
# Tivoli

## *Decision Support for Enterprise Risk Management Release Notes*

*Version 1.1*

GI11-0862-00


# Tivoli

## *Decision Support for Enterprise Risk Management Release Notes*

*Version 1.1*

GI11-0862-00

## Copyright Notice



## Trademarks

## Notices

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to Tivoli Systems or IBMs valid intellectual property or other legally protectable right, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user.

Tivoli Systems or IBM may have patents or pending patent applications covering subject matter 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 the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.

## Tivoli Decision Support Guide Documentation

Each Tivoli Discovery Guide is delivered with online documentation. During the installation process, the applicable documentation is copied to the TDS\Guide Docs installation directory on your system.

# Contents

# 1

# Preface

This document describes the Tivoli Decision Support for Enterprise Risk Management, version 1.1 product. The Enterprise Risk Management guide is designed to augment the Risk Manager product. Where Risk Manager provides a powerful, rule-based event management application that integrates network, security systems, and other intrusion detection systems through adapters, the Enterprise Risk Management guide provides the IT managers of the business enterprise an overview of how well the Network Security systems, such as firewalls and intrusion detection systems, are performing within the enterprise.

**Note:** The Tivoli® guides as a group are called *discovery guides*. The Tivoli Decision Support for Enterprise Risk Management product is a discovery guide that is also called the *Enterprise Risk Management guide* or the *ERM guide*.

## Who Should Read This Book

This document is intended for the users of the Enterprise Risk Management guide and anyone responsible for the administration of Tivoli Decision Support.

Before using the Enterprise Risk Management guide, you must be familiar with the following:

- The operating system on your computer
- The basic use of discovery guides and the Tivoli Discovery Interface

To set up the Enterprise Risk Management guide, your system administrator must be familiar with the following:

- Tivoli Discovery Administrator
- Basic use of Crystal Reports and Cognos PowerPlay
- Tivoli Enterprise Console (TEC) database
- Open Database Connectivity (ODBC) for your database

## Tivoli Decision Support and Enterprise Risk Management Guide Documentation

To install and use the Enterprise Risk Management guide, you must be familiar with the following Tivoli Decision Support publications:

| Document | Description<br>Location |
|---|---|
| *Tivoli Decision Support Installation Guide* | Provides installation procedures for Tivoli Decision Support and its components in stand-alone and network mode.<br>File name on your system: *TDS*\Docs\Pdf\install.pdf (where *TDS* represents the directory where Tivoli Decision Support 2.1 resides) |
| *Tivoli Decision Support (TDS) 2.1 Readme.txt* | Review this document before installing Tivoli Decision Support for Enterprise Risk Management. It contains the latest information about the Tivoli Decision Support product. This document also describes the features of the Tivoli Discovery Interface that are not documented in version 2.1. These features are found in the Tivoli Discovery Interface, and not in the Tivoli Discovery Administrator. The Tivoli Decision Support 2.1 User Online Help system provides detailed information and procedures for using the undocumented features.<br>File name on the CD-ROM: *d*:\Readme.txt (where *d*: represents the drive letter for your CD-ROM Drive)<br>File name on your system: *TDS*\Readme.txt (where *TDS* represents the directory where Tivoli Decision Support 2.1 resides) |
| *Tivoli Decision Support for Enterprise Risk Management Release Notes* | Provides copyright, prerequisite, installation procedures, and trouble shooting for the Enterprise Risk Management guide.<br>File name on the CD-ROM: *d*:\books\tdserm11.pdf (where *d*: represents the drive letter for your CD-ROM Drive)<br>File name on your system: *TDS_Share*\Guide Docs\Tivoli Decision Support for Enterprise Risk Management\tdserm11.pdf (where *TDS_Share* represents the shared data file path configured using the Tivoli Discovery Administrator program). |
| *Tivoli Decision Support Users Guide* | Describes Tivoli Decision Support features, concepts, and provides procedures for using the Tivoli Discovery Interface.<br>File name on your system: *TDS*\Docs\Pdf\user-gd.pdf (where *TDS* is the directory in which Tivoli Decision Support 2.1 is installed) |
| *Tivoli Decision Support Administrator Guide* | Explains the features of the Tivoli Discovery Administrator.<br>File name on your system: *TDS*\Docs\Pdf\admin-gd.pdf (where *TDS* represents the directory where Tivoli Decision Support 2.1 resides) |
| Other guides | Each Tivoli discovery guide is delivered with online documentation. During the installation process for each discovery guide, the applicable discovery guide documentation is copied to the system.<br>Directory on your system: *TDS_Share*\Guide Docs (where *TDS_Share* represents the shared data file path defined during installation and configuration of Tivoli Decision Support 2.1). |

## Contacting Customer Support

**To contact Tivoli Customer Support:**

**Note:** When you contact Tivoli Customer Support, please have your customer identification information available.

- Access the Tivoli Customer Support home page at:

  http://www.support.tivoli.com

  After you link to and submit the customer registration form, you can access many customer support services on the World Wide Web. Refer to the *Customer Support Handbook* for a listing of Tivoli Customer Support services, hours of operation, and contact numbers. This handbook is available online at :

  http://www.support.tivoli.com

- Send an e-mail to support@tivoli.com
- In the United States, call Tivoli Customer Support at 1-800-TIVOLI-8.
- Outside the United States, refer to your *Customer Support Handbook* for a list of support numbers in your country. This handbook is available online at:

  http://www.support.tivoli.com

**To provide comments and suggestions about our documentation:**

At Tivoli, we are very interested in hearing from you about your experience with Tivoli products, documentation, and services. We welcome your suggestions for improvements. If you have comments or suggestions about our documentation, please send e-mail to pubs@tivoli.com.

# 2

# Introduction



Tivoli Decision Support for Enterprise Risk Management, version 1.1 (Enterprise Risk Management guide) provides a strategic view of network security activity. Enterprise Risk Management adapters report security events to the Tivoli Enterprise Console as Tivoli Enterprise Console events.

Tivoli Decision Support for Enterprise Risk Management enables you to perform the following analysis and reporting capabilities:

- Gather and review information based on a set of questions and reports that address trends, peak volume, and sources of events.
- Present event management information as charts and tabular reports.
- Automate data acquisition and cube building.

Tivoli Decision Support for Enterprise Risk Management, version 1.1 supports Oracle, DB2®, and Sybase versions of the Tivoli Enterprise Console database.

## Understanding the Tivoli Decision Support for Enterprise Risk Management Environment

In the Tivoli Decision Support for Enterprise Risk Management environment, endpoint adapters send Risk Manager events to the Risk Manager server. The Tivoli Enterprise Console event repository table (tec_t_evt_rep) stores Risk Manager events. When you run the Archive Sensor Events job, a trigger copies the Risk Manager events into the Risk Manager Archived Events table (rm_t_arc). The trigger and the Risk Manager Archived Events table reside in the Tivoli Enterprise Console database.

**Note:** The Risk Manager Archived Events table and trigger do not affect the functionality of the Tivoli Enterprise Console.

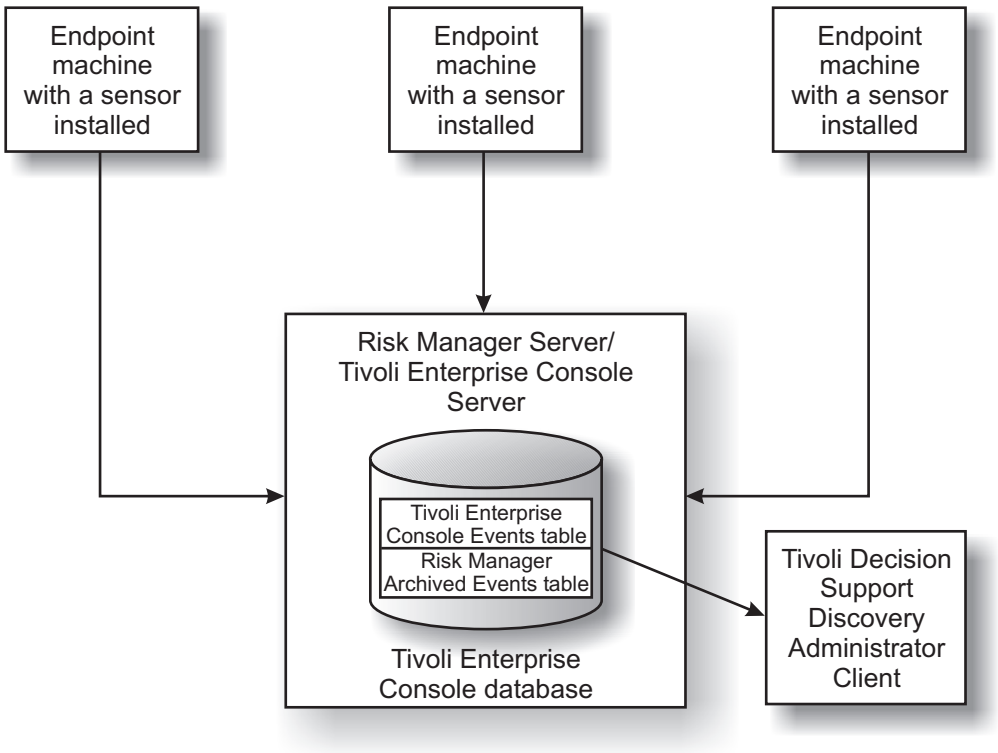


*Figure 1. Tivoli Decision Support for Enterprise Risk Management Environment*

# Understanding Tivoli Discovery Administrator Cubes

Tivoli Decision Support for Enterprise Risk Management builds two multidimensional cubes to support the topics and views described in "Categories, Topics, and Views" on page 59: the Archived Events Cube and the Anti-Virus Status Cube. Each multidimensional cube represents a compilation of the data in the Archived Events table. The cube depicts events (measures), aggregated across many categories (dimensions).

Cube building is a two-part process. First, you execute Structured Query Language (SQL) queries against the archive table to extract the latest data. Then, Tivoli Decision Support transforms the extracted data (rows of columns in flat files) into a multidimensional cube structure. Each cube contains only the data that it extracted from the database at the time when the cube was built. To view information from the most recently archived events, you must rebuild the cube at regular intervals. Each Tivoli Decision Support installation site can control when the multidimensional cube refreshes.

## Archived Events Cube

This cube is built from the measures and dimensions relating to Risk Manager events from the Tivoli Enterprise Console database. Risk Manager events are those Tivoli Enterprise Console event records defined by the **SOURCE** attribute equal to `'RISKMGR'` and the **SUB_SOURCE** attribute equal to `'IDSEVENT'` or `'MISCEVENT'`. These events are copied into the Risk Manager Archived Events table, which is used to build the cube.

For detailed information about this cube, see "Risk Manager Archived Events" on page 41.

## Anti-Virus Status Cube

This cube is built from the measures and dimensions relating to Risk Manager anti-virus administrator events from the Tivoli Enterprise Console database. Risk Manager anti-virus

administrator events are those Tivoli Enterprise Console event records defined by the **SOURCE** attribute equal to `'RISKMGR'`, the **SUB_SOURCE** attribute equal to `'MISCEVENT'`, and the **rm_SensorType** attribute beginning with `'AV_'`.

For detailed information about this cube, see "Risk Manager Anti-Virus Status" on page 52.

## What's New in Release 1.1

Tivoli Decision Support for Enterprise Risk Management, version 1.1 provides the following new features:

- Support for Sybase Adaptive Server Enterprise (ASE) databases.
- New archive table definition with more event attributes (extracted from the Tivoli Enterprise Console event tables).
- New trigger for populating the archive table with information from the Tivoli Enterprise Console event tables.
- Other small changes in the database schema to improve database integrity, performance, and usability.

# 3

# Planning for Installation

This chapter provides information to plan the installation and configuration of Tivoli Decision Support for Enterprise Risk Management. After you finish reading this chapter, you should be able to:

- Identify the software requirements for Tivoli Decision Support for Enterprise Risk Management.
- Size the Tivoli Enterprise Console database to accommodate the archive table used by Tivoli Decision Support for Enterprise Risk Management.
- Identify the major installation and configuration tasks.



## Software Requirements

This section lists the software products that are requirements for the Enterprise Risk Management guide. Refer to the product documentation for steps to install these products. Refer to the Tivoli Decision Support Installation Guide Version 2.1.1 for hardware requirements.

The following requirements apply to all configurations of the Enterprise Risk Management guide.

- Microsoft® Windows® 95, Windows 98 with year 2000 patches, or Windows NT® 4.0 with Service Pack 5 or later. See *Tivoli Decision Support Installation Guide Version 2.1* (GC32-0438) for more information regarding Tivoli Decision Support prerequisite software.
- Tivoli Decision Support 2.1.1 with the following components:
  - Tivoli Discovery Interface
  - Tivoli Discover Administrator (to build cubes)
  - Cognos PowerPlay
  - Seagate Crystal Reports (only required when creating new reports)

  The following Tivoli Decision Support 2.1.1 Core Patch is recommended: 2.1-TDS-0007
- Tivoli Risk Manager 3.8 on your network including its prerequisites.
- Access to the Tivoli Enterprise Console database.
- Access to the cube built by the administrator.

# Database Software Requirements

The Enterprise Risk Management guide supports the following databases:

- Oracle 8.x and 9.x
- DB2 6.1 and 7.1
- Sybase 11.5, 11.9.2, and 12.0

Each database requires software in addition to the software required for Tivoli Decision Support for Enterprise Risk Management. Before you install the Enterprise Risk Management guide, review the following sections to ensure that your system meets these requirements.

**Note:** Because the Enterprise Risk Management guide uses Open Database Connectivity (ODBC) Drivers to communicate with the Tivoli Enterprise Console database, no RIM (RDBMS Interface Module) support is required.

## DB2 Software Requirements

If you are a DB2 Universal Database™ (UDB) user, you need the following software:

- DB2 UDB 6.1 or 7.1 Client
- DB2 UDB 6.1 or 7.1 Client Application Enabler (CAE)

  The Client Application Enabler is contained on the DB2 Client Application Enablers™ CD-ROM or can be downloaded from the Web at:

  http://www.software.ibm.com/data/db2
- IBM® DB2 ODBC drivers (delivered with DB2)

  The IBM DB2 ODBC drivers are automatically installed with the DB2 client.

## Oracle Software Requirements

If you are an Oracle software user, you need the following software:

- The appropriate Oracle client and server software: Oracle 8.x or later.
- Oracle ODBC drivers. Generally, these drivers are included with the database software package or are available for download from the vendor's Web site. Refer to the following Web site for more information:

  http://otn.oracle.com/software/utilities/software_index.htm

  **Note:** Tivoli does not maintain the preceding Web site. It is included for your convenience.

## Sybase Software Requirements

If you are a Sybase software user, you need the following software:

- The appropriate Sybase client and server software: Sybase 11.5, 11.9.2, and 12.0.
- Sybase ODBC drivers. Generally, these drivers are included with the database software package or are available for download from the vendor's Web site. Refer to the following Web site for more information:

  http://downloads.sybase.com

  **Note:** Tivoli does not maintain the preceding Web site. It is included for your convenience.

## Sizing the Tivoli Enterprise Console Database for the Archive Table

During the configuration of the Enterprise Risk Management guide, you create a new table, called the Risk Manager Archived Events table, that is added to the existing Tivoli Enterprise Console database. Before you install the Enterprise Risk Management guide, you must size the existing Tivoli Enterprise Console database to accommodate the new Risk Manager Archived Events table. To size your database, determine the average volume of events that you receive per day and specify the number of days you want to retain as archive data. Allow approximately 1 KB of space per event record that you want to store in the archive table.

When the cube build initiates, Tivoli Decision Support reads the data from the Risk Manager Archived Events table and creates flat (.csv) files, which are used to build the cube. The Tivoli Discovery Administrator client creates the flat files in the shared data file path. Therefore, you should also verify that you have adequate disk space available to accommodate the .csv files created during the process of building the cube.

## Supported Languages

This version of Tivoli Decision Support only supports the English language.

## Roadmap of Installation and Configuration Tasks

The following table lists the sequence of activities required to install and configure the Enterprise Risk Management guide.

*Table 1. Roadmap of Installation and Configuration Tasks*

| Task | Type of Task | Location |
|---|---|---|
| Install the Enterprise Risk Management guide | Installation | Tivoli Discovery Administrator client |
| Configure the shared data file path | Configuration | Tivoli Discovery Administrator client |
| Import the Enterprise Risk Management guide | Configuration | Tivoli Discovery Administrator client |
| Create the Archive table, view, and trigger in the Tivoli Enterprise Console database | Configuration | Risk Manager/Tivoli Enterprise Console Server |
| Copy Archive Data from the Risk Manager version 3.7 Archive Table (optional) | Configuration | Risk Manager/Tivoli Enterprise Console Server |
| Run the Archive Sensor Events Job | Configuration | Risk Manager/Tivoli Enterprise Console Server |
| Set up an ODBC data source connection | Configuration | Tivoli Discovery Administrator client |
| Assign the ODBC data source for Tivoli Decision Support | Configuration | Tivoli Discovery Administrator client |
| Set the cube parameters | Configuration | Tivoli Discovery Administrator client |

# 4

# Installing the Enterprise Risk Management Guide

Use the following procedure to install Tivoli Decision Support for Enterprise Risk Management (from the Roadmap of Installation and Configuration Tasks, Table 1 on page 11):

**Note:** Verify that Tivoli Decision Support is installed before you install Tivoli Decision Support for Enterprise Risk Management.

1. Insert the Tivoli Decision Support for Enterprise Risk Management CD in the CD-ROM drive for your Tivoli Decision Support server, and from the **Start** menu, choose **Run**.

   The Run dialog box appears.

2. In the Run dialog box, type *d*:\tds_guide\setup.exe (where *d*: represents the drive letter for your CD-ROM drive), and click **OK**.

   The Tivoli Decision Support for Enterprise Risk Management Installation window appears.

3. Click **Next**.

   The discovery guide files are placed in the following shared data file directories: Cubes, Models, Reports, Install, and Guide Docs\Tivoli Decision Support for Risk Management.

   After you install Tivoli Decision Support for Enterprise Risk Management, the SQL scripts to build the table, trigger, and views reside in the following shared data file directory: Util\Tivoli Decision Support for Enterprise Risk Management

   **Note:** The SQL scripts that build the table, trigger, and views also reside on the Risk Manager Windows server system in the %BINDIR%\RISKMGR\corr\sql directory or in the Risk Manager Unix server system in the $BINDIR/RISKMGR/corr/sql directory .

4. Click **Finish** to complete the installation.

# 5

# Configuring the Enterprise Risk Management guide



This chapter provides instructions to complete the following configuration tasks (from the Roadmap of Installation and Configuration tasks, Table 1 on page 11):

- Configure the shared data file path.
- Import the Enterprise Risk Management guide.
- Create the archive table, view, and trigger in the Tivoli Enterprise Console database.
- Copy Archive Data from the Risk Manager Version 3.7 Archive Table (optional).
- Run the Archive Sensor Events Job.
- Set up an ODBC data source connection.
- Assign the ODBC data source for Tivoli Decision Support.
- Set the cube parameters.

## Configuring the Shared Data File Path

Before you use the Tivoli Discovery Administrator or the Tivoli Discovery Interface, you must configure the Tivoli Discovery Administrator and the Tivoli Discovery Interface to locate data files that are stored on your system (the local system) or on the network. The Tivoli Discovery Administrator and the Tivoli Discovery Interface uses these files to build cubes and display reports. Refer to ″Access to Shared Data Files″ in ″Chapter 2: Installing Tivoli Decision Support in Stand-alone Mode″ of the Tivoli Decision Support Installation Guide, version 2.1.1 for more information.

If you installed Tivoli Decision Support using the stand-alone installation option, your source files are on your system. For other installations, the shared data files usually reside on a network server. Specify the path to the shared data files when you start the Tivoli Discovery Administrator for the first time.

To set the shared data file path:

1. On the View menu, select **Options**.
   The Options dialog box appears.
2. On the **General** tab, in the **Network** text box, type the name of the drive (and folder, if appropriate) that contains the following folders:

Cubes
Data
Reports

3. Click **OK**.

## Importing the Enterprise Risk Management Guide

Use the following procedure to import the Enterprise Risk Management guide:

1. Start the Tivoli Discovery Administrator.

   If a discovery guide has not been installed on your system, you are prompted to import an installed discovery guide, and to create and assign a data source.

   **Note:** For a step-by-step procedure, see "Running the Tivoli Discovery Administrator for the First Time" in the *Administrator Guide* document.

   If you decline the prompt to import a guide or if you already have at least one guide installed on your system, the Tivoli Discovery Administrator main window opens.

2. From the main window, select **Decision Support Guides** and then select **Import**.
3. Select the **Tivoli Decision Support for Enterprise Risk Management** guide, and click **OK**.

   If you are prompted to add a data source, click **Yes** and complete the following steps:

   a. Select your configured data source and click **Next**.

      **Note:** If the data source you want is not in the list, you must create the data source before you can add the data source. Refer to "Setting Up an ODBC Data Source Connection" on page 19 for instructions.

   b. Type the database user ID and password.

   c. Type the database qualifier:

      For Oracle and Sybase, type `tec`.

      For DB2, leave the database qualifier field blank.

      **Note:** Your database qualifier might be different. Contact your database administrator for additional information.

4. Click **Finish**.

## Creating the Archive Table, View, and Trigger in the Tivoli Enterprise Console Database

Before you create the Archive table, view, and trigger, read "Sizing the Tivoli Enterprise Console Database for the Archive Table" on page 11, and verify that you sized your database to accommodate the increased volume of data. Then, complete the following SQL procedure to create the archive table, view, and the trigger for Oracle, DB2, and Sybase databases.

1. Locate the SQL procedure files. These files can be found in *TDS_Share*`\Util\Tivoli Decision Support for Enterprise Risk Management` (where *TDS_Share* represents the shared data file path defined using the Tivoli Discovery Administrator program). You can also find these files in the Risk Manager Unix server system in the

$BINDIR/RISKMGR/corr/sql directory or in the Risk Manager Windows server system in the %BINDIR%\RISKMGR\corr\sql directory.

2. Execute the SQL procedure files on the system where the Tivoli Enterprise Console database resides.

   **Note:** Copy the procedure files to the Tivoli Enterprise Console system before you execute them, if necessary.

3. For Oracle, type the following:

```
sqlplus userid/password @ service_name @ tds_rm_tec_t_arc.ora.sql
sqlplus userid/password @ service_name @ tds_rm_tec_v_evt.ora.sql
sqlplus userid/password @ service_name @ tds_rm_upd_trigger.ora.sql
```

   where:

   *userid* Represents the database user ID. The default value is tec.

   *password*
   Represents the database user password. The default value is tectec.

   *service_name*
   Represents the Net Service Name for the Oracle database as defined in the Oracle client configuration program (″Net8 Assistant″, ″Net8 Configuration Assistant″ or ″Net8 Easy Configuration″) or the name used to identify each entry in the %ORACLE_HOME%\NETWORK\ADMIN\TNSNAMES.ORA file on the client.

   For DB2, type the following:

```
db2 connect to tec user userid using password
db2 -t -f tds_rm_tec_t_arc.DB2.sql
db2 -t -f tds_rm_tec_v_evt.DB2.sql
db2 -t -f tds_rm_upd_trigger.DB2.sql
```

   where:

   *userid* Represents the database user ID. The default value for UNIX® is db2inst1. The default value for Windows NT is db2admin.

   *password*
   Represents the database user password.

   For Sybase, type the following:

```
isql -Uuserid -Ppassword -Dtec -Sserver -c/ -i tds_rm_t_arc.syb.sql
isql -Uuserid -Ppassword -Dtec -Sserver -c/ -i tds_rm_v_evt.syb.sql
isql -Uuserid -Ppassword -Dtec -Sserver -c/ -i tds_rm_upd_trigger.syb.sql
```

   where:

   *userid* Represents the database user ID. The default value is tec.

   *password*
   Represents the database user password. The default value is tectec.

   *server* Represents the Server Name for the Sybase database as defined by the DSEDIT client configuration program, or the name used to identify each entry in the Sybase interfaces file, %SYBASE%\INI\SQL.INI, on the client.

   **Note:** Your database name, user ID, and password are specific to your platform and environment. Contact your system administrator for additional information.

## Copying Archive Data from the Risk Manager Version 3.7 Archive Table

If you have a previous version of Risk Manager installed on your system and you want to migrate the archive data from the older version to this version, use the following instructions to copy your archive data. If you do not want to migrate your archive data to this version, you can skip this section.

**Note:** The archive table definition for Risk Manager 3.8 differs from previous versions. For Risk Manager 3.8, the archive table contains additional columns and has a different name.

`tds_rm_t_arc_migrate.sql`, which resides in the `TDS_Share\Util` directory, contains the sample SQL to copy event records from the old archive table to the Risk Manager 3.8 archive table. (`tds_rm_t_arc_migrate.sql` also resides in the `$BINDIR/RISKMGR/corr/sql` directory on the Risk Manager Unix server system or in the `%BINDIR%\RISKMGR\corr\sql` directory on the Risk Manager Windows server system.) For the columns that were not defined in previous archive tables, default values of `N/A` are used. If you want to use different values, you can customize the SQL.

The SQL is compatible for all of the database platforms Risk Manager supports. To execute the SQL, use the command line syntax that is appropriate for your database.

## Configuring DB2 for the Archive Sensor Events Job

The default statement heap size for DB2 is too small to support the complex SQL statements that execute when events are copied from the Tivoli Enterprise Console event repository to the Risk Manager archived events table. The following error message is displayed when you run the Archive Sensor Events Job (and its trigger): `SQL0101N The statement is too long or too complex`. To resolve this error, update the statement heap size to be 8000 or more.

To update the heap size, open a DB2 command prompt and type the following:

```
> db2 update db cfg for tec using stmtheap 8000
```

After you update the statement heap size, you must disconnect all applications from the DB2 server so that the change will take effect. After the change takes effect, the following warning message might display: `SQL0437W Performance of this complex query may be sub-optimal`. Because this message is only a warning, you can ignore it.

For more information about DB2 configuration, performance, and tuning refer to the following documents: *IBM DB2 UDB Administration Guide, Volumes 1 through 3* and *IBM DB2 UDB Command Reference*.

## Running the Archive Sensor Events Job

Run the Archive Sensor Events Job to populate the archive table with current event data.

**Note:** Before you can run the Archive Sensor Events Job for DB2 databases, you must make the configuration change described in “Configuring DB2 for the Archive Sensor Events Job”.

To run the Archive Sensor Events Job:

1. At the Tivoli desktop, double-click the **TEC-Region** icon.
2. Double-click the **Tasks for Enterprise Risk Management** icon.
3. Double-click the Job icon labeled **Archive_Sensor_Events**. A job output window opens. After the job completes, the results of the job display in the window.

   If no messages appear under **Standard Error Output**, then the job completed successfully.
4. Click **Close**.

To keep the data in the archive table current, execute the Archive Sensor Events job regularly. You can schedule the Archive Sensor Events job to run automatically. Refer to ″TEC tasks for Archiving Events″ in the *Tivoli Risk Manager User's Guide 3.8* for instructions.



## Setting Up an ODBC Data Source Connection

Before you create an ODBC connection, install and configure your database client. Consult your database administrator for the appropriate client configuration. Your system must have a valid client configuration for the ODBC connection that Tivoli Decision Support uses to access your database.

After you install and configure your database client, set up an ODBC Data Source Connection to create the network identification required to access the Tivoli Enterprise Console database from the systems running Tivoli Decision Support. Refer to the following sections to set up an ODBC data source connection for your database.

### Setting up an ODBC Data Source Connection to a DB2 database

Register the DB2 database with the ODBC driver manager as a data source. On Windows 95 and Windows NT, you can make the data source available to all users of the system (a system data source) or only the current user (a user data source). You can use any of the following three methods to add the data source; however, if you installed the Client Configuration Assistant (CCA) when you installed DB2, it is recommended that you use the first method.

#### Using the CCA to register the DB2 database as a data source

To use the CCA to register the DB2 database as a data source:

1. Start the DB2 Client Configuration Assistant program. A list of available DB2 databases is displayed.
2. If your database is in the list, select the database and complete the following steps:
   a. Click **Properties**. The Database Properties window opens.
   b. If it is not already selected, select the **Register this database for ODBC** check box.

      On Windows 95 and Windows NT, you can use the radio buttons to add the data source as either a user or system data source.
   c. Click **OK**.

   If your database is not in the list, complete the following steps:

   a. Click **Add**. The Add Database SmartGuide dialog box opens.

b. Select **Manually configure a connection to a DB2 database**. Click **Next**.

c. Enter the hostname and port number of the DB2 server.

   The default port number for DB2 servers is 50000. Check with your database administrator for the proper port number.

   Do not enter a service name.

d. Click **Next**.

e. Enter the name of the database as it is defined on the server.

   The name must be `TEC` for all Risk Manager installations.

f. Enter an alias and description.

   The alias can be any name not already used in the CCA database list.

g. Click **Next**.

h. Verify that the **Register this database for ODBC** check box is selected.

i. Click **Done**.

j. Click **Close** to finish.

**Note:** If you want to verify connectivity, click **Test Connection** before you click **Close** to finish.

### Using the Microsoft 32-bit ODBC Administration tool to register the DB2 database as a data source

To use the Microsoft 32-bit ODBC Administration tool to register the DB2 database as a data source:

1. Access the Microsoft 32-bit ODBC Administration tool from the icon in the Control Panel. Or, you might choose to access the tool by running the **odbcad32.exe** command from the command line.
2. On Windows 95 and Windows NT, the list of user data sources appears by default. If you want to add a system data source, click **System DSN** or select the **System DSN** tab (depending on the platform).
3. Click **Add**.
4. Double-click the **IBM DB2 ODBC Driver** in the list.

   If the DB2 database is in the dropdown list, then the database is already registered with ODBC. Click **Cancel** to finish.

   If the database is not in the dropdown list, use the following instructions to add the database.

   a. Click **Add** or **Add Database**. The Add Database SmartGuide dialog box opens.

   b. Select **Manually configure a connection to a DB2 database**. Click **Next**.

   c. Enter the hostname and port number of the DB2 server.

      The default port number for DB2 servers is 50000. Check with your database administrator for the proper port number.

      Do not enter a service name.

   d. Click **Next**.

   e. Enter the name of the database as it is defined on the server.

The name must be TEC for all Risk Manager installations.

f. Enter an alias and description.

The alias can be any name not already used in the CCA database list.

g. Click **Next**.

h. Verify that the **Register this database for ODBC** check box is selected.

i. Click **Done**.

j. Click **Close** to finish.

**Note:** If you want to verify connectivity, click **Test Connection** before you click **Close** to finish.

### Using the CATALOG ODBC DATA SOURCE command to register the DB2 database as a data source

To use the **CATALOG ODBC DATA SOURCE** command to register the DB2 database as a data source:

You can issue the **CATALOG ODBC DATA SOURCE** command at the command-line processor on Windows 95 and Windows NT to register the DB2 database with the ODBC driver manager as a data source. For example, to use this command you might create a command-line processor script to register the required databases. Then run this script on all of the machines that require access to the DB2 databases through ODBC. See the **CATALOG [ user | system ] ODBC DATA SOURCE** command in the *Command Reference* for more information.

## Setting Up an ODBC Data Source Connection to an Oracle database

This section describes how to set up an ODBC connection to an Oracle database.

During the database client configuration, you need to create a database alias (Net Service Name) for the Tivoli Enterprise Console database. Use this alias as the data source server name in step 7 of the following procedure.

**Note:** Contact your system administrator for specific information to set up your database client. Use the Net8 Easy Configuration program to create a database alias.

After you create an Oracle database alias, use the following procedure to create an ODBC data source for the Tivoli Enterprise Console database.

1. On the Control Panel, select the **Data Sources (ODBC)** icon, or run the **odbcad32.exe** command from the command line.
2. Select the **System DSN** tab.
3. Click **Add**.
4. Select **Oracle ODBC Driver**, and click **Finish**.
5. Type a meaningful name for this ODBC data source in the **Data Source Name** text box.

   **Note:** Record the data source name. Use this data source name when adding a data source for the guide in Tivoli Discovery Administrator.
6. Type a description for the data source in the **Description** text box.
7. Type the database Net Service Name in the **Service Name** text box.

**Note:** The database Net Service Name must be the alias that you gave to the database when you configured the database client.

8. Type the Tivoli Enterprise Console database user name (the default is `tec`) in the **Userid** text box.
9. Click **OK** twice to save Data Source Name and exit the ODBC Administrator.

## Setting Up an ODBC Data Source Connection to a Sybase Database

This section describes how to set up an ODBC connection to a Sybase database.

During the database client configuration, you need to create a database alias for the Tivoli Enterprise Console database. Use this alias as the data source server name in step 7 of the following procedure.

**Note:** Contact your system administrator for specific information to set up your database client. Use the Sybase DSEdit program to create a database alias.

After you create a Sybase database alias, use the following procedure to create an ODBC data source for the Tivoli Enterprise Console database.

1. On the Control Panel, select the **Data Sources (ODBC)** icon, or run the **odbcad32.exe** command from the command line.
2. Select the **System DSN** tab.
3. Click **Add**.
4. Select **Sybase ASE ODBC Driver**, and click **Finish**. The **ODBC Sybase ASE Setup** dialog box opens.
5. Type a meaningful name for this ODBC data source in the **Data Source Name** text box.

   **Note:** Record the data source name. Use this data source name when adding a data source for the guide in Tivoli Discovery Administrator.
6. Type a description for the data source in the **Description** text box.
7. Type the database server name in the **Server Name** text box.

   **Note:** The database server name must be the alias that you gave to the database when you configured the database client.
8. Type the Tivoli Enterprise Console database name (the default is `tec`) in the **Database Name** text box.
9. Click **Test Connect** to verify the data source connection. Enter the appropriate database user ID and password.
10. Click **OK** twice to save Data Source Name and exit the ODBC Administrator.

# Assigning the ODBC Data Source for Tivoli Decision Support

Assigning the ODBC data source for the Enterprise Risk Management guide enables Tivoli Decision Support to communicate with the Tivoli Enterprise Console database. Do the following to assign the ODBC data source for the Enterprise Risk Management guide:

1. Using the Tivoli Discovery Administrator, select the **Data Sources** folder.

If your data source is not in the **Properties** window, use the following to add your data source:

a. Right-click in the **Properties** window and click **Add**. The **Add Datasource** dialog box opens.

b. Select your data source from the dropdown list for the **DSN** field.

**Note:** If your data source is not in the dropdown list, you must create the data source using the instructions in "Setting Up an ODBC Data Source Connection" on page 19.

c. Type your database user ID and password. For DB2, the default user ID is `db2inst1` or `db2admin` and there is no default password. For Oracle and Sybase, the default user ID value is `tec` and the default password is `tectec`.

d. Type in the database qualifier. For Oracle and Sybase, use `tec`. For DB2, leave this field blank.

e. Click **OK**. Your data source is now listed in the dropdown list for the **DSN** field.

2. Right click the **Data Sources** folder and select **Assign Data Source**.

3. In the **Assign Data Source** dialog box, select the following Risk Manager queries to connect to the data source:

RM Anti-Virus DB Status
RM Anti-Virus Run Status
RM Anti-Virus Scan Status
RM Anti-Virus Workstations
RM TEC Archive
RM TEC Class Hierarchy
RM TEC Date Info
RM TEC Sensor Info
RM TEC Source Info
RM TEC Target Info

Alternatively, if you want to assign the desired data source to all queries, click the **Select All** button.

4. Select the desired data source from the list.

5. Click **OK** to assign the data source to the selected queries.

6. In the Properties pane of the Discovery Administrator, right click the data source you just assigned, and select **Test Connectivity**.

If the Tivoli Discovery Administrator message dialog box appears with the message `Error connecting to Data Source – DataSourceName`, click **Details** to display more information about the connection error. Click **OK**, and verify the data source definition, user ID, password, and qualifier.

If the connection is successful, the Test Data source dialog box appears with the message `Connection Successful`. Click **OK**.

## Setting the Cube Parameters

Tivoli Decision Support for Enterprise Risk Management builds two cubes, the archived events cube and the anti-virus status cube. These cubes extract specific records out of the Tivoli Enterprise Console database and generate reports that you can view.

The archived events cube and the anti-virus status cube contain three types of parameters: range, terminology, or categorization. You can change the default cube parameter values.

**Range parameters**

Range parameters specify a date range that limits the number of records that are returned by the database query.

For both Enterprise Risk Manager cubes, you can use the **Date Range** parameter to select a specific range of records. The **Date Range** parameter determines the time period that you want to examine using explicit values, such as start and end dates, or a calculated value, such as the last three months or the last six months. Calculated values are relative to the current date.

**Terminology parameters**

Terminology parameters customize the text displayed in your reports. Using terminology parameters, you can display more descriptive terms in your reports, instead of displaying data from the columns of the archive table.

The **Risk Manager Archived Events** cube includes the following **Terminology** parameter: **Alternate Severity**. The **Alternate Severity** parameter displays an alternate value for the **Severity** field in views or reports. For example, FATAL defaults to Serious and HARMLESS defaults to Informational.

**Categorization parameters**

Categorization parameters are used to customize reports. For example, the **Virus Scan Interval** parameter in the **Risk Manager Anti-Virus Status** cube can be used to specify the maximum number of days that can pass between executing the anti-virus software on each system in your network. You can specify the appropriate value for your cube by double-clicking on this parameter and editing the interval definition.

The **Risk Manager Archived Events** cube includes the following **Categorization** parameter: **Day or Night**. The **Day or Night** parameter specifies limits that you consider valid for distinguishing between day and night. The value for this parameter represents the hours in a day, using a twenty-four hour clock.

You can specify the correct values to build your cube by double-clicking on the parameter or right-clicking on the parameter and selecting the **Set Values** option.

# 6

# Managing the Enterprise Risk Management guide

After you install and configure the Enterprise Risk Management guide you can use the tasks described in this chapter to manage your environment. This chapter enables you to complete the following tasks:

- Build cubes
- Specify the database Logon for Crystal Reports
- Delete records from the archive table
- Uninstall the Enterprise Risk Management guide



## Building the Cubes

The archived events cube and the anti-virus status cube contain information from the last time you built them only. To update the data in your cube, rebuild the cube periodically. You can schedule cubes to be built at regular intervals or you can build the cubes manually. Refer to the following sections for instructions to schedule a cube build or to build a cube manually.

### Scheduling Cube Builds

When you schedule cube builds, you enable your cubes to be built at regular intervals. For example, you might schedule nightly builds. Because both cubes gather their data from the Tivoli Enterprise Console database, you can improve performance by staggering the start times between each cube build and by scheduling the builds during periods of decreased database activity.

After you create a cube build schedule, you must activate the scheduling program for the build to occur on schedule. Windows 95 and Windows 98 use a different scheduling program from Windows NT. For Windows 95 or Windows 98, you use the Cognos Scheduler; for Windows NT, you use the Tivoli Decision Support Scheduler. Refer to "Activating the Build Scheduler on Windows 95 or Windows 98" on page 26 and "Activating the Build Scheduler on Windows NT" on page 27 for instructions to activate the cube builds that you scheduled.

**Note:** The following procedures use the Tivoli Discovery Administrator to create a cube building schedule. See *Tivoli Decision Support Administrator Guide* for more information.

To create a cube build schedule:

1. Start the Tivoli Discovery Administrator. Be sure that the **Toggle Wizard Use** box is not selected.
2. On the **Scheduled Tasks** menu, click **Add**.

   The Add Schedule dialog box appears.
3. Type a name for the schedule that you are creating in the **Name** text box.
4. On the **Task** tab, select the cube that you want to build from the cube list.
5. On the **Schedule** tab, select the frequency of the cube builds.
6. Fill in the **Time** and **Duration** fields. If you wish the scheduled builds to occur indefinitely into the future, do not check the **To** box in the **Duration** field.
7. Click **OK**.

## Activating the Build Scheduler on Windows 95 or Windows 98

For scheduled cube builds to occur, the scheduler must be running. After you have created a cube build schedule, use the following instructions to activate the scheduler for Windows 95 or Windows 98:

**Note:** The following procedures use the Tivoli Discovery Administrator to determine the schedule task ID, and the Cognos Scheduler to execute the scheduled cube building task.

1. In the Tivoli Discovery Administrator program, click **Scheduled Tasks**.
2. In the Properties pane, double-click the task you want to schedule.
3. From the Edit Schedule dialog box, record the schedule Task ID for use in step 7.
4. Click **Cancel**.
5. On the **Start** menu, under Programs, choose **Cognos 6.5**, and click **Scheduler** to start the Cognos Scheduler.
6. On the **Insert** menu, click **Recurring task**.

   The Insert Task dialog box appears.
7. On the **Identification** tab, type the following command string in the **File name** text box:

   `"`*`directory path`*`\edamin.exe" /TaskID=`*`X`*

   where *directory path* is the installation directory path for Tivoli Decision Support and *X* is the schedule Task ID from step 3.

   **Note:** Enclose the directory path and the `edamin.exe` in quotation marks as shown in the following example:

   ```
   "c:\Program Files\TDS 2.1\edamin.exe" /TaskID=1
   ```
8. Type a brief description of the cube and the schedule in the **Description** text box.
9. On the **Timetable** tab, specify the cube building frequency, run time, and duration.
10. Repeat this procedure for each cube.
11. Minimize Cognos Scheduler.

    **Note:** Cognos Scheduler must be running for the cube to build at the scheduled time.

### Activating the Build Scheduler on Windows NT

For scheduled cube builds to occur, the scheduler must be running. After you have created a cube build schedule, use the following instructions to activate the scheduler for Windows NT:

**Note:** The following procedure uses the Tivoli Decision Support Scheduler service to execute the scheduled cube building task on Windows NT.

1. Open the Windows NT Control Panel and choose the **Services** icon.
2. In the Services dialog box, select **TDS Process Scheduler**.
3. If the service status is **Started**, then the scheduler is already active. Continue with step 6.

   If the status is **Stopped** or there is no status, then click **Start**.
4. Click **Startup** and select the frequency of the cube builds. For example, if you want the scheduler to run every time the host restarts, select **Automatic** for the **Startup Type**. If you want to schedule the cube builds manually, select **Manual** for the **Startup Type**.
5. Click **OK**.
6. Click **Close** to exit the Services dialog box.

## Building Cubes Manually

Use the following procedure to build a cube manually:

1. From the Administrator pane in the Tivoli Discovery Administrator window, double-click **Cubes**.
2. Right-click the **Enterprise Risk Manager Anti-Virus Status** cube, and select **Build**.

   The Confirm Cube Build dialog box appears. The date ranges appear in the dialog box.
3. Click **Yes** if you agree to build the cube.

   Tivoli Decision Support connects to your database and retrieves the records specified in your query. The size of your data and the network speed affect the time required to retrieve all records. Use the status bar to check the status of the processing.

   The Cube Transform Status dialog box appears. Processing messages appear in the dialog box.
4. Review the processing messages for any errors.

   If an error generates an error dialog box, review the error, and click **OK**.
5. Click **Close**.
6. Right-click the **Enterprise Risk Manager Archived Events** cube, and select **Build**.

   The Confirm Cube Build dialog box appears with the selected date range displayed.
7. Click **Yes** if you agree to build the cube.

   Tivoli Decision Support connects to your database and retrieves the records specified in your query. The size of your data and the network speed affect the time required to retrieve all records. Use the status bar to check the status of the processing.

   The Cube Transform Status dialog box appears. Processing messages appear in the dialog box.
8. Review the processing messages for any errors.

   If an error generates an error dialog box, review the error, and click **OK**.

9. Click **Close**.
10. Start the Tivoli Discovery Interface.
11. Use the discovery guide to review the views for each topic. Topics are presented as questions.

    For more information about how to use the Tivoli Decision Support Discovery Interface, see the Tivoli Decision Support *Users Guide*.

## Specifying the Database Logon for Crystal Reports

The first time you run a Crystal Report using the Tivoli Discovery Interface, the Logon dialog box displays. You can use the Logon dialog box to set the data source by specifying the User Name, Password, DSN, Qualifier, and the Database Name and type for the data source you defined. Then click **OK**.

**Note:** You set the qualifier value when you defined the database.

You can also configure the database logon by selecting **View —> Options** from the Tivoli Discovery Interface main menu. From the **Options** dialog box, select the **Database** tab, complete the required fields and click **OK**.

## Recommended Logon Values for Crystal Reports

Crystal Reports does not work with all ODBC drivers. If you enter a logon value in the wrong case, you will get an error when you try to run your report because Crystal Reports is case sensitive. The following table lists the recommended default logon values (case sensitive) and ODBC driver versions, which have had reports tested successfully. Other drivers might work, but have not been tested.

*Table 2. Crystal Report Default Logon Values*

| Database | User ID | Password | Qualifier | Database | ODBC Driver |
|---|---|---|---|---|---|
| DB2 | db2inst1 (Unix)<br>db2admin (Windows NT) | no default | DB2INST1 (Unix)<br>DB2ADMIN (Windows NT) | TEC | IBM DB2 ODBC Driver 6.1 |
| Oracle | tec | tectec | TEC | TEC | Oracle ODBC driver 8.1.5 |
| Sybase | tec | tectec | tec | tec | Intersolv 3.0 ODBC driver for Sybase System 10 and Crystal Reports |

## Deleting Records from the Archive Table

Periodically purge the archive table (used by Tivoli Decision Support for Enterprise Risk Management) to avoid building cubes that contain outdated data. By purging the archive table, you can manage the database resource and improve cube building performance. It is recommended that you back up the Archive table before you delete records. Refer to the following sections for steps to delete records from Oracle, DB2, and Sybase databases.

## Deleting Records from the Archive Table in an Oracle Database

Use the following steps to delete records from the archive table in an Oracle Database:

1. Connect to the Oracle database server. For example, type:

   ```
   sqlplus tec/password@service_name
   ```

   Where *password* represents the database user password and *service_name* represents the Net Service Name for the Oracle database as defined in the Oracle client configuration program (″Net8 Assistant″, ″Net8 Configuration Assistant″ or ″Net8 Easy Configuration″) or the name used to identify each entry in the %ORACLE_HOME%\NETWORK\ADMIN\TNSNAMES.ORA file on the client.

2. At the SQL> prompt, type the following command to delete records from the archive table (where dd-Mon-yyyy represents the two-digit number of the day, three-character abbreviation for the month, and the four-digit number of the year separated by hyphens):

   ```
   SQL>delete from rm_t_arc where date_event < 'dd-Mon-yyyy';
   ```

   For example, to delete all records prior to July 1, 2000, type:

   ```
   SQL>delete rm_t_arc where date_event < '01-JUL-2000'
   ```

3. At the SQL> prompt, type the following to display that status of autocommit:

   ```
   SQL>show autocommit
   ```

   The autocommit status appears. If the autocommit is on, you do not need to commit your delete because Oracle automatically commits your work. Continue with step 4.

   If autocommit is off, at the SQL> prompt, type the following to commit the deletion of the archive table entries:

   ```
   SQL>commit;
   ```

4. At the SQL> prompt, type the following to exit SQL:

   ```
   SQL>exit;
   ```

## Deleting Records from the Archive Table in a DB2 Database

Use the following steps to delete records from the archive table in a DB2 Database:

1. Open a DB2 Command Line Processor session.
2. Connect to the DB2 database.
3. Type the following command to delete the records from the archive table (where MM/DD/YYYY represents the two-digit number of the month, two-digit number of the day, and the four-digit number of the year separated by forward slashes):

   ```
   delete from rm_t_arc where date_event < 'MM/DD/YYYY'
   ```

   For example, to delete all records prior to July 1, 2000, type:

   ```
   delete from rm_t_arc where date_event < '07/01/2000'
   ```

4. Type the following command to disconnect from the database:

   ```
   terminate
   ```

**Note:** The DB2 UDB Command Line Processor automatically commits all commands. This feature can be overridden using the **UPDATE COMMAND OPTIONS** command. This command is documented in the *DB2 UDB Command Reference*.

## Deleting Records from the Archive Table in a Sybase Database

Use the following steps to delete records from the archive table in a Sybase database:

1. Connect to the Sybase database server. For example, type:

   ```
   isql -Utec  -Ppassword  -Dtec  -Sserver -C/
   ```

   Where *password* represents the database user password and *server* represents the Server Name for the Sybase database as defined by the DSEDIT client configuration program, or the name used to identify each entry in the Sybase interfaces file, `%SYBASE%\INI\SQL.INI`, on the client.

2. At the 1> prompt, type the following command to delete records from the archive table (where `MM/DD/YYYY` represents the two-digit number of the month in the order that the month comes in the year, the two-digit number of the day, and the four-digit number of the year separated by forward slashes):

   ```
   1> delete from rm_t_arc where date_event < 'MM/DD/YYYY'
   ```

   For example, to delete all records prior to July 1, 2000, type:

   ```
   1> delete from rm_t_arc where date_event < '07/01/2000'
   2>/
   ```

3. Type `quit` or `exit` to disconnect from the database.

# Uninstalling the Enterprise Risk Management guide

To uninstall a discovery guide, use the following procedure:

1. From the Administrator pane, select the Decision Support Guides object folder. The list of installed discovery guides appears in the Properties pane.
2. From the Properties pane, right-click the discovery guide you want to delete. A submenu appears.
3. From the submenu, choose **Delete**. The Delete Decision Support Guide dialog box appears.
4. Choose **Yes**. The Discovery Administrator window appears. The discovery guide is removed from the Properties pane and any associated views are removed from the Discovery Interface.

After you uninstall the Enterprise Risk Management guide, you can reinstall it by following the same instructions that you used for the initial installation (see “Installing the Enterprise Risk Management Guide” on page 13).

# 7

# Troubleshooting

## Troubleshooting Cube Builds

The table below lists potential cube building problems, the reasons why the problem might occur, and an action you can take to resolve the problem.

*Table 3. Troubleshooting Cube Builds*

| Problem | Reason | Action |
|---|---|---|
| The Tivoli Discovery Administrator reports that a cube cannot be built. | **Reason 1**: The current cube file is being used by another application. | **Solution 1**: Close all copies of the Tivoli Discovery Interface that are running. Copy the *CubeName*.mdc file from the Tds\Cubes\Temp directory to the Tds\cubes directory (where *Tds* represents the Tivoli Decision Support shared data file path), to replace the existing cube. |
| | **Reason 2**: The queries returned insufficient data to build a cube. | **Solution 2**:Verify your queries. |
| All of the Tivoli Discovery Interface processes are closed, and the cube still does not build. | A copy of Cognos PowerPlay might still be running in the background, which might also prevent cube builds from succeeding. | Open the Task manager, and look for the process pwrplay.exe. If you find it, end the process and rebuild the cube. |

## Troubleshooting Reports

The table below lists potential report problems, the reasons why the problem might occur, and an action you can take to resolve the problem.

*Table 4. Troubleshooting Reports*

| Problem | Reason | Action |
|---|---|---|
| While using the Tivoli Discovery Interface, a Cognos PowerPlay report icon appears with the X symbol (a circle bisected by a diagonal line), and you cannot open the report. | This symbol indicates that the cube is unavailable. | Contact your Tivoli Decision Support administrator, and request that the cube be rebuilt. |

*Table 4. Troubleshooting Reports (continued)*

| Problem | Reason | Action |
|---|---|---|
| The Tivoli Discovery Interface freezes at the wait cursor when you try to open a report. | The Tivoli Discovery Interface might have lost its connection to the Cognos PowerPlay task. | Close the Tivoli Discovery Interface and PowerPlay. Restart the Tivoli Discovery Interface, and your reports open. |
| The report you opened contained no data. | There might be data in the report, but there is no data in drill down. The report can be filtered on a dimension. | Look at the dimension bar, and check if any of the values (especially the date dimension) are drilled down. |
| Crystal Reports do not have a left margin. | The type of printer attached to a workstation influences the alignment of Crystal reports. | Try disconnecting the printer and restarting Tivoli Decision Support. |
| Crystal Reports, on a Sybase database, returns an ODBC error: `The keywords LEFT OUTER JOIN were not found in an outer join escape sequence.` | The Sybase ODBC driver you are using is not compatible with the Crystal Reports print engine used by the Tivoli Discovery Interface. | Log on to the database using an ODBC driver that is known to be compatible. Refer to "Recommended Logon Values for Crystal Reports" on page 28. |
| Crystal Reports returns an ODBC error that the table or column is undefined. | Column names are case sensitive. | For Sybase, verify that you executed the Sybase SQL script (tds_rm_t_arc.syb.sql) that defines an alternate view of the database using upper case names. Refer to "Creating the Archive Table, View, and Trigger in the Tivoli Enterprise Console Database" on page 16. |
| Crystal Reports returns an ODBC error that the table or view does not exist. | The Qualifier you entered in the database logon might be the wrong value or might be the wrong case. | Type the correct Qualifier in the correct case. Refer to "Recommended Logon Values for Crystal Reports" on page 28. |
| The Tivoli Discovery Interface cannot open a Crystal Report. | You might be addressing the wrong database. | The first time you open a Crystal Report, a logon dialog box is displayed. Verify that the user ID and the password are correct. Click Options on this dialog box and verify that you are using the correct ODBC connection and that the connection information is correct. If you change any connection parameters and save them, you must exit the Tivoli Discovery Interface and re-enter before the changes will take effect. |

# 8

# Limitations



This section lists the known software limitations for the 1.1 release of Tivoli Decision Support for Enterprise Risk Management. Workarounds are provided when applicable.

**Limitations:**

- Bar labels along the X-axis on bar graphs might appear unreadable because the software automatically selects a font small enough to fit the entire label within the width of the bar.

  **Workarounds:**

  - Maximize the Tivoli Discovery Interface window, or select Full Screen view, either from the **View** menu or by clicking the appropriate icon on the toolbar.
  - From the Discovery Interface horizontal menu, select **Format** → **Display Options** → **Scrolling**. Set Maximum Columns Displayed to 5 (the smallest number allowed). Click **OK**.

- By default, all events are stored in the Risk Manager database with event times represented in Coordinated Universal Time (UTC) format. When events are displayed, the event times might appear in local time or UTC, according to the following criteria:

  - Tivoli Enterprise Console and Crystal Reports (″All Closed Events - by Severity″ and ″Archived Events - in Date Range″) display the time of the event as the local time on the Risk Manager server when the event was received.
  - All other discovery guide views display the time of event as the time the event was generated, in Coordinated Universal Time (UTC).

  **Workarounds:**

  - If you want the discovery guide views to display local time at the Risk Manager server, then you can do so by customizing the SQL in the DB views (see “Risk Manager Event Views” on page 38). You must adjust the calculation of the TIME_EVENT (and DATE_EVENT for DB2) column in the view definitions to account for the difference between the local time and UTC.
  - If you want the Crystal Reports to display event time in UTC rather than local time, then you must customize the SQL queries in the Crystal Report definition files (.rpt) in the `<Shared_Data_Path>\Reports` directory. You must select the TIME_EVENT column, instead of the TIME_RECD column, in the queries. In order to customize the queries, you will need to have a copy of Seagate Crystal Reports 6.0 Report Designer software.

# A

# Database Schema

The source of data for the Enterprise Risk Management guide is the Tivoli Enterprise Console database. To lessen the impact on the Tivoli Enterprise Console, the Enterprise Risk Management guide only reads from an archived copy of the Tivoli Enterprise Console data. The Enterprise Risk Management guide reads from an archive table that is populated by a database trigger.

In addition to the trigger and archive table, the Enterprise Risk Management guide creates new database views to join together all the core Tivoli Enterprise Console event attributes with Risk Manager-specific slots of interest to the Enterprise Risk Management guide. These views make the trigger SQL simpler and facilitate debugging of the Tivoli Enterprise Console database with respect to Risk Manager events.

The archive table, views, and triggers must be created as part of the Enterprise Risk Management guide configuration (see "Creating the Archive Table, View, and Trigger in the Tivoli Enterprise Console Database" on page 16). The SQL files used to create the table, views, and triggers reside in `Util\Tivoli Decision Support for Enterprise Risk Management`, the shared data file path.

## Archive Table

The archive table (rm_t_arc) definition is based on a subset of columns from the core Tivoli Enterprise Console table (tec_t_evt_rep) and selected Risk Manager-specific slots from the Tivoli Enterprise Console slot table (tec_t_slots_evt). Each event is represented by one record in the event table and several records in the slot table.

Records in the slot table are tuples consisting of the slot name and slot value. Risk Manager only uses certain records with particular slot names.

The following table lists the SQL files that define the archive table for DB2, Oracle, and Sybase databases:

*Table 5. Archive Table SQL Files*

| Database | SQL File Name |
|---|---|
| DB2 | `tds_rm_tec_t_arc.DB2.sql` |
| Oracle | `tds_rm_tec_t_arc.ora.sql` |
| Sybase | `tds_rm_t_arc.syb.sql` |

The following table describes the columns in the archive table and indicates their origin in the Tivoli Enterprise Console database. Columns taken from the event table (tec_t_evt_rep) have the same column name in the archive table, except where indicated in the Origin Table

column. Columns taken from the slot table (tec_t_slots_evt) give the slot name in parentheses.

*Table 6. Archive Table Column Descriptions and Origins*

| Column Name | Datatype | Origin Table (Slot) | Column Description |
|---|---|---|---|
| SERVER_HNDL | Integer | tec_t_evt_rep | Unique ID for Tivoli Enterprise Console server (part of event record key) |
| DATE_RECEPTION | Integer | tec_t_evt_rep | Coordinated Universal Time (UTC) of event reception, expressed in seconds since January 1, 1970 (part of event record key). |
| EVENT_HNDL | Integer | tec_t_evt_rep | Unique ID for events with the same date_reception value (part of event record key) |
| DATE_EVENT | Date * | tec_t_slots_evt (rm_Timestamp32) | Date of event (UTC) |
| TIME_EVENT | Timestamp * | tec_t_slots_evt (rm_Timestamp32) | Date and time of event (UTC) |
| CLASS | Varchar(64) | tec_t_evt_rep | Event class name |
| SUB_SOURCE | Varchar(32) | tec_t_evt_rep | Type of Risk Manager event (IDS or Miscellaneous) |
| HOSTNAME | Varchar(128) | tec_t_slots_evt (rm_SensorHostname) | Name of host reporting event |
| ORIGIN | Varchar(32) | tec_t_evt_rep | IP address of host reporting event |
| SUB_ORIGIN | Varchar(32) | tec_t_evt_rep | Sensor type (netranger, webids, and so forth) of reporting host |
| SEVERITY | Integer | tec_t_evt_rep | Severity level of event |
| TIME_RECD | Varchar(30) | tec_t_evt_rep (DATE_EVENT) | ASCII representation of event reception date and time (local time on Risk Manager server) |
| MSG | Varchar(255) | tec_t_evt_rep | Descriptive message displayed on Tivoli Enterprise Console |
| REPEAT_COUNT | Integer | tec_t_evt_rep | Number of repeat occurrences of the same event |
| TIMESTAMP32 | Integer | tec_t_slots_evt (rm_Timestamp32) | Coordinated Universal Time (UTC) of event generation, expressed in seconds since January 1, 1970. |
| SRC_HOSTNAME | Varchar(128) | tec_t_slots_evt (rm_SourceHostname) | Name of host identified as source of intrusion event |

*Table 6. Archive Table Column Descriptions and Origins (continued)*

| Column Name | Datatype | Origin Table (Slot) | Column Description |
|---|---|---|---|
| SRC_IPADDR | Varchar(32) | tec_t_slots_evt (rm_SourceIPAddr) | IP address of host identified as source of intrusion event |
| SRC_PORT | Varchar(16) | tec_t_slots_evt (rm_SrcPort) | Host port number (or name) identified as source of intrusion event |
| DST_HOSTNAME | Varchar(128) | tec_t_slots_evt (rm_DestinationHostname) | Name of host identified as target of intrusion event |
| DST_IPADDR | Varchar(32) | tec_t_slots_evt (rm_DestinationIPAddr) | IP address of host identified as target of intrusion event |
| DST_PORT | Varchar(16) | tec_t_slots_evt (rm_DstPort) | Host port number (or name) identified as target intrusion event |
| SIGNATURE | Varchar(255) | tec_t_slots_evt (rm_Signature) | Descriptive string identifying intrusion event |
| CLASS_CAT | Varchar(64) | tec_t_slots_evt (rm_ ClassCategoriesDescription) | Description of category (defined in `riskmgr_categories.pro`) used for event correlation |
| SERVICE | Varchar(32) | tec_t_slots_evt (rm_Servicename) | Name of service (Telnet, FTP, and so forth) associated with the intrusion event |
| CUSTOMER_ID | Varchar(64) | tec_t_slots_evt (rm_CustomerID) | Identifier for customer (individual or company) that is the target of the intrusion event |
| CATEGORY | Varchar(64) | tec_t_slots_evt (rm_Category) | Miscellaneous event category (access, configuration, policy, state, and so forth) |
| PRINCIPAL | Varchar(64) | tec_t_slots_evt (rm_Principal) | User or group ID that initiated the miscellaneous event |
| OBJECT_TYPE | Varchar(64) | tec_t_slots_evt (rm_ObjectType) | Miscellaneous event object type (file, system, user, group, and so forth) |
| OBJECT | Varchar(64) | tec_t_slots_evt (rm_Object) | Miscellaneous event object name (file name, hostname, user name, user group, application name, and so forth) |
| ACTION | Varchar(32) | tec_t_slots_evt (rm_Action) | Miscellaneous event actions (create, modify, delete, start, stop, and so forth) |
| RESULT | Varchar(32) | tec_t_slots_evt (rm_Result) | Miscellaneous event result (success, complete, failure, denied and so forth) |

**Note:** * indicates that dates and times are represented differently in each of the three databases. For DB2, DATE_EVENT represents the date only, while TIME_EVENT represents both the date and time. For Oracle and Sybase databases, DATE_EVENT and TIME_EVENT represent the same value, which includes both the date and time.

## Risk Manager Event Views

For each database, one or more views are defined that select data from the Tivoli Enterprise Console event database, which can be inserted into the archive table described in the previous section. The views select a subset of columns from the core Tivoli Enterprise Console event table (tec_t_evt_rep) and selected Risk Manager-specific slots from the Tivoli Enterprise Console slot table (tec_t_slots_evt).

The following table lists the SQL files that define the views for DB2, Oracle, and Sybase:

*Table 7. View SQL Files*

| Database | SQL File Name |
|---|---|
| DB2 | `tds_rm_tec_v_evt.DB2.sql` |
| Oracle | `tds_rm_tec_v_evt.ora.sql` |
| Sybase | `tds_rm_v_evt.syb.sql` |

### DB2 and Oracle Views

For DB2 and Oracle, the following views are defined:

*Table 8. DB2 and Oracle Views*

| View | Description |
|---|---|
| rm_v_ids_evt | All Risk Manager events (SOURCE='RISKMGR') that are subclasses of RM_IDSEvent (SUB_SOURCE='IDSEVENT'). |
| rm_v_misc_evt | All Risk Manager events (SOURCE='RISKMGR') that are subclasses of RM_MiscEvent (SUB_SOURCE='MISCEVENT'). These events include additional slots (category, principal, object_type, object, action, result) that are not defined in RM_IDSEvent subclasses. |
| rm_v_evt | The union of the previous two views. This view encompasses all Risk Manager events that represent security events of interest to the Enterprise Risk Management guide. |

## Sybase Views

For Sybase, the following views are defined:

*Table 9. Sybase Views*

| View | Description |
|---|---|
| rm_v_evt | All Risk Manager events (SOURCE='RISKMGR') that are subclasses of RM_IDSEvent (SUB_SOURCE='IDSEVENT') and RM_MiscEvent (SUB_SOURCE='MISCEVENT'). |
| rm_v_misc_evt | All Risk Manager events (SOURCE='RISKMGR') that are subclasses of RM_MiscEvent (SUB_SOURCE='MISCEVENT'). This view omits slots (src_hostname, src_ipaddr, src_port, dst_hostname, dst_ipaddr, dst_port) that are common to all Risk Manager events and includes additional slots (category, principal, object_type, object, action, result) that are only defined in the RM_MiscEvent subclasses. |

# Database Trigger

The database trigger copies Risk Manager event data from the Tivoli Enterprise Console event and slot tables into the archive table. The trigger fires when the rm_Archived slot in the slot table (tec_t_slots_evt) changes from 0 to 1. You can update the rm_Archived slot using the Archive Sensor Events job in the Tivoli Enterprise Console Task Library.

When the trigger fires, it copies events from the views described in the previous section. The details and behavior of the trigger are described below.

The following table lists the SQL files that define the trigger for DB2, Oracle, and Sybase:

*Table 10. Trigger SQL Files*

| Database | SQL File Name |
|---|---|
| DB2 | `tds_rm_upd_trigger.DB2.sql` |
| Oracle | `tds_rm_upd_trigger.ora.sql` |
| Sybase | `tds_rm_upd_trigger.syb.sql` |

## DB2 Trigger

The DB2 implementation uses a single trigger (rm_update_trigger) that fires when the rm_Archived slot is changed from 0 to 1. The trigger then copies events from the Risk Manager event view (rm_v_evt) to the archive table.

## Oracle Trigger

Because Oracle triggers do not allow reading from a table that is being updated, the Oracle implementation must copy event keys to a temporary table first, and then copy the event records to the archive table when a second trigger fires.

The two Oracle triggers are described in the following table:

*Table 11. Oracle Triggers*

| Trigger | Description |
|---|---|
| rm_update_trigger | When the rm_Archived slot changes from 0 to 1, the trigger copies the primary key (server_hndl, date_reception, event_hndl) for each changed event into a temporary event key table (rm_t_evt_key). |
| rm_del_key_trigger | When records are deleted from the temporary event key table, the corresponding records from the Risk Manager event view (rm_v_evt) are copied to the archive table. |

## Sybase Trigger

The Sybase implementation requires two nested triggers because all of the desired Risk Manager event attributes cannot be defined in a single view, like DB2 and Oracle.

The two Sybase triggers are described in the following table:

*Table 12. Sybase Triggers*

| Trigger | Description |
|---|---|
| rm_update_trigger | When the rm_Archived slot changes from 0 to 1, the trigger copies all of the columns from the Risk Manager event view (rm_v_evt) to the archive table for each changed event. For events subclassed from RM_IDSEvent, this trigger is sufficient to copy all desired attributes to the archive. |
| rm_upd_misc_trigger | When the previous trigger inserts a new event subclassed from RM_MiscEvent into the archive table, this trigger fires and updates the archive table record with the missing miscellaneous event slots (category, principal, object_type, object, action, and result). |

# B

# Cube Details

The following sections describe the Administrator cubes and the queries used to build the multidimensional cubes that are used by the guide. This cube information is defined in the TDS Administrator product.

## Risk Manager Archived Events

The **Risk Manager Archived Events** administrator cube contains data related to all Risk Manager events in the Risk Manager archive table (rm_t_arc) of the Tivoli Enterprise Console database. The size of the cube depends on the number of events in the database. For a database of 500 events, the cube consumes 320 KB; for a database of 2500 events, the cube consumes 610 KB.

The primary measure for the cube is number of events. Many dimensions are defined: by time, by IP address, by host name, by event class, by event category, and so forth.

The cube is standalone and built solely from six queries, each of which produces a .csv file. Approximately 500 bytes of disk space per event are required to store the .csv files.

Drill through is not activated.

### Queries Used to Build the Cube

The following SQL queries are used to create the flat files in comma-separated values (.csv) format. One or more .csv files are used by the Cognos Transformer product to create a multidimensional cube.

#### Risk Manager Tivoli Enterprise Console Archive

This is the largest query for the **Risk Manager Archived Events** cube. It selects a row for every Risk Manager event in the archive table. The .csv file it produces takes up over 90% of all the space required for all query result files. Most of the measures and dimensions for the cube come from this query.

```
select
T1.class,
T1.sub_source,
T1.sub_origin as sensor_type,
T1.hostname as sensor_hostname,
T1.origin as sensor_ipaddr,
                    T1.src_hostname,
                    T1.src_ipaddr,
                    T1.dst_hostname,
                    T1.dst_ipaddr,
             T1.severity as severity_value,
       T2.description as severity,
T1.class_cat,
                     T1.category,
                     T1.object_type,
```

```
                    T1.object,
                    T1.action,
                    T1.result,
                    T1.signature,
                    T1.time_event,
                    1 as num_records,
                    1 + T1.repeat_count as num_events
 from ?[DB Qualifier].rm_t_arc T1,
       ?[DB Qualifier].tec_t_severity T2
where  T1.severity = T2.code
and
    T1.date_event
    Between ?[Date Range].[Start Date] AND
                   ?[Date Range].[End Date]
```

**.CSV File Name:** rm_tec_arc.csv

### Calculated Columns

| Field Name | Datatype |
|---|---|
| ALTERNATE_CLASS | String |
| ALTERNATE_SEVERITY | String |
| CC_ACCESS_DENIED | Long |
| CC_CFG_CHANGES | Long |
| CC_FIRST_CAT_CLASS | String |
| CC_FW_CFG_CHANGES | Long |
| CC_FW_CONN_DENIED | Long |
| CC_FW_EVENTS | Long |
| CC_IDS_ATTACKS | Long |
| CC_VIRUSES_FOUND | Long |
| CC_WEB_ATTACKS | Long |
| DATE_OPENED | String |
| DAY_AND_TIME | String |
| DAY_OR_NIGHT | String |
| DST_A_SUBNET | String |
| DST_B_SUBNET | String |
| DST_C_SUBNET | String |
| DST_HOSTNAME_ORIGIN | String |
| DST_HOSTTAG | String |
| DST_IP_NUM | Long |
| HOUR_OPENED | Integer |
| SENSOR_A_SUBNET | String |
| SENSOR_B_SUBNET | String |
| SENSOR_C_SUBNET | String |
| SENSOR_HOSTNAME_ORIGIN | String |
| SENSOR_HOSTTAG | String |
| SENSOR_IP_NUM | Long |
| SRC_A_SUBNET | String |
| SRC_B_SUBNET | String |

| Field Name | Datatype |
|---|---|
| SRC_C_SUBNET | String |
| SRC_HOSTNAME_ORIGIN | String |
| SRC_HOSTTAG | String |
| SRC_IP_NUM | Long |
| TIME_OF_DAY | String |
| WEEKDAY | Integer |
| WEEKDAY_NAME | String |
| WEEKDAY_OR_WEEKEND | String |

## Risk Manager Tivoli Enterprise Console Class Hierarchy

This the second largest query in the **Risk Manager Archived Events** cube. Unlike the other queries, it reads from the tec_t_isa table in the Tivoli Enterprise Console database. This query is a structural query whose purpose is to build a 3-level hierarchy of event classes used in the **By Event Class** dimension. Each selected row produces a grandparent-parent-child tuple for every event class in the Tivoli Enterprise Console database.

```
SELECT min(T2.parent) as grandparent_class,
              min(T1.parent) as parent,
              T1.child as class
from {oj ?[DB Qualifier].tec_t_isa T1 LEFT OUTER JOIN
           ?[DB Qualifier].tec_t_isa T2 ON T1.parent = T2.child}
where T1.child !='EVENT' and T2.child !='EVENT'
group by T1.child
```

**.CSV File Name:** rm_tec_classes.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| PARENT_CLASS | String |

## Risk Manager Tivoli Enterprise Console Date Info

This query selects a row for every unique date among all Risk Manager events in the archive table. Its purpose is to supply the count for the **Number of Days** measure, as well as data for the **By Date** and **By Day of Week** dimensions.

```
SELECT DISTINCT
     {fn year(time_event)} as year_event,
     {fn month(time_event)} as month_event,
     {fn dayofmonth(time_event)} as day_event,
     1 as num_days
FROM ?[DB Qualifier].rm_t_arc
WHERE
date_event
between  ?[Date Range].[Start Date] and ?[Date Range].[End Date]
```

**.CSV File Name:** rm_tec_dates.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| DATE_OPENED | String |

## Risk Manager Tivoli Enterprise Console Sensor Info

This query selects a row for every unique sensor host from all Risk Manager events in the archive table. Its purpose is to supply the count for the **Number of Sensors** measure and the values for the **By Sensor** and **By Sensor Network** dimensions.

```
select distinct
    1 as num_sensors,
    sub_origin as sensor_type,
    hostname as sensor_hostname,
    origin as sensor_ipaddr
from ?[DB Qualifier].rm_t_arc
WHERE
    date_event
    Between ?[Date Range].[Start Date] AND
            ?[Date Range].[End Date]
```

**.CSV File Name:** rm_tec_sensors.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| SENSOR_HOSTTAG | String |
| SENSOR_HOSTNAME_ORIGIN | String |

## Risk Manager Tivoli Enterprise Console Source Info

This query selects a row for every unique source host from all Risk Manager events in the archive table. Its purpose is to supply the count for the **Number of Sources** measure and the values for the **By Source of Attack** and **By Source Network** dimensions.

```
select distinct
    1 as num_sources,
    src_hostname,
    src_ipaddr
from ?[DB Qualifier].rm_t_arc
WHERE
    date_event
    Between ?[Date Range].[Start Date] AND
                ?[Date Range].[End Date]
```

**.CSV File Name:** rm_tec_src.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| SRC_HOSTTAG | String |
| SRC_HOSTNAME_ORIGIN | String |

## Risk Manager Tivoli Enterprise Console Target Info

This query selects a row for every unique target host from all Risk Manager events in the archive table. Its purpose is to supply the count for the **Number of Destinations** measure and the values for the **By Target of Attack** and **By Target Network** dimensions.

```
select distinct
    1 as num_destinations,
    dst_hostname,
    dst_ipaddr
from ?[DB Qualifier].rm_t_arc
WHERE
    date_event
    Between ?[Date Range].[Start Date] AND
                ?[Date Range].[End Date]
```

**.CSV File Name:** rm_tec_dst.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| DST_HOSTTAG | String |
| DST_HOSTNAME_ORIGIN | String |

## Parameters Used to Build Cube

| Parameter Name | Type | Default Values |
|---|---|---|
| Date Range | Range | Last Month plus Month-to-Date |
| Alternate Severity | Terminology | Serious, Minor, Informational |
| Day or Night | Categorization | Overnight (0 – 7), Day (7 – 17), Evening (17 – 24) |

## Dimensions

**Model Created[1]:** rm_tec_arc.mdl

**Multidimensional Cube File Created:** rm_tec_arc.mdc

[1] Always save the model as an .mdl file.

The following dimensions are defined for the **Risk Manager Archived Events** cube:

### By Date

| By Date | |
|---|---|
| Month | *Week* |
| Day | |

This is a standard Transformer date dimension, customized for the **Risk Manager Archived Events** cube. All of the categories are derived from the DATE_OPENED source column. Month is in the format YYYY/MMM, as in 2000/Oct. Week and day are in the format YYYY/MM/DD, as in 2000/09/28.

### By Day of Week

| By Day of Week | |
|---|---|
| | *Weekday_or_Weekend* |

| WEEKDAY_NAME |
|---|
| DATE_OPENED |

Weekday_or_Weekend is either ″Weekday″ or ″Weekend″ and is calculated from the WEEKDAY column. WEEKDAY_NAME is Monday, Tuesday, Wednesday, and so forth, It is also calculated from the WEEKDAY column. WEEKDAY_NAME values are sorted in the order from Monday through Sunday, according to the WEEKDAY_SORT calculated column in the Transformer model.

## By Time of Day

| **By Time of Day** | |
|---|---|
| | *Day_or_Night* |
| TIME_OF_DAY | |

TIME_OF_DAY is the hour of the day, such as 8 AM, 9 AM, 1 PM, and so forth. DAY_OR_NIGHT is ″Daytime″ or ″Night″. Both source columns are calculated from the HOUR_OPENED column. Values for this level are sorted in order according to the HOUR_OPENED column.

## By Day and Time

| **By Day and Time** |
|---|
| DAY_AND_TIME |

DAY_AND_TIME is the day of week plus hour of day, such as Monday 8 AM, Friday 9 PM, and so forth. Values in this level are sorted in order from Monday 12 AM to Sunday 12 PM, according to the DAY_TIME_SORT calculated column in the Transformer model.

## By Severity

| **By Severity** | |
|---|---|
| | *ALTERNATE_SEVERITY* |
| SEVERITY | |

SEVERITY comes from the Tivoli Enterprise Console database severity value assigned to each event, such as WARNING, HARMLESS, MINOR, CRITICAL and FATAL. ALTERNATE_SEVERITY is calculated from cube parameter **Alternate Severity**, using the Severity value as input. Values in both levels are sorted in order from least to most severe according to the SEVERITY_VALUE source column.

## By Sensor

| **By Sensor** | |
|---|---|
| SENSOR_TYPE | |
| SENSOR_HOSTTAG | |
| SENSOR_HOSTNAME_ORIGIN | |

SENSOR_TYPE comes from the **SUB_ORIGIN** attribute of the core Tivoli Enterprise Console event record for all Risk Manager events. Its value refers to a particular implementation of an intrusion detection system (IDS), such as: netranger, fw_pix, webids, and so forth. SENSOR_HOSTTAG is the host name where the IDS resides; or, if the host name is unknown, the IDS IP address. SENSOR_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If the either host name or IP address are unknown, only the known value is used, with no alternate value in parentheses.

## By Sensor Network

| By Sensor Network | | |
|---|---|---|
| SENSOR_A_SUBNET | | |
| SENSOR_B_SUBNET | | |
| SENSOR_C_SUBNET | | |
| SENSOR_IPADDR | | |
| SENSOR_HOSTNAME_ORIGIN | | |

This dimension allows drilling down through the higher level subnetworks for IDS sensor hosts. The A, B, C subnets refer to the high-to-low level IP domains. For example, for IP address 9.37.25.122, the A subnet is 9, the B subnet is 9.37, and the C subnet is 9.37.25. SENSOR_IPADDR is the full IP address of the sensor host. SENSOR_IP_ADDR values are sorted in IP address order according to the SENSOR_IP_NUM calculated column. SENSOR_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either host name or IP address are unknown, only the known value is used, with no alternate value in parentheses.

## By Source of Attack

| By Source of Attack |
|---|
| SRC_HOSTTAG |
| SRC_HOSTNAME_ORIGIN |

SRC_HOSTTAG is the host name from which a suspected intrusion originates; or, if the host name is unknown, the source IP address. SRC_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either the host name or IP address is unknow n, only the known value is used, with no alternate value in parentheses.

## By Source Network

| By Source Network | | |
|---|---|---|
| SRC_A_SUBNET | | |
| SRC_B_SUBNET | | |
| SRC_C_SUBNET | | |
| SRC_IPADDR | | |
| SRC_HOSTNAME_ORIGIN | | |

This dimension allows drilling down through the higher level subnetworks for intrusion source hosts. The A, B, C subnets refer to the high-to-low level IP domains. For example,

for IP address 9.37.25.122, the A subnet is 9, the B subnet is 9.37, and the C subnet is 9.37.25. SRC_IPADDR is the full IP address of the source host. SRC_IP_ADDR values are sorted in IP address order according to the SRC_IP_NUM calculated column. SRC_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either the host name or IP address is unknow n, only the known value is used, with no alternate value in parentheses.

## By Target of Attack

| By Target of Attack |
|---|
| DST_HOSTTAG |
| DST_HOSTNAME_ORIGIN |

DST_HOSTTAG is the host name that is the target of a suspected intrusion; or, if the host name is unknown, the target IP address. DST_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either the host name or IP address is unknown, only the known value is used, with no alternate value in parentheses.

## By Target Network

<table>
<tr><th colspan="3">By Target Network</th></tr>
<tr><td>DST_A_SUBNET</td><td rowspan="2"></td><td rowspan="3"></td></tr>
<tr><td>DST_B_SUBNET</td></tr>
<tr><td colspan="2">DST_C_SUBNET</td></tr>
<tr><td colspan="3">DST_IPADDR</td></tr>
<tr><td colspan="3">DST_HOSTNAME_ORIGIN</td></tr>
</table>

This dimension allows drilling down through the higher level subnetworks for intrusion target hosts. The A, B, and C subnets refer to the high-to-low level IP domains. For example, for IP address 9.37.25.122, the A subnet is 9, the B subnet is 9.37, and the C subnet is 9.37.25. DST_IPADDR is the full IP address of the target host. DST_IP_ADDR values are sorted in IP address order according to the DST_IP_NUM calculated column. DST_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either the host name or IP address is unknown, only the known value is used, with no alternate value in parentheses.

## By Event Class

<table>
<tr><th colspan="2">By Event Class</th></tr>
<tr><td>GRANDPARENT_CLASS</td><td rowspan="2"></td></tr>
<tr><td>PARENT_CLASS</td></tr>
<tr><td colspan="2">CLASS</td></tr>
</table>

All Risk Manager events are derived subclasses of previously defined event classes. Every event, therefore, has a class ancestry going back eventually to the core TEC EVENT class. This dimension allows drill down into the class hierarchy. The CLASS level is always populated by an event from the archive database, while PARENT_CLASS and GRANDPARENT_CLASS represent its ancestors in the class hierarchy.

## By Type of Attack

| By Type of Attack | |
|---|---|
| ATTACK_TYPE | |
| CLASS | |
| SIGNATURE | |

Risk Manager intrusion events can be classified in several ways. This dimension allows viewing the events under three different categorizations. ATTACK_TYPE is a general category whose values come from the **Class Categories** cube parameter, using the calculated column CC_FIRST_CAT_CLASS as input. CC_FIRST_CAT_CLASS is simply the first category name from the list of categories in the Risk Manager **rm_ClassCategories** Tivoli Enterprise Console attribute. CLASS is a more specific category taken from the name of the Tivoli Enterprise Console event. SIGNATURE values come from the Risk Manager **rm_Signature** Tivoli Enterprise Console attribute and often provide more specific information about the intrusion event.

### By Type of Change

| By Type of Change |
|---|
| CATEGORY |
| OBJECT_TYPE |
| ACTION |
| CLASS |

This dimension is useful only for non-IDS events, such as configuration changes, where the **SUB_SOURCE** TEC attribute value is `'MISCEVENT'`. The dimension provides a hierarchy of classification for examining the non-IDS events. CATEGORY values include: Access, AccountAdmin, AntiVirusScan, Configuration, Policy, State, and so forth. OBJECT_TYPE values include: User, Group, System, File, and so forth. ACTION values include: Create, Modify, Delete, Allow, Deny, Stop, Start, and so forth. CLASS, taken from the name of the Tivoli Enterprise Console event, is the most specific and descriptive categorization, often encompassing information from the previous three levels.

## Measures

The measures defined for the **Risk Manager Archived Events** cube:

| Measure Name | Purpose | Calculation | Included |
|---|---|---|---|
| Number of events | Count all events | One for each event from Risk Manager Archived Events query | Yes |
| Number of attacks | Count all IDS events | One for each event where `SUB_SOURCE = 'IDSEVENT'` and `SUB_ORIGIN != 'RMVirus'` | Yes |
| Number of violations | Count all access violations | One for each event where `SUB_SOURCE = 'MISCEVENT'` , `rm_Category = 'Access'`, and `rm_Action = 'DENY'`. | Yes |
| Number of detected viruses | Count all virus detection events | One for each event where `CLASS = 'RMV_VirusFound'` | Yes |
| Number of configuration changes | Count all configuration changes | One for each event where `SUB_SOURCE = 'MISCEVENT'` and `rm_Category` in `("AccountAdmin", "Configuration", "Policy", "State", "Installation")`. | Yes |
| Number of Web attacks | Count all suspected Web-based intrusions | One for each event where `SUB_SOURCE = 'IDSEVENT'` and `rm_ClassCategories ='WEB'` | Yes |
| Number of firewall events | Count all intrusion events originating from firewalls | One for each event where `SUB_SOURCE = 'IDSEVENT'` and `SUB_ORIGIN = 'fw_*'` | Yes |
| Number of firewall changes | Count all system changes (configuration, accounts, and so forth.) detected by firewalls | One for each event where `SUB_SOURCE = 'MISCEVENT'`, `SUB_ORIGIN = 'fw_*'` and `rm_Category` in `("AccountAdmin", "Configuration", "Policy", "State", "Installation")`. | Yes |
| Number of connections denied | Count all connection attempts refused by firewalls | One for each event where `SUB_SOURCE = 'IDSEVENT'`, `SUB_ORIGIN = 'fw_*'` and `rm_Signature = 'fw_conn_deny'` | Yes |

| Measure Name | Purpose | Calculation | Included |
|---|---|---|---|
| Number of sensors | Count all unique hosts reporting Risk Manager events | One for each unique hostname + origin. | No |
| Number of sources | Count all unique hosts reported as the source of intrusion events | One for each unique **rm_SourceHostname** + **rm_SourceIPAddr** | Yes |
| Number of destinations | Count all unique hosts reported as the target of intrusion events | One for each unique **rm_DestinationHostname** + **rm_DestinationIPAddr**. | No |
| Number of days | Count all days in which a Risk Manager event was reported | One for each unique **Date_Event** from Risk Manager archived event table | No |
| Events per system | Average number of events reported by each IDS host | Number of events / Number of sensors | Yes |
| Events per day | Average number of events reported for each day by all IDS hosts | Number of events / Number of days | Yes |
| Events per system per day | Average number of events reported for each day by each IDS host | Number of events / Number of sensors / Number of days | Yes |
| Attacks per system | Average number of intrusion events reported against each target host | Number of attacks / Number of destinations | Yes |
| Attacks per day | Average number of intrusion events reported for each day by all IDS hosts | Number of attacks / Number of days | Yes |
| Attacks per system per day | Average number of intrusion events reported for each day against each target host | Number of attacks / Number of destinations / Number of days | Yes |
| Violations per system | Average number of access violations reported by each IDS host | Number of violations / Number of sensors | Yes |
| Viruses per system | Average number of detected viruses reported by each IDS host | Number of detected viruses / Number of sensors | Yes |
| Viruses per system per day | Average number of detected viruses reported for each day by each IDS host | Number of detected viruses / Number of sensors / Number of days | Yes |
| Firewall changes per system | Average number of system changes (configuration, accounts, and so forth.) reported by each firewall | Number of firewall changes / Number of sensors | Yes |

| Measure Name | Purpose | Calculation | Included |
|---|---|---|---|
| Web attacks per system | Average number of Web-based intrusion events reported against each target host | Number of Web attacks / Number of destinations | Yes |
| Web attacks per system per day | Average number of Web-based intrusion events reported for each day against each target host | Number of Web attacks / Number of destinations / Number of days | Yes |
| Configuration changes per system | Average number of configuration changes reported by each IDS host | Number of configuration changes / Number of sensors | Yes |

# Risk Manager Anti-Virus Status

The **Risk Manager Anti-Virus Status** administrator cube contains data related to Risk Manager Anti-Virus status events in the Risk Manager archive table (rm_t_arc) of the Tivoli Enterprise Console database. The events of interest are limited to the following Tivoli Enterprise Console event classes: **RMV_AgentNotInstalled**, **RMV_AgentInstalled**, **RMV_AgentStopped**, **RMV_AgentStarted**, **RMV_VirusDBOutOfDate**, **RMV_VirusDBUpdated**, **RMV_VirusDBUpdateComplete** and **RMV_ScanComplete**.

The only measure for the cube is number of workstations reporting anti-virus events. Dimensions include: **by time**, **by IP address**, **by host name**, **by install state**, **by run state**, **by DB state**, and **by scan state**. The purpose of the cube is provide a summary of the status of the anti-virus software running on all reporting workstations. The primary status categories are:

- Install State—Installed or Not Installed
- Running State—Running or Not Running
- Virus Signature DB State—Up to Date or Out of Date
- Scanned State—Workstation Recently Scanned for viruses or Not Recently Scanned

The cube is standalone and built solely from four queries, each of which produces a .csv file. The size of the cube is 128 KB. Approximately 500 bytes of disk space for each reporting workstation are required to store the .csv files.

Drill through is not activated.

## Queries Used to Build the Cube

The following SQL queries are used to create the flat files in comma-separated values (.csv) format. One or more .csv files are used by the Cognos Transformer product to create a multidimensional cube.

### RM Anti-Virus Workstations

This query selects a single row for every host system that has reported at least one of the anti-virus status events of interest. Its primary purpose is to supply the count for the **Number of Workstations** measure.

```
select distinct
 1 as num_hosts,
 hostname as ws_hostname,
 origin as ws_ipaddr
from
  ?[DB Qualifier].rm_t_arc
where
    date_event
    Between ?[Date Range].[Start Date] AND
                ?[Date Range].[End Date]
and
 class in ('RMV_AgentNotInstalled', 'RMV_AgentInstalled', 'RMV_AgentStopped', 'RMV_AgentStarted', 'RMV_Viru
```

**.CSV File Name:** rm_av_systems.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| WS_IP_NUM | Long |
| WS_A_SUBNET | String |
| WS_B_SUBNET | String |
| WS_C_SUBNET | String |
| WS_HOSTTAG | String |
| WS_HOSTNAME_ORIGIN | String |

## Risk Manager Anti-Virus Run Status

This query selects a single row for each host system that has reported any of the following events: **RMV_AgentNotInstalled**, **RMV_AgentInstalled**, **RMV_AgentStopped**, and **RMV_AgentStarted**. It selects the event representing the latest status from each host system. Calculated columns are used to create descriptive terms for the install and run state of each system. These columns then feed the **By Installation** dimension.

```
select distinct
 timestamp32,
 date_event,
 class,
 hostname as ws_hostname,
 origin as ws_ipaddr
from
 ?[DB Qualifier].rm_t_arc t1
where
class  like 'RMV_Agent%' and timestamp32 =
(select max(timestamp32) from  ?[DB Qualifier].rm_t_arc t2
 where class  like 'RMV_Agent%' and t2.hostname = t1.hostname)
and
    date_event
    Between ?[Date Range].[Start Date] AND
                ?[Date Range].[End Date]
```

**.CSV File Name:** rm_av_runstat.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| CC_DATE_EVENT | String |
| WS_HOSTTAG | String |
| CC_INSTALL_STATE | String |

| Field Name | Datatype |
|---|---|
| CC_RUNNING_STATE | String |

## Risk Manager Anti-Virus DB Status

This query selects a single row for each host system that has reported either of the following events: **RMV_VirusDBOutOfDate**, **RMV_VirusUpdateComplete** or**RMV_VirusDBUpdated**. It selects the event representing the latest status from each host system. These events indicate whether the virus signature database on the host system has been updated or not. A calculated column is used to create a descriptive term for the state of the virus signature database of each system. This column then feeds the **By DB Status** dimension.

```
select distinct
 timestamp32,
 date_event,
 class,
 hostname as ws_hostname,
 origin as ws_ipaddr
from
 ?[DB Qualifier].rm_t_arc t1
where
 class like 'RMV_VirusDB%'  and timestamp32 =
(select max(timestamp32) from ?[DB Qualifier].rm_t_arc t2
where class like  'RMV_VirusDB%'  and t2.hostname = t1.hostname)
and
date_event
    Between ?[Date Range].[Start Date] AND
                  ?[Date Range].[End Date]
```

**.CSV File Name:** rm_av_dbstat.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| CC_DATE_EVENT | String |
| WS_HOSTTAG | String |
| CC_DB_STATE | String |

## Risk Manager Anti-Virus Scan Status

This query selects a single row for each host system that has reported the **RMV_ScanComplete** event. It selects the occurrence representing the latest report of the event from each host system. The **RMV_ScanComplete** event indicates that the host system has completed a full scan of its memory and disk to look for viruses. Calculated column CC_DAYS_SINCE_SCAN is created to determine how many days have elapsed since the virus scan. Parameter Virus Scan Interval is applied to the calculated value to determine whether that number of days constitutes a recent enough scan. The information from this query feeds the **By Scan Status** dimension.

```
select distinct
 timestamp32,
 date_event,
 class,
 hostname as ws_hostname,
 origin as ws_ipaddr
from
 ?[DB Qualifier].rm_t_arc t1
where
```

```
class =  'RMV_ScanComplete' and timestamp32 =
(select max(timestamp32) from
 ?[DB Qualifier].rm_t_arc t2
 where class = 'RMV_ScanComplete' and t2.hostname = t1.hostname)
and
    date_event
    Between ?[Date Range].[Start Date] AND
                  ?[Date Range].[End Date]
```

**.CSV File Name:** rm_av_scanstat.csv

**Calculated Columns**

| Field Name | Datatype |
|---|---|
| CC_DATE_EVENT | String |
| WS_HOSTTAG | String |
| CC_SCAN_STATUS | String |
| CC_DAYS_SINCE_SCAN | Integer |

## Parameters Used to Build Cube

| Parameter Name | Type | Default Values |
|---|---|---|
| Date range | Range | Last Month plus Month-to-Date |
| Virus Scan Interval | Categorization | Scanned (<=7 days), Not Scanned (>7 days) |

## Dimensions

**Model Created[2]:** rm_av_stat.mdl

**Multidimensional Cube File Created:** rm_av_stat.mdc

[2] Always save the model as an .mdl file.

The following dimensions are defined for the **Risk Manager Anti-Virus Status** cube:

### By Date

| By Date | |
|---|---|
| Month | *Week* |
| Day | |

This is a standard Transformer date dimension, customized for the **Risk Manager Anti-Virus Status** cube. All of the categories are derived from the CC_DATE_EVENT calculated column. Month is in the format YYYY/MMM, as in 2000/Oct. Week and Day are in the format YYYY/MM/DD, as in 2000/09/28.

### By Entire Network

| By Entire Network |
|---|

| | | |
|---|---|---|
| WS_A_SUBNET | | |
| WS_B_SUBNET | | |
| WS_C_SUBNET | | |
| WS_IPADDR | | |
| WS_HOSTNAME_ORIGIN | | |

This dimension allows drilling down through the higher level subnetworks for anti-virus workstations. The A, B, C subnets refer to the high-to-low level IP domains. For example, for IP address 9.37.25.122, the A subnet is 9, the B subnet is 9.37, and the C subnet is 9.37.25. WS_IPADDR is the full IP address of the workstation. WS_IP_ADDR values are sorted in IP address order according to the WS_IP_NUM calculated column. WS_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either the host name or IP address is unknown, only the known value is used, with no alternate value in parentheses.

## By Workstation

| **By Workstation** |
|---|
| WS_HOSTTAG |
| WS_HOSTNAME_ORIGIN |

WS_HOSTTAG is the host name that is the source of the anti-virus status report; or, if the host name is unknown, the target IP address. WS_HOSTNAME_ORIGIN is the host name plus IP address in the format: *name*(*n.n.n.n*). If either the host name or IP address is unknown, only the known value is used with no alternate value in parentheses.

## By Installation

| By Installation | | |
|---|---|---|
| CC_INSTALL_STATE | *CC_DB_STATE* | *CC_SCAN_STATUS* |
| CC_RUNNING_STATE | | |
| WS_HOSTTAG | | |

This dimension permits drilling down by any of the three status dimensions (installation, virus DB, or virus scan) supported by the cube. The primary drill down is done using the install and run state. The idea is to see a breakdown of all anti-virus systems between two categories: installed or not installed. If you drill down into the installed category, you will see the next breakdown between: running or not running. Finally, if you drill down in either of these latter two categories, you will see a breakdown by workstation name.

Alternate drill downs are shown in *italic* type.

## By DB Status

| **By DB Status** |
|---|
| CC_DB_STATE |
| WS_HOSTTAG |

This dimension permits drilling down by the virus signature DB state. The idea is to see a breakdown of all anti-virus systems between two categories: those with up-to-date virus database files and those with out-of-date files. If you drill down into either category, you will see a breakdown by workstation name.

### By Scan Status

| By Scan Status |
|---|
| CC_SCAN_STATUS |
| CC_DAYS_SINCE_SCAN |
| WS_HOSTTAG |

This dimension permits drilling down by the virus scan state. The idea is to see a breakdown of all anti-virus systems between two categories: those recently scanned for viruses and those not recently scanned. If you drill down into either category, you will see a breakdown by the number of days since the last scan. The maximum number of days allowed between scans is determined by the **Virus Scan Interval** cube parameter. Finally, you can drill down again to a breakdown by workstation name.

## Measures

The measure defined for the Tivoli Decision Support for Enterprise Risk Management:

| Measure Name | Purpose | Calculation | Included |
|---|---|---|---|
| Number of workstations | Count workstations falling into anti-virus status categories. | One for each workstation reporting at least one anti-virus status event. | Yes |

# C

# Categories, Topics, and Views

The Tivoli Decision Support Guide for Enterprise Risk Management presents five categories of topics that aid in analyzing the Enterprise Risk Management data collected from the TEC event repository. The categories are:

- Firewall Management
- Intrusion Detection
- Risk Assessment
- Tivoli Ready Management
- Virus Management

**Note:** You can modify your preferences in the *Tivoli Discovery Interface* for the five views representing the top 100 occurrences to display fewer values by right clicking on each of the reports and selecting **Properties**. Then select the **Ranking** tab and specify the number of occurrences you want displayed. Click **OK** to save your preference.

## Firewall Management

This category of the Enterprise Risk Management guide aids in the analysis of events generated by firewalls. Firewalls are concerned with preventing unauthorized access to host systems and networks. Unsuccessful attempts to breach a firewall might indicate a malicious attack.

### Configuration Changes

This topic helps you assess when someone has attempted to make a configuration change to the firewall.

| View Title | File Name | Data Source |
|---|---|---|
| Changes per System by Network Address | rm_fw_01.ppr | Archived Events Cube |

### Denied Connections

This topic helps you assess where and when denied connections are coming to the firewall..

| View Title | File Name | Data Source |
|---|---|---|
| Denied Connections by Day and Hour | rm_fw_03.ppr | Archived Events Cube |
| Denied Connections by Network Address | rm_fw_02.ppr | Archived Events Cube |

### What types of events were detected by the firewall?

This topic helps spot trends in the volume and types of events detected by the firewall as well as their sources and targets.

| View Title | File Name | Data Source |
|---|---|---|
| Events by Destination Network Address | rm_fw_06.ppr | Archived Events Cube |
| Events by Sensor Network Address | rm_fw_04.ppr | Archived Events Cube |
| Events by Source Network Address | rm_fw_05.ppr | Archived Events Cube |
| Top 100 Events by Severity | rm_fw_07.ppr | Archived Events Cube |

## Intrusion Detection

This category will help you access the attacks made against your systems that have been detected by Intrusion Detection Systems (IDS). These events by themselves might not be significant but in aggregate could indicate a security threat.

### What are my peak days and peak times for incidents?

This topic helps you detect patterns in attacks against your enterprise so adjustments can be made to reduce volume or reduce downtime.

| View Title | File Name | Data Source |
|---|---|---|
| Average Daily Event Volume | rm_ids_01.ppr | Archived Events Cube |
| Event Histogram by Day and Hour | rm_ids_02.ppr | Archived Events Cube |

### What resources are more frequently attacked?

This topic will help you detect patterns in what resources in your enterprise are most subject to attacks. This can help to identify corrective actions that might prevent future intrusions.

| View Title | File Name | Data Source |
|---|---|---|
| Attack Rate by Destination Network Address | rm_ids_03.ppr | Archived Events Cube |
| Top 100 Attacked Hosts | rm_ids_04.ppr | Archived Events Cube |
| Web Attack Rate by Destination Network Address | rm_ids_05.ppr | Archived Events Cube |

### What type of attacks were detected?

This topic will help analyze the most frequently occurring types of intrusion attacks that are being made against resources in the enterprise.

| View Title | File Name | Data Source |
|---|---|---|
| Attacks Detected by Sensor Network Address | rm_ids_06.ppr | Archived Events Cube |
| Attacks Detected by Severity | rm_ids_07.ppr | Archived Events Cube |
| Attacks Detected by Type | rm_ids_08.ppr | Archived Events Cube |
| Top 100 Attacks | rm_ids_09.ppr | Archived Events Cube |

### Who is attacking the enterprise?

This topic will help identify where attacks to your enterprise are coming from.

| View Title | File Name | Data Source |
|---|---|---|
| Location of Intruder by Severity | rm_ids_11.ppr | Archived Events Cube |
| Location of Intruder by Type of Attack | rm_ids_10.ppr | Archived Events Cube |
| Top 100 Intruders | rm_ids_12.ppr | Archived Events Cube |

## Risk Assessment

This category reports on events that are not necessarily attacks or intrusion attempts but might be considered suspicious activities. These events include denied access events and configuration changes to systems.

### Access Violations

This topic will help you identify which systems are getting access violations such as denied telnet, ftp, rlogin, rexec, and other applications that require an authentication.

| View Title | File Name | Data Source |
|---|---|---|
| Violations per System by Network Address | rm_ra_01.ppr | Archived Events Cube |

### System Changes

This topic will help identify which systems have configuration parameters changed. Most of the time, these changes are part of normal operations. However, sometimes these changes can represent an attempt to attack or disable the system.

| View Title | File Name | Data Source |
|---|---|---|
| Changes per System by Network Address | rm_ra_02.ppr | Archived Events Cube |

## Tivoli-Ready Management

This category is used to analyze the aggregate of all events generated by Risk Management-aware sensors.

### Summary of Data Received

This topic will summarize Risk Management data received from multiple sensor types in the enterprise. The data can be used to identify corrective actions that might prevent future problems.

| View Title | File Name | Data Source |
|---|---|---|
| All Closed Events—by Severity | rm_ClosedEvtsSev.rpt | Tivoli Event Console (TEC) Database |
| Archived Events—in Date Range | rm_DateRangeEvts.rpt | Tivoli Event Console (TEC) Database |
| Average Daily Event Volume | rm_tiv_01.ppr | Archived Events Cube |
| Event Histogram by Day | rm_tiv_02.ppr | Archived Events Cube |

| View Title | File Name | Data Source |
|---|---|---|
| Event Histogram by Day and Hour | rm_tiv_03.ppr | Archived Events Cube |
| Event Rate by Network Address | rm_tiv_04.ppr | Archived Events Cube |
| Event Rate by Network Address and Source | rm_tiv_05.ppr | Archived Events Cube |
| Event Volume by Source and Severity | rm_tiv_06.ppr | Archived Events Cube |

# Virus Management

This category aids in analyzing events generated by Risk Manager-compliant anti-virus products, such as Norton AntiVirus.

## Are users compliant with virus management policy?

This topic will help identify the systems in your enterprise that have up-to-date anti-virus software installed and running.

| View Title | File Name | Data Source |
|---|---|---|
| Systems not Recently Scanned | rm_av_08.ppr | Anti-Virus Status Cube |
| Systems not Running Anti-virus Software | rm_av_01.ppr | Anti-Virus Status Cube |
| Systems with Out-of-Date Virus Definitions | rm_av_07.ppr | Anti-Virus Status Cube |

## Can I be more effective at resolving virus incidents?

This topic will help you identify the rate and severity of detected viruses in your enterprise. By seeing upward or downward trends, the effectiveness of the enterprises anti-virus policy can be assessed.

| View Title | File Name | Data Source |
|---|---|---|
| Incidents by Severity | rm_av_02.ppr | Archived Events Cube |
| This Week vs. Last Week vs. Average | rm_av_03.ppr | Archived Events Cube |

## What type of viruses were detected?

This topic will help identify which viruses are infecting your enterprise.

| View Title | File Name | Data Source |
|---|---|---|
| Viruses Types by Day of Week | rm_av_05.ppr | Archived Events Cube |
| Viruses Detected by Network Address | rm_av_04.ppr | Archived Events Cube |

## Which desktops are more frequently infected?

This topic will help you identify which systems are reporting the most detected viruses.

| View Title | File Name | Data Source |
|---|---|---|
| Top 100 Infected Desktops | rm_av_06.ppr | Archived Events Cube |

## Related Views and Roles

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_fw_01 | Changes per System by Network Address | This view shows all changes detected by firewalls over the last 13 weeks, broken down by network address of the firewall and by type of change (account, configuration, policy, and so forth). | rm_ra_02 | standard |
| rm_fw_03 | Denied Connections by Day and Hour | This view shows the total number of denied connections by day and hour over the last four weeks. | rm_ra_01 | standard |
| rm_fw_02 | Denied Connections by Network Address | This view shows the total number of denied connections within the customer's subnets, broken down by the type of connection that is denied, such as telnet, ftp, login, and so forth. | rm_ra_01 | standard |
| rm_fw_06 | Events by Destination Network Address | This view shows all classes of firewall-detected intrusion events, over the last 13 weeks, broken down by the class of event and the network that was the target of the intended intrusion. | rm_ids_03<br>rm_ids_04<br>rm_ids_05 | standard |
| rm_fw_04 | Events by Sensor Network Address | This view shows all classes of firewall-detected intrusion events, broken down by the class of event and the network in which the firewall is located, over the last 13 weeks. | rm_tiv_04<br>rm_ids_06<br>rm_av_04 | standard |
| rm_fw_05 | Events by Source Network Address | This view shows all classes of firewall-detected intrusion events, broken down by the class of event and the network from which the intrusion originated, over the last 13 weeks. | rm_tiv_06<br>rm_ids_12 | standard |
| rm_fw_07 | Top 100 Events by Severity | This view shows all classes of firewall-detected events, ranked by the class of event, over the last 30 days. Each class of event is further broken down by its severity classification. | rm_ids_07<br>rm_av_02<br>rm_ids_11 | standard |

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_ids_01 | Average Daily Event Volume | This view shows the average number of intrusions per day, broken down by day of the week. | rm_tiv_01<br>rm_tiv_02<br>rm_tiv_04 | standard |
| rm_ids_02 | Event Histogram by Day and Hour | This view shows the number of intrusions that occurred on the specific day and hour for each week. | rm_fw_03<br>rm_tiv_03 | standard |
| rm_ids_03 | Attack Rate by Destination Network Address | This view shows which network addresses in your enterprise are the most frequent targets of intrusion events. | rm_fw_06 | standard |
| rm_ids_04 | Top 100 Attacked Hosts | This view shows the top 100 hosts that are the most frequent targets of intrusion events. | rm_fw_06<br>rm_av_06 | standard |
| rm_ids_05 | Web Attack Rate by Destination Network Address | Web-based attacks represent a special case of intrusion events. Web servers are an especially vulnerable link into an enterprise because they are designed to be accessed by clients outside the enterprise. Furthermore, the HTTP protocol, which is supported by Web servers, is vulnerable to special kinds of attacks not possible against other hosts. These attacks can take the form of invoking CGI scripts to gain control over a Web server.<br><br>This view shows the Web-based attack rate for subnetworks within your enterprise. | rm_fw_06 | standard |
| rm_ids_06 | Attacks Detected by Sensor Network Address | This view helps to isolate portions of the network that are generating a disproportionate number of events. | rm_tiv_04<br>rm_fw_04<br>rm_ra_01 | standard |
| rm_ids_07 | Attacks Detected by Severity | This view shows the total number of attacks against the enterprise in each of the last 13 weeks, broken down by severity. | rm_tiv_06<br>rm_av_02<br>rm_ids_11<br>rm_fw_07 | standard |

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_ids_08 | Attacks Detected by Type | This view shows the total number of attacks detected against the enterprise in each of the last 13 weeks, broken down by attack type. The type categories include: Web, e-mail, user, command, service scan, service compromise, denial of service, targeted denial of service. | rm_ids_10 | standard |
| rm_ids_09 | Top 100 Attacks | This view shows all classes of intrusion events, ranked by the number of events over the last 30 days. This view aids in determining which intrusion events might be having the greatest impact on the enterprise. | | standard |
| rm_ids_11 | Location of Intruder by Severity | This view shows the total number of attacks originating from specific hosts over the last 13 weeks, broken down by severity. Severity level names are the same as used by TEC and are ordered in increasing severity: HARMLESS, WARNING, MINOR, CRITICAL, FATAL | rm_ids_07<br>rm_fw_07<br>rm_tiv_06 | standard |
| rm_ids_10 | Location of Intruder by Type of Attack | This view shows the total number of attacks originating from specific hosts over the last 13 weeks, broken down by attack type. If the source of an attack cannot be determined, the source host name and address is 0.0.0.0. | rm_ids_08<br>rm_fw_05 | standard |
| rm_ids_12 | Top 100 Intruders | This view shows the top 100 hosts that are the most frequent sources of intrusion events. Severity level names are the same as used by TEC and are ordered in increasing severity: HARMLESS, WARNING, MINOR, CRITICAL, FATAL | rm_fw_05<br>rm_ids_04 | standard |

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_ra_01 | Violations per System by Network Address | This view shows denied access attempts within each subnetwork over the last 13 weeks, broken down by the class of denied access, such as telnet, ftp, login, and so forth. | rm_fw_03<br>rm_fw_02 | standard |
| rm_ra_02 | Changes per System by Network Address | This view shows all changes detected by all sensors over the last 13 weeks, broken down by network address of the sensor and by type of change (account, configuration, policy, and so forth). | rm_fw_01 | standard |
| rm_ClosedEvtsSev | All Closed Events—by Severity | This tabular report lists all closed events, grouped by severity level. For each event, the following attributes are displayed: **hostname**, **time of event**, **sensor type**, **event class**, **TEC message**. A filter is provided to request events with a specified severity. The report is sorted by severity, host name, and event class.<br><br>Entry of the severity parameter is case sensitive (for example, to match FATAL, you must type `FATAL`). Leaving the parameter entry field blank displays all closed events for all severities. | rm_ids_07<br>rm_av_02<br>rm_ids_09 | standard |
| rm_DateRangeEvts | Archived Events—in Date Range | This tabular report lists all archived events, within a given date range. For each event, the following attributes are displayed: **hostname**, **time of event**, **sensor type**, **event class**, **TEC message**. A filter is provided to request events within a specified date range. The report is sorted by severity, host name, and event class. | | standard |
| rm_tiv_01 | Average Daily Event Volume | This view shows the average daily number of Risk Manager events by day of week based on the previous 4 weeks. | rm_ids_01<br>rm_ids_02 | standard |

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_tiv_02 | Event Histogram by Day | This view shows event volume by day of week for the previous 4 weeks.<br><br>Use the 3-D Rotate tool to realign the graph for better viewing from other angles. Right click on the graph and select **Display Options → 3-D View Tool**. | rm_ids_01 | standard |
| rm_tiv_03 | Event Histogram by Day and Hour | This view lets you quickly detect patterns in the event arrival based on both day of the week and time of day. This could indicate a problem that is triggered by some regularly scheduled activity that you are not aware of. | rm_fw_03<br>rm_ids_02 | standard |
| rm_tiv_04 | Event Rate by Network Address | This view helps to isolate portions of the network that are having a disproportionate number of events. | rm_ids_06<br>rm_fw_04<br>rm_ra_01<br>rm_av_04 | standard |
| rm_tiv_05 | Event Rate by Network Address and Source | This view helps you see which sensor types are generating the most Risk Manager events in your network. | rm_ids_06<br>rm_fw_04<br>rm_ra_01<br>rm_av_04 | standard |
| rm_tiv_06 | Event Volume by Source and Severity | This view shows the number of events by sensor type and severity. Severity level names are the same as those used by TEC and are ordered in increasing severity: HARMLESS, WARNING, MINOR, CRITICAL, FATAL | rm_ids_07<br>rm_fw_05<br>rm_ids_11<br>rm_fw_07 | standard |

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_av_08 | Systems not Recently Scanned | This view shows what portion of host systems within a subnet have been recently scanned for viruses. Generally, systems should be scanned at least once every 7 days. If a host system has not reported a virus scan event within the last 7 days, it is considered not recently scanned. The parameter to define interval between scans can be modified using the Tivoli Discovery Administrator application.<br>**Note:** You might see individual hosts displayed at the top-level. These represent hosts that have not reported any scan status within the date range of the query. For example, these hosts can be treated as not recently scanned. | rm_tiv_04 | standard |
| rm_av_01 | Systems not Running Anti-virus Software | This view helps determine the status of systems in the enterprise with regard to anti-virus software being installed and operational. The systems are displayed in four categories: Anti-Virus Not Installed, Installed, Not Running, Running.<br>**Note:** You might see individual hosts displayed at the top-level. These represent hosts that have not reported any anti-virus software status with the date range of the query. For example, their status is unknown. | rm_tiv_04 | standard |

| File Name | View Title | View Description | Related Views | Roles Assigned |
|---|---|---|---|---|
| rm_av_07 | Systems with Out-of-Date Virus Definitions | This view shows what portion of host systems have out-of-date virus signature files. The count of systems is in one of two categories: Anti-Virus Out of Date, Up to Date.<br>**Note:** You might see individual hosts displayed at the top-level. These represent hosts that have not reported any virus signature file status within the date range of the query. For example, their status is unknown. | rm_tiv_04 | standard |
| rm_av_02 | Incidents by Severity | This view shows the number of detected viruses over the last 4 weeks, broken down by severity. | rm_ids_07 | standard |
| rm_av_03 | This Week vs. Last Week vs. Average | This view compares the daily virus count for each day of the week between the current week, last week, average over 4 weeks, and average over 13 weeks.<br>**Note:** If data for less than 4 weeks or 13 weeks is available, the averages for 4 and 13 weeks will be artificially low. | rm_tiv_01<br>rm_av_05 | standard |
| rm_av_05 | Virus Types by Day of Week | This view shows the frequency of particular viruses by day of week. | rm_tiv_02<br>rm_av_03 | standard |
| rm_av_04 | Viruses Detected by Network Address | This view shows the frequency of viruses within subnetworks of your enterprise. | rm_tiv_04 | standard |
| rm_av_06 | Top 100 Infected Desktops | This view shows the top 100 hosts with the most viruses detected, | rm_ids_04<br>rm_av_04 | standard |

# Report Definitions

| File Name | View Title | Rank | Report Type | Period | Measure | Row | Column | Other Information |
|---|---|---|---|---|---|---|---|---|
| rm_fw_01 | Changes per System by Network Address | | Explorer | Rolling 13 weeks | Firewall changes per system | | | |
| rm_fw_03 | Denied Connections by Day and Hour | | Explorer | Rolling 4 weeks | Number of connections denied | Rolling 4 weeks | By Day and hour | |
| rm_fw_02 | Denied Connections by Network Address | | Explorer | Rolling 13 weeks | Number of connections denied | By Connection type | By Subnetwork | |
| rm_fw_06 | Events by Destination Network Address | | Explorer | Rolling 13 weeks | Number of firewall events | By Event class | By Subnetwork | |
| rm_fw_04 | Events by Sensor Network Address | | Explorer | Rolling 13 weeks | Number of firewall events | By Event class | By Subnetwork | |
| rm_fw_05 | Events by Source Network Address | | Explorer | Rolling 13 weeks | Number of firewall events | By Event class | By Subnetwork | |
| rm_fw_07 | Top 100 Events by Severity | YES | Explorer | Rolling 30 days | Number of firewall events | By Severity | By Event | Rank by Severity |
| rm_ids_01 | Average Daily Event Volume | | Explorer | By Date | Attacks per day | By Day of week | By Day | |
| rm_ids_02 | Event Histogram by Day and Hour | | Explorer | Rolling 4 weeks | Number of attacks | By Day and hour | By Hour | |
| rm_ids_03 | Attack Rate by Destination Network Address | | Explorer | Rolling 4 weeks | Attacks per system per day | By day | By subnetwork | |
| rm_ids_04 | Top 100 Attacked Hosts | YES | Explorer | Rolling 30 days | Number of attacks | By Severity | By target of attack | Rank by severity |
| rm_ids_05 | Web Attack Rate by Destination Network Address | | Explorer | Rolling 4 weeks | Web attacks per system per day | By date | By target network | |

| File Name | View Title | Rank | Report Type | Period | Measure | Row | Column | Other Information |
|---|---|---|---|---|---|---|---|---|
| rm_ids_06 | Attacks Detected by Sensor Network Address | | Explorer | Rolling 4 weeks | Attacks per system per day | By date | By Sensor network | |
| rm_ids_07 | Attacks Detected by Severity | | Explorer | Rolling 13 weeks | Number of attacks | By Severity | Rolling 13 weeks | |
| rm_ids_08 | Attacks Detected by Type | | Explorer | Rolling 13 weeks | Number of attacks | By attack type | Rolling 13 weeks | |
| rm_ids_09 | Top 100 Attacks | YES | Explorer | Rolling 30 days | Number of attacks | By Severity | By Event | Rank by Severity |
| rm_ids_11 | Location of Intruder by Severity | | Explorer | Rolling 13 weeks | Number of attacks | By Severity | By Source of Attack | |
| rm_ids_10 | Location of Intruder by Type of Attack | | Explorer | Rolling 13 weeks | Number of attacks | By attack type | By Source of Attack | |
| rm_ids_12 | Top 100 Intruders | YES | Explorer | Rolling 30 days | Number of attacks | By Severity | By Source of Attack | Rank by Severity |
| rm_ra_01 | Violations per System by Network Address | | Explorer | Rolling 13 weeks | Violations per system | By Event class | By Sensor Network | |
| rm_ra_02 | Changes per System by Network Address | | Explorer | Rolling 13 weeks | Configuration changes per system | Bt state | By Subnetwork | |
| rm_ClosedEvtsSev | All Closed Events—by Severity | | Crystal Report | | | | | |
| rm_DateRangeEvts | Archived Events—in Date Range | | Crystal Report | | | | | |
| rm_tiv_01 | Average Daily Event Volume | | Explorer | Rolling 4 weeks | Events per day | By event | By day of the week | |
| rm_tiv_02 | Event Histogram by Day | | Explorer | Rolling 4 weeks | Number of Events | Rolling 4 weeks | By day of the week | |

| File Name | View Title | Rank | Report Type | Period | Measure | Row | Column | Other Information |
|---|---|---|---|---|---|---|---|---|
| rm_tiv_03 | Event Histogram by Day and Hour | | Explorer | Rolling 4 weeks | Number of Events | By event | By day and hour | |
| rm_tiv_04 | Event Rate by Network Address | | Explorer | Rolling 4 weeks | Events per system per day | By date | By Sensor Network | |
| rm_tiv_05 | Event Rate by Network Address and Source | | Explorer | Rolling 4 weeks | Events per system per day | By Event | By Sensor Network | |
| rm_tiv_06 | Event Volume by Source and Severity | YES | Explorer | Rolling 13 weeks | Number of events | By severity | By Sensor type | Rank by Severity |
| rm_av_08 | Systems not Recently Scanned | | Explorer | By Date | Number of workstations | By Scan Status | By Entire Network | |
| rm_av_01 | Systems not Running Anti-virus Software | | Explorer | By Date | Number of workstations | By Installation | By Entire Network | |
| rm_av_07 | Systems with Out-of-Date Virus Definitions | | Explorer | By Date | Number of workstations | By host | By Entire Network | |
| rm_av_02 | Incidents by Severity | | Explorer | Rolling 4 weeks | Number of detected viruses | By severity | Rolling 4 weeks | |
| rm_av_03 | This Week vs. Last Week vs. Average | | Reporter | Rolling 13 weeks | Number of detected viruses | Week to date | | |
| rm_av_05 | Virus Types by Day of Week | YES | Explorer | Rolling 4 weeks | Number of detected viruses | By Day of Week | By Signature | Rank by Day of Week |
| rm_av_04 | Viruses Detected by Network Address | | Explorer | Rolling 4 weeks | Number of detected viruses | Rolling 4 weeks | By Sensor Networks | |
| rm_av_06 | Top 100 Infected Desktops | YES | Explorer | Rolling 30 days | Number of detected viruses | By Severity | By Sensor Host | Rank by Severity |

# Index

## P



## R



## S



## T



## U



## V



## W

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GI11-0862-00