

ChangeAuditor™ for Active Directory®

Auditorías en tiempo real para Active Directory

EL DESAFÍO

Microsoft® Active Directory® es el núcleo de su infraestructura de red de misión crítica. Los problemas con el directorio pueden ocasionar tiempo fuera de la red que afecte el negocio e interrupciones del servicio no planificadas y costosas, así como infracciones dañinas a la seguridad y falta de cumplimiento de las críticas normativas gubernamentales como Sarbanes-Oxley (SOX), Industria de Pagos con Tarjeta (PCI, Payment Card Industry) y la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (HIPAA, Health Insurance Portability and Accountability Act). Se debe notificar a las organizaciones, en tiempo real, sobre los cambios críticos a Active Directory.

LA SOLUCIÓN

El reconocido software de Quest ChangeAuditor impulsa la seguridad y el control de Active Directory con el rastreo de todos los cambios de configuración de Active Directory claves en tiempo real. Desde los cambios de esquema y objetos de políticas de grupo (GPO) hasta los cambios operativos y

grupo anidado críticos, ChangeAuditor rastrea, audita, informa y alerta sobre los cambios que impactan en su directorio; sin la sobrecarga de activar la auditoría nativa. Con ChangeAuditor for Active Directory, obtendrá el “quién, qué, cuándo, dónde y la estación de trabajo” de los cambios y de cualquier detalle de evento relacionado con los valores del antes y después. También puede agregar comentarios que expliquen por qué se realizó un cambio específico para cumplir con los requisitos de su auditoría.

AUDITORÍA DE TODOS LOS CAMBIOS CRÍTICOS

ChangeAuditor ofrece una auditoría y generación de informes extensibles y personalizables de todos los cambios del sistema de archivos y de Active Directory, que incluyen GPO, sistema de nombre de dominio (DNS), configuraciones del servidor y grupos anidados. Obtendrá visibilidad total de todos los cambios con un análisis forense profundo sobre la relación de otros eventos con el transcurso del tiempo en orden con el transcurso del tiempo en orden

BENEFICIOS:

- Se instala en minutos con recopilación de eventos rápida para un análisis inmediato en ambientes Windows.
- Permite realizar auditorías en toda la empresa y el cumplimiento de normas de un cliente único.
- Elimina las inquietudes de seguridad desconocidas, asegura acceso continuo a las aplicaciones, los sistemas y los usuarios con un seguimiento de todos los eventos y esos cambios relacionados con incidentes específicos.
- Disminuye los riesgos de seguridad en segundos con alertas en tiempo real a cualquier dispositivo para una respuesta inmediata, dentro o fuera de la oficina.
- Fortalece los controles internos con protección contra cambios no deseados y limita el control de usuarios autorizados.
- Impulsa la disponibilidad al posibilitar la solución de problemas proactiva para bloqueos de cuenta.
- Disminuye el arrastre de rendimiento en los servidores y ahorra recursos de almacenamiento con la recopilación de eventos sin el uso de auditoría nativa.
- Optimiza el cumplimiento de las normativas y políticas empresariales y gubernamentales, incluidas SOX, PCI DSS, HIPAA, FISMA, SAS 70 y más.
- Convierte la información en un análisis forense profundo e inteligente para los auditores y la administración.

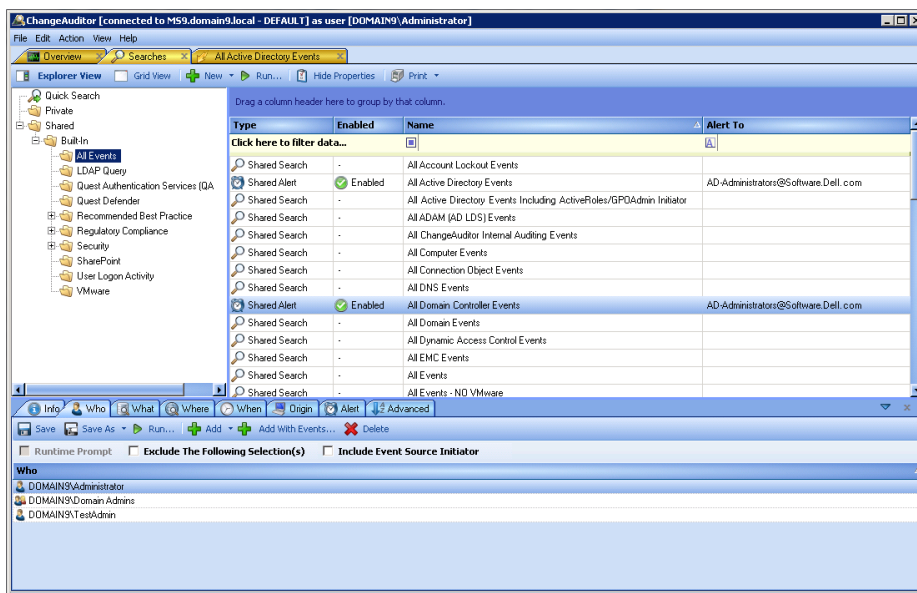


Figura 1. Con ChangeAuditor for Active Directory, verá quién, qué, cuándo, dónde y la estación de trabajo de todos los cambios en orden cronológico.

“En general, ChangeAuditor ha sido muy útil. Ningún otro producto que evaluamos ofreció el mismo nivel de protección y auditoría en tiempo real, sin necesidad de que la auditoría de Windows estuviera habilitada para todos los cambios de Active Directory”.

Patrick Rohe
Arquitecto de TI sénior
Towson University

REQUISITOS DEL SISTEMA

Para ver una lista detallada y actual de los requisitos del sistema, visite software.quest.com/products/changeauditor-for-active-directory.

cronológico de su ambiente de Windows completo. Y, con las alertas en tiempo real, mantendrá una concientización constante y la habilidad de responder desde cualquier lugar y cualquier dispositivo a los cambios de política vitales y las infracciones de la seguridad a medida que se produzcan, lo que disminuirá los riesgos asociados con las modificaciones día a día.

RASTREO DE LA ACTIVIDAD DE USUARIOS Y PREVENCIÓN DE CAMBIOS NO DESEADOS

ChangeAuditor for Active Directory ayuda a ajustar los cambios en toda la empresa y las políticas de control con el rastreo de la actividad de los usuarios y administradores para los bloqueos de cuenta y el acceso a las configuraciones de registro críticas. Con los controles proactivos para evitar cambios críticos en primer lugar, hasta alertas en tiempo real 24 horas al día, los siete días de la semana, análisis profundos, la habilidad de restaurar valores previstos y las funcionalidades de generación de informes, su Active Directory está protegido contra la exposición a un comportamiento sospechoso y al acceso no autorizado, y siempre está en cumplimiento con los estándares gubernamentales y corporativos.

CONVERTIR DATOS IRRELEVANTES EN INFORMACIÓN SIGNIFICATIVA PARA IMPULSAR LA SEGURIDAD Y EL CUMPLIMIENTO DE NORMAS

ChangeAuditor for Active Directory rastrea los cambios críticos a su entorno de Windows, luego traduce los datos sin procesar en datos inteligentes significativos para ayudar a proteger la seguridad y el cumplimiento de normas de su infraestructura. Las limitaciones de auditoría se convierten en historia pasada gracias al motor de auditoría de alto rendimiento de ChangeAuditor y, sin necesidad de registros de auditoría nativa, verá resultados más rápidos y ahorrará recursos de almacenamiento.

AUTOMATIZACIÓN DE GENERACIÓN DE INFORMES PARA NORMATIVAS GUBERNAMENTALES Y CORPORATIVAS

Con SQL Reporting Services (SRS) de Microsoft, ChangeAuditor for Active Directory ofrece informes de cumplimiento de normas y seguridad significativos y limpios sobre la marcha. Con una biblioteca de cumplimiento incorporada y la habilidad de crear sus propios informes, proporcionar el cumplimiento de normas para estándares como SOX, HIPAA, PCI DSS, FISMA y SAS 70 es fácil.

The screenshot shows the ChangeAuditor application interface. The top part displays a table of events with columns for Severity, Time Detected, Subsystem, User, Server, Action, Facility, and Site. Below this, a detailed view of a specific event is shown, including fields for Who, What, When, and Origin, along with a Result section.

Severity	Time Detected	Subsystem	User	Server	Action	Facility	Site
Medium	8/26/2013 8:49 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U...	DOMANR3
Medium	8/19/2013 12:23 PM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U... Default First S...	DOMANR3
Medium	8/14/2013 7:50 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U... Default First S...	DOMANR3
Medium	8/14/2013 7:47 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U... Default First S...	DOMANR3
Medium	5/5/2013 10:21 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U... Default First S...	DOMANR3
Medium	4/12/2013 10:11 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U...	DOMANR3
Medium	4/12/2013 10:08 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U...	DOMANR3
Medium	4/12/2013 9:55 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U...	DOMANR3
Medium	3/15/2013 8:49 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U...	DOMANR3
Medium	3/15/2013 8:45 AM	Active Directory	DOMANF\Administrator	DC3	Modify Attribute	Custom U...	DOMANR3

Who	DOMANF\Administrator (Administrator)	Source	ChangeAuditor	When	8/26/2013 8:49 AM
What	The user account ow-Randy F. Smith\OW-Randy.F. Smith\DC3-domain\DC3-local was disabled.	Origin	DC3-domain\local (10.6.162.91)	Result	Success
Class	user	Action	Modify Attribute	Facility	Custom (User Monitoring)
Object	domain\local\Users\Randy.F. Smith	Attribute	userAccountControl	SSL/TLS	No
				Sign/Seal	Yes

Figura 2: Las búsquedas relacionadas le brindan seguridad en contexto con detalles sobre usuarios específicos y todos los cambios que hicieron.

INFORMACIÓN SOBRE QUEST®

Quest ayuda a nuestros clientes con la reducción de las tediosas tareas de administración para que usted pueda centrarse en la innovación necesaria para que su empresa crezca. Las soluciones de Quest son escalables, rentables y simples de usar, y proporcionan eficiencia y productividad inigualables. Además de la invitación

de Quest hecha a la comunidad global para participar en esta innovación y de nuestro firme compromiso para garantizar la satisfacción del cliente, Quest continuará con la aceleración de la entrega de las soluciones más integrales para la administración de la nube de Azure, SaaS, seguridad, movilidad de la fuerza de trabajo e información impulsada por datos.

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.

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

© 2017 Quest Software Inc. ALL RIGHTS RESERVED.

DataSheet-Change-Auditor4AD-US-KS-24824_EC

The Quest logo consists of the word "Quest" in a bold, sans-serif font. The letter "Q" is significantly larger than the other letters and is colored in a vibrant orange-red. The remaining letters "uest" are in a dark blue color.