VDSS

Plannen voor de Cloud Monitoring

Inhoudsopgave

1 Inleiding....3
2 Huidige situatie....4
3 Nieuwe situatie....4
4 Functionele eisen en wensen....5
5 Voorgestelde veranderingen....6
5.1 Cloud omgeving Super User Menu....6
5.1.1 Cloud omgevingen toevoegen....7
5.1.2 Microsoft OneDrive en SharePoint toevoegen....8
5.2 OneDrive en SharePoint in Normal User menu....10
5.2.1 NUM → Cloud Settings → Files....11
5.2.2 NUM → Cloud Settings → Rules....13
5.2.3 VDSS Show → Details (voor OneDrive en SharePoint)....15

1 Inleiding

Er is grote vraag naar cloud monitoring via VDSS, klanten zien hier grote meerwaarde in. Gezien we nu met de VDSS Agents al File Servers en Workstations monitoren, is uitbreiding naar Cloud monitoren een logisch vervolg. Met deze uitbreiding kunnen wij alle files in hybride netwerken monitoren.

Dit document geeft een eerste indruk van de wijzigingen die wij van plan zijn in VDSS aan te passen. De Acceptatie levering zal eind oktober 2022 zijn.

2 Huidige situatie

Op dit moment kan VDSS met behulp van VDSS agents file monitoring doen op Windows, Linux en macOS, servers en workstations. Hierbij kan de VDSS agent zien wanneer welk bestand door wie aangepast/geopend/verwijderd wordt. VDSS kan ook zien welk programma of IP dit heeft gedaan en kan daardoor eventueel zelfs het programma of IP in quarantaine zetten.

3 Nieuwe situatie

VDSS kan met behulp van VDSS Agents file monitoring doen op de volgende cloud diensten Microsoft OneDrive en SharePoint. Hierbij kan de VDSS agent zien wanneer welk bestand is aangepast/verwijderd in de cloud. VDSS kan ook zien welke gebruiker dit heeft gedaan.

Bij dit project wordt gefocust op de Microsoft Cloud: OneDrive en SharePoint. In de toekomst komen er meer cloud diensten bij, daar wordt alvast rekening mee gehouden tijdens het ontwikkelen.

Een VDSS gebruiker kan in een aparte clouds menu OneDrives en SharePoints toevoegen, bewerken en verwijderen in de monitoring. Hierbij kan de VDSS gebruiker aangeven welke VDSS Agent de OneDrives en SharePoints mag uitvragen. Een VDSS Agent kan meerdere OneDrives en SharePoints uitvragen. De VDSS Agent vraagt de cloud uit en stuurt notificaties naar de Server als er bestanden zijn gewijzigd of gedelete binnen de betreffende OneDrive of SharePoint.

De VDSS Server behandeld notificaties, die namens een OneDrive of SharePoint door de VDSS Agent gestuurd wordt, hetzelfde als bij notificaties van een VDSS Agent.

4 Functionele eisen en wensen

In dit hoofdstuk worden de eisen en wensen voor deze feature beschreven.

- Microsoft OneDrive / Sharepoint file monitoring worden geleverd.
- Cloud monitoring zal impact hebben op de performance van de agent, hier wordt rekening mee gehouden.
- Agent met cloud monitoring gebruikt niet meer performance van de server dan een Agent zonder cloud.
- Als een IT bedrijf meerdere klanten heeft en elke klant zijn eigen Microsoft omgeving, dan kan dit met een enkele VDSS Agent gemonitord worden, dit maakt de Agent geschikt voor SaaS.
- Microsoft omgevingen kunnen worden toegevoegd als Cloud Environments aan de monitoring.
- Microsoft accounts kunnen worden toegevoegd als Microsoft OneDrives in de monitoring.
- Microsoft SharePoints kunnen worden toegevoegd als Microsoft SharePoints in de monitoring.

5 Voorgestelde veranderingen

Je kunt Cloud omgevingen toevoegen en instellen binnen de GUI van VDSS. Het toevoegen gebeurd via het Super User Menu en dan “Clouds”. De instellingen betreffende welke files je wilt monitoren kun je via het Normal User Menu en dan “Cloud Settings” configureren.

5.1 Cloud omgeving Super User Menu

Er komt een extra menu item in het Super User menu genaamd “Clouds”, hier kun je het volgende instellen:

- **Cloud Environments**, hierin kun je een Microsoft omgeving toevoegen aan de monitoring, dit is nodig om OneDrive of SharePoint te monitoren. Elke klant heeft vaak zijn eigen Microsoft omgeving.
- **Microsoft SharePoints**, hierin kun je een SharePoint toegang vragen om te kunnen monitoren met een VDSS Agent.
- **Microsoft OneDrives**, hierin kun je een OneDrive toegang vragen om te kunnen monitoring met een VDSS Agent.

Als de VDSS gebruiker op het menu “Clouds” klikt dan komt het onderstaande scherm naar voren. Hier zijn twee tabellen te zien: “Cloud environments” en “Cloud services”.

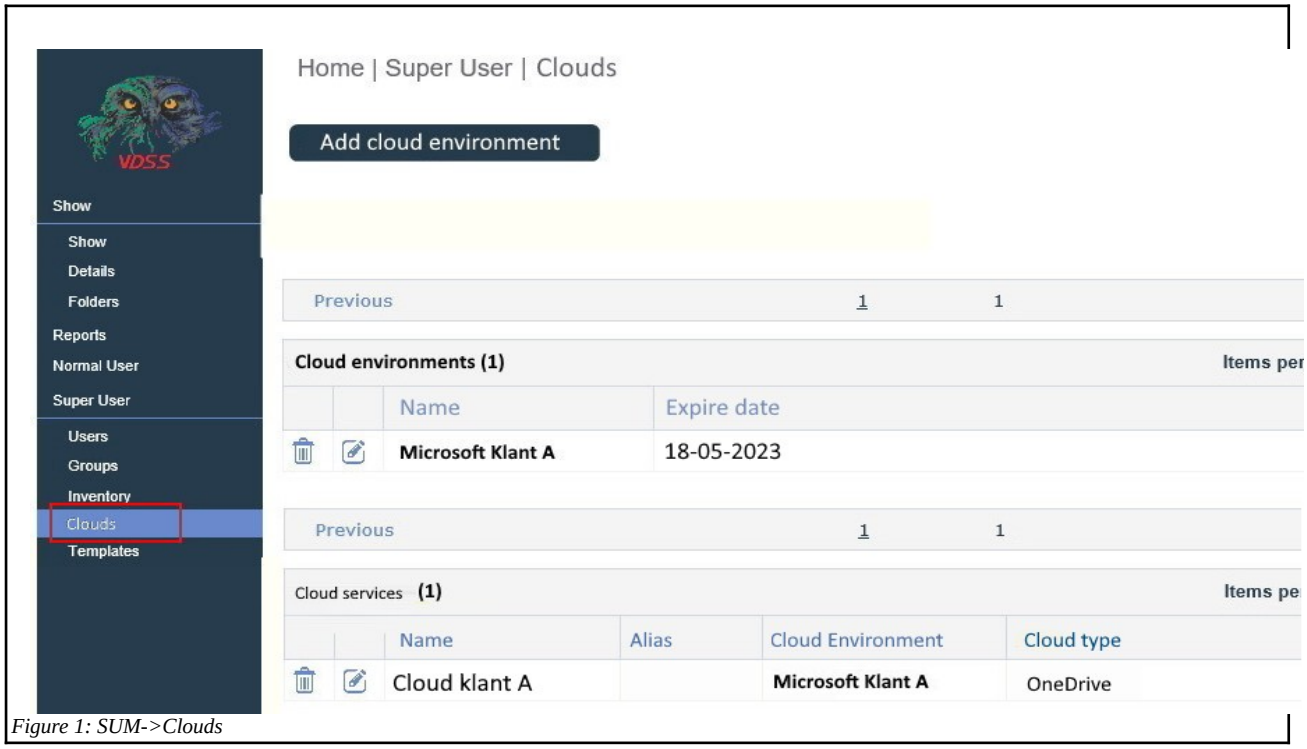


Figure 1: SUM->Clouds

5.1.1 Cloud omgevingen toevoegen

Als de VDSS gebruiker een cloudomgeving toevoegt of bewerkt dan wordt het onderstaande scherm weergeven. De volgende elementen zijn aanwezig:

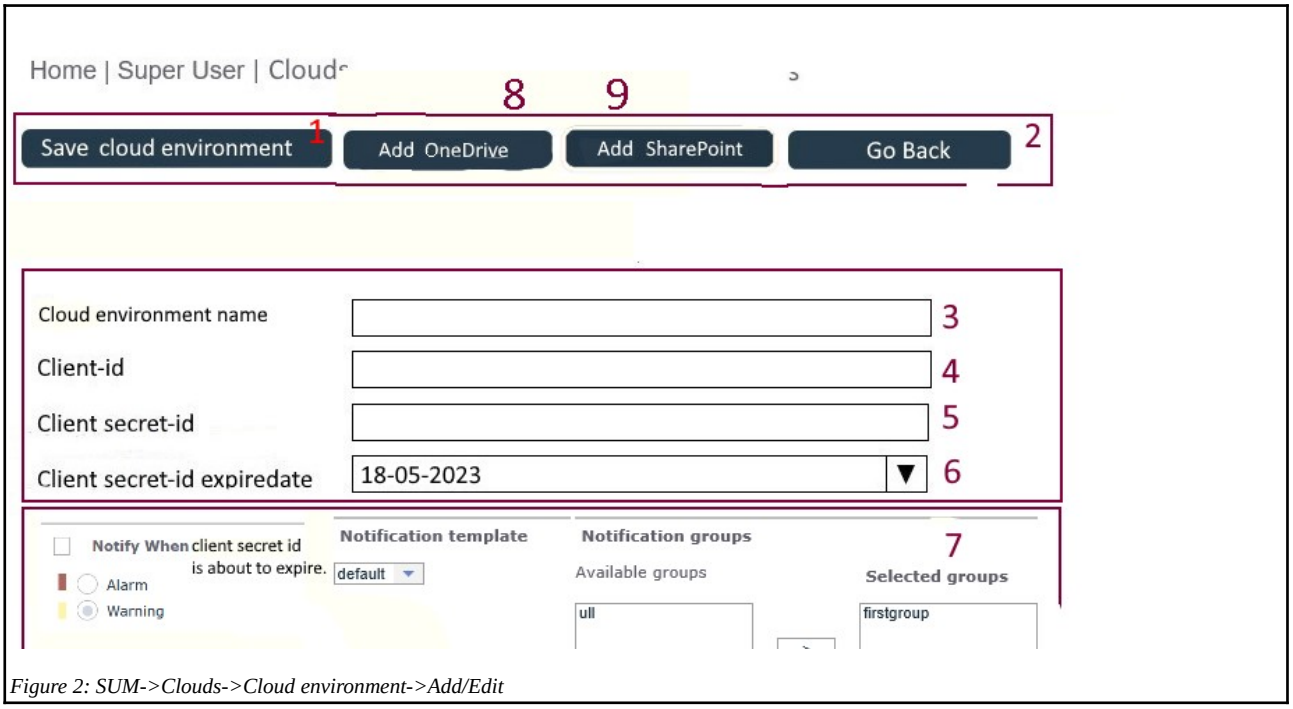


Figure 2: SUM->Clouds->Cloud environment->Add/Edit

1. Knop om cloudomgeving op te slaan
2. Knop om zonder opslaan terug te gaan
3. Veld om naam van cloudomgeving toe te voegen. De klant mag deze zelf bedenken en de naam kan later nog gewijzigd worden.
4. Veld om ‘Client ID’ toe te voegen. De cloudprovider genereerd deze. De VDSS gebruiker voert deze hier in. Dit veld kan later nog gewijzigd worden. Dit veld is een passwordveld, wat inhoudt dat de gebruiker bolletjes ziet bij het invoeren ipv letters en cijfers.
5. Veld om ‘Client Secret key’ toe te voegen. De cloudprovider genereerd deze. De VDSS gebruiker voert deze hier in. Dit veld kan later nog gewijzigd worden. Dit veld is een passwordveld, wat inhoudt dat de gebruiker bolletjes ziet bij het invoeren ipv letters en cijfers.
6. Datumveld om aan te geven wanneer de ‘Client Secret key expiration date’ verloopt. De cloudprovider geeft aan wanneer deze verloopt.

7. Notification aan/uit, notification template en notification groups, zodat tijdig door de Server genotificeerd kan worden dat de ‘client secret-id’ verloopt.
8. Add onedrive. Deze knop is alleen zichtbaar als de cloudomgeving bewerkt wordt.
9. Add sharepoint. Deze knop is alleen zichtbaar als de cloudomgeving bewerkt wordt.

5.1.2 Microsoft OneDrive en SharePoint toevoegen

De gebruiker kan vanuit SUM→Clouds ook Microsoft OneDrives en SharePoints monitoren. De instellingen voor zowel OneDrive als SharePoint zijn het zelfde onder deze pagina. Dit is de reden waarom de screenshots soms in roze aangeeft: “of SharePoint”.

OneDrive of SharePoint toevoegen of bewerken (tabblad ‘component settings’)
Als de VDSS gebruiker een OneDrive of SharePoint toevoegd of bewerkt dan wordt het onderstaande scherm weergeven. De volgende elementen zijn aanwezig:

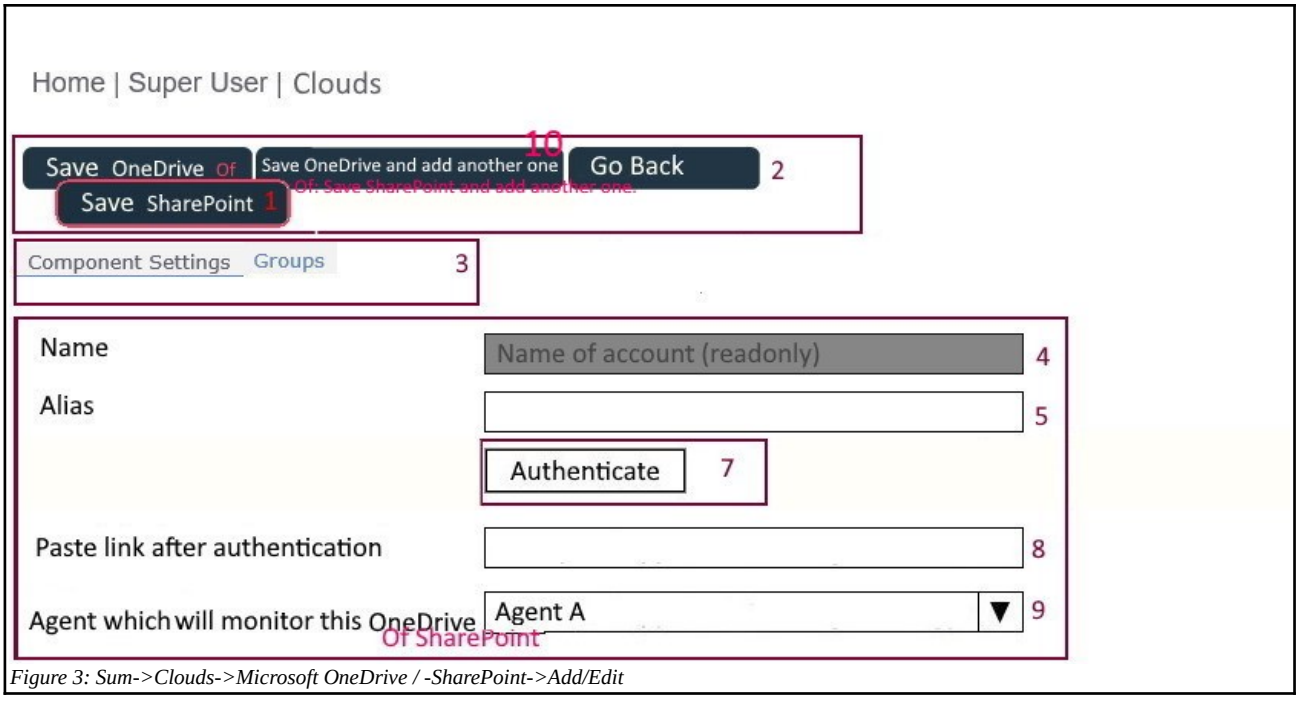
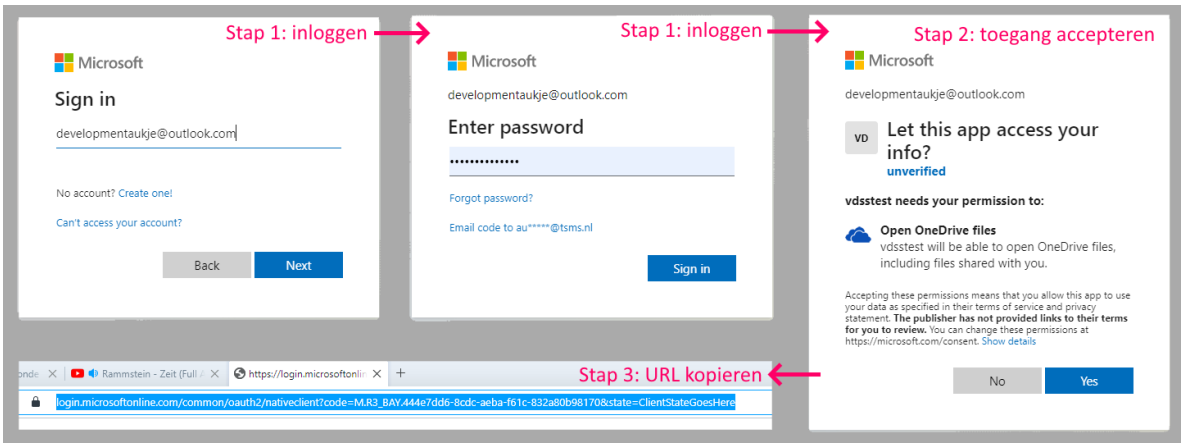


Figure 3: Sum->Clouds->Microsoft OneDrive / -SharePoint->Add/Edit

1. Knop om OneDrive of SharePoint op te slaan
2. Go Back knop om zonder opslaan terug te gaan.
3. Twee tabbladen (OneDrive settings, SharePoint settings en Groups)
4. Veld met de naam van de OneDrive of SharePoint. Bij nieuw toevoegen moet de VDSS gebruiker hier verplicht een naam invoeren. Bij bewerken kan deze niet meer worden gewijzigd. (readonly).

5. Veld om een alias in te voeren.
6. -
7. Authenticatieknop; de gebruiker klikt hierop zodra de juiste cloudomgeving is uitgekozen. De VDSS gebruiker krijgt nu een Microsoft inlogscherm te zien. De VDSS gebruiker logt hier in met het account dat aan de OneDrive of SharePoint gekoppeld is. Daarna krijgt de gebruiker de vraag of VDSS files mag uitlezen. De gebruiker klikt op Ja. Naarna krijgt de gebruiker een link bovenin het scherm. Deze link wordt geplakt in het element direct onder de Authenticatieknop.



8. Veld om authenticatielink in te plakken. De gebruiker klikt eerst op de “Authenticate” knop. Zodra de gebruiker klaar is, krijgt de gebruiker een link. De gebruiker dient deze hier te plakken.
9. Een lijst met Agents die cloud services mogen monitoren. Zo’n Agent wordt automatisch bij de VDSS Server gemeld wanneer er een Agent wordt geinstalleerd die ook clouds mag monitoren. Standaard is de bovenste in de lijst geselecteerd.
   Als de gebruiker dit scherm opent, en er zijn nog geen Agents die cloud componenten mogen monitoren geinstalleerd, dan staat de volgende foutmelding bovenin het scherm.

   EN: *First, install an Agent which can monitor clouds, before adding a Microsoft <OneDrive/SharePoint>. See documentation for instructions.*
   NL: *Installeer eerst een Agent die clouds kan monitoren, voordat een Microsoft <OneDrive/SharePoint> kan worden toegevoegd. Raadpleeg documentatie voor instructies.*
10. Knop om OneDrive of SharePoint op te slaan. Daarna opent dit scherm weer.

5.2 OneDrive en SharePoint in Normal User menu

Er komt een extra menu item in het Normal User menu genaamd “Cloud settings”, als de VDSS gebruiker hier op klikt dan zal er een scherm naar voren komen dat heel erg lijkt op de Agent Settings. Alleen werk je in dit scherm met Microsoft OneDrives en Microsoft SharePoints. Bij Agent Settings werk je met VDSS Agents.

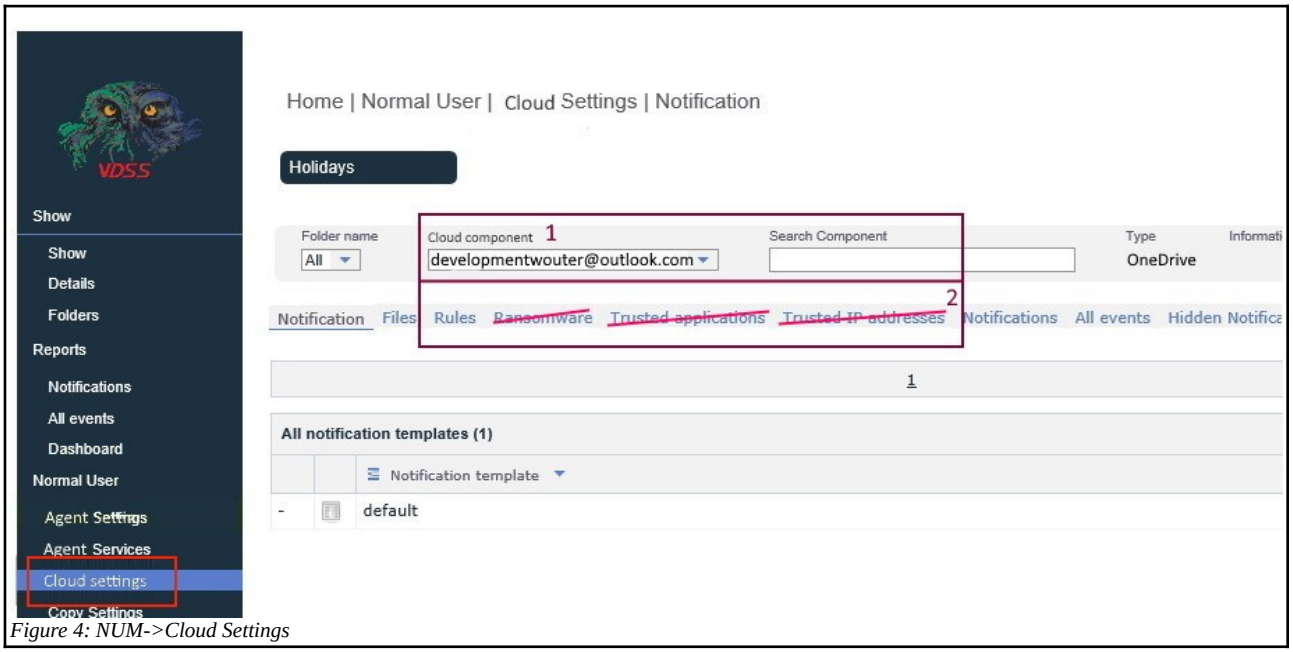


Figure 4: NUM->Cloud Settings

De volgende verschillen zijn er ten opzichte van het NUM → Agent Settings scherm:

1. De lijst waar het component uitgezocht kan wordt aangeduid met “cloud service”.
2. De volgende tabbladen missen: “ransomware”, “trusted applications” en “trusted ip addresses”:

5.2.1 NUM → Cloud Settings → Files

Voor cloud componenten kunnen files worden ingesteld.

Lijst van Files

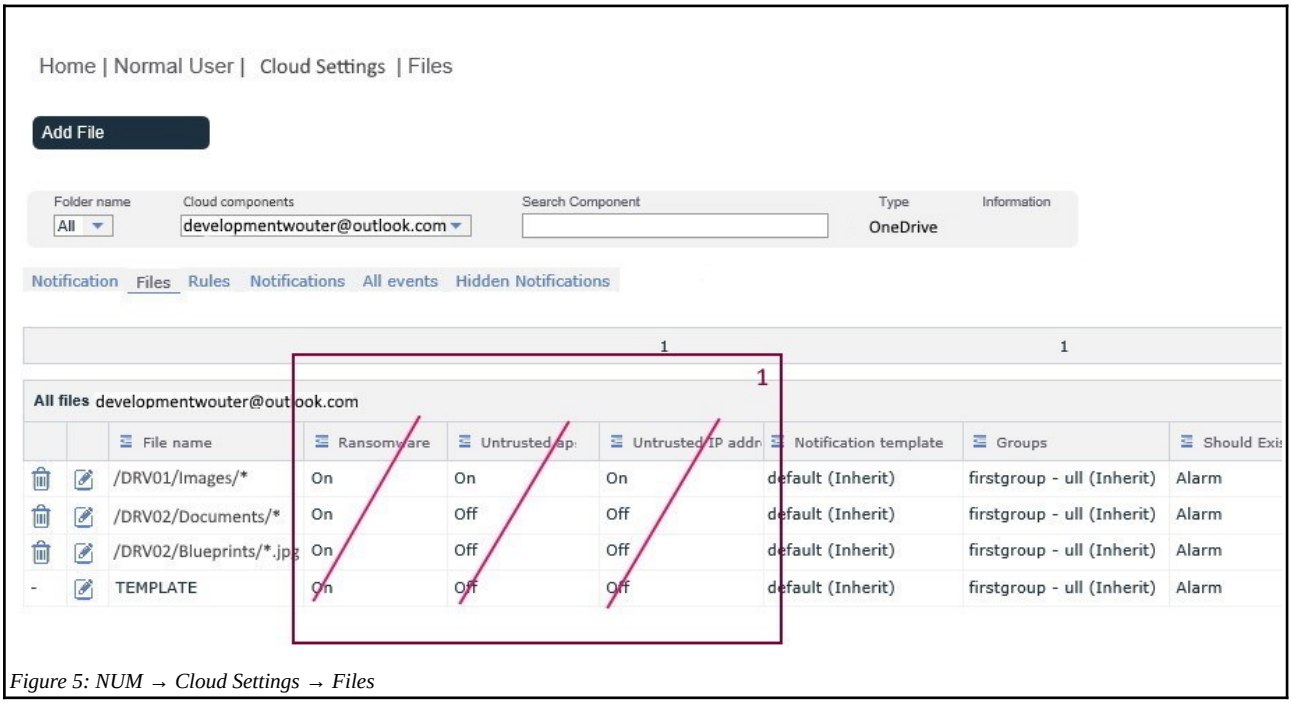


Figure 5: NUM → Cloud Settings → Files

De volgende verschillen zijn er ten opzichte van het NUM → Agent Settings → Files scherm:

1. De kolommen “Ransomware”, “Untrusted applications in quarantine” en “Untrusted IP addresses in quarantine” missen uit de All Files tabel.

Files toevoegen en bewerken

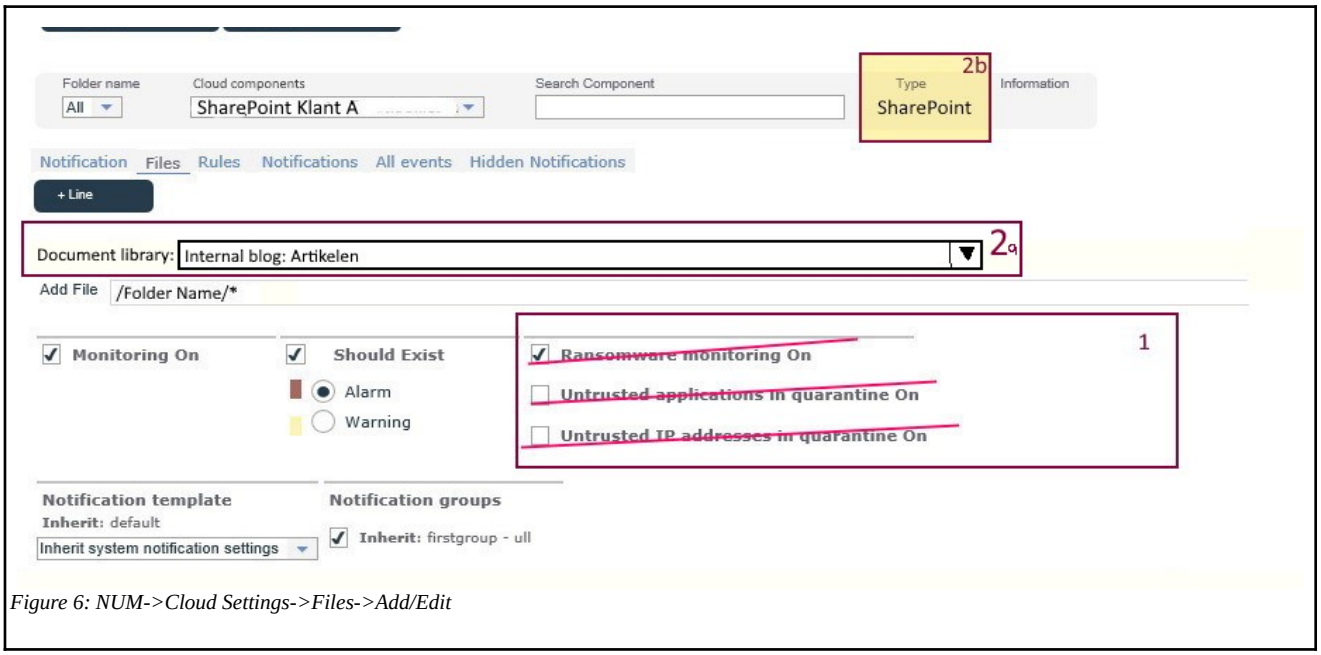


Figure 6: NUM->Cloud Settings->Files->Add/Edit

De volgende verschillen zijn er ten opzichte van het NUM → Agent Settings → Files → New/Edit:

1. De vinkjes “Ransomware on”, “Untrusted applications in quarantine on” en “Untrusted IP addresses in quarantine on” missen.
2. **Alleen als het type cloud een SharePoint is:** dan komt er boven “Add File” een dropdownlist genaamd “Document library”. De agent stuurt op welke document libraries aanwezig zijn. De gebruiker kan uit deze lijst kiezen in welke document library gemonitord moet worden.

   Een document library is in Microsoft SharePoint het zelfde als een Drive.

5.2.2 NUM → Cloud Settings → Rules

Voor cloud componenten kunnen rules worden ingesteld.

Lijst van Rules

Wanneer er onder het SUM→Templates→Rules menu globale rules zijn aangemaakt, dan kan het zijn dat hier rules tussen zitten die door OneDrive en SharePoint niet worden ondersteund.

Bij OneDrive en Sharepoint worden namelijk de acties “Opened” en “Listed” niet ondersteund. Ook kan bij een OneDrive en SharePoint niet achterhaald worden welk programma of ip adres een actie heeft uitgevoerd. Hierdoor worden regels die een programma of ip adres bevat niet ondersteund.

Globale regels die niet ondersteund worden, zijn doorgestreept. De tekst bij ‘notes’ wordt aangevuld met de tekst:

- EN: *This rule has incompatible settings for <OneDrive/SharePoint>.*
- NL: *Instellingen in deze regel worden niet ondersteund door <OneDrive/SharePoint>.*

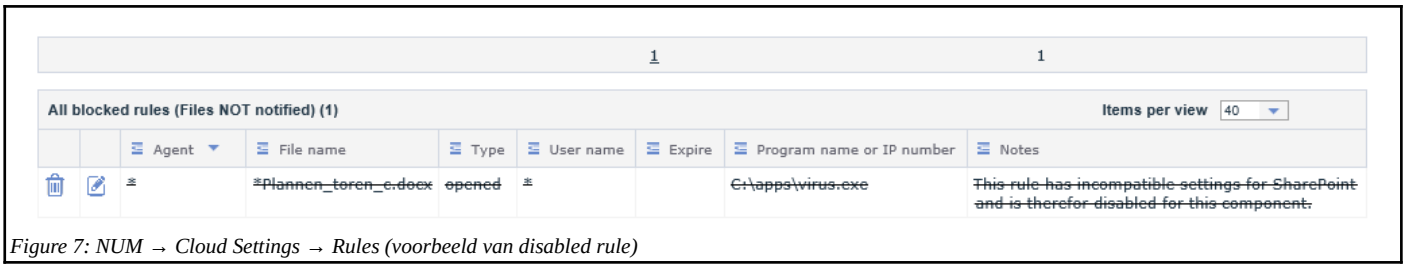


Figure 7: NUM → Cloud Settings → Rules (voorbeeld van disabled rule)

Rules toevoegen en bewerken

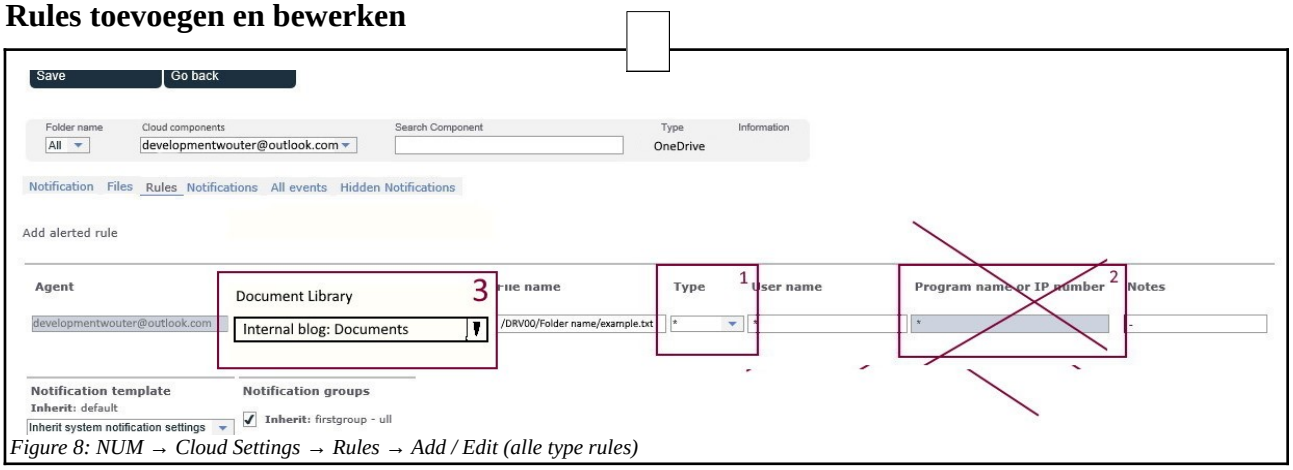


Figure 8: NUM → Cloud Settings → Rules → Add / Edit (alle type rules)

De volgende verschillen zijn er ten opzichte van het NUM → Agent Settings → Rules → New/Edit voor cloud typen “OneDrive” en “SharePoint”.*

1. De dropdownlist “type” mist de opties “Listed” en “Opened”.
2. Het veld “program name or IP number” verdwijnt. Onderwater wordt deze met * ingevuld bij opslaan.
3. **Alleen als het type cloud een SharePoint is:** dan komt er tussen “Agent” en “File name” een dropdownlist genaamd “Document library”. De agent stuurt op welke document libraries aanwezig zijn. De gebruiker kan uit deze lijst kiezen op welke document library deze rule slaat.

   Een document library is in Microsoft SharePoint het zelfde als een Drive.

** Om te zorgen dat deze pagina makkelijk uit te breiden is voor extra clouddiensten, worden de bovenstaande veranderingen gekoppeld aan het type cloud. In dit geval worden deze veranderingen toegepast als het cloud type OneDrive en SharePoint is. Het kan dus zijn dat een andere clouddienst wel Opened en Listed ondersteund, waardoor deze acties voor die clouddients wel ondersteund worden.*

5.2.3 VDSS Show → Details (voor OneDrive en SharePoint)

Discussie: De aanduiding voor het selecteren van de Agent wordt voortaan “Component”.

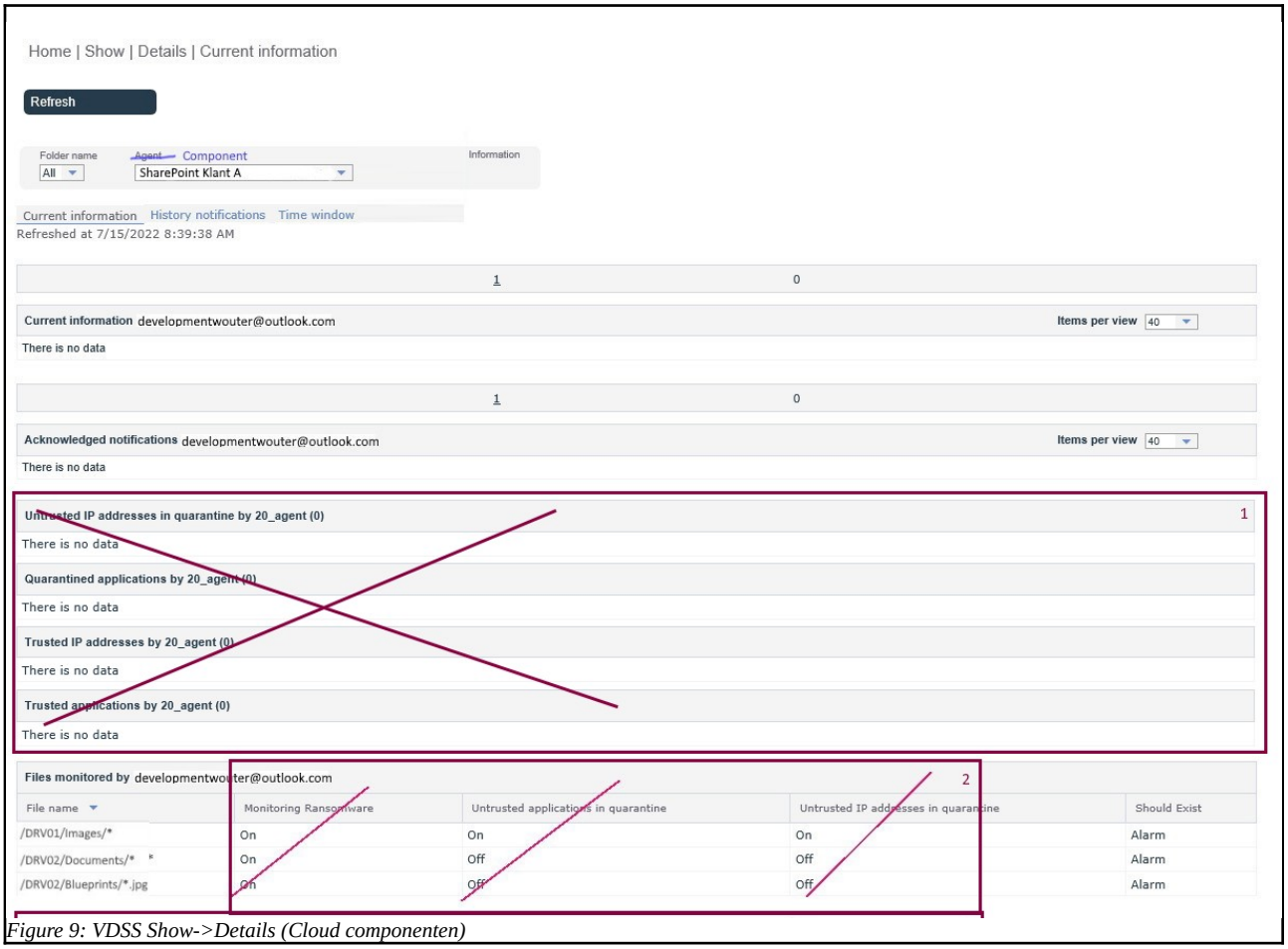


Figure 9: VDSS Show->Details (Cloud componenten)

De volgende verschillen zijn er ten opzichte van het details menu van normale Agents voor cloud typen “OneDrive” en “SharePoint”.

1. De tabellen “Untrusted IP adresses in quarantie”, “Quarantined applications”, “Trusted IP addresses” en “Trusted applications” missen uit dit scherm voor OneDrive en SharePoint.
2. De kolommen “Monitoring Ransomware”, “Untrusted applications in quarentine” en “Untrusted IP addresses in quarantine” missen uit de “files monitored” tabel.