Tivoli Security Compliance Manager

Version 5.1 – April, 2006

Collector and Message Reference Addendum

Table of Contents

Preface **4**
What this book contains 4
Chapter 1. Policies **5**
File Integrity policy 5
Notices **8**
Additional notices 9
Trademarks 10

Preface

The *IBM Tivoli Security Compliance Manager Collector and Message Reference Addendum* describes the following:

- The File Integrity policy checks the specified collection of files on the client's machine and compares it with the collection situated on the Golden host

Documentation for previously developed collectors that are used in File Integrity policy can be found in the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication.

The information in this book will be added to the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication the next time that publication is updated. This book is being used to provide documentation of new policies and new collectors until that time.

What this book contains

This document contains the following chapters:

- Chapter 1, Policies

  Provides information on the File Integrity policy.

Chapter 1.Policies

This chapter documents the following policy:

- File Integrity policy

File Integrity policy

The File Integrity policy template is a policy for checking compliance of a file collection on scanned desktop with a file collection on the Golden Host.

Deployment information for File Integrity policy template

The IBM Tivoli Security Compliance Manager File Integrity policy template consists of collectors and compliance queries that can be used to determine if a Windows™ desktop system complies with specific security requirements.

See the *IBM Tivoli Security Compliance Manager Administration Guide* for details regarding installing and deploying policies.

Policy overview

The queries included in this policy check the following items:

- Identifies files on the target system matching the collection criteria that do not exist on the reference system.
- Identifies files located both on the reference system and the target system with checksums that do not match.
- Identifies files on the reference system that do not exist on the target system.

Configuring this policy for your deployment

To configure the File Integrity policy for your environment, do the following:

- Specify a hostname of a computer which is the reference machine in your network.
- Update the following parameters in any.any.InventoryV1 so it matches your requirements:

  “INCLUDE_DIRECTORY”,

  “EXCLUDE_DIRECTORY”,

  “INCLUDE_FILE_TYPES”,

  “EXCLUDE_FILE_TYPES”

Compliance queries

The following sections contain additional information on all of the compliance queries contained within the File Integrity policy.

Extra Files

Examined system must not contain any extra files within specified directories.

Table 1.Account: Password Length Restriction Attributes

Priority	Normal
Collector instance name	InventoryV1.

Violation message:

The file {1} does not exist on the reference machine.

Note: The {1} in the message is replaced with the value of FILE_NAME as selected in the SQL.

SQL query:

```
SELECT b.cli_id, b.file_name, b.file_size, a.path_id
FROM
    (SELECT distinct file_name, path_id FROM jac_data.cit_file_desc_v1
     EXCEPT
     (SELECT file_name, path_id FROM (SELECT hostname, cli_id, file_name, file_size, path_id
      FROM jac_data.cit_file_desc_v1
            WHERE hostname='$(Golden Client Hostname)'
) AS RIGHT_LIST)) a
         INNER JOIN
                jac_data.cit_file_desc_v1 b
         ON (a.file_name=b.file_name AND a.path_id=b.path_id)
```

File Mismatch

Examined system must contain exactly the same files within specified directories.

Table 2.Account: Password Length Restriction Attributes

Priority	Normal
Collector instance name	InventoryV1.

Violation message:

File {1} (Size = {2}, Chksum = {3}) does not match reference file with Size = {4}, Chksum = {5}.

Note: The {1} in the message is replaced with the value of FILE_NAME, {2} is replaced with the value of FILE_SIZE, {3} is replaced with the FILE_ID, {4} is replaced with the with the FILE_SIZE gathered from the Golden Host, {5} is replaced with the FILE_ID gathered from the Golden Host.

SQL query:

```
SELECT DISTINCT c.cli_id, c.file_name, c.file_size, c.file_id, c.m_time,
          GOLDEN.file_size, GOLDEN.file_id, GOLDEN.m_time
FROM (SELECT a.cli_id, file_id, file_size, file_name, permissions, path_id, a.M_TIME
            FROM jac_data.cit_file_desc_v1 a
            INNER JOIN jac_sys.clients b ON a.cli_id=b.cli_id
            WHERE hostname='$(Golden Client Hostname)') AS GOLDEN,
jac_data.cit_file_desc_v1 c
WHERE ((c.file_id <> GOLDEN.file_id OR c.permissions <> GOLDEN.permissions)
AND (c.file_name = GOLDEN.file_name AND c.path_id = GOLDEN.path_id))
```

Missing Files

Examined system must not miss any files within specified directories.

Table 3.Account: Password Length Restriction Attributes

Priority	Normal
Collector instance name	InventoryV1.

Violation message:

The file {1} does not exist on the target system.

Note: The {1} in the message is replaced with the value of FILE_NAME as selected in the SQL.

SQL query:

```
SELECT DISTINCT b.cli_id, RIGHT_LIST.file_name, RIGHT_LIST.file_size, RIGHT_LIST.path_id
FROM
      (SELECT DISTINCT cli_id, value(file_name, '') AS file_name,
       file_size, path_id
      FROM jac_data.cit_file_desc_v1 WHERE
      hostname='$(Golden Client Hostname)')
      AS RIGHT_LIST, jac_data.cit_file_desc_v1 b
WHERE
      (RIGHT_LIST.file_name, RIGHT_LIST.path_id)
      NOT IN
      (SELECT DISTINCT value(file_name, ''), path_id
            FROM jac_data.cit_file_desc_v1 c
            WHERE c.cli_id=b.cli_id)
```

Collector Instances and Parameters

The table below associates each collector instance with a specific collector and lists any parameters it has and the values for those parameters. Each collector instance is scheduled to run once a day at a random time.

Table 4.Collector instances and parameters for File Integrity policy

Instance name	Collector name	Parameter name	Parameter value
InventoryV1	any.any.InventoryV1	1. INCLUDE_DIRECTORY 2. EXCLUDE_DIRECTORY 3. INCLUDE_FILE_TYPES 4. EXCLUDE_FILE_TYPES	Every parameter should be set accordingly to client's requirements, more information can be found in InventoryV1 documentation

Notices

This information was developed for products and services offered in the U.S.A. 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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
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:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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
USA

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

The licensed program describe in this information 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.

Customers are responsible for ensuring their own compliance with various laws such as the Graham-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal, accounting or auditing advice, or represent or warrant that its products or services will ensure that customer is in compliance with any law.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Additional notices

THIRD PARTY LICENSE TERMS AND CONDITIONS, NOTICES AND INFORMATION

The license agreement for this product refers you to this file for details concerning terms and conditions applicable to third party software code included in this product, and for certain notices and other information IBM must provide to you under its license to certain software code. The relevant terms and conditions, notices and other information are provided or referenced below. Please note that any non-English version of the licenses below is unofficial and is provided to you for your convenience only. The English version of the licenses below, provided as part of the English version of this file, is the official version.

Notwithstanding the terms and conditions of any other agreement you may have with IBM or any of its related or affiliated entities (collectively “IBM”), the third party software code identified below are “Excluded Components” and are subject to the following terms and conditions:

(a) the Excluded Components are provided on an “AS IS” basis;

(b) IBM DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS WITH RESPECT TO THE EXCLUDED COMPONENTS, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE;

(c) IBM will not be liable to you or indemnify you for any claims related to the Excluded Components; and

(d) IBM will not be liable for any direct, indirect, incidental, special, exemplary, punitive or consequential damages with respect to the Excluded Components.

Notice for Apache Software Foundation

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Notice for the MD5 Message-Digest Algorithm MD5 Message-Digest Algorithm.

The Program includes software developed by RSA Data Security, Inc. The portions of the Program which are based on software developed by RSA Data Security, Inc. are Copyright (c) 1991-2 RSA Data Security, Inc. All rights reserved. IBM obtained the MD5 Message-Digest Algorithm under the terms and conditions of the following license from RSA Data Security, Inc.:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AFS
AIX
DB2
DB2 Universal Database
Domino
IBM
IBM logo
iSeries
pSeries
Lotus
SmartSuite
Tivoli
Tivoli logo
WebSphere
xSeries
zSeries

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.