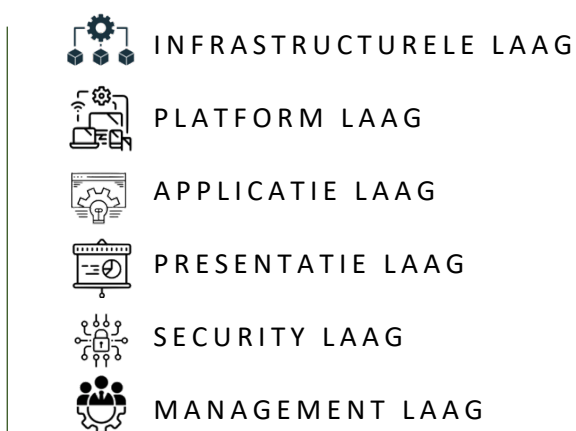


Huidige situatie IT-Informatisering Ergon



Datum: Januari 2022

Versie: 1.0

Status: Definitief

Dit document bevat informatie als input voor de Europese aanbesteding van Ergon voor ICT-diensten op het gebied van PaaS. Het doel van het document is de huidige ICT-omgeving te beschrijven en daarmee een helder beeld te verschaffen hoe de bestaande IT-omgeving is ingericht. En is daarbij een belangrijk naslagwerk voor de aanbesteding



INFRASTRUCTURELE LAAG

In de zogenaamde Infrastructurele laag worden de volgende componenten beschreven:

- Fysieke locaties (inclusief stroomvoorziening en koeling)
- Fysieke servers
- Storage
- Virtualisatie
- Netwerk

FYSIEKE LOCATIES

Ergon beschikt over meerdere locaties. De IT Infrastructuur bevindt zich grotendeels op de locaties “de Hurk” in Eindhoven. Ergon maakt op dit moment gebruik van een ‘active-active’ datacenter opstelling waarbij de server en storage infrastructuur wordt verdeeld over 2 locaties die onderling verbonden zijn door middel van 4 keer 10 Gb glasvezel. De primaire locatie draait op het hoofdkantoor, Rooijakkersstraat 3, en de uitwijk omgeving draait aan de overkant van de straat, Rooijakkersstraat 2B. Daarnaast wordt er nog gebruik gemaakt van twee back-up locaties:

1. Een locatie met een Veeam back-up server voor de korte retentie.
2. Een tweede locatie waar de tapes in de kluis liggen.

De overige (hoofd) locaties van de business units zijn voorzien van een patch ruimte waarin de noodzakelijke hardware aanwezig is om de betreffende locatie te verbinden met de hoofdlocatie op de Rooijakkersstraat. Het gaat hierbij om routers, firewalls en switches en Avaya gateway voor aansluiting analoge lijnen en verbinding naar ISDN 30. Op de andere locaties zijn geen servers aanwezig. Voor totaaloverzicht van de Ergon locaties zie het onderdeel Netwerk.

STROOMVOORZIENING

Om de risico's van eventuele stroomuitval te beperken zijn de serverruimtes en patchruimtes op de locaties de Hurk voorzien van een noodstroomvoorziening, ook wel UPS (Uninterruptible Power Supply) genoemd. Het betreft 3 stuks APC symmetra LX RM 8 kVA (computerruimtes Rooijakkersstraat 2B en 3 en de patchruimte op Rooijakkersstraat 3). De switches zijn verbonden met de UPS systemen om ervoor te zorgen dat de VoIP toestellen, die worden gevoed vanuit de power-over-ethernet switches, blijven functioneren tijdens een stroomuitval. In de centrale serverruimtes aan de Rooijakkersstraat 3 en Rooijakkersstraat 2B zijn de noodstroomvoorzieningen uitgerust met een netwerkaansluiting. De netwerkaansluiting wordt gebruikt voor het monitoren van een goede werking van de noodstroomvoorzieningen, maar ook voor het melden van spanningsuitval aan de overige ICT-componenten.

KOELING

Van het elektrisch vermogen die de ICT-componenten verbruiken, wordt het meeste vermogen omgezet in warmte. Voor de goede werking van ICT-componenten is het belangrijk dat de temperatuur in de server/patchruimtes niet te hoog en zoveel mogelijk constant blijft. Om de ICT-componenten zo goed mogelijk te laten werken zijn de volgende voorzieningen getroffen in de serverruimtes:

Rooijakkersstraat 3 en Rooijakkersstraat 2B zijn voorzien van Airco, type Stulz minispace XT-2000 CCD121 (x2) en type CCD61A (x2)? (Onderhoud 1600 euro per jaar)

Op de andere locaties is geen airco aanwezig.

FYSIEKE SERVERS

Zoals beschreven bevinden zich op de hoofdlocatie de gecentraliseerde servers. In de onderstaande tabel zijn fysieke servers opgesomd welke in productie zijn. In de betreffende server ruimtes zijn meerdere fysieke servers aanwezig.

Overzicht fysieke servers 4 maal HPE Hyper Converged 380 (1-8-2017)



Servers Recorded

Server Name	Total Capacity	Free Capacity	Used Capacity	IOPS	Peak Disk Throughput	Read/Write Ratio	Peak Network
esrv16.eb.local	12.22 TB	158.00 GB	12.06 TB	2337 at 95%	465.00 MB/s	67% / 33%	1.04 GB/s
esrv17.eb.local	48.61 TB	6.12 TB	42.49 TB	2761 at 95%	482.90 MB/s	70% / 30%	793.56 MB/s
esrv15.eb.local	12.22 TB	158.00 GB	12.06 TB	1921 at 95%	298.00 MB/s	54% / 46%	295.65 MB/s
esrv14.eb.local	12.22 TB	117.00 GB	12.10 TB	4599 at 95%	773.10 MB/s	84% / 16%	758.76 MB/s

Opmerking:

Vrije ruimte is hier niet van toepassing. Er is namelijk geen fysieke vrije ruimte meer omdat alle fysieke vrije ruimte is vergeben aan de virtuele store virtual servers die het weer ter beschikking stellen aan de vSphere server. Elke ESX server heeft 2 raid sets 1 van 192,5 GB voor het OS 1 van 12,02 TB voor Store Virtual. Totaal is dus 48,08 TB beschikbaar. Hiervan is 25,70TB uitgeven aan de virtuele machines. Hierin is opgenomen dat elke disk dubbel is uitgevoerd en 2 snapshots in gebruik heeft. Er is dus nog 22,37 TB beschikbaar.

HPE Store Easy 1650 WSS2016 Str ESRV18 - 17/01/2018 (huidige Veeam backup server)

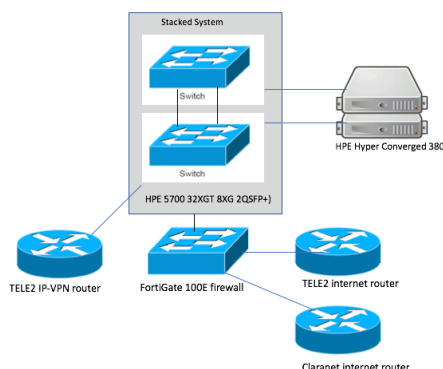
Voor aansturing van de wifi-access points is er een Aruba 7205 Mobility Controller aanwezig.

Tevens zijn er op verschillende locaties Pc's actief voor lokaal gebruik en Raspberry Pi's. Deze worden ingezet voor intern publicatie op tv-schermen.

HYPERVISOR/ VIRTUALISATIE

Binnen Ergon wordt er primair gebruik gemaakt van de VMWare vSphere hypervisor. Deze is geïnstalleerd op een 4-tal fysieke servers welke in de serverruimtes aan de Rooijakkersstraat 2B en Rooijakkersstraat 3 staan opgesteld. Deze VMWare vSphere hosts zijn de basis van het gehele HyperVisor productieplatform. Dit platform host alle virtuele servers (VMs) welke de benodigde services beschikbaar stelt binnen Ergon. Onderstaand is een schematische weergave van de hypervisor setup zoals deze bij Ergon is geïmplementeerd in elk van de 2 computerruimtes.

Iedere computerruimte bevat 2 servers die op 2 core switches (HPE 5700 32XGT 8XG 2QSFP+) zijn aangesloten. De 4 core switches die over de 2 computerruimtes zijn verdeeld vormen samen één stack.



VIRTUELE SERVERS

Server	Omschrijving	Virtueel	C	D	E	F	overig	VMFS	GB	CPU's	Windows versie
EVSrv01	SQL Server Informer B	ja	80	150			70	300	16	4	2012 R2 standard
EVSrv02	WSUS / WMS / Citrix License	ja	100	750			150	1000	16	4	2016 Standard
EVSrv03	Webserver WLB	ja	80				20	100	4	1	2016 Standard
EVSrv04	Metacom Test	ja	80	120			40	240	8	4	2016 Standard
EVSrv05	Metacom Productie	ja	80	140			70	290	16	8	2016 Standard
EVSrv06	Webserver Inception	ja	80	40			30	150	4	1	2016 Standard
EVSrv07	Suwi smtp mail server	ja	80				20	100	4	1	2016 Standard
EVSrv08	Bitdefender GravityZone	ja	160				40	200	16	8	Ubuntu Linux
EVSrv09	Printserver Konica Minolta	ja	60	200			40	300	8	2	2012 R2 standard
EVSrv10	Printserver Toshiba / WDMFTPServer	ja	80				20	100	8	2	2016 Standard
EVSrv11	Printserver	ja	80				20	100	8	2	2016 Standard
EVSrv12	Mavim webserver	ja	60				20	80	4	1	2012 R2 standard
EVSrv13	Metacom Test	ja	50	150			40	240	8	4	2012 R2 standard
EVSrv14	SQL2008	ja	100	200			50	350	4	2	2012 R2 standard
EVSrv16	PRTG	ja	80	80			40	200	4	1	2016 Standard
EVSrv20-1	domaincontroller 1	ja	80	10			20	110	4	1	2016 Standard
EVSrv21	Metacom Productie	ja	60	150			90	300	16	8	2012 R2 standard
EVSrv22-1	domaincontroller 2	ja	80	10			20	110	4	1	2016 Standard
EVSrv23	Print server oud	ja	80				20	100	4	1	2012 R2 standard
EVSrv24	Veeam Proxy en Radius Wifi netwerk	ja	80				20	100	4	1	2016 Standard
EVSrv25	Metacom Reportserver Test	ja	80	25	25		30	160	8	4	2016 Standard
EVSrv26	Metacom Reportserver Productie	ja	80	25	25		30	160	8	4	2016 Standard
EVSrv28	Intranet/extranet/internet ergon webserver	ja	60	35			25	120	4	2	2012 R2 standard
EVSrv29	TS voor Java 6 / KIS / Labelprint wasserij	ja	80				20	100	8	2	2012 R2 standard
EVSrv30											
EVSrv32	File server	ja	80	2000	2000		520	4600	8	2	2016 Standard
EVSrv33	Exchange 2016	ja	170	450			100	720	16	4	2016 Standard
EVSrv34	Exchange 2016 Edge Transport	ja	80				20	100	4	2	2016 Standard
EVSrv36	Virtual center							150	10	2	Linux
EVSrv40A	Isgram Red Hat linux server	ja	500				100	600	16	2	Red Hat 8
IPOFFICE11	Avaya telefooncentrale	ja	100				20	120	8	4	Red Hat 6
EVSrv42	Avaya beheerserver	ja	80				20	100	4	1	2012 R2 standard
EVSrv43	HP Oneview server							330	16	4	Other 3.x Linux
EVSrv44	HP Oneview appliance	ja	150				30	180	4	2	CentOs 6
EVSrv45	Metacom Reportserver Test	ja	50	25	50		25	150	8	4	2012 R2 standard
EVSrv46	Metacom Reportserver Productie	ja	50	25	50		25	150	8	4	2012 R2 standard
EVSrv47	Magistor production	ja	600				100	700	16	8	2012 R2 standard
EVSrv48	Magistor test	ja	400				100	500	8	4	2012 R2 standard
EVSrv56	Xenapp Delivery Controller Ergon	ja	150				60	210	8	2	2016 Standard
EVSrv60	Rapid7 InsightVM	ja	80	180			40	300	8	2	2016 Standard
EVSrv61	Webserver Ultimo	ja	80				20	100	4	1	2016 Standard
EVSrv62	SQL Server Ultimo	ja	80	140			40	260	8	2	2016 Standard
EVSrv70	Aruba Airwave	ja	120				180	300	16	4	CentOS 7
XenappXA	Xenapp template 7.15		150				60	210	24	4	2016 Standard
Xenapp01-19	Xenapp	ja	150				1020	1843,2	336	56	2016 Standard
XenappAnon	Xenapp Anoniem image	ja	150				30	210	24	4	2016 Standard
XenappAnon1	Xenapp Anoniem		150				1650	1800			
EVSrv82	IIS externe webserver	ja	60	20			20	100	4	1	2012 R2 standard
BEHEER	Clientele	ja	100				20		4	1	Windows 10 Pro
Systeembeheer	test werkstations en iso images	ja					75	75			
Werkstations	Virtuele werkstations	ja					800	800			
W1012	Mavim								4	1	Windows 10 Pro
W1017	Mavim								4	1	Windows 10 Pro
W1018	Adobe Creative Cloud								4	1	Windows 10 Pro
W1019	Outlook Textieldiensten	ja	80				20	100	4	1	Windows 10 Pro
W1023	XP Ivis en Istod technische dienst								0,5	1	XP
EBSrv27	Teamsft server	ja	15	5	30	470	70	590	3,75	2	2003 Enterprise 32 bits
ESRV07	tivoliserver	nee									2008 standard 64 bits
FOM	Storevirtual FOM								2	4	Centos
EFNA1	FortiAnalyzer	ja	2	600			198	800	8	2	Centos
EFNW1	FortiWeb	ja	80				40	120	8	1	Centos
Totaal			5637	5530				21228,2	728,25	182	

STORAGE

De HPE Hyper Converged servers voorzien in zowel de rekenkracht als in de storage. De RAID 10 configuratie (striping en mirroring) is zodanig geconfigureerd dat in het geval dat 1 locatie (2 servers dus) uitvalt, alle data beschikbaar blijft via de andere locatie.

NETWERK KOPPELINGEN EN ONTSLUITINGEN

Netwerk	Omschrijving
Default LAN	In dit LAN bevinden zich alle servers, printers en werkplekken.
DMZ	Binnen dit VLAN bevinden zich de publiek toegankelijke webserver.
WIFI LAN	Dit is een logisch gescheiden LAN met een eigen internet ontsluiting.
Management LAN	Het Management LAN wordt gebruikt door de afdeling ICT.
Storage LAN	Het storage ISCSI LAN is een niet routeerbaar LAN. Deze wordt alleen gebruikt door de servers en is daarom niet ingetekend in de schematische weergave.
IP-VPN	Om verschillende locaties met elkaar te verbinden wordt er gebruik gemaakt van een MPLS-netwerk geleverd en beheerd door TELE 2 of eigen beheer zie overzicht
eGem / Suwinet	Via dit VLAN wordt verbinding gemaakt met een terminal server van het UWV en wordt er e-mail uitgewisseld met de suwinet mailserver.
VoIP	Vaste telefoons en de telefooncentrale maken gebruik van dit VLAN.
vMotion	Voor vMotion verkeer tussen de VMware ESXi servers.

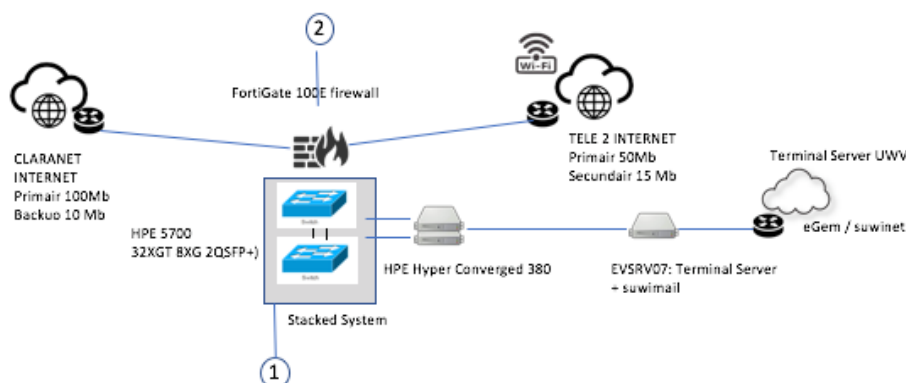
De netwerk infrastructuur wordt gefaciliteerd met behulp van onderstaande netwerkcomponenten

Type	Aantal	Model	Omschrijving
Core Switches	4	HPE 5700 32XGT 8XG 2QSFP+	Server LAN Core Switches
Workspace Switch PoE	24	HP/ 3com 4500 PWR switch 24*10/100	Werkplek connectiviteit op de verschillende locaties.
Workspace Switch	16	Cisco Catalyst 2950	Switches uit 2003 op verschillende locaties.
WIFI Controller	1	Aruba	WIFI controller voor Access Points
Access Points	104	HP Aruba AP-505	Access points
Firewall hoofdlocatie	2	FortiGate 100E	Cluster op Rooijakkersstraat 2B en 3
Firewalls nevenlocaties	14	FortiGate 50E	

WAN-VERBINDINGEN

Zoals eerder benoemd heeft Ergon een aantal locaties. Deze locaties zijn gekoppeld aan een IP-VPN welke beheerd wordt door TELE2 of in eigen beheer zie tekening. Tussen de 2 locaties op de Hurk 48 is een darkfiber verbinding actief, die geleverd wordt door Glasvezel Eindhoven.

De onderstaande tekeningen zijn schematische weergave betreffende de verbindingen tussen de vestigingen.





PLATFORM LAAG

OS SERVICES

Binnen Ergon wordt gebruik gemaakt van de diverse operating systemen. Deze worden toegepast op diverse fysieke -en virtuele servers en appliances. Onderstaand is een opsomming van de diverse Operating Systemen welke geïnterpreteerd zijn:

- Windows Server 2012 R2 Standard
- Windows Server 2016 Standard
- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 8
- Ubuntu Linux
- Windows 10 Professional
- Raspbian OS

ATHENTICATIE EN AUTORISATIE SERVICES

Binnen Ergon wordt gebruikt gemaakt van onderstaande authenticatie en autorisatie services:

- Microsoft Active Directory
- Forti Token Mobile
- LDAP-services
- Microsoft ADFS
- Microsoft MFA

ACTIVE DIRECTORY

De centrale authenticatie en autorisatie wordt verzorgd door een Microsoft Active Directory bestaande uit 2 domain-controllers. In de onderstaande tabellen zijn de details beschreven van de Microsoft Active Directory configuratie:

EVSRV20-1	domain controller 1
EVSRV22-1	domain controller 2

2-FACTOR AUTHENTICATIE

Binnen Ergon is vanaf externe bronnen een 2factor authenticatie vereist.

Deze 2factor authenticatie wordt verzorgd door het FortiGate 100E cluster. D.m.v. een token op de mobiele telefoon wordt er een VPN-verbinding opgezet naar de hoofdlocatie. Er zijn op dit moment 210 Fortinet Tokens actief.

LDAP-SERVICES

Vanuit diverse Linux besturingssystemen zijn LDAP-koppelingen opgebouwd naar de Microsoft Active Directory. Middels deze LDAP-koppeling wordt er een centrale authenticatie afgedwongen voor de niet domein-servers en appliances. In de meeste situaties is dit op basis van secure LDAP.

AUTHENTICATIE-SERVICES

Voor de koppeling met het intranet van Ergon wordt gebruik gemaakt van Secure LDAP.

FILE SERVICES

Als centrale file service binnen Ergon wordt er gebruik gemaakt van een Microsoft Windows Server 2016 (64-bit) Fileserver.

In de onderstaande tabel is de volume informatie, capaciteit en share-informatie weergegeven. Binnen ERGON wordt gebruik gemaakt van DFS-services om de shares te centraliseren.

Volume	Share	Capaciteit
G:\ (1 afdeling) H:\ (meerdere afdelingen)	Afdeling	Capaciteit: 5,5 TB
P:\	Afdeling overstijgende mappen	Valt onder bovenstaande
Citrix Profiles		
FSLogix virtuele VHD disk		

PRINT SERVICES

Er zijn nog een aantal HP/Samsung printers, maar het merendeel betreft Toshiba printers. Deze printers werken op basis van “follow-me” via een PaperCut officemanager server. Deze PaperCut server zorgt voor de juiste afhandeling van prints via 1 centrale queue. Op de printserver zijn in totaal 60 HP/Samsung printers geconfigureerd en ook een aantal labelprinters, verdeeld over de onderstaande types:

Omschrijving	Aantal		
Brady 360x Plus	1	HP Laserjet P2015DN	2
Brady BP-THT-300X PLUS-II	1	HP LaserJet P2055DN	20
Brady Printer BP3481	1	HP LaserJet Pro M227sdn MFP	1
Brady Printserver II	1	HPE 1/8 G2 LTO-7 SAS taperobot	1
Brother QL-580N labelprinter	4	IBM TS3200 - 3573-TL library	1
CAB A4+/300 Labelprinter	2	Konica Min. AccurioPress C2060	1
Canon ImageRunner 1133iF	1	Konica Min. bizhub PRESS 2250P	2
Canon ImageRunner Adv 400i	2	OCE OP20	2
Canon ImageRunner Adv C3330i	1	Samsung CLP-775ND Color Laser	1
Canon iR2520i V2	1	Samsung CLX-6260FR	1
Canon iR2525 V2	3	Samsung ML-3710ND Laser	2
Canon PIXMA iP100 Mobile +accu	1	Toshiba B-EX4t1 GS12-QM-R	2
DYMO Labelmanager 9000	2	Toshiba MFP e-STUDIO400AC	1
HP Color LaserJet CP3505N	1	Toshiba MFP e-STUDIO408P	7
HP Color LaserJet CP3505x	1	UPS LP 2844	1
HP Color LaserJet CP5225DN	1	Zebra 170 XI2	1
HP Color LaserJet M553dn	5	Zebra GK420t Printer 203dpi E	3
HP Color LaserJet M553n	2		
HP Color LaserJet Pro M181fw	4		
HP Color LaserJet Pro M477fdw	5		
HP DesignJet 500 Plus/EN A1	1		
HP DesignJet T520 24in	1		
HP LaserJet 600 M601dn	1		
HP LaserJet Enterprise M506dn	3		
HP LaserJet Enterprise M604dn	1		
HP LaserJet Enterprise M604n	1		
HP LaserJet Enterprise M608dn	1		
HP LaserJet Enterprise M608x	1		
		Eindtotaal	99

PRINTSERVERS

EVSrv09	Printserver Konica Minolta
EVSrv10	Printserver Toshiba/ WDMFTPServer
EVSrv11	Printserver

DATABASE SERVICES

Voor verschillende applicaties worden allerlei diverse database platformen gebruikt binnen Ergon. Onderstaande database platformen zijn actief op verschillende servers binnen Ergon organisatie:

- SQL
- Progress (voor Metacom)

EVSRV01	SQL Server PowerBI koppeling
EVSRV62	SQL Server Ultimo/WLB/Inception
EVSRV14	Kluwer MiniFmis, ClientProof

WEB SERVICES

Binnen Ergon zijn er diverse web-based applicaties welke aangeboden worden vanuit de onderstaande servers. Een aantal van deze webserveren zijn extern/publiekelijk benaderbaar. De websites in de ergon.nu en ergon.nl zone zijn beveiligd met een wildcard certificaat van een externe leverancier. De interne sites en de sites die alleen voor leveranciers toegankelijk zijn beveiligd door een intern certificaat wat door de CA server op de evsrv20-1 is uitgegeven. Webserver overzicht (zie overzicht virtuele servers)

DEPLOYMENT SERVICES

Ter standaardisatie en automatisering wordt er gebruik gemaakt van een XenApp delivery controller voor de deployment van de 17 Citrix servers met OS en applicaties.

XENAPPXA Citrix image

De clients worden hiermee voorzien van de volgende software (zie Citrix applicaties).

- Office 2016
- Adobe Reader
- Citrix Receiver
- VLC mediaplayer
- Firefox
- PDF Split and Merge
- Chrome
- Power BI
- Code Soft
- Metacom
- Xgram
- Magistor

REMOTE ACCESS SERVICES

Remote acces naar de aangeboden applicaties en services binnen de ICT-infrastructuur van Ergon kan middels 2 stappen:

- VPN-cliënt op laptop of tablet pc
- Vervolgens via de browser naar de Citrix Web Portal

Medewerkers kunnen via de Citrix Web Portal verbinding maken met de Citrix Desktop waar vanuit diverse applicaties gestart kunnen worden. Om een verbinding te kunnen opzetten via de Citrix Web Portal is een Forti Token vereist zoals eerder beschreven.

BACKUP SERVICES

Ergon maakt voor de dagelijkse back-up gebruik van back-up en recovery software van Veeam. Dagelijks worden er 's avonds en 's nachts backups op disk gemaakt. De volgende ochtend wordt de backup tevens weggeschreven naar LTO 7 tapes. Daarnaast wordt van elk servervolume elke dag een snapshot gemaakt op het storage niveau die 2 dagen bewaard blijft. Tapes worden op de andere locatie bewaard dan waar de backup server staat

UITWIJK

De computerruimtes aan de Rooijakkersstraat 2B en 3 zijn elkaars uitwijklocaties.



APPLICATIE LAAG

Binnen Ergon wordt de mail services aangeboden via een EVSRV33 Exchange 2016 Server. Daarnaast wordt gebruik gemaakt van de EVSRV34 Exchange 2016 Edge Transport Server. Mail verstuurd naar een suwi mailadres worden gerouteerd via de EVSRV07 die de mail doorgeeft naar de suwi SMTP-servers. Mail gestuurd naar ergon.nl.suwi komt via het suwinet binnen op de EVSRV07 en worden doorgestuurd naar de Exchange server EVSRV33.

Het totaal aantal aanwezige mailboxen betreft 561 (persoonlijke mailboxen en afdelingsmailboxen) welke verdeeld zijn over Office 365 (123 stuks) en de on-premise Exchange 206 server.

COLLABORATION SERVICES

Voor het samenwerken en met name uitwisselen van bestanden maakt men binnen de Ergon gebruik van onderstaande oplossingen:

- Microsoft Office365 omgeving

WEB SERVICES (APPLICATIES)

Ergon maakt gebruik van diverse webservices in de vorm van applicaties en websites. De meeste webservices worden gehost op de server EVSRV28 Intranet/extranet/internet ergon webserver. Op deze Windows 2012 R2 standaard server worden websites en applicaties gehost die met name publiekelijk benaderbaar zijn. Daarnaast is er ook een webserver voor Inception (Werkwijzer - Kwaliteit systeem)

- www.ergonline.nl
- <https://werkwijzer.ergon.nl>
- De publiekspagina op het internet en intranet voor de eigen werknemers
- Xgram en Magistor servers bevatten een website voor het plaatsen van orders vanaf internet
- Secure FTP wordt gebruikt voor uitwisselen bestanden met timetick en klanten van LDA (Unibind).

SPECIFIEKE APPLICATIE SERVICES

Applicatie	# Gebruikers	Omgeving	Opmerkingen
Brother Labelprint: P-touch editor	7	Citrix	Software voor labels printen
CodeSoft	25	Citrix	Barcode en etiketten printen, max 5 concurrent
ETC	1	Citrix	
FMIS	43	Citrix	Zaalreserveringen en meldingen naar monteurs
GeoVisia 6.3.5.3	5	Citrix	Niet meer in gebruik. Wel bewaren.
KabelCheck 2.0	1	Citrix	Check van kabels
Kis	13	Citrix	Access database wordt vervangen door Kwaliteit systeem
Magistor	15	Citrix	Nieuw voorstel ter goedkeuring
Management Informatie Systeem	75	Citrix	gegevens opgehaald uit AFAS
Metacom	47	Citrix	vervalt bij implementatie Groen Vision
MS Access 2016	23	Citrix	vervalt bij MS 365
MS Excel 2016	484	Citrix	vervalt bij MS 365
MS Onenote 2016	484	Citrix	vervalt bij MS 365
MS Outlook 2016	484	Citrix	vervalt bij MS 365
MS Powerpoint 2016	484	Citrix	vervalt bij MS 365
MS Publisher 2016	484	Citrix	vervalt bij MS 365
MS Teams	484	Citrix	vervalt bij MS 365
MS Word 2016	484	Citrix	vervalt bij MS 365
PlantenPaspoort	10	Citrix	Access database vervalt bij Groen Vision
PowerBI	6	Citrix	Lokaal of Azure
UWV Documentenhulp Werkgever	60	Citrix	
Xgram	70	Citrix	Wordt vervangen door Magistor/AFAS
Xgram Urenregistratie	0	Citrix	Wordt vervangen door Magistor/AFAS

Applicatie	# Gebruikers	Omgeving	Opmerkingen
Accurio Pro Flux (Konica Minolta)	3	PC	Printer opdrachten beheer
PrintShop Mail Suite	3	PC	Variable Publishing Software Minolta
Enfocus Pitstop Pro	1	PC	PDF controle en bewerkingsoplossing
Adobe Creative Cloud - Acrobat Pro	3	PC	PDF maken en bewerken
Adobe Creative Cloud - Alle apps	4	PC	Volledige Adobe Suite
Autodesk AutoCAD 2022 (Single user)	1	PC	2D EN 3D ontwerpen
Avaya Softconsole	1	PC	PC telefoon software
Cadac The Modus Suite Standard	1	PC	BIM software Building Information Modeling

Applicatie	# Gebruikers	Omgeving	Opmerkingen
CMS Eindhoven	8	Internet	
CompetenSYS	100	Internet	Diagnostiek, loonwaardemetingen en matching
Docuware	15	Internet	Archivering van documenten + 50 Gb opslag
MS 365	108	Internet	Migratie gestart met mailboxen
VDI_Eindhoven	68	Internet	Connectie met Suite van Gemeente
ViaDesk	0	Internet	Nog niet in gebruik, vervangen voor 365 portal
Virtual Laundry		Internet	Productie monitoring Wasserij
Profit AFAS	60	Internet	Zie excel Insite gebruikers
Insite AFAS	349	Internet	Zie excel Insite gebruikers
Leviy	3	Internet	Schoonmaak, kwaliteits controle
Paradigma online	30	Internet	Arbo systeem gegevens overdracht alle leidinggevende
Ergonline	alle gebruikers	Internet	http://www.ergonline.nl/ergonbreed/

Applicatie	# Gebruikers	Omgeving	Opmerkingen
AriSYS	114	Web	beheerd door Frans Lavrijsen zie overzicht AriSYS gebruikers
TeamSoft	2	Server	toegang tot VM op aanvraag (W2003)
Ultimo	15	Web	Gaat naar SaaS oplossing 1e kw 2022
WerkWijzer	alle gebruikers	Web	www.werkwijzer.ergon.nl
Ergon Intranet	alle gebruikers	Web	Intranet Ergon



PRESENTATIE LAAG

SERVER BASES COMPUTING (SBC)

Alle medewerkers hebben toegang vanuit het interne “userLan” en vanaf externe locaties tot de server based computing servers. Deze SBC-omgeving is ingericht op basis van Citrix XenApp. Middels een aangeboden desktop worden de diverse applicaties en services aangeboden aan de medewerkers.

De SBS-omgeving bestaat uit de onderstaande componenten:

- 1 Delivery controller.
- 1 Web interface webservers
- 18 XenApp Servers
- 1 Licentie server

Component	Software Versie	Server naam
XenApp		Xenapp01-19
XenApp template 7.15		XenAppXA
XenApp Anoniem image		XenappAnon
XenApp Anoniem		XenappAnon1
XenApp Delivery Controller Ergon		EVSRV56
WSUS/ WMS / Citrix License		EVSRV02

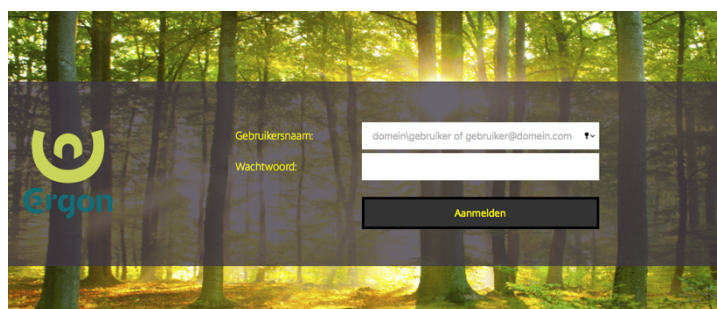
Citrix licentie 320 concurrent users tot 1/7/2022.

PORTALS

Zoals eerder benoemd worden er vanuit Ergon diverse portals en websites gepubliceerd. Met name de Citrix Web Portal is hierin de belangrijkste en geeft toegang tot de Server Based Computer omgeving van Ergon.

De Citrix Web Portal is via het interne netwerk te benaderen middels onderstaand URL:

<https://evsrv56.eb.local/Citrix/GRWREWeb/>



De bovenstaande portal wordt ook aangeboden aan degenen die van buitenaf via een VPN-verbinding inloggen. Om verbinding te kunnen maken is een 2factor authenticatie vereist middels de eerder benoemde Forti Tokens.

Verbinding vanaf het Ergon netwerk is mogelijk middels grotendeels Wyse thin clients met ThinOS en middels een aantal pc's en laptops.

APPLICATION DEPLOYMENT

Applicatie deployment wordt op dit moment vooral verzorgd d.m.v. de XenApp delivery controller voor de deployment van de 17 Citrix servers met OS en applicaties (en 1 aparte omgeving waarop anoniem wordt ingelogd voor o.a. leslokalen).

USER PROFILES

De gebruikers profielen bij Ergon zijn op basis van een roaming profile. Voor het cachen van de Office 365 omgeving wordt via FSLogix een virtuele VHD-disk gebruikt.

De gebruikers beschikken NIET over een eigen "Home Drive".

WERKPLEKKEN – CLIENTS

Binnen Ergon kent men 2 type werkplekken, vast en mobiel. De mobiele werkplek wil zeggen dat er een laptop en/of tablet PC ter beschikking is gesteld zodat de betreffende gebruiker op diverse locaties kan werken. De vaste werkplek is gelokaliseerd op de eerder benoemde locaties en is voorzien van een Thin-client of desktop PC.

THIN-CLIENTS

De HP thin-clients welke over de vestigingen verdeeld zijn worden centraal beheerd door een managementserver. Deze server wordt gebruikt voor het beheren en updaten van de Thin-clients.

In totaal zijn er 370 Dell Wyse 5070 Thin Client (aanschaf november 2018) opgenomen en actief.

Soort Client	OS	Merk/Type	Firmware	Aantal
Thin Client	ThinOS	Dell Wyse 5070	9.1.x	370

DESKTOP PC/ LAPTOPS/ TABLETS

Verdeeld over de verschillende locaties zijn er diverse desktop pc's in gebruik. Volgens de CMDB zijn er 26 Desktop Pc's actief van het merk HP/Compaq. De onderstaande types zijn momenteel in gebruik:

Dell OptiPlex 3040 MFF PC	2
DELL optiplex GX260 SMT 2,4 Gh	1
DELL optiplex GX620 SMT 3 Gh	1
HP COMPAQ DC5800	5
HP ProDesk 600 G1 SFF i5-4570	8
HP ProDesk 600 G2 SFF i5-6500	1
HP ProDesk 600 G4 SFF i5-8500	7
HP Z2 G4 Workstation i7-9700K 32GB	1
	26

Apple iPad Air 2 128GB Wi-Fi S	1
Apple iPad Pro 256GB 12.9 WiFi	1
Apple iPad Pro 32GB Wi-Fi Silv	1
Apple iPad Pro 64GB 12.9 WiFi	1
Dell Latitude E7480	3
Panasonic FZ-G1 mk4 LAN/LTE	1
Panasonic Toughpad FZ-G1	3
Panasonic Toughpad FZ-G1 MK2	5
Samsung Galaxy Tab A (2019) - 10.1" LTE	3
Samsung Galaxy Tab A 2016 WiFi	5
Samsung Galaxy Tab S5e - LTE	3
	27

DELL Latitude E6400	1
Dell Latitude E7440	7
Dell Latitude E7450	3
Dell Latitude E7470	6
Dell Latitude E74x0	1
Dynabook Satellite Pro L50-G-11H	23
HP Elitebook 850 G5 i5-8250U	3
HP Elitebook 850 G6 i5-8250U	7
Lenovo ThinkBook 15-IIL	10
Microsoft Surface Pro 128GB i5	7
Microsoft Surface Pro 3 128GB	28
Microsoft Surface Pro 3 256GB	2
Microsoft Surface Pro 4 128GB	8
Microsoft Surface Pro 7 128GB i5	2
Microsoft Surface Pro 7 256GB i5	2
MS Surface Pro 6 - i5-8350U	4
Toshiba Portege Z30-A-152	1
Toshiba Portege Z930-13G	4
Toshiba Portege Z930-188	1
Toshiba Tecra Z40-A-13Q Notebo	3
Toshiba Tecra Z50-A-10N	2
Toshiba Tecra Z50-C-10P	1
Toshiba Tecra Z50-C-138	4
Toshiba Tecra Z50-E-105	7
	137



SECURITY LAAG

De internet ontsluiting vanuit het server -en user lan verlopen middels een Firewall (FortiGate, maar ook Forti Web voor bescherming van de webserver en Forti Analyzer voor analyse van het netwerkverkeer) en beschermt tegen:

- SQL-injecties en willekeurige code-uitvoeringen
- Pogingen tot toegangscontrole en privilege-escalaties
- Cross-Site Scripting en buffer overflows
- Denial of Service (Dos) en Distributed Denial of Service-aanvallen (DDoS) Trajectopnames en peiling- en scanpogingen
- Backdoor-aanvallen, Trojaanse paarden, rootkits, virussen, wormen en spyware

InsightVM wordt gebruikt voor het dagelijks scannen op kwetsbaarheden.

AUTHENTICATIE/AUTORISATIE

Zoals beschreven in de platform laag wordt de authenticatie en autorisatie afhandeling gedaan door Microsoft Active Directory. Voor de remote toegang naar Citrix Web Portal is een 2factor authenticatie vereist. Deze wordt zoals genoemd afgehandeld door het FortiGate 100E cluster. Onderstaand is een samenvatting van het wachtwoord beleid welke binnen Active Directory geconfigureerd is.

Omschrijving	Waarde
Wachtwoord geschiedenis	8 wachtwoorden
Wachtwoord maximumleeftijd	n.v.t.
Minimumlengte wachtwoord	8 karakters
Duur account blokkade	10 minuten
Account blokkade	3 pogingen

Voor beheer doeleinden hebben alle ICT-beheerders een eigen beheer account.

Dit account is voorzien van Active Directory groepen waarmee “elevated” toegang tot apparatuur en systemen mogelijk is. Door het gebruik van dit type beheer accounts is het mogelijk om te achterhalen in events en logging wie welke aanpassing op welke systemen heeft gemaakt.

ANTIVIRUS/ ANTISPAM

Om de data binnen de ICT-infrastructuur zo goed mogelijk te beschermen tegen virussen en malware wordt er gebruik gemaakt van Bitdefender GravityZone. Tevens zorgt Bitdefender op de Exchange servers voor antispam. De client welke geïnstalleerd is op servers en werkstations is zoekt ieder uur naar updates.

Naast een up-to-date virusscanner zijn er nog meer maatregelen van toepassing binnen het Ergon netwerk:

- Firewalls; om het aantal servers en services te beperken die als toegangspunt kunnen dienen.
- Beperken van gebruikerstoegang tot systemen.
- Zoveel mogelijk gebruik maken van Read-Only filesystemen.
- Hierbij zijn na een herstart alle aangebrachte wijzigingen verdwenen.
- Beleid voor het Up-to-date houden van de systemen.
- Gebruik van Proxyserver om besmettingen via het web te beperken.
- Gebruik van Mail-gateway om besmettingen via email te beperken.

DMZ/VLAN/ACCESSLIST/FIREWALL

Zoals beschreven in het netwerk hoofdstuk is er binnen Ergon een virtuele scheiding aangebracht tussen de verschillende netwerken. In de praktijk betekent dit, dat het verkeer tussen het productie VLAN (servers, printers en werkplekken) gecontroleerd en beperkt is middels de interne firewall. Deze firewall heeft diverse access-list welke het verkeer toelaten of blokkeren conform het beleid. Een aantal gestelde beleidspunten betreffende het verkeer zijn:

- Het internet wordt per-definitie niet vertrouwd. Net als Wifi.
- Het Server Lan dient waar mogelijk afgeschermd te worden van het User-Lan



MANAGEMENT LAAG

Er is een aparte terminal server ingericht waarmee de beheerders het beheer verrichten, zodat er niet meer met hoge privilege accounts op de pc's hoeft te worden gewerkt.

MONITORING

Voor monitoring wordt gebruik gemaakt van PRTG Network Monitor. Het betreft een licentie van 1000 sensoren waarmee diverse componenten van de infrastructuur gemonitord worden.

SUPPORT

Voor de Hyper Converged servers en de core switches hebben we support contracten met HPE. Voor de meeste printers wordt de ondersteuning verzorgd door Toshiba.

Voor Firewall zijn er support contracten met Fortinet, maar tevens ook extra ondersteuning vanuit 4IP voor overige netwerkvraagstukken.

Stulz verzorgt het onderhoud van de 4 airco units die verdeeld zijn over de 2 computerruimtes.

TOOLING

Op de beheerserver zijn diverse tooling actief die bijdragen aan het eenvoudiger beheren van de ICT-infrastructuur. Veelal hebben de diverse systemen software of web interfaces om centraal diverse componenten te beheren. Hierdoor wordt het beheer zoveel mogelijk vanuit 1 centrale server/plaats gedaan. Onderstaande tooling is actief binnen Ergon:

- Dell Wyse Management Suite.
- WSUS voor het centraal updaten van servers en werkplekken.

Ook via andere systemen is er de beschikking over tools m.b.t. het beheer:

- Forti Analyzer voor het analyseren van het netwerkverkeer.
- InsightVM voor het monitoren van kwetsbaarheden.
- PRTG voor het monitoren van beschikbaarheid en capaciteit van diverse systemen.
- Citrix Director voor het beheer van de actieve sessies en ondersteuning van de eindgebruiker.
- Virtual center server voor het beheren en monitoren van de VMWare vSphere omgeving
- Store virtual Central management console voor het beheren van de storage omgeving
- VEEAM back-up & Replication manager en Enterprise manager voor het beheren van de VEEAM-omgeving
- Windows Configuration Designer voor het maken van installatie packages voor het installeren van de laptops.
- BitDefender gravity zone voor het beheer van de BitDefender antivirus/antispam software
- Aruba Wifi controller en Aruba Air wave voor het beheren van de wifi-access points