CHAPTER 40

Security Events

This section describes the Cisco ANA security events. Security events are related to client logins and user activities when managing Cisco ANA and the Cisco ANA environment. Table 40-1 lists Cisco ANA security events. Security events are displayed in the Security tab in Cisco ANA EventVision.

For definitions of terms and acronyms used in Table 40-1, see Table 40-2 on page 40-7. For information about Cisco ANA EventVision, see the *Cisco Active Network Abstraction 3.7.1 User Guide.*

Table 40-1 Cisco ANA Security Events

Event Name	Source OID	Short Description	Severity	Cause	Action
Category: Administrator Action					
avm-added	IAvm	AVM <ip>:<avmid> (<avmkey>) was added.	CLEARED	Administrator action.	None needed.
avm-classesjar-changed	IAvm	The class JAR list of AVM <ip>:<avmid> (<avmkey>) was changed to <classesjar>.	CLEARED	Administrator action.	None needed.
avm-disabled	IAvm	AVM <ip>:<avmid> (<avmkey>) was disabled.	CLEARED	Administrator action.	None needed.
avm-enabled	IAvm	AVM <ip>:<avmid> (<avmkey>) was enabled.	CLEARED	Administrator action.	None needed.
avm-high-availability-disabled	IAvm	High availability was disabled for AVM <ip>:<avmid> (<avmkey>).	CLEARED	Administrator action.	None needed.
avm-high-availability-enabled	IAvm	High availability was enabled for AVM <ip>:<avmid> (<avmkey>).	CLEARED	Administrator action.	None needed.
avm-key-changed	IAvm	The key of AVM <ip>:<avmid> (<avmkey>) was changed to <newkey>.	CLEARED	Administrator action.	None needed.
avm-maxmem-changed	IAvm	The maximum heap size of AVM <ip>:<avmid> (<avmkey>) was changed to <maxmem>.	CLEARED	Administrator action.	None needed.
avm-moved	IAvm	AVM <ip>:<avmid> (<avmkey>) was moved to <newip>.	CLEARED	Administrator action.	None needed.
avm-patchjar-changed	IAvm	The patch JAR list of AVM <ip>:<avmid> (<avmkey>) was changed to <patchjar>.	CLEARED	Administrator action.	None needed.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
avm-removed	IAvm	AVM <ip>:<avmid> (<avmkey>) was removed.	CLEARED	Administrator action.	None needed.
avm-restarted	IAvm	AVM <ip>:<avmid> (<avmkey>) was restarted.	CLEARED	Administrator action.	None needed.
client-license-added	IClient License Management	Client license <key> was added.	CLEARED	Administrator action.	None needed.
client-license-removed	IClient License Management	Client license <key> was removed.	CLEARED	Administrator action.	None needed.
element-added	IElement Management	Element <key> was added to AVM <unitip>:<avmid>.	CLEARED	Administrator action.	None needed.
element-alias-added	IElement Management	The alias <alias> was added to element <key> (in AVM <unitip>:<avmid>).	CLEARED	Administrator action.	None needed.
element-alias-removed	IElement Management	The alias <alias> was removed from element <key> (in AVM <unitip>:<avmid>).	CLEARED	Administrator action.	None needed.
element-disabled	IElement Management	Element <key> (in AVM <unitip>:<avmid>) was disabled.	CLEARED	Administrator action.	None needed.
element-enabled	IElement Management	Element <key> (in AVM <unitip>:<avmid>) was enabled.	CLEARED	Administrator action.	None needed.
element-moved	IElement Management	Element <key> was moved from AVM <unitip>:<avmid> to AVM <newip>:<newavmid>.	CLEARED	Administrator action.	None needed.
element-removed	IElement Management	Element <key> was removed from AVM <unitip>:<avmid>.	CLEARED	Administrator action.	None needed.
mc-network-high-availability-disabled	IMC Network	High availability was disabled for the BOS network.	CLEARED	Administrator action.	None needed.
mc-network-high-availability-enabled	IMC Network	High availability was enabled for the BOS network.	CLEARED	Administrator action.	None needed.
permission-added	IPermission	User <username> was granted permission for scope <scope> with role <role>.	CLEARED	Administrator executed grant permission to user command.	None needed.
permission-deleted	IPermission	User <username>'s permission for scope <scope> was revoked (previous role: <role>).	CLEARED	Administrator executed revoke permission to user command.	None needed.
permission-role-changed	IPermission	User <username>'s role in scope <scope> was changed to <role>.	CLEARED	Administrator executed change role to user command.	None needed.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
polling-group-added	IPolling Group Management	Polling group <name> (description: <description>) was added.	CLEARED	Administrator action.	None needed.
polling-group-description-changed	IPolling Group Management	The description of polling group <name> was changed to <description>.	CLEARED	Administrator action.	None needed.
polling-group-removed	IPolling Group Management	Polling group <name> (description: <description>) was removed.	CLEARED	Administrator action.	None needed.
polling-interval-added	IPolling Interval	Polling interval <group>/<name> (interval: <interval>) was added.	CLEARED	Administrator action.	None needed.
polling-interval-changed	IPolling Interval	Polling interval <group>/<name> was changed to <interval>.	CLEARED	Administrator action.	None needed.
polling-interval-removed	IPolling Interval	Polling interval <group>/<name> (interval: <interval>) was removed.	CLEARED	Administrator action.	None needed.
protection-group-added	IProtection Group	Protection group <key> (description: <description>) was added.	CLEARED	Administrator action.	None needed.
protection-group-description-changed	IProtection Group	The description of protection group <key> was changed to <description>.	CLEARED	Administrator action.	None needed.
protection-group-removed	IProtection Group	Protection group <key> (description: <description>) was removed.	CLEARED	Administrator action.	None needed.
redundant-unit-added	IMC	DNA Redundant Unit <ip> was added.	CLEARED	Administrator action.	None needed.
scope-created	IScope	Scope <scope> was created.	CLEARED	Administrator executed create scope command.	None needed.
scope-deleted	IScope	Scope <scope> was deleted.	CLEARED	Administrator executed delete scope command.	None needed.
scope-elements-added	IScope	The following elements were added to scope <scope>: <elements>.	CLEARED	Administrator executed add elements to scope command.	None needed.
scope-elements-removed	IScope	The following elements were removed from scope <scope>: <elements>.	CLEARED	Administrator executed remove elements from scope command.	None needed.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
static-link-added	IStatic Topology Management	A static topology link from <source> to <destination> was added.	CLEARED	Administrator action.	None needed.
static-link-removed	IStatic Topology Management	The static topology link from <source> to <destination> was removed.	CLEARED	Administrator action.	None needed.
transport-uplink-added	IMC Network	A transport uplink was added between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>).	CLEARED	Administrator action.	None needed.
transport-uplink-disabled	IMC Network	The transport uplink between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>) was disabled.	CLEARED	Administrator action.	None needed.
transport-uplink-enabled	IMC Network	The transport uplink between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>) was enabled.	CLEARED	Administrator action.	None needed.
transport-uplink-removed	IMC Network	The transport uplink between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>) was removed.	CLEARED	Administrator action.	None needed.
unit-added	IMC	DNA Unit <ip> was added.	CLEARED	Administrator action.	None needed.
unit-high-availability-disabled	IMC	High availability was disabled for BOS Unit <ip>.	CLEARED	Administrator action.	None needed.
unit-high-availability-enabled	IMC	High availability was enabled for BOS Unit <ip>.	CLEARED	Administrator action.	None needed.
unit-manual-failover	IMC	Manual failover was started in BOS Unit <ip>.	CLEARED	Administrator action.	None needed.
unit-protection-group-changed	IMC	The protection group of BOS Unit <ip> was changed to <protectiongroup>.	CLEARED	Administrator action.	None needed.
unit-removed	IMC	BOS Unit <ip> was removed.	CLEARED	Administrator action.	None needed.
unit-restart	IMC	BOS Unit <ip> was restarted.	CLEARED	Administrator action.	None needed.
unit-restarted	IMC	BOS Unit <ip> was restarted	CLEARED	Administrator action.	None needed.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
user-created	IBOSUser	User <username> was created	CLEARED	Administrator executed create user command.	None needed.
user-deleted	IBOSUser	User <username> was deleted.	CLEARED	Administrator executed delete user command.	None needed.
user-map-added	IBOSUser	User <username> was granted permission to use map <map>.	CLEARED	Administrator action.	None needed.
user-map-removed	IBOSUser	User <username>'s permission to use map <map> was revoked.	CLEARED	Administrator action.	None needed.
user-password-changed	IBOSUser	User <username>'s password was changed.	CLEARED	Administrator executed change password command.	None needed.
user-property-changed	IBOSUser	The property <property> of user <username> was changed to <value>.	CLEARED	Administrator executed change user property command.	None needed.
Category: Insufficient Permissions					
execute command	IAvm	User <username> doesn't have required permission to run command <command name> .	MAJOR	A user executed a command with insufficient permissions. Might be a security attack.	Examine the log and identify the user and the command. Take the appropriate action according to organizational security policies.
Category: License					
license_cap_exceeded	IAvm	License capacity exceeded for user = <username>, ip = <ip>.	MAJOR	User attempted to log in but is already using the maximum number of connections.	Close some of the user connections to the application.
license_expired	IAvm	License expired for user = <username>, ip = <ip>.	MAJOR	The user's license has expired.	Buy a license or log in as another user.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
no_license	IAvm	No license exists for user = <username>, ip = <ip>.	MAJOR	The user does not have a license to use the application.	Buy a license.
Category: Login					
invalid password	IAvm	Invalid password. Couldn't authenticate user <username>.	MINOR	User entered an invalid password.	Enter the password correctly.
invalid user	IAvm	Invalid login. Unknown user <username>.	MINOR	User entered invalid login name.	Enter the login name correctly.
session number exceeded	IAvm	Number of open sessions for user <username> exceeded.	MINOR	User has opened more sessions than allowed.	Increase the number of allowed sessions for this user or do not open so many.
success	IAvm	Successful login <username>.	CLEARED	User entered the correct login information.	None needed.
total number session exceeded	IAvm	Maximum open sessions number exceeded (<maxOpenSessions>).	MINOR	The users of the system have opened too many connections.	Close some of the connections to the system.
user disabled	IAvm	User <username> is disabled.	MINOR	User tried too many times to log in with an incorrect password; the account is disabled.	Enable the account.
Category: Logoff					
user logoff	IAvm	User <username> logged off.	CLEARED	User closed the application that was connected to the system.	None needed.
Category: Password Changed					
password changed	IAvm	User <username> changed password.	CLEARED	The user changed their password.	None needed.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
Category: Password Expired					
authenticate	IAvm	Password expired. Couldn't authenticate user <username>.	MINOR	User password expiration date has arrived.	Update user password.
disabled	IAvm	Account inactivity timeout expired. Account disabled. Couldn't authenticate user <username>.	MINOR	The user has not logged in within the specified time period and the account is disabled.	Enable user account.

Table 40-2 defines terms and acronyms that appear in the security events table.

Table 40-2 Security Event Terms and Acronyms

Term	Definition
avmid	AVM identifier
avmkey	AVM key
BOS	Cisco ANA
DNA	Cisco ANA
MC	Cisco ANA unit
VNE	Virtual Network Element