

Oracle[®] Solaris Studio 12.4: Security Guide

ORACLE[®]

Part No: E37092
October 2014

Copyright © 2013, 2014, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2013, 2014, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Contents

Using This Documentation	5
1 Oracle Solaris Studio Security Information	7
Oracle Solaris Studio Security Considerations	7
Precautions for System Administrators and Users Installing Oracle Solaris Studio	8
Precautions for Developers	8
Using Oracle Solaris Studio Libraries	8
Using Remote Development in the IDE	9
Using Remote Development in Performance Analyzer	9

Using This Documentation

- **Overview** – Describes the security issues users need to be aware of with this Oracle Solaris Studio 12.4 release.
- **Audience** – Application developers, system developers, architects, support engineers
- **Required knowledge** – Programming experience, software development testing, aptitude to build and compile software products

Product Documentation Library

Documentation, late-breaking information, and known issues for this product are included in the documentation library at http://docs.oracle.com/cd/E37069_01.

The known issues for this Oracle Solaris Studio release can be found in the chapter “[Known Problems, Limitations, and Workarounds in This Release](#)” in “[Oracle Solaris Studio 12.4: Release Notes](#)”. For more information about compilers and tools, see the relevant man pages or Help.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Feedback

Provide feedback about this documentation at <http://www.oracle.com/goto/docfeedback>.

Oracle Solaris Studio Security Information

This document includes information about the following:

- [“Oracle Solaris Studio Security Considerations” on page 7](#)
- [“Precautions for System Administrators and Users Installing Oracle Solaris Studio” on page 8](#)
- [“Precautions for Developers” on page 8](#)
- [“Using Oracle Solaris Studio Libraries” on page 8](#)
- [“Using Remote Development in the IDE” on page 9](#)
- [“Using Remote Development in Performance Analyzer” on page 9](#)

Oracle Solaris Studio Security Considerations

Oracle Solaris Studio is a suite of compilers, debuggers, and analysis tools, and an integrated development environment (IDE), for developing, debugging, and tuning applications for the Solaris and Linux platforms. Like other development tools, the Oracle Solaris Studio compilers and tools are intended to be used in an environment that is isolated from production environments since these tools can be accessed by users to manipulate applications during execution. While production environments are typically the focus of security considerations, developer tools and development environments should also be considered from a security perspective.

System administrators play an important role in determining which assets require protection and putting in place controls and policies to protect these assets. By itself, Oracle Solaris Studio does not provide any access to assets or operating environment features that the user does not already have. The risk that Oracle Solaris Studio adds is that it allows users who have gained un-entitled access to assets or systems by means that don't include Oracle Solaris Studio to use the capabilities of the Oracle Solaris Studio developer tools to cause a security breach. A user who is running the Oracle Solaris Studio tools has access to all of the capabilities exploited by the debuggers and analyzers by using the operating system interfaces directly. But the Oracle Solaris Studio tools make it easier to understand and use these operating system capabilities to probe the internals of applications, manipulate hardware registers, memory, and stack, and control the execution of an application.

Precautions for System Administrators and Users Installing Oracle Solaris Studio

Oracle Solaris Studio compilers and tools are intended primarily for use in development environments. If Oracle Solaris Studio is needed in a production environment (for example, to debug a production application or analyze a performance bottleneck), take measures to limit access to these tools. Install only the Oracle Solaris Studio components needed for development or production tasks. The Oracle Solaris Studio package installer lets you select which Studio components to install.

Oracle Solaris Studio IDE lets you install non-Oracle supported plugins. Before downloading any third-party software such as these plugins, assess the security safety of such plugins.

Keep installations of Oracle Solaris Studio current with the latest patches, especially security patches.

Oracle Solaris Studio Performance Analyzer requires elevated privileges for certain debugging and analysis tasks. Provide these privileges through temporary accounts, and monitor these accounts accordingly.

Precautions for Developers

Oracle Solaris Studio compilers and tools create output files such as logs, core dumps, and object files. The permissions on these files are set using the user's default permissions. To protect the output files from unwanted access, limit the default permissions to allow only access that is absolutely needed. Users set the default permissions using the Solaris and Linux `umask` command.

Using Oracle Solaris Studio Libraries

Oracle Solaris Studio includes a set of libraries that provide runtime support on supported platforms: performance libraries targeted for compute-intensive applications, and debugging and performance analysis libraries used in tuning applications in a development environment. Performance and runtime libraries are used in production environments and are installed by system administrators as required for the applications that will be run.

As the name implies, performance libraries are optimized for performance, which means that data checking is kept to a minimum insuring maximum performance. When using performance libraries, the application developer is responsible for validating data being passed to these libraries.

Using Remote Development in the IDE

Using remote build hosts in the IDE requires login credentials. Compromised security on the client system running the IDE might lead to unauthorized access of remote server hosts. In shared desktop environments, storing login credentials is not advisable for situations requiring a high level of security.

Another area of consideration with respect to remote development is the caching of source code on client systems during remote development. To increase IDE performance and responsiveness, the remote development feature in the IDE caches files from the server, including source code, on the client machine. The cache folder on the client machine is `user_directory/var/cache/remote-files`.

On Solaris and Linux platforms, `user_directory` is: `~/solstudio/ide-version-OS-architecture` (for example, `~/solstudio/ide-12.4-SunOS-i386`).

On Microsoft Windows platforms, `user_directory` is `~/Application Data/solstudio/dd-version`.

On Mac OS X platforms, `user_directory` is `~/Library/Application/Support/solstudio/dd-version`.

In sensitive security environments, take care with this cache folder, including deletion or encryption.

Using Remote Development in Performance Analyzer

The Performance Analyzer remote client requires a user name and password to connect to the remote server. The user name is stored to the disk in the user's home directory, but the password is never stored to the disk.

The Performance Analyzer remote client uses a Java implementation of ssh (jsch version 0.1.49) for connection to the sshd server on the remote host.

The Performance Analyzer client stores information in the file `~/solstudio/analyzer-12.4/analyzer.xml` on all client platforms including Oracle Solaris, Linux, MacOS, and Microsoft Windows.

