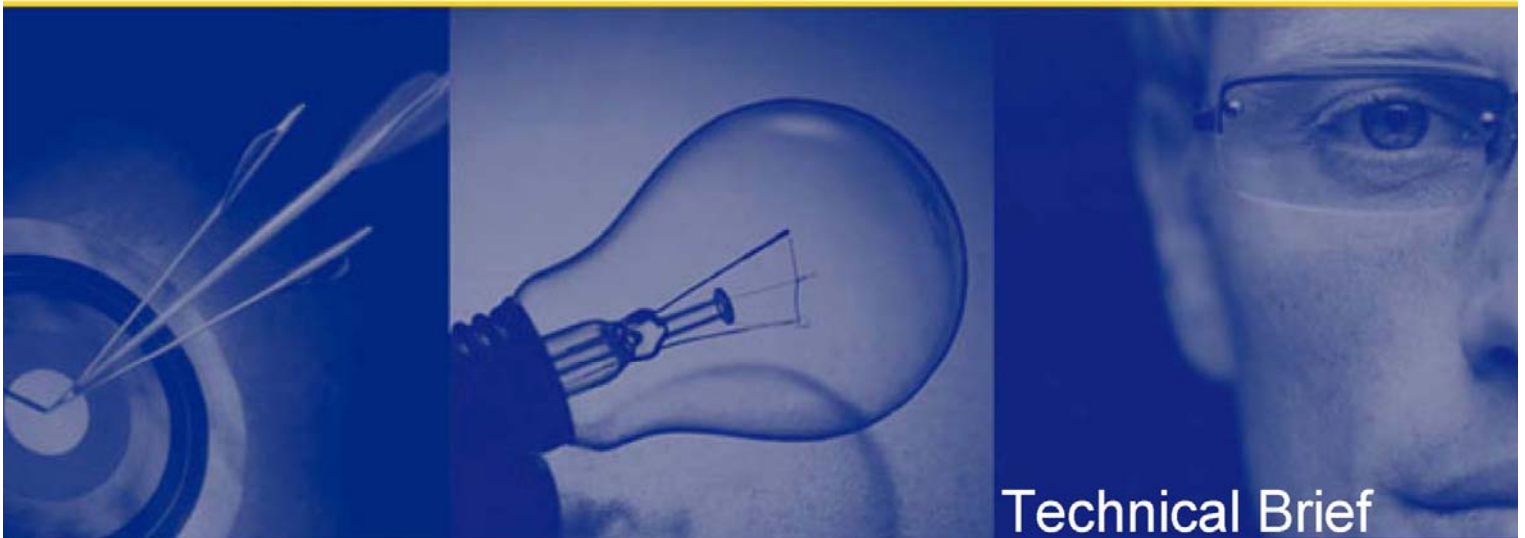


Quest Password Manager



Technical Brief

© Copyright Quest® Software, Inc. 2007. Todos los derechos reservados.

Esta guía contiene información protegida por Copyright. El software descrito en este documento está cubierto por una licencia de software o acuerdo de confidencialidad. Este software puede utilizarse o copiarse únicamente dentro de las condiciones del acuerdo aplicable al mismo. Ninguna parte de esta guía puede ser reproducida o transmitida de modo alguno o por medio alguno, electrónico, mecánico –incluyendo fotocopia o grabación- para ningún fin distinto del uso personal del comprador sin autorización por escrito de Quest Software, Inc.

GARANTIA

La información contenida en este documento está sujeta a cambios sin previo aviso. Quest Software no ofrece garantías de ningún tipo respecto de esta información. QUEST SOFTWARE DECLINA EXPRESAMENTE LA GARANTÍA IMPLÍCITA DE COMERCIALIZACIÓN Y ADAPTACIÓN A UN FIN PARTICULAR. Quest Software no asumirá ninguna responsabilidad por daños directos, indirectos, incidentales, consecutivos o de cualquier otra naturaleza que pudiera exigirse en conexión con la modificación o uso de esta información.

MARCAS REGISTRADAS

Todas las marcas registradas y marcas comerciales utilizadas en esta guía son propiedad de sus respectivos dueños.

Sede principal: 5 Polaris Way. Aliso Viejo, CA 92656

www.quest.com

e-mail: info@quest.com

Tel. (EE.UU. y Canadá): 949.754.8000

Por favor, consulte nuestra Web si desea información sobre nuestras oficinas regionales o internacionales.

BORRADOR

Índice de Contenidos

| | |
|--|----|
| INTRODUCCIÓN | 4 |
| Arquitectura de QPM | 5 |
| CAPA DE APLICACIÓN WEB | 6 |
| CAPA DE BASE DE DATOS SQL SERVER | 8 |
| ACTIVE DIRECTORY | 9 |
| Actualizaciones de passwords en el Active Directory..... | 9 |
| Implicaciones para el despliegue de QPM..... | 9 |
| CONCLUSIÓN | 11 |
| Acerca de Quest Software, Inc. | 12 |
| Contacto con Quest Software..... | 12 |
| Soporte técnico de Quest..... | 12 |

INTRODUCCIÓN

Las grandes empresas con grupos de usuarios distribuidos por todo el mundo ponen en marcha distintas estrategias e infraestructuras para resolver los servicios e autenticación y de directorio de estos usuarios utilizando el Active Directory.

En la vida real puede darse cualquier combinación posible de configuraciones de sites, dominios/bosques y topologías de red física como consecuencia del propio crecimiento natural de la organización, fusiones y adquisiciones de empresas, características de las estructuras organizativas, aspectos de eficiencia operativa o, lo más frecuente, una mezcla de todos estos factores.

Recomendar una única “buena práctica” que pudiera adaptarse a todos los escenarios posibles, objetivos de servicio y topologías el Active Directory queda fuera del alcance de un documento como éste, de propósito general. Lo que aquí se exponen son diversas consideraciones de carácter técnico que han de tenerse en cuenta y aplicarse en consonancia con los requisitos de cada organización concreta y la infraestructura de que dispone.

Arquitectura de QPM

Quest Password Manager (QPM) consta de un componente de desktop (La Extensión de Password Segura o *Secure Password Extension*), y un componente de servicio. Lo que se analiza aquí es el despliegue del componente de servicio del back-end.

La infraestructura de servicios de back-end de Quest Password Manager consta de::

- Una capa de aplicación Web desplegada sobre un servidor Windows Internet Information Services (IIS);
- Una base de datos SQL Server utilizada para almacenar los logs de eventos;
- Una conexión con el Active Directory.

Cada elemento debe considerarse por orden para que una organización pueda determinar de forma precisa cuáles son los requisitos específicos de su solución para cada uno de ellos.

CAPA DE APLICACIÓN WEB

La aplicación Web de QPM aporta el enlace entre el usuario y el Active Directory, donde se almacenan los datos de estado del usuario (configuración e información privada) y que es, en último término, el objetivo del proceso de reset de la password. La aplicación Web dispone de un help desk en modo autoservicio e interfaces de administrador. Podemos decir que a la hora de evaluar los requisitos de rendimiento y fiabilidad para conseguir una capa de aplicación Web de rendimiento óptimo, se consideran los mismos aspectos que se tienen en cuenta para cualquier otra aplicación Web ligera.

La capa Web ejecuta acciones de usuario, help desk y administrativas. La función de reset en modo autoservicio es la más crítica desde el plano operativo; el sitio de autoservicio de QPM validará la identidad del usuario basándose en el conocimiento de ciertas preguntas secretas. Si se responden correctamente, la aplicación QPM inicia un reset de la password (o cambio de contraseña), o desbloquea la cuenta.

Cada servidor QPM mantiene su propio estado de sesión localmente y utiliza el Active Directory para el almacenamiento de datos persistentes. Esto permite que QPM pueda duplicarse para permitir el balanceo de carga. Por esto mismo pueden existir instancias duplicadas si se considera necesario instalar una instancia adicional situada cerca de un grupo de usuarios concreto, simplemente para obtener mejores rendimientos de la aplicación y la red. Adviértase que el esquema de balanceo de carga debe soportar la gestión de sesión de la instancia de QPM.

Todos los datos de tipo permanente utilizados por la aplicación se guardan en el Active Directory, por lo que se replican e forma automática para garantizar su disponibilidad sobre cualquier Controlador de Dominio adyacente a una instancia dada de la aplicación Web. Así, un usuario en movilidad siempre obtendrá los mismos datos independientemente de la instancia QPM, dependiendo únicamente de la latencia de replicación del Active Directory.

La carga de un servidor Web concreto está en función del número de usuarios a los que dará servicio y la frecuencia con que se soliciten los servicios de Reset de Password (debido a bloqueos o pérdida de la password). Las series históricas estadísticas serán de gran utilidad a la hora de valorar la cantidad probable de peticiones de reset de password diarias. Se tiene que calcular también una carga adicional en el caso de que se considere que QPM va a ser el vector principal para la tarea de cambio de password periódica (p.ej. cada 90 días) en modo autoservicio como consecuencia de la aplicación de políticas de usuario.

Así pues, a la hora de planificar el despliegue de la capa de aplicación Web –es decir, de las propias instancias de QPM- tenemos que tener en cuenta dos factores: el rendimiento de la instancia QPM como aplicación Web exclusivamente y el impacto de

la adyacencia dentro de la red e los servicios conexos (SQL Server y Active Directory, como veremos más adelante).

CAPA DE BASE DE DATOS SQL SERVER

El servidor SQL Server se emplea únicamente para registro de eventos y acciones, que quedan así disponibles para la elaboración de informes desde la interfaz administrativa de QPM. El servicio QPM seguirá funcionando aunque este servicio no esté disponible; no es un elemento especialmente crítico a la hora del cálculo de rendimiento, aunque la latencia el acceso al servidor SQL Server puede tener impacto sobre las operaciones del Web. Las instancias de QPM pueden apuntar hacia una instancia de SQL Server centralizada o local.

Adviértase que las funciones de elaboración de informes del sitio Web de Administración solamente producen informes a partir de datos almacenados en aquella instancia de SQL Server a la cual se conecta una instancia de QPM dada, de manera que los informes solamente incluirán aquellos eventos relativos a dicha instancia de QPM . Los logs se guardan en formato no cifrado por lo que se pueden consolidar informes utilizando SQL Server Reporting Services. No obstante, el producto por sí mismo no ofrece la posibilidad de consolidar informes.

ACTIVE DIRECTORY

Actualizaciones de passwords en el Active Directory

Después de autenticarse correctamente ante QPM, la aplicación Web QPM realizará un reset o cambio de password sobre cualquier Controlador de Dominio que quede cercano a la instancia de QPM en una configuración de site dada. Estos cambios de password se redirigen hacia el máster de emulación del Controlador Primario de Dominio aplicando un criterio de prioridad.

Cuando la autenticación de credenciales de un usuario falla aparentemente por no coincidir con la noción de password actual de su Controlador de Dominio local, ese Controlador de Dominio consultará acto seguido al máster de Controlador Primario de Dominio si la password ha cambiado realmente; si es así, el PDC comunicará la nueva password al margen de los mecanismos normales de replicación, permitiendo que se complete la autenticación correctamente, si la password introducida coincide efectivamente con la nueva password. Esta comunicación para verificar passwords incorrectas se aplica a cualquier controlador de dominio dentro del dominio, no solo dentro del site local.

Este comportamiento es el propio del Active Directory y es completamente independiente del producto QPM. (Este comportamiento por defecto, no obstante, puede cambiarse por reconfiguración o bloquearse atendiendo a aspectos de seguridad a nivel de firewall). Obviamente, la configuración del site, la latencia de la red y otros factores condicionan los distintos niveles de respuesta a la hora de autenticar al usuario contra un DC pendiente de replicar. Con todo, si la comunicación del PDC para cambios de password está correctamente configurada, este proceso debería completarse con éxito.

Implicaciones para el despliegue de QPM

Los aspectos a tener en cuenta para el despliegue de QPM, ya sea de forma centralizada o distribuida en los sites primarios son básicamente equiparables (aunque no idénticos) a los que se deben considerar en el caso de los resets de passwords efectuados manualmente por un help desk, puesto que QPM únicamente automatiza una función que de otra manera ha de realizarse a mano por parte de un operador de este servicio.

Si la organización dispone de un único servicio de help desk centralizado que se encarga de resetear las passwords para todos los usuarios, las características de rendimiento de QPM serán equiparables a las que se producen en el escenario manual. Por el contrario, si esta actividad se ha resuelto en el pasado desde servicios de help desk distribuidos por unidades geográficas, la topología recomendada para QPM puede ser la misma.

En cuanto a las diferencias de respuesta esperada por parte del usuario y de niveles de servicio son, por lógica, que un reset iniciado mediante llamada telefónica mostrará un plazo de retardo mayor entre el momento en que el help desk receta la password manualmente y el usuario puede hacer login con su nueva clave, frente a un reset en modo autoservicio mediante el uso de Secure Password Extension accediendo desde la GINA en tiempo de login del usuario. Normalmente en este último caso el proceso de login de usuario se inicia inmediatamente después. Sin embargo, si en ambos casos volvemos a suponer que el reset no se ha realizado en el mismo Controlador de Dominio que está autenticando al usuario y aún no se ha completado la replicación a dicho Controlador de Dominio local, nos encontramos que se tiene que dar el mismo proceso de comunicación desde el PDC con la latencia que le corresponda a cada topología de Controlador de Dominio.

Estas condiciones de rendimiento dan como resultado que, para una red dada, la latencia concreta de un proceso de inicio de sesión solo pueda determinarse de forma empírica habida cuenta de la cantidad de factores que le afectan. Puede ser insignificante o casi imperceptible, o puede ser muy evidente dependiendo de configuración de la red y del site.

Como regla de oro operativa, la idea de crear una infraestructura paralela a la actual regionalización del help desk (salvo que esta función se haya delegado a un nivel local de forma muy descentralizada), es recomendable a la vista de estas consideraciones. En una red de Controladores de Dominio y topologías de site muy eficiente, la centralización de la función de reset de password en base a grandes áreas regionales o incluso en un punto único puede ser factible, pero consideramos más prudente adoptar una disposición que reproduzca la arquitectura primaria de sites de la organización.

CONCLUSIÓN

El aspecto principal a considerar de cara al despliegue de QPM es garantizar que los resets de password se ejecutan en el Controlador de Dominio que valida al usuario con una latencia aceptable. Aunque la arquitectura del Active Directory garantice que la evaluación de la password se efectúa contra la password más reciente en todo el ámbito del dominio, la latencia de replicación puede degradar el rendimiento del proceso de login. Si este impacto deriva de la infraestructura de red que soporta el Active Directory, se recomienda que las instancias de QPM se desplieguen más próximas a los sitios de usuario distribuidos.

Las implicaciones de la duplicación de instancias de QPM en la organización son::

Se ha de informar/enseñar o encaminar a los usuarios hacia el site e QPM local más adecuado

Se recomienda que cada instancia esté próxima a su instancia de SQL Server.

La creación de múltiples instancias de SQL Server fragmenta el proceso de elaboración de informes, ya que esta tarea opera exclusivamente con los datos de su propia instancia.

Con respecto al rendimiento de la aplicación Web, los puntos a considerar son de carácter secundario y pueden evaluarse a partir del rendimiento de aplicaciones Web similares con un elevado número de accesos dentro de la organización.

Acerca de Quest Software, Inc.

Quest Software, Inc., empresa líder en gestión de sistemas de IT corporativos, ofrece productos innovadores que ayudan a las organizaciones a obtener más rendimiento y productividad de sus aplicaciones, bases de datos, infraestructuras Windows y entornos virtuales. Gracias a una profunda experiencia en operaciones de IT y una atención permanente a la mejora continua, Quest ayuda a más de 100.000 clientes en todo el mundo a cumplir con sus máximas expectativas en sus Tecnologías de Información corporativas. Quest ofrece a sus clientes gestión de entornos de cliente y soluciones de virtualización de servidor y desktop mediante sus subsidiarias ScriptLogic y Vizioncore. Quest Software dispone de oficinas en todo el mundo y puede encontrarse en Internet en www.quest.com.

Contacto con Quest Software

Correo: Quest Software, Inc. Sede central: 5 Polaris Way. Aliso Viejo, CA 92656 USA

Sitio Web: www.quest.com

Email: info@quest.com

Teléf.: 949.754.8000 (EE.UU y Canadá)

Consulte nuestra Web si desea información sobre nuestras oficinas regionales o internacionales.

Soporte técnico de Quest

Pueden acceder a Soporte de Quest los clientes que dispongan de una versión de evaluación de un producto de Quest o que hayan adquirido una versión comercial y dispongan de un contrato de mantenimiento en vigor. El Soporte de Quest está disponible de forma permanente a través de SupportLink, nuestro autoservicio Web. Visite SupportLink en la web <http://support.quest.com>

Desde SupportLink, puede hacer lo siguiente:

- Encontrar rápidamente miles de soluciones (artículos/documentos de la Knowledge Base).
- Descargar parches y actualizaciones.
- Solicitar ayuda de un ingeniero de Soporte.
- Registrarse y actualizar su caso, y comprobar su estado.

Consulte la **Global Support Guide** si desea una exposición detallada de los programas de soporte, servicios online, información de contacto y políticas y procedimientos. Esta guía está disponible en: [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)