bwCloud & bwIDM-Entitlements

Information zur Einführung von bwIDM-Entitlements für die Nutzung der bwCloud

Autoren:
Janne Chr. Schulz ① (Universität Mannheim)
Thomas Nau ② (Universität Ulm)

Version / Rev.: **20190710-a / 379**

Kontaktinformationen:

- **Projektleitung bwCloud (Janne Schulz)**
  janne.schulz@rz.uni-mannheim.de
- **Technische Hilfe**
  idp-help@bw-cloud.org
- **Webseite mit aktualisierten Informationen**
  https://bw-cloud.org/q/4cXv
- **bwIDM-Webseite mit technischen Informationen**
  https://www.bwidm.de/dienste/#bwcloudscope

① E-Mail: janne.schulz@rz.uni-mannheim.de
② E-Mail: thomas.nau@uni-ulm.de

Inhaltsverzeichnis

1 Zusammenfassung

Mittlerweile nutzen über 1.700 Nutzerinnen und Nutzer von über 34 verschiedenen Heimatstandorten die bwCloud. Die vier Regionen Mannheim, Freiburg, Karlsruhe und Ulm hosten insgesamt über 1.900 virtuelle Maschinen – Tendenz steigend![1] Mit Hilfe von bwCloud können nutzungsberechtigte Personen auf dem Wege der Selbstprovisionierung sehr zeitnah und ohne langwieriges Antragsverfahren virtuelle Maschinen zur Unterstützung bei der Erfüllung von Dienstaufgaben, für Forschung und Lehre betreiben.

Wer nutzungsberechtigt ist und wer nicht können die Heimatstandorte zukünftig selber entscheiden: **Ab** dem **1.10.2019** wird der Registrierungs- und Nutzungsprozess der bwCloud auf die Nutzung von bwIDM-Entitlements **umgestellt**. Nach dem 1.10.2019 gilt dann: wer nicht über wenigstens eines der beiden Entitlements *bwCloud-Basic* oder *bwCloud-Extended* verfügt kann die bwCloud nicht mehr weiter nutzen.

Mit der Umstellung auf die Auswertung von Entitlements werden mehrere Dinge geregelt:

1. Die Heimatstandorte der Nutzer können nun selber entscheiden wer Zugang zur bwCloud bekommt
2. Den Registrierungsprozess wird weiter automatisiert und erleichtert den Zugang zur bwCloud
3. Es werden die Voraussetzungen für eine zukünftige Leistungs- und Kostenverrechnung[2] geschaffen

Die bwCloud ist für den Einsatz der Entitlements vorbereitet. Das bedeutet: Sobald eine Heimateinrichtung die Entitlements einsetzt, werden die Nutzer_innen gemäß des auf Seite 5 beschriebenen Vorgehens in der bwCloud angelegt und provisioniert.

Dieses Dokument enthält Informationen zur geplanten Einführung und Umstellung von / auf Entitlements zur Steuerung und Organisation des Zugangs zum Landesdienst bwCloud.

1 Stand der Daten: 24.06.2019

2 Die Einführung der Entitlements findet nicht ausschließlich aufgrund einer zukünftigen Leistungs- und Kostenver-rechnung statt, ist aber ein wichtiger technischer Baustein zur Vorbereitung entsprechender Ab- und Verrechnungsmechanismen. Die notwendigen Dokumente für eine Leistungs- und Kostenverrechnung sind derzeit noch in der Ausarbeitung und gehen den teilnehmenden Universitäten und Hochschulen zeitnah zu. Derzeit ist die Einführung der Verrechnung für 2020 geplant. (Stand: Juni 2019)

2 Wieso wird auf bwIDM-Entitlements umgestellt?

Zukünftig wird der Zugang zur Nutzung der bwCloud auf Basis einer persönlichen Nutzungsberechtigung – dem Entitlement welches durch die Heimateinrichtung vergeben wird - gesteuert.

Es wird zwischen **zwei** verschiedenen Entitlements unterschieden:

- *bwCloud-Basic* und
- *bwCloud-Extended*

2.1 Was mit den Entitlements geregelt wird

Die Heimatstandorte entscheiden selbständig wer Zugang zur bwCloud bekommt

Auf der bwCloud Seite gilt ab dem 1.10.2019:

Keine Freigabe durch die Heimateinrichtung mittels Entitlement = Kein Zugang zur bwCloud

Mit den Entitlements wird geregelt, wie viele Ressourcen ein Nutzer nutzen darf

Grundlage für Unterscheidung bildet die Flavortabelle (siehe „3 - Die aktuelle Flavortabelle“):

1. Nutzer, die ausschließlich über das Entitlement *bwCloud-Basic* verfügen, können eine Instanz entweder von "nano" oder "tiny" starten. Das ist quasi ein "Schnupperzugang" und richtet sich hauptsächlich an Studierende. Instanzen von diesem Flavor sind kostenfrei.
2. Nutzer die über das Entitlement *bwCloud-Extended* verfügen bekommen deutlich mehr Quota eingerichtet und können damit alle angebotenen Flavors nutzen. Für die Nutzung der bwCloud fallen perspektivisch Kosten an.

Basierend auf den Entitlements wird unterschiedlich mit den Instanzen umgegangen

Das Entitlement *bwCloud-Basic* richtet sich hauptsächlich an Studierende, die die bwCloud für diverse Zwecke wie beispielsweise Abschlussarbeiten oder als Software-Repositorium nutzen möchten. Da es eine große Anzahl Studierender in Baden-Württemberg gibt, erwarten wir eine entsprechend große Anzahl kleiner VMs.

Gleichzeitig gehen wir davon aus, dass diese VMs bei Wegfall des ursprüngliches Zwecks nicht immer unmittelbar gelöscht werden. Es werden daher alle VMs, die von Nutzern mit *bwCloud-Basic* gestartet wurden, regelmäßig gelöscht[3]. Einmal um die Systeme aufzuräumen und um anderen um neuen Nutzern die Chance zu geben, auch eine Instanz zu starten. Das Entitlement *bwCloud-Basic* ist nicht dazu gedacht, einen (System-) Dienst dauerhaft zu betreiben.

Bei *bwCloud-Extended* gibt es diese Einschränkungen dagegen nicht. Hier gilt: die VMs laufen so lange bis sie von den Nutzern selbständig gelöscht werden.

Die Entitlements zeigen an wer die virtuellen Maschinen bezahlen kann

Um den nachhaltigen Betrieb der bwCloud und einen regelmäßigen Austausch der Hard- und Software sicherstellen zu können ist eine Verrechnung der in Anspruch genommen Leistungen notwendig. Wir möchten ein Leistungs- und Kostenverrechnungsmodell einführen mit dessen Einnahmen die Hardwareinfrastruktur regelmäßig erneuert und den

3 Wir planen in einem halbjährlichen Rhythmus die „nano“ und „tiny“ Instanzen zu löschen, Stichtage hierzu sind der 31.3. und der 30.9. des jeweiligen Kalenderjahres.

Bedarfen anpasst werden soll. Um Einzelabrechnungen mit den Nutzern zu vermeiden wird es für die Heimatstandorte der Nutzer „Sammelübersichten und -rechnungen“ geben, da nur sie ihre Nutzer kennen und wissen, wer über entsprechende Mittel für den Betrieb von VMs verfügt.

Mit der Vergabe des Entitlements *bwCloud-Extended* für einen Nutzer signalisiert der jeweilige Heimatstandort, dass der Nutzer Zugriff auf ein Konto mit entsprechenden Mitteln hat. Wie die Kosten dann am Heimatstandort intern umgelegt werden ist Sache des jeweiligen Standortes und kann individuell und nach den lokalen Prinzipien organisiert werden.

Durch die Förderung des Ministeriums für Wissenschaft, Forschung und Kunst (MWK) bleiben Ressourcen, die mit dem Entitlement *bwCloud-Basic* betrieben werden, kostenfrei.

Beschleunigung des Registrierungsprozess

Durch die automatisierte Auswertung der Entitlements im Verlauf der Registrierung für den Service bekommen die Nutzer unmittelbar Rückmeldung, wenn die Einrichtung des Accounts in der bwCloud durchgeführt wurde. Es ist keine manuelle Interaktion mehr von unserer Seite aus notwendig, die Nutzer kommen innerhalb weniger Minuten in die bwCloud und niemand muss mehr per Hand freigeschaltet werden.

3 Die aktuelle Flavortabelle

Virtuelle Maschinen verfügen über unterschiedliche Ressourcen wie „Anzahl der Rechenkerne“ oder „Größe des verfügbaren Hauptspeichers“. Eine spezifische Konfiguration wird als „Flavor“ bezeichnet. Die unterschiedlichen Konfigurationen sind in der folgenden „Flavortabelle“ aufgelistet.

Flavor	Ressourcenumfang			
	Anzahl vCPUs	Größe Rootdisk[4]	Größe RAM[5]	Gesamtgröße Festplattenspeicher[6]
m1.nano	1	12	0,5	50
m1.tiny	1	12	1	
m1.small	1	12	2	128
m1.medium	2	12	4	
m1.large	4	12	8	
m1.xlarge	8	12	16	
m1.xxlarge	16	12	32	

Stand: 21.06.2019

Dem Entitlement *bwCloud-Basic* (grüne Hintergrundfarbe) werden die Flavors „m1.nano“ und „m1.tiny“ zugeordnet. Alle anderen Flavors sind dem Entitlement *bwCloud-Extended* zugeordnet.

4 In GByte

5 In GByte

6 In GByte. Die Gesamtgröße bezeichnet das intial insgesamt zur Verfügung stehende „Volume Quota“ was jedem Nutze basierend auf dem verknüpften Entitlement eingerichtet wird. Dieses Volume Quota kann auf beliebig viele unterschiedlich große Volumes (= „Festplatten“) aufgeteilt werden und ist unabhängig von der Anzahl der laufenden Instanzen oder deren Flavors.

4 Der Registrierungsprozess

Unabhängig ob für das Entitlement *bwCloud-Basic* oder *bwCloud-Extended*, die ersten fünf Schritte sind immer gleich:

1. Falls noch nicht geschehen: eines der beiden Entitlements zum eigenen Account durch den Heimatstandort hinzufügen
2. Registrieren für die Nutzung der bwCloud
3. Warten bis die E-Mail zur erfolgreichen Einrichtung vorliegt
4. Dienstpasswort für den Login sezten
5. Die bwCloud nutzen

4.1 Der Registrierungsprozess zu bwCloud-Basic

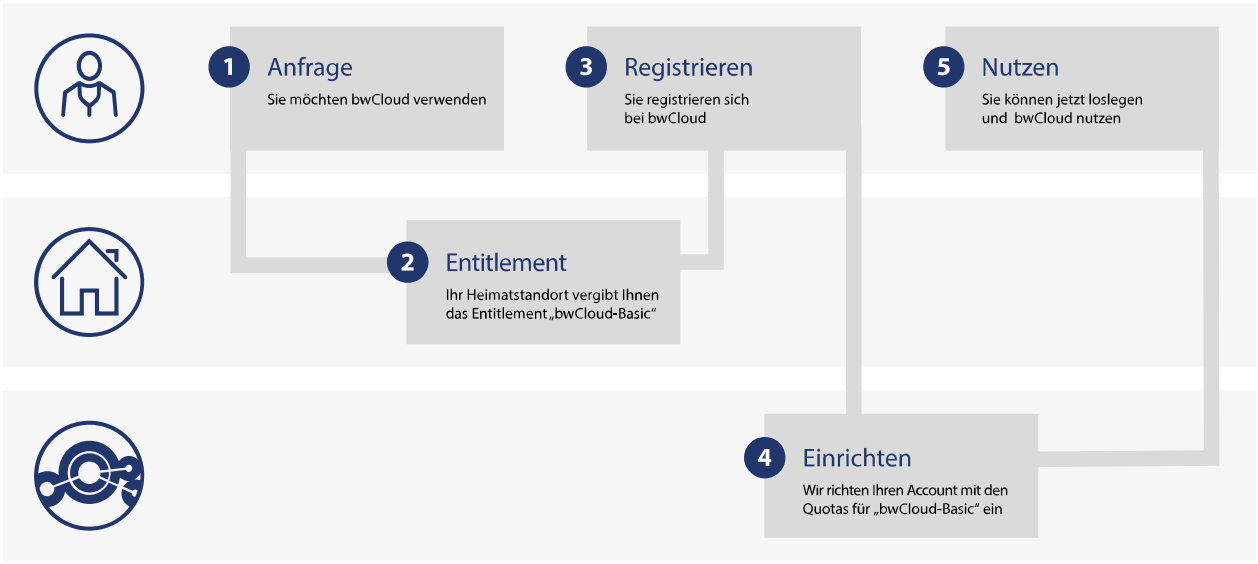

Illustration 1: Schematische Darstellung des Registrierungsprozess zum Entitlement bwCloud-Basic (oberer Balken = Nutzer_in, mittlerer Balken = Heimatstandort des/der Nutzer_in, unterer Balken = bwCloud)

4.2 Der Registrierungsprozess zu bwCloud-Extended

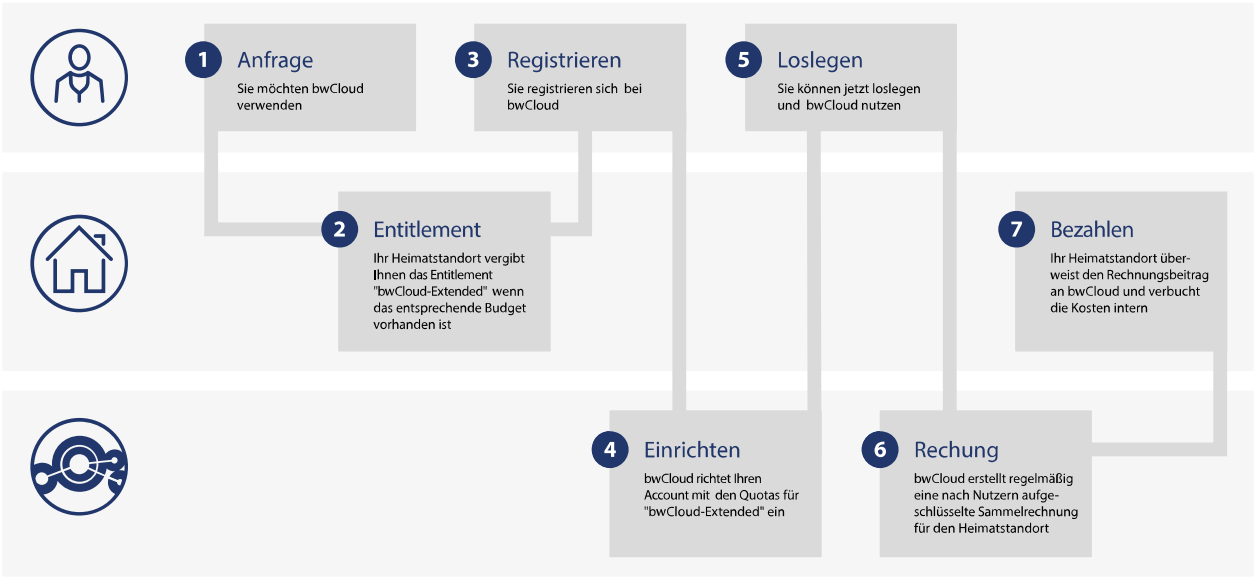

Illustration 2: Schematische Darstellung des Registrierungsprozess zum Entitlement bwCloud-Extended (oberer Balken = Nutzer_in, mittlerer Balken = Heimatstandort des/der Nutzer_in, unterer Balken = bwCloud)

1. Sollte eine Heimateinrichtung **nicht** an das **bwIDM angeschlossen** sein oder keines der Entitlements *bwCloud-Basic* oder *bwCloud-Extended* vergeben, kann **kein Angehöriger** dieser Heimateinrichtung den Landesdienst bwCloud nach dem 01.10.2019 **nutzen**.

2. Sind einem Nutzer **beide Entitlements** zugeordnet, so werden ihm die Berechtigungen für das **höherwertige Entitlement** (in diesem Fall die Quota-Einstellungen für *bwCloud-Extended*) **eingerichtet**

5 Initialer Ressourcenumfang der Entitlements

Folgende Ressourcen werden bei der Registrierung eines neuen Nutzers abhängig von dem übermittelten Entitlement eingerichtet:

5.1 Entitlement bwCloud-Basic

Anzahl Instanzen	1
Anzahl vCores	1
Hauptspeicher	1.024 MByte
Anzahl Volumes	4
Gesamtgröße Festplattenspeicher[7]	50 GByte

7 In GByte. Die Gesamtgröße bezeichnet das intial insgesamt zur Verfügung stehende „Volume Quota“ was jedem Nutze basierend auf dem verknüpften Entitlement eingerichtet wird. Dieses Volume Quota kann auf beliebig viele unterschiedlich große Volumes (= „Festplatten“) aufgeteilt werden und ist unabhängig von der Anzahl der laufenden Instanzen oder deren Flavors.

Anzahl Snapshots	4
Gesamtgröße Snapshots	50 GByte
Anzahl Netzwerke (= IP Adressen)	1

Stand: 05.03.2019

5.2 Entitlement bwCloud-Extended

Anzahl Instanzen	8
Anzahl vCores	16
Hauptspeicher	16.384 MByte
Anzahl Volumes	16
Gesamtgröße Festplattenspeicher[8]	128 GByte
Anzahl Snapshots	16
Gesamtgröße Snapshots	128 GByte
Anzahl Netzwerke (= IP Adressen)	2
Anzahl Subnetze	mind. 2

Stand: 05.03.2019

6 Zeitplan und Umsetzung

6.1 Technische Vorbereitung der bwCloud: abgeschlossen

Die bwCloud ist technisch und organisatorisch seit Q1 2019 in der Lage, die Entitlements auszuwerten und die entsprechenden Quotaeinstellungen bei der Einrichtung der Nutzer zuzuordnen.

6.2 Registrierung neuer Nutzer

Die vollständige Umstellung des Registrierungsprozesses für die Nutzung von bwCloud ist für den

1. Oktober 2019 (01.10.2019)

geplant. Ab diesem Zeitpunkt werden **keine neuen Nutzer**, die **nicht** wenigstens über eines der beiden **Entitlements verfügen**, für die Nutzung der bwCloud **freigeschaltet**.

8 In GByte. Die Gesamtgröße bezeichnet das intial insgesamt zur Verfügung stehende „Volume Quota“ was jedem Nutze basierend auf dem verknüpften Entitlement eingerichtet wird. Dieses Volume Quota kann auf beliebig viele unterschiedlich große Volumes (= „Festplatten“) aufgeteilt werden und ist unabhängig von der Anzahl der laufenden Instanzen oder deren Flavors.

6.3 Überprüfung bestehender Nutzer

6.3.1 Automatische Prüfung vor Einführung (ab dem 01.09.2019)

Ab dem 1. September 2019 (01.09.2019) werden alle bereits registrierten Nutzer automatisch bei den IdPs ihrer Heimateinrichtung auf die Existenz der / des Entitlements geprüft. Sollte diese Prüfung ergeben, dass kein Entitlement vorhanden ist oder das Ressourcen genutzt werden, für die das Entitlement *bwCloud-Extended* benötigt wird, dieses aber nicht mit dem Account verknüpft ist, wird der Nutzer darüber via E-Mail an die bei uns hinterlegte Adresse benachrichtigt.

6.3.2 Automatische Prüfung nach Einführung (ab dem 01.10.2019)

Ergibt die automatische Prüfung bereits registrierter Accounts nach dem 1. Oktober 2019, dass keines der beiden Entitlements mit dem Account verknüpft ist oder dass Ressourcen verwendet werden, die das Entitlement *bwCloud-Extended* voraussetzen und dieses nicht vorhanden ist, dann werden alle Ressourcen gestoppt und der Nutzer darüber per E-Mail informiert.

7 Technische Details

Die technischen Details können auch auf der zentralen bwIDM-Website[9] unter

https://www.bwidm.de/dienste/#bwcloudscope

nachgelesen werden. Im Zweifel oder bei unterschiedlichen Angaben gelten die Angaben auf der zentralen bwIDM-Website!

Notwendige Attribute	`sn`
	`mail`
	`givenName`
	`bwidmOrgid`
	`eduPersonEntitlement`
	`eduPersonPrincipalName`
	`eduPersonScopedAffiliation`
Belegung für eduPersonEntitlement	`http://bwidm.de/entitlement/bwCloud-Basic`
	`http://bwidm.de/entitlement/bwCloud-Extended`
entityIds	`https://bwservices.uni-freiburg.de/sp (bwCloud SCOPE)`

9 Siehe auch https://www.bwidm.de/dienste (Zuletzt abgerufen: 25.06.2019)

8 Kontakt und Hilfe

Für Fragen zur Umstellung der lokalen IdP-Systeme haben wir die E-Mail Adresse

idp-help@bw-cloud.org

eingerichtet. Sie ist eine Weiterleitung an unsere interne Administrations-Mailingliste, so dass Fragen an alle Administratoren weitergeleitet und von diesen beantwortet werden können.

Auf der Spezialseite

https://bw-cloud.org/q/4cXv

werden wir aktualisierte Informationen bereitstellen, beispielsweise eine „Frage – Antwort“ Sektion mit häufig auftretenden Fragestellungen und deren Lösungen.

Auf der bwIDM-Webseite

https://www.bwidm.de/dienste/#bwcloudscope

sind weitere technische Informationen zu dem Landesdienst verfügbar.