

LEVERKENMERKEN DIENST BACK-UP EN DISASTER RECOVERY.

UITGANGSPUNT

De dienst Back-up en Disaster Recovery (B&R) (kort genoemd “de dienst”) is gebaseerd op de richtlijnen zoals deze vastgelegd zijn in ISO 27002 (NORA, 2018), control nummer 12.3.1 met een BBN waarde van 2. Deze zijn overgenomen in de Baseline Informatiebeveiliging Overheid (Overheid, 2019)

Volgens deze richtlijnen moet De Dienst Back-up in geval van een Disaster Recovery situatie minimaal voldoen aan:

- Een Recovery Point Objective (RPO) tijd van maximaal 28 uur dataverlies. De dienst houdt zelf maximaal 24 uur aan om daarmee een T3 dienst te kunnen aanbieden;
- Een Recovery Time Objective (RTO). Hersteltijd in geval van **incidenten** is maximaal 16 werkuren (2 dagen van 8 uur). De dienst heeft dit vertaald in 16 klokuren. In geval van een **disaster** wordt op dat moment bekeken wat haalbaar is.

De Belastingdienst hanteert, op basis van de architectuurkaders, een strenger beleid voor incident situaties. Op basis van de T3 classificatie gelden voor een incident situatie de volgende termen en normen (B/DCS, 2015):

- Acceptable Data Loss (ADL); maximaal aantal uren aan data wat verloren mag gaan, is vastgesteld op 12 klokuren;
- Acceptable Recovery Time (ART); tijd waarbinnen de dienstverlening hervat moet worden is eveneens vastgesteld op 12 klokuren.

Buiten de reguliere werktijden zal men aan het oplossen van het **incident** blijven werken.

BACK-UP PRODUCTEN

Om aan de vereisten te voldoen gebruikt de dienst het back-up product IBM Spectrum Protect en enkele aanvullende producten uit de Spectrum Protect Suite.

Tevens biedt de dienst de mogelijkheid om eigen back-up producten te gebruiken in combinatie met de backend van de dienst (Data Domain of SVC).

Naast deze twee mogelijkheden beheert de dienst ook nog het back-up cluster van de Dell/EMC Isilon NAS. De primaire taak van het back-up cluster bestaat uit het opslaan van back-ups met een langere bewaartermijn dan 30 dagen met als bron het primaire Isilon cluster. Echter, in overleg, kan het back-up cluster ook als backend fungeren zoals de Data Domain of SVC dit doen.

OMGEVINGSKENMERKEN

- De dienst is beschikbaar in beide ODC locaties van de Belastingdienst in Apeldoorn;
- De back-up data is binnen 24 uur (asynchrone replicatie) beschikbaar op beide locaties (voor zover hier door de klant om gevraagd wordt) zodat, in geval van een calamiteit, er uitgeweken kan worden;
- De dienst voldoet aan de richtlijnen voor het verwerken van departement vertrouwelijke gegevens (BBN2);
- De connectiviteit is IP gebaseerd (ethernet 1 of 10Gbit);
- Er is keuze uit SMB, NFS;
- De dienst heeft een gegarandeerde beschikbaarheid van 99,9% (zolang de netwerkdienst ook beschikbaar is).

Alles terug te vinden in de Dienstencatalogus (DCS, 2019)

- Back-up doorlooptijden. De volgende factoren bepalen de doorlooptijd van een back-up, te weten:
 - + het aantal bestanden;
 - + de grootte van bestanden of databases;

- + de structuur van databases;
- + de netwerksnelheid;
- + drukte op het netwerk.

De dienst heeft geen invloed op deze factoren en er kan een punt bereikt worden waarop de back-up doorlooptijd niet meer binnen het verwachtingspatroon past. Gekeken kan worden naar mogelijkheden tot tuning of dat er naar een andere back-up oplossing gezocht moet worden.

DATABASES EN APPLICATIES

Spectrum Protect ondersteunt de volgende database types:

- Microsoft SQL server;
- Oracle (en SAP Oracle);
- DB2;
- Lotus Notes.

Hiervoor dient lokaal op de client vaak een specifiek client software product geïnstalleerd te worden, een TDP (Tivoli Data Protection).

OPERATING SYSTEMS

Spectrum Protect biedt voor de volgende platformen clients aan:

- Unix/AIX;
- Windows;
- Linux (red hat, debian e.a.);
- Z/os.

APPLIANCES

De dienst biedt klanten een mogelijkheid om, buiten Spectrum Protect om, zelf een back-up te maken van hun omgeving. Hiervoor biedt de dienst een backend omgeving aan in de vorm van een Dell/EMC Data Domain (of een logische opvolger hiervan). De dienst is verantwoordelijk voor het operationeel houden van de Data Domain en de replicatie naar de andere ODC locatie. De klant is verantwoordelijk voor het maken en onderhouden van zijn back-ups alsmede de integriteit en monitoring van zijn back-ups.

De klant heeft de keuze uit SMB, NFS protocollen om een connectie te maken met de Data Domain.

MONITORING

De 1^e lijns eventmonitoring is uitbesteed aan de Centrale Monitoring en Oplossgroep (CMO), zij ontvangen als eerste de events over eventuele gemiste of gefaalde back-ups en zullen deze proberen op te lossen. Lukt dit niet dan wordt een incident doorgezet naar de 2^e lijn, de platform- of database teams. 3^e Lijns DevOps van het teamonderdeel B&R kan hierbij assisteren.

AANVRAGEN OM AAN TE SLUITEN OP DEZE GENERIEKE DIENST

Voor nieuwe klanten geldt dat er eerst een verzoek/intake moet worden gedaan bij de architect Storage. Deze bepaald of het qua hoeveelheid of data type past binnen de dienstverlening. Na goedkeuring kan er via de kavel catalogus, bij de aanvraag voor een nieuwe server, aangegeven worden of u wil aansluiten op Spectrum Protect (TSM). Het platform team zal dan een extra BNR interface beschikbaar stellen en configureren waarmee de koppeling naar de BNR server tot stand gebracht kan worden. Indien u met fysieke hardware aan wil sluiten kan dit ook, u dient hiervoor in uw systeem een separate interface voor te reserveren welke geconfigureerd kan worden om aan te sluiten op het BNR cliënt vlan. Het verdient de voorkeur dat deze interface 10Gb ondersteunt om voldoende snelheid te kunnen garanderen. Tevens dient u een Spectrum Protect cliënt te installeren waarmee de koppeling met de BNR server gemaakt kan worden. De software zal u door de dienst aangeleverd worden alsmede consultancy zodat u de software kunt configureren.

BRON DOCUMENTEN

B/DCS. (2015, juni 25). Technische Architectuurkaders BCM CIE V1.0. Apeldoorn.

DCS. (2019). ICT Dienstencatalogus. (kwartaal 1).

NORA. (2018, December 12). *Basisprincipes*. Opgeroepen op februari 10, 2019, van Noraonline: <https://www.noraonline.nl/wiki/Basisprincipes>

Overheid. (2019, 05 23). Baseline Informatiebeveiliging Overheid (BIO). (Versie 1).