

Liste der vom Joker.com Nameservice Unterstützten DNS-Einträge

Übersicht über die unterstützten DNS-Einträge und kurze Erklärungen. Der Eintrag erfolgt jeweils über Joker.com und den Menüpunkt "DNS" in der Domainliste.

Unterstützte Einträge	
URL Weiterleitung	Leitet Ihre Domain auf eine externe Website (URL) um. Bitte beachten Sie auch die Hinweise zur Nutzung der Web/URL-Weiterleitungsfunktion von Joker.com.
Email Weiterleitung	Erstellt E-Mail-Adressen für Ihre Domain. E-Mails werden an Ihr bestehendes externes Mailkonto weitergeleitet, siehe auch URL Weiterleitungen und E-Mail Weiterleitung
A	Verknüpft Ihre Domain oder Hosts innerhalb der Domain mit einer IPv4 -Adresse. Ermöglicht die Erstellung von z.B. "www.your-domain.com" als Verweis auf eine externe IP-Adresse.
DYNA	Teil des Dynamic DNS (DynDNS) Service - verbindet Ihre Domain oder Ihren Host mit der temporären IP-Adresse Ihres Providers. Die IP kann automatisch über Ihr Routergerät oder ein Client-Programm aktualisiert werden. Dynamic DNS (DynDNS) muss für Ihre Domain aktiviert sein.

MX	Legt fest, welcher E-Mail-Server für die Annahme von E-Mails für Ihre Domain zuständig ist. Weitere Details finden Sie hier: MX Eintrag .
AAAA	Verknüpft Ihre Domain oder Ihren Host innerhalb der Domain mit einer IPv6 -Adresse.
DYNAAAA	Teil des <i>Dynamic DNS (DynDNS) Service</i> - verbindet Ihre Domain oder Ihren Host mit der temporären IPv6 -Adresse Ihres Providers. Die IP kann automatisch über Ihr Routergerät oder ein Client-Programm aktualisiert werden. <i>Dynamic DNS (DynDNS)</i> muss für Ihre Domain aktiviert sein.
CNAME	Ordnet Ihren Domain- oder Hostnamen einem anderen Domain- oder Hostnamen zu. Dies ist eine einfache Möglichkeit, einen einzelnen Host mit einem A-Eintrag zu definieren (your-domain.com zeigt auf IP) und sodann Aliase für 'www.your-domain.com' und 'blog.your-domain.com' zu erstellen. Weitere Details finden Sie hier CNAME records .
ALIAS	Ähnlich CNAME, allerdings kann ALIAS auch auf die Domain selbst angewendet werden. ALIAS-Einträge sind nicht mit DNSSEC kompatibel.
DNAME	Ähnlich CNAME, allerdings verweist DNAME auf alle untergeordneten Hosts (Subdomains) eines Eintrages. Weitere Details finden Sie hier DNAME records .
SPF	<u>Sender Policy Framework</u> - wird verwendet, um E-Mail-Spoofing zu erkennen und SPAM zu verhindern. Es stehen mehrere kostenlose Online-SPF-Record-Generatoren zur Verfügung, z.B. hier .
TXT	Erstellt einen TXT-Datensatz, um die Implementierung spezifischer Aufgaben zu ermöglichen. Wird u.a. auch verwendet, um <u>Let's Encrypt SSL Zertifikate</u> zu erstellen. Weitere Details finden Sie hier TXT records .

SRV	Gibt den Standort der Server für ein bestimmtes Protokoll und eine bestimmte Domain an. Weitere Details finden Sie hier: SRV Eintrag .
NAPTR	Gibt eine auf regulären Ausdrücken basierende Umschreibungsregel an, die, wenn sie auf eine bestehende Zeichenkette angewendet wird, ein neues Domainlabel oder eine neue URI erzeugt. Weitere Details finden Sie hier: NAPTR Eintrag .
NS	ständigen Nameserver für eine Subdomain an und ist auf Top-Level nicht erlaubt. Weitere Details finden Sie hier: NS Eintrag .
CAA	Hier können Sie angeben, welche Zertifizierungsstelle (CA) SSL-Zertifikate für Ihre Domain oder Ihren Hostnamen ausstellen darf. Weitere Details finden Sie hier: CAA Eintrag .
TLSA	Erstellen eines TLSA-Eintrages für DANE zur Validierung von Zertifikaten. Weitere Details finden Sie hier: TLSA Eintrag .
SSHFP	Erstellen eines SSHFP-Eintrages zur Validierung von ssh Fingerprints. Weitere Details finden Sie hier: SSHFP Eintrag .
SMIMEA	Erstellen eines SMIMEA-Eintrages zur Absicherung von SMIME. Weitere Details finden Sie hier: SMIMEA Eintrag .
SVCB	Erstellen eines Verweises auf einen beliebigen Dienst. Weitere Details finden Sie hier: SVCB DNS Eintrag .
HTTPS	Erstellen eines Verweises auf einen HTTP Dienst. Weitere Details finden Sie hier: HTTPS DNS Eintrag .

Wie man SPF Einträge erstellt

SPF bedeutet "Sender Policy Framework" und kann verwendet werden, um die Fälschung von Absenderadressen in E-Mails zu verhindern. Es ist kein eigener Eintragstyp, sondern verwendet dafür **TXT-Einträge**.

Es sollte immer nur einen SPF-Eintrag für eine Domain geben, während die SPF-Policy durchaus mehrere verschiedene Regeln enthalten kann, die bei Bedarf auf mehrere TXT-Einträge aufgeteilt werden können.

Es gibt viele Online-Tools, die bei der Erstellung eines SPF-Eintrags für eine bestimmte Domain helfen, z. B. [dieses hier](#).

Wenn Ihre Joker.com-Domain beispielsweise "example.com" lautet und Sie E-Mails von Gmail zulassen möchten, müssen Sie einen DNS-Eintrag vom Typ "TXT" für Ihre Domain "example.com" erstellen und diese Zeile eingeben:

```
v=spf1 include:_spf.google.com ~all
```

Wenn Sie einen SPF-Eintrag für eine Joker.com-Domain verwenden und sicherstellen möchten, dass E-Mails von Joker.com an E-Mail-Adressen mit Ihrer Joker.com-Domain weitergeleitet werden, müssen Sie diese zusätzliche Regel in Ihre SPF-Richtlinie aufnehmen:

```
include:_spf.joker.com
```

insgesamt ergibt dies dann diesen SPF-Eintrag:

```
v=spf1 include:_spf.google.com include:_spf.joker.com ~all
```

Sie können mehr als einen TXT-Eintrag erstellen, um die SPF-Regeln aufzuteilen, dann sollten die Einträge alle mit `v=spf1` beginnen, um eine SPF-Richtlinie zu definieren, und jeder Eintrag muss einen anderen Namen haben, oder anders gesagt - für jeden eindeutigen Namen (einschließlich der Domain selbst) ist nur ein mit "`v=spf1`" beginnender Eintrag zulässig:

Richtig:

example.com	TXT "v=spf1 include:_spf.google.com ~all"
spf1.example.com	TXT "v=spf1 include:_spf.joker.com ~all"

Falsch:

example.com	TXT "v=spf1 include:_spf.google.com ~all"
example.com	TXT "v=spf1 include:_spf.joker.com ~all"

DNS PTR Einträge

Ein DNS-Pointer-Record (kurz PTR) liefert den Domainnamen, der mit einer IP-Adresse verknüpft ist.

Ein DNS-PTR-Record ist damit genau das Gegenteil des "A"-Records der die mit einem Domainnamen verbundene IP-Adresse liefert.

DNS-PTR-Einträge werden bei Reverse-DNS-Lookups verwendet. Wenn ein Benutzer versucht, einen Domainnamen in seinem Browser zu erreichen, wird ein DNS-Lookup durchgeführt, bei dem der Domainname mit der IP-Adresse abgeglichen wird.

Ein Reverse-DNS-Lookup ist das Gegenteil davon - es wird nach einem Domainnamen mit der angegebenen IP-Adresse gesucht.

Dies bedeutet auch: **PTR-Records können nicht über die Name-Server der Domain definiert werden, sondern müssen beim Provider der IP-Adresse beantragt werden**, falls dieser dies unterstützt.

Revision #9

Created 28 August 2023 10:11:01 by Admin

Updated 24 January 2025 09:50:45 by Administrator