van geüpgrade niet-productie- en productieomgevingen.	Klant
Fase van implementatie en ondersteuning	
Gesprek over gereedheid voor implementatie – maximaal een uur.	Inbegrepen

Gelieve er rekening mee te houden dat configuratie van nieuwe features, diensten voor projectbeheer en overige professionele, beheerde en educatieve diensten en training niet onder de Upgradediensten vallen. Indien gewenst kunnen deze apart worden aangekocht.

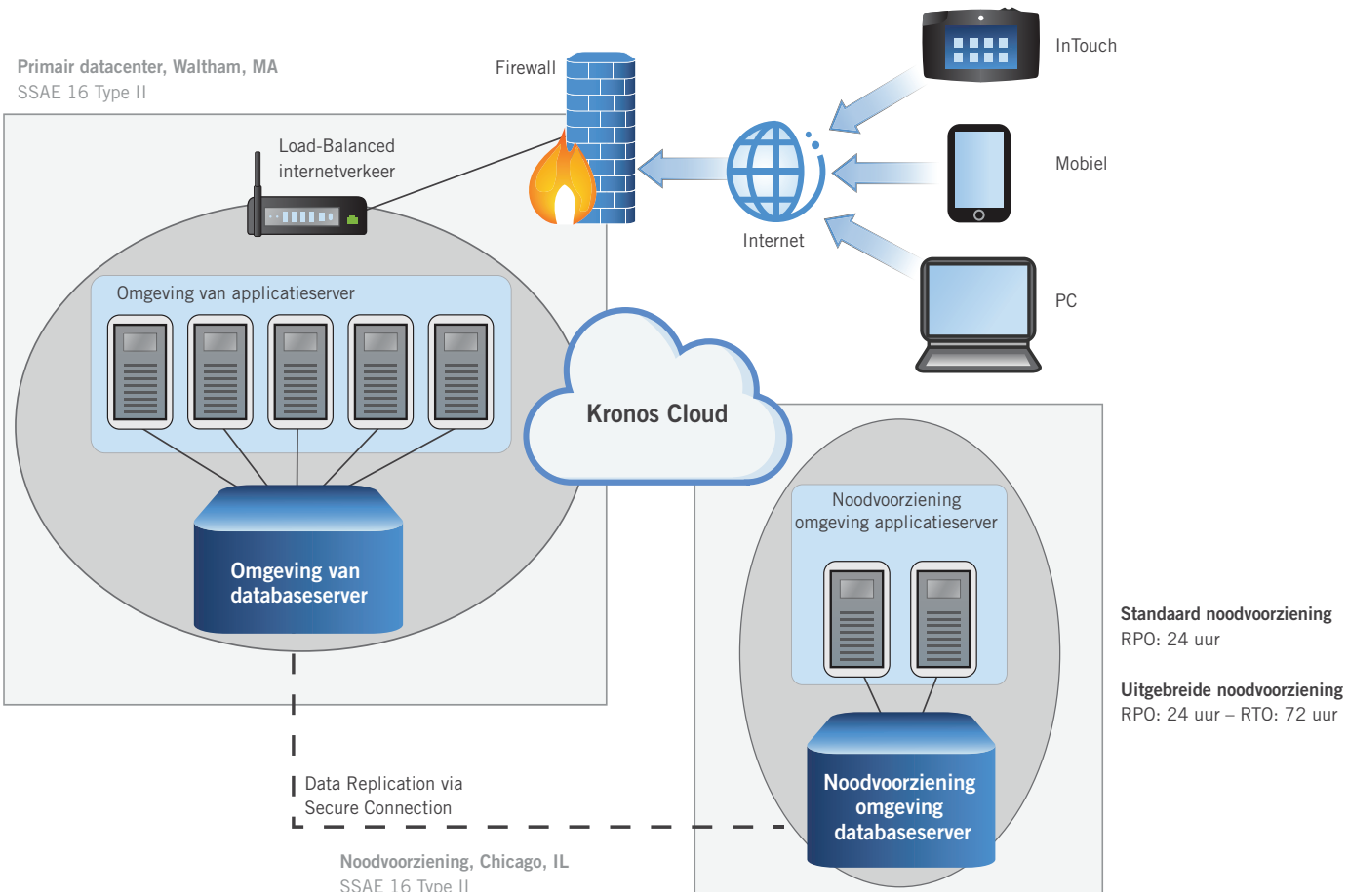
De projectcoördinatie duurt maximaal acht weken. Aan het einde van deze periode rondt Kronos de productie-upgrade af. Als Kronos om welke reden ook de technische upgradestappen niet binnen acht weken kan uitvoeren vanwege een door Kronos veroorzaakte vertraging, dan wordt de projectcoördinatie evenredig voortgezet om de door Kronos veroorzaakte vertraging goed te maken. Als Kronos bijvoorbeeld een vertraging van twee weken veroorzaakt omdat resources van Kronos niet beschikbaar zijn, dan zal de projectcoördinatie niet langer dan 10 weken duren.

Tenzij specifiek vermeld, dient de klant verantwoordelijkheid te nemen voor de taak en/of het af te leveren product.

OVERZICHT VAN HET DATACENTER

ONTWERP VAN ARCHITECTUUR/SYSTEEM:

De Kronos Cloud datacenters in Waltham, Massachusetts en in Chicago, Illinois, bieden faciliteiten van wereldklasse voor stroombeheer, verwarming/ventilatie/airconditioning (HVAC), branddetectie en -bestrijding, fysieke beveiliging en Tier 1-internetconnectiviteit. De faciliteit is ontworpen om te voldoen aan de strenge eisen van klanten, die de hoogste beschikbaarheid van kritieke IT-assets eisen, waaronder applicaties en gegevens voor personeelsmanagement. De omgevingscondities worden streng gemonitord en gecontroleerd.



DATASTROOM CLOUD:

Soort data	Methode datastroom
Terminalverkeer	Initieel certificaat via poort 444 (beveiligde HTTP/TLS). Lopende communicatie is door apparaat geïnitieerd via poort 443.
Internetverkeer eindgebruiker	Al het verkeer loopt via beveiligde HTTP (TLS) via internet en direct door de centrale infrastructuur van Kronos (waaronder firewalls, routers en switches in eigendom en onder beheer van Kronos).
Batchinterfaces	Uitgaande en binnenkomende interfaces met klant worden geïnitieerd door de klant en beveiligd verzonden via SFTP. Optioneel kan PGP-versleuteling worden geïmplementeerd tegen meerprijs.
XML-API interfaces	HTTPS (TLS)
Ontwikkeling van interfaces en rapporten	HTTPS (TLS)
Wijze van authenticatie	Één van drie methoden: Native applicatie authenticatie; LDAPS-authenticatie; single sign-on op basis van SAML 2.0.
Uitgaand-geïnitieerde sessies	Niet toegestaan.
Directe toegang tot database	Alleen lezen. ODBC-toegangsdiensten beschikbaar tegen meerprijs.

ONDERHOUDSPERIODEN:

Kronos stelt geplande onderhoudsperioden vast, waarin de diensten indien nodig worden onderhouden en bijgewerkt. Tijdens deze onderhoudsperioden beschikt Kronos over de diensten om periodieke onderhoudsdiensten uit te voeren, waaronder belangrijke software-updates. Kronos zal tijdens de onderhoudsperioden al het commercieel redelijke doen om de diensten beschikbaar te stellen voor de klant. Als Kronos verwacht een wijziging te implementeren, wordt u van tevoren op de hoogte gesteld van dit geplande werk. Kronos zal alles in het werk stellen om vijf (5) werkdagen vooraf een melding te verzenden. In een dergelijke melding wordt u geïnformeerd, of de onderhoudsactiviteiten voor een onderbreking van de dienst zullen zorgen. Hoewel de wijziging tijdens de onderhoudsperiode zal worden uitgevoerd, kan de timing afhangen van de onderhoudsitems.

Momenteel zijn de geplande onderhoudsperioden voor de diensten:

Maandag tot en met vrijdag	8:00 a.m. – 5:00 p.m. (U.S. ET) voor kleine wijzigingen in de productie- en niet-productieomgevingen.
Maandag tot en met vrijdag	4:00 a.m. – 6:00 a.m. (U.S. ET) voor dagelijks geplande wijzigingen.
Zaterdag en zondag	Middernacht – 6:00 a.m. (U.S. ET) voor grotere en langere geplande wijzigingen.

Onder de onderhoudsperioden vallen ook die perioden, die in onderling overleg door de klant en Kronos overeengekomen zijn.

ONDERHOUD:

Kronos onderhoudt de apparatuur die specifiek betrekking heeft op uw Kronos-oplossing voor personeelsmanagement om hoge beschikbaarheid te garanderen. Daarnaast bieden we 24 uur per dag, 7 dagen in de week observatie van netwerkcommunicatie, schijfruimte op de server, CPU-gebruik en andere factoren, die een aanzienlijke impact op uw oplossing en dus op de ervaring van de eindgebruiker kunnen hebben.

Kronos biedt ook onderhoudsdiensten met betrekking tot de software. We installeren applicatie-updates, servicepakketten, nieuwe softwareversies en updates m.b.t. wetgeving (indien van toepassing), zodat u kunt profiteren van de nieuwste softwarefuncties en -uitbreidingen, terwijl u uw compliance risico zo beperkt mogelijk houdt.

Om uitzonderlijke service en permanente klanttevredenheid te garanderen, is aan elke organisatie in de Kronos Cloud een ervaren en zeer snel reagerende Cloud Customer Manager toegewezen, die:

- Als de eerste contactpersoon van Kronos voor de klant dient voor niet-technische cloud-based initiatieven, zodra de klant live in de Kronos Cloud is.
- Regelmatig proactief contact opneemt met klanten om ze te informeren over servicepakketten, updates m.b.t. wetgeving en overige belangrijke updates van systeemapplicaties
- Rapportages levert over SLA-beschikbaarheid, analyses van onderliggende oorzaken en indien nodig documenten over de respons op voorvallen

AANVULLEND AANBOD AAN CLOUDDIENSTEN

Kronos Cloud-klanten hebben de mogelijkheid om aanvullende applicatiediensten te kopen. Met het configuratieaanbod voor applicaties zal Kronos op kwartaalbasis een vooraf vastgesteld aantal wijzigingen in uw bestaande configuratie uitvoeren, testen, vastleggen en implementeren, waaronder interfaces, Workforce Genies®, HyperFinds™ en arbeidsniveaus. Het aantal inbegrepen configuratiewijzigingen kan na verloop van tijd toenemen. Zo kan rekening worden gehouden met toenames in het aantal werknemers en met de toegenomen complexiteit van de configuratie.

BACK-UP VAN HET SYSTEEM EN HERSTELPROCESSEN

Kronos voert wekelijks een volledige en dagelijks een oplopende back-up uit van applicaties en gegevens van de klant. Alle gegevens van de database worden via beveiligde verbindingen gekopieerd naar een secundaire Kronos Cloud-omgeving in een ander datacenter. Gedurende de eerste 28 dagen worden back-ups bewaard. Kronos voert formele tests uit op kwartaalbasis om er zeker van te zijn dat de infrastructuur van de back-up succesvol is en dat de gegevens hersteld kunnen worden.

OPTIONELE UITGEBREIDE NOODVOORZIENING

De dienst Uitgebreide Noodvoorziening biedt klanten een DR-omgeving in een secundaire Kronos Private Cloud-faciliteit (KPC). De configuratiebestanden en -gegevens van de applicatie van de klant worden naar deze faciliteit gekopieerd. Deze DR-dienst heeft een recovery time objective (hersteltijd doelstelling, RTO) van 72 uur en een recovery point objective (herstelpunt doelstelling, RPO) van 24 uur. Deze DR-omgeving bevat geen niet-productie instanties, Workforce Analytics™, Workforce Record Manager™ of telefonie-oplossingen.

De diensten bestaan uit:

- Implementatie van het DR-systeem in de Kronos-noodvoorziening
- Configuratie van back-up(s) van data en replicatie van het primaire datacenter naar de DR-locatie
- Mogelijk maken van de replicatie van het primaire systeem van de klant naar de DR-locatie

In het onwaarschijnlijke geval dat Kronos een noodgeval uitroept in het primaire datacenter, zal Kronos dit melden aan de klant en de noodzakelijke DR-stappen nemen om de beschikbaarheid van de applicatie binnen de vastgestelde RTO te herstellen.

VEILIGHEIDSBELEID EN PROCESSEN

Bij Kronos is veiligheid van gegevens een topprioriteit. Onze corporate security officer is de speciale vertegenwoordiger van het management, die verantwoordelijk is voor de implementatie van beleid en procedures om de personeelsgegevens van de klant te beveiligen en te waarborgen. Werknemers die op afstand toegang willen tot de private cloud van de klant, moeten een two-factor authenticatie doorlopen om toegang te verkrijgen tot de omgeving. Fysieke en logische toegang tot de Cloud omgeving is beperkt tot bevoegde werknemers gebaseerd op hun rol in het bedrijf. Toegang met privileges is verder beperkt tot een subgroep van bevoegde werknemers, zoals systeembeheerders, en logische toegang wordt verleend met een gebruikers-ID met naam en een uniek, complex wachtwoord.

Om ons streven naar veiligheid te versterken, moeten werknemers van Kronos binnen 60 dagen na indiensttreding en vervolgens jaarlijks een training in bewustwording van veiligheid en privacy volgen.

Kronos onderhoudt een hostingomgeving die door een onafhankelijke auditor getest wordt op basis van de American Institute of Certified Public Accountants SSAE 16 (i.e., SOC 1) en de AICPA Principes van Vertrouwensdiensten Paragraaf 100a, Vertrouwensdiensten voor Veiligheid, Beschikbaarheid, Procesintegriteit, Vertrouwelijkheid en Privacy (i.e., SOC 2). De Kronos Private Cloud wordt door de onafhankelijke auditor beoordeeld op de principes van veiligheid, beschikbaarheid en vertrouwelijkheid. De Kronos Private Cloud bevindt zich in datacenters, die gecontroleerd worden op basis van SSAE 16. Toegang voor beheer van de KPC is beperkt tot geautoriseerd ondersteunend personeel van Kronos en tot integraties, die door de klant goedgekeurd zijn. De veiligheidsarchitectuur is ontworpen om de logische toegang tot de KPC te controleren en zo te voldoen aan de Principes van Vertrouwensdiensten van Veiligheid, Beschikbaarheid en Vertrouwelijkheid. De applicaties bieden de klant de mogelijkheid om de veiligheid en de logische toegang van de applicatie te configureren volgens de bedrijfsprocessen van de klant.

De klant stemt erin toe geen gegevens van betaalkaarten te uploaden, aangezien de dienst niet gecertificeerd is voor PCI DSS. De klant stemt erin toe geen informatie over de gezondheid te uploaden die onder HIPAA valt.

TOEGANG VOOR DE KLANT

Klanten hebben toegang tot de Kronos-webapplicatie via versleutelde TLS-sessies. De applicatie biedt de klant de mogelijkheid om de veiligheid en de logische toegang van de applicatie te configureren volgens het bedrijfsproces van de klant. Als de klant een probleem vaststelt met betrekking tot veiligheid, beschikbaarheid of vertrouwelijkheid van de gegevens of het systeem, meldt de klant dit aan Kronos.

Wellicht moet de klant bestanden verzenden om gegevens van de Kronos-applicatie in te voeren of op te roepen. Bestanden worden met behulp van SFTP naar de applicatieserver van de klant verzonden of hieruit opgeroepen. Daarnaast heeft elke klant een gebruikersnaam met een unieke naam en een bijbehorend wachtwoord.

TOEGANG VOOR BEHEER DOOR KRONOS

Toegang voor beheer van de omgeving is beperkt tot geautoriseerd ondersteunend personeel van Kronos en tot integraties die door de klant goedgekeurd zijn.

Transfers van gegevens tussen de klant en zijn Cloud omgeving worden mogelijk gemaakt door een gecentraliseerde, beveiligde oplossing voor transfers van bestanden. Deze oplossing biedt een versleutelde verzending en logging van alle bestanden, die naar of uit een klantomgeving worden verzonden.

Kronos voert continue monitoring uit in de Cloud omgeving.

CHANGE CONTROL

Kronos heeft een formeel proces ingesteld, ondersteund door geautomatiseerde hulpmiddelen en systemen, om ervoor te zorgen dat de planning, uitvoering en opvolging van wijzigingen op een gecontroleerde en gecoördineerde manier verlopen. Zo moeten onderbrekingen van Cloud diensten tot een minimum worden beperkt en een tijdig change management voor klanten worden gewaarborgd.

Het Kronos Change Control-team ontvangt aanvragen voor wijzigingen uit twee bronnen: Cloud Customer Managers en Kronos Global Support. Uw Cloud Customer Manager coördineert alle geplande wijzigingen, waaronder de installatie van nieuwe softwareversies, puntreleases en updates m.b.t. wetgeving met onze Kronos Cloud-consultants. Kronos Global Support kan tijdens het oplossen van een probleem van een klant ook op ongeplande wijzigingen stuiten, die direct behandeld moeten worden om het probleem op te lossen.

Zodra een verzoek tot wijziging ingediend is bij het Change Control-team, worden alle geplande en ongeplande wijzigingen ingedeeld als minder belangrijk, standaard, belangrijk of kritisch op basis van het risiconiveau en worden deze beoordeeld door het Change Control-management. Zodra de aanvragen goedgekeurd zijn, worden de wijzigingen ontwikkeld, getest en geïmplementeerd binnen het tijdskader dat voor elke categorie vastgelegd is. Standaardwijzigingen worden doorgaans binnen vijf dagen doorgevoerd. Kronos volgt standaard procedures voor alle geplande wijzigingen. Voorafgaand aan een aanvraag voor een productiewijziging worden wijzigingen doorgaans in de niet-productieomgeving ingevoerd.

Bepaalde wijzigingen hebben gevolgen voor meer dan één klant. In die gevallen verzendt Kronos een bericht aan de betroffen klanten.

Kronos voert ook noodzakelijke wijzigingen uit voor het onderhoud van het besturingssysteem en van andere applicaties van derden, die de basis vormen van het Kronos-platform voor personeelsmanagement. Implementatie van deze wijzigingen wordt zorgvuldig gepland om onderbrekingen van de dienst tot een minimum te beperken, in het bijzonder tijdens kritische perioden in de loonadministratiecyclus van de klant. Verder beoordeelt Kronos veiligheidsberichten van verkopers en derden om noodzakelijke patches vast te stellen en aan te bevelen en implementeert het die patches, die de veiligheid van de klantgegevens beschermen.

INTEGRATIE MET KLANTGEGEVENS EN APPLICATIEOMGEVING

Als u Kronos Workforce Integration Manager-interfaces laat ontwikkelen, wordt de integratie van gegevens tussen cloud-based Kronos-applicaties en systemen van derden bereikt via SFTP-transfers van bestanden die door de klant geïnitieerd worden. Met deze transfers kunt u probleemloos en veilig gegevens verplaatsen tussen systemen. Zo kunt u een masterbestand van een werknemer uploaden voor import in het Kronos-systeem voor personeelsmanagement of elke betalingsperiode een bestand met gegevens uit de loonadministratie downloaden. Hoewel veel Kronos Cloud-klanten deze processen automatiseren, is automatisering niet vereist. Overige op maat gemaakte integratiemogelijkheden zijn beschikbaar tegen meerprijs.

Op Kronos gebaseerde authenticatie met gebruikersnaam en wachtwoord is beschikbaar. Integratie met Active Directory/LDAP kan beschikbaar zijn afhankelijk van uw netwerkconfiguratie.

ONDERSTEUNING VAN KRONOS VOOR SINGLE SIGN-ON:

Met Single sign-on (SSO) kunnen gebruikers probleemloos toegang verkrijgen tot geautoriseerde netwerken op basis van een enkele aanmelding of authenticatie, die uitgevoerd wordt als ze zich de eerste maal aanmelden voor het netwerk. Single sign-on kan de productiviteit van netwerkgebruikers verhogen, de kosten van netwerkactiviteiten verminderen en de veiligheid van het netwerk verbeteren. Specifieke voordelen zijn:

- Gemak van beheer: De aanmeldgegevens worden opgeslagen en bijgehouden op een enkele locatie met een enkel mechanisme (zoals LDAP).
- Hogere productiviteit van de gebruikers: Gebruikers hoeven zich niet op meerdere systemen aan te melden. Daarnaast hoeven gebruikers niet langer hun combinaties van gebruikersnaam en wachtwoord voor elke applicatie handmatig te synchroniseren.
- Verbeterde veiligheid: Als een gebruikersaccount bijvoorbeeld opgeheven wordt, wordt het in alle applicaties in het gehele netwerk opgeheven. Aangezien een gebruiker een enkel wachtwoord heeft, is het minder waarschijnlijk dat hij of zij het wachtwoord hoeft op te schrijven.

Kronos ondersteunt single sign-on op basis van de SAML (Security Assertion Markup Language) 2.0-norm, waar de gebruiker in een portaal van de klant doorgeleid wordt naar de Kronos Cloud-applicatie.

SLA-BELEID EN BEHEER

In de SLA, een servicegarantie tussen Kronos en uw organisatie, worden de verwachtingen van de klant betreffende de beschikbaarheid van de service en de oplossing(en) voor personeelsmanagement van Kronos geformuleerd. Daarnaast worden in de SLA boetes vastgelegd, als Kronos niet voldoet aan die beloften inzake beschikbaarheid. In de standaard Kronos Cloud SLA wordt een percentage van 99,75 gehanteerd voor beschikbaarheid van de oplossing(en) voor personeelsmanagement voor de klant en worden creditbedragen vastgesteld die aan de klant worden uitgekeerd, zodra niet aan de voorwaarden van de SLA wordt voldaan.

Om transparantie en naleving van de SLA te waarborgen, ontvangt elke Kronos Cloud-klant van zijn of haar Cloud Customer Manager cijfers over de beschikbaarheid.

WORKFORCE CENTRAL 8 COMPATIBILITEITSEISEN

Browser			Besturingssysteem	
Vendor	**Product**	**Versie**	**Vendor**	**Product**
Microsoft	Internet Explorer	9, 10 & 11 (32- & 64-bit)	Microsoft	Windows 8 * 8.1 — 64-bit (Desktop Modus)
Google	Chrome	40+		Windows 7 — 32- & 64-bit
Mozilla	Firefox 32-bit	36+		Windows Server 2012
				Windows Server 2012R2
Apple	Safari	7.x & 8.x	Apple	Mac OS-X 10.9 & 10.10

Opmerking: Voor Safari-browser/OS-X-klanten wordt JRE geleverd door Oracle.
Firefox en IE11 worden niet ondersteund met HRMS Admin.
Chrome & Firefox — Alleen ondersteuning voor recente versies (i.e.: Current & 2 back)

CPU	Intel-based Pentium 4 of AMD equivalent; 2 GHz+ aanbevolen
RAM	2 GB minimum; 4 GB aanbevolen
Cache	256KB/L2 aanbevolen
Display	1024 x 768 met 256 kleuren aanbevolen; minimale grafisch geheugen: 128 MB
Harde-schijfruimte	Minimale vrije schijfruimte: 100MB
Netwerkprotocol	HTTPS
Bandbreedte netwerk	LAN-verbinding: Gigabit netwerk aanbevolen WAN-verbinding: Fractional T1, or T1+ aanbevolen

Voor Workforce Timekeeper™ 8 moet het gebruik van cookies mogelijk gemaakt worden. Voor Kronos HRMS moet ActiveX-besturing toegestaan worden.

Navigator Gebruikersinterface			
Vendor	**Product**	**Versie**	**Besturingssysteem**
Adobe	Flash	15+	Zelfde als ondersteunde browsers

Java Plug-in			
Vendor	**Product**	**Versie**	**Besturingssysteem**
Oracle	Java plug-in (JRE)	Ondersteunt JRE 1.8 van JRE 1.8.40 (meegeleverd met product)	Zelfde als ondersteunde browsers

Mobiel	
Soort apparaat	**Platform**
Apple	iPad®, iPhone®, en iPod Touch® — met iOS7.0
Android	OS 4.1 en hoger

Tablet	
Soort apparaat	**Platform**
Apple	iPad met iOS7.0+

Soort apparaat	Communicatiewijze	Minimum Firmware
InTouch	Geïnitieerd door apparaat	1.1.1+
4500	Geïnitieerd door apparaat	3.0+
	Geïnitieerd door server	02.01.xx+

Desktop Virtualisatie			
Product	**Besturingssysteem van Platform**	**Product**	**Besturingssysteem van Platform**
Citrix XenApp v6	Microsoft Windows 2012 Server 64-bit	Terminaldiensten	Microsoft Windows Server 2012 SE
	Microsoft Windows 2012 R2 Server 64-bit		Microsoft Windows Server 2012 SE

KRONOS® | Workforce Innovation That Works™

Kronos Nederland Newtonlaan 115 3584 BH Utrecht, Nederland +31 (0)85 273 64 53 www.kronosglobal.nl

SV0138-NLv5