

dSecureCloud

Kurzanleitung zum dSecureCloud Self-Service Portal

verantwortlich: 

Version: 1.21 vom: 22.03.2019

Status: Gültig

Aktenzeichen: -

Schutzstufe: keine Schutzstufe

Zielgruppe: Benutzer des dSecureCloud IaaS Self-Service Portals

Inhaltsverzeichnis

1	Allgemeine Informationen zum Portal.....	1
1.1	Auswahl der Domäne und Einloggen.....	2
1.2	Homepage.....	3
1.2.1	Service-Katalog	3
1.2.2	Bereitstellungen.....	3
1.2.3	Posteingang.....	4
1.2.4	Globale Suche	4
1.2.5	Auswahl der Standard-Ansicht der Homepage.....	5
1.3	Aktivieren der Mail-Benachrichtigungen	6
2	Rollen und Berechtigungen	7
3	Bereitstellen und Verwalten einer VM.....	8
3.1	Anfordern eines Katalog Elements und Genehmigung der Bereitstellung.....	8
3.2	In welchen Fällen ist eine Genehmigung des KStV nötig?	13
3.3	Abrufen der Details einer bereitgestellten VM	13
3.4	Ausführen von Aktionen auf einer VM und Bereitstellung	15
3.5	Verhalten bei fehlgeschlagener Bereitstellung.....	16
3.6	Es werden nur wenige oder keine Aktionen bei virtuellen Maschinen angezeigt	17
4	Neukonfigurieren einer VM	18
5	Zusätzliche Services.....	22
5.1	Snapshots.....	22
5.1.1	Allgemeine Infos zu Snapshots	22
5.1.2	Erstellen und Löschen\Zurückspielen der Snapshots	22
5.2	Einrichten einer Systemsicherung und Wiederherstellen einer VM aus dem Backup	25
5.3	Proxy für den Internetzugriff	28
5.4	Freischaltungsbeauftragung und initiale Platzierung der Server	29
5.4.1	Firewall Service – Bericht über eingerichtete Freischaltungen	31
5.4.2	Firewall Service – Bericht über Regelverstöße	31
5.4.3	Firewall Service - Neue Freischaltung einrichten, eingehend in Richtung Dataport Cloud oder innerhalb der Umgebung	32
5.4.4	Firewall Service - Regel einem vorhandenem Firewall-Abschnitt hinzufügen	35
5.4.5	Firewall Service - Bearbeitung vorhandener Freischaltungen.....	38
5.4.6	Firewall Service – Überwachung aktiver Ausführungen und Bestätigung der Änderung am Regelwerk	40
5.5	SLES – Installserver	42
5.6	Virenschutz	43
5.6.1	Windows	43
5.6.2	Linux (SLES und Ubuntu).....	44
5.7	Kopieren einer VM aus dSecureCloud auf lokalen Speicher mit dem vCenter Converter	45
5.7.1	Installation	45
5.7.2	Kopieren einer VM Windows auf lokalen Speicher	46
5.7.3	Kopieren einer Remote Windows VM	48
5.7.4	Verbinden & Migration einer entfernten VM – Linux	54
5.7.5	Nützliche Links	54
6	Business Management	55
7	FAQ – häufig gestellt Fragen	57
7.1	Eine RDP Verbindung schlägt fehl mit Fehler "Die angeforderte Funktion wird nicht unterstützt.	57

7.2	Die Login-Seite des Portals wird nicht angezeigt. Sie geraten stattdessen auf die URL Idclopa013.dpaor.de und folgender Fehler wird angezeigt: Kein Zugriff auf Seite	57
7.3	RAM-Erweiterung eines Linux Systems schlägt fehl	58
7.4	Routing interner und externer Netzwerkadapter.....	58
7.5	Bereitstellung oder Neukonfiguration schlägt fehl mit Meldung: Delegated token must be instance of class com.vmware.vcac.authentication.http.spring.oauth2.OAuth2Token: null	59
8	Ergänzende Dokumentation	60
9	Änderungsverzeichnis	61

1 Allgemeine Informationen zum Portal

- Basiert auf VMware vRealize Automation
- Vereinfacht den Bereitstellungsprozess von Testsystemen, da Server direkt vom Benutzer provisioniert (bereitgestellt) werden können
- Zur Zeit nur IaaS, d.h. Server in Basisausstattung:
 - Keine Basisdienste (DNS, AD, etc.)
 - Reines Betriebssystem ohne Applikationen
 - Netzwerkanschluß mit Internetzugriff
 - Optional Backup und Virenschutz

Der Zugriff erfolgt über folgende URL (*bitte Mandant beachten*):

Mandant Dataport:

<https://dataportcloudportal.servicedpaor.de/vcac/org/Dataport>

Mandant Hamburg

<https://dataportcloudportal.servicedpaor.de/vcac/org/MandantHH>

Mandant Schleswig-Holstein

<https://dataportcloudportal.servicedpaor.de/vcac/org/MandantSH>

Mandant Bremen

<https://dataportcloudportal.servicedpaor.de/vcac/org/MandantHB>

Mandant Sachsen-Anhalt

<https://dataportcloudportal.servicedpaor.de/vcac/org/MandantST>

Mandant PAED

<https://dataportcloudportal.servicedpaor.de/vcac/org/MandantPAED>

Für den Zugriff soll auch nur die oben genannte URL genutzt werden. Bitte nur diese als Favorit speichern.

Verwenden Sie bitte eine aktuelle Web-Browser Version, ansonsten können einige GUI Elemente nicht korrekt angezeigt werden.

Authentifizierung erfolgt mit dem regulären Domänen-Account.

Diese Anleitung und weitere Informationen werden auch auf dem [Dataport Kundenportal - Dataport Cloud](#) veröffentlicht.

1.1 Auswahl der Domäne und Einloggen

Nach Aufruf der URL erreicht man die Login-Seite. Hier wird im ersten Schritt die Domäne gewählt, in welcher sich das Benutzeraccount befindet. Die Auswahl kann gespeichert werden:



Abbildung 1 - Domänenauswahl

Danach wird der Benutzername (ohne Domänenkürzel) und Passwort eingetippt:



Abbildung 2 - Eingabe des Benutzernamens und Kennworts

Nach erfolgreicher Anmeldung erreicht man die Homepage.

1.2 Homepage

1.2.1 Service-Katalog

Beim ersten Zugriff wird der Katalog angezeigt, wo die Ihnen zugewiesenen Elemente präsentiert sind:

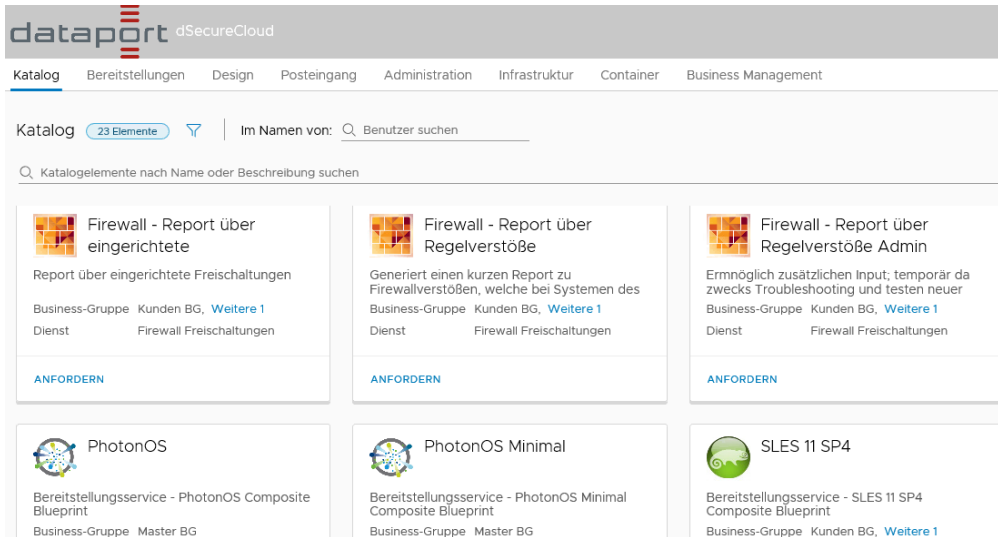


Abbildung 3 - Hauptmenu: Service-Katalog

Die Liste können Sie filtern, indem auf das Filter-Symbol geklickt wird:

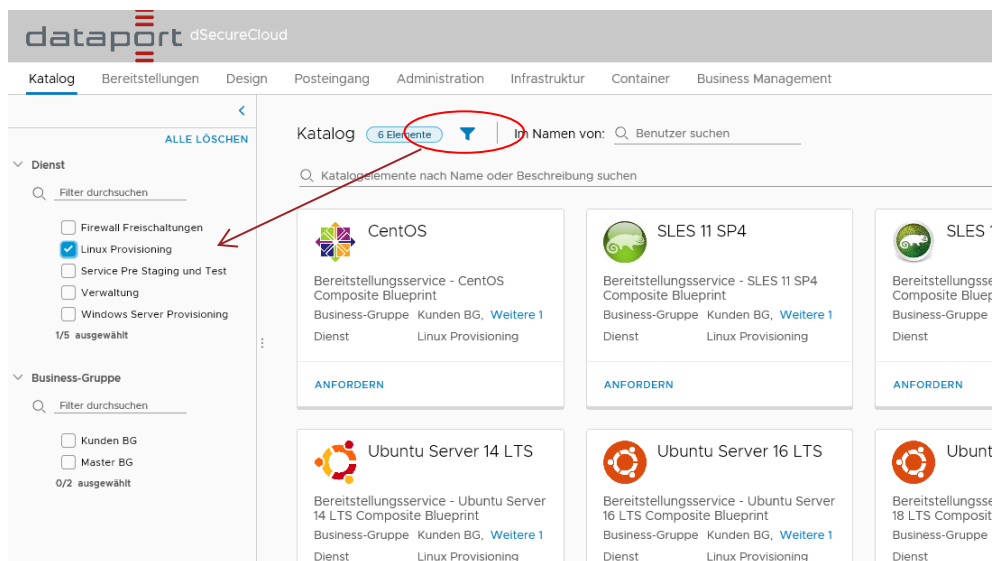


Abbildung 4 - Homepage - Service-Katalog Filter

Somit kann man Elemente filtern, die einem der Services zugeordnet sind, oder einer bestimmten Business Group, sollten Sie Elemente mehrerer Gruppen verwalten.

1.2.2 Bereitstellungen

Bestehende Elemente erreicht man über das Tab „Bereitstellungen“. Virtuelle Maschinen werden in Bereitstellungen gruppiert. Ähnlich wie in dem Katalog können Filter als auch eine Suche angewendet werden:

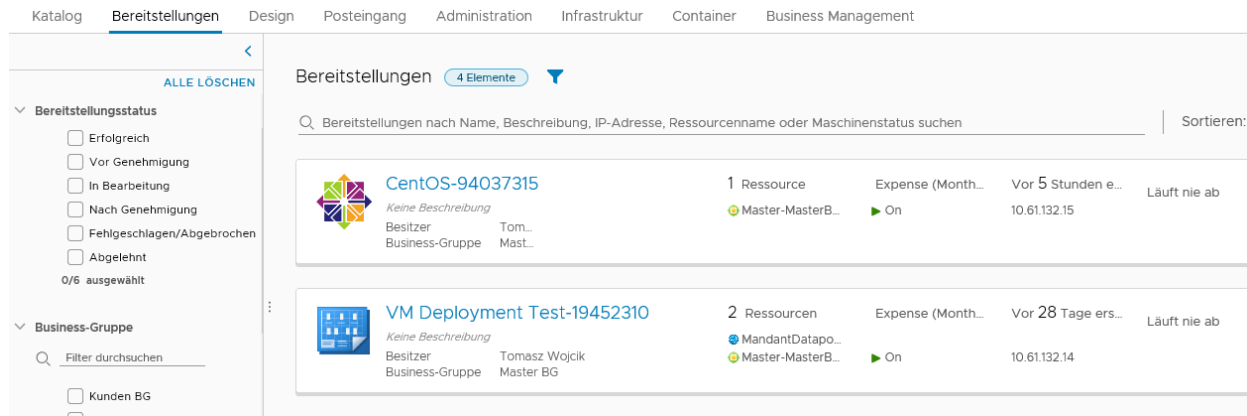


Abbildung 5 - Homepage – Bereitstellungen

1.2.3 Posteingang

Über den Posteingang werden Nachrichten zu ausstehenden Genehmigungen und Benutzeraktionen sowie Rückanforderungsanfragen, welche auf Antwort auf Genehmigungen erstellt werden können:

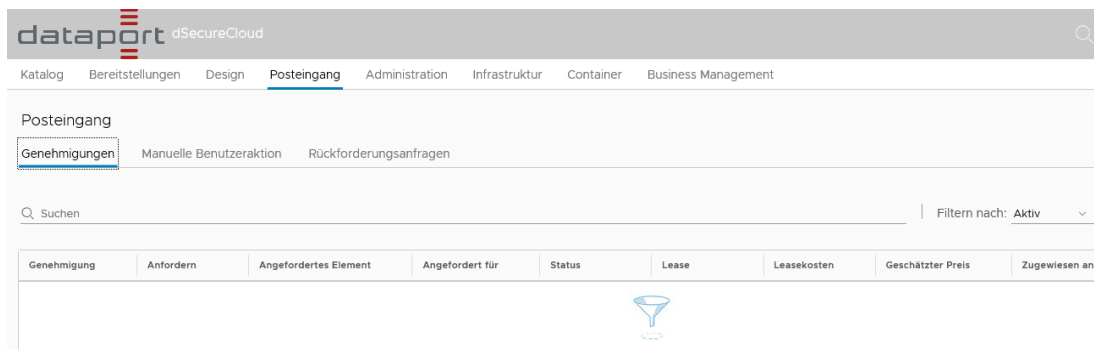


Abbildung 6 - Homepage - Posteingang

Die genannten Posteingang-Elemente kommen zum Einsatz bei Bereitstellungen von virtuellen Maschinen.

1.2.4 Globale Suche

Eine bequeme Methode zur Suche eigener Elemente oder Katalog-services ist die Nutzung der globalen Suche. Es kann einfach der Name des Elementes, oder nur dessen Teil ins Suchfeld eingetippt werden und bei einer Übereinstimmung kann man per Klick zum Element gelangen:

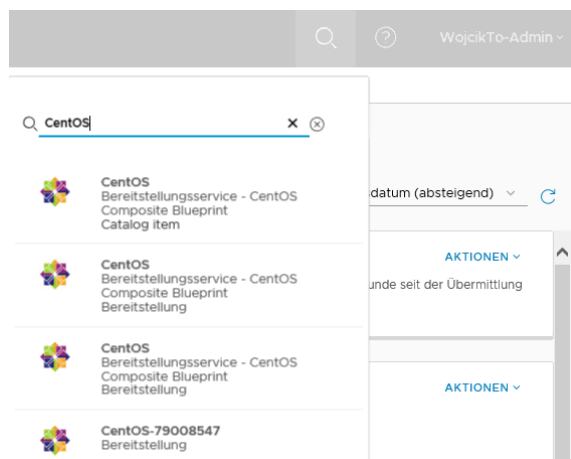


Abbildung 7 - Globale Suche

1.2.5 Auswahl der Standard-Ansicht der Homepage

Über das unten dargestellte Menü kann man wählen, welches der erwähnten Elemente die Standard-Ansicht sein soll beim Aufrufen der Homepage:

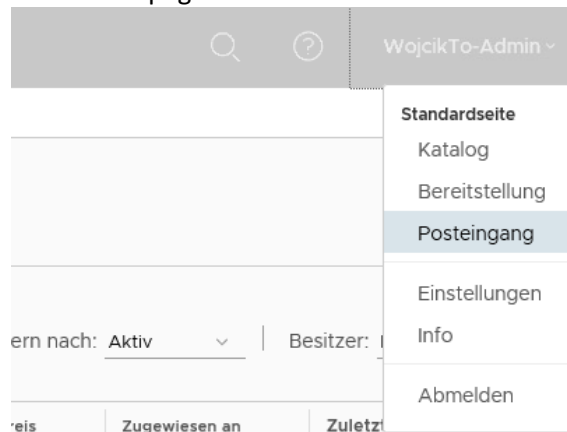


Abbildung 8 - Standard-Ansicht und Einstellungen

1.3 Aktivieren der Mail-Benachrichtigungen

Zum Schluss kann noch der Empfang von E-Mail Benachrichtigungen bestätigt werden. Diese sollten bei allen neuen Accounts standardmäßig aktiviert sein. Zusätzlich kann die Sprache der Benachrichtigungen geändert werden.

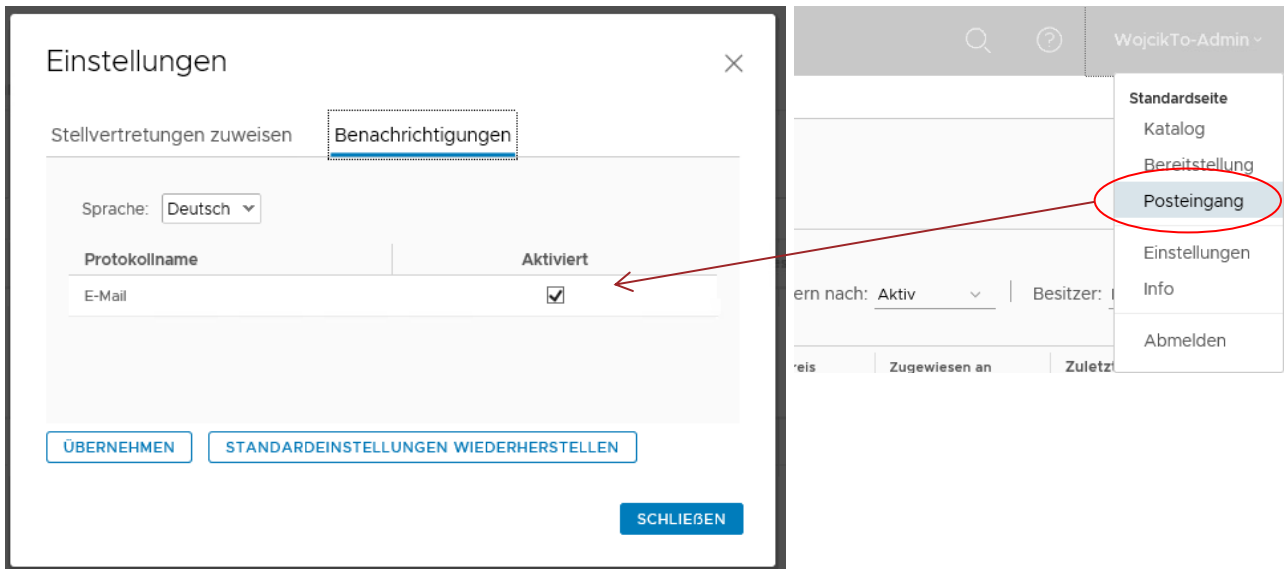


Abbildung 9 - E-Mail Benachrichtigungen aktivieren

2 Rollen und Berechtigungen

Einzelne Dataport Gruppen\Abteilungen und organisatorische Einheiten der Kunden werden auf dem Portal als sog. „Business Groups“ abgebildet. Innerhalb dieser Business Groups werden Benutzern des Dataport Cloud Portals eine oder mehrere der 3 Rollen zugewiesen:

1. User Role - Benutzerrolle

Können Anträge bezüglich VM Provisionieren, Editieren und Löschen erstellen und ihre eigenen VMs verwalten. Die Rolle wird in der Regel normalen AD-Gruppen zugewiesen, z.B. FHHNET\G-D-B-LS##

2. Group Manager Role - Gruppenmanagerrolle

Erhalten Berechtigungen der User + können alle VMs, welche der Gruppe (Business Group) angehören verwalten, können Benutzerrechte der VMs zwischen den Usern übertragen.

3. Support Role – Supportrolle, Kostenstellenverantwortliche, Genehmiger

Können Aufträge genehmigen.

4. Shared Access Role - Rolle mit gemeinsam genutztem Zugriff

Ähnlich wie die Benutzerrolle, ermöglicht aber Zugriff auf alle innerhalb der Business Group bereitgestellten Elemente

Berechtigungen, die ein Benutzer erhalten hat, können an andere Benutzer delegiert werden, über den Menüpunkt „Einstellungen“ auf der Homepage. In dem Eingabefeld muss der Benutzername eingetippt werden um nach einem Account zu suchen:

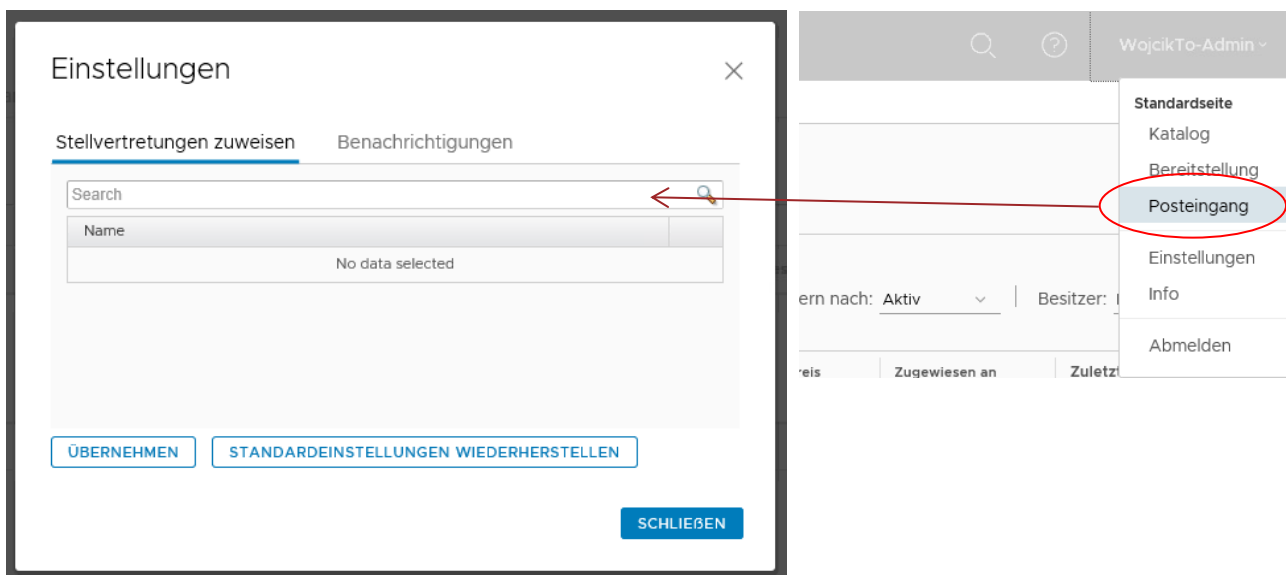


Abbildung 10 - Stellvertretung zuweisen

Rechte können z.B. vor dem Antreten der Urlaubszeit an einen Benutzer aus der gleichen Business Group delegiert werden.

3 Bereitstellen und Verwalten einer VM

3.1 Anfordern eines Katalog Elements und Genehmigung der Bereitstellung

Das Bereitstellen virtueller Maschinen wird im Portal in Form eines Services angeboten. Es stehen mehrere Betriebssystemversionen bereit. Der Service Katalog enthält alle Services, für welche eine Business Group berechtigt wurde.

Den Service Katalog erreicht man über die Registerkarte Katalog (Catalog):

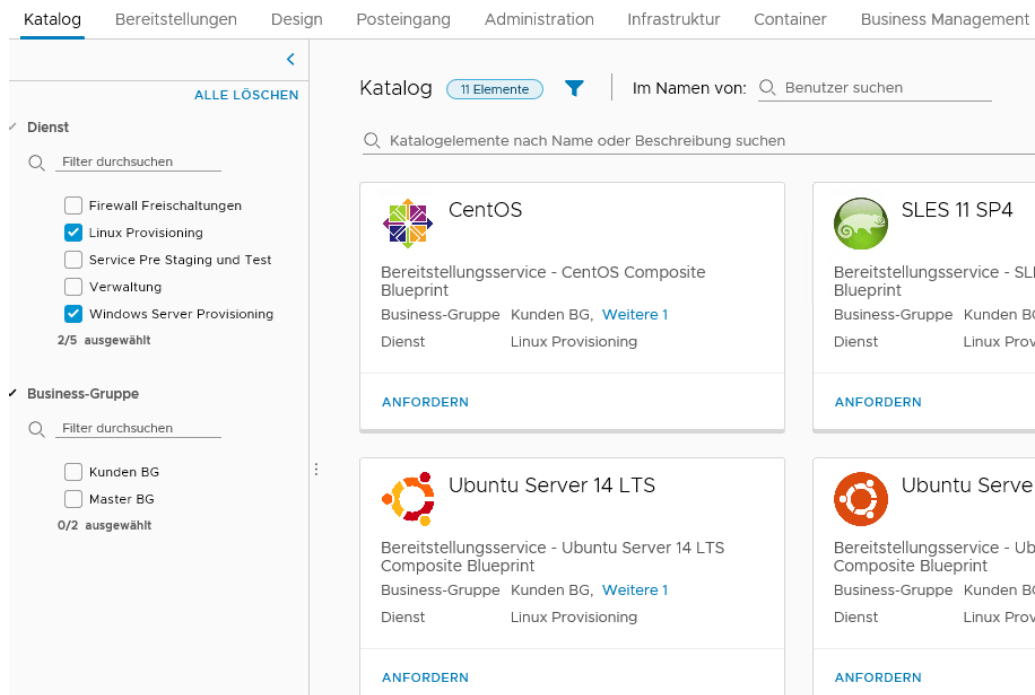


Abbildung 11 - Elemente des Service Katalogs

Hier kann man die einzelnen Services anfordern. Eine Anforderung startet man, indem der Button „Anfordern“ (Request) geklickt wird. Sollte man Mitglied mehrere Business Groups sein, soll man über das Drop-Down Feld die Gruppe wählen, für welche die Bereitstellung stattfindet:

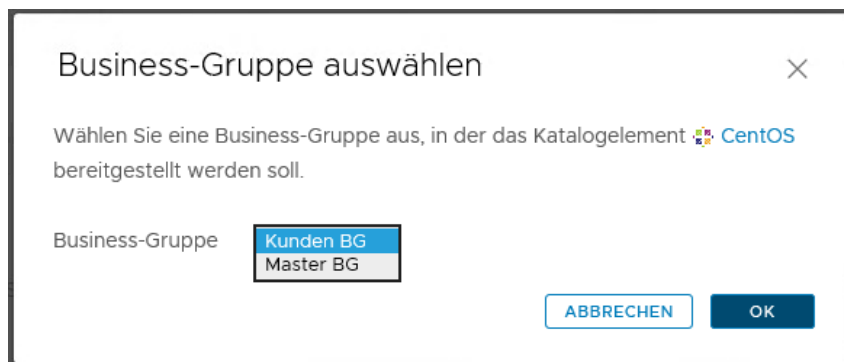


Abbildung 12 - Auswahl der BG für eine Bereitstellung

Somit gelangt man zur Stelle, wo eine Beschreibung für die neue Bereitstellung und eine Begründung, welche den Genehmigern angezeigt wird, eintragen:



Abbildung 13 - Bereitstellung: Hinzufügen einer Beschreibung

Im weiteren Schritt kann das Sizing des Systems, weitere Parameter wie Netzplatzierung (nur beim Mandanten Dataport), Backup und zusätzliche Festplatten definiert werden:

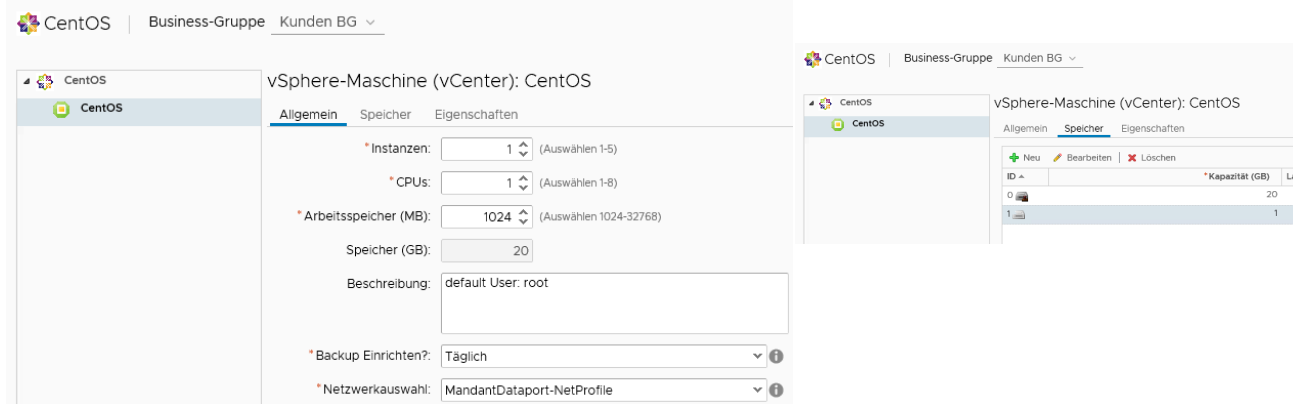


Abbildung 14 - Bereitstellung: Sizing und weitere Eigenschaften

Sollten weitere Platten dem System hinzugefügt werden, so müssen diese nach der Bereitstellung vom Administrator des Systems formatiert werden.

Das Ändern der Größe der ersten Festplatte ist gesperrt, da diese aus der Systemvorlage geklont wird.

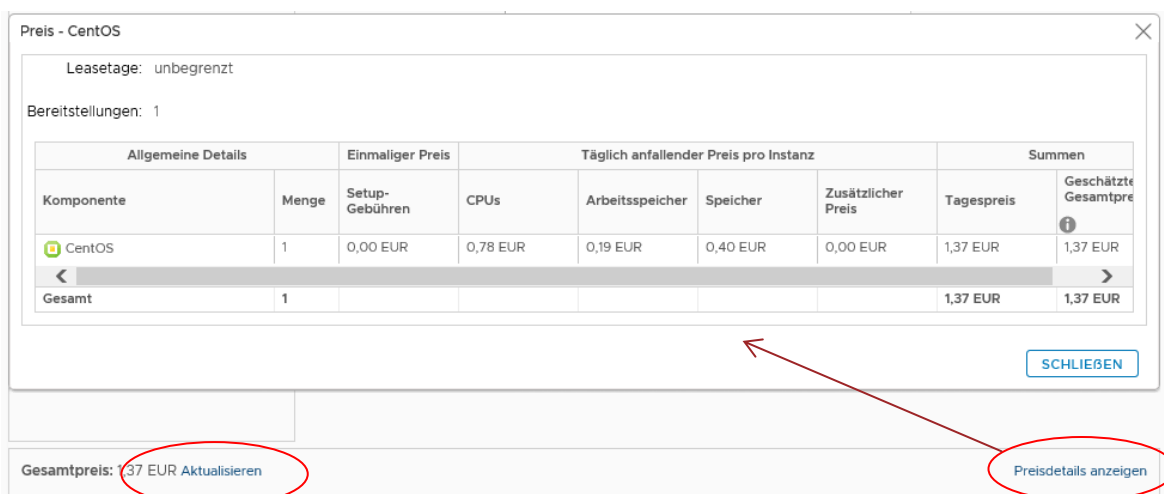


Abbildung 15 - Aktualisieren der Preisdetails bei einer Bereitstellung

Nachdem das Sizing festgelegt wurde, kann der Antrag abgesendet werden. Man wird auf den „Bereitstellung“ Reiter weitergeleitet und der Status wird angezeigt:

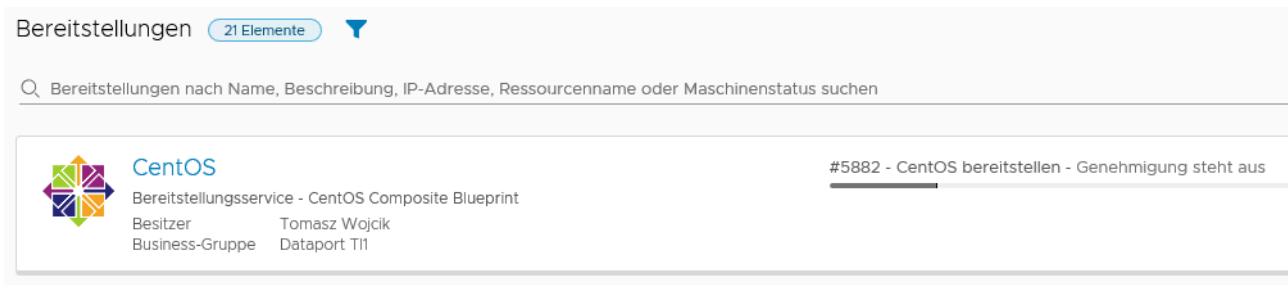


Abbildung 16 - Status der Bereitstellung nach Übermittlung

Die Kostenstellenverantwortlichen (KStV) erhalten zur gleichen Zeit eine Benachrichtigung zur ausstehenden Genehmigung des Antrags:

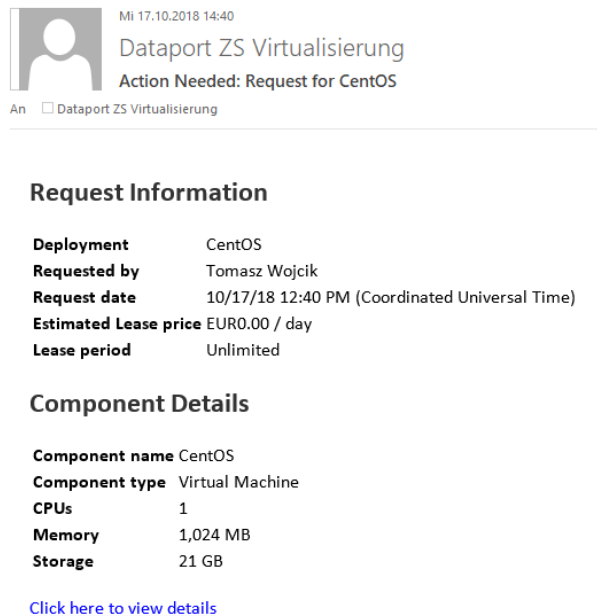


Abbildung 17 - Mail-Benachrichtigung zur ausstehenden Genehmigung

Eine entsprechende Nachricht erscheint auch in dem Posteingang direkt in dem Portal:

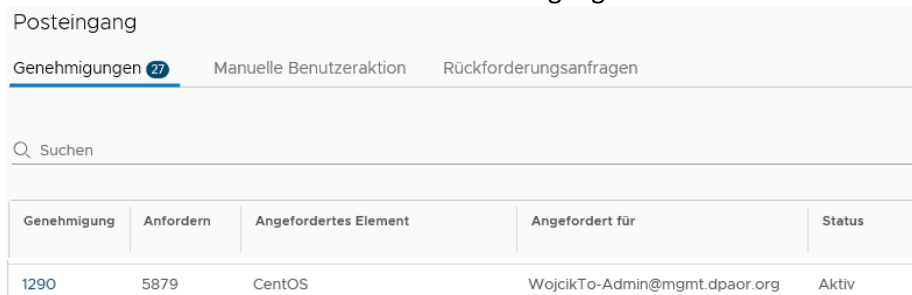


Abbildung 18 - Genehmigungsanfrage im Posteingang

Durch klicken auf die Genehmigungs-ID kann der KStV die Details abrufen und den Antrag bestätigen oder ablehnen:

Katalog Bereitstellungen Design **Posteingang** Administration Infrastruktur

Genehmigung # 1290

Status	Aktiv	Anfordern #	5879
Angefordertes Element	CentOS	Anforderer	Tomasz Wojcik
Beschreibung	Bereitstellungsservice - CentOS Composite Blueprint	Angefordert auf	17. Oktober 2018 14:40
Angefordert für	Tomasz Wojcik	Lease	Unbegrenzt
		Geschätzter Preis	N/A

Details Eingeben Anforderungsdetails

*Begründung:

GENEHMIGEN **ABLEHNEN** ABBRECHEN


Abbildung 19 - Details einer Genehmigung

Direkt danach wird auf den Reiter „Bereitstellungen“ weitergeleitet, wo der Fortschritt der Bereitstellung angezeigt wird. Durch Klicken auf den Status gelangt man zu einer detaillierten Ansicht:

Katalog **Bereitstellungen** Design Posteingang Administration Infrastruktur Container Business Management

Bereitstellungen 8 Elemente

Suche: Bereitstellungen nach Name, Beschreibung, IP-Adresse, Ressourcenname oder Ma | Sortieren: Erstellungsdatum (absteigend)


	CentOS Bereitstellungsservice - CentOS Composite Blueprint Besitzer: Tomasz Wojcik Business-Gruppe: Master BG	#5865 - CentOS bereitstellen - In Bearbeitung	7%	ABBRECHEN
---	---	--	----	------------------

0 Minuten seit der Übermittlung

Abbildung 20 - Fortschritt der Bereitstellung

Katalog **Bereitstellungen** Design Posteingang Administration Infrastruktur Container Business Management

[< Zurück](#)

 CentOS-79008547 In Bearbeitung ABBRECHEN | ↻

Keine Beschreibung

Besitzer	Tomasz	Expense (Month to date)	N/A
Bereitgestellt auf	17. Okt	Leasedauer	Unbesti
Business-Gruppe	Master	Läuft ab am	Nie
Katalogelement	CentOS	Löschdatum	Nie

[DETAILS AUSBLENDEN](#) ⤴

Komponenten **Verlauf**

Anforderungen 1

10/17/18 1:08 PM i **CENTOS BER...** Tomasz Wojcik

Ereignisse Eingaben Anfordern


#5865 - CentOS be... In Bearbeitung Angefordert von: Tomasz Wojcik Angefordert am: 17. Okt

Aufgaben	Komponente	Status
Übermittelt	Deployment	✔ Erfolgreich
Vor Genehmigung	Deployment	✔ Genehmigt
> Bereitstellung	Deployment	🔄 In Bearbei...


Abbildung 21 - Fortschritt der Bereitstellung: Detaillierte Ansicht

Der Auftraggeber erhält zugleich eine Bestätigung per E-Mail:

Mi 17.10.2018 15:41

 Dataport ZS Virtualisierung

Request #5879 for "CentOS" for "WojcikTo-Admin@mgmt.dpaor.org" has been approved

An  Wojcik, Tomasz

Approval Phase Pre Approval
Approver Tomasz Wojcik
Status Approved

Request Information

Deployment CentOS
Requested by Tomasz Wojcik
Request date 10/17/18 12:40 PM (Coordinated Universal Time)
Estimated Lease price EURO.00 / day
Lease period Unlimited

Component Details


Component name CentOS
Component type Virtual Machine
CPUs 1
Memory 1,024 MB
Storage 21 GB

[Click here to view details](#)

Abbildung 22 - Nachricht zur erteilten Genehmigung

Zum Schluss kommen weitere Nachrichten zur erfolgreichen Bereitstellung der VM:

Mi 17.10.2018 15:45

 Dataport ZS Virtualisierung

Request #5879 for "CentOS" for WojcikTo-Admin@mgmt.dpaor.org was completed successfully


An  Wojcik, Tomasz

Abbildung 23 - Nachricht zur erfolgreichen Bereitstellung

Der Antragsteller erhält noch zusätzliche Informationen zur bereitgestellten VM:



Abbildung 24 - Informationen zur bereitgestellten VM

Als auch das Zugangsdaten und die IP Adresse des Systems:



Abbildung 25 - Zugangsdaten und IP des bereitgestellten Systems

3.2 In welchen Fällen ist eine Genehmigung des KStV nötig?

Eine Genehmigung des KStV ist immer in folgenden Fällen nötig:

- VM Bereitstellen
- VM Löschen
- VM Neukonfigurieren
- Skalierung einer Bereitstellung
- Backup Einrichtung\Abschaltung

3.3 Abrufen der Details einer bereitgestellten VM

Die eigenen Elemente erreicht man über den Reiter „Bereitstellungen“. Hier werden alle Bereitstellungen, also Elemente, welche sowohl virtuelle Maschinen als auch andere Objekttypen beinhalten können, dargestellt.

Sollte eine Großzahl von Objekten dargestellt werden, kann man diese Filter. In dem Filter kann nach Besitzer, zugehöriger Business Group oder Objekttyp gefiltert werden.

Neben dem Bereitstellungsnamen werden VMs gelistet, welche der Bereitstellung zugeordnet sind:

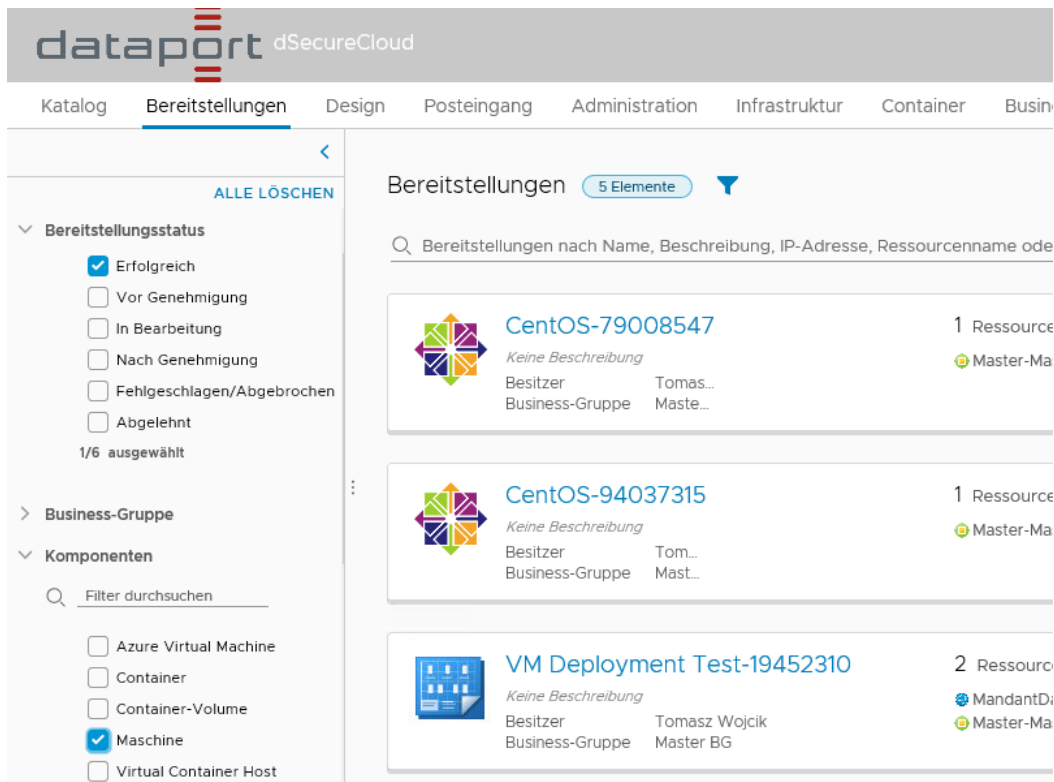


Abbildung 26 - Bereitstellungen: Filter

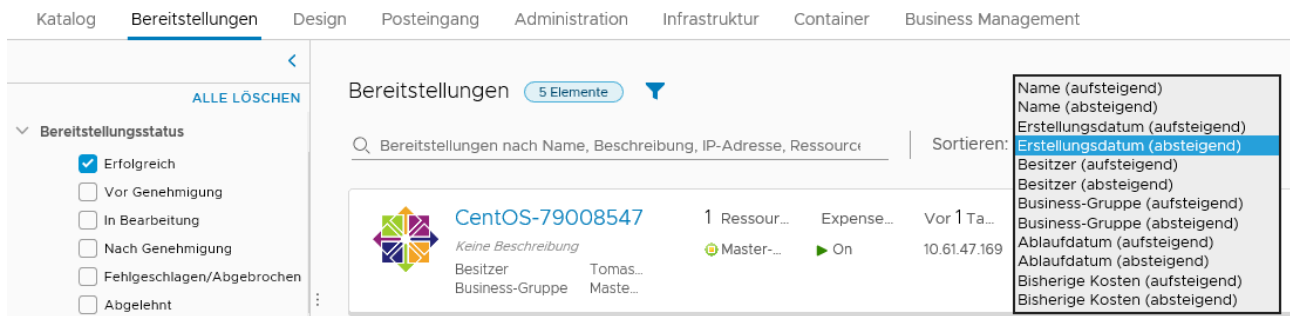


Abbildung 27 - Bereitstellungen: Sortierung

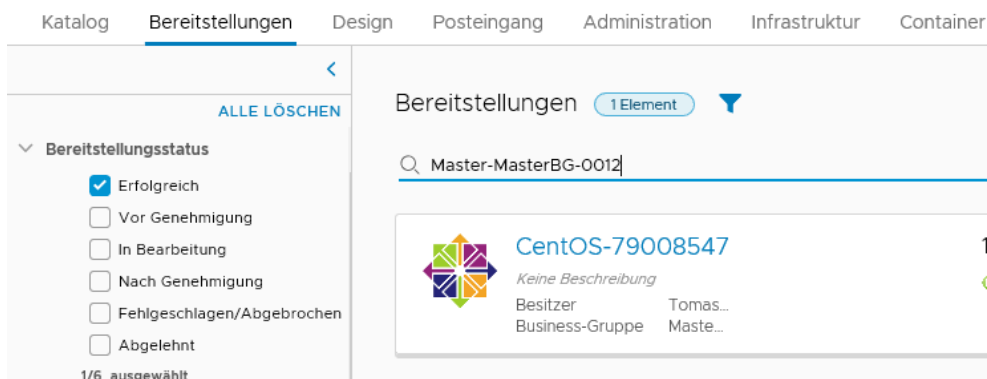


Abbildung 28 - Bereitstellung: Suche

Zu der virtuellen Maschine gelangt man, indem auf den Namen der Bereitstellung geklickt hat. Somit erreicht man die Detailansicht:

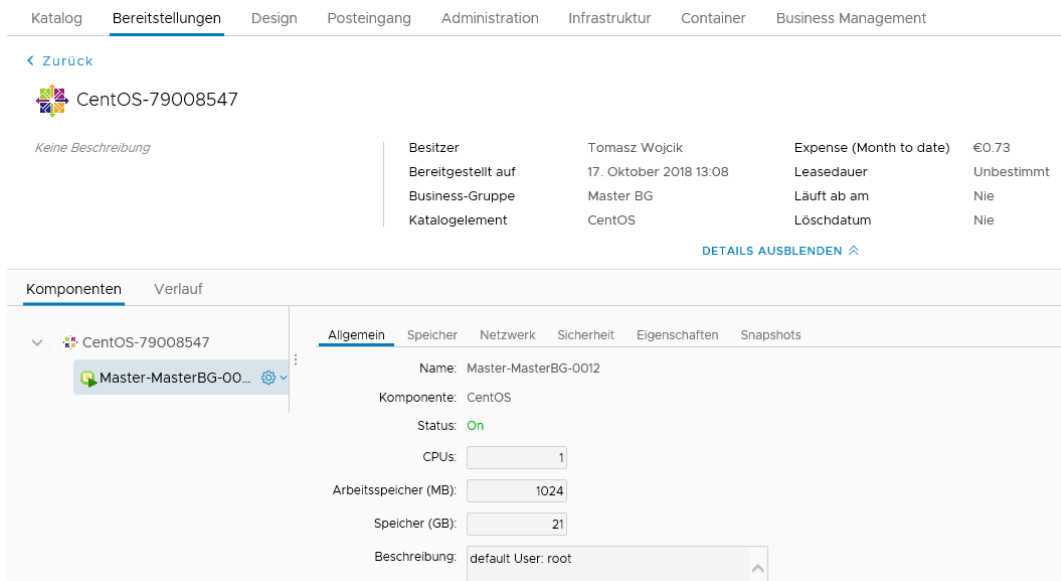


Abbildung 29 - Detailansicht einer Bereitstellung

In der Detailansicht können einzelne Systeme untersucht werden.

Über die Reiter werden Details zum Ressourcennutzung und Konfiguration der Komponenten einer VM abgerufen.

3.4 Ausführen von Aktionen auf einer VM und Bereitstellung

In der Detailansicht stehen mehrere Aktionen zur Verfügung. Dadurch kann die Anzahl und Kofiguration der Elemente geändert werden.



Abbildung 30 - Verfügbare Aktionen bei einer Bereitstellung

Über die horizontale Skalierung können Sie die Anzahl der in einer Bereitstellung beinhalteten virtuellen Maschinen ändern.

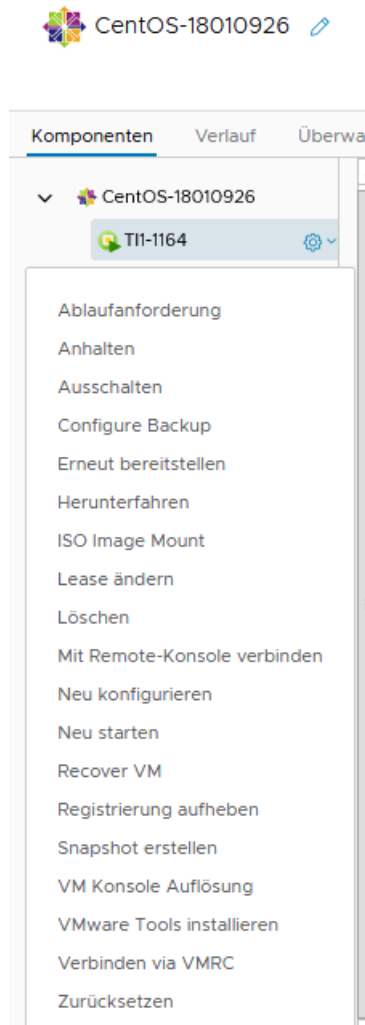


Abbildung 31 - Aktionen bei einer virtuellen Maschine

Über das Drop-Down Menü können Standardaktionen wie Neustart, Löschung und Snapshot Erstellung als auch spezielle Aktionen wie Backup Einrichten und das Mounten einer ISO Datei angefordert werden.

3.5 Verhalten bei fehlgeschlagener Bereitstellung

Bedingt durch eine fehlgeschlagene Input-Validierung oder einen Systemfehler kann es zum Abbruch einer Bereitstellung kommen. In diesem Fall gibt es die Möglichkeit, die Anforderung zu wiederholen, ohne nochmal alle Input-Felder auszufüllen.

Nachdem der Fehler identifiziert wurde, kann der Service erneut ausgeführt werden. Bereits ausgefüllte Input-Felder sind mit den vorher eingetragenen Informationen befüllt und man kann auch diese nach Bedarf ändern:

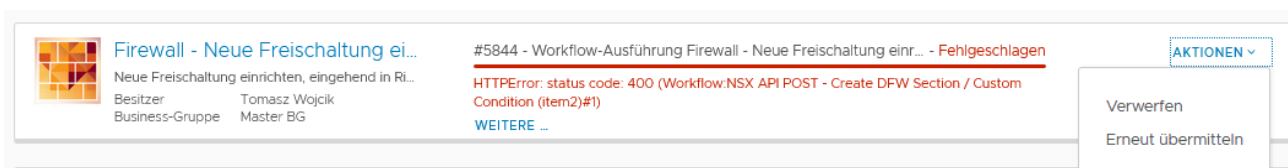


Abbildung 32 - Fehlerhafte Ausführung eines Services

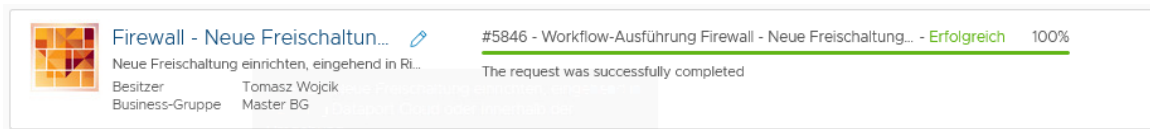


Abbildung 33 – Nach Input-Korrektur war wiederholte Ausführung erfolgreich

3.6 Es werden nur wenige oder keine Aktionen bei virtuellen Maschinen angezeigt

In einigen Fällen ist das Ausführen der zugewiesenen Aktionen nicht möglich, da nur wenige oder keine Aktionen bei dem Objekt angezeigt werden, ähnlich wie hier:

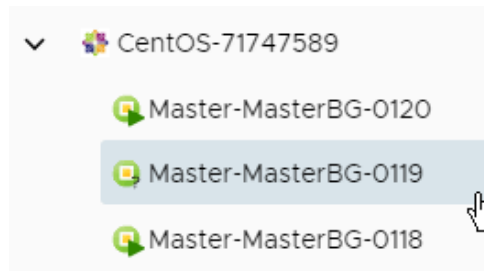


Abbildung 34 - Keine Aktionen verfügbar

In diesem Fall muss man prüfen, ob:

- Bei dem betroffenen Objekt eine Aufgabe aktiv ist, z.B. Neukonfiguration (Reconfigure). Den Status kann man bei dem Objekt untersuchen, oder, sollte die Ansicht nicht automatisch aktualisiert werden, zur Liste der Bereitstellungen (Deployments) wechseln
- Bei der übergeordneten Bereitstellung (Deployment) eine Aufgabe aktiv ist. Solange diese Aufgabe aktiv ist, z.B. eine Neukonfiguration einer der dazugehörigen virtuellen Maschinen, können bei keinem der dazugehörigen Objekte neue Aktionen ausgeführt werden. Eventuell muss die Ansicht aktualisiert werden
- Eine Aufgabe ist fehlgeschlagen, ähnlich wie bei Punkt 3.5. In diesem Fall muss die Fehlgeschlagene Ausführung verworfen (Dismiss) werden, ansonsten dürfen keine weiteren Aktionen ausgeführt werden:

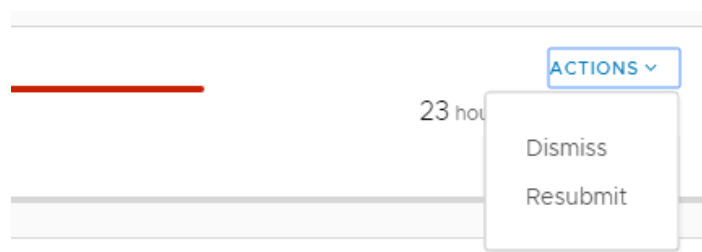


Abbildung 35 - Fehlgeschlagene Ausführung verworfen oder wiederholen

4 Neukonfigurieren einer VM

Änderungen an einer VM können über die Aktion „Neu konfigurieren“ durchgeführt werden:

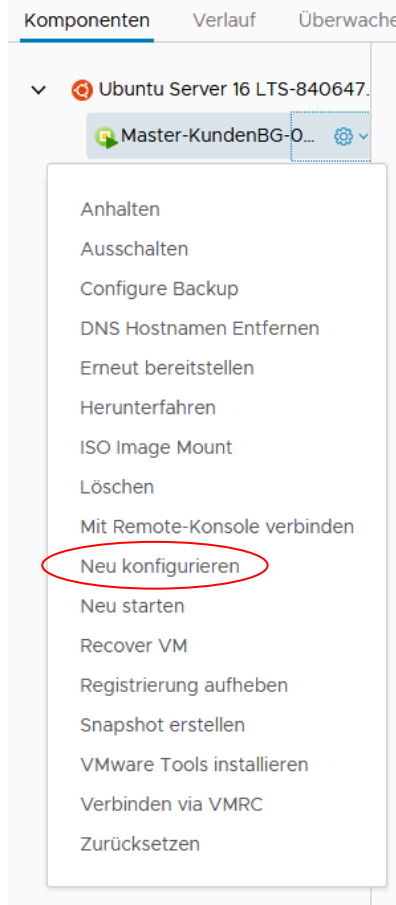


Abbildung 36 - Platzierung der "Neu konfigurieren" Aktion

Folgende Änderungen können durchgeführt werden:

- **CPU & RAM Speicher**

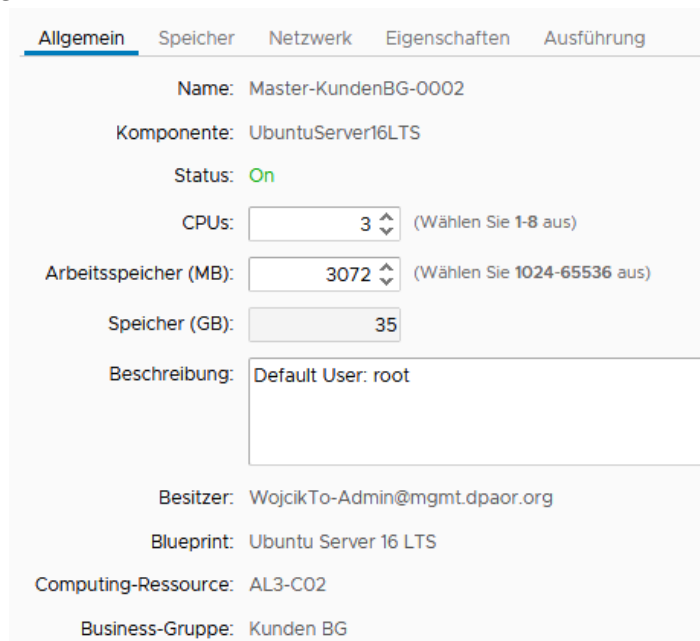


Abbildung 37 - Angaben zum CPU & RAM Sizing

- **Erweitern vorhandener und Hinzufügen neuer Festplatten**



Abbildung 38 - Änderung an der Festplattenkonfiguration

Achtung! – solange ein Snapshot aktiv ist, kann keine Plattenerweiterung an der virtuellen Maschine durchgeführt werden! Snapshots werden bei aktiver Backup-Option automatisiert bei jedem Backup-Durchlauf erstellt und auch automatisch wieder entfernt, eine Plattenerweiterung ist deswegen zu der Zeit nicht umsetzbar.

- **Hinzufügen neuer Netzwerkkarten oder Ändern eines zugewiesenen Netzwerks**



Abbildung 39 - Ändern der Netzwerkkonfiguration

Alternative Netzwerke (Netzwerkprofile) sind nur über den Mandanten Dataport erreichbar. Netzwerke sind folgenden Profilen zugewiesen:

Netzwerkname	Netzwerkprofil	Beschreibung
1300_ASBR_EXT	MandantDataport-NetProfile	1. Netzbereich für VMs des Mandanten Dataport
1316_AHHR_INT	MandantDataport-NetProfile-2	2. Netzbereich für VMs des Mandanten Dataport (default)
1306_AHHR_EXT	MandantDataportHH-ExterneIPs	1. Netzbereich mit öffentlichen IPs des Mandanten Dataport und HH
1315_AHHR_EXT	MandantDataportHH-ExterneIPs-2	2. Netzbereich mit öffentlichen IPs des Mandanten Dataport und HH
1307_AHHR_INT	MandantHH-NetProfile	Netzbereich für VMs des Mandanten HH
1406_NSHTS_INT	MandantSH-NetProfile	Netzbereich für VMs des Mandanten SH
1457_NSHR_EXT	MandantSH-ExterneIPs	Netzbereich mit öffentlichen IPs des Mandanten SH
1500_AHBR_INT	MandantHB-NetProfile	Netzbereich für VMs des Mandanten HB
1554_AHBR_EXT	MandantHB-ExterneIPs	Netzbereich mit öffentlichen IPs des Mandanten HB
1600_NSTR_INT	MandantST-NetProfile	Netzbereich für VMs des Mandanten ST
1655_NSTR_EXT	MandantST-ExterneIPs	Netzbereich mit öffentlichen IPs des Mandanten ST

1900_APAR_INT	MandantPAED-NetProfile	Netzbereich für VMs des Mandanten PAED
---------------	------------------------	--

Nachdem der Netzwerkkarte ein anderes Netzwerk zugewiesen wurde, erhält das System eine IP aus dem verknüpften Netzwerkprofil mit. Die IP Konfiguration ist in dem Portal und den Eigenschaften des Elements sichtbar. Diese muss manuell vom Benutzer im System eingetragen werden.

Zum Schluss muss eine Option für die Ausführung gewählt werden. Abhängig vom Inhalt der Anforderung kann ein Neustart der VM nötig sein. Wenn ein Neustart erforderlich ist und die Option „Nicht neustarten“ gewählt wurde, wird die Anforderung fehlschlagen und muss erneut abgesendet werden:

Abbildung 40 - Ausführungsoptionen festlegen

Die Ausführung der Neukonfiguration kann man, ähnlich wie bei einer Neubereitstellung, unter dem Tab „Bereitstellungen“ überwachen:

Abbildung 41 - Statusüberwachung einer Neukonfiguration

Sollte ein Fehler auftreten, wird eine Meldung in der GUI angezeigt. Diese muss über das Aktionsmenü verworfen werden, bevor man die Anforderung wiederholen kann:

Abbildung 42 - Fehler bei einer Neukonfiguration

Das Neukonfigurieren der VM unterliegt einer Genehmigung, ähnlich wie bei einer Neubereitstellung. Nach einer erfolgreichen Ausführung erhält man in der GUI eine Statusmeldung als auch eine Bestätigungsmail:

The screenshot shows the dSecureCloud interface. On the left, there is a sidebar titled 'Anforderungen' with a list of requests. The main area is titled 'Ereignisse' and shows a specific event: '#7185 - Neu konfigurieren Master-Kunde...' with a status of 'Erfolgreich'. Below this, there is a detailed message: 'CPU changed, it was [2] and [3] were requested. Memory changed, it was [2048] MB and [3072] MB was requested. Volume 'Festplatte 1' updated, [30] GB changed to [35] GB. Total storage changed from [30] GB to [35] GB. Network updated, [1406_NSHS_INT] changed to [1316_AHHR_INT]'. A table below lists the tasks performed:

Aufgaben	Komponente	Status	Hängt ab von	Startzeit	Abschlusszeit
Übermittelt	Deployment	Erfolgreich		02/05/2019 1:34:47 PM	02/05/2019 1:34:47 PM
> Vor Genehmigung	Deployment	Genehmigt		02/05/2019 1:34:47 PM	02/05/2019 1:35:02 PM
Neu konfigurieren	Deployment	Erfolgreich		02/05/2019 1:35:02 PM	02/05/2019 1:38:22 PM
Nach Genehmigung	Deployment	Genehmigt		02/05/2019 1:38:22 PM	02/05/2019 1:38:24 PM
Abgeschlossen	Deployment	Erfolgreich		02/05/2019 1:38:24 PM	02/05/2019 1:38:26 PM

Abbildung 43 - Erfolgreich ausgeführte Anforderung

The screenshot shows an email confirmation. At the top, there are action buttons: 'Antworten', 'Allen antworten', 'Weiterleiten', and 'Chat'. The date and time are 'Di 05.02.2019 13:37'. The sender is 'Dataport dsecurecloud'. The subject is 'dSecureCloud - VM EDIT: Master-KundenBG-0002'. The recipient is 'Wojcik, Tomasz; Dataport dsecurecloud'. The main body of the email contains the following information:

Informationen zu Änderungen an der VM:
VM Name: Master-KundenBG-0002
CPUs: 3
RAM: 3072 MB
Plattenplatz: 30 GB
OS: Ubuntu Linux (64-bit)
Erstellt am: Tue Jan 22 2019 13:53:43 GMT-0000 (UTC)
Erstellt in: MasterKundenBG
Erstellt von: WojcikTo-Admin@mgmt.dpaor.org, E-Mail: tomasz.wojcik@dataport.de

Abbildung 44 - Bestätigung der Änderung

5 Zusätzliche Services

5.1 Snapshots

5.1.1 Allgemeine Infos zu Snapshots

WAS IST EIN SNAPSHOT?

Bei einem Snapshot wird der aktuelle Zustand einer VM „eingefroren“ und eine neue Datei erstellt (*Delta.vmdk). In diese Datei werden alle Änderungen geschrieben.

Wichtig – solange ein Snapshot aktiv ist, kann keine Plattenerweiterung an der virtuellen Maschine durchgeführt werden!

FÜR WELCHEN ZWECK NUTZEN WIR SNAPSHOTS?

Snapshots sind **keine** Backups oder Sicherungen! Sie frieren den Zustand einer VM für kurze Zeit (nicht mehr als 1 Woche) ein. Dies kann zum Beispiel bei Updatearbeiten oder zum Test von neuen Applikationen, Anwendungen finden. Schlägt eine der durchgeführten Aufgaben fehl, kann die VM auf den Ursprungsstand zurückgesetzt werden. Hier werden die Differenzdateien auf „Nullgröße“ zurückgesetzt. Der Snapshot wird neugestartet. Läuft der Server nach einem Update ohne Beeinträchtigungen, kann der Snapshot übernommen werden. Die Differenzdateien werden mit den Originaldateien zusammengeführt. Es wird kein Snapshot mehr fortgeführt bzw. neu gestartet.

5.1.2 Erstellen und Löschen\Zurückspielen der Snapshots

Jeder Benutzer kann für die VMs in seiner Gruppe Snapshots erstellen. Diese Funktionalität sollte immer vor wichtigen Updates\Upgrades, riskanten Änderungen etc. am System genutzt werden!

Snapshots können über die GUI auf folgendem Weg erstellt werden, nachdem die VM aus der Liste ausgewählt wurde:

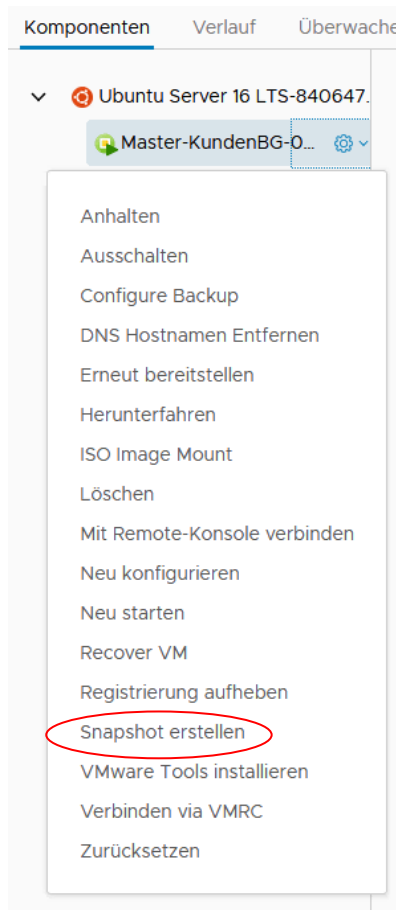


Abbildung 45 - Aktion für das Erstellen von Snapshots

Nachdem auf „Snapshot erstellen“ geklickt wurde, kann man den Snapshot-Namen und die Bezeichnung editieren. Die Auswahl der „Snapshot des Arbeitsspeichers der Maschine erstellen“ Option hat zu Folge, dass der gesamte Inhalt des Arbeitsspeichers auf die Platte gedumpt wird. Das kann Hilfreich sein, wenn eine Dump-Analyse stattfinden soll:

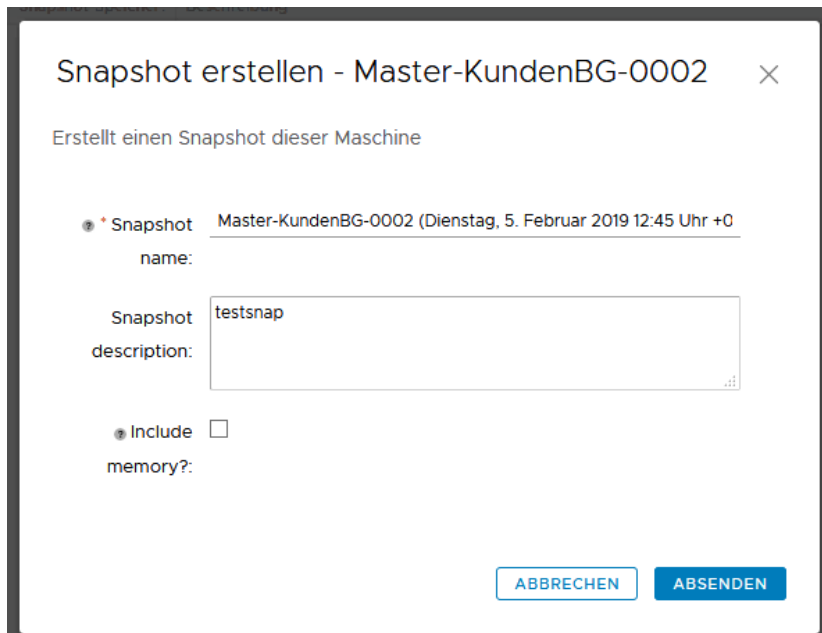
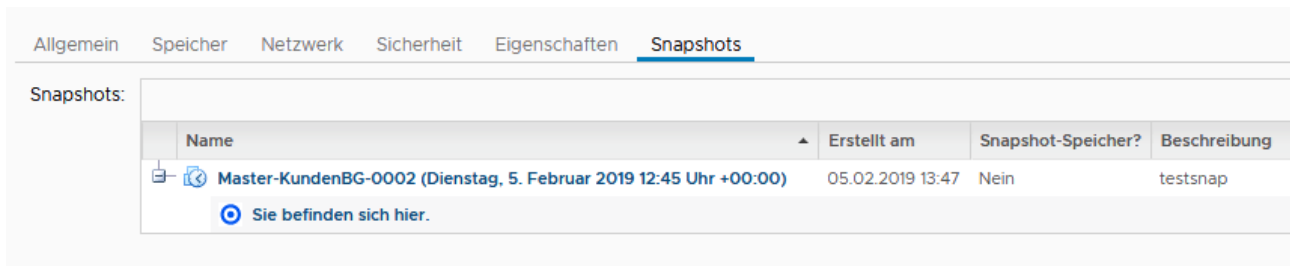


Abbildung 46 - Details zur Snapshoteinrichtung

Nachdem OK geklickt wird kommt eine kurze Bestätigung und der Snapshot erscheint in dem „Snapshots“ Tab:



Name	Erstellt am	Snapshot-Speicher?	Beschreibung
Master-KundenBG-0002 (Dienstag, 5. Februar 2019 12:45 Uhr +00:00)	05.02.2019 13:47	Nein	testsnap

Abbildung 47 - Liste eingerichteter Snapshots

Bei vorhandenem Snapshot, erscheinen im Aktionen-Menü zusätzliche Auswahlfelder:

Snapshot löschen

Snapshot wiederherstellen

Abbildung 48 - Aktionen bei vorhandenem Snapshot

- Snapshot wiederherstellen (Revert to Snapshot) – zurücksetzen der VM auf den Ursprungszustand zur Zeit, als der Snapshot erstellt wurde. Dabei werden alle Änderungen, die bisher betätigt wurden, verworfen. Die VM wird dabei abgeschaltet und muss neugestartet werden.
- Snapshot löschen (Delete Snapshot) – der Snapshot wird entfernt, d.h. der aktuelle Stand der VM wird übernommen.

Es können maximal 3 Snapshots pro VM erstellt werden. Es gibt keinen Zeitlimit, nach dem ein Snapshot gelöscht bzw. übernommen wird, es empfiehlt sich aber die Snapshots nicht länger als 1 Woche laufen zu lassen.

5.2 Einrichten einer Systemsicherung und Wiederherstellen einer VM aus dem Backup

Benutzer des dSecureCloud Portals können selbstständig eine Systemsicherung (Backup) einrichten als auch ihre virtuellen Maschinen aus einem Backup wiederherstellen. Die Backup-Option kann während der initialen Bereitstellung eingerichtet oder nachträglich, per Aktion „Configure Backup“, eingerichtet oder deaktiviert werden:

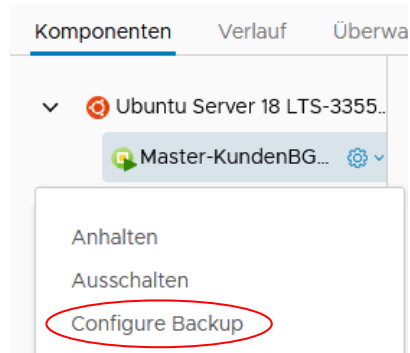


Abbildung 49 - Aktion zum Einrichten oder deaktivieren des Backups

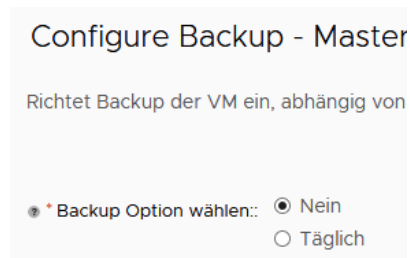


Abbildung 50 - Backup-Optionen

Das ausführen der Maßnahme unterliegt einer Genehmigung.

Es werden komplette virtuelle Maschinen gesichert, eine Wiederherstellung einzelner Dateien ist nicht vorgesehen.

Um eine VM wiederherzustellen, muss in der Detailansicht die folgende Aktion gewählt werden:

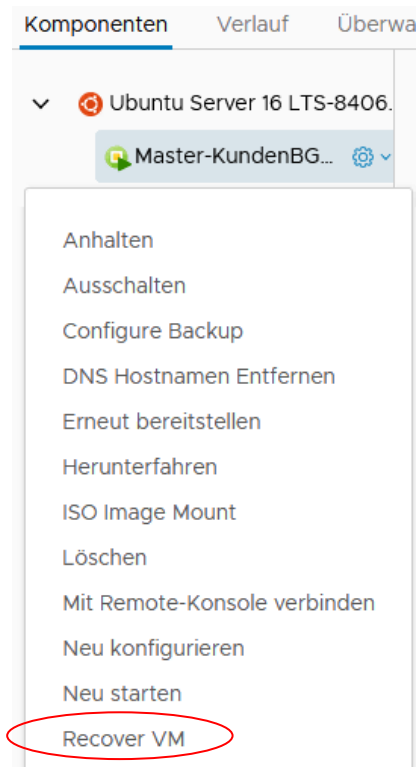


Abbildung 51 - Aktion für das Wiederherstellen einer VM aus dem Backup

Somit wird eine neue Anforderung aufgerufen. Neben der kurzen Beschreibung erscheint ein drop-down Feld, in dem man eine Backup Instanz auswählen kann:



Abbildung 52 - Auswahl eines Backups

Es werden maximal 30 Einträge angezeigt, was 30 täglichen Sicherungen entspricht.

Ob eine VM gesichert wird, erkennt man dem Parameterwert in der VM Detailansicht:

Allgemein Speicher Netzwerk Sicherheit **Eigenschaften** Snapshots

Benutzerdefinierte Eigenschaften:

Name	Wert
_snapshot_propagation	true
Cafe.Shim.VirtualMachine.TotalStorageSize	20
Dataport.Abrechnungstyp	intern
Dataport.Auftragsnummer	000000
Dataport.BackupEinrichten	Täglich
Dataport.BusinessGroupName	Master RG

Abbildung 53 - VM Parameter mit Backup-Konfiguration

5.3 Proxy für den Internetzugriff

Sollte bei einem der bereitgestellten Server die Proxy-Konfiguration nicht mehr vorhanden sein, muss die IP Adresse des Proxies erneut eingetragen werden: **10.61.16.6:3128**.

Der Proxy benötigt für die Verbindung keine Authentifizierung.

Folgende Protokolle werden vom Proxy übermittelt: http, https, dns.

Sollten vom betroffenen System aus andere Server über ihre RZ-interne (lokale) IP Adressen, in der gleichen Umgebung oder im RZ, erreicht werden soll man bei der Proxy Konfiguration daran denken, die Zieladressen in eine Ausnahme eintragen (no_proxy, lokale Adressen etc.).

5.4 Freischaltungsbeauftragung und initiale Platzierung der Server

Eingehende Freischaltungen in Richtung der Server in der dSecureCloud können über einen Service im Portal eingerichtet werden. Jedes Mitglied einer Business Group kann eingehende Freischaltungen für seine virtuellen Maschinen, bzw. für alle VMs, welche der Gruppe zugehören, einrichten.

Ausgehende Freischaltungen müssen in der Kommunikationsmatrix beschrieben und vom Dataport Policy Management genehmigt werden, die Umsetzung erfolgt über den Dataport Netzbetrieb.

Dabei gilt folgendes Schema:

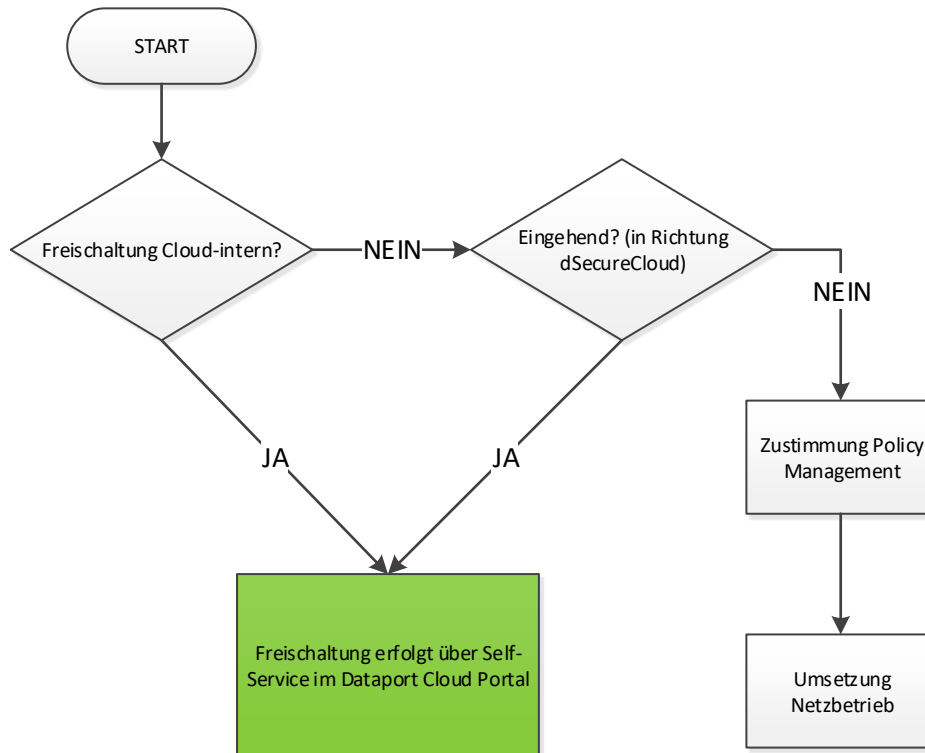


Abbildung 54 - Wann ist eine Ausnahmegenehmigung nötig?

Für die Einrichtung oder Änderung einer Freischaltung werden Informationen über eine User Form erfasst, Details dazu finden Sie in den weiteren Unterkapiteln.

Änderungen im Firewall-Regelwerk, welche auf Grund von Bearbeitung vorhandener Regeln oder Einrichtung neuer virtuellen Maschinen umgesetzt wurden, sind nach ca. 10 Minuten in den Eingabemasken und in den Berichten der Firewall Services sichtbar.

Vorhandene Freischaltungen können deaktiviert, aber nicht gelöscht werden. Die Entfernung wird manuell durchgeführt, während der regulären Wartungsfenster.

Brauchen Sie eine eingehende Freischaltung, die alle validen IPv4-Kreise umfasst („any“) muss als Quelle das Netz 0.0.0.0/0 eingetragen werden.

Folgendes Diagramm stellt eine grobe Übersicht der zulässigen Kommunikationsbeziehungen dar:

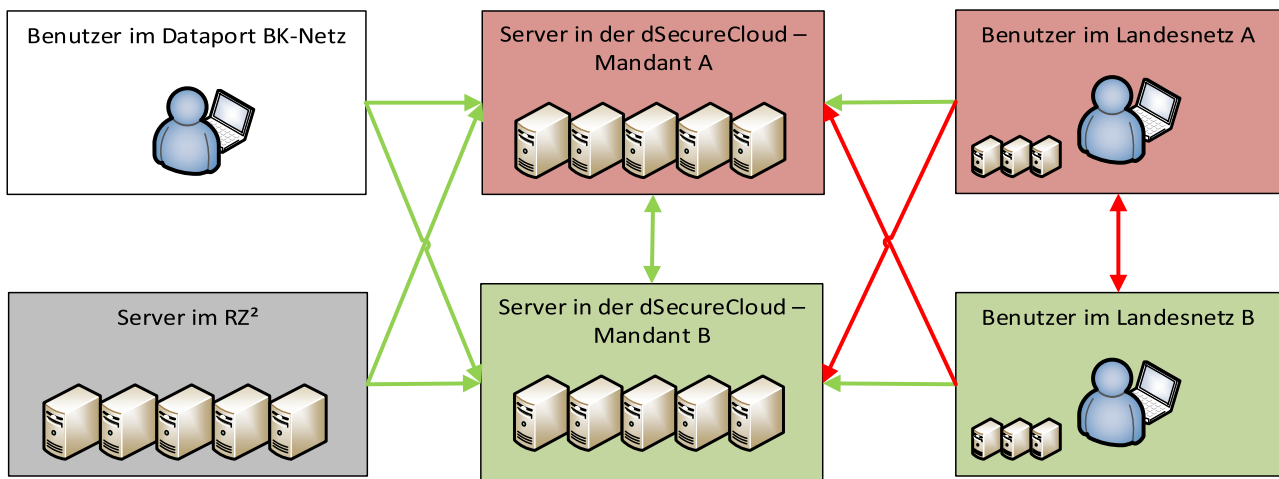


Abbildung 55 - valide Kommunikationswege

Vor allem bei der Neueinrichtung einer Gruppe in dem dSecureCloud Portal muss darauf geachtet werden, von wo nach wo die Kommunikation zugelassen ist.

Für die in der Abbildung mit einem grünen Pfeil dargestellten Wege können über einen Service im Portal selbstständig Firewall-Freischaltungen eingerichtet werden. Auf diesen Wegen wurden auf den Firewall im RZ „any“ (any IP & any Port) Freischaltungen eingerichtet und die Kommunikation wird direkt von der Firewall der dSecureCloud gefiltert.

Die mit dem roten Pfeil gekennzeichneten Wege können aus technischen Gründen nicht freigeschaltet werden – daher ist es wichtig, die virtuellen Server in dem korrekten dSecureCloud Mandanten zu platzieren. Dabei gilt die Regel, dass Server eines Mandanten nur aus dem dazugehörigen Landesnetz erreichbar sind und zusätzlich aus dem BK-Netz und von Servern in dem Dataport RZ² aus. **Wichtig!** - das hinzufügen mehrerer Netzwerkadapter, wobei jeder Adapter einem anderen Mandantenbereich (Netzbereich) zugeordnet wurde (Mandantenkopplung), ist untersagt und wird zu Problemen beim Routing führen.

Beispiel: Kunden aus dem Landesnetz HH können nur auf Server des Mandanten HH zugreifen, Kunden aus dem Landesnetz SH nur auf Server des Mandanten SH etc.

5.4.1 Firewall Service – Bericht über eingerichtete Freischaltungen

Den Service ruft man in dem Servicekatalog auf, die Anforderung kann sofort abgesendet werden:

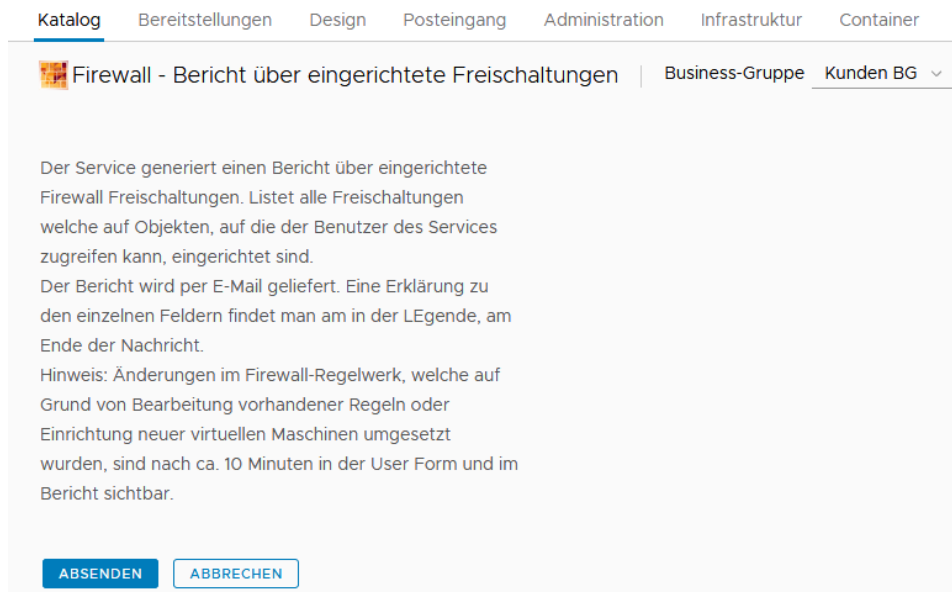
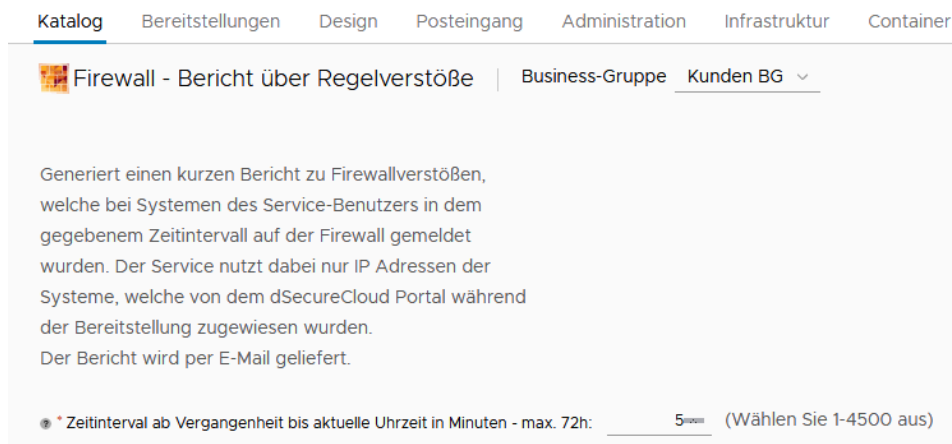


Abbildung 56 - Bericht zu eingerichteten Freischaltungen anfordern

Der Benutzer des Services erhält per E-Mail einen Bericht zu eingerichteten Freischaltungen. Am Ende der E-Mail befindet sich eine Legende welche den Inhalt der einzelnen Tabellenfelder erläutert.

5.4.2 Firewall Service – Bericht über Regelverstöße

Den Service ruft man in dem Servicekatalog auf, nach Eingabe des Zeitraums kann die Anforderung abgesendet werden:



Der Benutzer des Services erhält per E-Mail einen Bericht zu Firewallregelverstößen, welche bei allen seinen VMs aufgetreten sind. Im E-Mail Inhalt werden maximal 50 Verstöße aufgelistet und falls in dem definierten Zeitintervall mehr erkannt wurden, findet man eine vollständige Liste im E-Mail Anhang.

5.4.3 Firewall Service - Neue Freischaltung einrichten, eingehend in Richtung Dataport Cloud oder innerhalb der Umgebung

Den Service ruft man in dem Servicekatalog auf:

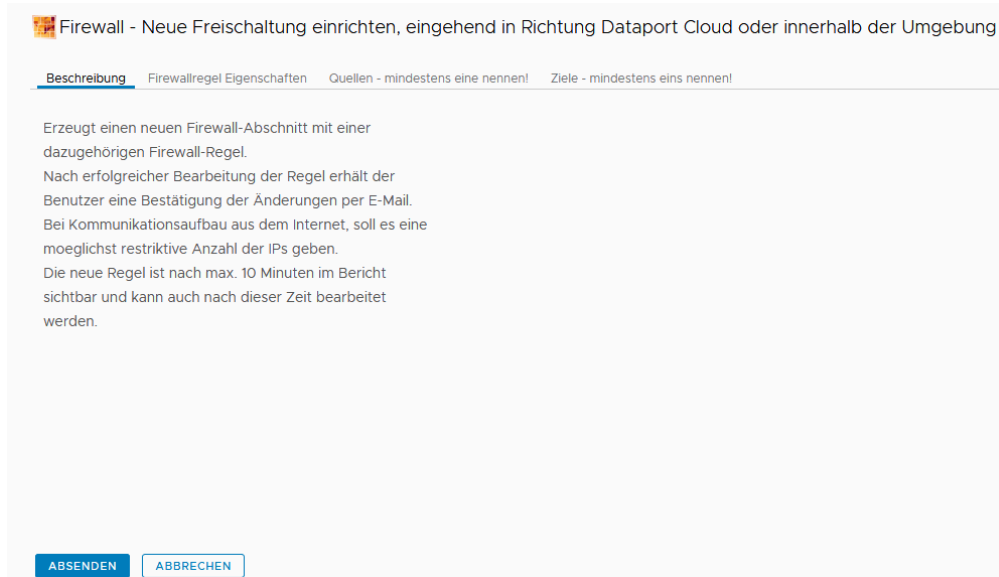


Abbildung 57 – Service aufrufen zwecks Hinzufügen eines neuen Firewall-Abschnitts

Quellen, Ziele und zusätzliche Inputs, die das Verhalten der Regel definieren, werden in weiteren Tabs eingefügt:



Abbildung 58 - Festlegen der Details einer Firewall-Freischaltung

- **Verhalten der Firewall Regel:** [allow\block\reject]
 - allow – Kommunikation erlaubt; ist der Standardwert
 - block – Kommunikation gesperrt
 - reject – Kommunikation gesperrt, sendet Meldung mit Ablehnung

Quellen:

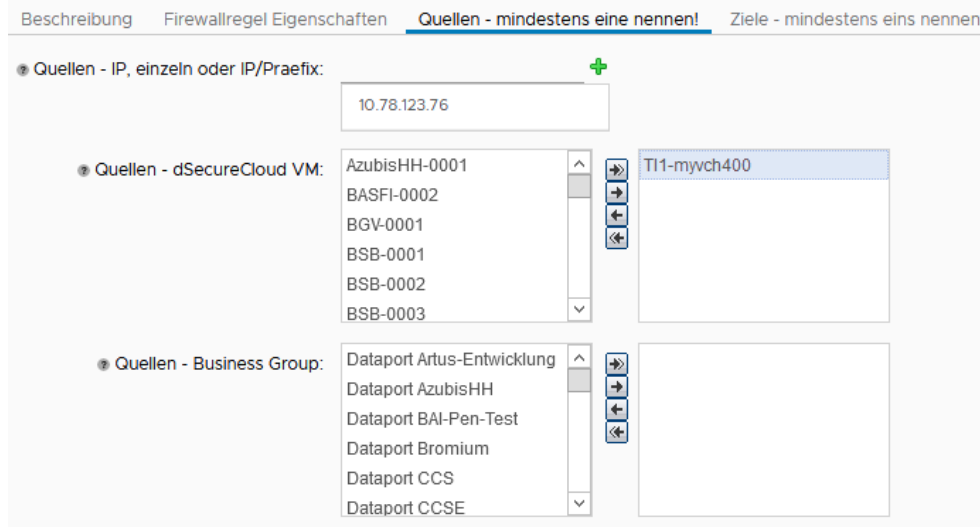


Abbildung 59 - Neue Freischaltung - Auswahl der Quellen

- **IPs** - In dem ersten Feld können IPv4 Adressen eingetragen werden, optional mit Präfix. Hier handelt es sich um Adressen der Systeme außerhalb der Dataport Cloud – IP der Systeme aus dieser Umgebung führen bei der Validierung zum Abbruch des Workflows.
- **dSecureCloud VM** - hier werden nur die virtuellen Maschinen angezeigt, welche der Business Group des Anforderungsstellers gehören. Beispiel – wenn der Benutzer Mitglied der Gruppe Dataport TZ3 und TZ1 ist, werden in dieser Ansicht alle VMs der Gruppe Dataport TZ3 und Dataport TZ1 angezeigt. Wichtig!
 - o innerhalb der Dataport Cloud Umgebung werden virtuelle Maschinen anhand der IP Adressen gewählt, es wird nur mit VM Namen (VM Objekt) gearbeitet. Grund dafür ist, dass Freischaltungen in dem System auf VM Objekten (und anderen Objekten der virtuellen Umgebung) basieren. Falls sich die IP Adresse des Systems ändern sollte, greifen die Freischaltungen immer noch.
- **Business Group** – ähnlich wie bei virtuellen Maschinen, kann jede bestehende Business Group als Quelle gewählt werden. Bei Auswahl einer Business Group werden alle dieser Gruppe zugehörigen virtuellen Maschinen mit in die neue Freischaltung aufgenommen – auch Systeme die zukünftig von Benutzern erstellt werden. So muss die Freischaltung nicht jedes Mal um neue Systeme erweitert werden.

Ziele:

Beschreibung	Firewallregel	Eigenschaften	Quellen - mindestens eine nennen!	Ziele - mindestens eins nennen!
<ul style="list-style-type: none"> Ziele - dSecureCloud VM: 			<ul style="list-style-type: none"> AzubisHH-0001 BASFI-0002 BGV-0001 BSB-0001 BSB-0002 BSB-0003 	
<ul style="list-style-type: none"> Ziele - Business Group: 			<ul style="list-style-type: none"> Dataport ZIAF-Entwicklung Dataport dAbstimmBox MHB SJFIS MHB SUBV MHB SWAH MHB ZERD.Web 	<ul style="list-style-type: none"> Kunden BG
<ul style="list-style-type: none"> Ziele - TCP Ports, leer = any: 				<input type="text" value="443"/>
<ul style="list-style-type: none"> Ziele - UDP Ports, leer = any: 				<input type="text" value="5143"/>

Abbildung 60 - Neue Freischaltung - Ziele und Netzwerkports

- **dSecureCloud VM** – hier werden nur die virtuellen Maschinen angezeigt, welche der Business Group des Anforderungsstellers gehören. Beispiel – wenn der Benutzer Mitglied der Gruppe Dataport TZ3 und TZ1 ist, werden in dieser Ansicht alle VMs der Gruppe Dataport TZ3 und Dataport TZ1 angezeigt.
- **Business Groups** – ähnlich wie oben, stehen hier Business Groups zur Auswahl, bei welchen der Anforderungssteller Mitglied ist. Auch hier muss man beachten, dass das Ziel sich im gleichen Mandantenbereich befindet, wie die Quelle.
- **Ports TCP/UDP** – Netzwerkports beim Zielsystem, einzeln oder als Range eintragen. Den Eintrag mit (+) bestätigen.

Zum Schluss wird das Workflow mit „Absenden“ („Submit“) gestartet. Der Status der Ausführung kann überwacht werden, s. Punkt [5.4.6](#).

5.4.4 Firewall Service - Regel einem vorhandenem Firewall-Abschnitt hinzufügen

Den Service ruft man in dem Servicekatalog auf, die Anforderung kann sofort übernommen werden:

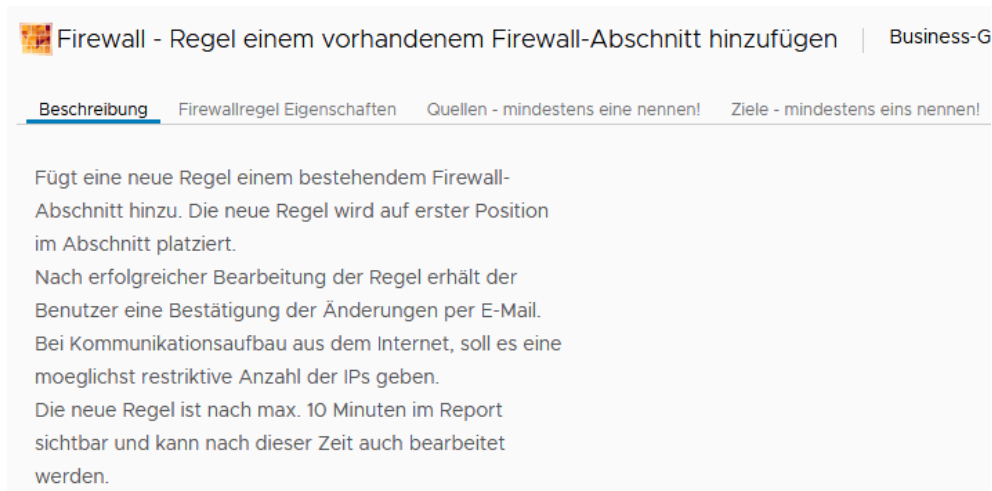


Abbildung 61 - Regel einem vorhandenem Firewall-Abschnitt hinzufügen - Aufruf des Services

Im nächsten Schritt wird ein bestehender Firewall-Abschnitt gewählt, danach kann der neue Regelname eingefügt und das Verhalten der Regel festgelegt werden. Optional wird ein Kommentar hinzugefügt:

Beschreibung **Firewallregel Eigenschaften** Quellen - mindestens eine nennen! Ziele - mindestens eins nennen!

* Firewall-Abschnitt:

* Firewall Regel - Name (max. 30 Zeichen, nur a-Z,0-9,-,_ erlaubt):

(optional) Firewall Regel - Kommentar (max. 200 Zeichen):

* Firewall-Regel - Verhalten:

* Firewall-Regel Status - ist die Regel deaktiviert?:

Abbildung 62 - Regel einem vorhandenem Firewall-Abschnitt hinzufügen - Benennung und Verhalten festlegen

- **Verhalten der Firewall-Regel:** [allow\block\reject]
 - allow – Kommunikation erlaubt; ist der Standardwert
 - block – Kommunikation gesperrt
 - reject – Kommunikation gesperrt, sendet Meldung mit Ablehnung
- **Firewall-Regel Status:** [true>false]
 - false – Regel ist aktiv (Standardwert)
 - true – Regel wird deaktiviert

Quellen und Ziele werden ähnlich wie bei einer neuen Freischaltung eingetragen.

Quellen:

Abbildung 63 - Regel einem vorhandenem Firewall-Abschnitt hinzufügen – Auswahl der Quellen

- **IPs** - In dem ersten Feld können IPv4 Adressen eingetragen werden, optional mit Präfix. Hier handelt es sich um Adressen der Systeme außerhalb der Dataport Cloud – IP der Systeme aus dieser Umgebung führen bei der Validierung zum Abbruch des Workflows.
- **dSecureCloud VM** - hier werden nur die virtuellen Maschinen angezeigt, welche der Business Group des Anforderungsstellers gehören. Beispiel – wenn der Benutzer Mitglied der Gruppe Dataport TZ3 und TZ1 ist, werden in dieser Ansicht alle VMs der Gruppe Dataport TZ3 und Dataport TZ1 angezeigt. Wichtig!
 - innerhalb der Dataport Cloud Umgebung werden virtuelle Maschinen anhand der IP Adressen gewählt, es wird nur mit VM Namen (VM Objekt) gearbeitet. Grund dafür ist, dass Freischaltungen in dem System auf VM Objekten (und anderen Objekten der virtuellen Umgebung) basieren. Falls sich die IP Adresse des Systems ändern sollte, greifen die Freischaltungen immer noch.
- **Business Group** – ähnlich wie bei virtuellen Maschinen, kann jede bestehende Business Group als Quelle gewählt werden. Bei Auswahl einer Business Group werden alle dieser Gruppe zugehörigen virtuellen Maschinen mit in die neue Freischaltung aufgenommen – auch Systeme die zukünftig von Benutzern erstellt werden. So muss die Freischaltung nicht jedes Mal um neue Systeme erweitert werden.

Ziele:

Beschreibung Firewallregel Eigenschaften Quellen - mindestens eine nennen! **Ziele - mindestens eins nennen!**

Mindestens ein Ziel muss gewählt werden!

Ziele - Dataport Cloud VM:

AzubisHH-0001
BASFI-0002
BGV-0001
BSB-0001
BSB-0002
BSB-0003

Ziele - Business Group:

MHB SJFIS
MHB SUBV
MHB SWAH
MHB ZERD-Web
MHH Jira LGV
MSH SVS-SH

Ziele - TCP Ports, leer = any: +
 Keine Daten ausgewählt

Ziele - UDP Ports, leer = any: +
 514

Abbildung 64 - Regel einem vorhandenem Firewall-Abschnitt hinzufügen – Ziele und Netzwerkports

- **dSecureCloud VM** – hier werden nur die virtuellen Maschinen angezeigt, welche der Business Group des Anforderungsstellers gehören. Beispiel – wenn der Benutzer Mitglied der Gruppe Dataport TZ3 und TZ1 ist, werden in dieser Ansicht alle VMs der Gruppe Dataport TZ3 und Dataport TZ1 angezeigt.
- **Business Groups** – ähnlich wie oben, stehen hier Business Groups zur Auswahl, bei welchen der Anforderungssteller Mitglied ist. Auch hier muss man beachten, dass das Ziel sich im gleichen Mandantenbereich befindet, wie die Quelle.
- **Ports TCP/UDP** – Netzwerkports beim Zielsystem, einzeln oder als Range eintragen. Den Eintrag mit (+) bestätigen.

Zum Schluss wird das Workflow mit „Absenden“ („Submit“) gestartet. Der Status der Ausführung kann überwacht werden, s. Punkt [5.4.6](#).

5.4.5 Firewall Service - Bearbeitung vorhandener Freischaltungen

Den Service ruft man in dem Servicekatalog auf, die Anforderung kann sofort übernommen werden:

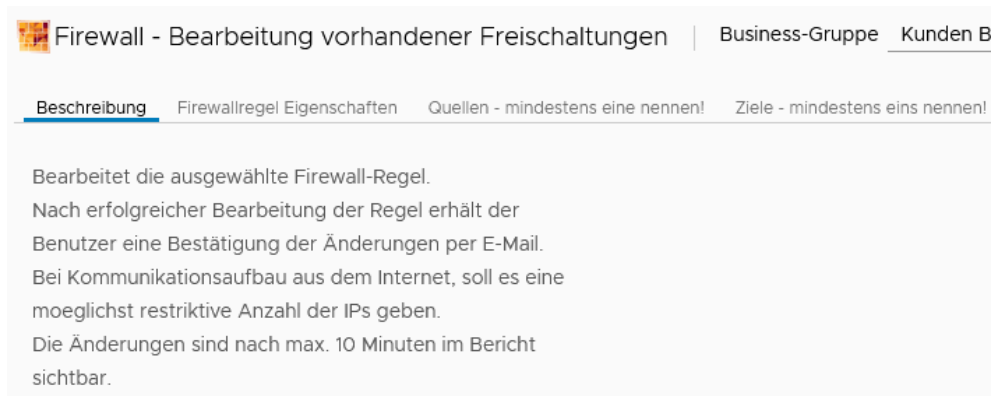


Abbildung 65 – Bearbeitung vorhandener Freischaltungen - Aufruf des Services

Im nächsten Schritt kommt man zum Eingabeformular.
Eigenschaften der Firewall-Regel:

Abbildung 66 – Bearbeitung vorhandener Freischaltungen - Aufrufen der Details

Anfangs sind alle Felder leer. Über die Drop-Down Felder wählt man den betroffenen Firewall-Abschnitt aus, danach kann aus einer Liste eine dem Abschnitt untergeordnete Regeln gewählt werden:

Abbildung 67 - Bearbeitung vorhandener Freischaltungen - Bearbeitung der Details

Optional können hier auch die der Regelname geändert, ein Kommentar zur Regel hinzugefügt\geändert und das Verhalten der Regel festgelegt werden.

In den nächsten Eingabemasken können Änderungen am Regelwerk vorgenommen werden. Bereits hinzugefügte Objekte werden ins Formular geladen.

Quellen:

Abbildung 68 - Bearbeitung vorhandener Freischaltungen - Auswahl der Quellen

- **IPs** - In dem ersten Feld können IPv4 Adressen eingetragen werden, optional mit Präfix. Hier handelt es sich um Adressen der Systeme außerhalb der Dataport Cloud – IP der Systeme aus dieser Umgebung führen bei der Validierung zum Abbruch des Workflows.
- **dSecureCloud VM** - hier werden nur die virtuellen Maschinen angezeigt, welche der Business Group des Anforderungsstellers gehören. Beispiel – wenn der Benutzer Mitglied der Gruppe Dataport TZ3 und TZ1 ist, werden in dieser Ansicht alle VMs der Gruppe Dataport TZ3 und Dataport TZ1 angezeigt. Wichtig!
 - o innerhalb der Dataport Cloud Umgebung werden virtuelle Maschinen anhand der IP Adressen gewählt, es wird nur mit VM Namen (VM Objekt) gearbeitet. Grund dafür ist, dass Freischaltungen in dem System auf VM Objekten (und anderen Objekten der virtuellen Umgebung) basieren. Falls sich die IP Adresse des Systems ändern sollte, greifen die Freischaltungen immer noch.
- **Business Group** – ähnlich wie bei virtuellen Maschinen, kann jede bestehende Business Group als Quelle gewählt werden. Bei Auswahl einer Business Group werden alle dieser Gruppe zugehörigen virtuellen Maschinen mit in die neue Freischaltung aufgenommen – auch Systeme die zukünftig von Benutzern erstellt werden. So muss die Freischaltung nicht jedes Mal um neue Systeme erweitert werden.

Ziele:

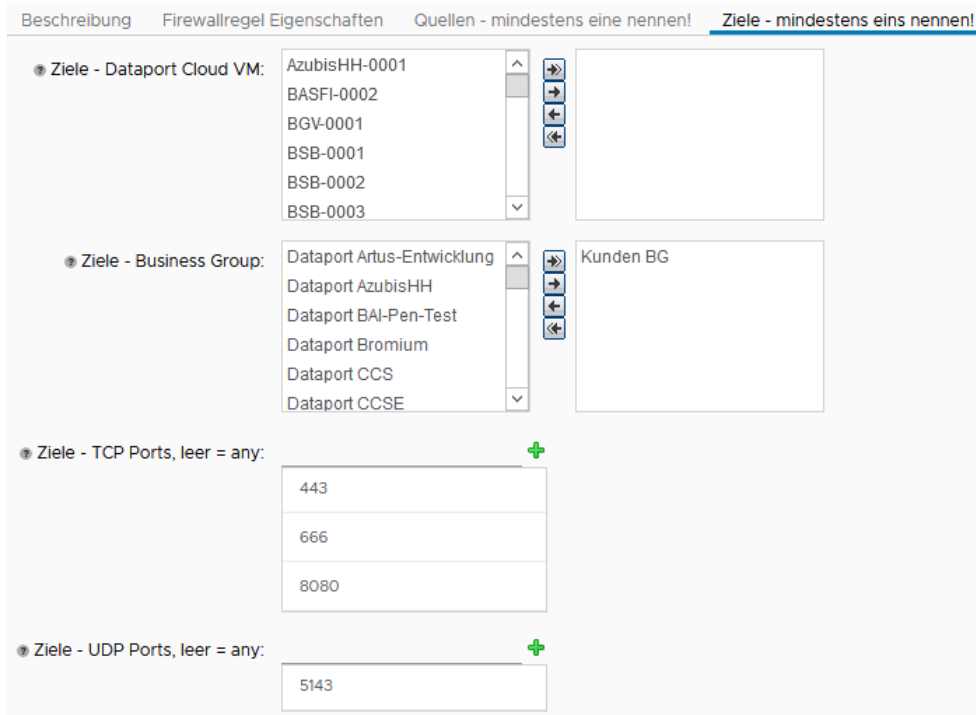


Abbildung 69 - Bearbeitung vorhandener Freischaltungen - Ziele und Netzwerkports

- **dSecureCloud VM** – hier werden nur die virtuellen Maschinen angezeigt, welche der Business Group des Anforderungsstellers gehören. Beispiel – wenn der Benutzer Mitglied der Gruppe Dataport TZ3 und TZ1 ist, werden in dieser Ansicht alle VMs der Gruppe Dataport TZ3 und Dataport TZ1 angezeigt.
- **Business Groups** – ähnlich wie oben, stehen hier Business Groups zur Auswahl, bei welchen der Anforderungssteller Mitglied ist. Auch hier muss man beachten, dass das Ziel sich im gleichen Mandantenbereich befindet, wie die Quelle.
- **Ports TCP/UDP** – Netzwerkports beim Zielsystem, einzeln oder als Range eintragen. Den Eintrag mit (+) bestätigen.

Zum Schluss wird das Workflow mit „Absenden“ („Submit“) gestartet. Der Status der Ausführung kann überwacht werden, s. Punkt 5.4.6.

5.4.6 Firewall Service – Überwachung aktiver Ausführungen und Bestätigung der Änderung am Regelwerk

Sobald sie über die Schaltfläche „Absenden“ den Service angefordert haben, kann der aktuelle Status der Ausführung in dem übergeordneten Tab „Bereitstellungen“ erfolgen:

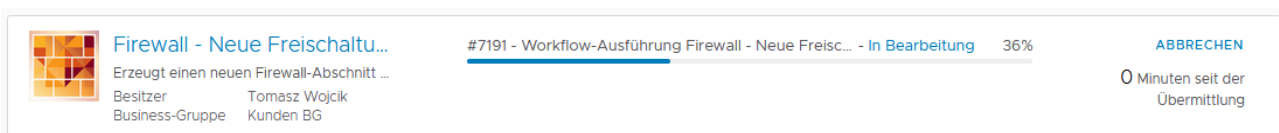


Abbildung 70 - Status der Freischaltungseinrichtung

Sollte die Bereitstellung fehlschlagen, kann diese über einen Menüpunkt erneut übermittelt werden:

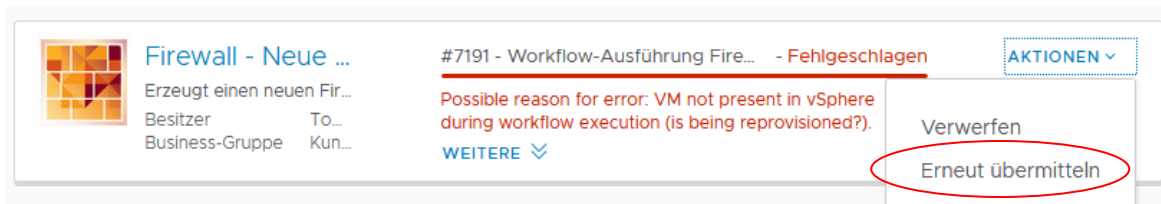


Abbildung 71 – Wiederholung einer fehlgeschlagenen Anforderung

Nach einer erfolgreichen Umsetzung der Anforderung (hier: Erstellung der Regel) erhält der Benutzer eine E-Mail mit Bestätigung des Auftrags:

Antworten | Allen antworten | Weiterleiten | Chat

Di 05.02.2019 16:26

Dataport dsecurecloud

NSX Firewallregel Erzeugung - Info

An Wojcik, Tomasz

Firewall Regel erfolgreich erzeugt!

Name der Firewall Regel: dSC-Testregel
Regel ID: 1800
Firewall-Abschnitt Name: dSC-Testabschnitt
Workflow User: WojcikTo-Admin@mgmt.dpaor.org

- Quellen -
VMs: Master-KundenBG-0002
IPs: 10.78.123.76

- Ziele -
Business Groups: Kunden BG
TCP Ports: 443
UDP Ports: 5143

Mit freundlichen Grüßen
Ihr Dataport Cloud Team
Diese Mail wurde automatisiert erzeugt.

Abbildung 72 - Firewall Service - Bestätigung der Umsetzung

Die Regel ID ist einzigartig und dient der schnelleren Identifizierung einer Regel im System.

5.5 SLES – Installserver

Zum Patchen der SLES 11 und SLES 12 Server in der Dataport Cloud Umgebung werden folgende Schritte benötigt:

1. Zuerst muss der Installserver 10.61.127.60 im Proxy als Ausnahme eingetragen werden.
2. Danach werden Repositories hinzugefügt:

für SLES11 SP4 64bit

zypper ar http://10.61.127.60/YUP/SLES11-SP4-Pool/sle-11-x86_64 PoolRepo

zypper ar http://10.61.127.60/YUP/SLES11-SP4-Updates/sle-11-x86_64 Updates

für SLES12 SP2 64bit

zypper ar [url] [repo], z.B. *zypper ar http://10.61.127.60/repo/SUSE/Updates/SLE-SERVER/12-SP2/x86_64/update Dataport-SLES12-SP2-Updates*

Dataport-SLES12-SP2-Updates.repo:baseurl=http://10.61.127.60/repo/SUSE/Updates/SLE-SERVER/12-SP2/x86_64/update

Dataport-SLES12-SP2.repo:baseurl=http://10.61.127.60/repo/SUSE/Products/SLE-SERVER/12-SP2/x86_64/product/

Legacy-module-sles-updates.repo:baseurl=http://10.61.127.60/repo/SUSE/Updates/SLE-Module-Legacy/12/x86_64/update

Legacy-module-sles.repo:baseurl=http://10.61.127.60/repo/SUSE/Products/SLE-Module-Legacy/12/x86_64/product

SLE-Module-Adv-Systems-Management-updates.repo:baseurl=http://10.61.127.60/repo/SUSE/Updates/SLE-Module-Adv-Systems-Management/12/x86_64/update/

SLE-Module-Adv-Systems-Management.repo:baseurl=http://10.61.127.60/repo/SUSE/Products/SLE-Module-Adv-Systems-Management/12/x86_64/product/

SLE-Module-Containers-updates.repo:baseurl=http://10.61.127.60/repo/SUSE/Updates/SLE-Module-Containers/12/x86_64/update/

SLE-Module-Containers.repo:baseurl=http://10.61.127.60/repo/SUSE/Products/SLE-Module-Containers/12/x86_64/product/

SLE-Module-Public-Cloud-updates.repo:baseurl=http://10.61.127.60/repo/SUSE/Updates/SLE-Module-Public-Cloud/12/x86_64/update/

SLE-Module-Public-Cloud.repo:baseurl=http://10.61.127.60/repo/SUSE/Products/SLE-Module-Public-Cloud/12/x86_64/product/

SLE-SDK-updates.repo:baseurl=http://10.61.127.60/repo/SUSE/Updates/SLE-SDK/12-SP2/x86_64/update/
SLE-SDK.repo:baseurl=http://10.61.127.60/repo/SUSE/Products/SLE-SDK/12-SP2/x86_64/product/

Welche Repos nötig sind, hängt davon ab, welches Produkt installiert wurde, diese kann man mit *zypper se -i -t product* ermitteln. Zu jedem installierten Produkt braucht man die entsprechenden Pool und Update Channels.

3. Refresh der Repositories:

zypper ref

4. Preview des Updates:

zypper lu

5. Patches installieren:

zypper up

zypper up -y (ohne Nachfrage)

5.6 Virenschutz

Auf den bereitgestellten VMs wird das Installationspaket für den VirusScan Enterprise von McAfee mitgeliefert.

5.6.1 Windows

Das Paket befindet sich im Ordner C:_INSTALL

Nachdem die Batchdatei „Virenschutz_Installation“ ausgeführt wird, werden alle Komponenten automatisch installiert:

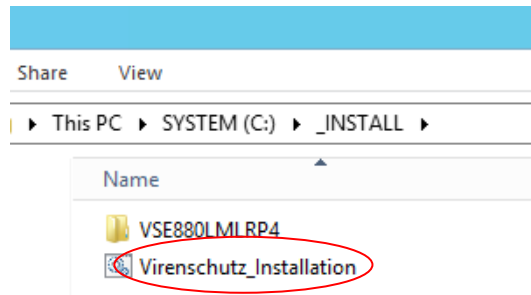


Abbildung 73 - Pfad zu der AV Installationsdatei – MS Windows

Nach einiger Zeit erscheint eine Bestätigung:



Abbildung 74 - McAfee Installationsbestätigung

Das Programm setzt die Arbeit automatisch fort:

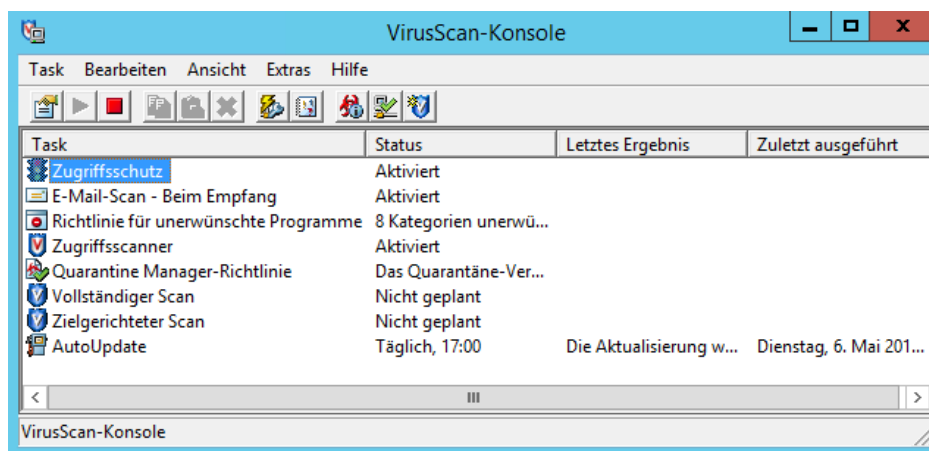


Abbildung 75 - McAfee VSE Konsole

5.6.2 Linux (SLES und Ubuntu)

Das Paket befindet sich in dem Ordner:

SLES, Ubuntu: /tmp_AV

Vor der Installation auf Ubuntu Systemen muss zuvor unzip installiert werden (sudo apt-get install unzip).

Bei der Installation bitte folgend vorgehen:

1. McAfee Runtime Installation :

```
SLES: # rpm -ivh MFErt.i686.rpm
```

```
Ubuntu: # dpkg -i MFErt.i686.deb
```

2. McAfee Agent Installation:

```
SLES: # rpm -ivh MFEma.x86_64.rpm
```

```
Ubuntu: # dpkg -i MFEma.x86_64.deb
```

3. ISec Installation:

```
Ubuntu: chmod +x install-isectp.sh
```

```
sudo ./install-isectp.sh
```

4. Installation prüfen:

```
cd /opt/isec/ens/threatprevention/bin
```

```
Version abrufen: ./isecav --version
```

```
Status prüfen: ./isecav --getoasconfig --summary
```

Weitere Details zur Bedienung des Programms entnehmen Sie bitte aus der Bedienungsanleitung, welche sich in dem gleichen Ordner befindet, wie das Installationskript.

5.7 Kopieren einer VM aus dSecureCloud auf lokalen Speicher mit dem vCenter Converter

Das Kopieren einer VM auf lokalen Speicher (Runterladen einer VM) ist kein Service, der über das dSecureCloud Portal angeboten wird. Die Maßnahme wird vom Benutzer selbstständig ausgeführt. Hier wird ein optionaler Weg für die Umsetzung der Kopiervorgangs dargestellt.

Für das Runterladen einer VM kann das Tool „VMware vCenter Converter Standalone“ genutzt werden. Die Software kommt in den meisten Fällen zum Einsatz, wenn ein physikalischer Server in eine VM migriert wird (P2V Migration). Sie kann aber auch für die Migration einer VM in eine andere eingesetzt werden (V2V Migration). Mehr dazu:

<https://www.vmware.com/de/products/converter.html>

In dieser Anleitung wird die Version 6.2 genutzt, dabei werden 2 Möglichkeiten einer VM Migration – lokal und auf einem entfernten (Remote) System. Es ist nötig, Netzwerkfreischaltungen einzurichten, damit die Migration erfolgreich durchgeführt wird.

5.7.1 Installation

Das Tool kann unter folgendem Link runtergeladen werden:

<https://my.vmware.com/de/web/vmware/details?productId=701&downloadGroup=CONV62>

Die Installation erfolgt auf einem Windows-basiertem Betriebssystem. Eine Liste der für die Migration unterstützten Systeme befindet sich hier:

https://docs.vmware.com/en/vCenter-Converter-Standalone/6.2/rn/conv_sa_62_rel_notes.html#supportedguestOS

Nach erfolgreicher Installation sollen folgende Services als aktiv angezeigt werden; der Agent Dienst ist nur auf dem Zielsystem, welches migriert wird, nötig, dazu mehr in 5.5.2:




 VMware vCenter Converter Standalone Agent	VMware vC...	Running	Automatic (D...	Local Systeme...
 VMware vCenter Converter Standalone Server	VMware vC...	Running	Automatic (D...	Local Systeme...
 VMware vCenter Converter Standalone Worker	VMware vC...	Running	Automatic (D...	Local Systeme...

Abbildung 76 - VMware Converter Services

Mithilfe des Clients verbindet man sich mit dem lokalen Server:



Abbildung 77 - VMware Converter - Verbindungsaufbau zum lokalen oder remote Server

Nun kann man mit der Migration beginnen. Folgende Schritte sind in der offiziellen Anleitung im Kap. 6 „Convert a Physical or Virtual Machine“ beschrieben.

5.7.2 Kopieren einer VM Windows auf lokalen Speicher

Der Converter bietet die Möglichkeit, die VM, wo der Converter installiert wurde, direkt auf lokalen Speicher des Systems zu konvertieren. Dafür wählt man als Quelle das lokale System:

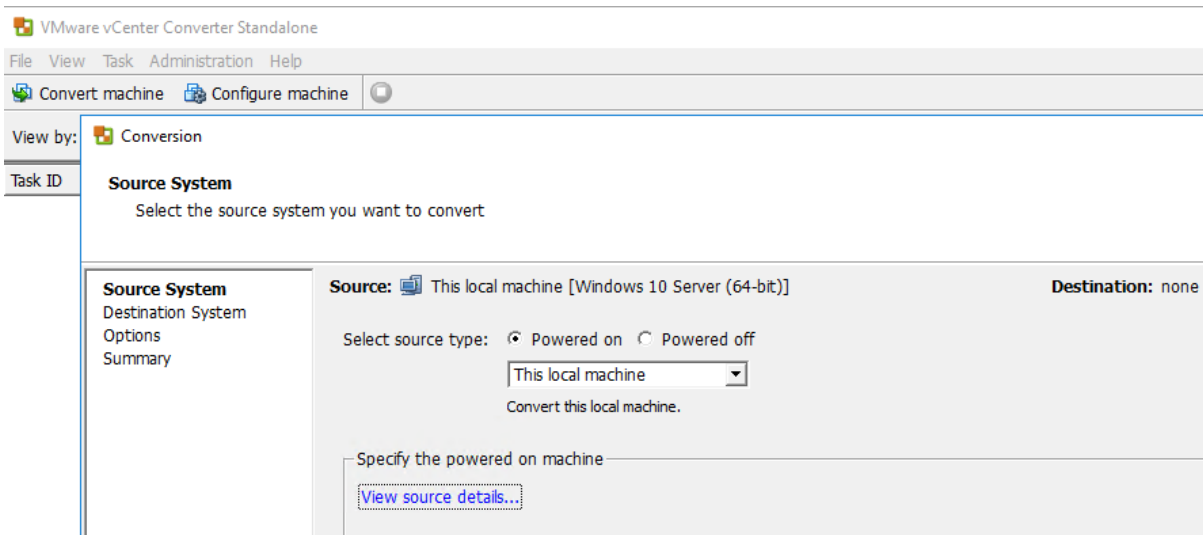


Abbildung 78 - VMware Converter - Auswahl des lokalen Systems

Ziel ist eine „VMware Workstation“ VM. In folgendem Punkt kann ein lokaler Ordner als Datenablage gewählt werden:

Destination System

Select a host for the new virtual machine

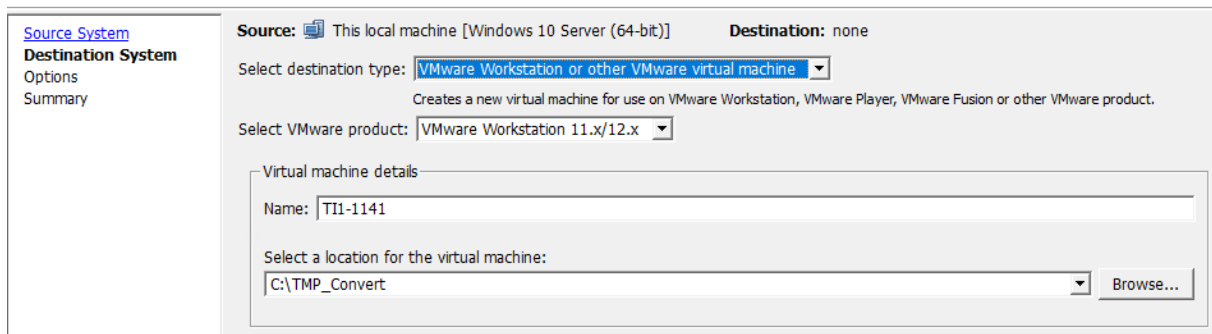


Abbildung 79 - VMware Converter - Auswahl des Zielsystems

Im nächsten Schritt können diverse Optionen der Konvertierung definiert werden. Im Beispiel unten wird eine Warnung angezeigt in welcher darauf hingedeutet wird, dass im Zielordner nicht genügend freier Speicher vorhanden sein könnte – dabei wird aber die Größe der Festplatte in Betracht genommen, bei der Konvertierung werden aber nur der Inhalt der Platte kopiert.

Options

Set up the parameters for the conversion task

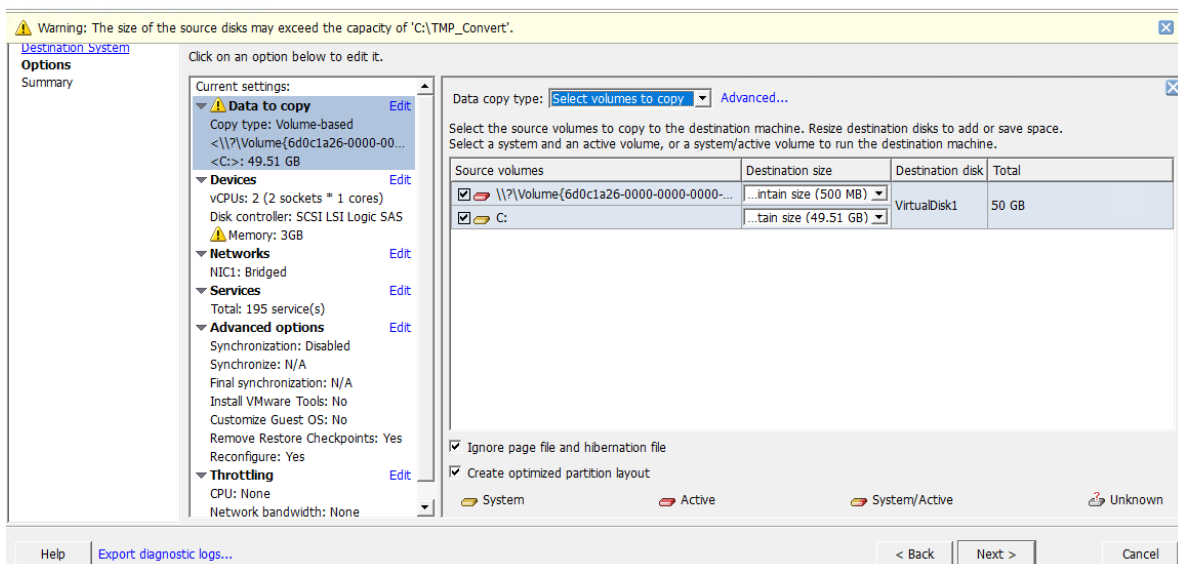


Abbildung 80 - VMware Converter - Optionen für die Konvertierung

Zum Schluss gibt es eine Zusammenfassung der gewählten Optionen und die Konvertierung kann beginnen:

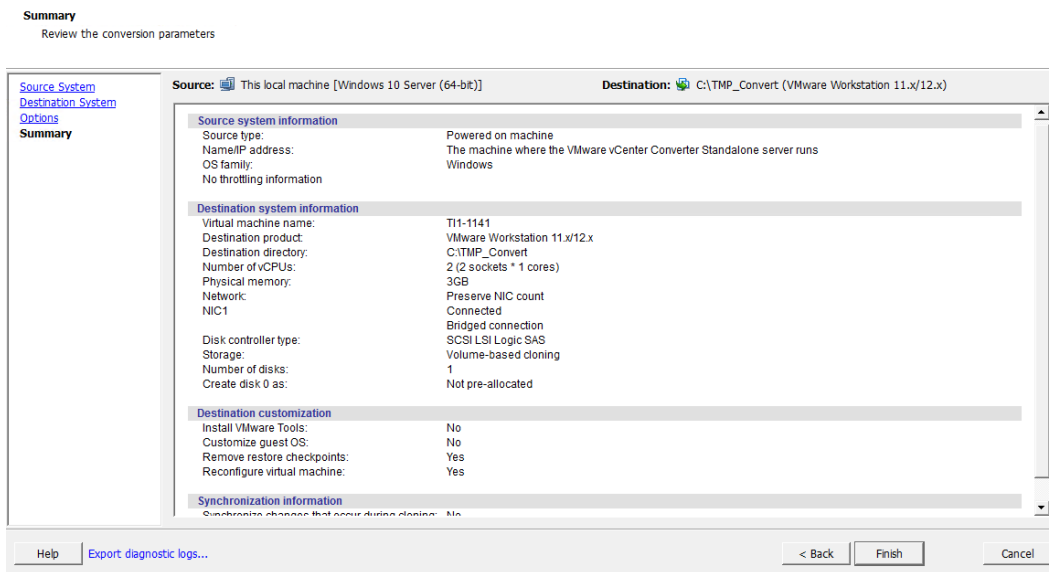


Abbildung 81 - VMware Converter - Zusammenfassung der gewählten Optionen

Der Status der Konvertierung wird im Hauptfenster des Converters angezeigt:

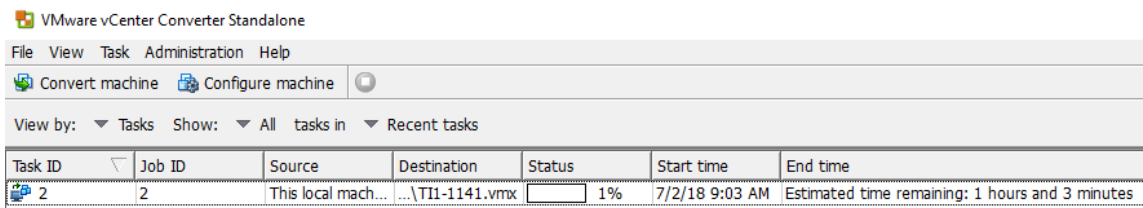


Abbildung 82 - VMware Converter - Status der Konvertierung

Die erzeugte Kopie der VM kann man aus dem Zielordner runterladen:

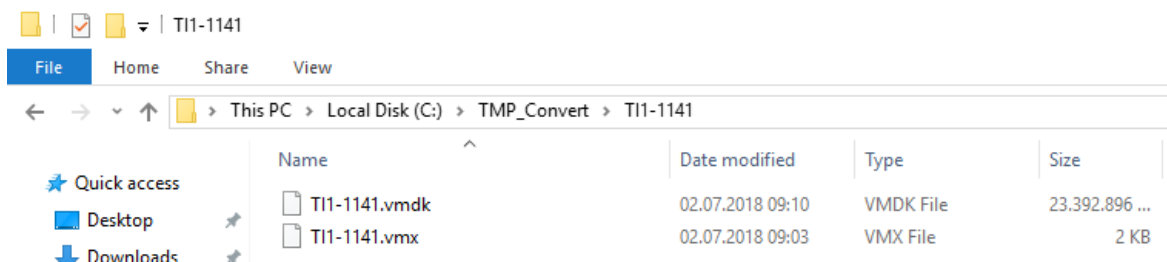


Abbildung 83 – VMware Converter - Pfad zum lokal konvertierten System

5.7.3 Kopieren einer Remote Windows VM

Converter Agent Installation

Auf dem System, welches kopiert werden soll, muss der Converter Agent Dienst laufen. Die Installation kann man manuell ausführen, indem der Converter Installer ausgeführt und nur die Agent Rolle ausgewählt wird:

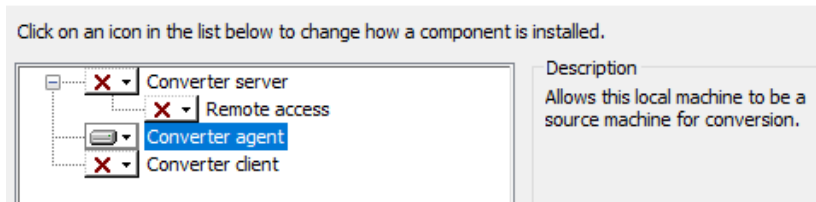


Abbildung 84 - VMware Converter - Installation des Agenten auf dem remote System

Wichtig! Der Converter Agent Dienst muss mit den Credentials des lokalen Administratoren, bzw. eines anderen Accounts, welches Admin-Privilegien hat, konfiguriert werden, ansonsten startet der Dienst nicht:

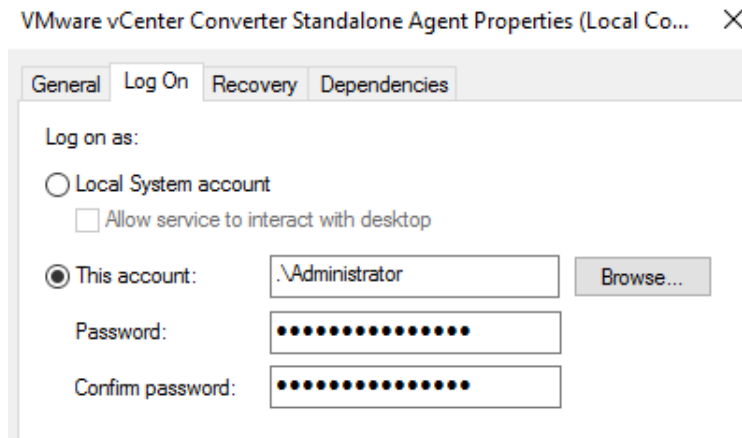


Abbildung 85 - VMware Converter - Agent Service User Privilegien

Diese Einstellung kann man nach der Installation ändern, danach wird der Dienst gestartet.

Alternativ kann der Agent automatisch, beim Aufbau der Verbindung über den Converter Client, installiert werden, dabei muss man beachten, dass die Dienst Properties wie oben angepasst werden.

Verbindung mit Quellsystem herstellen und Konvertierung starten

Nachdem die Verbindung aufgebaut wurde, kann man den Converter Client mit einer VM verbinden:

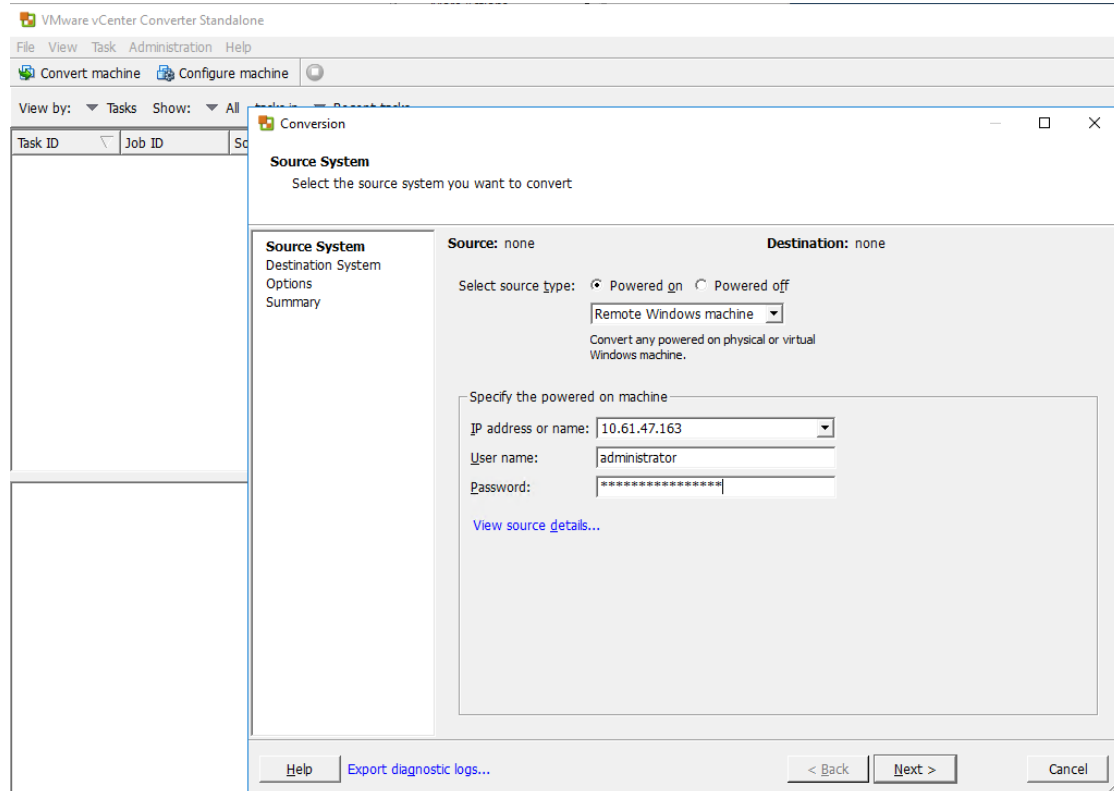


Abbildung 86 - VMware Converter - Verbindung Aufbauen zum remote System

Als Eingabe werden Credentials erwartet, welche administrative Rechte auf dem Remote System haben.

Nach Klicken auf „Next“ wird die Verbindung hergestellt. Der Status wird über einen Balken angezeigt:

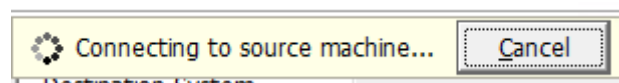


Abbildung 87 - VMware Converter - Verbindungsaufbau zum remote System

Damit die Verbindung erfolgreich hergestellt wird ist es wichtig, damit der Rechner, wo der Converter Server Dienst läuft, die Remote VM auch netztechnisch erreichen kann. Eine Liste der benötigten Netzwerkports kann man dem Benutzerhandbuch entnehmen:

https://www.vmware.com/pdf/convsa_61_guide.pdf#unique_28_Connect_42_AD966461, s. „Converter Standalone server to powered on source machine“

Zusätzlich dazu sollten weitere Voraussetzungen, die im oben genannten Kapitel genannt wurden, erfüllt sein, diese sind abhängig vom Betriebssystem.

Nach erfolgreicher Verbindung wird geprüft, ob auf dem Remote System auch der Converter Agent installiert wurde, in diesem Schritt kann entschieden werden, ob die Dateien nach der Konvertierung automatisch gelöscht werden sollen:

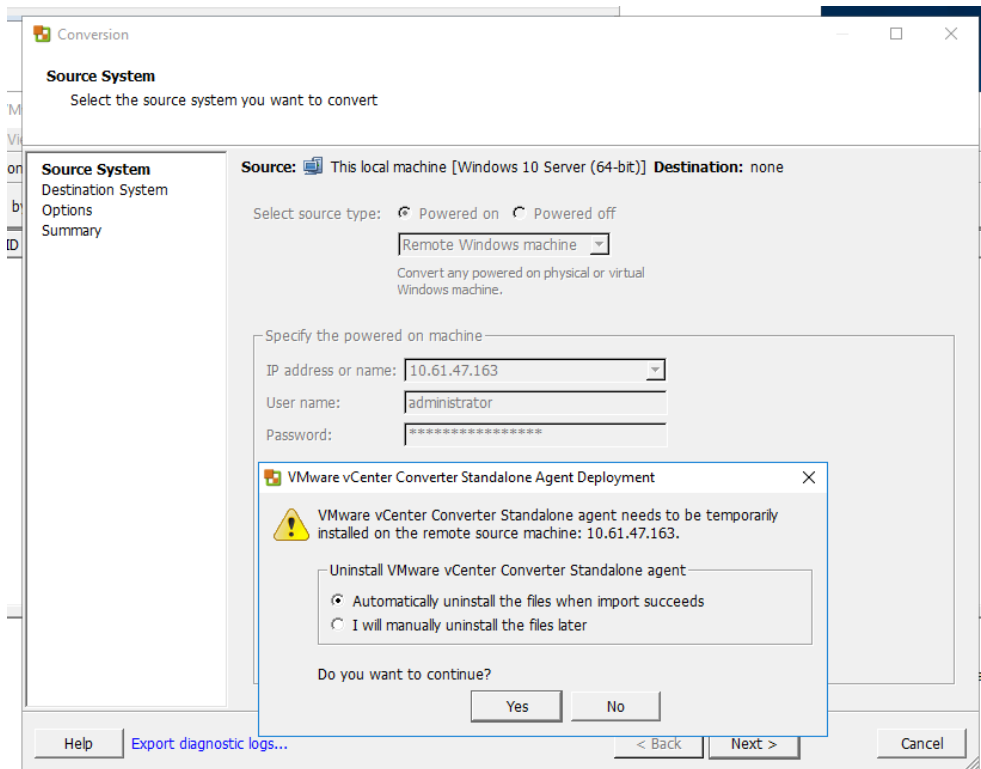


Abbildung 88 - VMware Converter - Verhalten nach Konvertierung festlegen

Falls nicht bereits erfolgt vorhanden, erfolgt die Installation des Converter Agenten auf dem Remote System:

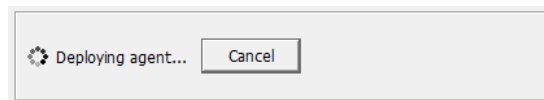


Abbildung 89 - VMware Converter - Optionale, automatische Installation des Agenten

Wenn das Zertifikat des Zielsystems nicht vertraut ist, kommt der Prompt:

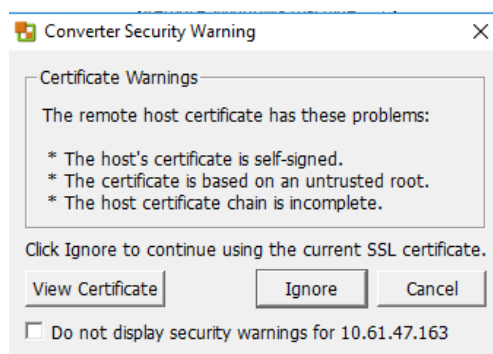


Abbildung 90 - VMware Converter - Zertifikatswarnung bei Verbindungsaufbau

Nachfolgend werden Einstellungen zur Ablage der konvertierten VM auf dem Zielsystems konfiguriert. Als „Destination Type“ soll „VMware Workstation...“ aus dem drop-down Feld gewählt werden. Danach können weitere Details definiert werden, wie hier:

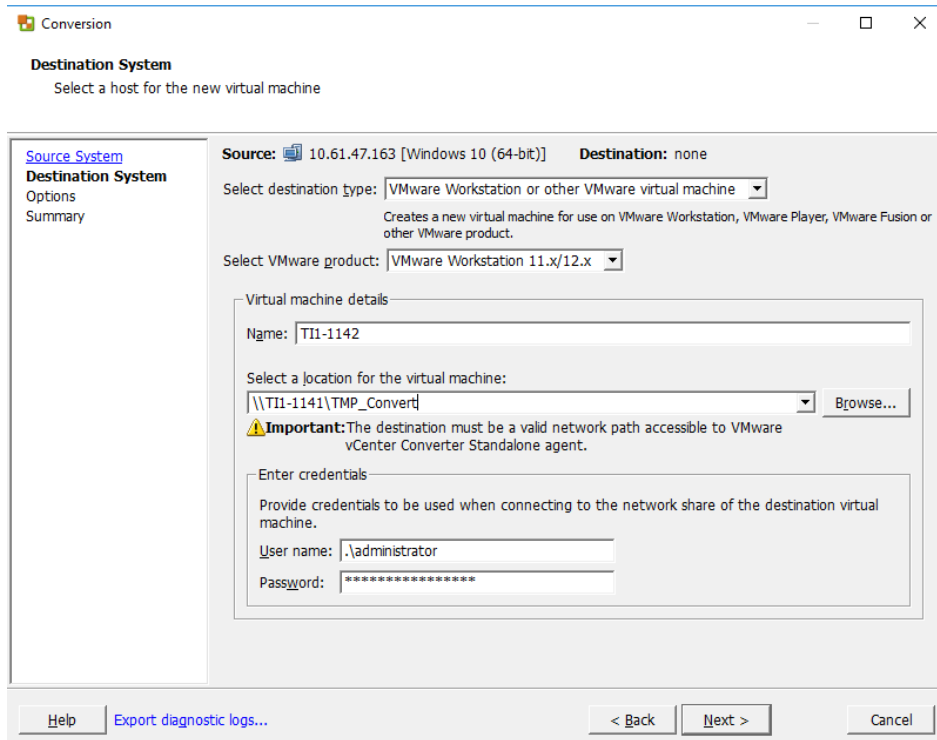


Abbildung 91 - VMware Converter - Wahl des Zielsystems

Wichtig! Beim Zielordner muss ein valider Netzwerkpfad angegeben werden, nicht ein Pfad zum lokalen Ordner. Wenn Sie die konvertierte VM lokal abspeichern möchten, auf dem System wo der Converter Client ausgeführt wird, muss lokal ein Netzwerk-Share eingerichtet werden.

Im nächsten Schritt können detaillierte Einstellungen einzelner Optionen gesetzt werden, z.B. die Auswahl, welche Festplatten konvertiert werden sollen. In dem Punkt „Data to copy“ kann die Warnung kommen, wo darauf hingewiesen wird, dass auf dem Zielsystem (lokales Share in diesem Fall) nicht genügend Speicherplatz vorhanden ist, um die Migration erfolgreich durchzuführen:

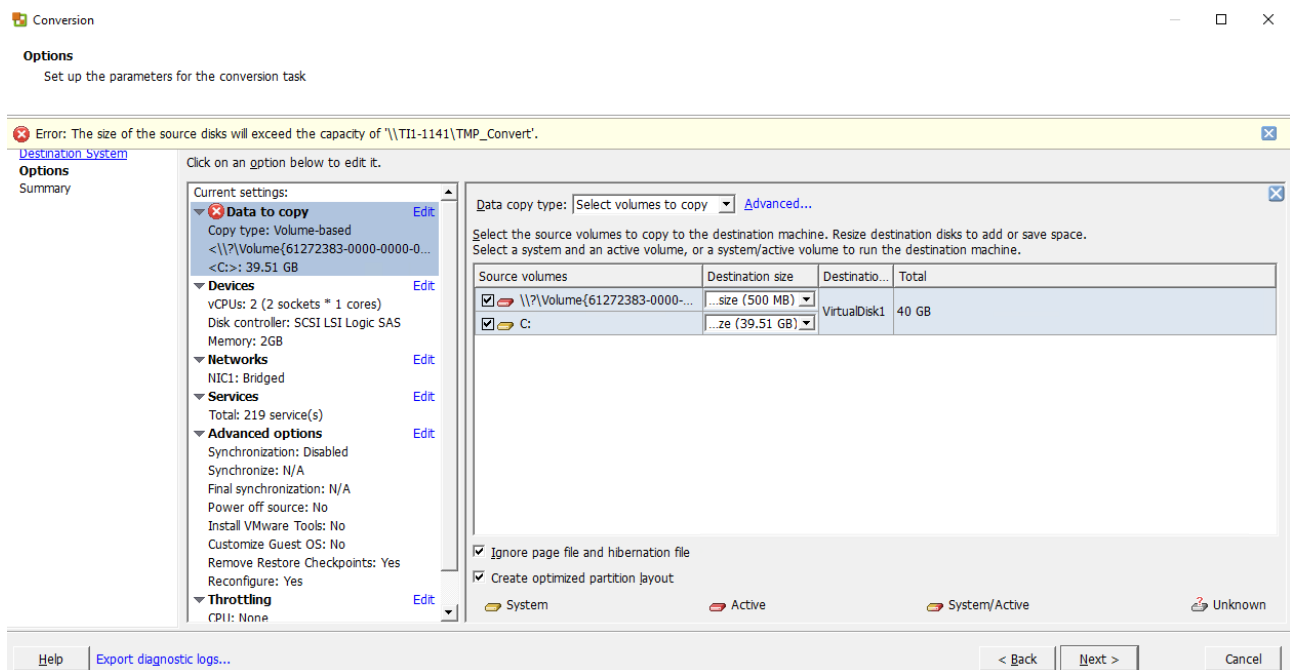


Abbildung 92 - VMware Converter - Details der Konvertierung festlegen

Dabei prüft der Converter Client, wie groß die Festplatte der VM ist, und nicht wie viele Daten sich dort tatsächlich befinden. In dem obigen Beispiel ist die Festplatte C: auf dem Quellsystem 40 GB groß und so viel Speicher erwartet der Converter auch auf der Platte des Zielsystems. Wenn aber nur 20 GB belegt sind, brauchen Sie auf dem Zielsystem auch nur ca. 20 GB Speicher und die Meldung kann ignoriert werden.

Im letzten Schritt wird eine Zusammenfassung der Einstellungen angezeigt und die Konvertierung kann beginnen:

Summary

Review the conversion parameters

Warning: The size of the source disks may exceed the capacity of '\\TI1-1141\TMP_Convert'.

[Destination System](#)
[Options](#)
Summary

Source system information	
Source type:	Powered on machine
Name/IP address:	10.61.47.163
Connected as:	administrator
OS family:	Windows
CPU throttling:	None
Network throttling:	None

Destination system information	
Virtual machine name:	TI1-1142
Destination product:	VMware Workstation 11.x/12.x
Destination directory:	\\TI1-1141\TMP_Convert
Number of vCPUs:	2 (2 sockets * 1 cores)
Physical memory:	2GB
Network:	Preserve NIC count
NIC1:	Connected
	Bridged connection
Disk controller type:	SCSI LSI Logic SAS
Storage:	Volume-based cloning
Number of disks:	1
Create disk 0 as:	Not pre-allocated

Destination customization	
Install VMware Tools:	No
Customize guest OS:	No
Remove restore checkpoints:	Yes
Reconfigure virtual machine:	Yes

Abbildung 93 - VMware Converter - Zusammenfassung der gewählten Optionen

Ein neuer Task wird erzeugt und man kann den Fortschritt prüfen:

Task ID	Job ID	Source	Destination	Status	Start time	End time
1	1	10.61.47.163 [...]	...\\TI1-1142.vmx	1%	6/29/18 4:14 PM	Estimated time remaining: 1 hours and 3 minutes

Abbildung 94 - VMware Converter - Statusüberwachung der Konvertierung

Nachdem der Task erfolgreich abgeschlossen wurde, kann man die Migrierte VM in dem Zielordner finden:

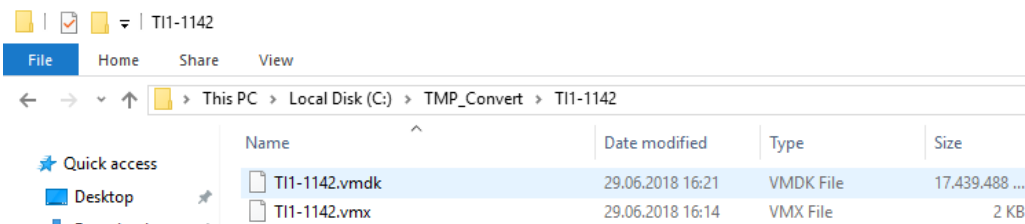


Abbildung 95 - VMware Converter - Pfad zum konvertiertem System

5.7.4 Verbinden & Migration einer entfernten VM – Linux

Als Ziel einer Linux VM Migration kann ausschließlich ein verwaltetes System genutzt werden – VMware vCenter oder ein ESXi Host sein – siehe https://www.vmware.com/pdf/convsa_61_guide.pdf#unique_32

Da in der dSecureCloud Umgebung kein Zugriff auf die Managementkomponenten vorhanden ist, kann diese Option nicht genutzt werden.

5.7.5 Nützliche Links

Liste der benötigten Netzwerkports: <https://kb.vmware.com/s/article/1010056>

vCenter Converter Troubleshooting: <https://kb.vmware.com/s/article/1016330>

6 Business Management

Die Benutzer, die den Rollen „Business Group Manager“ und/oder „Support Role“ zugeordnet sind, haben die Berechtigungen, sich im Bereich „Business Management“ eine Kostenaufstellung anzeigen zu lassen und die Daten zu exportieren. Dies sind die Benutzer, die Bestellungen genehmigen können.

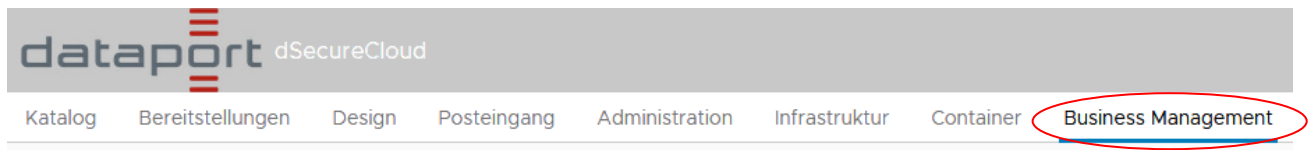


Abbildung 96 - Business Management Tab auf der Webportal Hauptseite

Auf der Startseite (Kostenaufstellung-Angaben) wird eine Übersicht über die für den aktuellen Monat aufgelaufenen Kosten, sowie ein prognostizierten Betrag für den gesamten Monat angezeigt. Die historische Kostenentwicklung lässt sich dort ebenfalls ablesen.

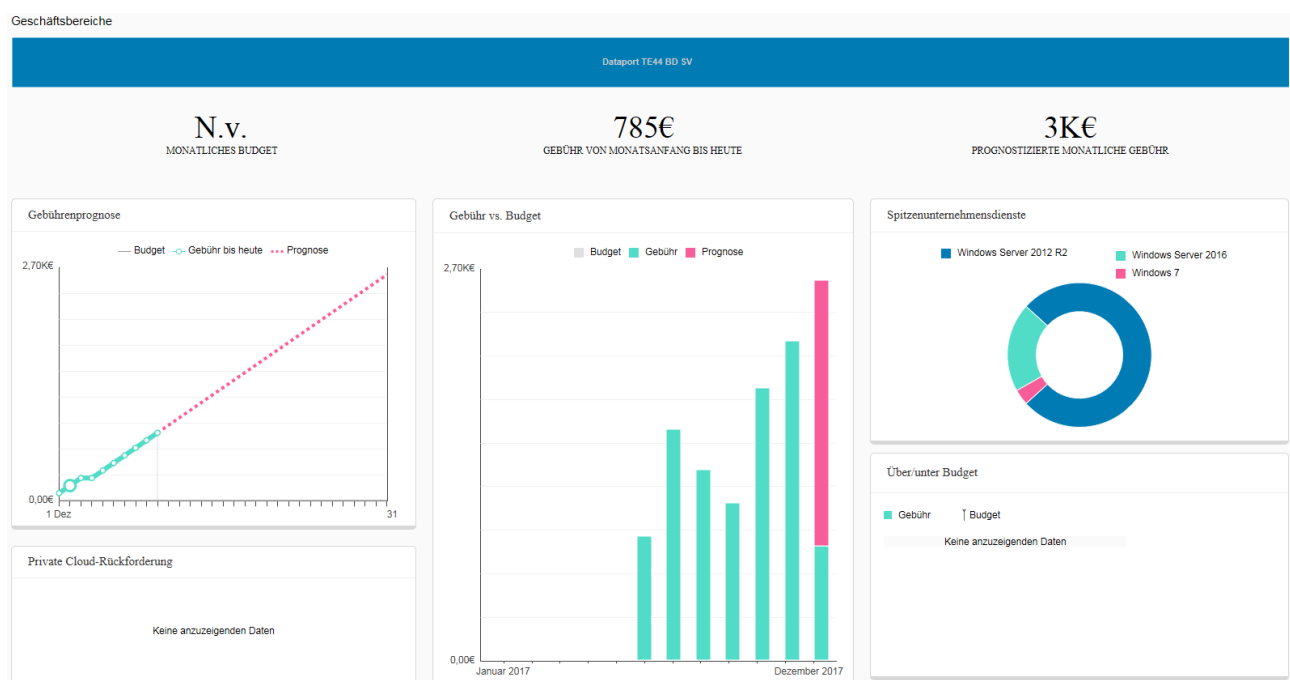


Abbildung 97 - Einsicht in die historische Kostenentwicklung

Über die Navigationsleiste am linken Rand lassen sich weitere detaillierte Berichte abrufen. Unter „Kostenaufstellung > Berichte > Virtuelle Maschinen“ findet man eine Aufstellung der Kosten je VM, aufgeschlüsselt auf die einzelnen Kostenblöcke für CPU, RAM, usw.

VM-Name	Monatl. Gesamtgebühr	VM-Details						
		Geschäftsbereich	Unternehmensdie	vCPUs	Konfigurierter RAM (GB)	Konfigurierter Speicher (GB)	Gelöscht	CPU-Gebühr
TE44BD-SV-0006	27,63€	Dataport TE4...	Windows 7	1,00	1,00GB	32,00GB	Nein	7,02€
TE44BD-SV-0013	66,06€	Dataport TE4...	Windows Ser...	4,00	8,00GB	62,00GB	Nein	28,09€
TE44BD-SV-0002	59,22€	Dataport TE4...	Windows Ser...	2,00	4,00GB	140,00GB	Nein	14,04€
TE44BD-SV-0018	109,26€	Dataport TE4...	Windows Ser...	4,00	8,00GB	302,00GB	Nein	28,09€
TE44BD-SV-0004	36,36€	Dataport TE4...	Windows Ser...	2,00	2,00GB	32,00GB	Nein	14,04€
TE44BD-SV-0022	50,76€	Dataport TE4...	Windows Ser...	1,00	4,00GB	132,00GB	Nein	7,02€
TE44BD-SV-0024	50,76€	Dataport TE4...	Windows Ser...	1,00	4,00GB	132,00GB	Nein	7,02€
TE44BD-SV-0023	40,05€	Dataport TE4...	Windows Ser...	1,00	3,00GB	82,00GB	Nein	7,02€
TE44BD-SV-0003	78,45€	Dataport TE4...	Windows Ser...	4,00	5,99GB	150,00GB	Nein	28,09€
TE44BD-SV-0001	56,07€	Dataport TE4...	Windows Ser...	2,00	3,00GB	132,00GB	Nein	14,04€
TE44BD-SV-0015	78,3€	Dataport TE4...	Windows Ser...	4,00	8,00GB	130,00GB	Nein	28,09€
TE44BD-SV-0016	78,3€	Dataport TE4...	Windows Ser...	4,00	8,00GB	130,00GB	Nein	28,09€
TE44BD-SV-0005	53,82€	Dataport TE4...	Windows Ser...	2,00	4,00GB	110,00GB	Nein	14,04€

Abbildung 98 - Bericht: Kostenauflistung

Die Daten lassen sich dort über die Punkte „Exportieren“ und „Täglicher Preisbericht“ in eine Excel-Datei exportieren.

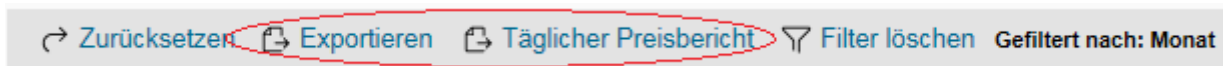


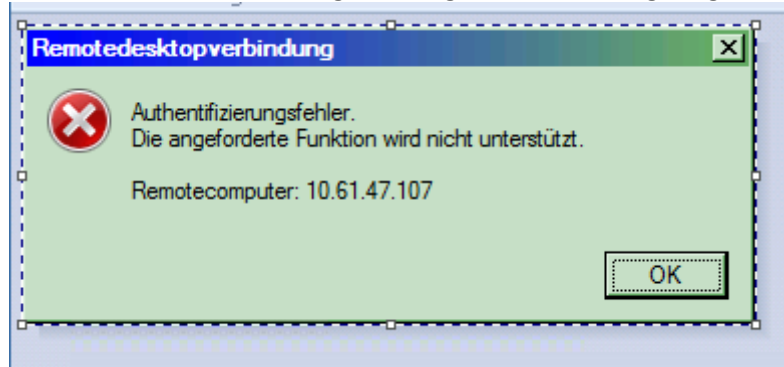
Abbildung 99 - Exportieren eines Berichts

Unter „Kostenauflistung > Berichte > Benutzerdefinierte Berichte“ findet sich der Bericht „Kosten pro Monat“, über den sich die detaillierten Kosten je VM für die vorherigen Monate anzeigen und exportieren lassen.

7 FAQ – häufig gestellt Fragen

7.1 Eine RDP Verbindung schlägt fehl mit Fehler "Die angeforderte Funktion wird nicht unterstützt."

Beim Aufruf der Verbindung wird folgender Fehler angezeigt:



Dieser tritt auf, wenn die Patchversionen des Clients und des Servers nicht kompatibel sind. Beide Seiten müssen auf aktuellen Patchstand gebracht werden, siehe auch: <https://support.microsoft.com/de-de/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018>

7.2 Die Login-Seite des Portals wird nicht angezeigt. Sie geraten stattdessen auf die URL Idclopa013.dpaor.de und folgender Fehler wird angezeigt: Kein Zugriff auf Seite

Kein Zugriff auf Seite

- Vergewissern Sie sich, dass die Webadresse <https://dclopa013.dpaor.de> stimmt.
- [Diese Website auf Bing suchen](#)
- [Seite aktualisieren](#)

▼ Weitere Informationen

Verbindungsprobleme beheben

Test: Rufen sie eine private Session in ihrem Browser auf, mit der Tastenkombination Strg + Shift + P oder über das Browser-Menü und versuche Sie erneut die URL des Portals aufzurufen:



Wenn der Test erfolgreich ist, können Sie die private Session schließen und in ihrer standard-Session den Cache und Cookies entfernen. Daraufhin sollte der Zugriff auf das Portal wieder funktionieren.

Der Fehler kann vermieden werden, indem bei der Domänenauswahl darauf geachtet wird, dass die korrekte Domäne ausgewählt wird, wie z.B. hier:



Ihre Domäne auswählen

fhhnet.stadt.hamburg.de

 Diese Einstellung merken

Weiter

Sollten Sie eine andere Domäne auswählen und den Haken bei „Diese Einstellung merken“ wird der Browser permanent auf die inkorrekte URL umleiten.

7.3 RAM-Erweiterung eines Linux Systems schlägt fehl

Symptom: Eine RAM-Erweiterung auf mehr als 3GB RAM bei einem Linux System, wo bisher weniger als 3 GB RAM zugewiesen waren, schlägt fehl.

Lösung: Die Erweiterung muss offline stattfinden. Beim Aufrufen einer neuen Aktion zum Neukonfigurieren der VM muss die Option fürs Runterfahren der VM gewählt werden.

7.4 Routing interner und externer Netzwerkadapter

Bei VMs mit einem internen und externen Netzwerkadapter muss das Default-Gateway das des externen Adapters sein. Die Kommunikation zu lokalen Netzen (z.B. 10.0.0.0/8) muss über das Gateway des internen Adapters erfolgen.

Beispiel für Ubuntu16:

/etc/network/interfaces

```
Terminal - [Datei Bearbeiten Ansicht Terminal Reiter Hilfe]
iface lo inet loopback
auto lo

auto ens33 Extern
iface ens33 inet static
address 141.91.163.202
netmask 255.255.255.192
gateway 141.91.163.193

auto ens160 Intern
iface ens160 inet static
address 10.61.47.146
netmask 255.255.255.0
up route add -net 10.0.0.0 netmask 255.0.0.0 gw 10.61.47.1
dns-nameservers 10.61.16.6

interfaces (END)
```

Routingtabelle:

```
Terminal - [Title Bar]
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
:~# route -v
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 141.91.163.193 0.0.0.0 UG 0 0 0 ens33
10.0.0.0 10.61.47.1 255.0.0.0 UG 0 0 0 ens160
localnet * 255.255.255.0 U 0 0 0 ens160
141.91.163.192 * 255.255.255.192 U 0 0 0 ens33
link-local * 255.255.0.0 U 1000 0 0 ens33
```

7.5 Bereitstellung oder Neukonfiguration schlägt fehl mit Meldung: Delegated token must be instance of class com.vmware.vcac.authentication.http.spring.oauth2.OAuth2Token: null

Nachdem eine Bereitstellung oder Neukonfiguration eines Systems genehmigt wurde, schlägt der Vorgang fehl und folgende Meldung wird angezeigt:

#7219 - Provision Windows Server 2016 - Failed

Delegated token must be instance of class com.vmware.vcac.authentication.http.spring.oauth2.OAuth2Token: null

Grund dafür ist das Ablaufende der maximalen zulässigen Zeit von 7 Tagen, während welcher die Genehmigung erteilt werden soll; wenn die Genehmigung nach als 7 Tagen nach dem Einreichen eines Auftrags erteilt wird, wird der oben genannte Fehler ausgelöst und der Auftrag muss erneut eingereicht werden.

8 Ergänzende Dokumentation

- Offizielle Dokumentation:

<https://docs.vmware.com/en/vRealize-Automation/index.html>

- API Dokumentation:

<https://vdc-download.vmware.com/vmwb-repository/dcr-public/3f9ab622-499d-4caf-801b-2a6c1f83a6d4/ba2d7e2c-3320-4dfb-9ef0-39588cadda2e/vrealize-automation-75-programming-guide.pdf>

9 Änderungsverzeichnis

Version	Änderungsdatum	Erläuterung der Änderung	Autor/in
0.0.1	09.04.2014	Initialversion	
0.0.2	06.05.2014	Infos zu AV, Gliederung geändert	
0.0.3	10.06.2014	Infos zur Freischaltungsbeauftragung hinzugefügt	
0.0.4	31.07.2014	Inhalt aktualisiert, neue Screenshots	
0.0.5	06.08.2014	Infos zu Snapshots hinzugefügt	
0.0.6	09.10.2014	Infos zu Berechtigungen	
0.0.7	30.09.2015	Überarbeitung Freischaltung	
0.0.8	16.02.2016	Infos zum Installserver hinzugefügt.	
0.0.9	29.04.2016	Infos zu öffentlichen IPs und Freischaltungen eingetragen; generelle Überarbeitung der Anleitung	
0.0.10	03.06.2016	Info zur öffentlichen IP korrigiert	
1.0.0	16.06.2016	Finales Release der Anleitung	
1.0.1	22.06.2016	Ergänzt um Infos zur InternetZone als Quelle	
1.0.2	29.06.2016	Infos zur Internet Zone geändert – Freischaltung wird jetzt standardmäßig aktiviert	
1.0.3	02.12.2016	Infos zu neuen Firewall Service eingetragen, Abschn. 4.2.1-4.2.3 Repo Server für SLES11SP2 gelöscht, für SLES12 eingetragen	
1.0.4	13.12.2016	Infos zu neuen Firewall Service eingetragen, Abschn. 4.2.4-4.2.5 Text- und Screenshot Überarbeitung 4.21-4.25	
1.0.5	01.06.2017	Angepasst nach Migration in ondataport.de	
1.0.6	12.06.2017	Kap. 4 hinzugefügt	
1.0.7	23.06.2017	Info zum Zusammenhang zwischen Snapshot und HDD Erweiterung hinzugefügt	
1.0.8	14.07.2017	Schreibfehler korrigiert	
1.0.9	02.08.2017	Anleitung für Virenschutz überarbeitet Hinweis zum Ablauf der Firewall Freischaltung User Form hinzugefügt	
1.10	29.08.2017	Anleitung für Virenschutz korrigiert	
1.11	17.10.2017	5.2 Firewallfreischaltungen bearbeitet	
1.12	02.11.2017	Anpassung wegen neuen Template Versionen und Umzug in die servicedpaor.de	
1.13	11.12.2017	Abschnitt Business Management hinzugefügt	
1.14	05.07.2018	Neue Abschnitte: Firewall - Report über Regelverstöße, Kopieren einer VM aus dSecureCloud auf lokalen Speicher mit dem vCenter Converter, Wiederherstellen einer VM aus dem Backup; aktualisiert: 5.4 SLES – Installserver	
1.15	16.10.2018	Neue Version passend zum Release Upgrade, Kap. 1 aktualisiert	
1.16	18.10.2018	Weitere Abschnitte aktualisieret, bis Abschnitt 5.2; Abbild-Beschreibungen hinzugefügt bis 5.2	
1.17	25.10.2018	Weitere Screenshots aus vRA 7.5 hinzugefügt	
1.18	22.01.2019	Veröffentlichung nach Upgrade auf vRA 7.5	
1.19	06.02.2019	Überarbeitung des Kap. 5.4; Beschriftungen bei Screenshots eingefügt	
1.20	11.02.2019	div. Layout-Korrekturen	
1.21	22.03.2019	3.6 hinzugefügt	