ACL Syslog Correlation

Last Updated: March 4, 2013

The Access Control List (ACL) Syslog Correlation feature appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to access control entry (ACE) syslog entries. This tag uniquely identifies the ACE , within the ACL, that generated the syslog entry.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for ACL Syslog Correlation

Before you configure the ACL Syslog Correlation feature you should understand the concepts in the "IP Access List Overview" module.

The ACL Syslog Correlation feature appends a user-defined cookie or a router-generated hash value to ACE messages in the syslog. These values are only appended to ACE messages when the log option is enabled for the ACE.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About ACL Syslog Correlation

ACL Syslog Correlation Tags

The ACL Syslog Correlation feature appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to ACE syslog entries. This tag uniquely identifies the ACE that generated the syslog entry.

Network management software can use the tag to identify which ACE generated a specific syslog event. For example, network administrators can select an ACE rule in the network management application and can then view the corresponding syslog events for that ACE rule.

To append a tag to the syslog message, the ACE that generates the syslog event must have the log option enabled. The system appends only one type of tag (either a user-defined cookie or a router-generated MD5 hash value) to each message.

To specify a user-defined cookie tag, the user must enter the cookie value when configuring the ACE log option. The cookie must be in alpha-numeric form, it cannot be greater than 64 characters, and it cannot start with hex-decimal notation (such as 0x).

To specify a router-generated MD5 hash value tag, the hash-generation mechanism must be enabled on the router and the user must not enter a cookie value while configuring the ACE log option.

ACE Syslog Messages

When a packet is matched against an ACE in an ACL, the system checks whether the log option is enabled for that event. If the log option is enabled and the ACL Syslog Correlation feature is configured on the router, the system attaches the tag to the syslog message. The tag is displayed at the end of the syslog message, in addition to the standard information.

The following is a sample syslog message showing a user-defined cookie tag:

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402) ->
192.168.16.2(23), 1 packet [User_permiited_ACE]
```

The following is a sample syslog message showing a hash value tag:

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402) ->
192.168.16.2(23), 1 packet [0x723E6E12]
```

How to Configure ACL Syslog Correlation

Enabling Hash Value Generation on a Router

Perform this task to configure the router to generate an MD5 hash value for each log-enabled ACE in the system that is not configured with a user-defined cookie.

When the hash value generation setting is enabled, the system checks all existing ACEs and generates a hash value for each ACE that requires one. When the hash value generation setting is disabled, all previously generated hash values are removed from the system.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list logging hash-generation**
4. **end**
5. Do one of the following:
   - **show ip access-list** *access-list-number*
   - **show ip access-list** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list logging hash-generation** **Example:** `Router(config)# ip access-list logging hash-generation`	Enables hash value generation on the router. • If an ACE exists that is log enabled, and requires a hash value, the router automatically generates the value and displays the value on the console.

Step 4	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose

Step 5	Do one of the following:
	• **show ip access-list** *access-list-number*
	• **show ip access-list** *access-list-name*
	Example:
	`Router# show ip access-list 101`
	Example:
	`Router# show ip access-list acl`
		(Optional) Displays the contents of the numbered or named IP access list.
		• Review the output to confirm that the access list for a log-enabled ACE includes the generated hash value.

Examples

The following is sample output from the **show ip access-list** command when hash generation is enabled for the specified access-list.

```
Router# show ip access-list 101
Extended IP access list 101
10 permit tcp any any log (hash = 0x75F078B9)
Router# show ip access-list acl
Extended IP access list acl
10 permit tcp any any log (hash = 0x3027EB26)
```

Disabling Hash Value Generation on a Router

Perform this task to disable hash value generation on the router. When the hash value generation setting is disabled, all previously generated hash values are removed from the system.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip access-list logging hash-generation**
4. **end**
5. Do one of the following:
    - **show ip access-list** *access-list-number*
    - **show ip access-list** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip access-list logging hash-generation** **Example:** `Router(config)# no ip access-list logging hash-generation`	Disables hash value generation on the router. • The system removes any previously created hash values from the system.

Step 4	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Step 5	Do one of the following:
	• **show ip access-list** *access-list-number*
	• **show ip access-list** *access-list-name*
	Example:
	`Router# show ip access-list 101`
	Example:
	`Router# show ip access-list acl`
		(Optional) Displays the contents of the IP access list.
		• Review the output to confirm that the access list for a log-enabled ACE does not have a generated hash value.

Examples

The following is sample output from the **show ip access-list** command when hash generation is disabled and no cookie value has been specified.

```
Router# show ip access-list
101
Extended IP access list 101
10 permit tcp any any log
```

```
Router# show ip access-list
acl
Extended IP access list acl
10 permit tcp any any log
```

Configuring ACL Syslog Correlation Using a User-Defined Cookie

Perform this task to configure the ACL Syslog Correlation feature on a router for a specific access list, using a user-defined cookie as the syslog message tag.

The example in this section shows how to configure the ACL Syslog Correlation feature using a user-defined cookie for a numbered access list. However, you can configure the ACL Syslog Correlation feature using a user-defined cookie for both numbered and named access lists, and for both standard and extended access lists.

Note The following restrictions apply when choosing the user-defined cookie value:

- The maximum number of characters is 64.
- The cookie cannot start with hexadecimal notation (such as 0x).
- The cookie cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range**. For example, reflect and ref are not valid values. However, the cookie can start with the keywords. For example, reflectedACE and fragment_33 are valid values
- The cookie must contains only alphanumeric characters.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **permit** *protocol source destination* **log** *word*
4. **end**
5. **show ip access-list** *access-list-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**access-list** *access-list-number* **permit** *protocol source destination* **log** *word* **Example:** `Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log UserDefinedValue`	Defines an extended IP access list and a user-defined cookie value. • Enter the cookie value as the *word*argument.

Step 4	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Step 5	**show ip access-list** *access-list-number* **Example:** `Router# show ip access-list 101`	(Optional) Displays the contents of the IP access list. • Review the output to confirm that the access list includes the user-defined cookie value.

Examples

The following is sample output from the **show ip access-list** command for an access list with a user-defined cookie value.

```
Router# show ip access-list
101
Extended IP access list 101
30 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = UserDefinedValue)
```

Configuring ACL Syslog Correlation Using a Hash Value

Perform this task to configure the ACL Syslog Correlation feature on a router for a specific access list, using a router-generated hash value as the syslog message tag.

The steps in this section shows how to configure the ACL Syslog Correlation feature using a router-generated hash value for a numbered access list. However, you can configure the ACL Syslog Correlation feature using a router-generated hash value for both numbered and named access lists, and for both standard and extended access lists.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list logging hash-generation**
4. access-list *access-list-number* **permit** *protocol source destination* **log**
5. **end**
6. **show ip access-list** *access-list-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list logging hash-generation** **Example:** `Router(config)# ip access-list logging hash-generation`	Enables hash value generation on the router. - If an ACE exists that is log enabled, and requires a hash value, the router automatically generates the value and displays the value on the console.
Step 4	access-list *access-list-number* **permit** *protocol source destination* **log** **Example:** `Router(config)# access-list 102 permit tcp host 10.1.1.1 host 10.1.1.2 log`	Defines an extended IP access list. - Enable the log option for the access list, but do not specify a cookie value. - The router automatically generates a hash value for the newly defined access list.

Step 5	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Step 6	**show ip access-list** *access-list-number* **Example:** `Router# show ip access-list 102`	(Optional) Displays the contents of the IP access list. - Review the output to confirm that the access list includes the router-generated hash value.

Examples

The following is sample output from the **show ip access-list** command for an access list with a router-generated hash value.

```
Router# show ip access-list
102
```

```
Extended IP access list 102
10 permit tcp host 10.1.1.1 host 10.1.1.2 log (hash = 0x7F9CF6B9)
```

Changing the ACL Syslog Correlation Tag Value

Perform this task to change the value of the user-defined cookie or replace a router-generated hash value with a user-defined cookie.

The steps in this section shows how to change the ACL Syslog Correlation tag value on a numbered access list. However, you can change the ACL Syslog Correlation tag value for both numbered and named access lists, and for both standard and extended access lists.

SUMMARY STEPS

1. **enable**
2. show access-list
3. **configure terminal**
4. access-list *access-list-number* **permit** *protocol source destination* **log** *word*
5. **end**
6. **show ip access-list** *access-list-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show access-list **Example:** `Router(config)# show access-list`	(Optional) Displays the contents of the access list.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 4	access-list *access-list-number* **permit** *protocol source destination* **log** *word*
	Example:
	`Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV`
	Example:
	`OR`
	Example:
	Example:
	`Router(config)# access-list 101 permit tcp any any log replacehash`
		Modifies the cookie or changes the hash value to a cookie.
		• You must enter the entire access list configuration command, replacing the previous tag value with the new tag value.

Step 5	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Step 6	**show ip access-list** *access-list-number* **Example:** `Router# show ip access-list 101`	(Optional) Displays the contents of the IP access list. • Review the output to confirm the changes.

- Troubleshooting Tips, page 10

Troubleshooting Tips

Use the **debug ip access-list hash-generation** command to display access list debug information. The following is an example of the **debug** command output:

```
Router# debug ip access-list hash-generation
 Syslog hash code generation debugging is on
Router# show debug
IP ACL:
 Syslog hash code generation debugging is on
Router# no debug ip access-list hash-generation

 Syslog hash code generation debugging is off
```

```
Router# show debug
Router#
```

Configuration Examples for ACL Syslog Correlation

Example Configuring ACL Syslog Correlation Using a User-Defined Cookie

The following example shows how to configure the ACL Syslog Correlation feature on a router using a user-defined cookie.

```
Router#
Router# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-list 33 permit 10.10.10.6 log cook_33_std
Router(config)# do show ip access 33
Standard IP access list 33
10 permit 10.10.10.6 log (tag = cook_33_std)
Router(config)# end
Router#
```

Example Configuring ACL Syslog Correlation using a Hash Value

The following examples shows how to configure the ACL Syslog Correlation feature on a router using a router-generated hash value.

```
Router# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-list 33 permit 10.10.10.7 log
Router(config)#
*Nov 7 13:51:23.615: %IPACL-HASHGEN: Hash Input: 33 standard permit 10.10.10.7
Hash Output: 0xCE87F535
Router(config)#
do show ip access 33

Standard IP access list 33
    10 permit 10.10.10.6 log (tag = cook_33_std)
    20 permit 10.10.10.7 log (hash = 0xCE87F535)
Router(config)#
```

Example Changing the ACL Syslog Correlation Tag Value

The following example shows how to replace an existing access list user-defined cookie with a new cookie value, and how to replace a router-generated hash value with a user-defined cookie value.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# do show ip access-list 101
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = MyCookie)
    20 permit tcp any any log (hash = 0x75F078B9)
```

```
Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV
Router(config)# do show access-list
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
    20 permit tcp any any log (hash = 0x75F078B9)
Router(config)# access-list 101 permit tcp any any log replacehash
Router(config)# do show access-list
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
    20 permit tcp any any log (tag = replacehash)
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ACL commands	*Cisco IOS Security Command Reference*
Configuring and Creating ACLs	"Creating an IP Access List and Applying it to an Interface"

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ACL Syslog Correlation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for ACL Syslog Correlation

Feature Name	Releases	Feature Information
ACL Syslog Correlation	12.4(22)T 15.2(2)S	The ACL Syslog Correlation feature appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to ACE syslog entries. This tag uniquely identifies the ACE , within the ACL, that generated the syslog entry. The following commands were introduced or modified: **ip access-list logging hash-generation**, **debug ip access-list hash-generation**, **access-list (IP extended)**, **access-list (IP standard)**, **permit**, **permit (Catalyst 6500 series switches)**, **permit (IP)**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.