Nortel Secure Network Access Switch

Software Release 2.0.1.2

Nortel Health Agent

Software Release 5.2

1. Release Summary

Release Date: October 24, 2008
Purpose: Maintenance software to address internal/external issues.

2. Important Notes Before Upgrading to This Patch

Nortel Secure Network Access Solution
Product Link: http://products.nortel.com/go/product_content.jsp?segId=0&parId=0&prod_id=55260&locale=en-US

3. Platforms Supported

NSNAS 4050
NSNAS 4070

4. Version of Previous Release

NSNAS-2.0.1
NHA 5.0

5. Compatibility

6. Changes in This Release

New Features in This Release

Following new features have been added to the existing functionality in Release 2.0 software.

- Support for unmanaged switches
- Granular action on SRS failure
- Verify SRS rules till completion
- Report generation

Unmanaged Switches

With Nortel Health Agent installed on the client machine, if the client system (e.g. a laptop) is connected to network through a "SNAS Controller - controlled switch", the client system functions as expected. However, if the same client system is connected to network through a switch which is "NOT controlled by the SNAS Controller", the client system releases & renews it's IP address every FOUR seconds.

This occurs if the portal VIP of the "SNAS Controller" is reachable by the client system via a routed network topology and a "System profile" is configured on that client system.

In an ideal scenario, SNAS has to associate Switch ID/Port with Client's Mac/IP address. In SSCP-Lite environment, SNAS receives MAC address/Port mapping from the switch. Once the Nortel Health Agent logs in

from the client machine either using a system or user account, it will report MAC/IP address back to the SNAS. At this point SNAS will associate physical port with Mac/IP address of the device and determine the vlan/filters to be enforced on that port.

In this case, since the client machine is connected from a switch which is UNKNOWN to the SNAS, Agent running on the client machine will perform a login. The authentication will be successful as the system profile is predefined with correct credentials. But when it reports MAC/IP the SNAS won't be able to enforce vlan/filter on the port and will immediately logs out the session.

Because of the server logout, the agent remains in an unknown state and tries to get clean by performing a DHCP (thinking that server logout has happened and the port will be in RED vlan). It expects that the ip address changes to RED but in this case the ip address will never change. Once it cleans up, it will start the login again if the system profile is configured and this process repeats.

The solution that is available in 2.0.1.2 and NHA 5.2 is as follows:

After successful login either using System or User account, the agent tries to claim the session by establishing the connection with the server. At this point it reports Mac/Ip address and the server can accept or reject the connection.

The changes on the server end will verify if the Mac/IP addresses reported by the agent can be tied to a physical port. If the association fails, the server will reject the connection using a newly defined response code “ACCESS_STATUS_UNMANAGED".

On receiving “ACCESS_STATUS_UNMANAGED” error code, the agent stops further system connection attempts until the user moves to a new network where by the device gets a new ip address.

No configuration changes are required for this functionality.

Granular action on SRS failure

Currently in release 2.0, there is an action that can be associated with SRS using the admin tool. This action can be used to specify the script (for example the bat file on Windows) that can be executed by the agent when the SRS check passes or fails for the first time.

Each SRS definition consists of SRS Rules and Each SRS Rule is a logical expression of multiple SRS entries.

The NHA 5.2 will pass on the arguments (failed SRS and SRS Rules) which will help the customer to write scripts which can parse the arguments and decide on action.
In NHA Administrator Applet, administrator can configure action scripts for each Rule and can add following command line parameters.

Options	Details
/rule or /r	Informs the action script of the Rule Name executed by NHA. Rule name can be found either in “Rule Definitions” tab of NHA Administration Applet or in the exported XML file under “<srsRule>” element. “SRSRuleName” attribute’s value is passed to the action script.
/srsfail or /sf	Informs the action script of all the Software Definitions (SRSs) that have failed the check. If NHA is configured with “stop at first failure”, this option will report the first and only SRS that has failed compliance checking. If NHA is configured with “check all”, then all the SRSs that have failed compliance will be reported as a “,” (comma) separated list. Software definitions can be located in NHA Administration under “Predefined Software Definitions” or “Custom Software Definitions” tab. They can also be located in exported XML file under “<srs>” element. “SRSName” attribute’s value is passed to the action script.

Verify SRS Rules till completion

In the current implementation, for the endpoint compliance checking, the agent stops at the first rule failure. New configuration item has been added to finish the scan process and reports all the SRS rules that fail.

CLI and BBI provide a configuration to turn on/off full compliance check. The default value if off.

```
>> Main# /cfg/domain nsnas73local/aaa/nha/verfallsrs
Current value: off
Enable executing all SRS-rules (on/off):

>> Nortel Health Agent# help verfallsrs
Nortel Health Agent performs a health assessment on devices by sequentially
checking rules in a security policy created using the NHA
Health Editor. If verification of all SRS rules is enabled, NHA will run the
compliance scan till the completion and report all the SRS rules that are failing.
If disabled, NHA when detects a compliance rule
failure it stops processing the security policy check and reports a
"compliance failed" status to the SNAS.
```

Old Features Removed From This Release
None

Problems Resolved in this Release

Nortel Secure Network Access Switch version 2.0.1.2 and Nortel Health Agent version 5.2.0_004 resolves the following issues:

CR Id	Description
Q01938209	NAP with Dot1x not working in build NSNAS-2.0.1_081001
Q01923085	DNS query carries a predicted fashion of port number and transaction id. The fix addresses DNS Issue Exposed Vulnerability Note VU#800113.
Q01858288	SSCPLite: Switch Health Check does not work for Cisco switch
Q01935606	Cisco: There is crash_report if using snmpv3 profile which created by copy/paste
Q01936546	BBI: SNAS cannot join the 2008 domain. A new configuration has been added to NTLM authentication server to accept the NETBIOS name of the Windows Domain Server.
Q01941967	AW: BBI: Maximum login time CRM:0283000021. The default session Time-To-Live has been changed from 31days to 9999days. The new range allows the configuration of session TTL between 2m and 9999days.
Q01892751	In secupdate when I set wsus false pc goes to wrong vlan
Q01921052	Captive Portal: Some extra characters are getting appended to the homepage url
Q01920646	Auto-Blacklisting: Blacklisting is not happening
Q01920019	BBI: CLI catch up : Recheck interval should be at least 30 seconds > heartbeat
Q01918713	Trial 2.0. ER: BBI:There's no option for filtering Blacklisted users. A new information item has been added to retrieve the list of blacklisted sessions.

Q01916849	AW: Maximum login time CRM:0283000021. The default session Time-To-Live has been changed from 31days to 9999days. The new range allows the configuration of session TTL between 2m and 9999days.
Q01916844	BASF feature request for 802.1x with SSCP Lite. Addresses the co-existence of EAP and SSCP-Lite functionality on the same ethernet port.
Q01913531	Sscplite crashes when the uplink port is disabled
Q01915017	Support of secureport with SSCPlite is broken. Addresses the co-existence of EAP and SSCP-Lite functionality on the same ethernet port.
Q01903712	Not able to connect to cisco sscplite switch using ssh login type
Q01900180	Trial 2.0. ER : There's no option for filtering Blacklisted users. A new information command has been added to retrieve the list of blacklisted sessions.
Q01893454	Enhacement: Add syslog messages for nap
Q01653526	Space of Custom Content was not updated completely
Q01927804	Typo in MacDB add functionality
Q01908341	SSCPLite doesn't work when SNMPv2 and SNMPv3 traps are configured from the switch
Q01936683	NSNA Trial 2.0: BBI ER: Auto close feature for DNS cache issue not configurable
Q01545408	Need help for settings that are available in BBI /Connected clients page
Q01742283	SSCPLite: Should support importing multiple switches from a single template file
Q01749084	BBI: Unclear err message incase SSL and HTTP Redirect are not synchronous
Q01877709	SNAS traces does not give the correct information for OPSWAT
Q01918111	Could not launch the TG ADMIN TOOL
Q01928470	SNAS has been reinitiated when authenticate EAP with SSCPLite switch
Q01925762	NHA will not reconnect after client (laptop) suspended and connected back again.
Q01918708	Trial 2.0. ER: BBI:There's no option for filtering Blacklisted users. A new information item has been added to retrieve the list of blacklisted sessions.
Q01903735	sscplite-cisco: Reboot switch, most of ports move to green unexpectedly.
Q01900689	Trial NSNA 2.0-SNAS 4070 IP address release/renew in every 4 seconds. Support for unmanaged access points has been added. The NHA will be commanded to stop performing the logins if the device is not associated with the managed access point.
Q01915685	NSNA 2.0 Trial: ER :System accounts can't be automatically updated without a usr. The system credentials will be updated to the agent even if the user session is not established.
Q01926785	Enhancement - TG Icon in the Add/Remove program still displays old TG icon
Q01918886	BBI: Telus: help text grammar correction needed for "Verify All SRS-rules"
Q01920629-01	Memory Leak in Tunnel Guard agent
Q01935572	NAP_DOT1X - Vista (wlan) clnt logs out wth Java Err while chking Autorem Feature
Q01930411-01	VANOC: Tunnel Guard doesn't recognize Entrust cert
Q01938850	Action script parameter

Q01938333	NAP option should remove from the custom option of NHA installation
Q01936089	Enhancement - TG Icon in the Add/Remove program still displays old TG icon
Q01936189	MS Security Health Agent Warning about NAP after Nortel Health Agent installatio
Q01936074	NHA:- Manage profile window is getting closed
Q01943549	Not allowing unicode characters to be displayed in the admin applet.
Q01930833	BBI: Auto-Blacklisting: Blacklisting is not happening
Q01941967	AW: BBI: Maximum login time CRM:0283000021
Q01909970	early push configuration, loges out the sessions
Q01908833	BBI: Cannot Does not display dot1x client info in "session information"
Q01944518	NHA fails to uninstall with error 1722
Q01943549	Not allowing unicode characters to be displayed in the admin applet.
Q01911013	Compliance failed on Linux if "NOT" expression is used in the rule
Q01947583	NHA:After waking from hibernation mode, plugout/plugin sys session is not UP

7. Outstanding Issues

Q01920210	NHA Desktop - Vista fail to get new IP address. This problem is seen mostly on Windows Vista Ultimate

8. Known Limitations

None

9. Documentation Corrections

Syslog messages have been updated for ease of parsing by report generation tool.

SYSLOG MESSAGES

Module (aaa_ldap_isd)

1) If isd_type is isdsac
"LDAP backend(s) unreachable Domain<Xid> AuthId<Aid> "
else
"LDAP backend(s) unreachable Vpn=<Xid> AuthId<Aid> "

Severity : ERROR
Description : Shown if LDAP server(s) cannot be reached when a user tries to login to the Portal.
Event-Class: FAULT

Module (aaa_ldap_usr)

1) If isd_type is isdsac
"LDAP backend(s) unreachable Domain<Xid> AuthId<Aid> "
else
"LDAP backend(s) unreachable Vpn=<Xid> AuthId<Aid> "

Severity : ERROR
Description : Shown if LDAP server(s) cannot be reached when a user tries to login to the Portal.
Event-Class : FAULT

module(aaa_license)

1) "Host <host> has been down too long: is no longer accounted for in the license pool."
Severity : WARNING
Description : Reporting about a dead node.
Event-class : Audit

2) "Host<host> is up: accounted for in the license pool."
Severity : INFORMATIONAL
Description : Reporting about an up node.
Event-class : Audit

module (aaa_server)

1) "Syscred Passwd for group <Group> <Reason>"
Severity : INFORMATIONAL
Description : Reporting about failure of decrypting system password.
Event_Class: Security

2) "Downgrade to system reject logout to Red VLAN"
Severity : INFORMATIONAL
Description :System login rejected and moving to Red VLAN.
Event_Class: Security

3) "Error during system down grade <Reason>"
Severity : INFORMATIONAL
Description : Reporting about failure of decrypting system password.
Event_Class: fault

4) "Downgrade to system rejected. Logout to Red VLAN"
Severity : INFORMATIONAL
Description : System login rejected and moving to Red VLAN.
Event_Class: fault

5) "Syscred Passwd for group <Unknown Reason>"
Severity : INFORMATIONAL
Description : Reporting about failure of decrypting system password.

6) userID=\"<UserID>\" sourceAddress=\"<ADDR>\" domainID=\"<XID>\" switchID=\"<SWITCH>\"Login Attempt" (sac_pc:syslog)
Severity : INFORMATIONAL
Description : When a an attempt from user for login.The user-id and the source address have shown.
Event_Class: Security

7)"[x-nortel eventClass=\"security\" severity=\"info\" userID=\"<USER-ID>\" sourceAddress=\"<SOURCE-ADDRESS>\" method=\"<ACCESS_METHOD>\" domainID=\"<DOMAIN-ID>\" groups=\"<GROUP>\"] Login

Succeeded" (syslog:ssp_send)
Severity : INFORMATIONAL
Description : Login of the user to the Domain succeeded . The user-id,source address, acces method, domain-Id and groups is shown.
Event_Class: Audit

8) ["VPN LoginSucceeded Vpn=\"", <XNET_ID>,
"\" SrcIp=\"",<SOURCE_IP>,
"\" Method=\"", <ACCESS_METHOD>,
"\" User=\"", <USER>, "\" Groups=\"", <GROUPS>,
"\" TunIP=\"", <TUN_IP>, "
"\""] (syslog:ssp_send)
Severity : INFORMATIONAL
Description : Login to the VPN domain succeeded. The remote user's access method, client IP address, user name and group membership is shown.
Event-class : Audit

9) "[x-nortel eventClass=\"security\" severity=\"info\" userID=\"<USERID>\" sourceAddress=\"<SOURCE-ADDRESS>\" method=\"<ACCESS_METHOD>\" domain=\"<DOMAIN_ID>\" reason=\"<REASON>\"] Login Failed" (syslog:ssp_send)
Severity : INFORMATIONAL
Description : Login of the user to the Domain succeeded . The user-id,source address, acces method, domain-Id and groups is shown.
Event_Class: Audit

10) ["VPN LoginFailed Vpn=\"", <XNET_ID>,
"\" SrcIp=\"",<SOURCE-IP>,
"\" Method=\"", <ACCESS_METHOD>,
"\" User=\"", <USER-ID>,
"\" Error=\"", <CODE>, "\""] (syslog:ssp_send)
Severity : INFORMATIONAL
Description : Login to the VPN domain failed. The VPN-id, remote user's access method,client IP address and user-id and error code is shown.
Event Class : Security

11) ["VPN AddressAssigned Vpn=\"", <XNET_ID>,
"\" SrcIp=\"",<SIP>,
"\" Method=\"", <ACCESS_METHOD>,
"\" User=\"",<USER>,
"\" TunIp=\"", <TUN_IP>,
"\""] (ssp_send)
Severity : INFORMATIONAL
Description : Source IP address for the connection between the VPN Gateway and the destination address (innertunnel) has been allocated
Event Class : Audit

12) "[x-nortel eventClass=\"security\" severity=\"info\" userID=\"<USER-ID>\" sourceAddress=\"<SOURCE_IP>\" macAddress=\"<MAC>\"domainID=\"<DOMAIN_ID>\"] Logout" (syslog:ssp_send)
Severity : INFORMATIONAL
Description : User has logged out from the domain.
Event Class: Audit

13) ["VPN Logout Vpn=\"", <XID>,
"\" SrcIp=\"",<SOURCE_IP>,
"\" User=\"", <User>, "\""](syslog:ssp_send)
Severity : INFORMATIONAL

Description: Remote user has logged out from the VPN domain.
Event Class : Audit.

Module (inet_server)

1) "Failed to init hwcard: <ERROR>"
Severity : CRITICAL
Descripion : Failed to init ssl hardware card.
Event Class : Fault.

Module (is_core)
1) "Revoked cert serialno=<Integer> " "rejected on IP <IP_ADDR>"
Severity : INFORMATIONAL
Description : The client certificate with serial number %d was revoked and thus login failed..
Event Class: Information

Module (is_gw_sup)

1) "Starting gw at <IP_ADDRESS:PORT>"
Severity : INFORMAIONAL
Description : Starting Gateway.
Event-Class: Audit

2) "Failed to start gw at <IP_ADDRESS:PORT>"
Severity : INFORMATIONAL
Description: Failed to start the Gate way.
Event-Class : Fault

3) "Stopping gateway at <IP_ADDRESS:PORT> "
Severity : INFORMATIONAL
Description : Stopping the gateway.
Event-class : Information + Audit

Module (ip_pool)
1) "Allocated IP <IP> to <USER> at <NODE> for vpn=<XID>"
Severity : INFORMATIONAL
Description : An IP address was allocated from the IP pool.

2) "Failed to allocate IP addr from empty pool"
Severity : WARNING
Description : Failed to allocate ip-address from the empty pool.

3)"Returned IP <IP> to pool for vpn <XID>"
Severity : INFORMATIONAL
Description: Returned ip back to the ip-pool for VPN.

Module (ipsec)

1) "Ike not started due: No license"
Severity: NOTICE
Description: If no licence can be found (such as on old ASA 310), IKE is not started..

2) "ike: <cleanup_msg(...)>"
Severity:
Description:

3) "No Secure Service Partitioning license loaded: IPSEC server <server> *will not* use interface <InterfaceNo>"

Severity : Warning
Description :

4) "IPSEC server <Server> uses default interface (interface <InterfaceNo> not configured)"
Severity : Warning
Decsription : This indicates possible badly configured default gateways on some Secure Service Partitioning interface.

Module (ipsec_aaa)

1) "VPN = <XID> Failed to create ike session:<Args>"
Severity: NOTICE
Description : Failed to create ike session for the user.

2) "VPN = <XID> User tried to login with a groupname unknown to me "
Severity: NOTICE
Description : User tried to login with an invalid group name.

3) "VPN = <XID> No such user defined in local auth db"
Severity: NOTICE
Description : User who attempted login is not there in the Local database.

4) "VPN = <XID> Failed to auth session:<Args>"
Severity: NOTICE
Description: Failed to create authe session for the user.

5) "VPN = <XID> Warning: Hash clash between <NewGroupname> and <OldGroupname> in VPN <XID>, two <Group> cannot be equal for ipsec users when lower cased"
Severity: NOTICE
Description: Conflict in the the group name for the same domain.

6) "VPN = <XID> Failed to allocate IP <IP>.
Severity: NOTICE
Description: Failed to allocate Ip.

Module (logger)

1) "System started <Name> <Version name>"
Severity : INFORMATIONAL
Description : Server get started

2) <Node> halted abnormally,started again at <timestamp>
Severity: INFORMATIONAL
Description:

3) <Node details> , started again at <Timestamp>"
Severity:INFORMATIONAL
Description:

4) "<Node> started at <Timestamp>"
Severity:INFORMATIONAL
Description:

5) "<Node> halted abnormally,started again at <TimeStamp>"
Severity: INFORMATIONAL
Description:

Module (syslog).

1) "Internal Memory Logging is Enabled"
Severity: INFORMATIONAL
Description: Internal memory logging is enabled for syslog server.
EVENT-CLASS: Information

2) "Internal Memory Logging is Disabled"
Severity: INFORMATIONAL
Description: Internal memory logging is disabled for syslog server.
EVENT-CLASS: Information

3) "Buffer size of internal memory logging is changed to [<BUFFER> messages]"
Severity: INFORMATIONAL
Description:Buffer size is changed for the syslog server.
EVENT-CLASS: Information

Module (net_ctrl_server).

1) [x-nortel eventClass=\"<security>\" severity=\"<syslog_warning>\" <New Master-Master>< NewMaster>]
Severity : WARNING
Description:
EventClass: Security

Module (oam_eva_adaptation)

1) "Alarm Cleared Name=\"<ALARM.NAME>\" Id=\"<ALARM.INDEX>\" Sender=\"ALARM.SENDER\""
Severity : NOTICE
Description: Alarm with Alarm.name is Cleared.
Event-Class: Information

2)"Alarm Cleared Id=\"<EVENT.SENDER>\""
Severity : NOTICE
Description: Alarm with Alarm-id is Cleared.
Event-Class: Information

3)"Event Name=\"<EVENT-NAME>\" Sender=\"<EVENT.SENDER>\" "Extra=\"EVENT.EXTRA\""
Severity : NOTICE
Description:
Event-Class: Information

4) "Alarm Name=\"<ALARM.NAME>\" Id=\"ALARM.ID\" Sender=\"<ALARM.SENDER>\"
"Cause=\"ALARAM.CAUSE\" Extra=\"<ALARM.EXTRA>\""

Severity: Notice
Description:
Event –Class : Information

Module (dhcp_cli_srv).

1) Received DHCPDECLINE from client. Requested IP =<IP>
Severity:INFORMATIONAL
Description: Received DHCPDECLINE from Client.
Event-Class: Security

Module (dhcp_proto_srv)

1) Received DHCPDECLINE from client
Severity:INFORMATIONAL
Description: Received DHCPDECLINE from Client.

Event-Class: Information

Module (oaml_license).

1) License expired
Severity: WARNING
Description: License of the node has expired.

Module (sac_dhcp_server)

1) Allocated <IP> to <MAC> at <NODE>, domain <XID>, subnet <SID> (<SETTING>)
Severity: INFORMATIONAL
Description: Allocated IP address for a particular mac, which belongs to specific domain and subnet.
Event-Class: Information

2) Failed to allocate IP address from empty pool, domain <XID>, subnet <SID>"
Severity: WARNING
Description: Failed to allocate Ip address from empty pool.
Event-Class : Audit

3) "Returned IP <IP> to DHCP for MAC <MAC>"
Severity: Information
Description: Returned the Ip back to the pool.
Event-Class: Information.

Module (sac_server)

1) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>"
"Sscplite switch, filter_only is not supported, logging out user"
Severity: INFORMATIONAL
Descrption : When user tries to Filter_only mode with sscp_lite switch. It is not allowed.
EVENT_CLASS: Security

2) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>"
"<sscp/sscplite> client, Change to new filter"
Severity: INFORMATIONAL
Description: Change to new filter after getting aaa access login.
Event-Class: Security

3) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>"
"<AuthOnly/sscp/sscplite> client, Change to <Vlan name> VLAN"
Severity: INFORMATIONAL
Description: Change to new filter after getting aaa access login.
Event-Class: Security

4) domainID=\"<XID>\" switchID=\"<SWITCH>\" switchIP=\"<IP>\"switchName=\"<Switch-name>\" Modified
Severity: INFORMATIONAL
Description: This message is send as part of syncing the swicth state with the registry changes and restarting the modified switches.
Event-Class: Security

5) domainID=\"<XID>\" switchID=\"<SWITCH>\" switchIP=\"<IP>\"switchName=\"<Switch-name>\" Disconnected
Severity: INFORMATIONAL
Description: The swicth got disconnected and cleaniing up all the red sessions.
Event-Class: SECURITY

6) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>"
"Mac <MAC> trying to use ip <IP> which belongs to <MAC>"
Severity: INFORMATIONAL
Description: Logging out the client since Mac trying to use the ip which belong to other Mac.
Event-Class:SECURITY

7)domainID=\"<XID>\" switchID=\"<SWITCH>\" switchIP=\"<IP>\"switchName=\"<Switch-name>\" Switch <SWITCH> status changed: <STATUS>
Severity: INFORMATIONAL
Description: Notification for status of sscplite switches.
Event-Class : Security

8) MAC authentication successful, MAC : <MAC>
Severity: INFORMATIONAL
Description: This message is got as a result of successful mac database lookup.
Event_Class : Information

9) MAC authentication failed, MAC : <MAC>
Severity: INFORMATIONAL
Description: This message is got as a result of mac database lookup failure.
Event_Class : Information

10) domainID=\"<XID>\" switchIP=\"<IP>\" group=\"<Group>\" macAddress=\"<MAC>\" MAC Blacklisted
Severity: INFORMATIONAL
Description: This message is got as a result of mac database lookup and mac is blacklisted.
Event_Class : Information

11) Domain:<>XID, Switch: <SWITCH-ID> ERROR portlist timeout
Severity: ERROR
Description: Error occurred since the portList command has been time out.
Event-Class : Information

12) new NSNA portup
Severity: INFORMATIONAL
Description: NSNA port has come up.
Event_Class : Information

13) NSNA portdown
Severity: INFORMATIONAL
Description: NSNA port has come down.
Event_Class : Information

14) switch authenticated static device, MAC:<MAC>
Severity: INFORMATIONAL
Description: Authentication notification has come from the switch for a static device.
Event_Class : Information

15) domainID=\"<XID>\" switchID=\"<SWITCH>\" switchIP=\"<IP>\"switchName=\"<Switch-name>\" Added
Severity: INFORMATIONAL
Description: Switch has been added to the list of switches.
Event-Class: Security

16) domainID=\"<XID>\" switchID=\"<SWITCH>\" switchIP=\"<IP>\"switchName=\"<Switch-name>\" Deleted
Severity: INFORMATIONAL
Description: Switch has been deleted from the list of switches.
Event-Class: Security

17) domainID=\"<XID>\" switchID=\"<SWITCH>\" switchIP=\"<IP>\"switchName=\"<Switch-name>\" Connected
Severity: INFORMATIONAL
Description: current status of Switch.
Event-Class: Security

Module (sched_utils)

1) Error executing scheduled task <TASK>, Error: <ERROR>
Severity: ERROR
Description: Scheduled task not properly executed as per the schedule.
Event-Class: Fault

2) Successfully executed scheduled task <TASK>
Severity: INFORMATIONAL
Description: Task executed as per the schedule.
Event-Class: Information

3) (scheduled_selftest): Testing <CMDSTR><IFSTR>:<VALSTR>...
Severity: INFORMATIONAL
Description: Self Testing the scheduler
Event-Class: Information

4) (scheduledselftest): ok
Severity: INFORMATIONAL
Description: Self Testing worked correctly.
Event-Class: Information

5) (scheduled_selftest): <PROTOCOl>
Severity: INFORMATIONAL
Description: Staus of scheduled self-testing for a particular protocol.
Event-Class: Information

6) (scheduled_selftest): error:
Severity: ERROR
Description: Error in Scheduled_self test.
Event-Class: Fault

Module (simpleproxy)

1) failed to start auto-crl handling
Severity: ERROR
Description:

2) auoto-crl failed, no Certificates found
Severity: ERROR
Description:

3) syntax error when parsing the CRL-URL
Severity: ERROR
Description:

4) automatic retrieval of HTTP-CRL failed - lookup failure <HOST>
Severity: ERROR
Description:

5) automatic retrieval of HTTP-CRL failed - parse error
Severity: ERROR
Description:

6) auto-crl over HTTP failed, reason:<REASON
Severity: ERROR
Description:

7) automatic retrieval of HTTP-CRL failed
Severity: ERROR
Description:

8) failed to create TFTP-CRL temp file
Severity: ERROR
Description:

9) parsing of TFTP-CRL URL failed
Severity: ERROR
Description:

10) automatic retrieval of TFTP-CRL failed - lookup failure <HOST>
Severity: ERROR
Description:

11) automatic retrieval of LDAP-CRL failed - lookup failure <HOST>
Severity: ERROR
Description:

12) failed to contact LDAP server at <HOST>
Severity: ERROR
Description:

13) no CRL (1) found at LDAP server
Severity: ERROR
Description:

14) CRL authentication failed
Severity: ERROR
Description:

15) no CRL (2) found at LDAP server
Severity: ERROR
Description:

16) no CRL (3) found at LDAP server
Severity: ERROR
Description:

17) no CRL passwd found
Severity: ERROR
Description:

18) no CRL interval found for cert
Severity: ERROR
Description:

19) CRL revocation failed - <REASON>
Severity: ERROR
Description:

20) CRL revocation failed - internal error
Severity: ERROR

Description:

21) "Ambiguous CRL configuration,all usage of certificate <CERT> does not bind to the same interface and/or DNS environment - using gateway <GW> settings\n
Severity: WARNING
Description:

22) no CRL-URL specified
Severity: WARNING
Description

23) invalid escape sequence in DN, ignoring...
Severity: WARNING
Description

24) no CRL filter was found.
Severity: ERROR
Description:

Module (tg).

1) "Error with auth hash from client <REASON>
Severity: INFORMATIONAL
Description: Error with authentication hash from the client.
Event-Class: Security

2) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" domainID=\"<XID>\" IP changing to <IP>
Severity: INFORMATIONAL
Description: Ip Updation
Event-Class: Security

3) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\" domainID=\"<XID>\"Compliancy checks ok, open session
Severity: INFORMATIONAL
Description: Compliance checking succesfully completed
Event-Class: Security

4) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" domainID=\"<XID>\" NHA:<STATUS> NAP:<STATUS> Patchlink:<STATUS>. Compliancy check failed, tearing down session - <FailureReason>.
Severity: INFORMATIONAL
Description: Compliance check failed tearing down session
Event-Class: Security

5) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" domainID=\"<XID>\" NHA:<Status> NAP:< Status> Patchlink:<Status >. Compliancy check failed, restricting session - <FailureReason>
Severity: INFORMATIONAL
Description: Compliance check failed restricting the user..
Event-Class: Security

6) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" domainID=\"<XID>\" NHA:<Status> NAP:< Status> Patchlink:<Status >. Compliancy check failed, allowing session - <FailureReason>
Severity: INFORMATIONAL
Description: Compliance check failed allowing the user..
Event-Class: Security

Module (tg_ssl)

1) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>" "No heart beat from agent. Switch connection lost. Keeping the user session alive"
Severity: WARNING
Description: Heart-beat from the client timed-out and Entering Status-Quo mode.
Event-Class: Security

2)userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>" no heart beat receieved from agent <IP>, switch connected, no status-quo mode
Severity: WARNING
Description: Heart-beat from the client timed-out and and the switch is in connected state.
Event-Class: Security

3) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>" TG Agent active tgmode runonce ignored, using continous
Severity: INFORMATIONAL
Description: TG Agent active tgmode runonce ignored, using continous.
Event-Class: Security

4) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>" TG Agent active honor tgmode continous"
Severity: INFORMATIONAL
Description: TG TG Agent active honor tgmode continous.
Event-Class: Security

5) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>" TG Agent active tgmode never ignored, using continous
Severity: INFORMATIONAL
Description: TG Agent active tgmode never ignored, using co.
Event-Class: Security

6) userID=\"<UserId>\" sourceAddress=\"<ADDR>\" macAddress=\"<MAC>\"domainID=\"<XID>\" switchID=\"<SWITCH>\"switchIP=\"<IP>\"switchName=\"<Switch-NAME>\"portID=\"<PORT>\"vlanID=\"<VLAN>" "No heart beat from agent. Status_Quo mode disabled"
Severity: WARNING
Description: Heart-beat from the client timed-out and Status-Quo modei disabled.
Event-Class: Security

7)userID=\"<UserId>"\ sourceAddress=\"<SOURCE_IP>"\ macAddress=\"<MAC>"\ A device trying to gain access from an unmanaged network, logging out
Severity: INFORMATIONAL
Description: User connected to an umnaged switch is trying to authenticate and get network access
Event-Class: Security

Module (radius_server)

1) domainID="1" userID="host/VISTA1.edo.local" macAddress="00-0C-41-DB-F4-0A" switchIP="134.177.220.195" portID="54271"] radius authentication success

Severity: INFORMATIONAL
Description: RADIUS authentication is successful
Event-Class: INFORMATION

2) domainID="1" userID="host/VISTA1.edo.local" macAddress="00-0C-41-DB-F4-0A" switchIP="134.177.220.195" portID="54271"] radius authentication failed

Severity: INFORMATIONAL
Description: RADIUS authentication failed
Event-Class: INFORMATION

3) domainID="1" userID="host/VISTA1.edo.local" sourceAddress=”192.168.0.100” macAddress="00-0C-41-DB-F4-0A" switchIP="134.177.220.195" portID="54271"] StatusType = X

Where X is one of Stop, Start, Interim-Update, Accounting-On, Accounting-Off or Failed

Severity: INFORMATIONAL
Description: Received RADIUS accounting message with StatusType = X and no Framed-IP-Address
Event-Class: INFORMATION

4) domainID="1" userID="host/VISTA1.edo.local" sourceAddress=”192.168.0.100” macAddress="00-0C-41-DB-F4-0A" switchIP="134.177.220.195" portID="54271"] StatusType = X

Where X is one of Stop, Start, Interim-Update, Accounting-On, Accounting-Off or Failed

Severity: INFORMATIONAL
Description: Received RADIUS accounting message which contains Framed-IP-Address = “192.168.0.100” (Note: this is typically included when AcctStatusType = Interim-Update)
Event-Class: INFORMATION

Module (aaa_nap)

1) userID=\"<userId>\" groups=\"<Group>\" macAddress=\"<MAC>\" domainID=\"<DOMAIN_ID>\"] 802.1x Client, Change to <Vlan> VLAN. Compliancy checks ok
Severity: INFORMATIONAL
Description: Compliance checking succesfully completed
Event-Class: Security

2) userID=\"<userId>\" groups=\"<Group>\" macAddress=\"<MAC>\" domainID=\"<DOMAIN_ID>\"] 802.1x Client, Change to <Vlan> VLAN. NHA:<Status>NAP:<Status> Patchlink:<Status>.Compliancy check failed, restricting session
Severity: INFORMATIONAL
Description: Compliance check failed, restricting session
Event-Class: Security

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support .