Hochverfügbarkeit (HA) einrichten – Anleitung

Nov 3, 2026 · @Viktor

Mit der Hochverfügbarkeit (HA) arbeiten mehrere SMS Gateways als Cluster: Fällt der aktive Node (Master) aus, übernimmt ein anderer Node (Slave) automatisch. Clients sprechen den Cluster über eine gemeinsame virtuelle IP an. Bis Version 25.x besteht ein Cluster aus genau zwei Gateways, ab 26.00 aus zwei oder mehr (2, 3, 4 usw.).

Welcher Abschnitt gilt, hängt von der Firmware-Version ab:

Firmware	Abschnitt
26.00 und neuer	Hochverfügbarkeit ab Version 26.00
24.00 bis 25.x	Hochverfügbarkeit ab Version 24.00
älter als 24.00	Hochverfügbarkeit für Versionen vor 24.00

Die Firmware-Version finden Sie im Webinterface unter Hilfe → Info (Software Version). Beide Gateways müssen dieselbe Firmware-Version haben.

Hochverfügbarkeit ab Version 26.00

Ab 26.00 kann ein Cluster aus beliebig vielen Gateways bestehen, z. B. 2, 3 oder 4. Ein Gateway ist Master, alle anderen sind Slaves. Sie richten den Cluster nur auf dem Master ein: Dort tragen Sie alle weiteren Knoten ein, aktivieren HA und übertragen die Konfiguration per Klick auf jeden Slave. Neu sind außerdem die Cluster-Strategie (inklusive Round-Robin-Load-Balancing) und die Buttons Standby und Wiederaufnehmen für einen manuellen Failover.

Voraussetzungen

1. Alle Gateways des Clusters laufen mit Firmware 26.00 und haben eine aktive HA-Lizenz. Jeder Slave prüft die Lizenz beim Import ebenfalls.
2. Alle Gateways haben statische IP-Adressen oder feste Zuweisungen im DHCP-Server (Konfiguration → Netzwerk) und liegen im selben Subnetz bzw. VLAN.
3. Jedes Gateway hat einen eigenen, eindeutigen Hostnamen (Konfiguration → Allgemein → Hostname). Notieren Sie die Hostnamen aller Slaves exakt, Sie brauchen sie auf dem Master.

4. Auf allen Gateways ist ein funktionierender DNS-Server eingetragen (Konfiguration → Netzwerk → Primärer DNS-Server).
5. Die virtuelle IP ist frei und kommt im Netz nur einmal vor.
6. Der Master erreicht jeden Slave per HTTPS (Port 443). Firewalls zwischen den Knoten lassen die Cluster-Kommunikation zu.

Schritt 1: Slaves vorbereiten

Auf den Slaves ist keine HA-Konfiguration nötig. Prüfen Sie auf jedem Slave nur unter Konfiguration → Restful API:

- "Aktivieren / Deaktivieren der HTTP Basic Authentication" ist angehakt (Standard ab 26.00). Ein zusätzliches Speichern wie in 24.00 ist nicht mehr nötig.
- Falls Sie eine IP-Zugriffsliste nutzen: Die IP des Masters ist erlaubt (Whitelist) bzw. nicht gesperrt (Blacklist).
- Es gibt einen Benutzer mit Administratorrechten inklusive Recht Hochverfügbarkeit. Mit diesem Benutzer meldet sich der Master in Schritt 4 am jeweiligen Slave an.

Schritt 2: Slaves als Knoten auf dem Master eintragen

1. Melden Sie sich auf dem Master an und öffnen Sie Konfiguration → Hochverfügbarkeit.
2. HA muss noch deaktiviert sein. Im Bereich Cluster Information sehen Sie das eigene Gateway als "Dieses Gateway (Master-Knoten)".
3. Tragen Sie darunter den ersten Slave ein:
   - Hostname des neuen Knoten: der Hostname des Slaves, z. B. gw2. Er muss exakt dem Hostnamen auf dem Slave entsprechen.
   - IP des neuen Knoten: die IP-Adresse des Slaves, z. B. 10.66.115.139.
4. Klicken Sie auf "Knoten zum Cluster hinzufügen". Der Knoten erscheint in der Liste.
5. Wiederholen Sie Punkt 3 und 4 für jeden weiteren Slave, z. B. gw3 und gw4.
6. Prüfen Sie die Liste: Sie muss alle Gateways des Clusters enthalten. Mit "Knoten entfernen" löschen Sie einen falschen Eintrag.

Schritt 3: HA auf dem Master aktivieren

Setzen Sie im oberen Formular:

Feld	Wert	Beispiel
Hochverfügbarkeit aktivieren	Aktiviert	

Feld	Wert	Beispiel
Node	Master	
Cluster-Strategie	siehe Tabelle unten	Kein Load Balancing
Virtuelle IP	IP, über die Clients den Cluster erreichen	10.66.115.141
Virtuelle Netzmaske	Netzmaske des HA-Netzes	255.255.255.0

Klicken Sie auf Speichern. Die Meldung "Die Einstellungen wurden erfolgreich gespeichert" bestätigt die Aktivierung.

Cluster-Strategie	Verhalten
Kein Load Balancing	Der konfigurierte Master ist immer aktiv, ein Slave übernimmt nur bei Ausfall.
Gateway mit bestem Empfang als Master nutzen	Die Signalstärke fließt in den HA-Score ein. Das Gateway mit dem besten Empfang wird Master.
Load Balancing (Round Robin)	Web- und API-Anfragen an die virtuelle IP werden auf alle Knoten verteilt.

Solange HA aktiv ist, sind Cluster-Strategie, virtuelle IP und Netzmaske gesperrt. Um sie zu ändern, deaktivieren Sie HA, speichern, ändern die Werte und aktivieren HA wieder.

Schritt 4: Slaves per Klick konfigurieren

1. In der Tabelle Cluster Information stehen die Slaves zunächst als OFFLINE.
2. Geben Sie in der Zeile des ersten Slaves unter Clusternode Switch Benutzername und Passwort des Administrators auf diesem Slave ein.
3. Klicken Sie auf Aktivieren.
4. Wiederholen Sie Punkt 2 und 3 für jeden weiteren Slave.

Der Master überträgt die Cluster-Konfiguration per REST API auf den Slave. Der Slave prüft, ob sein Hostname in der Knotenliste steht, übernimmt die Konfiguration und startet HA automatisch. Das kann bis zu zwei Minuten dauern.

Schritt 5: Cluster-Status prüfen

Nach kurzer Zeit zeigt die Tabelle Cluster Information alle Knoten des Clusters:

Spalte	Bedeutung
Node / Netzwerkadresse	Hostname und IP des Knotens
Health	Online, OFFLINE oder standby
Services	"Started - <Hostname>" beim Knoten, der gerade die virtuelle IP hält
Signalempfangsstärke	Empfang des Modems in dBm
Clusternode Switch	Standby oder Wiederaufnehmen für einen manuellen Failover

Rufen Sie danach die Weboberfläche über die virtuelle IP auf, z. B. https://10.66.115.141/.

Beispiel-Setup mit drei Knoten

Node	IP	Hostname	Rolle
gw1	10.66.115.140	gw1	Master
gw2	10.66.115.139	gw2	Slave
gw3	10.66.115.138	gw3	Slave

Virtuelle IP: 10.66.115.141, Netzmaske: 255.255.255.0. Auf gw1 tragen Sie gw2 und gw3 als Knoten ein und aktivieren anschließend beide Slaves einzeln. Ein vierter Knoten wird genauso ergänzt.

Manueller Failover

- Standby: Der Knoten gibt die virtuelle IP ab, ein anderer Knoten übernimmt.
- Wiederaufnehmen: Der Knoten nimmt wieder am Cluster teil.

Nutzen Sie das z. B. vor Wartungsarbeiten oder einem Firmware-Update.

Fehlermeldungen

Meldung	Ursache und Lösung
Ungültiger Benutzername oder Passwort	Zugangsdaten des Slaves prüfen. Basic Authentication auf dem Slave muss aktiv sein.

Meldung	Ursache und Lösung
Kann nicht auf den Server zugreifen	Der Master erreicht den Slave nicht per HTTPS. IP, Firewall und REST-API-Zugriffsliste prüfen.
Knoten nicht eingerichtet: Der Knotenname stimmt nicht mit dem Hostnamen des Ziel-Gateways überein	Den Knoten auf dem Master entfernen und mit dem exakten Hostnamen des Slaves neu anlegen.
Der eigene Hostname dieses Knotens kann nicht als Cluster-Knoten hinzugefügt werden	Es wurde der Hostname des Masters statt des Slaves eingetragen.
In der DNS-Konfiguration ist ein Fehler aufgetreten	Cluster deaktivieren, Hostnamen, Domäne und DNS-Server prüfen, dann neu einrichten.
Ihre Lizenz umfasst dieses Modul nicht	HA-Lizenz fehlt. Ab 26.00 wird HA dann dauerhaft deaktiviert. Nach dem Einspielen der Lizenz HA wieder aktivieren.

Hochverfügbarkeit ab Version 24.00

Gilt für Firmware 24.00 bis 25.x. Sie konfigurieren HA auf dem Master und richten den Slave anschließend per Klick automatisch ein.

Voraussetzungen

1. Beide Gateways haben statische IP-Adressen oder sind fest über den DHCP-Server gebunden (Konfiguration → Netzwerk).
2. Beide Gateways haben unterschiedliche Hostnamen (Konfiguration → Allgemein).
3. Beide Geräte befinden sich im selben Subnetz, z. B. 10.66.115.0/24.
4. DNS ist Pflicht: Tragen Sie unter Konfiguration → Netzwerk einen gültigen DNS-Server ein (z. B. Firewall, Router oder DNS-Server). Ohne funktionierenden DNS-Eintrag kann der Master den Slave nicht automatisch konfigurieren, auch wenn die IP bekannt ist.
5. Die Netzwerkkommunikation zwischen den Geräten funktioniert (Ping-Test empfohlen).
6. Die HA-Lizenz ist aktiviert.

Schritt-für-Schritt-Konfiguration

1. **Anmeldung:** Melden Sie sich mit einem administrativen Benutzer auf beiden SMS Gateways an, z. B. http://<IP-Adresse Ihres SMS-Gateways>/.
2. **RESTful API vorbereiten (nur auf dem Slave):** Öffnen Sie Konfiguration → RESTful API und klicken Sie auf Speichern, auch wenn die Häkchen bereits gesetzt sind. Erst dadurch wird die REST-Konfiguration vollständig initialisiert. Das ist entscheidend für die HA-Kommunikation.
3. **HA-Konfiguration auf dem Master aufrufen:** Konfiguration → Hochverfügbarkeit.
4. **HA aktivieren (auf dem Master):**
   - Hochverfügbarkeit aktivieren: Aktiviert
   - Node: Master
   - Optional: "Gateway mit bestem Empfang als Master nutzen" aktivieren
5. **Netzwerkeinstellungen setzen:**

Feld	Beschreibung	Beispiel
Virtuelle IP	IP, die für Clients erreichbar ist	10.66.115.141
Virtuelle Netzmaske	Netzmaske des HA-Netzes	255.255.255.0
Other Node IP	IP des zweiten Gateways	10.66.115.139
Other Node Hostname	Hostname des zweiten Gateways	gw2

6. **Konfiguration speichern:** Klicken Sie auf Speichern. Laden Sie die HA-Seite neu, falls die Nodes nicht angezeigt werden.
7. **Slave konfigurieren:** Tragen Sie im Bereich Cluster Information Benutzer und Passwort beim inaktiven Slave ein und klicken Sie auf Aktivieren. Der Slave wird automatisch konfiguriert.
8. **Cluster-Status prüfen:** Health zeigt den Online-/Offline-Status, Services die aktuelle Rolle (z. B. Master oder Standby), Signale die Empfangsstärke in dBm.
9. **Neustart (nur bei Bedarf):** Falls vom System empfohlen, starten Sie neu, um die HA-Dienste vollständig zu aktivieren.

Beispiel-Setup

Node	IP	Hostname	Rolle
gw1	10.66.115.140	gw1	Master
gw2	10.66.115.139	gw2	Slave

Virtuelle IP: 10.66.115.141, Netzmaske: 255.255.255.0.

Wichtige Hinweise

- Beide Nodes müssen identische Konfigurationen haben (außer IP und Hostname). Zum Abgleich nutzen Sie Konfiguration → Konfiguration Export/Import.
- Die virtuelle IP darf im Netz nur einmal vorkommen.
- Wenn DHCP genutzt wird: IPs im DHCP-Server fix binden.
- Keine Firewalls zwischen den Nodes, die die HA-Kommunikation blockieren, oder die Firewall für die Gateways freischalten.
- Testen Sie den Failover, indem Sie einen Node abschalten (z. B. Netzwerk trennen). Prüfen Sie regelmäßig die Signalstärken und exportieren Sie die Konfiguration.

Hochverfügbarkeit für Versionen vor 24.00

Bei Firmware vor 24.00 konfigurieren Sie beide Gateways einzeln und spiegelbildlich: Jedes Gateway kennt die IP und den Hostnamen des jeweils anderen. Geräte ohne Support-Service brauchen eine Lizenz für das Modul High Availability.

Konfiguration

1. Konfigurieren Sie beide Gateways mit einer statischen IP-Adresse (Configuration → Network) oder stellen Sie im DHCP-Dienst ein, dass beide Gateways immer dieselbe IP-Adresse erhalten. Beide Gateways müssen im selben Netzwerk (VLAN) liegen.
2. Aktivieren Sie unter Konfiguration → Hochverfügbarkeit die Hochverfügbarkeit und wählen Sie einen Modus (Broadcast oder Unicast). Beide Geräte müssen denselben Modus haben.
3. Vergeben Sie eine virtuelle IP-Adresse aus dem Netz der beiden SMS Gateways. Unter dieser IP-Adresse ist die Weboberfläche anschließend erreichbar.
4. Tragen Sie als Secret eine SHA1-kodierte Zeichenkette ein. Das Secret identifiziert die Nodes untereinander, ist 40 Zeichen lang und auf beiden Gateways identisch.
5. Setzen Sie das Häkchen Master Node nur auf dem primären Gateway.
6. Geben Sie unter Other node IP die IP-Adresse des jeweils anderen Gateways an.

7. Geben Sie unter Other Node Hostname den Hostnamen des jeweils anderen Gateways an.
8. Speichern Sie die Einstellungen.
9. Starten Sie beide SMS Gateways neu.

Beispielkonfiguration

Feld	Primäres Gateway (Master)	Backup-Gateway (Slave)
Hostname	test-sms-gw1	test-sms-gw2
Hochverfügbarkeit aktivieren	Aktiviert	Aktiviert
Modus	Broadcast	Broadcast
Virtuelle IP	10.66.115.199	10.66.115.199
Virtuelle Netzmaske	255.255.255.0	255.255.255.0
Secret (40 bytes Hex)	identischer SHA1-Wert	identischer SHA1-Wert
Master Node	angehakt	nicht angehakt
Other node IP	IP von test-sms-gw2, z. B. 10.66.115.108	IP von test-sms-gw1
Other Node Hostname	test-sms-gw2	test-sms-gw1

Nach dem Neustart zeigt Cluster Information "Heartbeat is running on this machine" und beide Nodes. Über "Manual cluster failover" schalten Sie manuell auf den anderen Node um.

Geräte ohne Support-Service benötigen auf beiden Gateways identisch lizenzierte Module. Nur dann kann das Backup-Gateway das primäre bei einem Ausfall vollwertig ersetzen.