Enterprise Reporter for Windows Servers

Windows Server configuration reporting for security and auditing

Windows® infrastructure administrators today have a broad range of responsibilities, including supporting migration activities, achieving and maintaining IT compliance, or fulfilling requests for information about the configuration of Windows file servers. On a daily basis, they must answer questions like the following:

- Who has administrative access to Windows servers and workstations?
- How are my servers configured, including general computer information, network settings, services running, installed programs and custom registry keys?
- How does the configuration of my servers change over time?
- What local users and groups exist on every server, and what is their membership?

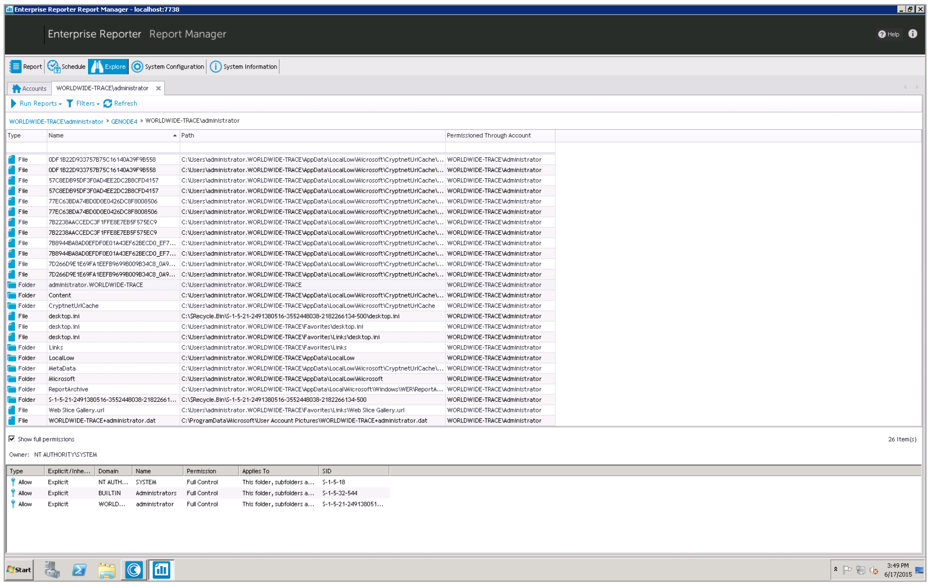
Only one solution identifies the current and historical configuration of their Windows servers to help administrators answer these questions. Enterprise Reporter for Windows Servers provides visibility into Microsoft® Windows Server® configuration. Armed with this information, organizations can perform change audits, security assessments, and pre- and post-migration analyses — enabling informed strategic planning and proactive management of their IT infrastructure.

FEATURES

- **Compliance and security visibility** — Gain visibility into configuration of critical IT assets in Windows file servers and NAS devices for complete Windows Server file audit. Comply with security best practices, internal policies and external regulations, and ensure Active Directory® security.

BENEFITS:

- Enhances security by increasing visibility into where selected users and groups have permissions — across the entire Windows file server and NAS environment
- Improves compliance by ensuring that local security configuration is aligned with domain-wide policies
- Enables effective change review and Windows Server file audit by capturing the historical configuration of Windows file servers and providing detailed change history reports
- Collects and reports on permissions of shares, files and folders, printers, registry keys and services
- Is scalable, secure and customizable to support large and complex Windows environments with multiple groups of report consumers



WORLDWIDE-TRACE\administrator > GENODE4 > WORLDWIDE-TRACE\administrator

Type	Name	Path	Permissioned Through Account
File	0DF1B22D933757B75C16140A39F9B558	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	0DF1B22D933757B75C16140A39F9B558	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	57C8EDB95DF3F0AD4EE2DC2B8CFD4157	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	57C8EDB95DF3F0AD4EE2DC2B8CFD4157	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	77EC63BDA74BD0D0E0426DC8F8008506	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	77EC63BDA74BD0D0E0426DC8F8008506	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	7B2238AACCEDC3F1FFE8E7EB5F575EC9	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	7B2238AACCEDC3F1FFE8E7EB5F575EC9	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	7B8944BA8AD0EFDF0E01A43EF62BECD0_EF7...	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	7B8944BA8AD0EFDF0E01A43EF62BECD0_EF7...	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	7D266D9E1E69FA1EEFB9699B009B34C8_0A9...	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
File	7D266D9E1E69FA1EEFB9699B009B34C8_0A9...	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
Folder	administrator.WORLDWIDE-TRACE	C:\Users\administrator.WORLDWIDE-TRACE	WORLDWIDE-TRACE\Administrator
Folder	Content	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
Folder	CryptnetUrlCache	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache	WORLDWIDE-TRACE\Administrator
File	desktop.ini	C:\$Recycle.Bin\S-1-5-21-2491380516-3552448038-2182266134-500\desktop.ini	WORLDWIDE-TRACE\Administrator
File	desktop.ini	C:\Users\administrator.WORLDWIDE-TRACE\Favorites\desktop.ini	WORLDWIDE-TRACE\Administrator
File	desktop.ini	C:\Users\administrator.WORLDWIDE-TRACE\Favorites\Links\desktop.ini	WORLDWIDE-TRACE\Administrator
Folder	Links	C:\Users\administrator.WORLDWIDE-TRACE\Favorites\Links	WORLDWIDE-TRACE\Administrator
Folder	LocalLow	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow	WORLDWIDE-TRACE\Administrator
Folder	MetaData	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft\CryptnetUrlCache\...	WORLDWIDE-TRACE\Administrator
Folder	Microsoft	C:\Users\administrator.WORLDWIDE-TRACE\AppData\LocalLow\Microsoft	WORLDWIDE-TRACE\Administrator
Folder	ReportArchive	C:\Users\administrator.WORLDWIDE-TRACE\AppData\Local\Microsoft\Windows\WER\ReportA...	WORLDWIDE-TRACE\Administrator
Folder	S-1-5-21-2491380516-3552448038-21822661...	C:\$Recycle.Bin\S-1-5-21-2491380516-3552448038-2182266134-500	WORLDWIDE-TRACE\Administrator
File	Web Slice Gallery.url	C:\Users\administrator.WORLDWIDE-TRACE\Favorites\Links\Web Slice Gallery.url	WORLDWIDE-TRACE\Administrator
File	WORLDWIDE-TRACE+administrator.dat	C:\ProgramData\Microsoft\User Account Pictures\WORLDWIDE-TRACE+administrator.dat	WORLDWIDE-TRACE\Administrator

☑ Show full permissions

26 Item(s)

Owner: NT AUTHORITY\SYSTEM

Type	Explicit/Inhe...	Domain	Name	Permission	Applies To	SID
Allow	Explicit	NT AUTH...	SYSTEM	Full Control	This folder, subfolders a...	S-1-5-18
Allow	Explicit	BUILTIN	Administrators	Full Control	This folder, subfolders a...	S-1-5-32-544
Allow	Explicit	WORLD...	administrator	Full Control	This folder, subfolders a...	S-1-5-21-249138051...

Figure 1: Enterprise Reporter for Windows File Servers lets you interactively analyze explicit permissions of a user or a group across all of your file servers and network filers.

Enterprise Reporter for Windows Servers provides automated discovery and reporting on configuration of Windows servers for migration planning, security assessment and change auditing processes.

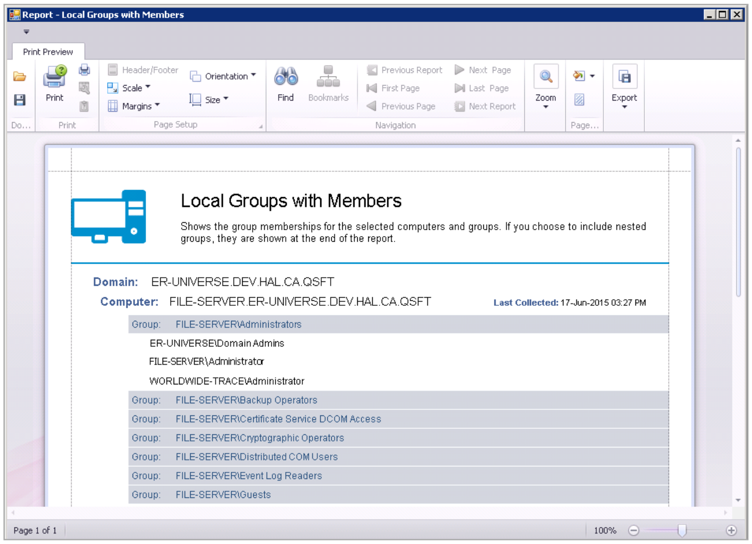
SYSTEM REQUIREMENTS

For complete system requirements, please visit quest.com/products/enterprise-reporter-for-windows-servers.

- **Access assessment** — Rapidly find out in real time where selected users and groups have permissions across the entire Windows file server and NAS environment. This Windows Server access reporting enables tightened security and ensures access is provided on a business-need-to-know basis.
- **Local policy assessment** — Make sure local security configuration is aligned with domain-wide policies. Check local security policies, membership of local administrative groups and other security configuration stored in registry keys.
- **Change history** — Capture historical configuration information on Windows Server and view detailed change history reports. Gain in-depth insight for historical analysis and compliance reporting.
- **Permission reporting** — Collect and report on permissions of shares, files and folders, printers, registry keys and services for comprehensive Windows Server permission reporting. Identify access control entries explicitly set on files in a folder hierarchy of a specified depth.
- **Scalable data collection** — Scale to Windows environments of any size. Schedule collections during off-peak hours to minimize the impact of data collection on network and server performance, and leverage distributed collection architecture for load balancing.
- **Efficient storage** — Reduce database storage requirements and save more change history data by comparing Windows Server discoveries and storing only the changes.
- **Customizable reports** — Use predefined reports with advanced filtering and multiple formats, including PDF, HTML, MHT, RTF, XLS, XLSX, CSV, text and images. Create customized reports with added attributes and advanced filtering. Perform efficient, effective data analysis and satisfy the unique informational needs of your organization.
- **Automated reporting workflows** — Automate report generation and delivery for multiple report consumers according to different schedules.
- **Common reporting portal** — Export reports to Knowledge Portal for a unified reporting interface across the entire family of Quest compliance and IT governance solutions.

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple to use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.



Local Groups with Members

Shows the group memberships for the selected computers and groups. If you choose to include nested groups, they are shown at the end of the report.

Domain: ER-UNIVERSE.DEV.HAL.CA.QSFT

Computer: FILE-SERVER.ER-UNIVERSE.DEV.HAL.CA.QSFT Last Collected: 17-Jun-2015 03:27 PM

Group: FILE-SERVER\Administrators

ER-UNIVERSE\Domain Admins

FILE-SERVER\Administrator

WORLDWIDE-TRACE\Administrator

Group: FILE-SERVER\Backup Operators

Group: FILE-SERVER\Certificate Service DCOM Access

Group: FILE-SERVER\Cryptographic Operators

Group: FILE-SERVER\Distributed COM Users

Group: FILE-SERVER\Event Log Readers

Group: FILE-SERVER\Guests

Figure 2. Enterprise Reporter for Windows File Servers can show local administrators, factoring in nested group memberships.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find
local office information on our Web site.