



IBM India Software Labs

Tivoli Security Information and Event Manager Configuring Policies and Alert Rules

Aslam Siddiqui

Boudhayan Chakrabarty

Configuring policies

- **A Security policy consists of group definition sets, policy rules, and attention rules defined for one or more platforms.**
- **When systems whose activity is audited are registered, IBM® Tivoli® Security Information and Event Manager applies the policy and attention rules in your security policy to load audit data from each system into a SIM Reporting Database, organizing the data using the groups you defined, and displaying the results in the Compliance Dashboard.**

Creating a policy

- **We can create a blank policy and then use the Policy Wizard to define the policy.**
- **Open the Policy Explorer.**
- **Click Create. The Create Policy window opens.**
- **In the Policy Name field, enter the name of the policy.**
- **Click Create. The Create Policy window closes. A new policy is created and displayed in the Policy Explorer.**

Deleting policies

- **Only users with the "Commit or delete policy" role can delete policies.**
- **Open the Policy Explorer.**
- **Select the policy that you want to delete.**
- **Click Delete. The Delete Policy confirmation window opens.**
- **Click Delete to confirm deletion. The policy is deleted. The Delete Policy confirmation window closes, and you are returned to the Policy Explorer.**

Duplicating policies

- **We can create a policy by copying an existing policy and using it as a template for the new policy.**
- **Only users with the "Create or edit policy" role can create or duplicate policies.**
- **Open the Policy Explorer. Select the policy that you want to duplicate. Click Duplicate. The Duplicate Policy window opens. In the Policy Name field, enter a name for the duplicated policy. The default name is Duplicate of *selected policy name*.**
- **Click Duplicate. The duplicated policy is displayed in the Policy Explorer.**

Committing policies

- A committed policy is used to run automated compliance checks. A committed policy cannot be edited or deleted.
- Only work policies can be committed. After a policy is committed, it cannot be modified or deleted.

Policy Explorer ? _ □

Select a policy to view or work with. Only unlocked Working policies can be changed.

Create Open Duplicate Show Automatic

↑↓ ↻ ✎ ✏ --- Select Action --- Go Filter

Select	Policy Name	Policy Type	Policy Locked
<input type="radio"/>	Friday, December 31, 1999 6:00:00 PM CST	Committed	
<input checked="" type="radio"/>	Security Policy	Work	

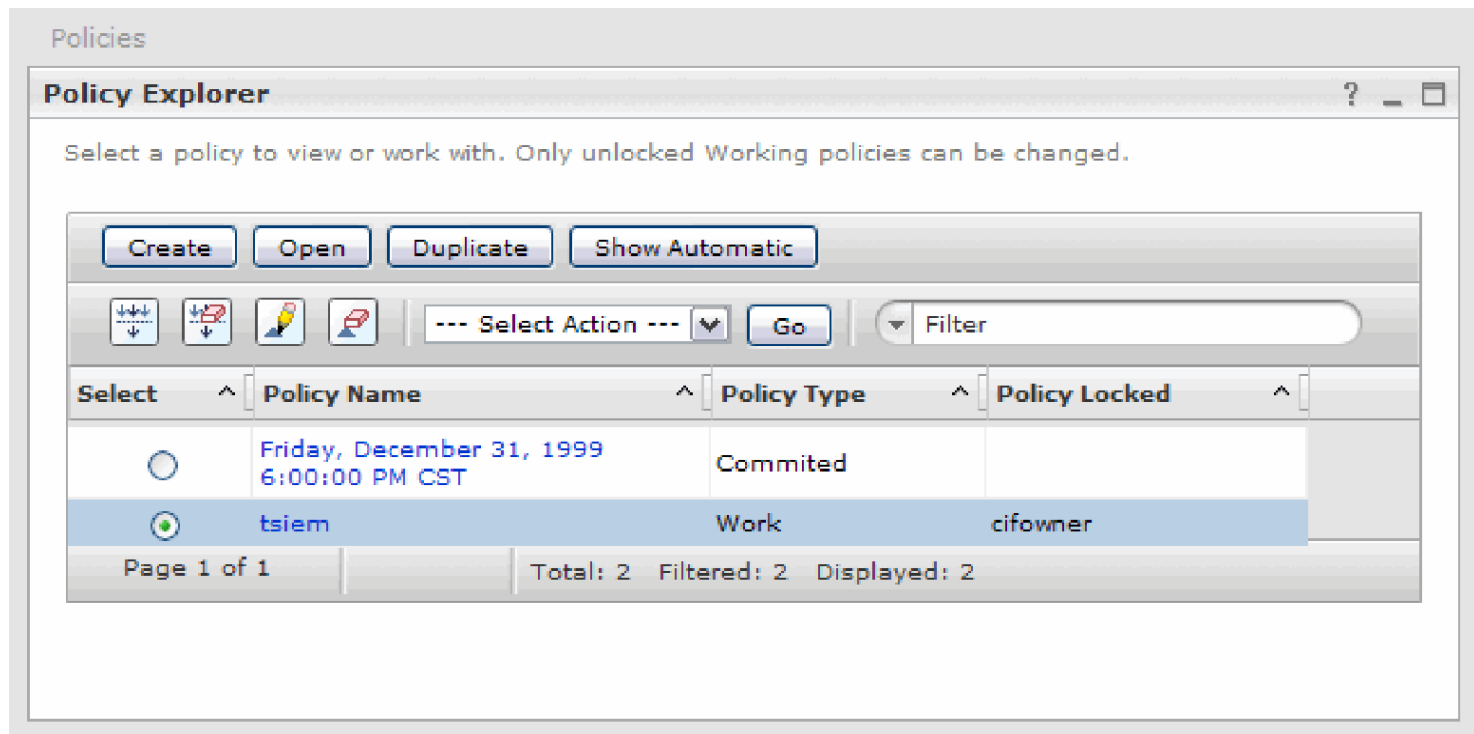
Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2

Committing policies(continued)..

- **1. Open the Policy Explorer.**
- **2. Select the policy that you want to commit.**
- **3. Open the Select Actions menu.**
- **4. Click Commit. The Commit Policy confirmation window opens.**
- **5. Click Commit. The policy is committed.**
- **6.The Commit Policy confirmation window closes, and you are returned to the Policy Explorer.**

Unlocking policies

- Policies that are being used by another user are locked. However, you can unlock locked policies.
- Only administrators and users with the "Unlock policy" role can unlock policies.



Policies

Policy Explorer

Select a policy to view or work with. Only unlocked Working policies can be changed.

Create Open Duplicate Show Automatic

--- Select Action --- Go Filter

Select	Policy Name	Policy Type	Policy Locked
<input type="radio"/>	Friday, December 31, 1999 6:00:00 PM CST	Committed	
<input checked="" type="radio"/>	tsiem	Work	cifowner

Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2

Unlocking policies(continued)..

- **All unsaved work is lost when a locked policy is unlocked.**
- **You may want to consult with the user who has locked the policy before unlocking the policy to prevent losing any unsaved work.**
 - **1. Open the Policy Explorer.**
 - **2. Select the policy that you want to unlock.**
 - **3. Open the Select Actions menu.**
 - **4. Click Unlock. The policy is unlocked.**

Generating automatic policies

- **An automatic policy displays the policy in effect for a specified date and time.**
- **Automatic policies are used to generate group definition sets so that the group definition sets can be copied into a Work policy.**
- **1. Open the Policy Explorer.**
- **2. Click Show Automatic. The Select Automatic Policy window opens.**
- **3. In the Date field, either type the date in M/D/YY format or use the calendar widget to select a date.**

Generating automatic policies(continued)..

- **4. In the Time field, either type the time in H:MM AM/PM (for 12-hour clock format locales) or in HH:MM (for 24-hour clock format locales) or use the clock widget to select a time. The time picker field varies by geographic locale. Users in locales that typically use a 12-hour clock format with AM and PM will see a field that allows you to specify AM or PM. Users in locales that typically use a 24-hour clock format will see a field that allows you to specify time using the 24-hour clock format.**
- **5. Click Show Automatic. The automatic policy is generated and is displayed in the Policy Explorer.**

Elements of a security policy

- **When you create a security policy, you must define the following elements:**
- **Platforms**
- **Group definition sets**
- **Groups**
- **Conditions**
- **Requirements**
- **Policy rules**
- **Attention rules**

Elements of a security policy (continued)..

Name	Description
Platforms	The platform defines the type of operating system or application that is audited by the policy.
Group definition sets	Every platform contains group definition sets. A group definition set is a collection of groups defined using the W7 methodology.
Groups	Every group contains conditions and requirements. An event is classified as a member of a group if it meets at least one condition. To satisfy the condition, the event must meet all requirements defined in the condition.
Conditions	An event is classified as a member of a group if it satisfies at least one condition defined in the group.
Requirements	An event meets a condition when it meets all of the requirements defined in the condition.
Policy rules	A set of rules that define all types of behavior that is permitted in your company. These rules are based on the group definitions. All events that are outside these rules are policy exceptions and can be viewed as such in Compliance Dashboard.
Attention rules	A set of rules used to identify events that might require extra scrutiny. These events might be policy exceptions or legitimate events.

Managing Platforms

- **We can use the Policy Editor to create, modify, and delete platforms that are used in a policy.**
- **The Policy Editor contains a table in which you can view and select platforms to work with.**
- **The tables below describe the user interface controls available in the Policy Editor and the policy attributes shown in the Policy Editor.**
- **Select a platform, and then select an action to perform on the selected platform from the toolbar at the top of the window or from the Select Actions menu.**

Managing Platforms(continued)..

Name of button	Description
Create	Opens the Create Platform window where you can select a platform to create in the policy. You can only create platforms in Work policies.
Open	Opens the Group Definition Sets window where you can view a content summary of the platform.
Delete	Confirms the deletion of the selected platform in the policy and returns to the Platform View window. You can only delete platforms in Work policies.

Column heading	Description
Select	Radio button that you can use to select the platform that you want to view, copy, modify, or delete. You can select only one platform.
Platform	Name of the platform.

Creating a Platform

- **After a policy is created, you must add a platform to be audited to the policy**
- **Open the Policy Editor.**
- **Click Manage Groups. The Platforms window opens.**
- **Click Create. The Create Platform window opens.**
- **Select the platform that you want to use from the menu.**
- **Click OK. The platform is added to the policy. The Create Platform window closes, and you are returned to the Policy Editor.**

Deleting a Platform

- **Deleting a platform removes the platform from the policy so that Tivoli® Security Information and Event Manager no longer maps audited data to the deleted platform**
- **Open the Policy Editor.**
- **Click Manage Groups.**
- **The Platforms window opens. Select the platform that you want to delete.**
- **Click Delete.**
- **The Delete Platform confirmation window opens. Click Yes to confirm deletion. The platform is removed from the policy.**

Managing group definition sets

- **A group definition set is a collection of folders called Who, What, When, Where, and OnWhat.**
- **Each folder holds groups that fit into one of the auditing categories.**
- **After group definition set folders have been created, groups of people, events, times, systems, and platforms should be defined for any or all folders in the group definition set.**
- **Select a group definition sets, and then select an action to perform on the selected group definition sets from the toolbar at the top of the window or from the Select Actions menu.**

Managing group definition sets(continued)..

Action	Description
Create	Opens the Create Group Definition Set window that enables you to define a group definition set to add to a platform. You can only create group definition sets in Work policies.
Open	Opens a window where you can drill down into the group definition set.
Delete	Confirms the deletion of the selected group definition set and returns to the Group Definition Sets window. You can only delete group definition sets in Work policies.
Rename	Enables you to rename a group definition set.
Copy	Enables you to copy a group definition set.
Paste	Enables you to paste a group definition set that you had copied.
Import Group Definition Set	Enables you to import the sub-elements of a group definition set. You can use an import group definition set as a template for creating other definition sets.

Creating group definition sets

- **We can create a new group definition set in the selected platform.**
- **Open the Group Definition Sets window. (Policy Editor > Platforms > Group Definition Sets)**
- **Click Create.**
- **The Create Group Definition Set window opens.**
- **In the Group Definition Set Name field, enter the name of the new group definition set.**
- **Click Create. The group definition set is created.**
- **The new group definition set is displayed in the Group Definition Sets window.**

Deleting group definition sets

- We can delete a group definition set from a work policy.
- Group definition sets cannot be deleted from committed policies.
- Deleting a group definition set deletes all groups, conditions, and requirements defined within the group definition set.
- Open the Group Definition Sets window. (Policy Editor > Platforms > Group Definition Sets) Select the group definition set that you want to delete. You can select one or more group definition sets to delete. Click Delete. The Delete Group Definition Sets confirmation window opens. Click Delete to confirm deletion

Importing a group definition set

- We can import a group definition set and use it with any work policy.
- Open the Group Definition Sets window. (Policy Editor > Platforms > Group Definition Sets)
- Open the Select Action menu.
- Click Import. The Import window opens.
- Click Browse to open a file browser.
- Select the file that you want to import.
- Click Import. The file is imported and is displayed in the Group Definition Sets window. The Import window closes, and you are returned to the Group Definition Sets window.

Managing groups

- We can view, create, edit, and delete groups using the Policy Editor.
- Select a group, and then select an action to perform on the selected group from the toolbar at the top of the window or from the Select Actions menu.

Action	Description
Create	Opens a window enabling you to create a new group.
Open	Opens a window enabling you to drill down into the group.
Delete	Confirms the deletion of the selected group.
Rename	Enables you to rename a group.
Change Significance	Opens a window where you can change the significance level associated with the group.
Copy	Enables you to copy a group.
Paste	Enables you to paste a group definition set that you had copied.

Creating a group

- **We can define a group to use in a grouping policy.**
- **Open the Groups window. (Policy Editor > Platforms > Group Definition Sets >Groups)**
- **Click Create. The Create Group window opens.**
- **In the Group Name field, enter a name for the new group.**
- **In the Dimension field, select the W7 category that the group belongs to.**
- **Click Create. A new group is created and displayed in the Groups window.**

Deleting a group

- **We can delete a group from a group definition set in a work policy.**
- **Groups cannot be deleted from committed policies. Deleting a group deletes all conditions and requirements defined within the group.**
- **Open the Groups window. (Policy Editor > Platforms > Group Definition Sets >Groups)**
- **Select the group that you want to delete. Click Delete. The Delete Group confirmation window opens.**
- **Click Delete to confirm deletion. The group, and all conditions and requirements associated with it, are deleted.**

Changing the group significance

- **We can define a significance percentage for a group to indicate the severity of events belonging to the group. Tivoli Security Information and Event Manager uses the significance percentage and the specified severity threshold to determine when to send alert messages.**
- **A higher group significance percentage assigns a higher severity level to group events. For example, if you were concerned primarily about external firewall breaches, then you might assign a high group significance percentage to network login failures.**
- **Note: By default, a new group is given the default significance of 10**

Changing the group significance (continued)..

- **Open the Groups window. (Policy Editor > Platforms > Group Definition Sets >Groups).**
- **Select the group that you want to change. Open the Select Action menu.**
- **Click Change Significance. The Change Significance window opens.**
- **In the Significance field, type the new significance percentage. The significance must be a whole integer between 10 and 99. It cannot contain any punctuation or symbols (such as a % sign). A new group is given the default significance of 10. Click Change. The changed significance is displayed in parentheses after the group name in the Groups window..**

Managing conditions for groups

- **A condition is a statement that describes a member of a group. We can create and delete conditions, and you can paste conditions into a group.**
- **For example, if a group is titled “All Employees,” the condition for group membership is a valid employee ID. If a group is created called “Finance Managers,” then the condition for group membership is an employee ID that identifies a group member as a management employee in the Finance department. When groups are created, you must specify the conditions for group membership.**

Managing conditions for groups(continued)..

- **Select a condition, and then select an action to perform on the selected condition from the toolbar at the top of the window or from the Select Actions menu.**

Action	Description
Create	Opens the Requirements window where you can define requirements for the condition. You can only create conditions and requirements in work policies.
Open	Opens a window where you can drill down into the conditions
Delete	Confirms the deletion of the selected condition in the group and returns to the Conditions window. You can only delete conditions in work policies.
Copy	Enables you to copy a condition.
Paste	Pastes a copied condition into the selected group and returns to the Conditions window. You can only copy and paste conditions in work policies.

Defining requirements

- We can define requirements for a selected condition.
- We need to create a condition before defining the requirements for the condition.

Action	Description
Create	Opens the Requirements window where you can define requirements for the condition. You can only create requirements in work policies.
Open	Opens a window where you can drill down into the requirements.
Delete	Confirms the deletion of the selected requirement. You can only delete conditions in work policies.
Copy	Enables you to copy a requirement.
Paste	Pastes a copied requirement into the selected condition. You can only copy and paste requirements in work policies.

Defining requirements (continued)..

- **Open the Conditions window. (Policy Editor > Platforms > Group Definition Sets > Groups > Conditions). Select the condition for which you want to define requirements. Click Create. The Requirements window opens. In the middle field, select the condition that you want to use. In the field on the right, enter the parameter that the field name and condition should match. Click Create. The requirement is created. If you are editing a requirement, then the Update button displays instead of the Create button. When you are finished defining requirements, click Close. The Requirements window closes, and you are returned to the Conditions window.**

Managing policy rules

- **Policy rules specify the events that are permitted and not permitted for a selected policy.**
- **In essence, the policy rules define the security policy.**
- **We can use the Policy Editor to view policy rules, create rules, delete rules, edit rules, copy rules, paste rules and import rules.**
- **Policy rules are also referred as White listed policies**

Managing policy rules

- **Policy rules specify the events that are permitted and not permitted for a selected policy.**
- **In essence, the policy rules define the security policy.**
- **We can use the Policy Editor to view policy rules, create rules, delete rules, edit rules, copy rules, paste rules and import rules.**
- **Policy rules are also referred as White listed policies.**

Creating policy rules

- We can create a new policy rule by specifying the W7 categories that will trigger the rule.
- We can only create policy rules in Work policies, because committed policies cannot be modified.
- In the Policy Rules window, click Create. The Create Rule window displays.
- Click Select Group to view a list of available groups for the appropriate W7 category. The *Select Groupname window opens showing the groups that have been defined for the given W7 category.*

Creating policy rules (continued)..

- In the **Select a Platform** field, select the platform. The table is refreshed with the group names and definition sets for the selected platform. Select the group that you want by clicking the appropriate radio button. Click **Select**. The group is added to the rule. The window closes and returns to the **Create Rule** window.
- Specify additional **W7** categories that you want (for example, *Who*, *What*, *When*, and so on). It is not necessary to specify every category. Add an optional description of the rule in the **Description** field. Click **OK**. The new rule is saved. The **Create Rule** window closes, and you are returned to the **Policy Rules** window.

Editing policy rules

- We can edit a policy rule by modifying the W7 categories that trigger the rule or by modifying the description of the rule.
- In the Policy Rules window, select the rule that you want to edit. Click Edit. The Edit Rule window displays. Click Select Group to view a list of available groups for the appropriate W7 category. The *Select Groupname window is displayed showing the groups that have been defined for the given W7 category.* In the Select a Platform field, select the platform. The table is refreshed with the group names and definition sets for the selected platform.

Editing policy rules (continued)..

- **Select the group that you want by clicking the appropriate radio button. You can only select one group at a time. Click Select. The group is added to the rule. The window is closed and you are returned to the Edit Rule window.**
- **Specify additional W7 categories that you want. It is not necessary to specify every category.**
- **Add an optional description of the rule in the Description field.**
- **Click OK. The modified rule is saved**

Deleting policy rules

- **We can delete policy rules from Work policies.**
- **Open the Policy Rules window. (Policy Editor > Policy Rules)**
- **Select the policy rules that you want to delete. You can select one or more sets of rules.**
- **Click Delete. The Delete Policy Rule(s) confirmation window opens.**
- **Click Delete to confirm deletion. The rules are deleted. The Delete Policy Rule(s) confirmation window closes, and you are returned to the Policy Rules window.**

Importing policy rules

- **We can import policy rules and use them with any Work policy.**
- **The Policy Wizard creates and saves policy rules as a .pcy file. You can import these files to use with Work policies.**
- **Open the Policy Rules window. (Policy Editor > Policy Rules). Open the Select Action menu. Click Import rules. The Import window opens.**
- **Click Browse to open a file browser. Select the file that you want to import. Click Import. The file is imported and is displayed in the Policy Rules window**

Managing attention rules

- **Attention rules determine which events trigger an alert.**
- **The trigger criteria is based on a rule or combination of rules.**
- **We can use the Policy Editor to view attention rules, create rules, delete rules, edit rules, copy rules, paste rules, and import rules.**
- **Attention rules are also referred to as Black listed policies or Alert rules.**

Creating attention rules

- We can create a new attention rule by specifying the W7 categories that will trigger the rule. We can create attention rules for a Work policy.
- In the Attention Rules window, click Create. The Create Rule window displays. Click Select Group to view a list of available groups for the appropriate W7 category. The *Select Groupname window opens showing the groups that have been defined for the given W7 category*. In the Select a Platform field, select the platform. The table is refreshed with the group names and definition sets for the selected platform.

Creating attention rules (continued)..

- **Select the group that you want by clicking the appropriate radio button. Click Select. The group is added to the rule. The window closes and returns to the Create Rule window. Specify additional W7 categories that you want. Specify the severity level in the Severity field. Attention rules contain a severity metric, which triggers the rule if an event or combination of events goes above a specified threshold. The severity level can be between 1 and 99. A higher number indicates a greater severity (that is, a more severe incident). Specify a rule ID in the Rule ID field. The Rule ID is the name of the rule. Click OK. The new rule is saved.**

Editing attention rules

- We can edit an attention rule by modifying the W7 categories that trigger the rule or by modifying the description of the rule.
- In the Attention Rules window, select the rule that you want to edit. Click Edit. The Edit Rule window displays. Click Select Group to view a list of available groups for the appropriate W7category. The *Select Groupname window is displayed showing the groups that* have been defined for the given W7 category. In the Select a Platform field, select the platform. The table is refreshed with the group names and definition sets for the selected platform.

Editing attention rules (continued)..

- **Select the group that you want by clicking the appropriate radio button. You can only select one group at a time. Click Select. The group is added to the rule. The window is closed and you are returned to the Edit Rule window.**
- **Specify additional W7 categories that you want. It is not necessary to specify every category. Add an optional description of the rule in the Description field.**
- **Click OK. The modified rule is saved.**

Deleting attention rules

- **We can delete attention rules from Work policies.**
- **Open the Attention Rules window. (Policy Editor > Attention Rules)**
- **Select the attention rules that you want to delete. You can select one or more sets of rules.**
- **Click Delete. The Delete Attention Rule(s) confirmation window opens.**
- **Click Delete to confirm deletion. The rules are deleted. The Delete Attention Rule(s) confirmation window closes, and you are returned to the Attention Rules window.**

Importing attention rules

- **We can import attention rules and use them with any Work policy.**
- **The Policy Wizard creates and saves attention rules as a .PCY file. We can import these files to use with Work policies.**
- **Open the Attention Rules window. (Policy Editor > Attention Rules).Open the Select Action menu. Click Import rules. The Import window opens. Click Browse to open a file browser. Select the file that you want to import. Click Import. The file is imported and is displayed in the Attention Rules window.**

Testing policies

- **Before you commit a Work policy, it can be helpful to test it and see how it analyzes the audit data.**
- **When you test a policy, you load audit data and map the W7 data against the policy definitions. Only Work policies can be tested. The testing functionality is not available for Committed policies.**
- **Open the Policy Editor. Click Test Policy. The Load Database Wizard opens. Manually map and load audit data into a Reporting Database and run the dataset against a Work policy**

Managing alerts

- **All defined alerts are displayed in the Alerts page. You can create, edit, and delete alerts, and you can also configure the protocol settings used to send the alerts.**
- **The purpose of an alert is to raise attention for events that require a follow-up, that is, special attention events or events that are above a defined severity level, such as security policy exceptions. Alerts notify specified recipients, such as a system administrator, when a serious or potentially harmful security event has occurred. The relevance (severity) of an event is defined in the security policy.**

Managing alerts (continued)..

- **The following attributes for each alert are displayed in the table on the Alerts page.**

Field	Description
Protocol	<p>The protocol used to send the alert. The default protocol is email.</p> <p>Protocols include:</p> <ul style="list-style-type: none">• SNMP• email• Script
Recipient	<p>The email address of the person to whom the alert is sent.</p> <p>You can specify multiple recipients by separating the email addresses with either a semicolon (;) or a space ().</p> <p>This field is not valid for SNMP alerts.</p>
Severity	<p>The severity threshold that triggers the alert. If an event exceeds the threshold, then Tivoli® Security Information and Event Manager sends an alert.</p> <p>Severity metrics can range from 0–99, where a higher number indicates a greater severity.</p>
Rule Identifiers	<p>A comma-separated list of rules (shown by their rule identifiers) that trigger the alert. If an event matches the specified rules, then Tivoli Security Information and Event Manager sends an alert.</p>

Creating alerts

- **Define criteria that are used to trigger an alert, and specify who receives the alert.**
- **Open the Alerts page. Click Create. The Create Alert window opens. In the Protocol menu, select the protocol that you want to use. The default protocol is email. In the Severity field, type a number representing the severity threshold that triggers the alert. This is a required field. In the Rule Identifiers field, type the rules that trigger the alert. Click OK. The alert is created, and you are returned to the Alerts window.**

Deleting alerts

- **We must have the "Manage databases, alerts, and archiving" role in order to delete alerts.**
- **Open the Alerts page.**
- **Select the alert or alerts that you want to delete.**
- **Click Delete. All selected alerts are deleted.**
- **Alternatively, you can click Delete in the Select Action menu, and then click Go.**

Editing an alert

- **We can modify an alert.**
- **We must have the "Manage databases, alerts, and archiving" role in order to delete alerts.**
- **Open the Alerts page. Select the alert that you want to edit. Click Edit. The Edit Alert window opens. Alternatively, you can click Edit in the Select Action menu, and then click Go. Modify the fields as needed. Click OK. The changes to the alert are saved, and you are returned to the Alerts window.**

Demo on Policies

Questions/Comments!!!!