

Tactical RMM

Tactical RMM ist ein Open-Source Tool zur Fernüberwachung und -verwaltung, das mit Django, Vue und Golang entwickelt wurde. Es verwendet einen in Golang geschriebenen Agenten und ist mit MeshCentral integriert.

- [Aktualisieren des RMM](#)
- [Aktualisieren des Let's Encrypt SSL-Zertifikat](#)

Aktualisieren des RMM

Server auf dem neuesten Stand halten

Sie sollten in regelmäßigen Abständen `sudo apt update` und `sudo apt -y upgrade` ausführen, um Ihren Server auf dem neuesten Stand zu halten. Ansonsten sollten Sie keine Änderungen an Ihrem Server vornehmen und alles andere dem Skript `update.sh` überlassen.

Versuchen Sie NICHT, Betriebssystem-Upgrades an Ort und Stelle durchzuführen, wie z.B. ein Upgrade von Debian 11 auf 12 an Ort und Stelle. Sie werden Ihren Server zerstören!

Aktualisierung auf die neueste RMM-Version¶

Machen Sie vor dem Update immer ein Backup resp. ein Snapshot der aktuellen Installation

Melden Sie sich per SSH an Ihren Server an mit dem Benutzer, den Sie während der Installation angelegt haben.

Führen Sie niemals Update-Skripte oder -Befehle als Root-Benutzer aus. Das bringt die Berechtigungen durcheinander und macht Ihre Installation kaputt.

Laden Sie das Update-Skript herunter und führen Sie es aus:

```
wget -N https://raw.githubusercontent.com/amidaware/tacticalrmm/master/update.sh
chmod +x update.sh
./update.sh
```

Wenn Sie bereits auf der neuesten Version sind, wird das Update-Skript Sie darüber informieren und sofort zurückkehren.

Sie können die optionale Option `--force` an das Update-Skript übergeben, um ein Update zu erzwingen, wodurch die Prüfung auf die neueste Version umgangen wird.

```
wget -N https://raw.githubusercontent.com/amidaware/tacticalrmm/master/update.sh  
chmod +x update.sh  
./update.sh --force
```

Dies ist nützlich für eine verpfuschte Aktualisierung, die möglicherweise nicht vollständig abgeschlossen wurde.

Das Update-Skript korrigiert auch alle Berechtigungen, die während eines verpfuschten Updates durcheinander geraten sind, oder wenn Sie das Update-Skript versehentlich als Root-Benutzer ausgeführt haben.

Versuchen Sie nicht, MeshCentral manuell auf eine neuere Version zu aktualisieren. Sie sollten dies dem update.sh-Skript überlassen. Die Entwickler testen MeshCentral und stellen sicher, dass die Integration nicht unterbrochen wird, bevor sie die Mesh-Version aktualisieren.

Aktualisieren des Let's Encrypt SSL-Zertifikat

Derzeit erneuert das Update-Skript Ihr Let's Encrypt-Wildcard-Zertifikat, das alle 3 Monate abläuft, nicht automatisch, da es nicht ohne weiteres möglich ist, dies mit der DNS-TXT-Eintragsmethode zu automatisieren.

Let's Encrypt Wildcard Zertifikat erneuern

Um Ihre Let's Encrypt Wildcard Cert SSL-Zertifikate zu erneuern und zu aktualisieren, führen Sie den folgenden Befehl aus, wobei Sie `example.com` durch Ihre Domain und `admin@example.com` durch Ihre E-Mail-Adresse ersetzen:

```
sudo certbot certonly --manual -d *.example.com --agree-tos --no-bootstrap --preferred-challenges dns -m admin@example.com --no-eff-email
```

DNS TXT Eintrag aktualisieren

Die Propagierung von TXT-Einträgen kann je nach DNS-Anbieter zwischen 1 Minute und einigen Stunden dauern.

Bevor Sie die Eingabetaste drücken, sollten Sie überprüfen, ob der TXT-Datensatz bereitgestellt wurde.

Mit dem folgenden Befehl können Sie dies schnell überprüfen:

```
dig -t txt _acme-challenge.example.com
```

 (nicht vom TRMM-Server)

oder testen Sie mit: <https://viewdns.info/dnsrecord/> Enter: `_acme-herausforderung.beispiel.com`

```
-----
Getting wildcard cert
-----
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for example.com
```

```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:
```

```
nNw19h-muxNN9ZeDmIHvvtNCao9IMGyLuEu0EbmvfPE
```

```
Before continuing, verify the record is deployed.
```

```
-----
Press Enter to Continue
```

TXT	_acme-challenge	nNw19h-muxNN9ZeDmIHvvtNCa...	Auto	DNS only	Edit ▼
Type	Name	TTL			
TXT	<input type="text" value="_acme-challenge"/>	<input type="text" value="Auto"/>			
Content					
<input type="text" value="nNw19h-muxNN9ZeDmIHvvtNCao9IMGyLuEu0EbmvfPE"/>					
<input type="button" value="Delete"/>		<input type="button" value="Cancel"/>		<input type="button" value="Save"/>	

Neues Wildcard Zertifikat einbinden

Das erneuerte Zertifikat wird immer noch vollständig in Tactical verwendet. Führen Sie nun das Update Skript.

```
./update.sh --force
```