Baden-Württemberg Support Portal for:

bwUniCluster bwDataArchive
bwForCluster bwSync&Share
bwCloud

Home Submit ticket Support staff Contact Logout

Information Ticket-ID: 12505

Submitter:	**Alexander Krug**	Date of issue:	2023-03-06 13:32:22	Origin SG:	bwsupportPortal
E-Mail:	wi21141@lehre.dhbw-stuttgart.de	Priority:	urgent	Responsible unit:	**bwCloud Mannheim**
User notification:	on Every Change			Status:	**verified**

Description:

IP/Domain blocking und Probleme mit IPv6

Detailed Description:

Guten Tag,

Im Rahmen eines Gruppenprojektes haben wir folgende Probleme:

1. CURL auf github.com ist nicht ausführbar, konkret: https:/github.com/docker/compose/releases/download/1.23.2/docker-compose-Linux-x86_64. Wir haben das umgangen, indem wir die binary local gedownloadet und per Ansible verteilt haben, aber trotzdem wäre es interessant zu wissen, ob generell curls auf GitHub geblockt werden?

2. Das Aufsetzen von express-gateway geht nicht, da die Adresse „https://registry.npmjs.org/express-gateway“ nicht erreichbar ist. Ping auf die Adresse ergibt „Network is unreachable“. Wird diese Adresse geblockt? Kann sie entlockt werden? Ohne sie können wir den API Gateway nicht aufsetzen, den wir im Serververbund brauchen. Gerne kann ich die 2 Server nennen auf denen die Freischaltung notwendig ist.

3. Das DHBW Stuttgart Netz (und andere Netze) können keine IPv6 Adressen auflösen, ich muss daher von Zuhause oder vom mobilen Hotspot zugreifen. Ist geplant, zukünftig auch IPv4 Adressen zu vergeben oder ist dies aufgrund mangelnder Adressen nicht möglich?

Vielen Dank schon im Voraus für Ihre Rückmeldung.

Mit besten Grüßen
Alexander Krug

Solution:

Sehr geehrte Damen und Herren,

Die bwCloud hat keine IPv4 Adressen für externe Mitarbeiter mehr, das betroffene Netz ist das public-belwue. Das wird sich frühestens 1 Monat nach dem Wartungstag, am 30.4.23 entspannen. Bitte nutzt das public-belwue-v6only, das ist NICHT von Openstack supported, es ist kein Dualstack Netz. DNS Fehler sind möglich. Bei Verbindungsfehlern keine Tickets aufmachen, sondern erst Konfiguration anpassen, z.B. die IPv6 DNS Server (z.B. BelWue(https://support.belwue.de/anleitungen/dns/): 2001:7c0::53:1) in der /etc/resolve.conf nachtragen oder den Zielserver in der /etc/hosts.

mit freundlichen Grüßen
Hr. Schwarz

✔ This solution has been verified by the submitter

[Refresh page] [Top] [History]

History Ticket-ID: 12505

Date	Time (UTC)	Action taken/comments
Collapse/expand old history entries ?		
2023-03-06	13:32	assigned (bwsupportPortal First Level Support)
2023-03-06	14:09	Public diary: Hallo Herr Krug, Auf welcher Infrastruktur haben Sie diese Probleme? bwUniCluster, bwCloud,....? Danke. Günter 1st Line Support
2023-03-06	14:09	waiting for reply (bwsupportPortal First Level Support)
2023-03-06	16:04	Public diary: Guten Tag, es geht um ein Projekt in der bwCloud. Projektbesitzer: Alexander, KRUG, User-ID: 28112d7f758a440ca3e992540d095df8e Projektname: WWI2021A Kanban Bitte entschuldigen Sie, diese Infos hatte ich in der Anfrage initial vergessen. Gruß Alexander Krug

2023-03-06 16:04 in progress (bwsupportPortal First Level Support)

2023-03-07 08:06 assigned (bwCloud)

2023-03-07 08:27 Internal diary: *hidden*

2023-03-07 08:27 assigned (bwCloud Mannheim)

2023-03-09 09:37 Public diary: Sehr geehrter Herr Krug,

1. curl muss man mit -6 aufrufen.

2. Er sollte erreichbar sein:
host registry.npmjs.org
registry.npmjs.org has address 104.16.26.35
registry.npmjs.org has address 104.16.20.35
registry.npmjs.org has address 104.16.27.35
registry.npmjs.org has address 104.16.18.35
registry.npmjs.org has address 104.16.21.35
registry.npmjs.org has address 104.16.22.35
registry.npmjs.org has address 104.16.19.35
registry.npmjs.org has address 104.16.23.35
registry.npmjs.org has address 104.16.25.35
registry.npmjs.org has address 104.16.16.35
registry.npmjs.org has address 104.16.24.35
registry.npmjs.org has address 104.16.17.35
registry.npmjs.org has IPv6 address 2606:4700::6810:1323
registry.npmjs.org has IPv6 address 2606:4700::6810:1223
registry.npmjs.org has IPv6 address 2606:4700::6810:1923
registry.npmjs.org has IPv6 address 2606:4700::6810:1823
registry.npmjs.org has IPv6 address 2606:4700::6810:1423
registry.npmjs.org has IPv6 address 2606:4700::6810:1023
registry.npmjs.org has IPv6 address 2606:4700::6810:1723
registry.npmjs.org has IPv6 address 2606:4700::6810:1623
registry.npmjs.org has IPv6 address 2606:4700::6810:1123
registry.npmjs.org has IPv6 address 2606:4700::6810:1a23
registry.npmjs.org has IPv6 address 2606:4700::6810:1b23
registry.npmjs.org has IPv6 address 2606:4700::6810:1523

Allgemein:
Die Netzwerker der Uni Mannheim blocken seit 21.10.20 Ports und weitere https://unitwikis.uni-mannheim.de/xwiki/bin/view/UNIT-intern/Architekturen%20%26%20L%C3%B6sungen/MannhAttaN/Zentrale%20Filter/ aus Sicherheitsgründen auf Hardware - Switchebene (Cisco ACLs / andere HWFW), eine Freigabe ist nicht möglich. Bitte stellen Sie keine Freigabeanfragen, bzgl. bwCloud Netze

mit freundlichen Grüßen
Hr. Schwarz

https://unitwikis.uni-mannheim.de/xwiki/bin/view/UNIT-intern/Architekturen%20%26%20L%C3%B6sungen/MannhAttaN/Zentrale%20Filter/

Auszug:
Zentrale Filter
Zuletzt geändert von Gerd Rohde am 2022/08/05 16:04
Zentrale Filter der Universität Mannheim
Bearbeiten

Um einen gewissen Grundschutz im Netz der Uni Mannheim zu gewährleisten, sind seit Oktober 1999 an den Grenzen des Uni-Netzes zum BelWü bestimmte Anwendungen gesperrt. Dies soll allerdings keine zentrale Firewall der Uni darstellen, sondern nach dem "Zwiebelschalenprinzip" den gröbsten Unfug an den Außengrenzen der Uni Mannheim herausfiltern. An den Außengrenzen des BelWü sind ebenfalls Filter installiert. Bei Bedarf können Ausnahmen zugelassen werden.

Im Bereich - (wellknown Ports) sind in Servernetzen folgende Ports offen:

Transport	Port	Protokoll	Beschreibung	offene Richtung
TCP (offen)	22	ssh	SSH-Server	beide
TCP (offen)	80	http	Web-Server	beide
TCP (offen)	443	https	Web-Server mit ssl	beide
TCP (offen)	465	smtps	SMTP mit ssl	beide
TCP (offen)	587	submission	Message Submission	beide
TCP (offen)	990	FTPs	ftp protocol, control, over TLS/SSL	beide
TCP (offen)	993	IMAPs	IMAP Mail über ssl	beide
TCP (offen)	995	POPs	POP Mail über ssl	beide

Im Bereich oberhalb 1023 sind folgende Ports gesperrt:

Transport	Port	Protokoll	Beschreibung	gesperrte Richtung
TCP	1433,1434	MS-SQL	MS-Office	von außen
TCP	1501	TSM	Backup	von außen
TCP	1900	SSDP	Service Discovery	von außen
UDP, TCP	2049	NFS	Filesystem	von außen
TCP	2967	Symantec	Symantec	von außen
UDP	3283	Apple	Apple Remote Desktop	von außen
TCP	3306	mysql	mysql	von außen
UDP, TCP	3389	RDP	Remote Desktop	von außen
UDP, TCP	4045	lockd	Filesystem	von außen
TCP	4369	EPMD	PortMapper	von außen
TCP	5000	UPnP	Universal Plug and Play	von außen
UDP	5353	mdns	Multicast DNS	von außen
TCP	5432	PostgreSQL	PostgreSQL	von außen
TCP	5985	WinRM	WinRM	von außen
TCP	8333	Bitcoin	Bitcoin Full Bode	von außen
TCP	8080	www-alt	Alternativer www Port	von außen
TCP	9075	nx-os	Cisco Nexus	von außen
UDP	11211	memcached		von außen
TCP	27017	MongoDB	MongoDB	von außen
UDP	32100	IoT	IoT	nach außen
UDP	32414	open-SSDP	Plex Media Servers	von außen

Folgen der Packet Firewall für die Benutzer:

Die wichtigste Auswirkung für die Nutzer ist, dass das Datennetz zuverlässiger und sicherer läuft. Hackerangriffe werden zu einem großen Teil schon an der Packet Firewall abgewehrt und gelangen nicht mehr auf den Campus und zu den Endsystemen. Wie wichtig dieser Schutz ist, erkennt man daran, dass Angriffsversuche inzwischen fast täglich stattfinden, wie stichprobenartige Kontrollen an der "Außenseite" der Packet Firewall zeigen.

Daneben gibt es aber eine Reihe von Einschränkungen, die es zu bedenken gilt: Sollen andere als die oben aufgeführten und generell frei geschalteten Dienste von außen erreichbar sein, muss dies muss der Universitäts-IT gemeldet werden. Der entsprechende Dienst wird dann auf der Packet Firewall freigeschaltet.

Es kann auch vorkommen, dass vermeintlich von Mannheim aus aufgebaute Verbindungen zu bestimmten Diensten nicht funktionieren. Das ist immer dann der Fall, wenn der außen liegende Server zur Erbringung des Dienstes eine Verbindung zurück nach Mannheim aufbauen will, was für den Anwender oft nicht einfach nachzuprüfen ist. Wenn daher festgestellt wird, dass ein Dienst nicht funktioniert, der funktionieren sollte, und der Rechner, auf dem dieser Dienst läuft, über das Internet erreichbar ist, sollte über den zuständigen Rechner-Administrator bzw. Sicherheitsbeauftragten des Instituts die Universitäts-IT benachrichtigt werden (netzproblem@uni-mannheim.de). Von dort erfolgt dann weitere Unterstützung und ggfs. die Freischaltung der notwendigen Dienste.

Die Meldungen zur Freischaltung weiterer Dienste können formlos, aber in schriftlicher Form und mit Briefkopf des jeweiligen Instituts, vom Rechner-Administrator bzw. Sicherheitsbeauftragten des Instituts bei der Universitäts-IT eingereicht werden. Sie sind an Joachim Nerz bzw. Gerd Rohde zu richten.

Resümee:

Die Packet Firewall hat sich bisher sehr gut bewährt. Trotzdem müssen zwei Dinge jedem Betreiber und Benutzer eines an das Netz angeschlossenen Rechners bewusst sein: die Packet Firewall schützt nur vor Angriffen, die außerhalb des Mannheimer Datennetzes gestartet werden und sie bietet nur einen teilweisen, keinen absoluten Schutz. Die Verantwortung dafür, den eigenen Rechner dem Stand der Technik entsprechend sicher zu konfigurieren und zu betreiben, verbleibt bei den Benutzern und den jeweiligen Systemverantwortlichen.

-----Ursprüngliche Nachricht-----
Von: Sdintern <sdintern-bounces@mailman.uni-mannheim.de> Im Auftrag von Joachim Nerz
Gesendet: Mittwoch, 21. Oktober 2020 11:11
An: sdintern@mailman.uni-mannheim.de
Betreff: [Sdintern] Change: Sperrung msql Postgresql und bitcoin von aussen

Am 2.11.2020 9:00 Uhr

Sperrung der Ports:

TCP 3086 mysql
TCP 5432 PostgreSQL
TCP 8333 Bitcoin

Für alle Server von ausserhalb der Uni-Mannheim.

von VPN IP Adressen sind die Ports weiterhin erreichbar.

Liste der offenen/gesperrten Ports für Server:

https://ncc.uni-mannheim.de/ZentraleFilter

Zentrale Filter der Uni-Mannheim

Um einen gewissen Grundschutz im Netz der Uni-Mannheim zu gewährleisten, sind seit Oktober 1999 an den Grenzen des Uni-Netzes zum BelWü bestimmte Anwendungen gesperrt. Dies soll allerdings keine Uni-Mannheim-zentrale Firewall darstellen sondern nach dem Zwiebelschalenprinzip den gröbsten Unfug an den Außengrenzen der Uni Mannheim herausfiltern. An den Außengrenzen des BelWü sind ebenfalls Filter installiert. Bei Bedarf können Ausnahmen zugelassen werden.
Im Bereich 1-1023 (wellknown Ports) sind in Servernetzen folgende Ports offen:

Transport	Port	Protokoll	Beschreibung	offene Richtung
TCP (offen)	22	ssh	SSH-Server	beide
TCP (offen)	80	http	Web-Server	beide
TCP (offen)	443	https	Web-Server mit ssl	beide
TCP (offen)	465	smtps	SMTP mit ssl	beide
TCP (offen)	587	submission	Message Submission	beide
TCP (offen)	990	FTPs	ftp protocol, control, over TLS/SSL	beide
TCP (offen)	993	IMAPs	IMAP Mail ueber ssl	beide
TCP (offen)	995	POPs	POP Mail ueber ssl	beide

Im Bereich oberhalb 1023 sind folgende Ports gesperrt:

Transport	Port	Protokoll	Beschreibung	gesperrte Richtung
TCP	1433	MS-SQL	MS-Office	von außen
TCP	1501	TSM	Backup	von außen
TCP	1900	SSDP	Service Discovery	von außen
UDP, TCP	2049	NFS	Filesystem	von außen
TCP	2967	Symantec	Symantec	von außen
UDP	3283	Apple	Apple Remote Desktop	von außen
TCP	3306	mysql	mysql	von außen
UDP, TCP	3389	RDP	Remote Desktop	von außen
UDP, TCP	4045	lockd	Filesystem	von außen
TCP	5000	UPnP	Universal Plug and Play	von außen
UDP	5353	mdns	Multicast DNS	von außen
TCP	5432	PostgreSQL	PostgreSQL	von außen
TCP	5985	WinRM	WinRM	von außen
TCP	8333	Bitcoin	Bitcoin Full Node	von außen
TCP	8080	www-alt	Alternativer www Port	von außen
TCP	27017	MongoDB	MongoDB	von außen
UDP	32100	IoT	IoT	nach außen

Folgen der Packet Firewall für die Benutzer:

Vorneweg die wichtigste Auswirkung für den Benutzer: das Datennetz läuft zuverlässiger und sicherer. Hackerangriffe werden zu einem großen Teil schon an der Packet Firewall abgewehrt und gelangen nicht mehr auf den Campus und zu den Endsystemen. Wie wichtig dieser Schutz ist, ersieht man daran, daß Angriffsversuche inzwischen fast täglich stattfinden, wie stichprobenartige Kontrollen an der "Außenseite" der Packet Firewall zeigen.

Daneben gibt es aber eine Reihe von Einschränkungen, die es zu bedenken gilt. Sollen andere als die oben aufgeführten und generell frei geschalteten Dienste von außen erreichbar sein, muß dies muss der Universitäts-IT gemeldet werden. Der entsprechende Dienst wird dann auf der Packet Firewall freigeschaltet.

Es kann auch vorkommen, daß vermeintlich von Mannheim aus aufgebaute Verbindungen zu bestimmten Diensten nicht funktionieren. Das ist immer dann der Fall, wenn der außen liegende Server zur Erbringung des Dienstes eine Verbindung zurück nach Mannheim aufbauen will, was für den Anwender oft nicht einfach nachzuprüfen ist. Wenn daher festgestellt wird, daß ein Dienst nicht funktioniert, der funktionieren sollte, und der Rechner, auf dem dieser Dienst läuft, über das Internet erreichbar ist, sollte über den zuständigen Rechner-Administrator bzw. Sicherheitsbeauftragten des Instituts die Universitäts-IT benachrichtigt werden (netzproblem@uni-mannheim.de). Von dort erfolgt dann weitere Unterstützung und ggfs. die Freischaltung der notwendigen Dienste.

Die Meldungen zur Freischaltung weiterer Dienste können formlos, aber in schriftlicher Form und mit Briefkopf des jeweiligen Instituts, vom Rechner-Administrator bzw. Sicherheitsbeauftragten des Instituts bei der Universitäts-IT eingereicht werden. Sie sind an Herrn Nerz bzw. Herrn Rohde zu richten.
Resümee:

Die Packet Firewall hat sich bisher sehr gut bewährt. Trotzdem müssen zwei Dinge jedem Betreiber und Benutzer eines an das Netz angeschlossenen

Rechners bewußt sein: die Packet Firewall schützt nur vor Angriffen, die außerhalb des Mannheimer Datennetzes gestartet werden, und sie bietet nur einen teilweisen, keinen absoluten Schutz. Die Verantwortung dafür, den eigenen Rechner dem Stand der Technik entsprechend sicher zu konfigurieren und zu betreiben, verbleibt bei den Benutzern und den jeweiligen Systemverantwortlichen.
Ansprechpartner:
IT Support
(itsupport@uni-mannheim.de

3. Das kann gut sein.

Starten Sie einfach ein Server im 4v Netz und verteilen Sie von dort, 3 sind noch frei. Geduldigen Sie sich bitte bis 4 Wochen nach der Wartung.

mit freundlichen Grüßen
Hr. Schwarz

2023-03-09 09:37 waiting for reply (bwCloud Mannheim)

2023-03-09 20:24 Public diary: Sehr geehrter Herr Schwarz,

danke für Ihre Rückmeldung, Sie haben mir den entscheidenden Input gegeben.

Zu 1.: Danke, ich hatte bei curl die Option zu IPv6 nicht bedacht.
Zu 2.: Ich habe das Problem jetzt über feste, manuelle Einträge in /etc/hosts gelöst.
Zu 3.: Danke für das Feedback, aktuell arbeiten unsere Teams mit Handy-Hotspots, wenn das Heimnetz kein IPv6 unterstützt.

Ich wünsche Ihnen noch eine schöne Restwoche.

Mit freundlichen Grüßen
Alexander Krug

2023-03-09 20:24 in progress (bwCloud Mannheim)

2023-03-10 15:17 Public diary: Sehr geehrte Damen und Herren,

Die bwCloud hat keine IPv4 Adressen für externe Mitarbeiter mehr, das betroffene Netz ist das public-belwue. Das wird sich frühestens 1 Monat nach dem Wartungstag, am 30.4.23 entspannen. Bitte nutzt das public-belwue-v6only, das ist NICHT von Openstack supported, es ist kein Dualstack Netz. DNS Fehler sind möglich. Bei Verbindungsfehlern keine Tickets aufmachen, sondern erst Konfiguration anpassen, z.B. die IPv6 DNS Server (z.B. BelWue(https://support.belwue.de/anleitungen/dns/): 2001:7c0::53:1) in der /etc/resolve.conf nachtragen oder den Zielserver in der /etc/hosts.

mit freundlichen Grüßen
Hr. Schwarz

2023-03-10 15:17 solved (bwCloud Mannheim)
Solution: Sehr geehrte Damen und Herren,

Die bwCloud hat keine IPv4 Adressen für externe Mitarbeiter mehr, das betroffene Netz ist das public-belwue. Das wird sich frühestens 1 Monat nach dem Wartungstag, am 30.4.23 entspannen. Bitte nutzt das public-belwue-v6only, das ist NICHT von Openstack supported, es ist kein Dualstack Netz. DNS Fehler sind möglich. Bei Verbindungsfehlern keine Tickets aufmachen, sondern erst Konfiguration anpassen, z.B. die IPv6 DNS Server (z.B. BelWue(https://support.belwue.de/anleitungen/dns/): 2001:7c0::53:1) in der /etc/resolve.conf nachtragen oder den Zielserver in der /etc/hosts.

mit freundlichen Grüßen
Hr. Schwarz

2023-03-10 18:16 verified (bwCloud Mannheim)

[Refresh page] [Top] [History]