Tivoli.

Security and Compliance Analytics

Release Notes

for release version 1.0

February 23, 2011

IBM

Note: Before using this information and the product it supports, read the information in Notices.

Contents

Introduction 1
System Requirements 1
Setup Considerations 2
Late-breaking Information 3
Known Issues 4
Support 7
Additional Documentation 7
Technical Support 7
Notices 8

Introduction

Tivoli® Endpoint Manager for Security and Compliance Analytics (SCA) is a web-based application for security and risk assessment. The system archives security compliance check results to identify configuration issues and report levels of compliance toward security configuration goals.

SCA is a component of Tivoli® Endpoint Manager for Security and Compliance, which includes libraries of technical controls and tools based on industry best practices and standards for endpoint and server security configuration. The technical controls enable continuous, automated detection and remediation of security configuration issues. More information about the technical controls is available in the Security Configuration Management documentation on the BigFix support website at http://support.bigfix.com/resources.html#SCM.

Report views and tools for managing the SCM checks are provided by SCA.

SCA generates the following reports, which can be filtered, sorted, grouped, customized using any set of Tivoli Endpoint Manager properties, and exported:

- **Overviews** of Compliance Status and History
- **Checklists**: Compliance Status and History
- **Checks**: Compliance Status, Values, and History
- **Computers**: Compliance Status, Values, and History
- **Computer Groups**: Compliance Status and History
- **Exceptions**: Management, Status, and History

System Requirements

Your SCA deployment must be configured according to the following requirements:

Minimum supported browser versions:

- Internet Explorer 7.0 or 8.0
- FireFox 3

Minimum Tivoli Endpoint Manager component versions:

- Server and Console V7.2.5.21, 8.0, or 8.1
- Web Reports V7.2.5.21, 8.0, or 8.1
- Windows Client V7.2.5.21, 8.0, or 8.1
- UNIX Client V7.2.5.21, 8.0, or 8.1

SCA server operating system requirements:

- Microsoft Windows Server 2003, Microsoft Windows Server 2008, or Microsoft Windows Server 2008 R2
- Oracle Java JDK 6 update 18 or greater (available at http://www.oracle.com/technetwork/java/javase/downloads/)

SCA database server requirements:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008

SCA server, SCA database, and Tivoli Endpoint Manager database user permissions:

- To install and configure the SCA server, you must have Administrator privileges on the target SCA server, sa permissions on the target SCA database server, and sa permissions are recommended on the associated Tivoli Endpoint Manager database server (although “SELECT” and “EXECUTE” permissions on the BFEnterprise and Master databases are sufficient after the initial install and configuration is complete).

SCM mastheads and fixlet sites:

- You may have a range of “legacy” BigFix fixlets, Tivoli Endpoint Manager fixlets, and custom fixlets for security compliance in your deployment. These will continue to function correctly, however, only certain fixlets will appear within the SCA reports.

- For a current list of SCM content sites that are supported with SCA, please refer to the Knowledge Base article: http://support.bigfix.com/cgi-bin/kbdirect.pl?id=1770

Setup Considerations

During setup, consider your desired deployment size according to your hardware. Use the recommendations below as general guidance.

- A 2-3 GHz CPU with 4 GB RAM is sufficient for a few hundred Tivoli Endpoint Manager clients, but the requirements scale with the number of computers. To support up to 250,000 computers, you will likely need 16 cores and 64 GB RAM.

- Although you can install the SCA server on the same computer as your SQL Server, because SQL Server typically consumes a significant amount of memory, it may starve the SCA application. Carefully manage the SQL Server memory and use a dedicated SQL Server computer if necessary.

- To help manage your database storage requirements, consider setting the SCA database to use ‘simple’ transaction logging, and you may want to regularly shrink or truncate the transaction log. Please refer to Microsoft SQL Server documentation for additional information.

- A minimum of 1 GB free disk space is needed by the SCA application server.

- A minimum of 20 GB free disk space is needed by the SCA database server for one thousand Tivoli Endpoint Manager clients.

- Plan for 1 GB free disk space for the SCA database server for each 1K additional clients. However, growth is compounded by many factors, such as the number of computer groups, the number of checks, and the number of exceptions you have in your deployment.

- The above disk space recommendations are based on the following assumptions:
  - Your deployment environment has an average of 2000 SCM checks
  - 2% check result change over each import (daily)
  - 5% of the checks have associated exceptions managed in SCA
  - All measured value analyses for all checks are activated
  - Your deployment contains one year of archived compliance data

You can add additional disk space for future growth of endpoint and additional security compliance checks.

> ***Note: The key elements that affect disk space size are based on (# check results and their compliance change over time) + (Computer Group * Checks * # of imports over time) + (# exceptions + # Measured Values)***

Late-breaking Information

From time-to-time, documentation is updated through Knowledge Base articles. At the time of publishing, the following relevant Knowledge Base Articles were available:

- For a list of SCM content sites supported with SCA:
  http://support.bigfix.com/cgi-bin/kbdirect.pl?id=1770
- To set up a self-signed SSL certificate for your SCA server, or if you wish to use a certificate already trusted within your organization:
  http://support.bigfix.com/cgi-bin/kbdirect.pl?id=1783
- For guidance about how to secure file and database permissions for your SCA server:
  http://support.bigfix.com/cgi-bin/kbdirect.pl?id=1784
- To collect verbose logging information on your SCA server:
  http://support.bigfix.com/cgi-bin/kbdirect.pl?id=1785

Note: Additional Knowledge Base articles may be added after this document is published. You may search the Knowledge Base for additional information at http://support.bigfix.com/.

Known Issues

Review the contents of the list of **Known Issues** for **Tivoli Endpoint Manager for Security and Compliance Analytics 1.0** below before contacting Support or reporting new issues.

Issue	Category	Description of Issue	Workaround
40946	Performance	Exception Results and Check Results pages load very slowly with large datasets if the "State" column is visible.	By default, the “State” column is not visible because it is redundant with the “Compliance” column. Only make it visible if you need to export the data to CSV.
40999	Navigation	Checklist and Check "Total Compliance" columns show historical counts, but link to reports that show the current status.	After following the link to the relevant report, reapply filters and configurations in order to access historical information.
41159	Export	CSV exports do not include the "Compliance" column even though it is visible on the screen.	The "Compliance" column encapsulates historical information that isn't practical to include in the current CSV export format. To export similar information, add "Total Compliance" columns to your report and use time filters to show data for the appropriate date, then export to CSV.
37492, 39296	Export	CSV Export of Check Results "State" column shows numeric value instead of English description.	Use the following mapping to understand the results: 0 - Compliant; 1 - Excepted (Compliant); 2 - Excepted (Non-Compliant); 3 - Non-Compliant; 4 - Not Applicable.
41271	Exceptions Management	The number of checks and the number of computers displayed in each row in the Exceptions History form for an exception show the current count, not the count at the time the edit represented by the row was completed.	The complete audit log is archived in the database and can be retrieved through SQL queries. Please contact customer support if you need assistance.
41133	Configure View	Filtering UI contains confusing "ID" and "Computer ID" options	"ID" refers to "Datasource ID", and is irrelevant when your deployment is only connected to a single datasource. "Computer ID" refers to the GUID number used for computers in the Tivoli Endpoint Manager system.
36576	Configure View	No visual indicator when report data is being filtered	Click "Configure View" to see the filters in effect for a given report.
38933	Configure View	Filtering on computer groups before they have been imported leads to empty reports.	After creating a computer group, wait until an initial import of the group is complete before using the group in the filtering interface

38989	Export	CSV export column order doesn't reflect column order in source report.	Use a spreadsheet editing tool to re-arrange column order in CSV exports.
39386	Report display	Adding too many columns to reports leads to poor layout.	Adjust the columns to be shown in your report so that the most important data fits within available screen space.
39388	Exception Management	Create Exception page doesn't clear error warnings after failed exception creation.	If the error has been corrected, clicking the "Create" button will create the exception even if the error message persists.
40255	Configure View	Entering invalid "Source Release Date" filter causes "unknown error".	Choose a valid date using the built in date picker.
40265	Measured Values	Impossible to tell if empty measured values indicate that no value has been defined or that the measured value analysis is not activate.	Log in to the Tivoli Endpoint Manager Console and search in Analyses by check name to find the relevant measured value analysis to see if it has been activated.
40279	Configure View	Clicking the "X" to close the "Configure View" dialog will leave configuration changes set in the dialog even though they haven't been applied to the report.	To return the "Configure View" dialog to a state that reflects the current report configuration, navigate away from the report and then navigate back to it.
40313	Import	Import fails with "Sequel::DatabaseConnectionError" message if the associated Web Reports database cannot be reached.	Either re-establish your connection to the linked Web Reports database, or remove the connection using the Datasource management page.
40318	Configure View	"Configure View" column picker shows all possible columns regardless of data included in the report.	When you see columns with no data, the most likely reason is that the column is not relevant for the checklist you are reporting on. Remove the column.
40544	User Management	"User name has been taken" error on attempting to re-create a user that has previously existed.	Use a different user name.
40781	Computer Properties Management	"Create Computer Property" drop down menu contains all "measured value" properties.	These properties are included in the reports by default. You do not need to add them using the Computer Properties management interface.
40815	Navigation	Using a URL to a deleted report generates a mis-rendered page.	None.
40880	Saved Reports	After modifying a Saved Report through the "Configure View" dialog, there is no indication that the current report is different from the original Saved Report.	Save the report with a new name in order to differentiate it from the old report.
40884	User Management	If a linked Web Reports user is deleted from SCA, there is no way to link that user again.	Manually create a new user account for that user. It will not be linked to Web Reports.

41235	Installation	Application will not run if the install path contains a "+"	Install the product in a directory without “+” in the path.
39355	User Management	If a username in Web Reports is changed while that username is linked to a SCA user, a new user will be created in SCA for the new username.	If you change linked user names, you will need to use the SCA User Management form to entitle the new user to computers.
41522	Report display	When using the web browser “view” commands to zoom in or out, the report layout may break or columns may appear blank.	Reset the browser zoom level back to normal/default.
41418	Check/Fixlet Properties	Editing certain fixlet properties, such as “Category,” using the Tivoli Endpoint Manager Console, has no effect on these properties when displayed in SCA.	If you would like to edit the properties of fixlets (i.e. checks), please contact customer support for assistance.
40263, 41275	Configure View	Cannot sort or filter on Measured Values or Desired Values columns.	None.
38890	User Management	The set of permissions that can be granted to non-Administrator users is very limited compared to the Administrator privileges.	None.
41366	Exception Reporting	Exceptions with expiration date of “Never” do not display in reports filtered by date.	None.
40667, 35926	Database configuration	It is not possible to change the datasource of a SCA installation once it is configured.	To use a different datasource, you must reinstall or reinitialize the SCA server configuration. Please contact customer support for assistance.
40377	Report display	Checklists and checks that are not subscribed to any computers appear in the reports, correctly showing zero computers and no compliance results.	If you have checklists that are not in use, you may remove them using the Tivoli Endpoint Manager Console.
41204	Configure View	If you have a long list of items in a filter menu, it may be constrained by the size of your browser window.	Enlarge your browser window or use the browser View menu to zoom out to fit the Configure View filter menu.

Support

Additional Documentation

- Security and Compliance Analytics User's Guide
- Security and Compliance Analytics Setup Guide
- Security Compliance Setup Guide
- Security Compliance User's Guide
- SCAP QuickStart Guide
- SCAP User's Guide
- Security Compliance Benchmarks Guide

Technical Support

Tivoli Endpoint Manager technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- Support Site - http://support.bigfix.com
- Documentation - http://support.bigfix.com/resources.html
- Knowledge Base - http://support.bigfix.com/search.html
- Forums and Communities - http://forum.bigfix.com/

Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs

(including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.