Alkum DCS

Data Continuity Services

Inhoud

Introductie DCS

Data **C**ontinuïteit **S**ervices: Het efficiënt beheren veiligstellen en herstellen van data.

Samen met onze partners biedt Alkum een continuïteitsoplossing met het oogpunt op veiligheid en beschikbaarheid van data. Of deze data zich nu lokaal, in de Cloud of verspreid over meerdere locaties bevindt, is voor DCS geen belemmering. DCS volgt de data door overal dezelfde graad van bescherming te bieden en past bij ieder type organisatie!

DCS is een service die Alkum levert als een volledige outsourcingsoplossing en wordt aangeboden met als primair doel om klanten te ontzorgen. Door te helpen met de back-up, herstel en Disaster Recovery (DR) strategieën, het aanbieden van onze DCS Cloud en het leveren van de benodigde lokale resources (hard- en software incl. installatie en configuratie diensten) hoeft men geen zorgen meer te hebben over het ingewikkelde en tijdrovende proces om back-ups te controleren, herstelacties uit te voeren en tevens na te moeten denken hoe DR-processen gedefinieerd moeten worden. Alkum levert DCS als een end-to-end service!

Zijn we klaar voor het datatijdperk?

Gebruikersfouten, hardware- en connectiviteitsproblemen en niet in de laatste plaats cybercriminaliteit kunnen leiden tot downtime en dataverlies. Downtime is niet meer acceptabel voor de bedrijfscontinuïteit en dataverlies niet vanwege de strenge privacyregels.

Dit alles speelt zich af in steeds complexer wordende IT-infrastructuren, waarin het beheer steeds meer tijd in beslag neemt, ook als het gaat om dataprotectie en disaster recovery. Om data te beschermen en tegelijkertijd de snelle veranderingen te blijven ondersteunen is een dynamische dataprotectie oplossing nodig die brede ondersteuning van applicaties en systemen combineert met eenvoudig centraal management en efficiënte centrale en decentrale dataopslag.

Voor maximale flexibiliteit zou een dataprotectie-oplossing onafhankelijk moeten zijn van de onderliggende, complexe IT-infrastructuur.

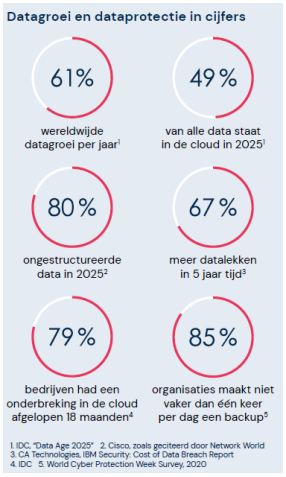
En dat is nu precies waar Alkum zich in heeft gespecialiseerd: één oplossing, één systeem, met één enkele interface waarmee alle data binnen een organisatie kan worden beheerd en beschermd, of deze zich nu bevindt op lokale servers, in de private of public Cloud of op endpoints.

Bescherming van digitaal bedrijfskapitaal

Nu bedrijven en organisaties volledig afhankelijk zijn van IT-systemen en data in feite het bedrijfskapitaal vormt, zijn hardware problemen, gebruikersfouten en de onveilige cyberwereld een immens risico voor de bedrijfscontinuïteit.
Downtime van cruciale systemen legt de bedrijfsvoering plat en verlies van cruciale data is onacceptabel vanwege omzetverlies, reputatieschade en de strenge wet- en regelgeving rond privacygevoelige data.
In dit datatijdperk wordt beschikbaarheid van data dan ook steeds belangrijker, maar tegelijkertijd ook complexer.

Complexiteit

Ondertussen groeit de hoeveelheid data exponentieel, volgens IDC zelfs met zo'n 61% per jaar, en worden IT-infrastructuren almaar complexer, met steeds meer al dan niet gevirtualiseerde workloads, public Cloud en verschillende typen systemen die elkaar aanvullen.
Consolideren van systemen blijkt niet overal te werken of te lukken, waardoor data verspreid staat over uiteenlopende platformen.
Deze complexiteit leidt tot tijdrovend beheer, vooral als het gaat om data- en opslagbeheer, dataprotectie en disaster recovery. Vaak worden verschillende tools naast elkaar gebruikt en is niet te achterhalen of alles wel voldoende wordt beschermd.



Kwetsbare infrastructuren

Digitale transformatie zorgt voor een enorme groei van het aantal 'connected' systemen en gebruikers. De groeiende hoeveelheid data, de spreiding van data over verschillende systemen en steeds meer endpoints maken IT-infrastructuren kwetsbaar, ook in verband met cybercriminaliteit. De snelle opkomst van ransomware aanvallen via phishing, credential theft en social engineering is een steeds groter probleem aan te worden. Niet voor niets blijkt uit de jaarlijkse World Cyber Protection Week Survey, dat bijna 90% van alle IT-managers zich zorgen maakt over cybercriminaliteit. De vraag is niet meer óf, maar wanneer een organisatie slachtoffer wordt. Snel herstel na een cyberaanval is dan ook essentieel voor **iedere** organisatie.

Dataprotectie wordt datamanagement

Waar lang geleden een eenvoudige back-up van data leek te volstaan, stellen moderne, Multi-Cloud omgevingen veel hogere eisen. Daarbij lopen dataprotectie, disaster recovery en het managen van de groeiende hoeveelheid data steeds meer door elkaar.

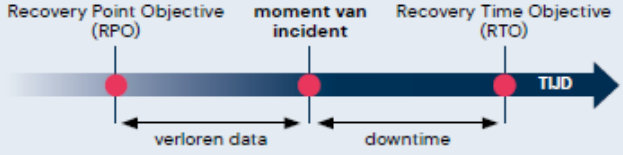
Back-up en Herstel

De spreiding van data over een groot aantal systemen, endpoints en de Cloud maakt van dataprotectie voor veel organisaties een uitdaging. Bovendien groeit de hoeveelheid data razendsnel en neemt het aandeel ongestructureerde data toe. Deze is lastiger te beheren, wat de situatie alleen maar complexer maakt. Waar staat alle data eigenlijk? Wordt er wel van alle data een back-up gemaakt? Wat gebeurt er met data in de Cloud? En hoeveel systemen voor back-up zijn er in gebruik? Kunnen bestanden, applicaties en systemen eenvoudig worden teruggezet na een incident?

Disaster Recovery

Bovendien is back-up maar één aspect van dataprotectie. Naast de mogelijkheid om data terug te kunnen zetten gaat het vooral om het vermijden van downtime. Bedrijfskritische applicaties die offline zijn kosten bedrijven veel geld en kunnen zelfs fataal worden. Naast back-up en herstel wordt daarom disaster recovery steeds belangrijker: zorgen dat systemen snel weer online komen, dat applicaties weer volledig werken, dat het bedrijf verder kan. Het maximale aantal uren downtime (RTO) en dataverlies (RPO) dienen te worden vastgelegd in een Service Level Agreement (SLA), waaraan een dataprotectie oplossing moet voldoen. Door de voortdurende datagroei, een toenemend aantal workloads en een steeds grotere afhankelijkheid van IT worden deze SLA's scherper en complexer. Hoe kan dataprotectie aan deze SLA's blijven voldoen?

RTO en RPO



Recovery Time Objective (RTO), zoals vastgelegd in een SLA, is de maximale tijd die acceptabel is om applicaties weer online te krijgen na een calamiteit.

Recovery Point Objective (RPO) in een SLA staat voor de maximaal acceptabele hoeveelheid dataverlies door een calamiteit, uitgedrukt in een tijdseenheid, bijvoorbeeld in uren voorafgaand aan systeemuitval.

Datamanagement en archivering

Die enorme hoeveelheid data maakt ook het beheren, het efficiënt opslaan en het archiveren van data steeds belangrijker. Welke data is cruciaal voor de bedrijfsvoering? Welke data wordt het meest geraadpleegd en welke data nauwelijks? En is alles wel eenvoudig terug te vinden? Efficiënt plaatsen van data, zoals het plaatsen van de cruciale data op snelle systemen en minder vaak geraadpleegde data op goedkopere of tragere media, kan een organisatie veel geld besparen terwijl data toch volledig toegankelijk blijft. Daarnaast is het belangrijk privacygevoelige data veilig en vindbaar op te slaan, om te kunnen voldoen aan strenge wet- en regelgeving zoals de AVG, maar ook om deze te beschermen tegen diefstal en andere cybercriminaliteit.

Eenvoudige wensen leiden tot lastige uitdagingen

Wensen vanuit de bedrijfsvoering...

De wensen vanuit de bedrijfsvoering ten aanzien van datamanagement en -protectie klinken vrij eenvoudig: data en applicaties moeten 24/7 beschikbaar zijn, voldoen aan regelgeving en systemen moeten flexibel genoeg zijn om snel innovatieve toepassingen te implementeren. En uiteraard moeten de kosten niet uit de hand lopen.

... worden uitdagingen voor IT

In een wereld waarin de hoeveelheid data groeit, het aantal applicaties en workloads toeneemt, systemen steeds complexer worden door virtualisatie en Cloud-toepassingen, betekenen eenvoudige eisen al gauw een flinke uitdaging voor IT-managers. Die uitdaging vormt het eisenpakket voor een datamanagement-oplossing.

Wensen vanuit de business		IT-uitdagingen en -eisen aan datamanagement
Zekerheid	Permanente beschikbaarheid van data en applicaties, vindbaarheid van informatie	Minimaliseren van downtime, snel en betrouwbaar herstel van data, applicaties en systemen na incidenten, kunnen voldoen aan SLA's, uitgebreide zoekfuncties binnen data
Veiligheid en Reputatie	Bescherming van gevoelige data tegen cybercriminaliteit en diefstal	Versleuteling van data, monitoren van dataprocessen en snel kunnen reageren op verdachte afwijkingen en Ransomware
Compliance	Voldoen aan dataprivacy- regels en intern governance-beleid	Beleidsmatige omgang met data en archivering, vindbaarheid privacygevoelige data
Volledigheid	Zeker weten dat alle data beschikbaar is en beschermd wordt	Brede ondersteuning voor besturingssystemen, hardware, tape, snapshots, software, hypervisors, Cloud providers, eindpunten
Flexibiliteit	Geen belemmeringen voor innovatie	Snelle acceptatie van nieuwe applicaties en workloads, eenvoudig schaalbare oplossing, ondersteuning voor applicatieontwikkeling en testen
Overzicht	Controle over IT-omgeving en minder risico	Inzicht in de status van systemen in 1 oogopslag, permanente en slimme analyse van systeemstatus, databeheer en beveiliging op een consistente manier, inclusief rapportagemogelijkheden
Eenvoud	Minder risico	Houd complexe omgeving beheer(s)baar door eenvoudig (zelfgestuurd) beheer en 1 enkele interface voor gegevensbeheer en -bescherming
Tijdwinst	Ruimte voor innovatie, hogere productiviteit, minder fouten	Automatisering van tijdrovende handmatige beheertaken (zoals provisioning en migratie), zelfgestuurde gegevensbescherming op basis van AI en machine learning
Efficiëntie	Kostenbesparing en hogere prestaties	Efficiënte opslag van data, de-duplicatie, databescherming die minder bandbreedte gebruikt, archivering van ongebruikte data of goedkope(re) media, cruciale data op de snelste systemen

Dataprotectie en datamanagement volgens Alkum

DCS levert een complete, geïntegreerde dataprotectie- en datamanagement oplossing voor Multi-Cloud IT-omgevingen. DCS ondersteunt ieder type workload en iedere locatie: hybride, lokaal, Cloud, fysieke servers, virtual machines (VM's), applicaties en databases, endpoints-apparatuur en meer ondersteund door SLA's die samen met de klant worden gedefinieerd. Door de rijke functionaliteit en de zeer brede ondersteuning van platformen, applicaties, snapshots, hardware, hypervisors en Cloud-providers is DCS overal inzetbaar. Naast back-up, herstel en archivering, biedt DCS veilige encryptie, efficiënte de-duplicering en bedrijfszekere disaster recovery (DR). Daarbij kunnen o.a. ook endpoints, Microsoft Office365, Microsoft Dynamics, (Azure) Active directory en Salesforce volledig beschermd worden.

Het unieke van DCS ligt in de holistische aanpak van datamanagement die volledig voldoet aan de eisen die hedendaags aan een datamanagement oplossing worden gesteld. DCS maakt overal gebruik van dezelfde backend services die naadloos samenwerken met alle functionaliteit welke beschikbaar is vanuit één enkele, centraal aangeboden, interface. Bovendien is DCS zo ontwikkeld dat datamanagement onafhankelijk van de onderliggende infrastructuur functioneert. Daarmee consolideert DCS-dataprotectie en vergemakkelijkt de service het verplaatsen van data en workloads.

DCS beschermt

Multi-Cloud back-up

Back-up binnen moderne Multi-Cloud omgevingen is vaak problematisch. DCS ondersteunt meer dan 40 Cloud opslag-opties in public en private Cloud. Hiermee wordt vanuit een hybride Cloud omgeving back-up en herstel van data mogelijk naar de Cloud, binnen de Cloud en tussen Clouds.

Virtuele machines

Virtualisatie is een krachtige en flexibele manier om de explosie van data en applicaties een plaats te geven. Maar het creëren van virtuele servers, opslag en applicaties tussen private en public Cloud-omgevingen levert weer nieuwe uitdagingen op. Back-up, herstel en beheer van VM's wordt door DCS eenvoudig gemaakt, waar deze zich ook bevinden en welke hypervisor ook wordt gebruikt. Geen standalone producten meer, geen datasilo's, geen overbodige infrastructuur en geen VM-versplintering.

Applicaties en databases

Applicaties en Databases hoeven niet meer met behulp van verschillende tools beschermd te worden. De brede ondersteuning door DCS van applicaties en databases is ongeëvenaard. Workloads kunnen naar de Cloud gemigreerd worden, databases kunnen efficiënt veiliggesteld worden en toegang tot data wordt versneld, dit alles binnen één enkele oplossing.

Endpoints

Bescherming van applicaties en databases is noodzakelijk, maar van endpoints net zo. Zo'n beetje de helft van alle data staat op desktops, laptops en mobiele systemen. Daaronder bevindt zich ook belangrijke klantinformatie en intellectueel eigendom. Vaak worden deze systemen misbruikt voor cyberaanvallen, waaronder ransomware. Des te meer een reden om ook deze systemen te beschermen.

Disaster Recovery

Hardware problemen, datacorruptie en ransomware aanvallen zijn bijna niet te vermijden. De crux zit hem in het hebben van een goed, sluitend herstelplan mocht het zo ver zijn. Daarbij is het belangrijk de balans te zoeken tussen herstel-eisen, kosten en de afgesproken serviceniveaus. Niet alle data is gelijk, RPO's en RTO's moeten gekoppeld zijn aan het belang van de data en de applicaties, zonder het herstelplan complex te maken door inzet van verschillende tools. De eenvoudig te gebruiken oplossing van DCS maakt herstel van elk type data mogelijk op elke mogelijke locatie – ook in de Cloud.

DCS beheert

Data groeit, de complexiteit van IT-omgevingen wordt groter en er worden steeds hogere eisen gesteld op gebied van veiligheid en compliance. Door integratie van datamanagement en dataprotectie ondersteunt DCS de volledige levenscyclus van data en stroomlijnt het alle dataprocessen.

Cloud en Hybride IT datamanagement

Met DCS kan data flexibel gemigreerd, beheerd en gebruikt worden van, naar en tussen meerdere Cloud- en lokale- omgevingen. DCS maakt een geautomatiseerde en georkestreerde aanpak mogelijk van provisioning, migratie en beheer van data binnen hybride Cloud omgevingen. Dat zorgt voor minder risico's en lagere kosten in vergelijking tot de complexe handmatige processen van point-producten. In één oogopslag is de status van data binnen public, private en hybride Cloud-omgevingen vanuit één dashboard te overzien.

Veiligheid

Beveiliging is een standaard onderdeel van DCS, waar de data ook staat en of de data nu stilstaat of in beweging is: lokaal, in de Cloud, of op desktops en laptops. Door efficiënte encryptie, granulaire toegang op maat, rol gebaseerde beveiliging, veiligheidsmeldingen en audits blijft data veilig en behoren privacy-schendingen tot het verleden.

Archivering

Retentiebeleid kan worden gedefinieerd op basis van relevante criteria als bestandsnaam, type, inhoud, tags en keywords. Op basis daarvan wordt data automatisch georganiseerd, geclassificeerd en gearchiveerd op secundaire opslagsystemen. Inactieve data wordt automatisch gedetecteerd en er wordt in één handeling zowel een back-up gemaakt als een archief aangelegd. Bovendien zijn er vervolgens eenvoudig kopieën te maken voor ontwikkeling- en testdoeleinden.

Indexering

De DCS-indexering lokaliseert alle mogelijke informatie, waar deze ook is opgeslagen in de infrastructuur: operationele systemen, archieven, media en endpoints. Met de intuïtieve interface kan gezocht worden, gecategoriseerd en kan data worden teruggehaald. Er kan zowel op metadata als op inhoud worden gezocht, waardoor zeer specifieke informatie teruggevonden kan worden.

Compliance

Om te voldoen aan compliance-eisen is vindbaarheid van data belangrijk. Op basis van het retentiebeleid wordt alleen die data opgeslagen die echt belangrijk is en met de zoekmachine kan data, ook al is deze opgeslagen op secundaire opslagsystemen en media, eenvoudig worden teruggevonden voor juridische en compliance-doeleinden. Doordat zowel binnen gestructureerde als ongestructureerde gezocht kan worden naar privacygevoelige informatie, kan deze snel gevonden worden om te kunnen voldoen aan de AVG. Daarnaast kunnen weloverwogen besluiten genomen over het al dan niet plaatsen van privacygevoelige data in de public Cloud.

Analyse en Rapportage

Inzicht in systeemstatus, compliance- en veiligheid risico's is essentieel om de juiste beslissingen te nemen rondom datamanagement. DCS monitort een groot aantal kritische factoren en biedt een breed scala aan mogelijke rapportages, volledig aan te passen aan de specifieke behoeften van een organisatie. De software analyseert de onderliggende processen en patronen en kan zowel waardevolle inzichten als waarschuwingen geven indien bepaalde processen afwijkingen laten zien.

DCS vereenvoudigd

Ondanks – of juist dankzij – de brede functionaliteit vereenvoudigt DCS-dataprotectie en datamanagement. Alle functionaliteit gebruikt dezelfde backend-processen en is via één enkele interface toegankelijk. Veel tijdrovende beheerprocessen zijn geautomatiseerd en data wordt zo efficiënt mogelijk opgeslagen.

Eén interface

Alle DCS-functionaliteit is te benaderen via één enkele interface. In de web gebaseerde interface worden back-ups en herstel policies geconfigureerd, dataprotectie beleid vastgesteld, taken gepland en de operatie gemonitord en gerapporteerd. Veel taken kunnen geautomatiseerd worden en via één dashboard kunnen taken, gebeurtenissen en meldingen binnen de gehele operatie worden overzien.

Omdat DCS het datamanagement van de totale omgeving op zich kan nemen, worden andere tools overbodig, wat resulteert in een flinke vereenvoudiging van het datamanagement.

Schaalbaarheid

Data groeit met de dag en de back-up omgeving mag dan niet achterblijven. DCS is eenvoudig, plug & play, te schalen waardoor deze mee kan groeien met de behoeften van de organisatie.

Efficiënte dataprocessen

Door data slim te verwerken bespaart DCS zowel op de directe opslagkosten als op de managementkosten die met dataopslag gepaard gaan. Back-up data wordt gededupliceerd voordat deze naar het secundaire opslagsysteem wordt verplaatst, wat veel tijd, bandbreedte en opslagruimte scheelt en bovendien herstellen flink versnelt. Daarnaast kunnen beleidsregels voor data ervoor zorgen dat ongebruikte data wordt verplaatst naar archieven of naar tragere systemen, waardoor de kostbare, snelle opslagsystemen efficiënter gebruikt worden. Tot slot kunnen dataprocessen geautomatiseerd worden en zorgt machine-learning ervoor dat tijdrovende, handmatige processen zoals provisioning of datamigratie grotendeels automatisch geschieden. Op deze drie manieren zorgt DCS dat minder tijd hoeft te worden besteed aan beheertaken en minder geld worden geïnvesteerd in opslagsystemen en benodigde opslagmedia.

Integratie en ondersteuning

Standaard ondersteunt DCS alle mainstream besturingssystemen, applicaties, arrays, hypervisors, Big Data-toepassingen en Cloud-providers. Door specifieke agents in te zetten voor complexe applicaties kunnen deze worden beschermd en door orkestratie werkend worden hersteld inclusief onderlinge afhankelijkheden. De brede ondersteuning van hypervisors en Cloud-providers samen met de onafhankelijkheid van onderliggende infrastructuren zorgt ervoor dat data eenvoudig verplaatst kan worden tussen Clouds en hypervisors onderling.

Snapshot beheer

De in DCS gebruikte snapshot beheertechnologie integreert de complexe levenscyclus van snapshots in een naadloos raamwerk. Deze geïntegreerde aanpak maakt het eenvoudiger de kracht van array gebaseerde snapshots te gebruiken en back-up en herstel te versnellen. Bovendien indexeert DCS de inhoud van alle snapshots, zodat deze niet slechts een ‘fotokopie’ blijven, maar dat individuele bestanden kunnen worden teruggevonden en hersteld indien nodig.

Ransomware protectie

Ransomware.... Eén klik op de verkeerde link en systemen of bedrijven worden gegijzeld. DCS gebruikt een combinatie van machine-learning, anomalie detectie en air gap technieken om ransomware aanvallen proactief te detecteren voordat deze schade kunnen aanrichten. De versleutelde back-up van bestanden kan worden getest in een veilige omgeving en daarna worden teruggezet. Multi-factor authenticatie, bedreigingsdetectie en onveranderlijke WORM (Write Once Read Many) opslag zorgen voor extra veiligheid waardoor DCS een hoge graad van veiligheid levert. Zo biedt DCS ook end-to-end beveiliging tegen infectie van ransomware en cyberaanvallen.

AAA-beveiligingsraamwerk

DCS beschermt de toegang, privacy en controle van back-up gegevens die zich op meerdere locaties bevinden, inclusief de Cloud. De onveranderlijke back-up gegevens van DCS maken gebruik van een uitgebreide reeks functies en bevatten de AAA-beveiligingsraamwerk principes:

Authenticatie biedt en verleent toegang tot back-up gegevens. Dit kan worden gezien als de 'poortwachter'. Functies omvatten certificaatverificatie, Multi-Factor authenticatie en integratie met meerdere externe identiteitsproviders met behulp van veilige protocollen zoals LDAPS, SAML en OpenID.

Autorisatie bepaalt welk toegangsniveau is toegestaan op DCS. Zodra authenticatie is toegestaan, heeft DCS verschillende controles, zoals op rollen gebaseerde beveiliging, privacy vergrendelingen en authenticatie op meerdere niveaus. Elk van deze functies werkt samen om te voorkomen dat gegevens worden geopend, opgehaald en verwijderd. Door deze controles toe te voegen ontstaat software-isolatie, waarbij zelfs beheerders worden geblokkeerd voor het verwijderen en openen van back-upgegevens en het ongedaan maken van beveiligingscontroles. Evenzo, als een kwaadwillende persoon/identiteit de toegang tot DCS steelt, worden de back-up gegevens beveiligd tegen kwaadwillende activiteiten binnen het platform.

Accountancy: Ten slotte dwingt DCS-aansprakelijkheid af door gebeurtenissen en acties binnen DCS te controleren en een uitgebreide aanpasbare interface te bieden om deze informatie te bekijken. Honderden rapporten zijn direct beschikbaar en bieden diepgaande informatie over de operaties, gebeurtenissen en acties binnen DCS. Informatie in rapporten en dashboards is alleen zichtbaar voor gebruikers die hier toegang toe hebben gekregen. Hierdoor kunnen eigenaren dezelfde auditrapporten en dashboards bekijken als beheerders, zonder bronnen te zien waarvoor ze geen toestemming hebben.

Onveranderlijke (immutable) back-ups in de Cloud

DCS biedt onveranderlijkheid van back-ups op locatie door het AAA-beveiligingsraamwerk, beveiligingscontroles, verharding, gegevensversleuteling en standaard ransomware-beveiliging te combineren. Bij het ontwerpen van een oplossing voor bescherming tegen ransomware en cyberdreigingen is het echter noodzakelijk om externe kopieën van gegevens te maken. Cloudopslag (private en/of public) is een voordelige oplossing omdat resources direct beschikbaar, elastisch en gelaagd zijn.

Bij gebruik van Cloudopslag (zoals DCS-opslag, Amazon Web Services (AWS) of Microsoft Azure), worden onveranderlijkheidsopties ingeschakeld op opslagniveau bij de Cloud leverancier. De Cloud bestemming is geconfigureerd als bibliotheek binnen DCS voor secundaire en/of tertiaire kopieën. Wanneer onveranderlijkheid in de Cloud is ingeschakeld, is de gehele opslagcontainer vergrendeld en kan de inhoud in de container niet worden gewijzigd of verwijderd gedurende het opgegeven tijdsbestek van onveranderlijkheid. Het gebruik van DCS met onveranderlijke cloudopslag heeft belangrijke voordelen ten opzichte van andere back-up serviceproviders.

Versleuteling en sleutelbeheer

Versleuteling van cloudopslag is prima om te voorkomen dat gegevens in rust worden gebruikt als ze worden gestolen. Dit voldoet echter niet aan de coderingsbehoeften aan de bronzijde. De FIPS 140-2 gecertificeerde versleutelingsmodule binnen DCS zorgt voor versleuteling bij de bron, voordat gegevens naar de Cloud worden verzonden. Dit zorgt ervoor dat elk gegevensblok dat naar de Cloud wordt verzonden, versleuteld en beveiligd is. Voor diepere beveiligingsniveaus kunnen versleutelingssleutels worden overgedragen aan externe sleutelbeheerservers, waaronder DCS, AWS, Azure of elk ander KMIP-compatibel systeem.

Waarom kiezen voor DCS?

Eén platform

In moderne, complexe en snel veranderende IT-omgevingen is vereenvoudigen en centraliseren van dataprotectie noodzakelijk voor de bedrijfscontinuïteit. DCS biedt een converged datamanagementplatform met één index om data te beheren, te verplaatsen en te herstellen binnen en tussen lokale systemen, hybride omgevingen en Cloud-locaties.

- Eén verenigd dataplatform – Via het intuïtieve DCS-beheerportaal is het eenvoudig data te beheren en te migreren van, tussen en naar waar dan ook.
- Gecentraliseerd beleid – Intelligente beleidsautomatisering beheert en beschermt de juiste data en applicaties met het juiste retentiebeleid.
- Single namespace index – Eén index waarin data wordt beheerd voor alle locaties, opslag typen (disk, Cloud of tape) en workloads. Dit vereenvoudigd beheer, de vindbaarheid van data en geeft betere inzicht.

Slimmer

Een intelligente aanpak vermindert repetitieve, tijdrovende taken en helpt organisaties te reageren op digitale bedreigingen en tegemoet te komen aan hedendaagse, strikte back-up vereisten. Met machine-learning, detectie van afwijkingen, slimme provisioning en efficiënt gebruik van opslag kunnen bedrijven data met vertrouwen herstellen.

- Machine-learning geïntegreerd – Identificatie, monitoring en automatisering van operationele processen zorgt voor zelfsturende back-up.
- Detectie van afwijkingen – Bestandsactiviteit wordt gemonitord op afwijkend gedrag dat wijst op ransomware en andere cyber criminele activiteiten.
- Slimme opslag/provisioning – Slimme opslag en provisioning analyseert en voorspelt opslaggebruik, optimaliseert back-up schema's en waarborgt beschikbare opslag om Recovery Point Objectives te kunnen blijven behalen.

Herstel met vertrouwen

Welk type data of welk platform dan ook, of het nu in de Cloud staat of lokaal, het kan met vertrouwen worden hersteld. DCS biedt een eenvoudige, moderne en kosteneffectieve oplossing voor Disaster Recovery (DR), die data kan beschermen en herstellen vanaf vrijwel iedere locatie.

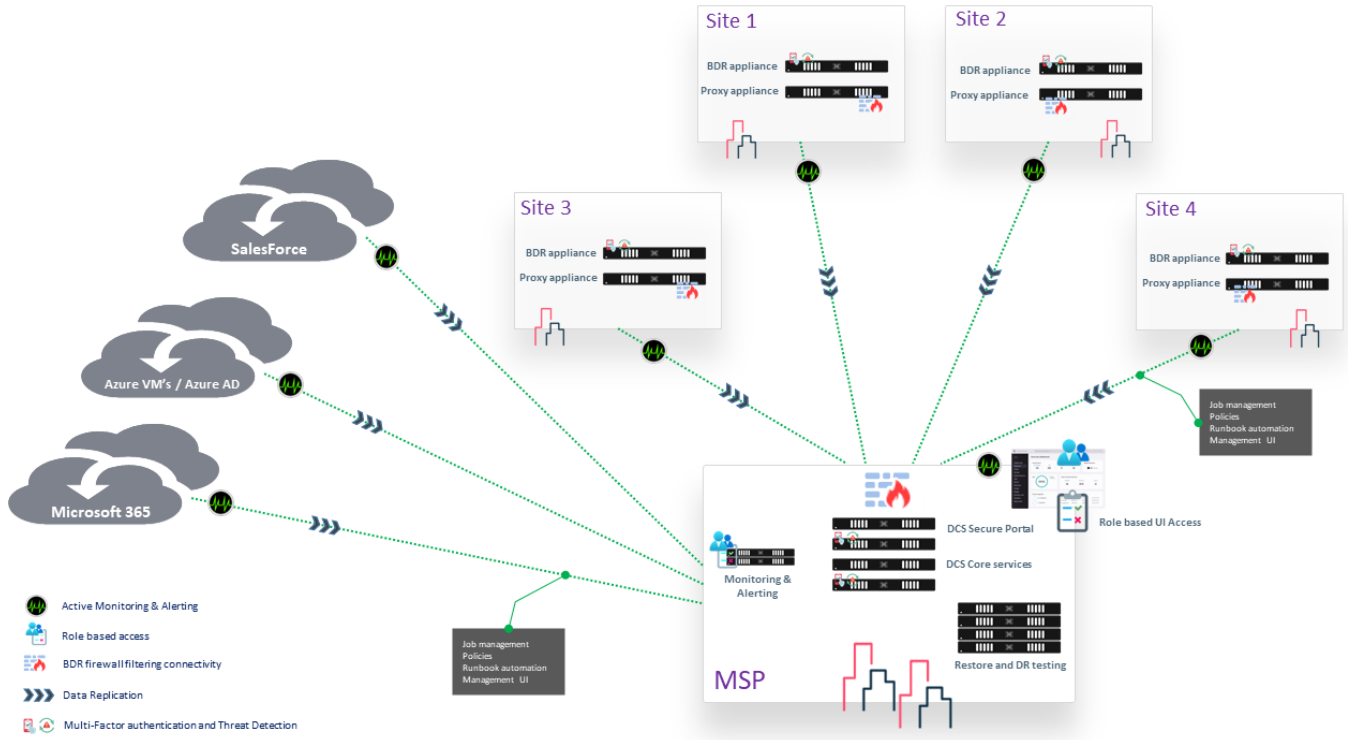
- Meerdere replicatietypen – Door de meest ideale replicatietechnologie op een platform toe te passen kan tegemoetgekomen worden aan specifieke dataprotectie-behoeften.
- Meerdere datatypen – DCS biedt robuuste dataprotectie en recovery met ondersteuning voor de meeste applicaties, databases, bestandssystemen en hypervisors.
- Meerdere platformen – Richt data herstel flexibel in voor fysieke servers, opslag systemen, hypervisors, applicaties, databases, Cloud-omgevingen, containers en zelfs Big Data-platformen.

Hoe werkt DCS?

Het fundament van DCS is gebaseerd op een aantal gemeenschappelijke kernfuncties, te weten: verzamelen, verplaatsen, opslaan, volgen en analyseren van data. Doordat al deze functies dezelfde backend-technologie delen wordt een holistische aanpak van bescherming, beheer en toegankelijkheid van data mogelijk. Deze aanpak is gebaseerd op beleidsregels die de nadruk leggen op gebruik, niet op locatie van data.

De productieservers worden met of zonder agent geconfigureerd. Deze kleine stukjes software sturen protectie- en archiefdata door naar de “Media Agents”. Hier wordt data geïndexeerd voor de Content Store en opgeslagen op back-up of archiefmedia. De Content Store is de centrale index van DCS en maakt alle andere functionaliteit mogelijk.

Het geheel wordt aangestuurd door de DCS Core systemen in ons datacenter. Het portaal via één enkele, web gebaseerde interface te benaderen. Toegang tot het portaal wordt op basis van, met de klant doorgesproken en vastgelegde, rollen bepaald. Een 1ste lijn supportmedewerker is bijvoorbeeld in staat om bestanden en folders te herstellen waar een beheerder meer granulaire controle heeft over volume of server herstel. Alkum kan deze rollen ook volledig op zich nemen waardoor de klant geen omkijken meer heeft naar de systemen en de herstelacties die plaats moeten vinden.



DCS Cloud protectie

1

Dataverspreiding & Silo's

IDC voorspelt dat in 2023 **60%** van de gegevens zich in de Cloud bevinden

2

Risico's zijn hoger

Cybercriminaliteit stijgt met **400%**
41% toename van Ransomware

3

Verhoogde aansprakelijkheid

Uw gegevens = uw verantwoordelijkheid. Bescherm Endpoints + SaaS-apps

Een nieuwe manier om Cloud gegevens te beheren en te beschermen?

Je hoort het – en beleeft het – elke dag: in de digitale wereld is verandering de enige constante. Nieuwe klantbehoeften, veranderende marktomstandigheden en opkomende omzetmogelijkheden kunnen de winnaars van vandaag veranderen in het "waar zijn ze nu?" Uw bedrijf is afhankelijk van gegevens om aan de top te blijven - en het hangt van u af om die gegevens beschikbaar en gereed voor actie te houden. Elke minuut. Elke dag. Elke keer.

Maar er is een brutale ironie in de kern van digitale zaken. Dezelfde getransformeerde infrastructuur die uw bedrijf helpt om razendsnel te schalen, draaien en innoveren, maakt het ook steeds moeilijker om gegevens te beschermen. Multi Cloud- en hybride omgevingen kunnen kostbaar en uitdagend zijn om mee te werken, waardoor het moeilijk is om uw gegevens te verplaatsen, beheren en gebruiken.

Hoe gegevensbescherming in de Cloud past in IT-modernisering

Moderniseren, moderniseren, moderniseren – die stem heeft u de hele dag in uw hoofd. Ondertussen weet u dat u iets moet doen aan gegevensbescherming in de Cloud. Er is namelijk een natuurlijke fit tussen de twee initiatieven.

Door back-ups en archieven van tape of schijf naar de Cloud te verplaatsen, kunt u de focus (en het budget) verleggen van het onderhoud van legacy hardware naar inspanningen rond modernisering en transformatie. Tegelijkertijd, terwijl IT-modernisering gegevens naar meer soorten omgevingen verplaatst, helpt Cloud gegevensbescherming te voorkomen dat er verouderde silo's en processen meegenomen worden - of er zelfs meer gecreëerd worden - naarmate de organisatie verder komt in uw digitale toekomst.

De combinatie van tape of disk naar Cloud heeft veel te bieden. Betere toegang tot kritieke gegevens. Nieuwe technologieën zoals machine learning en kunstmatige intelligentie die u meer vertrouwen geven in de kwaliteit en beschikbaarheid van uw back-ups. Automatisering die de productiviteit, snelheid en nauwkeurigheid verbetert. Tools om activiteiten te stroomlijnen en de beveiliging te verbeteren, bijvoorbeeld door u te waarschuwen een toepassing of bestandssysteem op Ransomware te controleren als deze plotselinge of abnormale activiteit vertoont.

Microsoft Office 365-gegevensbescherming

Microsoft Office 365™ is een cruciaal onderdeel van de moderne bedrijfsgegevensomgeving, maar veel organisaties laten het buiten hun strategie voor gegevensbescherming in de Cloud. Dat is deels te wijten aan een veel voorkomende misvatting dat Microsoft dit soort dingen afhandelt. Het Office 365-abonnement omvat immers hoge beschikbaarheid en datareplicatie tussen Office 365-datacenters. Maar verwar replicatie en beschikbaarheid niet met back-up en herstel. Als de gegevens op uw primaire site gecompromitteerd of beschadigd zijn, wordt dat ook naar de secundaire site gerepliceerd. En het hebben van twee sets slechte gegevens zal niemand helpen.

Er zijn andere potentiële risico's voor Office 365-gegevens. Afgezien van de gebruikelijke risico's van hacking, malware en kwaadwillende insiders, is er altijd een kans op onbedoelde verwijdering. Als iemand de verkeerde toets indrukt en kritieke bedrijfsinformatie verdwijnt, heeft u dan een manier om deze snel terug te krijgen, voordat deze de bedrijfsvoering verstoort?

Hardware speciaal ontwikkeld voor DCS

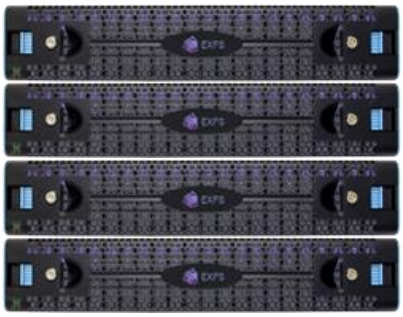
DCS ondersteund een grote variatie aan hardware leveranciers waaronder merken zoals Dell, HP, Nutanix, Cisco etc.

Alkum is zich er echter bewust van dat een back-up en DR-omgeving niet op hetzelfde platform zou moeten draaien als wat er in de productieomgeving wordt gebruikt. Met name veiligheid (firmware injecties en andere mogelijke aanvallen op hardware) ligt hierbij ten grondslag. Alkum heeft daarom hardware beschikbaar die specifiek ingezet wordt voor DCS, hierdoor ontstaat er een scheiding tussen productie en back-up resources niet alleen op software maar ook op de hardware laag.

Door de focus te leggen op de workloads die de hardware dient te kunnen leveren heeft DCS een zeer krachtig platform beschikbaar waarop de dienst volledig tot zijn recht zal komen.

Gecombineerd met replicatie naar meerdere locaties, bescherming van Microsoft Office365, Salesforce en ondersteuning voor vele andere Cloud providers en ons MSP model om de volledige zorgen uit handen van de klant te halen, is DCS in staat om klanten rust te bieden en zich geen zorgen meer te hoeven maken of de data veilig is tegen vele invloeden van binnen- en buitenaf waaronder cyberaanvallen en uitval van volledige locaties. Hierdoor is DCS de meest robuuste, simpelste, veiligste en krachtigste oplossing voor alle back-up en herstel, DR, archiverings-, beschikbaarheids- en veiligheidsuitdagingen.

EXFS voor DCS



Back-up producten zijn niet bedoeld om ransomware tegen te houden, maar om data veilig te stellen voor mogelijk herstel van bestanden, folders, volumes en zelfs volledige servers. Helaas zijn deze producten dus niet volledig opgewassen tegen cybercriminelen.
Om ervoor te zorgen dat back-up oplossingen beter bestand zijn tegen cyberaanvallen heeft Alkum met haar partners EXFS ontwikkeld.

Bescherm en beheer alles, altijd en overal!

Wat maakt EXFS uniek?

EXFS is een gesloten systeem en transporteert data vanaf de primaire back-up omgeving, via willekeurige schema's en poorten naar de EXFS Data Vault. Eenmaal veiliggesteld wordt de data integriteit gecontroleerd, willekeurige herstelacties om data integriteit te valideren uitgevoerd, en de benodigde virtuele stand-by's klaargezet om direct weer op te kunnen starten. Daarnaast zorgt Out-of-Band replicatie en management voor een hoge graad van beveiliging. Dit alles zonder dat er enige open connectie bestaat met de productieomgeving.

Het is een combinatie van, op een innovatieve methode, de back-up systemen in te richten van de klanten met "proven technology" back-up en veiligheidsproducten van vooraanstaande internationale leveranciers.

Extra bescherming met EXFS

Elke onderneming wil graag cybercriminelen buiten de deur houden en neemt daar de nodige frontlinie maatregelen voor met firewalls, server en end-point beveiliging.
Er wordt geïnvesteerd in goede back-up producten die op basis van softwareoplossingen ook eventuele cyberaanvallen (deels) afslaan.

De focus van een cyberaanval ligt op de volledige omgeving, beginnend bij het versleutelen van de back-up omgeving en vervolgens de productie omgeving. Bij een succesvolle aanval is er geen weg terug meer en is betalen een noodzakelijk kwaad geworden om de bedrijfscontinuïteit te waarborgen.

Let op: Back-up producten zijn tegenwoordig veelal uitgerust met een softwareoplossing tegen ransomware aanvallen. Het is een misverstand dat dit voldoende is!
Deze worden omzeild door de volledige opslag te vernietigen door bijv. RAID configuraties te verwijderen (zowel hard- als software RAID) en onherstelbaar te maken.

Een integrale aanpak van deze cyberbedreiging is dus nodig. EXFS is bestand tegen deze aanvallen en waarborgt ook uw bedrijfscontinuïteit door de gelaagdheid van veiligheidsmaatregelen die zich binnen de oplossing bevinden.

Ook voor de veeleisende grote of Enterprise-organisaties hebben we dezelfde oplossingsbenadering. Back-up servers, geïntegreerd 10 tot 100Gbe-netwerk connectiviteit, redundante firewalls, DR hypervisors, Out-of-band Cloudbeheer (vaste lijnen en optioneel 4G/5G LTE) om de hele omgeving af te sluiten van ongeautoriseerde toegang vanuit productie netwerken.

DCS: Een beter pad voorwaarts

DCS is een betere manier om back-up data te beheren en te consolideren die zorgt voor verbeterde flexibiliteit en schaalbaarheid, lagere kosten en vereenvoudigd beheer, terwijl de hoge beschikbaarheid behouden blijft die men van back-up softwareoplossingen gewend is/mag zijn. Een schaalbare architectuur beheert door Alkum maakt deze belofte waar.

Met DCS kunnen organisaties zowel de back-up oplossingen als de secundaire opslag back-up infrastructuur consolideren voor een efficiëntere, koste effectievere en schaalbare oplossing die met de organisatie meegroeit. Nog niet overtuigd? Neem contact met ons op en vertel ons uw uitdaging(en), wij helpen graag om vanuit een onduidelijke situatie duidelijkheid te bieden.

DCS is **DE** oplossing voor datamanagement, integriteit, continuïteit, en weerbaarheid in back-up en herstel, Disaster Recovery, archivering en data beschikbaarheid voor de volledige organisatie**!**

Tel: +31(0)85 0653 250
Mail: Info@alkum.nl
Inet: https://www.alkum.nl