QEMU 5.0: Dateizugriff durch VirtIO-FS

Mit Version 5.0 erweitert das QEMU-Projekt seinen freien Hardware-Emulator um viele Funktionen. Hierzu gehört auch VirtIO-FS, eine Schnittstelle, die Maschinen nun einen deutlich schnelleren Zugriff auf von Host und VMs gemeinsam genutzte Dateien bietet. VirtIO-FS kann direkt auf den Host-Page-Cache zugreifen, wodurch die Daten zuvor nicht mehr in den Speicherbereich des Gastsystems kopiert werden müssen.

Außerdem wollen die Entwickler den VirtIO-FS-Code offenbar von C auf Rust umstellen. Darüber hinaus führen sie mit D-Bus-VMstate eine Bibliothek für QEMU-spezifische Interprozesskommunikation ein. Den Bluetooth-Code hat das Projekt komplett aus QEMU entfernt, da ihn seit Jahren niemand mehr pflegt und er nicht mehr funktioniert. Als Alternative empfehlen die Entwickler, dass Nutzer im emulierten Betriebssystem ein Bluetooth-Dongle per USB mit passendem Treiber verwenden.

Ebenfalls entfernt haben die Entwickler die PowerPC Reference Platform (PReP), eine Standardimplementierung der PowerPC-Architektur aus dem Jahre 1994 von IBM. Statt prep sollen QEMU-Anwender für PPC-Maschinen nun 40p nutzen (RS/6000). Die r4k-Emulation für die 64-bittige MIPS-R4000-CPU (beispielsweise SGI Indy) soll in QEMU 5.2 wegfallen, stattdessen soll ab sofort malta – entspricht dem MIPS Malta-Board – als Ersatz dienen. Auch die Einbindung von KVM auf AArch32-Systemen – jedoch nicht AArch64 – wird in einer der nächsten QEMU-Versionen verschwinden, weil der Code aus dem aktuellen Linux-Kernel ebenfalls rausgeflogen ist.

Viel Neues gibt es bei der ARM-Emulation: Das Projekt hat mehr als ein Dutzend neue Features der ARMv8-Architektur implementiert, beispielsweise VHE, PAN, PMU, DCPoP, TTCNP oder RCPC. Als neue Boards stehen der Netduino Plus 2 und der Orange Pi PC zur Verfügung. Neu ist auch die Berücksichtigung von Cortex-M7-Prozessoren, es handelt sich um den Nachfolger der Cortex-M4-CPU. Einige Mikrocontroller-Boards von Atmel, ST Microelectronics und NXP basieren auf dem Cortex M7. Für sicherheitsrelevante Aufgaben können ARM-Maschinen nun auf ein Trusted Platform Module (TPM) zugreifen.

Die RISC-V-Emulation hat ebenfalls einige Erweiterungen erfahren, unter anderem eine Echtzeituhr (Goldfish RTC) und experimentelle Implementierung für den RISC-V-v0.5-Draft eines nativen Hypervisors. Änderungen und eventuelle Inkompatibilitäten von QEMU 5.0 zur Vorgängerversion 4.2 sind im Changelog dokumentiert (siehe ix.de/zqaz).

Michael Plura (avr@ix.de)

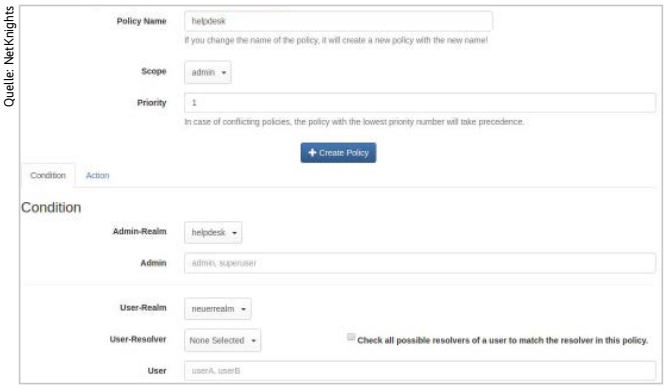
privacyIDEA 3.3 verwaltet Token zentral

In das Authentifizierungssystem privacyIDEA 3.3 hat die auf Open Source und Sicherheit spezialisierte Firma NetKnights neue Funktionen für Unternehmen eingebaut. So können Firmen die Token für die webbasierte, passwortlose Authentifizierung WebAuthn zentral über das multiinstanzfähige privacyIDEA verwalten. Die auf GitHub gehostete Software gibt es in den Repositories von Ubuntu 16.04 und 18.04. NetKnights bietet auch eine Enterprise-Variante für Ubuntu LTS, RHEL und CentOS an.

Das W3C hatte die zu FIDO2 gehörende Komponente WebAuthn 2019 zum Standard erhoben. Über diese API können Webanwendungen Benutzern eine PKI-basierte Authentifizierung im Browser bieten. NetKnights hat das Protokoll in privacyIDEA eingebaut und so diese Authentifizierungsmethode auch in Enterprise-Umgebungen verfügbar gemacht. Nutzer der Software können nun schrittweise ihre Zwei-Faktor-Authentifizierung modernisieren, indem sie bisherige Methoden wie SMS, OTP-Hardwaretoken oder Smartphone-Apps parallel zu modernen Verfahren wie YubiKey, U2F oder eben WebAuthn nutzen können.

Eine weitere Neuerung für den Unternehmenseinsatz ist das Event-Handler-Modul für die Protokollierung. Es kann ereignisgesteuert frei definierbare Log-Informationen sowohl lokal speichern als auch an einen zentralen Logging-Dienst weiterreichen. Die Entwickler stellen dies im Community-Blog des Projekts anhand des Beispiels einer Anbindung an Logstash mit Weiterverarbeitung per Elasticsearch und Kibana vor. Weiter steht mit dem Indexed-Secret Token ein Tokentyp bereit, mit dem sich Benutzer auf Basis eines existierenden Geheimnisses anmelden können. Das kann in Rollout-Szenarien hilfreich sein. (avr@ix.de)

Quelle: NetKnights



In der Weboberfläche von privacyIDEA kann der Administrator diverse Einstellungen vornehmen.

AWS MAP: Cloud-Migration zu Open Source

Mit dem Migration Acceleration Program (MAP) will Amazon Windows- durch Open-Source-Dienste aus der Cloud ablösen. Windows-Workloads (Server und SQL Server) lassen sich darüber in die AWS-Cloud zu freien Paketen verschieben, so spart man Lizenzkosten ein.

Im ersten Schritt untersucht das MAP die Eignung der Kundensysteme für eine Migration. Anschließend will Amazon die vorhandenen Ressourcen mobilisieren: Die Kunden aktualisieren die ermittelten Workloads auf einen für den Umzug geeigneten Stand. Abschließend findet die Migration zu AWS statt. Hierfür arbeitet Amazon auch mit Drittanbietern zusammen. (avr@ix.de)