

Dataverwijderingsoplossingen voor de beveiliging van datacentra en cloud computing

Blancco White Paper

Gepubliceerd op 23 oktober 2012

Tweede uitgave

Inhoudsopgave

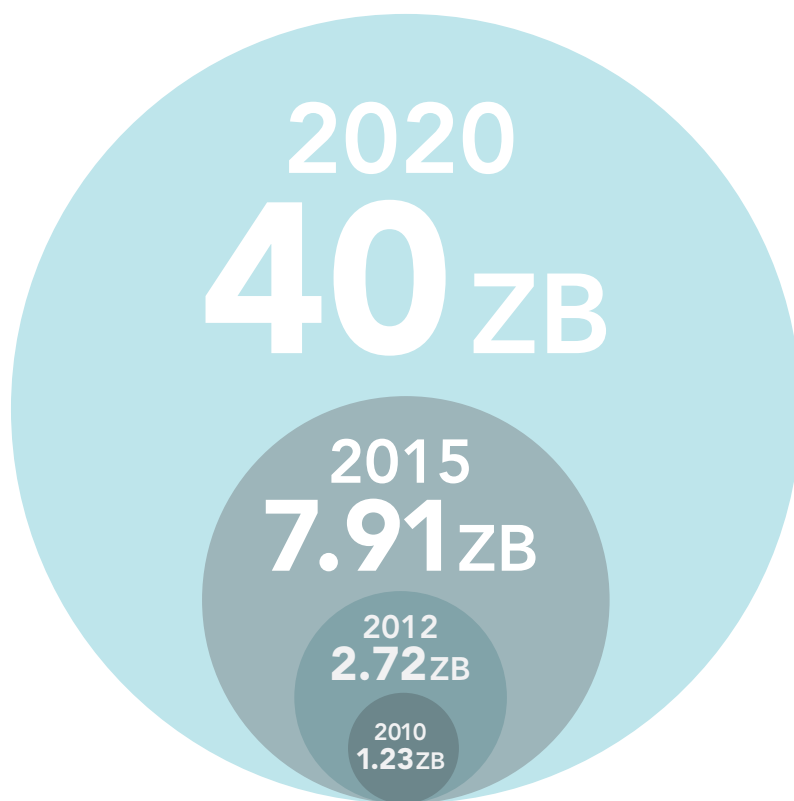
Samenvatting	3
De explosieve toename van data en informatiebeveiliging	4
Trends en verwijderingsbehoeften van datacentra	5
Milieuvriendelijke bedrijfsactiviteiten	5
Voorschriften en richtlijnen voor de beveiliging van informatie.....	6
Cloud computing	7
Consolidatie.....	7
Vijf niveaus van dataverwijdering	8
1. Verwijdering op bestandsniveau	8
2. Verwijdering op lun-niveau.....	9
3. Verwijdering op schijfniveau	11
4. Verwijdering op serverniveau	12
5. Verwijdering op opslagniveau	13
Gecertificeerde dataverwijdering voor complexe omgevingen.....	15
Referenties	16

Samenvatting

Door continue ontwikkelingen met betrekking tot wettelijke voorwaarden, consolidatie, milieueisen en cloud computing hebben datacentra behoefte aan betrouwbare, snelle en flexibele tools zoals gecertificeerde dataverwijdering voor de beveiliging van toenemende hoeveelheden klantgegevens. Datacentra zijn complexe hardware-omgevingen, met minstens zo complexe dataverwijderingsbehoeften. Gecertificeerde dataverwijdering voldoet aan deze behoeften door geautomatiseerde dataverwijdering voor een scala aan scenario's, van gerichte verwijderingsprocessen van bestanden voor PCI DSS-doelstellingen tot de verwijdering van data van logische eenheden, servers, losse harde schijven en opslagarrays.

Door alle informatie te verwijderen en door controleerbaar bewijs te leveren van dataverwijdering op kwetsbare hardware overgangspunten biedt gecertificeerde dataverwijdering datacentra de mogelijkheid om:

- Te voldoen aan de vereisten voor duurzame datacentrumactiviteiten door hergebruik van apparatuur.
- Het gebruik van IT-middelen intern te maximaliseren door hardware op een veilige manier opnieuw toe te wijzen.
- Klanten aan te trekken in gereguleerde bedrijfstakken zoals de detailhandel, de gezondheidszorg en het de financiële sector.
- Te voldoen aan consolidatie-vereisten met veilige overgangprocessen voor apparatuur.
- Een beveiligde en kostenbesparende cloud computing-omgeving te creëren, met solide dataverwijderingsprocessen.
- Dit witboek onderzoekt belangrijke trends in de branche die van invloed zijn op datacentra, met directe implicaties voor de noodzaak van gecertificeerde dataverwijdering. Ook worden gecertificeerde dataverwijderingsoplossingen belicht voor een scala aan hardware- en massaopslagconfiguraties die worden gebruikt in datacentra en cloud computing infrastructuur.
- Extra inkomsten te ontwikkelen met de veilige verkoop van apparatuur.



De explosieve toename van data en informatiebeveiliging

IDC voorspelt dat de hoeveelheid gecreëerde en geduplicateerde digitale informatie in 2020 zal zijn gegroeid tot bijna 40 biljoen gigabytes – oftewel meer dan 40 keer zoveel als nu.¹ Op een gegeven moment zal veel van deze informatie zich bevinden in datacentra en zal het worden beheerd door bedrijven of externe providers van opslagoplossingen, vooral gezien de groei van cloud computing-omgevingen. Gartner heeft de uitgaven voor hardware van datacentra wereldwijd – inclusief servers, opslag- en netwerkapparatuur – geschat op \$106,4 miljard en voorspelt dat dit in 2015 zal zijn toegenomen tot \$126,2 miljard.²

Een groot deel van de informatie die zich op hardware van datacentra bevindt is gevoelig en moet worden beschermd volgens een toenemend aantal branchevoorschriften en regelgeving zoals de Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) en Sarbanes-Oxley. Daarom hebben assetmanagers van datacentra behoefte aan een manier waarop ze informatie op kwetsbare overdrachtspunten kunnen beveiligen, en tegelijkertijd de levenscyclus van zakelijke opslagsystemen kunnen verlengen.

Het verwijderen van data is een belangrijke maatregel om te voorkomen dat data die niet worden gebruikt in beweging worden gebracht. Bij het beschermen van data die onderweg zijn ligt de focus normaalgesproken op data die online worden vervoerd en niet op data die worden vervoerd binnen de apparatuur van een groot datacentrum, wat het geval zou kunnen zijn wanneer een datacentrum fysiek naar een andere locatie verhuist of als de apparatuur van een datacentrum van eigenaar verwisselt.

Door de explosieve toename van digitale informatie, de verspreiding van datacentra, nieuwe regelgeving die databeveiliging verplicht stelt en andere belangrijke trends in de branche, is er behoefte aan een veilige dataverwijderingsoplossing zoals gecertificeerde dataverwijderingssoftware. Gecertificeerde dataverwijderingssoftware voldoet aan hoge beveiligingseisen, met geautomatiseerde verwijderingsprocessen voor een scala aan reguliere hardware- en massaopslagconfiguraties. De software is gecertificeerd en voldoet aan alle internationale richtlijnen voor veilige dataverwijdering. Bovendien beschermt de software gevoelige klantgegevens en zorgt het ervoor dat kan worden voldaan aan de wettelijke voorschriften. Gecertificeerde

dataverwijdering is een veilige, kostenbesparende technologie die ervoor zorgt dat kostbare en complexe systemen veilig opnieuw kunnen worden gebruikt of veilig kunnen worden verwijderd.

Door de explosieve toename van digitale informatie, de verspreiding van datacentra, nieuwe regelgeving die databeveiliging verplicht stelt en andere belangrijke trends in de branche, is er behoefte aan een veilige dataverwijderingsoplossing zoals gecertificeerde dataverwijderingssoftware.



Trends en verwijderingsbehoeften van datacentra

De toename van data en regelgeving in de afgelopen 10 jaar heeft voor datacentra een scala aan wijzigingen en uitdagingen met zich meegebracht. Op dit moment zijn er verschillende grote trends die veel invloed hebben op datacentra, met directe implicaties voor de noodzaak van gecertificeerde dataverwijdering, waaronder de vereisten voor milieuvriendelijke bedrijfsactiviteiten, hogere eisen aan informatiebeveiliging en –regelgeving, de toename van cloud computing en consolidatie van datacentra.

MILIEUVRIENDELIJKE BEDRIJFSACTIVITEITEN

Consumenten hebben behoefte aan duurzaamheid. Hierdoor ligt de nadruk steeds meer op milieuvriendelijke bedrijfsactiviteiten van datacentra. Energiebesparende technologieën zoals server-virtualisatie hebben ervoor gezorgd dat er minder apparatuur nodig is voor dezelfde taak en er

een langzamere toename van energieverbruik te zien is. Er zijn echter nog andere belangrijke overwegingen voor duurzaam opereren, zoals de beperking van elektronisch afval, waaronder computers, servers en Smartphones, door effectief bezittingenbeheer.

Elektronisch afval is een belangrijk onderdeel van de materiaalstroom van datacentra en is de snelst groeiende nationale afvalstroom in the Verenigde Staten (en waarschijnlijk in de wereld). Rapporten tonen aan dat het groeipercentage 8,6 procent is. Alleen al in 2007 werden er 41 miljoen computers weggegooid in de Verenigde Staten. Slechts 18 procent daarvan werd op de juiste wijze gerecycled.³ Door gecertificeerde dataverwijdering kunnen datacentra hun elektronische afval reduceren, doordat alle data van de apparatuur kunnen worden verwijderd en de apparatuur opnieuw kan worden gebruikt of verkocht, zonder de extra zorg dat data wellicht in de verkeerde handen vallen. Door de grote hoeveelheid elektronisch afval dat op onjuist wijze wordt overgedragen aan Ghana, is dit land volgens het ministerie van Buitenlandse Zaken in de VS een van de grootste bronnen van cybercriminaliteit. Door de weggegooide elektronica heeft Ghana bovendien te kampen met lucht-, bodemverontreiniging en besmet water.⁴

VOORSCHRIFTEN EN RICHTLIJNEN VOOR DE BEVEILIGING VAN INFORMATIE

De toename van het aantal ingenieuze inbreuken op de beveiliging van gegevens heeft geleid tot extra inspanningen om gevoelige informatie te beveiligen – maar liefst 75 landen hebben nu wetgeving voor gegevensbescherming en talloze sectoren ontwikkelen hun eigen regelgeving. Veel datacentra en aanbieders van cloudgebaseerde diensten bieden hun diensten aan in branches met uiterst gereguleerde data, zoals de detailhandel, het bankwezen, overheidsinstanties en de gezondheidszorg. Om deze klanten aan te trekken is het van groot belang dat kan worden voldaan aan de branchevoorschriften, wettelijke regelgevingen en certificeringen zoals respectievelijk PCI DSS, HIPAA en Sarbanes-Oxley. Met name aanbieders van cloudgebaseerde diensten zullen differentiëren en concurreren op basis van de effectiviteit en de mate waarin ze voldoen aan wettelijke voorschriften. Wat voor datacentra echter vooral belangrijk is, is de absorptie van de kosten voor naleving van wetgeving in de vorm van geautomatiseerde processen.

Ook is op dit moment in de Verenigde Staten uitgebreide regelgeving omtrent vereisten voor dataverwijdering in behandeling via de Consumer Privacy Bill of Rights, en in Eu-

Geavanceerde verwijderingssoftware biedt een geautomatiseerd, controleerbaar en doelgericht proces voor het verwijderen van data van bestanden, LUN's, harde schijven, servers en opslagsystemen. Het voldoet aan de wettelijke voorschriften en branchevoorschriften.

ropa via de wet- en regelgeving van de EU over verbeteringen in gegevensbescherming. In de Consumer Privacy Bill of Rights wordt uiteengezet hoe voortdurende innovatie in nieuwe informatietechnologieën mogelijk kan zijn terwijl tegelijkertijd de privacy wordt beschermd, inclusief de vereiste dat gegevens worden verwijderd. In de EU wordt regelgeving uit 1995 herzien omdat er nu rekening gehouden moet worden met nieuwe technologische ontwikkelingen zoals sociale netwerksites, cloud computing en op locatie gebaseerde diensten. Het voorstel is op dit moment in behandeling bij alle lidstaten van de EU. In het voorstel worden eisen gesteld aan verwijdering van online gegevens en aan het gebruik van controleerbare procedures voor bedrijven die persoonlijke gegevens verwerken. Er wordt aanbevolen om gecertificeerde systemen en processen te gebruiken. Bedrijven met cloudservice moeten voldoen aan deze regelgeving wanneer ze gegevens verwerken van ingezetenen van de EU, ongeacht de locatie van hun servers (binnen of buiten de EU).

Geavanceerde verwijderingssoftware biedt een geautomatiseerd, controleerbaar en doelgericht proces voor het verwijderen van data van bestanden, LUN's, harde schijven, servers en opslagsystemen. Het voldoet aan de wettelijke voorschriften en branchevoorschriften. Een belangrijk onderdeel van de naleving van regelgeving is een controleerbaar verwijderingsrapport, dat bewijst dat data op grondige wijze verwijderd zijn op kwetsbare overdrachtpunten, zoals bijvoorbeeld bij het opnieuw toewijzen van hardware of bij verkoop, tests voor noodherstel of een back-up en

verhuizing. Het rapport biedt hardware-specificaties, inclusief het serienummer, het aantal serverstations, het formaat en de snelheid. Ook bevat het informatie over het verwijderingsproces, bijvoorbeeld hoeveel tijd ermee gemoeid was en door wie het is uitgevoerd.

Datacentra hebben een controleerbaar rapport nodig van een gecertificeerde dataverwijderingstool om te bewijzen dat data verwijderd zijn van apparatuur die verwijderd of verhuisd is.

CLOUD COMPUTING

Er zijn bedrijven die investeringen in informatietechnologie (IT) willen afhouden als gevolg van een instabiele economie. Daarnaast is het zo dat de huidige generatie werknemers gewend is aan technologie op verzoek. Hierdoor wordt de groei van cloud computing (diensten via het internet) wereldwijd versterkt. Gartner voorspelt dat winst voor cloud computing in 2014 zal stijgen tot \$148,8 miljard. Forrester voorspelt dat de winst in 2020 \$241 miljard zal bedragen.⁵

Virtualisatie is een essentiële technologie voor cloud computing-omgevingen. Verwacht wordt dat het segmenteren van fysieke stations voor virtuele machines (VM's) een trend is die zich zal voortzetten, omdat het een efficiënter en kostenbesparend gebruik van hardware mogelijk maakt. Volgens voorspellingen van Gartner zal in 2014 ongeveer 60% van de serverwerkbelasting gevirtualiseerd zijn.⁶ De verwijdering van VM's stelt datacentra voor een uitdaging, omdat het moet worden bewerkstelligd in een actieve, online omgeving zonder dat andere VM's die op een bepaalde hardware draaien erdoor worden beïnvloed.

Door groei in de cloud computing markt zullen datacentra moeten blijven investeren. Door de toename van opgeslagen informatie en beheerde toepassingen moeten datacentra niet alleen het gebouw beveiligen, maar ook de waardevolle data die zich op hardware bevinden. En hoewel het verplaatsen van data naar de cloud via 'pulling' voorheen centraal stond, wordt er nu steeds meer aandacht besteed aan het beveiligen van deze data bij het verlaten van de cloud, zoals bij een verandering van serviceprovider. Dataverwijdering helpt aanbieders van cloud- en beheerdiensten een hoger beveiligingsniveau te bereiken, door data te verwijderen wanneer apparatuur opnieuw wordt toegewezen. Het gericht verwijderen van specifieke informatie is mogelijk op basis van tijd of gebeurtenissen. Dit is voorgeschreven in databeveiligingsnormen zoals PCI DSS.

CONSOLIDATIE

Fusies, acquisities, inkrimping en een scala aan andere initiatieven hebben geleid tot de consolidatie van datacentra. In het initiatief U.S. Federal Data Center Consolidation van 2010 zijn bijvoorbeeld plannen opgenomen om in 2012 meer dan 370 datacentra te sluiten, in een poging de overheidsuitgaven en de ecologische voetafdruk te reduceren.⁷

Hoewel veel datacentra opteren voor het vervangen van hun hardware bij het plannen van een verhuizing, raadt Gartner aan gebruik te maken van hun contracten en te onderhandelen over snelle beschikbaarheid van "swing gear" apparatuur op de nieuwe locatie.⁸ Wat er ook wordt beslist, datacentra hebben een controleerbaar rapport nodig van een gecertificeerde dataverwijderingstool om te bewijzen dat data verwijderd is van apparatuur die verwijderd of verhuisd is.

Vijf niveaus van dataverwijdering

Door dataverwijderingstechnologie kunnen datacentra gevoelige klantgegevens beschermen en wordt er voor gezorgd dat kan worden voldaan aan de wettelijke voorschriften. Tegelijkertijd wordt de productiviteit ondersteund en zijn de bedrijfsactiviteiten milieuvriendelijker. Deze dataverwijderingsoplossingen zijn van groot belang als het gaat om bescherming tegen het onbedoeld uitlekken van gegevens op overdrachtpunten in de hardware-keten (chain of custody) en in het gebruik. Om te kunnen voldoen aan strengere beveiligingseisen voor datacentra, kunnen geautomatiseerde verwijderingsprocessen worden ingezet voor een scala aan reguliere hardware- en massaopslagconfiguraties.

1. VERWIJDERING OP BESTANDSNIVEAU

Datacentra die te maken hebben met hoge beschikbaarheidseisen bewaren diverse kopieën van hetzelfde databestand voor redundantiedoelinden. Omdat databeveiligingsnormen zoals PCI DSS met specifieke tussenpozen verwijdering van data op bestandsniveau vereisen, hebben beheerders een gecentraliseerde manier nodig voor verwijdering op afstand van specifieke bestanden of mappen, of kopieën van bestanden of mappen, op servers en in opslaggebieden binnen het netwerk.

In omgevingen van Windows Distributed File System (DFS) moet dataverwijdering gelijktijdig worden uitgevoerd binnen overbodige en gespiegelde systemen om de produc-

tieve tijd te kunnen waarborgen, terwijl er ook een audit-trail moet zijn als bewijs van naleving van regelgeving. In de meeste gevallen is de verwijderingstool onzichtbaar op serverknooppuntniveau en wordt deze centraal beheerd door een systeembeheerder.

In een virtuele omgeving kan een VM worden geconfigureerd met een virtueel station dat bestaat uit een enkel bestand op een opslagnetwerk (Storage Area Network – SAN), een opslagapparaat of een plaatselijke harde schijf. Bij bepaalde scenario's kan het van belang zijn om de VM in een live omgeving te verwijderen, zonder de activiteiten te verstoren op het fysieke hostapparaat.



Afbeelding 1: Verwijdering op bestandsniveau.

VOORBEELDESCENARIO'S VOOR HET VERWIJDEREN VAN INDIVIDUELE BESTANDEN:

Naleving van PCI DSS

Op grond van PCI DSS-databeveiligingsnormen mag betaalkaartinformatie niet langer dan vijf jaar worden bewaard. Dit betekent dat datacentra een verwijderingsproduct nodig hebben dat gericht specifieke bestanden aanpakt op basis van tijd of gebeurtenissen.

Omgang met data

Verwijdering is onderdeel van het goed omgaan met data, zodat er niet onnodig veel kopieën van gegevens op onnodig veel plaatsen zijn opgeslagen. Zo wordt het risico op dataverlies beperkt.

Een professionele dataverwijderings-tool vernietigt individuele bestanden op basis van tijd of gebeurtenissen, of op indicatie van de gebruiker of de systeembeheerder.

Verspilling van data

Soms wordt gevoelige of vertrouwelijke informatie gekopieerd naar een systeem of toepassing die niet officieel erkend of bevoegd is. Met andere woorden, de gegevens zijn nog steeds in beheer bij de organisatie, maar ze zijn gekopieerd naar de verkeerde locatie. Geclassificeerde data moeten bijvoorbeeld worden verwijderd en niet alleen maar worden gewist op een ongeclassificeerd systeem.

Einde abonnement hostingsevice voor virtuele stations

Gerichte verwijdering van een VM met een virtueel station op een opslagsysteem of plaatselijke harde schijf is nodig wanneer een klant van serviceprovider verandert of wanneer de VM naar een andere locatie binnen een datacentrum migreert. Hiervoor heeft u een tool nodig die de verwijdering kan uitvoeren zonder dat het hostapparaat opnieuw moet worden opgestart. Na de verwijdering kan de opslagruimte veilig opnieuw worden gebruikt zonder de klantgegevens in gevaar te brengen.

Een professionele dataverwijderingstool vernietigt individuele bestanden op basis van tijd of gebeurtenissen, of op indicatie van de gebruiker of de systeembeheerder. Deze tool kan zo worden ingesteld dat hij alle Windows delete-opdrachten vervangt met beveiligde en gerichte bestandsverwijdering in real-time, zoals aangegeven op Afbeelding 1. Systeembeheerders geven aan welke regels en opslaggebieden van toepassing zijn vanaf een centrale interface. Er worden geen tijdelijke bestanden of 'gewiste' informatie achtergelaten die een bron zou kunnen vormen voor het uitlekken van gegevens. De oplossing kan worden beheerd als een service voor volledige controle, en alle activiteiten voor bestandsvernietiging worden vastgelegd.

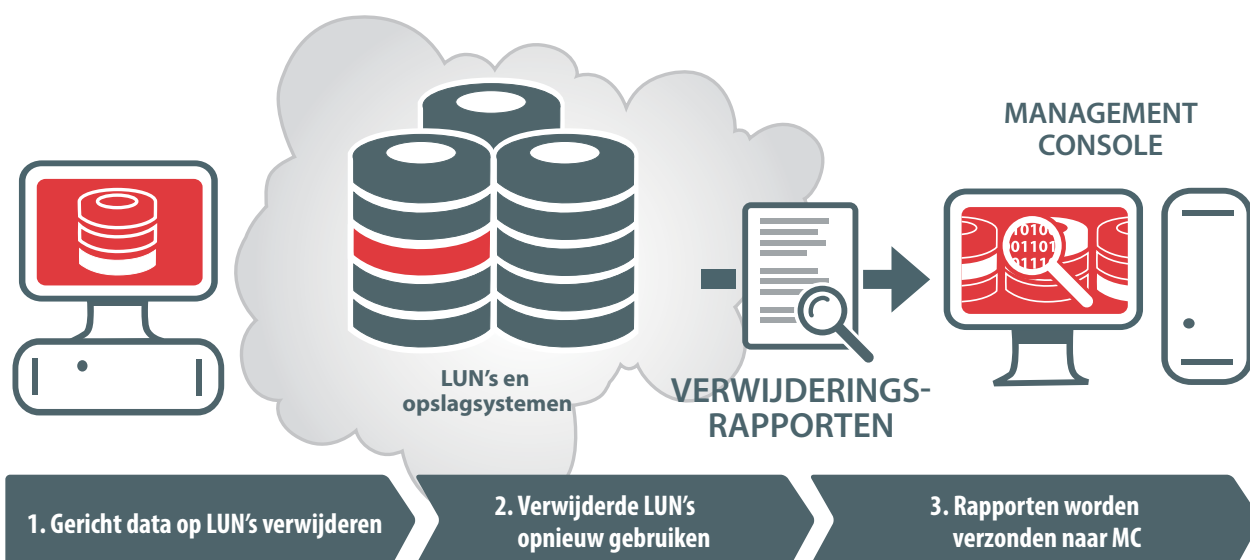
Bovendien is dataverwijderingssoftware compatibel met de Microsoft Windows Server 2008 R2 bestandsclassificatie infrastructuur (File Classification Infrastructure – FCI), waardoor de systeembeheerder specifiek bepaalde informatie kan verwijderen, zoals bijvoorbeeld beschermde gezondheidsinformatie (Protected Health Information – PHI) of PCI DSS-data, ongeacht de locatie op het netwerk. De tool heeft een flexibele backend waardoor eenvoudige integratie mogelijk is met intern ontwikkelde bestandsclassificatie en -beheersystemen.

2. VERWIJDERING OP LUN-NIVEAU

In de huidige cloud computing-omgeving hebben datacentra behoefte aan veilige, kostenbesparende opties voor hergebruik van systeemconfiguraties voor zakelijke opslagoplossingen, zonder deze opnieuw te moeten opbouwen. Om dit op een veilige manier te kunnen bewerkstelligen hebben systeembeheerders een gecentraliseerde tool nodig die data op logische stations zoals LUN's kan verwijderen in een live opslagomgeving waarin de opslagarray niet offline kan worden geplaatst.

In dit scenario kunnen VM's worden geconfigureerd voor toegewezen opslag van één of meer LUN's in een SAN-systeem.

Een verwijderingstool moet ondersteuning bieden voor een scala aan beleidslijnen, richtlijnen voor veilige dataverwijdering, regelgeving zoals PCI DSS, HIPAA en richtlijnen



Afbeelding 2: Verwijdering op LUN-niveau met live data.

van het Amerikaanse ministerie van Defensie (Department of Defense – DoD). Dit impliceert het aanbieden van controleerbare verwijderingsrapporten om verwijdering van LUN's te kunnen bewijzen, en tegelijkertijd gebruiksgemak en versnelde dataverwijdering. Verwijdering van LUN's gebeurt vanaf de toepassingsserver, waar de betreffende LUN doelgericht kan worden bekeken. Uiteraard biedt een goede verwijderingstool ook de mogelijkheid data op meerdere eenheden tegelijkertijd te verwijderen.

Veilige verwijdering van LUN's kan van groot belang zijn voor aanbieders van beheerde hosting en cloud computing, met klanten die zakendoen met bijvoorbeeld de Amerikaanse regering. Het Amerikaanse ministerie van Defensie vereist bewijs van verwijdering van alle klantgegevens wanneer een klant van serviceprovider verandert of wanneer een klant bij dezelfde serviceprovider van platform verandert. Zonder een LUN-verwijderaar die voldoet aan de vereisten van het Amerikaanse ministerie van Defensie moet de serviceprovider wellicht drastische maatregelen nemen om oude klantgegevens te verwijderen, bijvoorbeeld het offline plaatsen van een volledige opslagarray om data op fysieke stations te verwijderen of het in quarantaine plaatsen van oude LUN's met klantgegevens, waardoor opslagkosten oplopen. Met een LUN Eraser kan dezelfde serviceprovider nu, volgens de vereisten van het Amerikaanse ministerie van Defensie, data op een bestaande LUN verwijderen zonder dat andere gebruikers van de opslagarray hiervan hinder ondervinden.

VOORBEELDSCENARIO'S

VOOR VERWIJDERING OP LUN:

Einde abonnement hostingservice

Verwijdering van data is nodig om een LUN opnieuw te kunnen gebruiken in een host-omgeving als een klant vertrekt en een nieuwe klant aan een bestaande LUN wordt toegewezen. Dit scenario doet zich voor bij zowel fysieke servers die gebruikmaken van LUN's als opslag en voor VM's met toegewezen opslag op een bepaalde LUN.

Rampherstel-test (Disaster Recovery Test)

Na een test voor noodherstel bestaan er diverse kopieën van LUN-data. Om veiligheidsredenen moeten deze worden verwijderd.

Backup hersteltest (Back-up Recovery Test)

Net zoals bij een test voor noodherstel zal een test voor noodherstel met backup tape gemakkelijk terabytes aan data genereren op een groot aantal kopieën van LUN's en servers, die om veiligheidsredenen verwijderd moeten worden voordat de volgende klant gebruikmaakt van dezelfde hardware.

Zonder een LUN Eraser, die voldoet aan DoD of andere geldende voorschriften, moet de service provider drastische stappen ondernemen om oude klantgegevens te verwijderen.



1. HDD's aansluiten

2. Opschoning schijf uitvoeren

3. Rapporten worden verzonden naar MC

Afbeelding 3: Verwijdering van data op losse harde schijven.

Dataverwijdering biedt LUN-versies die gelijktijdige dataverwijdering bewerkstelligen op meer dan 200 eenheden door de software gelijktijdige meerdere keren in te zetten, hetgeen vanaf een centrale beheerdersinterface kan worden gestart zoals aangegeven op Afbeelding². De software zorgt voor verwijdering op elke willekeurige eenheid (fysiek of logisch) die door een Windows-, Unix-, of Linux-systeem kan worden opgespoord, door het gehele beschrijfbaar gebied sector voor sector te overschrijven, op het logische station of de harde schijf, afhankelijk van de geselecteerde verwijderingsprocedure. Er zijn dan verwijderingsrapporten beschikbaar ter ondersteuning van de mate waarin moet worden voldaan aan de gestelde voorwaarden.

3. VERWIJDERING OP SCHIJFNIVEAU

Verwijdering op schijfniveau is nodig voor het opschonen van harde schijven buiten de oorspronkelijke host, zoals bij losse harde schijven op Storage Area Network (SAN) servers. In veel gevallen betreffen het harde schijven waarvoor garantie geldt en waarvoor retourautorisatie nodig is (Return Material Authorization – RMA). De harde schijven moeten worden opgeschoond voordat ze worden teruggestuurd naar de merkleveranciers (Original Equipment Manufacturer – OEM).

Vanwege de vereisten met betrekking tot de afhandeling en mogelijke problemen in de hardware-keten (chain of custody) is het opschonen van lokale harde schijven noodzakelijk. Net als bij opschoning van een volledige array, is

bij het verwijderen van data op losse harde schijven een extern host-/opstartapparaat nodig, en de juiste connectiviteit tussen de op te schonen harde schijven en het betreffende host-verwijderingsapparaat. Tijdens de verwijdering dient een verwijderingstool ondersteuning te bieden voor controle en verwijderingsrapportage binnen het netwerk, wanneer een netwerkverbinding kan worden bewerkstelligd.

VOORBEELDCENARIO'S VOOR HET VERWIJDEREN VAN INDIVIDUELE SCHIJVEN:

Het vervangen van getourneerde harde schijven

Verwijdering op locatie van data op "falende" harde schijven verwijdert de inhoud van de schijf, zodat de schijf zonder risico's kan worden vervoerd naar de merkleverancier (OEM) voor vervanging. De hoge kosten voor het om veiligheidsredenen behouden van de falende harde schijf worden zo voorkomen.

Nog op te schonen harde schijven

Als er in het verleden aan het eind van de gebruiksduur geen veilige verwijderingsprocessen hebben plaatsgevonden, heeft een datacentrum harde schijven met gevoelige informatie die moet worden verwijderd om verlies van gegevens te voorkomen.

Het ruilen van harde schijven voor servers aan het eind van de gebruiksduur

Het omruilen en gebruiken van losse harde schijven als vervanging is een veel gebruikt en snel proces aan het eind van de gebruiksduur van een server. Er wordt gebruikge-



Afbeelding 4: Opschoning van servers op afstand.

maakt van vooraf opgeschoonde harde schijven, maar het genereert losse harde schijven met daarop onbeveiligde, intacte data.

Gecertificeerde dataverwijdering biedt de serveromgeving een dataverwijderingsoplossing op maat die razendsnelle, gelijktijdige verwijdering van data op alle aangesloten harde schijven (HDD's) garandeert. Het wordt uitgevoerd vanaf een verwijderingsapparaat op schijfniveau, zoals aangegeven op Afbeelding 3, om data te verwijderen vanaf harde schijven waarvoor garantie geldt (RMA-schijven), op indicatie van de systeembeheerder, die kan kiezen uit een scala aan internationaal ondersteunde richtlijnen voor veilige dataverwijdering. RMA-schijven van servers of opslagarrays worden simpelweg uit de behuizing gehaald en aangesloten op het verwijderingsapparaat, dat is uitgerust met dataverwijderingssoftware die herkent welke schijven moeten worden opgeschoond.

Met gecertificeerde dataverwijdering kunnen SCSI-, SAS-, SATA-, FC- en zelfs IDE-schijven tegelijkertijd worden opgeschoond. Wanneer het verwijderingsproces, dat gemiddeld één gigabyte per minuut in beslag neemt, voltooid is, wordt er automatisch een verwijderingsrapport gegenereerd en via het netwerk verzonden naar een beheerconsole of naar een database voor het beheer van IT-middelen. De console valideert het verwijderingsrapport als zijnde legitiem, controleert of de verwijdering compleet is en fungeert als opslagplaats voor verwijderingsrapporten. Gecertificeerde dataverwijdering ondersteunt ook de verwijdering van de

steeds gangbaardere Solid State Drives (SSD's) via een optie waarmee Flash-gebaseerde opslagmedia kunnen worden geselecteerd.

4. VERWIJDERING OP SERVERNIVEAU

Voor de volledige opschoning van servers dienen alle intern aangesloten schijven te worden opgeschoond. De opschoning van servers kan zowel plaatselijk als op afstand worden uitgevoerd. Verwijdering op afstand kan bijvoorbeeld eenvoudig worden geïmplementeerd met een virtueel CD-station voor servers met iLO/IPMI/DRAC-mogelijkheden. Controleerbare rapporten met betrekking tot hardwarefuncties en het dataverwijderingsproces zijn nodig voor het beveiligen van klantgegevens en om te kunnen voldoen aan de regelgeving van onder andere PCI DSS.

Voor complete beveiliging hebben datacentra verwijderingstools nodig die beschermde schijfgebieden en opnieuw ingedeelde sectoren tijdens het verwijderingsproces kunnen opsporen. Ze kunnen aangeven welke niet verwijderd mogen worden. Afhankelijk van het beleid en de risicotolerantie, kunnen datacentra de servers verkopen of op-

Gecertificeerde verwijdering biedt de serveromgeving een dataverwijderingsoplossing op maat die razendsnelle, gelijktijdige verwijdering van data op alle aangesloten harde schijven (HDD's) garandeert.



Afbeelding 5. Verwijdering op opslagniveau

nieuw gebruiken nadat dataverwijdering is uitgevoerd. Wat er ook wordt gekozen, data moeten worden verwijderd voordat een server het bedrijf verlaat.

Voor complete beveiliging hebben datacentra verwijderingstools nodig die beschermde schijfgebieden en opnieuw ingedeelde sectoren tijdens het verwijderingsproces kunnen opsporen. Ze kunnen aangeven welke niet verwijderd mogen worden.

VOORBEELDESCENARIO'S VOOR HET VOLLEDIG VERWIJDEREN VAN DATA OP SERVERS:

Einde gebruiksduur

Aan het einde van een hardware-vervangingscyclus moeten datacentra op een veilige manier alle informatie van servers verwijderen voor naleving van regelgeving en om klanten te beschermen. Hierdoor ontstaat de mogelijkheid gezonde schijven te verkopen of te recyclen. Tegelijkertijd wordt de datacentrumomgeving milieuvriendelijker en worden er inkomsten gegenereerd.

Einde abonnement hostingservice

Verwijdering van data is nodig om een server opnieuw te kunnen gebruiken in een hostomgeving, wanneer een bestaande klant niet langer gebruik wenst te maken van de hostingservice.

Verhuizing van een datacentrum

Er is regelmatig sprake van uitbreiding of verhuizing van datacentra, waardoor ook servers moeten worden verplaatst naar elders. Wanneer servers niet goed worden opgeschoond voordat ze worden vervoerd, bestaat de kans op verlies van gegevens.

Net als bij verwijdering op schijfniveau, is gecertificeerde dataverwijdering beschikbaar voor servers. In Afbeelding 4 ziet u hoe de systeembeheerder de verwijderingssoftware opstart vanaf een CD, USB of via het netwerk. De software identificeert vervolgens de geïnstalleerde schijven voor verwijdering, voert de verwijdering uit en stuurt het rapport naar een beheerconsole, database, of USB-geheugenstick.

X86- en x64-servers worden opgeschoond met gecertificeerde dataverwijderingssoftware. Gecertificeerde dataverwijdering kan bovendien data verwijderen van RAID en niet-RAID servers. Voor servers met een geïntegreerde RAID controller, "breekt" de verwijderingssoftware de RAID en schoont dan onmiddellijk alle interne harde schijven op volgens een door de systeembeheerder gekozen verwijderingsprocedure. Omdat SPARC-servers vaak worden gebruikt door datacentra ter ondersteuning van massaopslagbehoeften, zoals voor financiële instellingen, werkt een versie van de gecertificeerde dataverwijderingssoftware ook met de SPARC-architectuur van bedrijven zoals Oracle.

5. VERWIJDERING OP OPSLAGNIVEAU

Datacentra werken met een scala aan complexe opslagconfiguraties die inkomsten kunnen genereren aan het einde van de gebruiksduur. SAN-schijven en andere apparaten voor massaopslag kunnen worden verkocht als data op een veilige manier worden verwijderd voordat ze van eigenaar verwisselen.

Om de behoefte aan verschillende verwijderingsproducten te elimineren hebben datacentra met professionele server- en SAN-omgevingen een tool nodig die data op uiteenlopende hardware kan verwijderen, zoals Serial ATA-, SAS-, SCSI- en Fiber Channel-schijven. Vanwege de omvang van datacentra is gelijktijdige dataverwijdering op grote aantallen schijven een noodzaak.

VOORBEELDESCENARIO'S VOOR HET VERWIJDEREN VAN DATA OP OPSLAGSYSTEMEN:

Einde lease-periode

Aan het einde van een hardware-vervangingscyclus moeten data worden verwijderd voordat opslagsystemen worden teruggebracht naar het lease-bedrijf. Het behouden van de opslagsystemen is vanwege de kosten niet mogelijk, net als fysieke vernietiging – er zijn grote bedragen gemoeid met het niet teruggeven van apparatuur.

Het vervangen van hardware is aantrekkelijk

Aan het eind van een hardware-vervangingscyclus moeten datacentra op een veilige manier alle informatie van opslagarrays verwijderen, zodat ze gezonde schijven kunnen verkopen of recyclen. Tegelijkertijd creëert men zo een milieuvriendelijkere datacentrumomgeving. Het datacentrum – niet de merkleverancier – is eigenaar van de data en is verantwoordelijk voor de verwijdering ervan om het uitlekken van informatie te voorkomen.

Verhuizing van een datacentrum

Er is regelmatig sprake van uitbreiding of verhuizing van datacentra, waardoor ook opslagsystemen moeten worden verplaatst naar elders. Wanneer opslagsystemen niet goed

Om de behoefte aan verschillende verwijderingsproducten te elimineren hebben datacentra met professionele server- en SAN-omgevingen een tool nodig die data op uiteenlopende hardware kan verwijderen.

worden opgeschoond voordat ze worden vervoerd, bestaat de kans op verlies van gegevens of inbreuk op de beveiliging.

Een datacentrumversie van gecertificeerde datavernietigingssoftware biedt 100% veilige datavernietiging voor professionele opslagarrays. De software draait op een extern verbonden x86-server die niet direct is verbonden met SAN-hostpoorten, maar in plaats daarvan verbonden is met de Device Access Enclosure (DAE) voor opslag. Bepaalde opslagarrays zorgen voor rechtstreekse toegang tot diverse DAE's tegelijkertijd via geïntegreerde loop switches. Dit is bij opschoning de gewenste methode voor toegang tot schijven, omdat veel extra schijven gelijktijdig kunnen worden opgeschoond. De extern verbonden opstartserver moet worden geconfigureerd met de juiste Host Bus Adapter, zoals bij SCSI of Fiber Channel. Voor optimale prestaties is de juiste kabel nodig.

Na aansluiting start een systeembeheerder de dataverwijderingssoftware vanaf een externe opstartserver. De software kan tegelijkertijd meer dan 250 HDD's opsporen en opschonen binnen de opslagarray en de software kan snel data verwijderen op ATA-, SATA-, SCSI-, Fiber Channel- en SAS- harde schijven. Deze versie biedt ook de mogelijkheid opnieuw ingedeelde sectoren te verwijderen voor ATA/SATA/SCSI/Fiber Channel harde schijven, en genereert rapporten voor de registratie van IT-middelen, met statusindicatoren omtrent de gezondheid van harde schijven.



Gecertificeerde dataverwijdering voor complexe omgevingen

Omdat de cloud computing markt zich ontwikkelt en ook datacentra zich ontwikkelen om te kunnen voldoen aan de steeds hogere opslageisen, komt er steeds meer dataverwijderingssoftware op de markt als praktische, geautomatiseerde en controleerbare oplossing voor efficiënte en beveiligde bedrijfsactiviteiten. De software ondersteunt verwijdering van hardware en opslagconfiguraties binnen de datacentra, evenals gerichte verwijdering van mappen, bestanden en logische eenheden. Om minimale onderbreking en complete databeveiliging te waarborgen in een dynamisch datacentrum moeten systeembeheerders, gebruikers en klanten kunnen vertrouwen op gecertificeerde dataverwijdering als een tool voor de huidige en toekomstige vereisten.

Referenties

- ¹ <http://www.emc.com/about/news/press/2012/20121211-01.htm>
- ² Gartner, "Forecast: Data Centers, Worldwide, 2010-2015," oktober 2011
- ³ Emerson Network Power, "Recycling Ratios: The Next Step for Data Center Sustainability"
- ⁴ Newsweek, "Digital Dump," juli 2011
- ⁵ Wall Street Journal, "More Predictions on the Huge Growth of Cloud Computing," april 2011
- ⁶ Cloud Computing, "5 Cloud Computing Statistics You May Find Surprising," <http://cloudcomputingtopics.com/2011/11/5-cloud-computing-statistics-you-may-find-surprising/>, november 2011
- ⁷ Federal Data Center Consolidation Initiative (FDCCI) Data Center Closings 2010-2012, <http://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37>
- ⁸ Gartner, "Data Center Consolidation: Top 10 Best Practices for Project Success," Research Note, mei 2011

Delen van dit witboek verschenen eerder in het tijdschrift ITAK, jaargang 6, uitgave 8, gepubliceerd door de International Association of Information Technology Asset Managers.

Copyright © 2011 Blancco Oy Ltd. Alle rechten voorbehouden.

De informatie die in dit document is opgenomen vertegenwoordigt de huidige zienswijze van Blancco Oy Ltd met betrekking tot de aangegeven onderwerpen op het moment van publicatie. Vanwege veranderende marktomstandigheden kan Blancco de juistheid van informatie die na de publicatiedatum wordt gepresenteerd niet garanderen. Dit witboek dient uitsluitend ter informatie. Blancco geeft geen expliciete of impliciete garanties in dit document.

De gebruiker is zelf verantwoordelijk voor naleving van alle van toepassing zijnde wetten op auteursrecht. Zonder dat hierbij de inhoud van de wetten op auteursrecht wordt beperkt mag geen enkel onderdeel van dit document worden gereproduceerd, opgeslagen of worden geïntroduceerd in een archiveringsysteem, en in geen enkele vorm en op geen enkele wijze worden overgedragen (elektronisch, mechanisch, via kopieën, opnamen of anders), voor welke doelstelling dan ook, zonder expliciete schriftelijke toestemming van Blancco.



0800 5765 565, info@krollontrack.nl
www.ontrackdatarecovery.nl