

**IBM Tivoli Security Compliance Manager,  
Version 5.1  
Warehouse Enablement Pack, Version 1.1  
Implementation Guide  
for Tivoli Data Warehouse, Version 1.2**

**Note:**

Before using this information and the product it supports, read the information in Notices on page 25.

**First Edition (June 2004)**

This edition applies to IBM Tivoli Security Compliance Manager 5.1 and to all subsequent releases and modifications until otherwise indicated in new editions.

**© Copyright International Business Machines Corporation 2004. All rights reserved.**

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>1 About this guide.....</b>	<b>1</b>
1.1 Who should read this guide .....	1
1.2 Publications.....	1
1.2.1 IBM Tivoli Security Compliance Manager 5.1 library .....	1
1.2.2 Tivoli Data Warehouse library .....	2
1.2.3 Related publications.....	2
1.2.3.1 IBM Redbooks .....	2
1.2.3.2 IBM DB2, DB2 Data Warehouse Center, and DB2 Warehouse Manager library .....	3
1.2.4 Accessing publications online.....	4
1.2.5 Ordering publications .....	4
1.3 Accessibility .....	4
1.4 Contacting software support.....	4
1.5 Typeface conventions .....	4
 <b>2 Overview .....</b>	 <b>6</b>
2.1 Overview of Tivoli Data Warehouse.....	6
2.2 Overview of IBM Tivoli Security Compliance Manager warehouse pack .....	8
 <b>3 Reports .....</b>	 <b>10</b>
 <b>4 Installing and configuring the warehouse pack.....</b>	 <b>13</b>
4.1 Prerequisite hardware and software .....	13
4.2 Product notes and limitations .....	13
4.3 Database-sizing considerations.....	13
4.4 Pre-installation procedures .....	13
4.5 Installation of the warehouse pack .....	13
4.6 Post-installation procedures.....	14
4.7 Uninstallation of the warehouse pack.....	14
4.8 Multiple data centers .....	15
 <b>5 Maintenance and problem determination .....</b>	 <b>16</b>
5.1.1 Data mart .....	16
5.2 Extraction control (table Extract_Control).....	16
5.3 Problem determination.....	16
 <b>6 ETL processes.....</b>	 <b>17</b>
6.1 HCV_m05_Build_Mart_Process .....	17
 <b>7 Central data warehouse information .....</b>	 <b>20</b>
 <b>8 Data mart schema information.....</b>	 <b>21</b>
8.1 Data mart HCV_TWH_MART data mart.....	21
8.2 Star schemas .....	21
8.2.1.1 HCV Hourly Tivoli Security Compliance Manager event star schema .....	21
8.2.1.2 Fact table HCV.F_Event_Hour.....	22
HCV Hourly Tivoli Security Compliance Manager Event Star Schema .....	22
8.2.1.3 Fact table HCV.F_Event_Day.....	22

HCV Daily Tivoli Security Compliance Manager Event Star Schema .....	22
8.2.1.4 Fact table HCV.F_Event_Week.....	23
HCV Weekly Tivoli Security Compliance Manager Event Star Schema .....	23
8.2.1.5 Fact table HCV.F_Event_Month.....	23
HCV Monthly Tivoli Security Compliance Manager Event Star Schema .....	23
<b>8.3 Metric dimension tables .....</b>	<b>24</b>
8.3.1 HCV.D_Event_METRIC.....	24
<b>8.4 Dimension tables.....</b>	<b>24</b>
8.4.1 Dimension table HCV.D_CLASSCAT .....	24
8.4.2 Dimension table HCV.D_DST_HOST .....	24
8.4.3 Dimension table HCV.D_SRC_HOST .....	25
<b>9 Notices .....</b>	<b>26</b>

# 1 About this guide

This document describes the warehouse enablement pack, version 1.1 for IBM® Tivoli® Security Compliance Manager 5.1. This warehouse enablement pack is created for Tivoli Data Warehouse, Version 1.2.

With this warehouse enablement pack (hereafter referred to as warehouse pack), you can pull data from the central data warehouse and load it into the IBM Tivoli Security Compliance Manager data mart and provide reports.

## 1.1 Who should read this guide

This guide is for people who do any of the following activities:

- Plan for and install the warehouse pack
- Use and maintain the warehouse pack and its reports
- Create new reports
- Create additional warehouse packs that use data from this warehouse pack

Administrators and installers should have the following knowledge or experience:

- Basic system administration and file management of the operating systems on which the components of Tivoli Data Warehouse are installed
- An understanding of the basic concepts of relational database management
- Experience administering IBM DB2® Universal Database

Additionally, report designers and warehouse pack creators should have the following knowledge or experience:

- An understanding of the source data and application
- Data warehouse information and design, extract, transform, and load (ETL) processes, and online analytical processing (OLAP)

## 1.2 Publications

This section lists publications in the Tivoli Data Warehouse library and other related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

The following sets of documentation are available to help you understand, install, and manage this warehouse pack:

- IBM Tivoli Security Compliance Manager
- Tivoli Data Warehouse
- IBM DB2, DB2 Data Warehouse Center, and DB2 Warehouse Manager
- IBM Redbooks

### 1.2.1 IBM Tivoli Security Compliance Manager 5.1 library

The following documents are available in the Tivoli Security Compliance Manager 5.1 library:

- *IBM Tivoli Security Compliance Manager Version 5.1 Release Notes*, GI11-4695-00  
Provides late-breaking information about IBM Tivoli Security Compliance Manager.
- *IBM Tivoli Security Compliance Manager Version 5.1 Read this First*, GI11-4696-00
- Provides a list of CDs provided with the product, as well as pointers to documentation and product information on the Web.

- *IBM Tivoli Security Compliance Manager Version 5.1 Installation Guide: All Components*, GC32-1592-00  
Provides information about installing all components of the product.
- *IBM Tivoli Security Compliance Manager Version 5.1 Installation Guide: Client component*, GC32-1593-00  
Provides information about installing the client component of IBM Tivoli Security Compliance Manager 5.1.
- *IBM Tivoli Security Compliance Manager Version 5.1 Administration Guide*, SC32-1594-00  
Provides information about administering and using the product. Also provides troubleshooting information and a reference for collectors.
- *IBM Tivoli Security Compliance Manager Version 5.1 Collector Development Guide*, SC32-1595-00  
Provides information about designing and writing a collector for use with Tivoli Security Compliance Manager.

## 1.2.2 Tivoli Data Warehouse library

The following documents are available in the Tivoli Data Warehouse library. The library is available online, as described in “Accessing publications online” on page 4.

- *Tivoli Data Warehouse Release Notes*, SC32-1399  
Provides late-breaking information about Tivoli Data Warehouse and lists hardware requirements and software prerequisites.
- *Installing and Configuring Tivoli Data Warehouse*, GC32-0744  
Describes how Tivoli Data Warehouse fits into your enterprise, explains how to plan for its deployment, and gives installation and configuration instructions. It contains maintenance procedures and troubleshooting information.
- *Enabling an Application for Tivoli Data Warehouse*, GC32-0745  
Provides information about connecting an application to Tivoli Data Warehouse. This book is for application programmers who use Tivoli Data Warehouse to store and report on their application data, data warehousing experts who import Tivoli Data Warehouse data into business intelligence applications, and customers who put their local data in Tivoli Data Warehouse. This document is available only from the IBM Web site.
- *Tivoli Data Warehouse Messages*, SC09-7776  
Lists the messages generated by Tivoli Data Warehouse, and describes the corrective actions you should take.

## 1.2.3 Related publications

The following sections describe additional publications to help you understand and use Tivoli Data Warehouse.

### 1.2.3.1 IBM Redbooks

IBM Redbooks are developed and published by the IBM International Technical Support Organization, the ITSO. They explore integration, implementation, and operation of realistic customer scenarios. The following Redbooks contain information about Tivoli Data Warehouse:

- *Introduction to Tivoli Enterprise Data Warehouse*, SG24-6607-00

Provides a broad understanding of Tivoli Data Warehouse. Some of the topics that are covered are concepts, architecture, writing your own extract, transform, and load processes (ETLs), and best practices in creating data marts.

- *Planning a Tivoli Enterprise Data Warehouse Project*, SG24-6608-00

Describes the necessary planning you must complete before you can deploy Tivoli Data Warehouse. The guide shows how to apply these planning steps in a real-life deployment of a warehouse pack using IBM Tivoli Monitoring. It also contains frequently used Tivoli and DB2 commands and lists troubleshooting tips for Tivoli Data Warehouse.

### 1.2.3.2 IBM DB2, DB2 Data Warehouse Center, and DB2 Warehouse Manager library

The DB2 library contains important information about the database and data warehousing technology provided by IBM DB2, DB2 Data Warehouse Center, and DB2 Warehouse Manager. Refer to the DB2 library for help in installing, configuring, administering, and troubleshooting DB2, which is available on the IBM Web site:

<http://www.ibm.com/software/data/db2/library/>

After you install DB2, its library is also available on your system.

The following DB2 documents are particularly relevant for people working with Tivoli Data Warehouse:

- *IBM DB2 Universal Database for Windows Quick Beginnings*, GC09-2971  
Guides you through the planning, installation, migration (if necessary), and setup of a partitioned database system using the IBM DB2 product on Microsoft Windows.
- *IBM DB2 Universal Database for UNIX Quick Beginnings*, GC09-2970  
Guides you through the planning, installation, migration (if necessary), and setup of a partitioned database system using the IBM DB2 product on UNIX.
- *IBM DB2 Universal Database Administration Guide: Implementation*, SC09-2944  
Covers the details of implementing your database design. Topics include creating and altering a database, database security, database recovery, and administration using the Control Center, which is a DB2 graphical user interface.
- *IBM DB2 Universal Database Data Warehouse Center Administration Guide*, SC26-9993  
Provides information on how to build and maintain a data warehouse using the DB2 Data Warehouse Center.
- *IBM DB2 Warehouse Manager Installation Guide*, GC26-9998  
Provides information on how to install the following Warehouse Manager components: Information Catalog Manager, warehouse agents, and warehouse transformers.
- *IBM DB2 Universal Database and DB2 Connect Installation and Configuration Supplement*, GC09-2957  
Provides advanced installation considerations, and guides you through the planning, installation, migration (if necessary), and setup of a platform-specific DB2 client. This supplement also contains information on binding, setting up communications on the server, the DB2 GUI tools, DRDA® AS, distributed installation, the configuration of distributed requests, and accessing heterogeneous data sources.
- *IBM DB2 Universal Database Message Reference Volume 1*, GC09-2978 and *IBM DB2 Universal Database Message Reference Volume 2*, GC09-2979  
Lists the messages and codes issued by DB2, the Information Catalog Manager, and the DB2 Data Warehouse Center, and describes the actions you should take.

## 1.2.4 Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Software Information Center Web site. The Tivoli Software Information Center is located at the following Web address:

<http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>

**Note:** If you print PDF documents on other than letter-sized paper, select the **Fit to page** check box in the Adobe Acrobat Print dialog. This option is available when you click **File → Print**. **Fit to page** ensures that the full dimensions of a letter-sized page print on the paper that you are using.

## 1.2.5 Ordering publications

You can order many Tivoli publications online at the following Web site:

<http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968
- In other countries, for a list of telephone numbers, see the following Web site:

<http://www.ibm.com/software/tivoli/order-lit/>

## 1.3 Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. For the warehouse pack, you use the interfaces of IBM DB2 and the reporting tool. See those documentation sets for accessibility information.

## 1.4 Contacting software support

If you have a problem with a Tivoli product, refer to the following IBM Software Support Web site:

<http://www.ibm.com/software/sysmgmt/products/support/>

If you want to contact customer support, see the IBM Software Support Guide at the following Web site:

<http://techsupport.services.ibm.com/guides/handbook.html>

The guide provides information about how to contact IBM Software Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers, depending on the country in which you are located
- Information you must have before contacting IBM Software Support

## 1.5 Typeface conventions

This guide uses the following typeface conventions:

### **Bold**

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip** and **Operating system considerations**)



- Column headings in a table
- Keywords and parameters in text

*Italic*

- Citations (titles of books, diskettes, and CDs)
- Words defined in text
- Emphasis of words (words as words)
- Letters as letters
- New terms in text (except in a definition list)
- Variables and values you must provide

*Monospace*

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

## 2 Overview

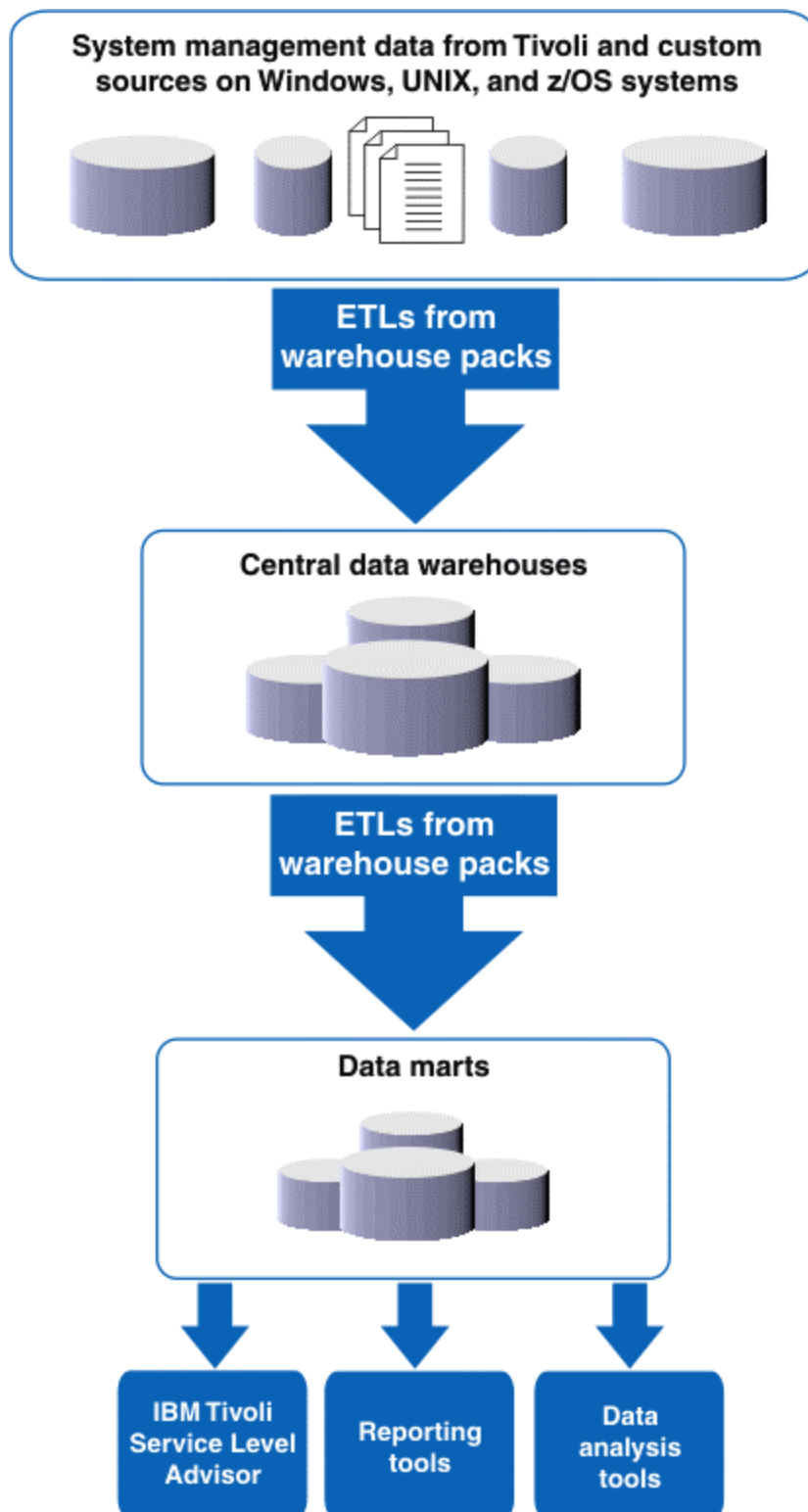
The following sections provide an overview of Tivoli Data Warehouse and the warehouse pack for IBM Tivoli Security Compliance Manager (SCM).

### ***2.1 Overview of Tivoli Data Warehouse***

Tivoli Data Warehouse provides the infrastructure for the following:

- Extract, transform, and load (ETL) processes through the IBM DB2 Data Warehouse Center tool
- Schema generation of the central data warehouse
- Historical reports

As shown in Figure 1, Tivoli Data Warehouse consists of a centralized data store where historical data from many management applications can be stored, aggregated, and correlated.



**Figure 1. Tivoli Data Warehouse basic architecture**

The *central data warehouse* uses a generic schema that is the same for all applications. As new components or new applications are added, more data is added to the database; however, no new database objects are added in the schema.

A *data mart* is a subset of a data warehouse that contains data that is tailored and optimized for the specific reporting needs of a department or team.

The *central data warehouse ETL* reads the data from the operational data stores of the application that collects it, verifies the data, makes the data conform to the schema, and places the data into the central data warehouse.

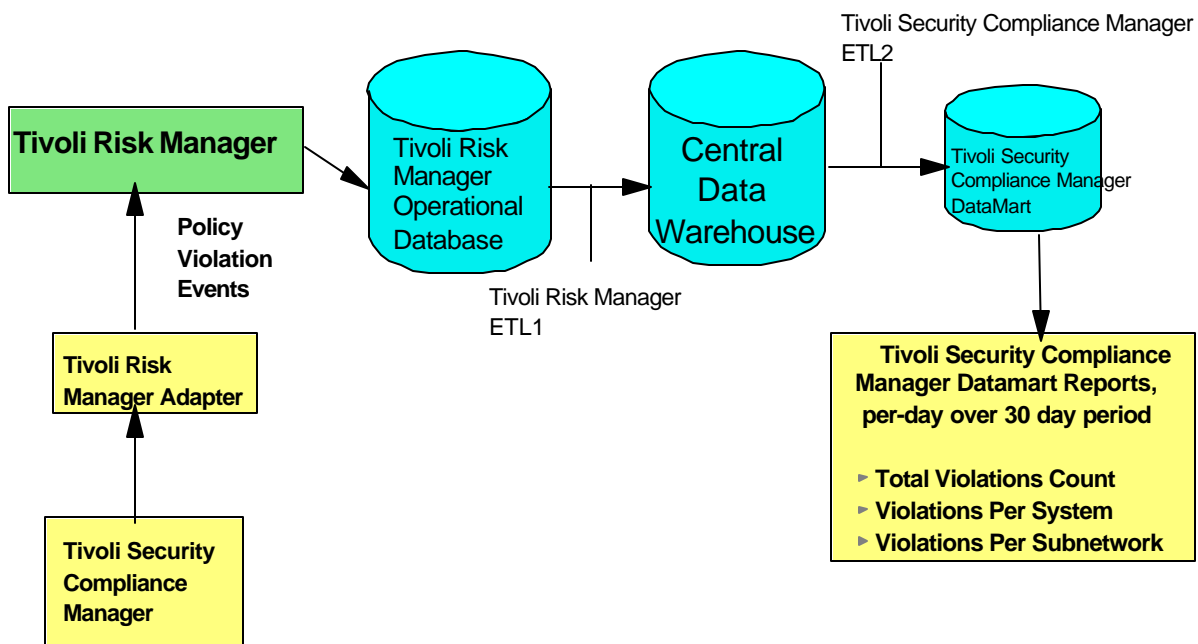
The *data mart ETL* extracts a subset of data from the central data warehouse, transforms it, and loads it into one or more star schemas, which can be included in data marts to answer specific business questions.

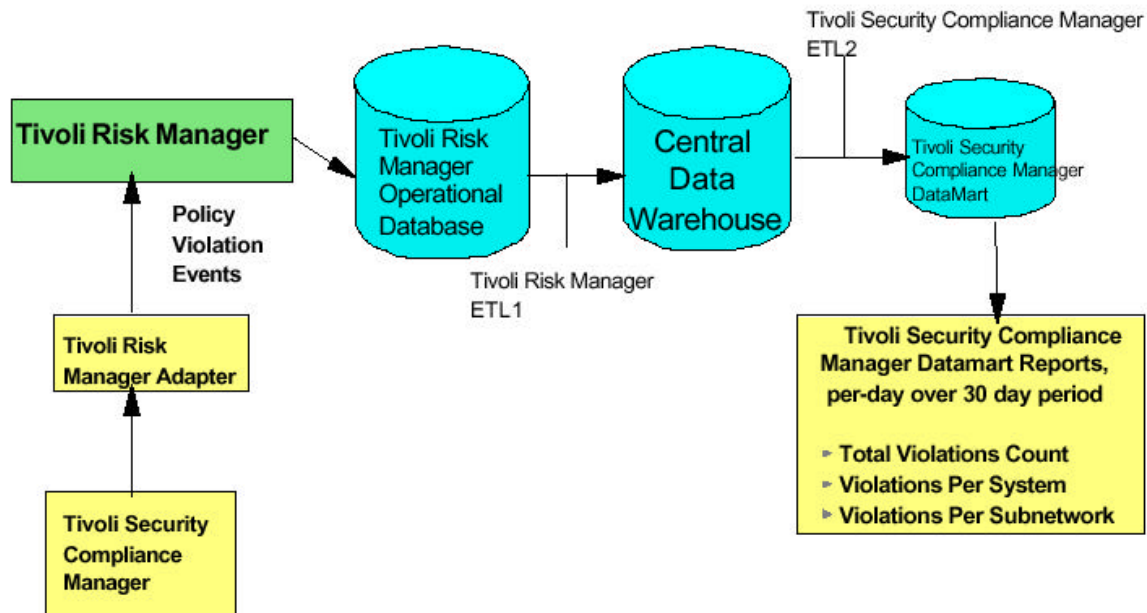
A program that provides these ETLs is called a *warehouse enablement pack* or simply *warehouse pack*.

The ETLs are typically scheduled to run periodically, usually during non-peak hours. If an ETL encounters data that it cannot correctly transform, it creates an entry in an exception table. Exception tables are described in the *IBM Tivoli Risk Manager Warehouse Enablement Pack Version 1.1 Implementation Guide*.

## 2.2 Overview of IBM Tivoli Security Compliance Manager warehouse pack

The warehouse pack for IBM Tivoli Security Compliance Manager 5.1 uses the Tivoli Risk Manager 4.2 pack to extract and load the Tivoli Security Compliance Manager policy violation data into the central data warehouse. The collection of data from Tivoli products into the central data warehouse lets you see trends in operation, resource usage, and cross-product interoperability. The warehouse pack for Tivoli Security Compliance Manager requires that the warehouse pack for the Tivoli Risk Manager be installed first. The following diagram illustrates how the Tivoli Risk Manager warehouse pack is used.





**Figure 2. Tivoli Security Compliance Manager Tivoli Data Warehouse integration architecture**

The Tivoli Security Compliance Manager policy violation data will be sent to the Tivoli Risk Manager operational database (Tivoli Risk Manager archive table) through the Tivoli Risk Manager adapter as shown in figure 2. The Tivoli Risk Manager warehouse pack contains both central data warehouse ETL and data mart ETL. The central data warehouse ETL of the Tivoli Risk Manager warehouse pack extracts the Tivoli Security Compliance Manager violation data from the archive table and transforms and loads the data into the central data warehouse. The Tivoli Security Compliance Manager warehouse pack contains only data mart ETL. The data mart ETL of the Tivoli Security Compliance Manager warehouse pack will extract the Tivoli Security Compliance Manager policy violation data from central data warehouse and then transform and load the data into the Tivoli Security Compliance Manager data mart. The collection of historical data of Tivoli Security Compliance Manager violations in the Tivoli Security Compliance Manager data mart lets the user see trends in violations by day/week/month or violations by system/sub network using reports. There are currently three pre-built reports. The reports are described in Section 3 on page 10.

The warehouse pack for IBM Tivoli Risk Manager aggregates events based on:

- Event category (CLASS\_CAT)
- Event Source token (SRC\_TOKEN), hostname (SRC\_HOSTNAME) or IP address (SRC\_IPADDR)
- Event target hostname (DST\_HOSTNAME) or IP address (DST\_IPADDR)

The CLASS\_CAT attribute will have a value “SecPolViolation” for SCM policy violations. Refer to the *IBM Tivoli Risk Manager Version 4.1, Warehouse Enablement pack version 1.1* for details on central data warehouse ETL of the Tivoli Risk Manager Warehouse Pack.

The source of violation data for the Tivoli Security Compliance Manager warehouse pack is the central data warehouse. The name of the ODBC driver for the TWH\_CDW is TWH\_CDW. Specifically, warehouse tables, TWG.MsmtTyp, TWG.MSrc, TWHG.Msmt, TWG.Comp, TWG.CompAttr, private table HRM.ClassCatDesc and staging table HCV.Event\_Metric are the tables of the TWH\_CDW that are defined as sources for the warehouse pack. The events with the CLASS\_CAT of “SecPolViolation” will be extracted from the central data warehouse by this warehouse pack because those are the Tivoli Security Compliance Manager policy violation events.

### 3 Reports

This section provides information about the predefined reports provided by the warehouse pack.

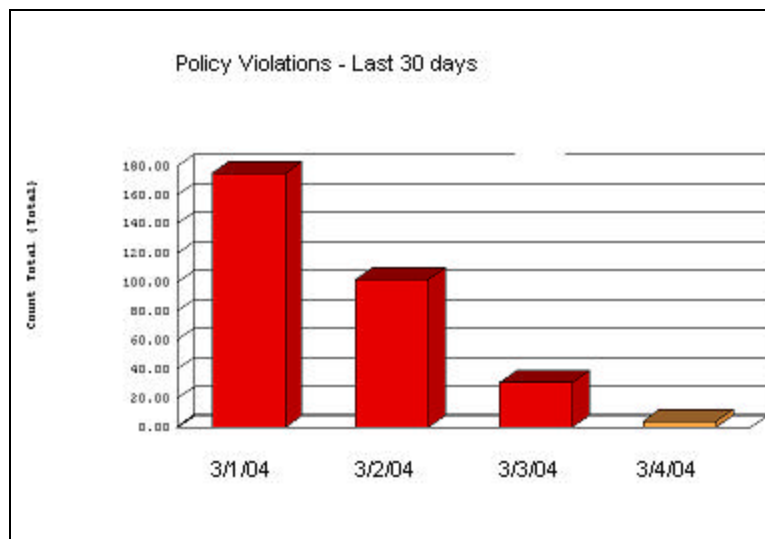
The following information is provided:

- A list of the reports
- A description of the information contained in the reports
- The names of the data mart tables that are used to create the reports
- SQL queries for modifying a report or creating a new report based on this one

#### Report 1: Compliance Violation Trends (violations per day/week/month)

Report name	Description	Table names
Compliance Violation Trends (per day, per week, or per month)	This report shows the total number of policy compliance violations per day, per week, or per month on a single bar chart. The time range for the report can be specified as a parameter.	HCV.F_EVENT_DAY

Figure 3 is a graphical representation of the Compliance Violation Trends report.



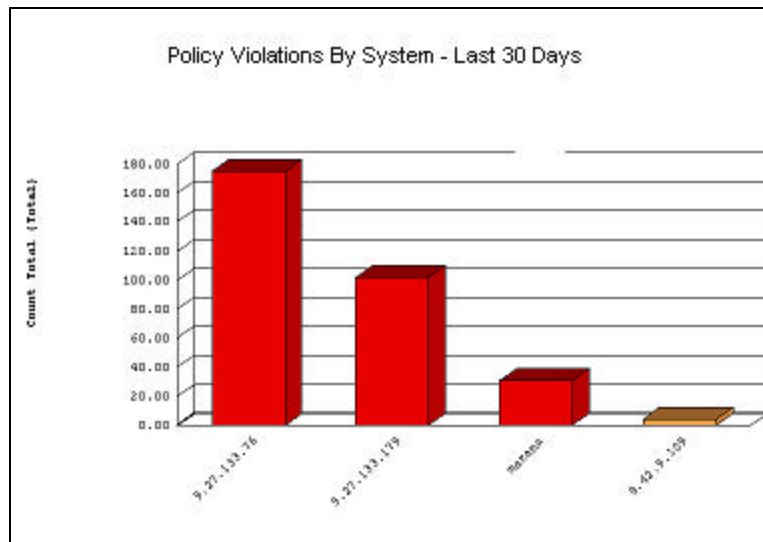
**Figure 3. Compliance Violation Trends**

#### Report 2: Policy Violations by System (per day/week/month)

Report name	Description	Table names
Policy violations by	This report ranks on a bar chart all the systems by the number of policy compliance violations per day, per	HCV.F_EVENT_DAY,

system per day, per week, or per month	week, or per month. The time range for the report can be specified as a parameter.	HCV.D_DST_HOST
--	--	----------------

Figure 4 is a graphical representation of the Policy Violations by System report.



**Figure 4. Policy Violations By System**

### Report 3: Policy Violations by subnet (per day/week/month)

Report name	Description	Table names
Policy violations by subnet per day, per week, or per month	This summary report breaks down all the policy compliance violations by subnetworks in the enterprise per day, per week, or per month. The time range for the report can be specified as a parameter.	HCV.F_EVENT_DAY, HCV.D_DST_HOST

Figure 5 is a graphical representation of the Policy Violations by Subnetwork report.

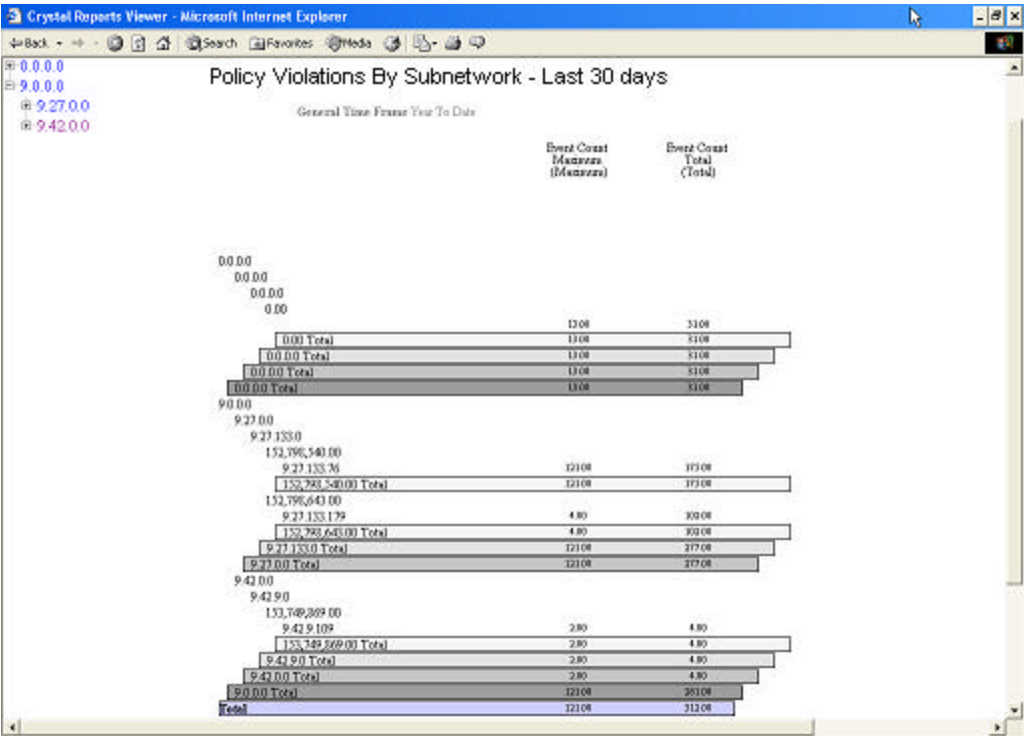


Figure 5. Policy Violations By Subnet



## 4 Installing and configuring the warehouse pack

This section describes the installation and configuration of the warehouse pack.

### 4.1 Prerequisite hardware and software

Before installing the warehouse pack for IBM Tivoli Security Compliance Manager, you must install the following software:

- IBM Tivoli Security Compliance Manager 5.1
- IBM Tivoli Risk Manager 4.1, Event Server component
- IBM DB2 Universal Database, Version 7.2
- Fix pack 8e, 9, 10, or 10a for IBM DB2 Universal Database, Version 7.2
- Tivoli Data Warehouse, Version 1.2
- Crystal Enterprise and its prerequisites
- IBM Tivoli Risk Manager 4.1 Warehouse Enablement Pack Version 1.1

This warehouse pack supports central data warehouses on DB2 Universal Database for Windows and UNIX systems. Also, this warehouse pack supports data marts on DB2 UDB for Windows and UNIX systems.

Refer to the *Tivoli Data Warehouse Release Notes* and IBM Tivoli Security Compliance Manager Release Notes for specific information about hardware prerequisites, database and operating system support, and product prerequisites. For late-breaking news about prerequisites, refer to the following IBM Software Support Web site:

<http://www.ibm.com/software/sysmgmt/products/support/>

### 4.2 Product notes and limitations

None.

### 4.3 Database-sizing considerations

Ensure that you have sufficient space in the central data warehouse for the historical data collected by the warehouse pack. Refer to the Tivoli Risk Manager warehouse pack for database sizing.

### 4.4 Pre-installation procedures

- Make sure that the Tivoli Enterprise Data Warehouse is installed. For instructions on installing the Tivoli Enterprise Data Warehouse, refer to *Installing and Configuring Tivoli Enterprise Data Warehouse*.
- Make sure that the IBM Tivoli Risk Manager is installed and that the RMDB data source is available.
- Make sure that the IBM Tivoli Risk Manager Warehouse Enablement Pack is installed.
- Make sure that the IBM Tivoli Security Compliance Manager is installed and that the Tivoli Risk Manager adapter for Tivoli Security Compliance Manager is installed and configured.
- Follow the instructions in the *IBM Tivoli Risk Manager 4.1 Warehouse Enablement Pack 1.1 Read me* and make sure you can run central data warehouse ETL (ETL1) in test mode.

### 4.5 Installation of the warehouse pack

Before installing the warehouse pack, record the user IDs, passwords, and server name, alias, or file path. You need this information to follow the installation procedures that are described in *Installing and Configuration Tivoli Data Warehouse*. The default data source names for the ODBC connections are HCV\_TWH\_CDW\_Source and HCV\_TWH\_MART\_Target.

Install the warehouse pack as described in *Installing and Configuring Tivoli Data Warehouse*, using the installation properties file (twh\_install\_props.cfg file):

<b>Location of the twh_install_props.cfg file</b>	tdw_weps/HCV/v110 in the Tivoli Security Compliance Manager warehouse pack
---	--

## 4.6 Post-installation procedures

After you install the warehouse pack, you must determine how you want to schedule the ETLs. See the information about installing warehouse packs in *Installing and Configuring Tivoli Data Warehouse* for the procedure to schedule ETLs using these processes:

<b>Initialization process</b>	HCV_m05_Build_mart_Process
<b>Process dependencies</b>	Located in the HCV_TivoliSecurityComplianceManager_V5.1.0_Subject_Area The processes should be scheduled to run after the central data warehouse ETL (ETL1) step, “HRM_c05_s040_Load_Msmt”, in the Tivoli Risk Manager warehouse pack is run.  1. HCV_m05_Build_Mart_Process.

For this warehouse pack, it is sufficient to schedule the first step in the process. All subsequent steps will execute automatically, after the first step succeeds. But it is important that the Tivoli Security Compliance Manager violation data from Tivoli Risk Manager archive table is extracted and loaded into the central data warehouse by the HRM\_c05\_s010\_Extract step of the Tivoli Risk Manager warehouse pack before this step is scheduled.

## 4.7 Uninstallation of the warehouse pack

Perform the following steps to uninstall the warehouse pack:

1. Run the script hcv\_cdw\_reset\_etl2\_extctl.generic (described below) to remove all the Tivoli Security Compliance Manager data from the Tivoli Security Compliance Manager data mart.
2. Uninstall the warehouse pack as described in *Installing and Configuring Tivoli Data Warehouse*.

hcv\_cdw\_reset\_etl2\_extctl.generic : This script must be run against the central data warehouse database (TWH\_CDW) because that database is where the extract control parameters are stored. To execute a script, you must first open a DB2 command window. From the Windows Start menu, select **Programs -> IBM DB2 -> Command Window**. Next, you must connect to the desired database (TWH\_CDW), using the following command (user ID and password may be different):

```
db2 connect to TWH_CDW user db2admin using password
```

To execute the script, enter the following command from the DB2 command window:

```
db2 -tvf hcv_cdw_reset_etl2_extctl.generic
```

You will see each statement of the script displayed in the window, followed by a DB2 message indicating success or failure of the statement. If you see any errors, refer to *IBM DB2 Universal Database Message Reference, Volume 1*.

When the warehouse pack is uninstalled, the following Tivoli Security Compliance Manager specific tables in the data mart are removed, but the data in the central data warehouse remains and is still useable by other applications:

- hcv.d\_classcat
- hcv.d\_dst\_host
- hcv.d\_Event\_metric

- hcv.d\_src\_host
- hcv.ext\_dst\_host
- hcv.f\_event\_day
- hcv.f\_event\_hour
- hcv.f\_event\_month
- hcv.f\_event\_week
- hcv.prune\_mart\_control
- hcv.prune\_mart\_log
- hcv.stage\_classcat
- hcv.stage\_dst\_host
- hcv.stage\_f\_event\_hour
- hcv.stage\_starschema
- hcv.t\_dst\_host
- hcv.t\_event\_metric
- hcv.t\_src\_host

## ***4.8 Multiple data centers***

This warehouse pack does not provide support for multiple data centers.

## 5 Maintenance and problem determination

This section describes maintenance tasks for the warehouse pack.

### 5.1.1 Data mart

Pruning data from the fact tables is implemented in the HCV\_m05\_s050\_Mart\_Prune step of HCV\_m05\_Load\_Mart\_Process. The prune mart control table HCV.Prune\_Mart\_Control governs which data is pruned and contains a date duration value for all the HCV\_F\_Event\_Hour, HCV\_F\_Event\_Day, HCV\_F\_Event\_Week, and HCV\_F\_Event\_Month fact tables. By default, all hourly data is pruned after 3 months, daily and weekly fact data is pruned after 1 year, and monthly fact data is pruned after 3 years when the process step runs. The HCV.Prune\_Mart\_Log table keeps a history of data pruning.

### 5.2 Extraction control (table *Extract\_Control*)

The extraction control table assists you in incrementally extracting data from a source database. For an example of incremental extraction, see the *Enabling an Application for Tivoli Data Warehouse* guide.

ExtCtl_Source VARCHAR (120)	ExtCtl_Target VARCHAR (120)	ExtCtl_From_RawSeq CHAR (10)	ExtCtl_to_RawSeq CHAR (10)	ExtCtl_From_IntSeq BIGINT	ExtCtl_To_IntSeq BIGINT	ExtCtl_From_DrTm TIMESTAMP	ExtCtl_To_DrTm TIMESTAMP	Msrc_Corr_Cd CHAR (6)

### 5.3 Problem determination

For common problems and solutions, see the *Installing and Configuring Tivoli Data Warehouse* guide.

## 6 ETL processes

The warehouse pack has the following process:

- **HCV\_m05\_Build\_Mart\_Process** – builds a data mart with four star schemas based on the Tivoli Security Compliance Manager violation event counts aggregated hourly, daily, weekly and monthly.

### 6.1 HCV\_m05\_Build\_Mart\_Process

This process extracts all new Tivoli Security Compliance Manager policy violation event data measurements from the central data warehouse and converts the measurements to facts in the Tivoli Security Compliance Manager data mart. The process also extracts new Tivoli Risk Manager host and event components, plus their attributes, from the central data warehouse and converts the data to dimensions in the Tivoli Security Compliance Manager data mart. It also prunes old facts from the data mart. The process runs in five steps that are described below. The process is configured to start with the first step and run each succeeding step if and only if the preceding step succeeds.

Run this process once after installing the warehouse pack; and on a regular scheduled basis (typically once a day during off-peak hours) after the running Tivoli Risk Manager central data warehouse ETL.

This process has the following steps:

- **HCV\_m05\_s010\_Mart\_Pre\_Extract**

Source: TWH\_CDW – tables TWG.MsmtTyp, TW.G.MSrc

Target: TWH\_CDW – staging table HCV.Event\_Metric

This step reinitializes the staging table HCV.Event\_Metric in the central data warehouse, creating a row for each Tivoli Security Compliance Manager measurement type. The staging table has the same structure as the metric dimension table in the data mart database. This step by default enables minimum, maximum, average, and total metrics for all measurements. In the hourly fact table, all measurement values for any hour are the same, but in the daily, weekly, and monthly fact tables, the minimum, maximum, and average values might be different from the total value.

- **HCV\_m05\_s020\_Extract**

Source: TWH\_CDW – staging table HCV.Event\_Metric, private table HRM.ClassCatDesc, TWG.Msmt, TWG.Comp, TWG.CompAttr tables

Target: TWH\_MART – translation dimension tables HCV.T\_Event\_Metric, HCV.T\_Dst\_Host, HCV.T\_Src\_Host, and staging tables HCV.Stage\_ClassCat, HCV.Stage\_F\_Event\_Hour

This step adds new Tivoli Security Compliance Manager violation event data from the central data warehouse to staging tables and translation dimension tables in the Tivoli Security Compliance Manager data mart. The staging tables are dropped and re-created each time this step is run. The translation dimension tables are permanent and have a structure exactly the same as their corresponding data mart dimension tables, but in addition they contain information to identify the central data warehouse (in a multi-central data warehouse environment) where the data originated, as well as the original component and measurement IDs. Translation dimension tables are used to track IDs from the original central data warehouse into the star schema so you can tell where the data actually came from when looking at a star schema.

The target staging and translation dimension tables are the following:

**HCV.Stage\_ClassCat** – contains all the event category descriptions defined in central data warehouse table HRM.ClassCatDesc.

**HCV.T\_Event\_Metric** – contains all Tivoli Security Compliance Manager measurement types expressed as data mart metrics. Currently, Tivoli Security Compliance Manager has only one metric – Event Count.

HCV.T\_Dst\_Host – contains one record for each distinct destination host in all the processed Tivoli Security Compliance Manager violation events. Each record maps from an IP\_HOST, IP\_INTERFACE or HRM\_HOST component in the central data warehouse. Each record also stores the hostname and IP address values from the LAST\_IP\_ADDRESS or HRM\_DST\_HOSTNAME attributes, if they exist. Finally, the table contains the IP address for each host represented as an integer, plus strings for the subnets represented by each portion of the dotted decimal IP address. Three source database central data warehouse views and several staging/intermediate tables are used in this step to populate this table.

- HCV.T\_Src\_Host – contains one record for each distinct source host in all the processed Tivoli Security Compliance Manager events. Each record maps from a HRM\_EVENT component, and its corresponding HRM\_SRC\_HOSTNAME or HRM\_SRC\_IPADDR attribute, in the central data warehouse.
- HCV.Stage\_F\_Event\_Hour – contains one record for each new measurement added to the central data warehouse. Each record contains foreign key integer fields pointing to the metric, event category, destination, and source host translation dimension tables.

Extract control is achieved by using the component and measurement IDs from the central data warehouse tables. The ExtCtl\_To\_IntSeq value is set to the maximum ID currently in the central data warehouse, as defined by an appropriate view. After the extraction is complete, this value is copied into ExtCtl\_From\_IntSeq to be used for the next extraction. The following table shows which tables and ID columns are used for extract control.

Target Tables (TWH_MART)	Source Tables (TWH_CDW)	Source Table Views (TWH_CDW)	Source Table Columns used for Extract Control (TWH_CDW)	Source Table Extract Control Views (TWH_CDW)
HCV.T_Event_Metric	HCV.Event_Metric	HCV.VD_Event_Metric	Metric_ID	HCV.VE_Event_Metric
HCV.T_Dst_Host	TWG.Comp, TWG.CompAttr	HRM.VD_Host_Dst_IP, HRM.VD_Host_Dst_NoIP, HRM.VD_Host_Dst_Name	Comp_ID	HRM.VE_Dst_Host
HCV.T_Src_Host	TWG.Comp, TWG.CompAttr	HRM.VD_Host_Src	Comp_ID	HRM.VE_Src_Host
HCV.Stage_F_Event_Hour	TWG.Msmt, TWG.Comp, TWG.CompAttr	HRM.VF_Stg_Evt_Hour	Msmt_ID	HRM.VE_Event_Hour

### • HCV\_m05\_s030\_Load

Source: TWH\_MART – staging tables HCV.Stage\_ClassCat, HCV.Stage\_F\_Event\_Hour; translation dimension tables HCV.T\_Event\_Metric, HCV.T\_Dst\_Host, HCV.T\_Src\_Host

Target: TWH\_MART – fact table HCV.F\_Event\_Hour; dimension tables HCV.D\_ClassCat, HCV.D\_Event\_Metric, HCV.D\_Dst\_Host, HCV.D\_Src\_Host

This step loads the dimension tables and hourly fact table with Tivoli Security Compliance Manager data from the translation dimension tables and a staging fact table. Translation dimension tables are used to track IDs from the original central data warehouse into the star schema so you can tell where the data actually came from when looking at a star schema. Each insert uses 'where not is' logic to ensure that duplicate dimensions or facts are not inserted.

- **HCV\_m05\_s040\_Rollup**

Source: TWH\_MART – tables HCV.Stage\_F\_Event\_Hour, HCV.F\_Event\_Hour; TWH\_MD – table IWH.STARSCHEMA

Target: TWH\_MD – table RPI.SSUPDATED; TWH\_MART – tables HCV.F\_Event\_Day, HCV.F\_Event\_Week, HCV.F\_Event\_Month

This step rolls up new hourly facts from the staging fact table into the daily, weekly, and monthly fact tables. Timestamps for daily, weekly, or monthly facts are converted from GMT to local time for Crystal Reports. If new data is rolled up for any of the above tables, the appropriate star schema (hourly, daily, weekly, monthly) is indicated as updated in table RPI.SSUPDATED, which enables any canned reports based on the updated schema to be automatically regenerated.

- **HCV\_m05\_s050\_Prune**

Source: TWH\_MART – table HCV.Prune\_Mart\_Control

Target: TWH\_MART – tables HCV.F\_Event\_Hour, HCV.F\_Event\_Day, HCV.F\_Event\_Week, HCV.F\_Event\_Month, HCV.Prune\_Mart\_Log

This step deletes facts from the hourly, daily, weekly, and monthly fact tables if the fact date is older than the prune control values. Prune control values are held in table HCV.Prune\_Mart\_Control and can be adjusted by the customer as desired. For the hourly fact table, adjustment is made for GMT but the other fact tables are in local time. The number of records deleted from each fact table is stored in permanent table HCV.Prune\_Mart\_Log.

## 7 Central data warehouse information

Refer to the Tivoli Risk Manager Warehouse Enablement Pack documentation for a description of how the data is stored in the central data warehouse.



## 8 Data mart schema information

The following sections contain the definition of star schemas, metric dimension tables, and data marts provided with the warehouse pack. This section is intended primarily for report designers and warehouse pack creators. For information about reports, see Section 3, Reports on page 10.

Shaded columns in the following tables are translated. These columns are also marked with an asterisk (\*) after the column name.

### 8.1 Data mart HCV\_TWH\_MART data mart

This data mart uses the following star schemas:

- HCV Hourly Security Compliance Manager event star schema
- HCV Daily Security Compliance Manager event star schema
- HCV Weekly Security Compliance Manager event star schema
- HCM Monthly Security Compliance Manager event star schema

### 8.2 Star schemas

Before using this section, read about the star schemas in *Enabling an Application for Tivoli Data Warehouse*. That document defines the content of each table and explains the relationships between the tables in this document.

The warehouse pack provides the following star schemas.

#### 8.2.1.1 HCV Hourly Tivoli Security Compliance Manager event star schema

The following table defines the star schema. The description of the star schema is translated.

Description of star schema (in IWH_STARSHEMA)	Tivoli Security Compliance Manager Event Hourly Data
Name of fact table	HCV.F_Event_Hour
Name of metric dimension table	HCV.D_Event_Metric
Names of other dimension tables	HCV.D_Dst_Host
	HCV.D_Src_Host
	HCV.D_ClassCat

Description of star schema (in IWH_STARSHEMA)	Tivoli Security Compliance Manager Event Daily Data
Name of fact table	HCV.F_Event_Day
Name of metric dimension table	HCV.D_Event_Metric
Names of other dimension tables	HCV.D_Dst_Host
	HCV.D_Src_Host
	HCV.D_ClassCat

Description of star schema (in IWH_STARSHEMA)	Tivoli Security Compliance Manager Event Weekly Data
Name of fact table	HCV.F_Event_Week
Name of metric dimension table	HCV.F_Event_Metric
Names of other dimension tables	HCV.D_Dst_Host
	HCV.D_Src_Host
	HCV.D_ClassCat

Description of star schema (in IWH_STARSHEMA)	Tivoli Security Compliance Manager Event Monthly Data
Name of fact table	HCV.F_Event_Month
Name of metric dimension table	HCV.F_Event_Metric
Names of other dimension tables	HCV.D_Dst_Host
	HCV.D_Src_Host
	HCV.D_ClassCat

### 8.2.1.2 Fact table HCV.F\_Event\_Hour

#### HCV Hourly Tivoli Security Compliance Manager Event Star Schema

The following columns are used in the fact table:

- Metric\_ID INTEGER
- Src\_Host\_ID INTEGER
- Dst\_Host\_ID INTEGER
- ClassCat\_ID INTEGER
- Meas\_hour TIMESTAMP
- Min\_value DOUBLE
- Max\_value DOUBLE
- Avg\_value DOUBLE
- Total\_value DOUBLE
- Sample\_count DOUBLE
- Fact\_ID INTEGER
- CDW\_ID INTEGER

### 8.2.1.3 Fact table HCV.F\_Event\_Day

#### HCV Daily Tivoli Security Compliance Manager Event Star Schema

The following columns are used in the fact table:

- Metric\_ID INTEGER
- Src\_Host\_ID INTEGER
- Dst\_Host\_ID INTEGER
- ClassCat\_ID INTEGER
- Meas\_date TIMESTAMP
- Min\_value DOUBLE
- Max\_value DOUBLE
- Avg\_value DOUBLE
- Total\_value DOUBLE
- Sample\_count DOUBLE
- Fact\_ID INTEGER
- CDW\_ID INTEGER

#### 8.2.1.4 Fact table HCV.F\_Event\_Week

##### HCV Weekly Tivoli Security Compliance Manager Event Star Schema

The following columns are used in the fact table:

- Metric\_ID INTEGER
- Src\_Host\_ID INTEGER
- Dst\_Host\_ID INTEGER
- ClassCat\_ID INTEGER
- Meas\_date TIMESTAMP
- Min\_value DOUBLE
- Max\_value DOUBLE
- Avg\_value DOUBLE
- Total\_value DOUBLE
- Sample\_count DOUBLE
- Fact\_ID INTEGER
- CDW\_ID INTEGER

#### 8.2.1.5 Fact table HCV.F\_Event\_Month

##### HCV Monthly Tivoli Security Compliance Manager Event Star Schema

The following columns are used in the fact table:

- Metric\_ID INTEGER
- Src\_Host\_ID INTEGER
- Dst\_Host\_ID INTEGER
- ClassCat\_ID INTEGER
- Meas\_date TIMESTAMP
- Min\_value DOUBLE
- Max\_value DOUBLE

- Avg\_value DOUBLE
- Total\_value DOUBLE
- Sample\_count DOUBLE
- Fact\_ID INTEGER
- CDW\_ID INTEGER

### 8.3 Metric dimension tables

This section describes the metric dimension tables used by the star schemas in the warehouse pack. Shaded columns indicate text that is translated. These column headings are also marked with an asterisk (\*).

#### 8.3.1 HCV.D\_Event\_METRIC

Metric_ID INTEGER	Met_Category * VARCHAR (254)	Met_Desc * VARCHAR (254)	Met_Name * VARCHAR (254)	Met_Units * VARCHAR (254)	Min_Exists CHAR (1)	Max_Exists CHAR (1)	Avg_Exists CHAR (1)	Total_Exists CHAR (1)	Msrc_Nm * VARCHAR (254)
1	N/A	Number of Tivoli Security Compliance Manager Violation Events	Event Count	QTY	Y	Y	Y	Y	IBM Tivoli Security Compliance Manager
* This column is translated.									

### 8.4 Dimension tables

The following sections describe the dimension tables (other than metric dimension tables) used by the star schemas in the warehouse pack.

#### 8.4.1 Dimension table HCV.D\_CLASSCAT

The following columns are used in this dimension table:

- Class\_Cat\_ID INTEGER
- Class\_Cat\_Name VARCHAR(16)
- Class\_Cat\_Desc VARCHAR(64)

#### 8.4.2 Dimension table HCV.D\_DST\_HOST

This dimension table contains attributes for each host identified as the target of a Tivoli Security Compliance Manager event.

The following columns are defined in this dimension table.

- Comp\_ID INTEGER not null – foreign key to component table
- Comp\_Name VARCHAR(120)
- Customer\_Name VARCHAR(120)

- Center\_Name VARCHAR(120)
- Hostname VARCHAR(128)
- IP\_Address VARCHAR(32)
- IP\_Number BIGINT default 0 – for sorting by IP address
- IP\_A\_Subnet VARCHAR(32)
- IP\_B\_Subnet VARCHAR(32)
- IP\_C\_Subnet VARCHAR(32)

### 8.4.3 Dimension table HCV.D\_SRC\_HOST

This dimension table contains attributes for each host identified as the source of a Tivoli SCM event.

The following columns are defined in this dimension table.

- Comp\_ID INTEGER not null – foreign key to component table
- Comp\_Name VARCHAR(120)
- Hostname VARCHAR(128)
- IP\_Address VARCHAR(32)

## 9 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 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:

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 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.

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.

#### **COPYRIGHT LICENSE:**

This information contains sample application programs in source language, which illustrates 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. 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 IBM's application programming interfaces.

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

## **Trademarks**

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

IBM, the IBM logo, Tivoli, the Tivoli logo, AIX, DB2, DRDA, Informix, OS/2, OS/400, Tivoli Enterprise Console, and TME are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Intel, the Intel Inside logos, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

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

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.



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

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





Printed in U.S.A.

SC32-1596-00