WinGuard Systemanforderungen

Stand November 2019

Die Hardwareanforderungen sind von der Ausbaustufe des Systems und den angebundenen Anlagen abhängig. Es gelten die folgenden Systemanforderungen für die typischen Ausbaustufen:

Server:

Basic

- Intel Xeon E3-1230v6 3,5GHz 8MB, Quad-Core CPU *(oder vergleichbar)*
- 8GB ECC DDR4-2400 RAM
- 250GB NVMe SSD*
- 1 Gbit NIC
- Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 (64 bit)

Professional

- Intel Xeon E5-1630v4 3,7GHz 15MB, Quad-Core CPU *(oder vergleichbar)*
- 16GB ECC DDR4-2400 RAM
- 500GB NVMe SSD*
- 1 Gbit NIC
- Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 (64 bit)

Enterprise

- Intel Xeon E5-1650v4 3,6GHz 15MB, Hexa-Core CPU *(oder vergleichbar)*
- 32GB ECC DDR4-2400 RAM
- 1TB NVMe SSD*
- 1 Gbit NIC
- Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 (64 bit)

Bedienplatz:

Express / Client

- Intel i5-7600 3,5 GHz, Quad-Core CPU *(oder vergleichbar)*
- 8GB DDR4-2133 RAM
- 2GB PCIe Graphics Card
- 100GB NVMe SSD*
- 1 Gbit NIC
- Windows 10 Pro (64 bit), Windows 8.1 Pro (64 bit)

**) Der benötigte Speicherplatz hängt von der Systemnutzung und den Systemeinstellungen ab. Für den Betrieb eines WinGuard Server werden mindestens 100GB, für den Betrieb einer WinGuard Workstation mindestens 50 GB freier lokaler Festplattenspeicher benötigt. Ferner empfehlen wir die Ausfallsicherheit der Festplatten durch Redundanzen (z.B. RAID-Technologie) zu erhöhen.*

Schnittstellenserver:

Die Spezifikation der Schnittstellenserver ist von den angebundenen Anlagen abhängig. Zur abgesetzten Anbindung einer einzelnen Anlage kann in vielen Fällen ein lüfterloser Embedded-PC (z.B. Intel Celeron N3150 1,6GHz CPU, 2GB SODIMM RAM *oder vergleichbar*) verwendet werden.

Hinweise

Kompatibilität

Eine verbindliche Aussage über die Kompatibilität des eingesetzten Betriebssystems mit den ggf. verwendeten Softwarekomponenten anderer Hersteller (z.B. benötigte SDKs oder APIs) kann nicht durch Advancis Software & Services GmbH, sondern ausschließlich durch den entsprechenden Hersteller erfolgen.

Zeitsynchronisierung

Für den Betrieb von WinGuard muss eine Zeitsynchronisierung zwischen den Netzwerkteilnehmern sichergestellt werden. Dies kann z.B. durch einen Domänenserver, einen NTP-Server oder auch über eine WinGuard-Funktion realisiert werden. Letzteres setzt allerdings voraus, dass WinGuard mit Administratorrechten gestartet wird.

Benutzerkontensteuerung

Zur Nutzung von WinGuard, im Speziellen der „Watch-Dog"-Funktionalität, werden Zugriffs- und Schreibrechte auf das Programmverzeichnis benötigt. Dies kann ab Windows 8.1 (oder höher) und ab Windows Server 2012 (oder höher) eine Konfiguration der Benutzerkontensteuerung erfordern.

Anti-Viren-Programme

Durch die Verwendung von Anti-Viren-Programmen kann es zu Überschneidungen zwischen Zugriffen von WinGuard und des Anti-Viren Programms auf systemkritische Dateien kommen. Da dadurch Zugriffe blockiert oder verzögert werden können, empfehlen wir, dies durch geeignete Maßnahmen (z.B. Hinzufügen der WinGuard-Dateien zur Ausnahmeliste des Virenscanners) zu verhindern.

Betriebssystem Patches/Updates

Es wird vorausgesetzt, dass Windows-Betriebssysteme stets auf aktuellem Stand gehalten werden, d.h. das von Microsoft empfohlene Patches/Updates installiert sind.

Virtuelle Maschinen

WinGuard ist darauf ausgelegt, auf dedizierter Hardware unter einem Windows Betriebssystem zu laufen. Eine Virtualisierung der Hardware mit Hilfe von Hardware-Emulation/Hardware-Virtualisierung oder Para-Virtualisierung ist mit nachfolgenden Einschränkungen möglich:

Systemeinschränkungen

Da WinGuard projektabhängig eine Reihe von Schnittstellenmodulen verwendet, welche Hard- und Software von Drittherstellern anbinden, ist sicherzustellen, dass alle am Gesamtsystem beteiligten Komponenten in einer (teil-) virtualisierten Umgebung funktionsfähig sind.
Bei seriellen Anbindungen ist sicherzustellen, dass die Verbindung keinerlei Einschränkungen oder abweichendes Verhalten im Vergleich zu echter Hardware zeigt, z. B. das Timing-Verhalten beim Senden/Empfangen von Telegrammen.

Advancis Software & Services GmbH kann für die angebundenen Systeme von Fremdherstellern keine verbindliche Aussage bezüglich ihrer Virtualisierbarkeit treffen. Hier kann es insbesondere beim Verschieben der virtuellen Maschine zu Lastausgleichs- oder Hochverfügbarkeitszwecken zu Problemen kommen. Um eine hohe Betriebssicherheit zu gewährleisten, kann alternativ das WinGuard-eigene Hot-Standby System verwendet werden.

Lizenzeinschränkungen

Werden WinGuard Softwarelizenzen verwendet, so ist zu beachten, dass die Hardwarespezifikationen der verwendeten virtuellen Maschine unveränderlich sein müssen, da ansonsten eine Neuaktivierung der Softwarelizenz notwendig wird. Die Bindung an die Systemhardware erfolgt aufgrund von zwei Faktoren:

- Seriennummer des Systemlaufwerks
- MAC-Adresse des primären Netzwerkadapters

Da es vom eingesetzten Virtualisierungssystem abhängig ist, welche Aktionen eine Änderung der Systemhardware des Gastsystems bewirken, kann an dieser Stelle keine Aussage über die generelle Kopierbarkeit/Verschiebbarkeit des Gastsystems zwischen verschiedenen Hosts ohne erneute Aktivierung getroffen werden.

Ändert sich die Systemhardware des Gastsystems regelmäßig, so sollte ein Hardware-Dongle verwendet werden, um den ansonsten notwendigen Aktivierungsaufwand zu verhindern.