Tarea de Java y su última versión

* **¿Cuál es la última versión de Java?**

La última versión es Java 8 Update 51 CPU 14 de julio de 2015

* **¿Qué características tiene la última versión de Java?**

Java 8 es la versión más reciente de Java que incluye nuevas características, mejoras y correcciones de bugs para mejorar la eficacia en el desarrollo y la ejecución de programas Java.

##### Características principales de la versión

* Datos IANA 2015e  
  JDK 8u60 contiene datos de zona horaria IANA versión 2015e.

**Corrección de bug:** dns\_lookup\_realm debe estar definido en false por defecto  
El valor de dns\_lookup\_realm del archivo Kerberos' krb5.conf es por defecto false.

* **Corrección del bug:** Agregar nuevas raíces de Comodo a las CA raíz  
  Se han agregado cuatro certificados raíz nuevos para Commodo:
  1. Autoridad de certificación COMODO ECC  
     alias: comodoeccca  
     DN: CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
  2. Autoridad de certificación COMODO RSA  
     alias: comodorsaca  
     DN: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
  3. Autoridad de certificación USERTrust ECC  
     alias: usertrusteccca  
     DN: CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
  4. Autoridad de certificación USERTrust RSA  
     alias: usertrustrsaca  
     DN: CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US

Consulte JDK-8077997 (no público).

* **Corrección del bug:** Agregar nuevas raíces de GlobalSign a las CA raíz  
  Se han agregado dos certificados raíz nuevos para GlobalSign:
  1. CA raíz de GlobalSign ECC - R4  
     alias: globalsigneccrootcar4  
     DN: CN=GlobalSign, O=GlobalSign, OU=GlobalSign ECC Root CA - R4
  2. CA raíz de GlobalSign ECC - R4  
     alias: globalsigneccrootcar5  
     DN: CN=GlobalSign, O=GlobalSign, OU=GlobalSign ECC Root CA - R5

Consulte JDK-8077995 (no público).

* **Corrección del bug:** Agregar Actalis a CA raíz  
  Se ha agregado un nuevo certificado raíz:  
  CA raíz de autenticación Actalis  
  alias: actalisauthenticationrootca  
  DN: CN=Actalis Authentication Root CA, O=Actalis S.p.A./03358520967, L=Milan, C=IT   
  Consulte JDK-8077903 (no público).
* **Corrección del bug:** Agregar nueva raíz de Entrust ECC  
  Se ha agregado un nuevo certificado raíz:  
  Autoridad de certificación raíz de Entrust - EC1  
  alias: entrustrootcaec1  
  DN: CN=Entrust Root Certification Authority - EC1, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US   
  Consulte JDK-8073286 (no público).
* **Corrección del bug:**: Eliminar las raíces de Valicert Class 1 y 2 Policy  
  Se han eliminado dos certificados raíz con claves de 1024 bits:
  1. Autoridad de validación de políticas ValiCert Class 1  
     alias: secomvalicertclass1ca  
     DN: EMAILADDRESS=info@valicert.com, CN=http://www.valicert.com/, OU=ValiCert Class 1 Policy Validation Authority, O="ValiCert, Inc.", L=ValiCert Validation Network
  2. Autoridad de validación de políticas ValiCert Class 2  
     alias: valicertclass2ca  
     DN: EMAILADDRESS=info@valicert.com, CN=http://www.valicert.com/, OU=ValiCert Class 2 Policy Validation Authority, O="ValiCert, Inc.", L=ValiCert Validation Network

Consulte JDK-8077886 (no público).

* **Corrección del bug:** Eliminar las raíces de Thawte antiguas  
  Se han eliminado dos certificados raíz con claves de 1024 bits:
  1. CA de servidor Thawte  
     alias: thawteserverca  
     DN: EMAILADDRESS=server-certs@thawte.com, CN=Thawte Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA
  2. CA de Thawte Personal Freemail  
     alias: thawtepersonalfreemailca  
     DN: EMAILADDRESS=personal-freemail@thawte.com, CN=Thawte Personal Freemail CA, OU=Certification Services Division, O=Thawte Consulting, L=Cape Town, ST=Western Cape, C=ZA

Consulte JDK-8074423 (no público).

* **Corrección del bug:** Eliminar más raíces de Verisign, Equifax y Thawte antiguas  
  Se han eliminado cinco certificados raíz con claves de 1024 bits:
  1. Autoridad de certificación principal pública de Verisign Class 3 - G2  
     alias: verisignclass3g2ca DN: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
  2. CA de servidor Thawte Premium  
     alias: thawtepremiumserverca  
     DN: EMAILADDRESS=premium-server@thawte.com, CN=Thawte Premium Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA
  3. Autoridad de certificación de Equifax Secure  
     alias: equifaxsecureca  
     DN: OU=Equifax Secure Certificate Authority, O=Equifax, C=US
  4. CA-1 de Equifax Secure eBusiness  
     alias: equifaxsecureebusinessca1  
     DN: CN=Equifax Secure eBusiness CA-1, O=Equifax Secure Inc., C=US
  5. CA-1 de Equifax Secure Global eBusiness  
     alias: equifaxsecureglobalebusinessca1  
     DN: CN=Equifax Secure eBusiness CA-1, O=Equifax Secure Inc., C=US

Consulte JDK-8076202 (no público).

* **Corrección del bug:** Eliminar las raíces de CA de TrustCenter antiguas  
  Se han eliminado tres certificados raíz:
  1. CA I de TC TrustCenter Universal   
     alias: trustcenteruniversalcai  
     DN: CN=TC TrustCenter Universal CA I, OU=TC TrustCenter Universal CA, O=TC TrustCenter GmbH, C=DE
  2. CA II de TC TrustCenter Class 2   
     alias: trustcenterclass2caii  
     DN: CN=TC TrustCenter Class 2 CA II, OU=TC TrustCenter Class 2 CA, O=TC TrustCenter GmbH, C=DE
  3. CA II de TC TrustCenter Class 4   
     alias: trustcenterclass4caii  
     DN: CN=TC TrustCenter Class 4 CA II, OU=TC TrustCenter Class 4 CA, O=TC TrustCenter GmbH, C=DE

Consulte JDK-8072958 (no público).

* **Corrección del bug:** RC4 en proveedor SunJSSE obsoleto   
  RC4 se considera un cifrado débil. Los servidores no deben seleccionar RC4 a menos que no haya otro cliente más fuerte en las suites de cifrado solicitadas. Se ha agregado una nueva propiedad de seguridad, jdk.tls.legacyAlgorithms, para definir los algoritmos antiguos en la implantación de Oracle JSSE. Se han agregado los algoritmos relacionados con RC4 a la lista de algoritmos antiguos. Consulte JDK-8074006 (no público).
* **Corrección del bug:** Prohibir suites de cifrado RC4  
  RC4 es ahora un cifrado no seguro. Se han eliminado las suites de cifrado RC4 de las listas de suites de cifrado activadas por defecto en el cliente y del servidor para la implantación de Oracle JSSE. Estas suites de cifrado aún se pueden activar con los métodos[SSLEngine.setEnabledCipherSuites()](http://docs.oracle.com/javase/8/docs/api/javax/net/ssl/SSLEngine.html#setEnabledCipherSuites-java.lang.String:A-) y [SSLSocket.setEnabledCipherSuites()](http://docs.oracle.com/javase/8/docs/api/javax/net/ssl/SSLSocket.html#setEnabledCipherSuites-java.lang.String:A-). Consulte JDK-8077109 (no público).
* **Corrección del error:** Comprobación de certificación mejorada  
  Con esta corrección, la identificación de punto final de JSSE no realiza la consulta de nombre inversa para las direcciones IP por defecto en JDK. Si una aplicación necesita realizar consulta de nombre inversa para las direcciones IP raíz en las conexiones SSL/TLS y encuentra un problema de compatibilidad de identificación de punto final, se puede utilizar la propiedad del sistema "jdk.tls.trustNameService" en la consulta de nombre inversa. Tenga en cuenta que si el servicio de nombres no es de confianza, al activar la consulta de nombre inversa se pueden producir ataques de MITM. Consulte JDK-8067695 (no público).

##### Fecha de caducidad de Java

La fecha de caducidad de 8u51 es el 20 de octubre de 2015. Java caduca cada vez que hay disponible una nueva versión con correcciones a las vulnerabilidades de seguridad. Para los sistemas que no se pueden ejecutar en servidores Oracle, un mecanismo secundario se encargará de caducar esta versión de JRE (versión 8u51) el 20 de noviembre de 2015. Una vez se haya cumplido cualquiera de las condiciones (la nueva versión esté disponible o se haya alcanzado la fecha de caducidad) Java enviará mensajes de advertencia y recordatorios sobre la nueva versión.

##### Correcciones de bugs

Esta versión incluye correcciones para vulnerabilidades de seguridad. Para obtener más información, consulte el [Asesor de actualización de parche crítico de Oracle Java SE](http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html#AppendixJAVA).

* **¿Cuándo se espera la próxima versión de java?**

Actualización limitada de Java 8 Update 60 18 de agosto de 2015