

PROVIDING ROOT DELEGATION WITH BEYONDBTRUST POWERBROKER®

About BeyondTrust

Founded in 1985, BeyondTrust is the global leader in privilege authorization management, access control and security solutions for virtualization and cloud computing environments.

BeyondTrust empowers IT governance to strengthen security, improve productivity, drive compliance and reduce expense. The company's products eliminate the risk of intentional, accidental and indirect misuse of privileges on desktops and servers in heterogeneous IT systems. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust's PowerBroker suite of products to secure their enterprises. Also, five of the top ten commercial banks and two of America's largest private companies adopted PowerBroker to secure guest operating systems and ESX hypervisors in a virtualized environment. For more information, visit www.beyondtrust.com.

Using QualysGuard's integration with BeyondTrust's PowerBroker Servers, system administrators can securely delegate privileges and authorization without disclosing the root password within QualysGuard when performing trusted scans. Instead, QualysGuard uses PowerBroker Servers' root delegation functionality for authenticated vulnerability and compliance scans on UNIX/Linux systems.

PowerBroker Servers equips enterprises with highly flexible policy language that allows fine grained control over what Qualys can access. This solution will unify security across heterogeneous platforms. PowerBroker Servers also offers comprehensive logging, including keystroke logging and entitlement reports for auditing purposes.

Benefits

- **Simplify privileged delegation:** PowerBroker Servers enables system administrators to delegate privileges and authorization without disclosing root passwords – preventing misuse of privileges on desktops and servers in heterogeneous IT environments.
- **Facilitate compliance scanning:** Manage all privileged delegation using PowerBroker Servers, which offers comprehensive logging, including audit-ready reports, addressing the present-day pressure for enterprise compliance and control.
- **Better vulnerability discovery and prioritization:** When a trusted scan is performed, QualysGuard scanner logs into the target machine and reads configuration data including registry values and configuration files on the file system, just like a regular user session could. QualysGuard uses the configuration data to verify whether or not certain vulnerabilities that require local access to the host exist; as well as the ability to collect compliance data from systems without the burden of deploying agents.

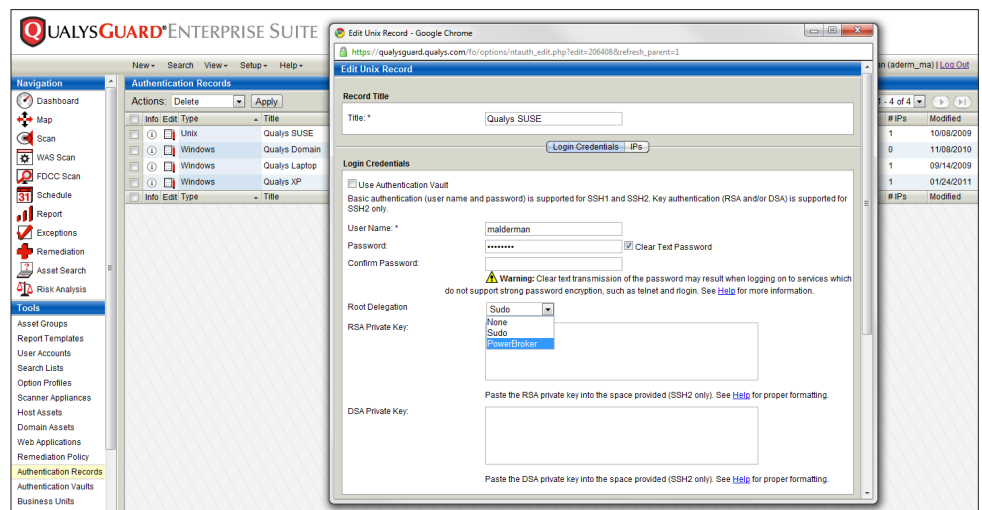


Figure 1: Enabling PowerBroker Servers in a Unix Authentication Record

Providing Root Delegation with BeyondTrust's PowerBroker

How it Works

To perform a scan with PowerBroker Servers enabled, QualysGuard completes these steps:

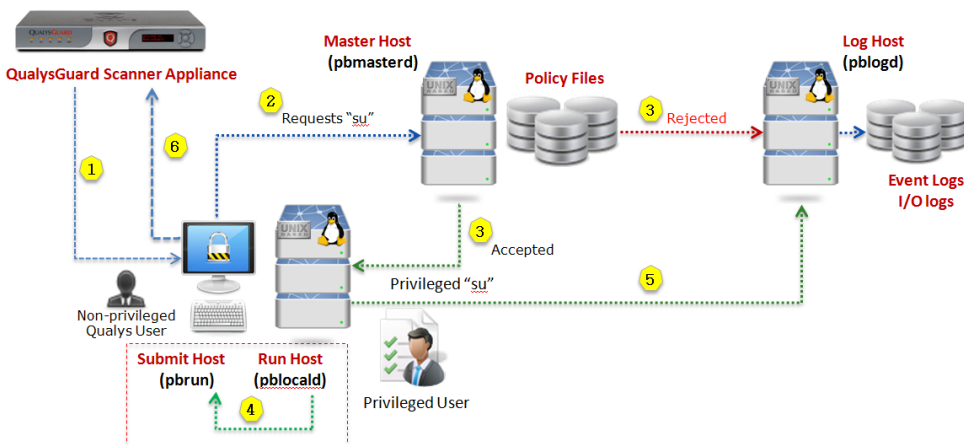


Figure 2: Overview of PowerBroker Servers

1. A connection is made from QualysGuard Scanner Appliance to the Target Host that has PowerBroker (or the PowerBroker "submithost").
2. Once the connection is successful and takes the QualysGuard user on the command line, the QualysGuard user makes a PowerBroker request for "su". From the "submithost", a pbrun request for "su" is sent to the PowerBroker agent on the "masterhost".
3. The agent on the "masterhost" receives the request data and processes this request along with the policy files that it maintains.
 - **REJECTED REQUESTS.** When the request is rejected (perhaps because the policy is written for the wrong user and command), the request is sent to the "loghost" for logging. This returns an error status back to the QualysGuard user and the scan does not run and stops.
 - **ACCEPTED REQUEST.** When the request is accepted, the agent on the "masterhost" calls on the PowerBroker agent on the "runhost" to initialize the process.
4. The PowerBroker agent on the "runhost" connects to pbrun on the "submithost" (the Target Host is both the PowerBroker "submithost" and "runhost").
5. The PowerBroker agent also connects to pblogd on the "loghost", then starts the privileged "su" request that is now iologged and monitored by PowerBroker.
6. The successful delegation of "su" by PowerBroker is communicated back to the QualysGuard Scanner Appliance and causes the scan to run, as PowerBroker iologs and monitors this privileged connection.

Supported Technologies

PowerBroker Servers supports multiple UNIX/Linux platforms. The following technology platforms have been verified for successful integration with QualysGuard: RedHat Enterprise Linux v3, v4, and v5.x, SUSE Linux Enterprise Server 9, 10, and 11, HP-UX 11i v1, v2, and v3, IBM AIX v5.x and 6.x, SUN Solaris 8, 9, and 10, VMware ESX 3.x and 4.x, Mac OS X 10.x.

About Qualys

Qualys, Inc. is the leading provider of on demand IT security risk and compliance management solutions – delivered as a service. Qualys' Software-as-a-Service (SaaS) solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures.

The QualysGuard® service is used today by more than 5,000 organizations in 85 countries, including 45 of the Fortune Global 100, and performs more than 500 million IP audits per year. Qualys has the largest vulnerability management deployment in the world at a Fortune Global 50 company, and has been recognized by leading industry analysts for its market leadership.

Qualys has established strategic agreements with leading managed service providers and consulting organizations including BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, NTT, SecureWorks, Symantec, Tata Communications and TELUS. Qualys is also a founding member of the Cloud Security Alliance (CSA).

For more information, please visit www.qualys.com.



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com

UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101

Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146

France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70

Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296

United Arab Emirates – Qualys FZE • PO Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225

China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

