



Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Common Criteria Configuration Guide

Version: 1.4

Date: January 24, 2022

Prepared By:
Acumen Security
2400 Research Blvd Suite 395
Rockville, MD, 20850
www.acumensecurity.net

Copyright and Trademark Notice

© CITRIX SYSTEMS, INC., 2019. ALL RIGHTS RESERVED. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS OR USED TO MAKE DERIVATIVE WORK (SUCH AS TRANSLATION, TRANSFORMATION, OR ADAPTATION) WITHOUT THE EXPRESS WRITTEN PERMISSION OF CITRIX SYSTEMS, INC.

ALTHOUGH THE MATERIAL PRESENTED IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE ALL RESPONSIBILITY FOR THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS MANUAL.

CITRIX SYSTEMS, INC. OR ITS SUPPLIERS DO NOT ASSUME ANY LIABILITY THAT MAY OCCUR DUE TO THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS DOCUMENT. INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. COMPANIES, NAMES, AND DATA USED IN EXAMPLES ARE FICTITIOUS UNLESS OTHERWISE NOTED.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the MPX 14000 Series equipment. If the NetScaler equipment causes interference, you can try to correct the interference by taking one or more of the following measures:

- Move the MPX equipment to one side or the other of your equipment.
- Move the MPX equipment farther away from your equipment.
- Plug the MPX equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

BroadCom is a registered trademark of BroadCom Corporation. Fast Ramp, NetScaler, WANScaler, Citrix XenApp, and NetScaler Request Switch are trademarks of Citrix Systems, Inc. Linux is a registered trademark of Linus Torvalds. Internet Explorer, Microsoft, PowerPoint, Windows and Windows product names such as Windows NT are trademarks or registered trademarks of the Microsoft Corporation. NetScape is a registered trademark of Netscape Communications Corporation. Red Hat is a trademark of Red Hat, Inc. Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Software covered by the following third party copyrights may be included with this product and will also be subject to the software license agreement: Copyright 1998 © Carnegie Mellon University. All rights reserved. Copyright © David L. Mills 1993, 1994. Copyright © 1992, 1993, 1994, 1997 Henry Spencer. Copyright © Jean-loup Gailly and Mark Adler. Copyright © 1999, 2000 by Jef Poskanzer. All rights reserved. Copyright © Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves. All rights reserved. Copyright © 1982, 1985, 1986, 1988-1991, 1993 Regents of the University of California. All rights reserved. Copyright © 1995 Tatu Ylonen, Espoo, Finland. All rights reserved. Copyright © UNIX System Laboratories, Inc. Copyright © 2001 Mark R V Murray. Copyright 1995-1998 © Eric Young. Copyright © 1995,1996,1997,1998. Lars Fenneberg. Copyright © 1992. Livingston Enterprises, Inc. Copyright © 1992, 1993, 1994, 1995. The Regents of the University of Michigan and Merit Network, Inc. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. Copyright © 1998 Juniper Networks, Inc. All rights reserved. Copyright © 2001, 2002 Networks Associates Technology, Inc. All rights reserved. Copyright (c) 2002 Networks Associates Technology, Inc. Copyright 1999-2001© The Open LDAP Foundation. All Rights Reserved. Copyright © 1999 Andrzej Bialecki. All rights reserved. Copyright © 2000 The Apache Software Foundation. All rights reserved. Copyright (C) 2001-2003 Robert A. van Engelen, Genivia inc. All Rights Reserved. Copyright (c) 1997-2004 University of Cambridge. All rights reserved. Copyright (c) 1995. David Greenman. Copyright (c) 2001 Jonathan Lemon. All rights reserved. Copyright (c) 1997, 1998, 1999. Bill Paul. All rights reserved. Copyright (c) 1994-1997 Matt Thomas. All rights reserved. Copyright © 2000 Jason L. Wright. Copyright © 2000 Theo de Raadt. Copyright © 2001 Patrik Lindergren. All rights reserved. Document code: June, 02, 2015 20:15:43

Table of Contents

| | | |
|--------|---|----|
| 1 | Introduction | 1 |
| 1.1 | About this Guide | 1 |
| 1.2 | TOE Overview..... | 1 |
| 1.3 | Common Criteria Evaluated Deployment | 2 |
| 1.4 | Environment Assumptions..... | 2 |
| 2 | TOE Description..... | 4 |
| 1.1.1 | TOE Evaluated Configuration | 4 |
| 1.1.2 | Physical Boundaries | 4 |
| 1.1.3 | Logical Boundaries | 5 |
| 3 | Installation | 8 |
| 3.1 | Acceptance..... | 8 |
| 3.2 | Initial Setup | 8 |
| 3.3 | FIPS Mode Self-test | 9 |
| 3.4 | Disabling NTP | 10 |
| 3.5 | Disable IPv6..... | 10 |
| 3.6 | Disable the GUI | 11 |
| 3.7 | Setting Up User Roles..... | 11 |
| 3.8 | Configuring an SSH Server..... | 11 |
| 3.9 | Cryptographic Keys | 13 |
| 3.10 | Configuring Command Policies | 13 |
| 3.10.1 | Creating Custom Command Policies..... | 14 |
| 3.10.2 | Common Criteria Command Policies | 16 |
| 3.11 | Completing Installation..... | 16 |
| 3.12 | Ongoing Administration..... | 16 |
| 4 | Upgrade the Appliance | 18 |
| 4.1 | Checking the Version | 18 |
| 4.2 | Installing a New Build..... | 18 |
| 5 | Administration and Management Security..... | 20 |
| 5.1 | Configuring a vserver | 20 |
| 5.2 | Configuring a Syslog Server..... | 22 |
| 5.3 | Configuring a LDAP Server | 23 |
| 5.4 | Configuring Password Policy | 23 |
| 5.5 | Limiting the Number of Failed Login Attempts..... | 24 |
| 5.6 | Configure Session Timeout | 24 |

| | | |
|-------|--|----|
| 5.7 | Configuring the Date and Time | 24 |
| 5.8 | Configuring Users, User Groups..... | 25 |
| 5.8.1 | Configuring user accounts..... | 25 |
| 5.8.2 | Configuring user groups..... | 26 |
| 5.8.3 | Binding command policies to users and groups | 27 |
| 5.9 | Configuring the SSH banner | 27 |
| 5.10 | Configuring a banner for console access | 28 |
| 6 | Audit Logs..... | 27 |
| 6.1 | Administrative Actions..... | 27 |
| 6.2 | Example Logs..... | 28 |
| 7 | Backup Current Configuration | 33 |
| 8 | Reverting to Factory Defaults | 35 |
| 9 | References | 36 |

Revision History

| Version | Date | Changes |
|---------|------------------|-------------------------------------|
| 1.0 | December 9, 2021 | Initial release |
| 1.1 | January 14, 2022 | Updates based on feedback |
| 1.2 | January 19, 2022 | Updated based on validator feedback |
| 1.3 | January 24, 2022 | Updated based on validator feedback |
| 1.4 | January 24, 2022 | Updated based on validator feedback |

1 Introduction

1.1 About this Guide

The Common Criteria Evaluated Configuration Guide for Citrix NetScaler 12.1 Platinum Edition describes the requirements and procedures for installing and configuring the Citrix NetScaler appliance in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require your NetScaler deployment to exactly match the Common Criteria Target of Evaluation configuration, follow the procedures in this guide.

1.2 TOE Overview

The Citrix Application Delivery Controller (ADC) are purpose-built networking appliances whose function is to improve the performance, security and resiliency of applications delivered over the web. The ADC intelligently distributes, optimizes application performance, enhances application availability with advanced Layer 4 – Layer 7 load balancing, secures applications from attacks, and lowers server expenses by offloading computationally intensive tasks. The TOE comprises Citrix ADC 12.1 software running on the following:

- Physical Platforms
 - MPX 8900 FIPS
 - MPX 15000-50G FIPS
- Virtual Platforms
 - VPX FIPS on ESXi 6.5 running on a Dell PowerEdge R630 Server

Citrix ADC MPX FIPS & Citrix ADC VPX FIPS are network devices and virtual network devices that combine Layer 4 - Layer 7 load balancing and content switching with application acceleration, data compression, static and dynamic content caching, SSL acceleration, network optimization, application performance monitoring, application visibility, and robust application security via an application firewall. The Citrix ADC MPX FIPS & Citrix ADC VPX FIPS appliances support all the NIST-approved FIPS 140-2 algorithms. The evaluation is limited to the security functionality defined in the SFRs.

1.3 Common Criteria Evaluated Deployment

The following figure provides a visual depiction of an example of a typical TOE deployment. The TOE boundary is surrounded with **red lines**.

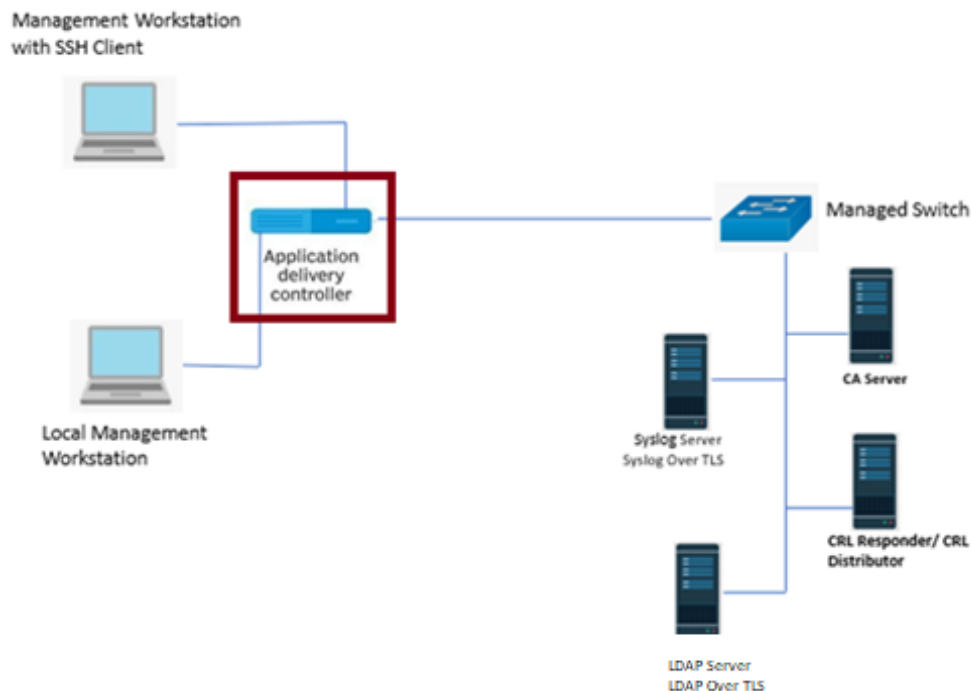


Figure 1 Deployment Configuration of TOE

NOTE: The TOE includes a CLI that may be accessed both remotely (accessed via SSH) and locally. Local access is provided by a console port located on the front of the TOE. This is accessed by directly connecting a serial console cable to the TOE. TOE administration is available at both interfaces.

1.4 Environment Assumptions

The following assumptions are made regarding the Target of Evaluation (TOE).

- The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.
- The TOE does not provide a computing platform for general purpose applications (unrelated to networking functionality).
- The TOE does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
- The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following

policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

- The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
- The administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

2 TOE Description

1.1.1 TOE Evaluated Configuration

The TOE evaluated configuration consists of the physical platforms, MPX 8900 FIPS and MPX 15000-50G FIPS. Both, the MPX 8900 FIPS and the MPX 15000-50G FIPS, operate using the Intel® Xeon E5-2620 v4 (Broadwell) processor. Additionally, the evaluated configuration includes the VPX FIPS virtual platform. This virtual platform is hosted within a Dell PowerEdge R630 Server running an instance of VMware ESXi 6.5 hypervisor. The VPX is hosted on a server which operates on an Intel® Xeon E5-2680 v4 (Broadwell) processor.

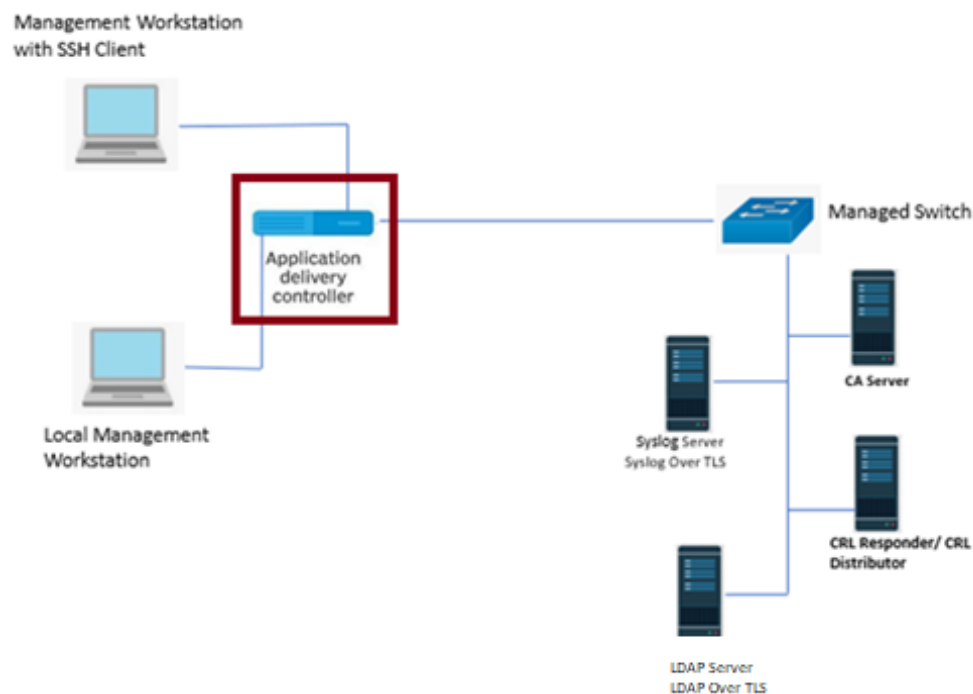


Figure 2 – Representative TOE Deployment

The above figure represents a typical deployment of the TOE. The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices.

1.1.2 Physical Boundaries

The TOE is a hardware and software solution that is comprised of the security appliance models described above in Section 1.1.1. For VPX, vND case 1 applies.

1.1.3 Logical Boundaries

The TOE provides the security functions required by NDcPP v2.2e. The TOE is composed of the FreeBSD OS running directly on the MPX appliance hardware and VPX Running on ESXi 6.5. It is also comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access
7. Trusted path/channels

These security functions are discussed in detail in the sections below.

1.1.3.1 Security Audit

The TOE keeps local and remote audit records of security relevant events. Remote audit records are transferred via TLS to the external audit server.

1.1.3.2 Cryptographic Support

The TOE provides cryptographic support for the SSH for remote administrative access and TLS connections to external IT devices.

| Algorithm | Description/Operation | Supported Mode/Standard | CAVP Cert. # | SFR |
|-----------|--|-------------------------|----------------|--|
| RSA | Signature Generation, Verification, and key transport | FIPS PUB 186-4 | C1918 C1920 | FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen FCS_COP.1/SigVer |
| ECDSA | EC Signature services in support of SSH and TLS authentication | FIPS PUB 186-4 | C1918 C1920 | FCS_CKM.1 FCS_COP.1/SigGen FCS_COP.1/SigVer |
| AES | | | C1918 | |

| Algorithm | Description/ Operation | Supported Mode/ Standard | CAVP Cert. # | SFR |
|-----------|--|---|-----------------|------------------------------|
| | Encryption in support of TLS and SSH protocols | ISO 18033-3 ISO 10116 ISO 19772 | C1920 | FCS_COP.1/ DataEncryption |
| SHA | Cryptographic hashing services | ISO/IEC 10118-3:2004 | C1918 C1920 | FCS_COP.1//Hash |
| HMAC | Keyed hashing services | ISO/IEC 9797-2:2011 | C1918 C1920 | FCS_COP.1/KeyedHash |
| DRBG | Random number generation | ISO/IEC 18031:2011 | C1918 C1920 | FCS_RBG_EXT.1 |
| KAS ECC | Key Agreement | NIST Special Publication 800-56A Revision 3 | A1919 A1920 | FCS_CKM.2 |

1.1.3.3 Identification and Authentication

The TOE provides two types of authentications to provide a trusted means for Security Administrators and remote endpoints to interact:

- Password-based or public-key authentication for Security Administrators
- X.509v3 certificate-based authentication for remote devices

Device-level authentication allows the TOE to establish a secure communication channel with a remote endpoint. Security Administrators can set a minimum length for passwords (between 4 and 127 characters). Additionally, the TOE detects and tracks consecutive unsuccessful remote authentication attempts and will prevent the offending attempts from authenticating when a Security Administrator defined threshold is reached.

1.1.3.4 Security Management

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Administrator authentication using a local database
- Timed user lockout after multiple failed authentication attempts
- Password complexity enforcement
- Role Based Access Control - the TOE supports several types of administrative user roles. Collectively these sub-roles comprise the "Security Administrator"
- Configurable banners to be displayed at login

- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

1.1.3.5 Protection of the TSF

The TOE ensures the authenticity and integrity of software updates through hash comparison and requires administrative intervention prior to the software updates being installed.

1.1.3.6 TOE Access

Prior to login, the TOE displays a banner with a message configurable by the Security Administrator. The TOE terminates user connections after an Authorized Administrator configurable amount of inactivity time.

1.1.3.7 Trusted Path/Channels

The TOE uses TLS to provide a trusted channel between itself and remote syslog and LDAP servers. The TOE uses SSH to provide a trusted path between itself and remote administrators.

3 Installation

For installation instructions, follow the “Installing the ADC Hardware” section of the Citrix Getting Started with Citrix ADC document. During the installation, an administrator will configure the initial settings.

3.1 Acceptance

When the hardware is received it should be examined for signs of tampering such as re-taped seams or punctured packaging material. If you suspect tampering, please contact your sales representative or Citrix Customer Service.

3.2 Initial Setup

After installing the hardware, access the ADC appliance through the serial console for initial configuration. Through the serial console, you can change the system IP address, create a subnet or mapped IP address, configure advanced network settings, and change the time zone. You can run a script to perform most of the initial configuration. This script is part of the software and not provided separately. You then specify a route for administrative access to the appliance through your network, and you can specify administrator credentials.

Only users with superuser privileges can perform the initial configuration. Use of the superuser role is not allowed after initial setup, so cmdPolicies must be configured to enable ongoing administration without the superuser account.

Note: The RS232 serial console port is on the front of each appliance and provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

To configure initial settings by using a serial console:

1. Connect the console cable to the appliance and your computer.
2. On your computer, run the vt100 terminal emulation program of your choice to connect to the appliance.
 - For Microsoft Windows, use a terminal emulation client such as PuTTY.
 - For Apple Macintosh OSX, use the GUI-based terminal program or the shell-based telnet client.

Note: OSX is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.
 - For UNIX-based workstations, use the shell-based Telnet client or any supported terminal emulation program.
3. Press ENTER. The terminal screen displays the logon prompt.
4. Log on to the appliance with the administrator credentials.

Your sales representative or Citrix Customer Service can provide the initial administrator credentials.
5. At the prompt, type `config ns` to run the ADC configuration command, which invokes a script. The script is built into the software.

When finished with the configurations in `config ns` script, run the following commands to set the ADC IP (NSIP) address (the management address) and administrator credentials:

```
add ns ip <IP> <subnetMask> -type NSIP -vServer DISABLED -telnet DISABLED -ftp
DISABLED -gui DISABLED -mgmtAccess ENABLED -dynamicRouting ENABLED
add route <network> <subnetMask> <gateway>
add dns nameServer <IP>
set system user nsroot -password
save ns config
```

Example

```
> add ns ip 20.0.0.20 255.255.255.0 -type NSIP -vServer DISABLED -telnet DISABLED -ftp
DISABLED -gui DISABLED -mgmtAccess ENABLED -dynamicRouting ENABLED
> add route 0.0.0.0 0.0.0.0 10.102.29.1
> add dns nameserver 10.102.29.1
> set system user nsroot -password
Enter password:
Confirm password:
Done
```

Note:

1. The NSIP address should be non-routable, to prevent an attacker from breaching your ability to send packets to the appliance. This is because dynamic routing is always enabled on the NSIP address and cannot be disabled.
2. The NSIP address should not be publicly accessible, and proper security measures should be in place to authorize users who access the NSIP address to configure the TOE. For more information, see "User Access Control".

3.3 FIPS Mode Self-test

When the ADC appliance boots up, a FIPS card self-test checks the integrity of the card. A power on self test is performed on the following three libraries:

- OpenSSL with FIPS object module in control plane (Citrix FIPS Cryptographic Module)
- Software Crypto library in dataplane/PE
- HW Crypto library in dataplane/PE.

The ADC additionally performs several additional health checks, including, Memory (RAM) walk, File integrity verification and kernel image verification. In totality, the following tests are performed at bootup,

- Memory (RAM) walk
- File integrity verification
- Kernel image verification
- Integrity checks for the Citrix FIPS Cryptographic Module
- Algorithm known answer tests for the Citrix FIPS Cryptographic Module

If any of the self tests fail, the system will reboot into non-FIPS mode. A user may verify if the self tests have passed or failed at the following locations:

- For control plane `/var/log/FIPS-post.log`
- For dataplane `/var/log/ns.log`

To verify that the device is operating in FIPS mode, the user may type the following command:

```
Show fipsStatus
```

The output will reflect either:

FipsStatus: "System is operating in FIPS mode"

Or

FipsStatus: "System is operating in non FIPS mode"

The successful completion or failure of the bootup tests can be verified by checking the log files. Successful completion of the bootup tests is indicated by "FIPS POST Successful" in /var/log/ns.log and successful completion of the Citrix ADC CP Cryptographic Library v4 specific self-tests is indicated by "POST Success" in /var/log/FIPS-post.log. Failure of the bootup tests is indicated by "FIPS Post Failed" in /var/log/ns.log and failure of the Citrix ADC CP Cryptographic Library v4 specific self-tests is indicated by "POST Failed" in /var/log/FIPS-post.log (both messages indicate a critical error state). In this state, the ADC will not provide any cryptographic services.

If any failures are detected during the Memory walk, the TOE will take the memory module out of service and log the error. The TOE will continue to operate if one memory module remains operational.

Additional information on FIPS mode may be found below:

MPX FIPS:

<https://docs.citrix.com/en-us/citrix-adc/12-1/ssl/citrix-adc-mpx-fips-certified-appliance.html>

VPX FIPS:

<https://docs.citrix.com/en-us/citrix-adc/12-1/ssl/citrix-adc-vpx-fips-appliances.html>

If the TOE enters the error state due to a failure of the integrity test, the boot sequence and entire system is halted. The only action available from this state is to reboot the TOE to trigger the re-execution of the integrity test. The error condition is considered to have been cleared if the TOE successfully passes the integrity test and then all subsequent power-up self-tests. If the TOE continues to return to a halted state, the TOE is considered to be malfunctioning or compromised, and Citrix Customer Support must be contacted.

If the TOE enters the error state due to a failure of any of the remaining self-tests, the TOE will automatically reboot to clear the error state. The Security Administrator must contact Citrix Customer Support if this error occurs.

3.4 Disabling NTP

When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that NTP synchronization is disabled.

To disable NTP sync

At the ADC command prompt, type

```
disable ntp sync
```

3.5 Disable IPv6

When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that IPv6 protocol translation is disabled.

To disable IPv6

At the ADC command prompt, type

```
disable ns feature IPv6protocoltranslation
```

3.6 Disable the GUI

To conform to the Common Criteria Evaluated deployment, you must disable the GUI. Disabling the GUI also disable other access methods, such as the NITRO API. No separate commands need to be run to disable those methods.

To disable the GUI

At the ADC command prompt, type

```
set ns ip <NSIP> -GUI DISABLED
```

3.7 Setting Up User Roles

To create a user dedicated to audit review, an administrator should create a user (e.g., audit_user) and set the cmdPolicy as described below:

```
> add system cmdPolicy audit_policy ALLOW '^man.*|^show\s+audit'
> bind system user audit_user audit_policy 100
```

More information can be found here: <http://docs.citrix.com/en-us/netscaler/11-1/reference/netscaler-command-reference/system/system-cmdpolicy.html>.

3.8 Configuring an SSH Server

Several parameters governing the TOE's SSH server behavior may be modified. To do this, login as a superuser and enter shell.

Edit the sshd_config file in /etc/sshd_config.

In the event that /nsconfig/sshd_config did not exist, then /etc/sshd_config must be manually linked to /nsconfig/sshd_config in order to avoid a reboot. The original file must be removed prior to the linking to avoid the following error:

```
root# ln -s /nsconfig/sshd_config /etc/sshd_config
ln: /etc/sshd_config: File exists
```

A host key must be generated for the SSH server. In order to do this use the following commands,

```
ssh-keygen -t rsa -b <2048, 3072> The 2048 or 3072 represent the key size.
```

The following options may be reconfigured:

```
Ciphers aes256-ctr,aes256-cbc,aes128-ctr,aes128-cbc
MACs hmac-sha2-256,hmac-sha2-512 (Note this disables all other MACs including the "none"
MAC)
```



```
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
Banner /nsconfig/ssh/sshd_banner

RekeyLimit 1G 1h (The rekey limit values are not limited by the TOE. However, in the
evaluated configuration the maximum that may be set is 1G and 1h)

LogLevel DEBUG
```

In order for any changes done to the `sshd_config` file to take effect, the process must be restarted with the following command:

```
kill -HUP `cat /var/run/sshd.pid`
```

Note: The TOE will only allow the algorithms specified in the above configuration file to be used in a remote session. All other algorithms will be rejected, resulting in a failure to establish a connection.

Note: Configuring SSH will ensure that only evaluated hashing is used in support of the SSH Key Derivation. No additional configuration is needed to ensure this functionality.

Note: Configuring the supported HMAC automatically configures the characteristics of the HMAC including, key length, hash function used, block size, and output MAC length. No additional configuration is necessary.

Note: The TOE will be rekeyed once either rekey threshold is reached (time or data), depending on which happens first.

To secure administrative access to the ADC appliance by using the public key authentication mechanism of SSH, complete the following procedure:

- If it does not exist, create the `/var/pubkey/<username>/.ssh/authorized_keys` file.
- Run the following command to set permissions for the file:

```
# chmod 644 /var/pubkey/<username>/.ssh/authorized_keys
```
- Run the following command to append the public key to the `/var/pubkey/<username>/.ssh/authorized_keys` file:

```
# cat id_rsa.pub >> /var/pubkey/<username>/.ssh/authorized_keys
```
- If the key must be removed for any reason, use the following command:

```
# rm id_rsa.pub
```

After initial setup, the TOE may be administered by physically connecting to the device via console cable or remotely through the use of SSH using a configured IP address. Once the connection is established, the user may login using a valid username and password. A user may terminate an active session anytime by typing 'exit' on the command prompt. For more information, please visit the link below:

<https://docs.citrix.com/en-us/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/ssh-key-based-authentication-for-system-users.html#user-specific-ssh-key-based-authentication-for-local-system-users>

3.9 Cryptographic Keys

The TOE generates a variety of cryptographic keys for several purposes. These keys are stored in locations inaccessible to the user with the SSH Public Key as the only exception. Only the SSH Public Key may be manually deleted by the user. The cryptographic keys are immediately deleted upon reboot of the device. Keys will be regenerated upon usage of each specific function. Please see the above section 3.8 for instructions on deleting the SSH Public Key as well as configuring specific ciphers and algorithms to be used during SSH and TLS connectivity. The table below outlines the different keys generated by the TOE, their purpose, and storage location as well as zeroization method:

| Keys/CSPs | Purpose | Storage Location | Method of Zeroization |
|-----------------------------------|---|-------------------------|--|
| EC/FFC Diffie Hellman private key | Key exchange private keys in support of TLS and SSH | RAM | Overwritten with zeros at the end of session or upon power off/reboot. |
| EC/FFC Diffie Hellman public key | Key exchange public keys in support of TLS and SSH | RAM | Overwritten with zeros at the end of session or upon power off/reboot. |
| SSH Private Key | SSH host private key used in server authentication | ACL protected directory | Overwritten with zeros when the zeroization command is issued. |
| SSH Public Key | SSH host public key used in server authentication | N/A public | Overwritten with zeros when the zeroization command is issued. |
| SSH Session Key | Encryption keys associated with the SSH protocol | RAM | Overwritten with zeros at the end of session or upon power off/reboot. |
| TLS Session Encryption Key | Encryption keys associated with the TLS protocol | RAM | Overwritten with zeros at the end of session or upon power off/reboot. |
| TLS Session Integrity Key | Integrity keys associated with the TLS protocol | RAM | Overwritten with zeros at the end of session or upon power off/reboot. |

The TOE performs all deterministic random bit generation services with a minimum of 256 bits of entropy at least equal to the greatest security strength in accordance with ISO/IEC 18031:2011.

Note: There are no situations that could prevent or delay key destruction within the product.

3.10 Configuring Command Policies

Command policies regulate which commands, command groups, virtual servers, and other entities that users and user groups are permitted to use.

The appliance provides a set of built-in command policies, and you can configure custom policies. To apply the policies, you bind them to users and/or groups.

Here are the key points to keep in mind when defining and applying command policies.

- You cannot create global command policies. Command policies must be bound directly to the users and groups on the appliance.
- Users or groups with no associated command policies are subject to the default (DENY-ALL) command policy, and are therefore unable to execute any configuration commands until the proper command policies are bound to their accounts.
- All users inherit the policies of the groups to which they belong.
- You must assign a priority to a command policy when you bind it to a user account or group account. This enables the appliance to determine which policy has priority when two or more conflicting policies apply to the same user or group.
- The following commands are available by default to any user and are unaffected by any command you specify:

help, show cli attribute, set cli prompt, clear cli prompt, show cli prompt, alias, unalias, history, quit, exit, whoami, config, set cli mode, unset cli mode, and show cli mode.

Built-in Command Policies

The following table describes the built-in policies.

Table 1. Built-in Command Policies

| Policy name | Allows |
|-------------|--|
| read-only | Read-only access to all show commands except show ns runningConfig, show ns ns.conf, and the show commands for the ADC command group. |
| Operator | Read-only access and access to commands to enable and disable services and servers. |
| Network | Full access, except to the set and unset SSL commands, show ns ns.conf, show ns runningConfig, and show gslb runningConfig commands. |
| Sysadmin | A sysadmin is lower than a superuser in terms of access allowed on the appliance. A sysadmin user can perform all Citrix ADC operations with the following exceptions: no access to the Citrix ADC shell, cannot perform user configurations, cannot perform partition configurations, and some other configurations as stated in the sysadmin command policy. |
| Superuser | Full access. Same privileges as the nsroot user. |

Please refer to the following link for more detailed information:

<https://docs.citrix.com/en-us/citrix-adc/12-1/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-config-users-and-grps-tsk.html#configuring-command-policies>

3.10.1 Creating Custom Command Policies

Regular expression support is offered for users with the resources to maintain more customized expressions, and for those deployments that require the flexibility that regular expressions

offer. For most users, the built-in command policies are sufficient. Users who need additional levels of control but are unfamiliar with regular expressions might want to use only simple expressions, such as those in the examples provided in this section, to maintain policy readability.

When you use a regular expression to create a command policy, keep the following in mind.

- When you use regular expressions to define commands that will be affected by a command policy, you must enclose the commands in double quotation marks. For example, to create a command policy that includes all commands that begin with show, type the following:
 - “^show.*\$”
- To create a command policy that includes all commands that begin with rm, type the following:
 - “^rm.*\$”
- Regular expressions used in command policies are not case sensitive.

The following table lists examples of regular expressions:

Table 2. Examples of Regular Expressions for Command Policies

| Command specification | Matches these commands |
|------------------------------|---|
| “^rm\s+.*\$” | All remove actions, because all remove actions begin with the rm string, followed by a space and additional parameters such as command groups, command object types, and arguments. |
| “^show\s+.*\$” | All show commands, because all show actions begin with the show string, followed by a space and additional parameters such as command groups, command object types, and arguments. |
| “^shell\$” | The shell command alone, but not combined with any additional parameters such as command groups, command object types, and arguments. |
| “^add\s+vserver\s+.*\$” | All create virtual server actions, which consist of the add virtual server command followed by a space and additional parameters such as command groups, command object types, and arguments. |
| “^add\s+(lb\s+vserver)\s+.*” | All create lb virtual server actions, which consist of the add lb virtual server command followed by a space and additional parameters such as command groups, command object types, and arguments. |

The following table shows the command specifications for each of the built-in command policies.

Table 3. Expressions Used in the Built-in Command Policies

| Policy name | Command specification regular expression |
|-------------|---|
| read-only | (^man.*) (^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*) (^stat.*) |
| operator | (^man.*) (^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*) (^stat.*) (^enable disable) (server service).* |
| network | ^(?!clear ns config.*)(?!scp.*)(?!set ssl fips)(?!reset ssl fips)(?!diff ns config)(?!shell)(?!reboot)(?!batch)\S+\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!techsupport).* |
| sysadmin | ^(?!shell)(?!sftp)(?!scp)(?!batch)(?!source)(?!.*superuser)(?!.*nsroot)(?!show\s+system\s+(user cmdPolicy))(?!(set add rm create export kill)\s+system)(?!(unbind bind)\s+system\s+(user group))(?!diff\s+ns\s+config)(?!S+\s+ns\s+partition).* |
| Superuser | .* |

To create a command policy by using the command line interface

At the command prompt, type the following commands to create a command policy and verify the configuration:

- add system cmdPolicy <policyname> <action> <cmdsSpec>
- show system cmdPolicy <policyName>

Example

```
> add system cmdPolicy read_all ALLOW (^shows+(!system)(!ns ns.conf)(!ns runningConfig).*)|(^stat.*)
```

3.10.2 Common Criteria Command Policies

The following command policies must be configured by the superuser to limit administrator access

```
> add system cmdPolicy shell ALLOW (shell (mkdir|tar|.*installns|cat /tmp/aaad.debug|date|tail -f /var/log/notice.log|.logkeys_1.sh.|scp *|vi /nsconfig/ssh/sshd_banner|vi /nsconfig/issue|date *|sha256 *))
```

```
> add system cmdPolicy show ALLOW (^show\s+.*$)
```

```
> add system cmdPolicy set ALLOW (^S+\s+(!system).*)
```

3.11 Completing Installation

When operating the TOE in the Common Criteria evaluated configuration, use of the nsroot and superuser accounts must be restricted by policy. These accounts may not be used while operating in the Common Criteria evaluated configuration.

3.12 Ongoing Administration

The TOE can be administered both locally via the console interface and remotely via an SSH client. Administration via the console interface requires the Security Administrator to directly plug into the TOE. This is not a networked interface. Administration via SSH requires that the Security Administrator connect to the TOE via port 22. Any SSH client may be used that meets the following:

- Support for SSHv2

- Support for cryptographic algorithms defined in the Security Target

Super User is not allowed for ongoing configuration only the Security Administrator may be used.

Once all the files are extracted, execute the following command to install the build:

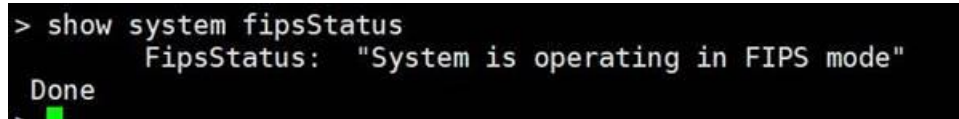
```
> ./installns -F
```

You will be prompted to reboot the box to install the build, please click on Yes to reboot the box.

5. Once the box has finished rebooting, verify that FIPS Mode is operational by executing following command:

```
> show system fipsstatus
```

The expected output will look as follows:



```
> show system fipsStatus
    FipsStatus: "System is operating in FIPS mode"
Done
```

Alternatively, the administrator may check if FIPS mode is operational through shell by inputting the following command to verify that the value is 1, indicating that the FIPS Mode is on:

```
> shell
root@ns# sysctl netcaler.fips_mode
root@ns# netcaler.fips_mode: 1
```

After the build is installed and the appliance reboots, type the command “show version” and verify the upgrade was successful.

5 Administration and Management

Security

5.1 Configuring a vserver

Following are the configuration steps on ADC for securely communicating over a TLSv1.1 or TLSv1.2 connection with an external TLS server. The examples in these steps assume the server is a syslog server. The bold text should be substituted for appropriate alternative labels to make identification of the service and LB vserver easier:

1. Copy the CA certificate (certificate of the Certificate Authority that issued the certificate to the TLS server) to the ADC Appliance (under /nsconfig/ssl folder). Note these steps designate the CA certificate as a Trust Anchor.
 - Issue the following command on the certificate:
`openssl x509 -noout -hash -in <ca_certificate>`
The result is a hash (for example 6d2962a8), a series of alphanumeric characters based on the Distinguished Name of the certificate.
 - Issue the following command to create a symbolic link to the certificate that uses the hash returned by the previous command and the .0 suffix.
`ln -s <ca_certificate> 6d2962a8.0`
2. Add ssl certkey by giving the CA certificate path.
`add ssl certkey server_cacert -cert <path_to_ca_cert>`

Note: In support certificate usage by the TOE, the environment must include the following:

- CA Server: This is required to provide the certificates used by the TOE
- CRL Server: This is required to provide revocation response to requests

The only prerequisite is that each server must support http for communication with the TOE. If a connection is not available, the TOE will not proceed with the connection. If this is the case, the Security Administrator must verify that the connection is available and resolve any issues resulting in lack of connection.

3. Add service of type SSL_TCP with the IP of syslog server and port on which the syslog server listens for SSL packets.
`add service syslog_service <syslog_server_ip> SSL_TCP <syslog_server_port>`

4. Bind the certkey to the service by giving the option -CA.
`bind ssl service syslog_service -certkeyName server_cacert -CA`
5. Enable the server authentication in the service.
`set ssl service syslog_service -serverAuth ENABLED`
6. Add LB vserver of type TCP with some IP and port 514. Add SNIP in the lb vserver IP's subnet.
`add lb vserver lb_vserver TCP <lb_vserver_ip> 514`
7. Bind the service to LB vserver.
`bind lb vserver lb_vserver syslog_service`

To configure the TLS ciphersuites, the administrator can use the following commands:

1> show ssl service [name of service created in step 3 above]

(if there is a default cipher name bound to it already as shown below, do 2. If not move on to 3)

```
1)      Cipher Name: cc_ciphers
        Description: User Created Cipher Group
Done
```

2> unbind ssl service [name of service] -ciphername [cc_ciphers]

3>add ssl cipher [name of custom ciphersuite list]

This will allow the administrator to add the ciphersuites he wants to use. *show ciphersuite* is used to display the available ciphersuites and the format. Ex: add ssl cipher test

4> bind ssl cipher [cipher list] -ciphername [name of ciphersuite]

Ex: bind ssl cipher test -ciphername TLS1-AES-128-CBC-SHA

NOTE: The allowed ciphernames include:

- TLS1-AES-128-CBC-SHA
- TLS1-AES-256-CBC-SHA
- TLS1-ECDHE-RSA-AES128-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1.2-AES-128-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-ECDHE-RSA-AES128-SHA256
- TLS1.2-ECDHE-RSA-AES256-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384

- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES256-GCM-SHA384

NOTE: The TLS version is set by the “TLS” portion of the command.

5> bind ssl service [service name] -ciphername [cipher list]

Ex: bind ssl service syslog -ciphername test

Note: Configuring ciphersuites automatically configures the characteristics of the HMAC used including, key length, hash function used, block size, and output MAC length. No additional configuration is necessary.

Note: The TOE automatically configures references identifiers based on the FQDN configured by the administrator to connect to the TLS server. When a FQDN has been configured, the TOE establishes reference identifiers of DNS-ID and CN-ID. When the TOE compares the reference identifiers to the identifiers in the presented certificate, it will consider the identifiers matching if they are an exact match or if the presented identifier exactly matches with the exception of a wildcard in the left most position matching the left most position of the reference identifier. The TOE will use the SAN(s) in the presented certificate if present. The TOE will only use the CN if the certificate does not contain any SANs.

Note: If a TLS connection to a remote server (e.g., syslog server or LDAP server) is broken, the TOE will automatically reconnect. However, if the connection remains broken, the Security Administrator must verify both the logical and physical availability of the remote device and resolve any issues resulting in lack of connection on a case-by-case basis.

The TOE does not support certificate pinning.

The TOE will not establish the connection if the server certificate is invalid, if the presented identifier does not match, or if the CRL cannot be retrieved.

All certificate validation is performed at the time the certificate is presented to the TOE.

All required rules for extendedKeyUsage validation is supported.

The TOE presents only the following Elliptic Curves secp256r1, secp384r1. This is by default. No configuration is required.

5.2 Configuring a Syslog Server

Configure a vserver to handle TLS connections as described above in “Configuring a vserver”

1. Add syslogaction with the IP address as LB VIP, port as 514 and transport as TCP.
`add syslogaction sys_act <lb_vserver_ip> -loglevel all -transport TCP -serverPort 514`
2. Add syslogpolicy and bind this policy to system global.
`add syslogpolicy sys_pol true sys_act`
`bind syslogglobal -policyname sys_pol -priority 1`

Note: When the connection to the syslog server is down, the audit records are stored locally. When the connection to the syslog server comes back up, the TOE will resume transmission of audit records to the syslog server; however, it does not transmit audit records generated while the connection was down.

5.3 Configuring a LDAP Server

Configure a vserver to handle TLS connections as described above in “Configuring a vserver”. The port in Step 6 should be 636 instead of 514.

1. Creating LDAP Server

```
add authentication ldapAction LDAP_mgmt -serverIP <lb_vserver_ip> -serverPort
636 -ldapBase <ldap Base name> -ldapBindDn <ldap bind DN> -ldapBindDnPassword
<ldap bind dn password> -ldapLoginName sAMAccountName -searchFilter <search
filter> -groupAttrName memberOf
```

2. Creating LDAP Policy

```
add authentication policy <ldap policy name> -rule true -action <ldap action
name>
```

3. Binding LDAP Policy

```
bind system global <ldap policy name> -priority 110
```

4. Assign privileges to your administrators

```
### Scenario A. Applying privileges on the group
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
### Scenario B. Applying the privileges individually for each users
add system user admyoa
bind system user admyoa superuser 100
```

5.4 Configuring Password Policy

The set system parameter CLI command must be used to enable a strong password policy. Execute the following command at the CLI console: `set system parameter -strongpassword enablelocal`. A warning message will be returned as follows: “Warning: Strong Password now enabled. Please ensure all the existing user passwords adhere to this restriction. Minimum Password Length is set to 4 as default.”

After enabling a strong password policy, the minimum password length must be set to 15 characters using the following command: `set system parameter -minpasswordlen 15`.

After the above commands are issued, the SUT will enforce a password complexity requiring the following:

- at least one uppercase character be used
- at least one lower-case character be used
- at least one numeric character be used
- at least one special character be used
- a minimum 15-character password length

Note: Passwords can be composed of any non-whitespace printable ASCII character. This does not include extended ASCII.

5.5 Limiting the Number of Failed Login Attempts

The CLI `aaa parameter` command may be used to set the global AAA configuration, including the maximum number of login attempts and the number of minutes an account will be locked if a user exceeds the maximum permissible attempts. To enforce user lock out after maximum number of allowed login attempts, the `maxloginAttempts` parameter should be set, and to enforce the account lock out period, the `failedLoginTimeout` parameter should be set. An administrator can use the following command and specify the values for configuring failed login attempts and account lock out period:

```
set aaa parameter maxloginAttempts <num> failedLoginTimeout <seconds> -
failedLoginTimeout <seconds> -persistentLoginAttempts ENABLED
```

Upon configuring the above, at login, SUT displays number of unsuccessful login attempts that occurred since the last successful login.

A locked account can be unlocked by running the following command:

```
unlock aaa user <username>
```

Note: The lock out only applies to remote login attempts. Local console administration is never locked.

5.6 Configure Session Timeout

Configure the session inactivity timeout to ensure that inactive sessions do not remain active for a long duration of time. The session inactivity timeout applies to both local and remote interactive sessions.

To configure session inactivity timeout

1. At the ADC command prompt, type the following command to enable restricted timeout:

```
set system parameter -restrictedtimeout enabled
```

2. Set a system-user specific timeout. The timeout parameter sets the CLI session inactivity timeout, in seconds. Timeout can have values in the range 300-86400 seconds. For example, the following command sets the timeout to 400 seconds for the user **testusr**. The user will be logged out after 400 seconds.

```
set system user testusr -timeout 400
```

5.7 Configuring the Date and Time

Configure the date and time by running

```
shell date YYYYMMDDHHmm
```

Where:

- YY – the two digit year
- MM – the two digit month
- DD – the two digit day of the month
- HH – the two digit hour using a 24 hour clock
- mm – the two digit minute

For example:

```
shell date 1903181230
```

Sets the date and time to March 18, 2019, 12:30PM

5.8 Configuring Users, User Groups

You must define your users by configuring accounts for them. To simplify the management of user accounts, you can organize them into groups. You can create command policies, or use built-in command policies, to regulate user access to commands.

You can also customize the command-line prompt for a user. Prompts can be defined in a user's configuration, in a user-group configuration, and in the global system configuration settings. The prompt displayed for a given user is determined by the following order of precedence:

- Display the prompt as defined in the user's configuration.
- Display the prompt as defined in the group configuration for the user's group.
- Display the prompt as defined in the system global configuration settings.

You can now specify a timeout value for inactive CLI sessions for a system user. If a user's CLI session is idle for a time that exceeds the timeout value, the ADC appliance terminates the connection. The timeout can be defined in a user's configuration, in a user-group configuration, and in the global system configuration settings. The timeout for inactive CLI sessions for a user is determined by the following order of precedence:

- Timeout value as defined in the user's configuration.
- Timeout value as defined in the group configuration for the user's group.
- Timeout value as defined in the global system configuration settings.

An ADC root administrator can configure the maximum concurrent session limit for system users. By restricting the limit, you can reduce the number of open connections and improve server performance. As long as the CLI count is within the configured limit, concurrent users can log on the GUI any number of times. However, if the number of CLI sessions reaches the configured limit, users can no longer log on to the GUI. For example, if the number of concurrent session is configured to 20, concurrent users can log on to 19 CLI sessions. But if the user is logged on to the 20th CLI session, any attempt to log on to the GUI, CLI or NITRO results in an error message (ERROR: Connection limit to CFE exceeded).

Additionally, each administrator may terminate their session via the **logout** or **exit** command

Note

The default the number of concurrent sessions is configured to 20 and the maximum number of concurrent sessions is configured to 40.

5.8.1 Configuring user accounts

To configure user accounts, you simply specify usernames and passwords. You can change passwords and remove user accounts at any time.

To create a user account by using the command line interface

At the command prompt, type the following commands to create a user account and verify the configuration:

- add system user <username> [-externalAuth (ENABLED | DISABLED)] [-promptString <string>] [-timeout \<secs>] [-logging (ENABLED | DISABLED)] [-maxsession <positive_integer>]
- show system user <userName>

Where Logging option is for external users to collect log data externally using weblogging or audit logging mechanism. If enabled, the auditing client authenticates itself with ADC to collect logs through this user account.

Example

```
> add system user johnd -promptString user-%u-at-%T
```

Enter password:

Confirm password:

```
> show system user johnd
```

user name: john

Timeout:900 Timeout Inherited From: Global

External Authentication: ENABLED

Logging: DISABLED

Maximum Client Sessions: 20

5.8.2 Configuring user groups

After configuring a user group, you can easily grant the same access rights to everyone in the group. To configure a group, you create the group and bind users to the group. You can bind each user account to more than one group. Binding user accounts to multiple groups might allow more flexibility when applying command policies.

To create a user group by using the command line interface

At the command prompt, type the following commands to create a user group and verify the configuration:

- add system group <groupName> [-promptString <string>] [-timeout <secs>]
- show system group <groupName>

Example

```
> add system group Managers -promptString Group-Managers-at-%h
```

To bind a user to a group by using the command line interface

At the command prompt, type the following commands to bind a user account to a group and verify the configuration:

- bind system group <groupName> -userName <userName>
- show system group <groupName>

Example

```
> bind system group Managers -userName user1
```

5.8.3 Binding command policies to users and groups

Once you have defined your command policies, you must bind them to the appropriate user accounts and groups. When you bind a policy, you must assign it a priority so that the appliance can determine which command policy to follow when two or more applicable command policies are in conflict.

Command policies are evaluated in the following order:

- Command policies bound directly to users and the corresponding groups are evaluated according to priority number. A command policy with a lower priority number is evaluated before one with a higher priority number. Therefore, any privileges the lower-numbered command policy explicitly grants or denies are not overridden by a higher-numbered command policy.
- When two command policies, one bound to a user account and other to a group, have the same priority number, the command policy bound directly to the user account is evaluated first.

To bind command policies to a user by using the command line interface

At the command prompt, type the following commands to bind a command policy to a user and verify the configuration:

- `bind system user <userName> -policyName <policyName> <priority>`
- `show system user <userName>`

Example

```
> bind system user user1 -policyName read_all 1
```

To bind command policies to a group by using the command line interface

At the command prompt, type the following commands to bind a command policy to a user group and verify the configuration:

- `bind system group <groupName> -policyName <policyName> <priority>`
- `show system group <groupName>`

Example

```
> bind system group Managers -policyName read_all 1
```

5.9 Configuring the SSH banner

To Configure a notice and a warning message, do the following:

1. Edit the banner

```
> shell vi /nsconfig/ssh/sshd_banner
```

2. Enter the message that you want to be displayed and save the file. For example:

```
***** Warning - Warning - Warning*****  
This system is restricted to authorized individuals and is the  
property of <Company>. Unauthorized access is prohibited and all  
access attempts are monitored.  
***** Warning - Warning - Warning*****
```

3. Restart your ADC appliance. At the command prompt, type:

```
> reboot
```



```
Are you sure you want to restart NetScaler (Y/N)?[N]y
Done
>
```

5.10 Configuring a banner for console access

Please follow the below steps to configure a warning message for the serial console:

1. Edit the /nsconfig/issue file

```
> shell vi /nsconfig/issue
```

2. Add the desired warning message. For example:

```
"Warning: You are connecting to a secure resource"
```

3. Restart your ADC appliance. At the command prompt, type:

```
> reboot
Are you sure you want to restart NetScaler (Y/N)?[N]y
Done
```

6 Audit Logs

The administrator can collect logs from 2 different locations:

- Using the CLI command: show messages
- Using the CLI command: shell cat /var/log/[log file admin wants to open]

Enable DEBUG Log Level for Syslog Events from ADC CLI

Run the following command to enable debugging:

```
set audit syslogParams -logLevel ALL
```

Run the following command to disable debugging:

```
set audit syslogParams -logLevel EMERGENCY ALERT CRITICAL ERROR WARNING NOTICE INFORMATIONAL
```

6.1 Administrative Actions

The TOE shall be able to generate an audit record of the following administrative actions:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators). Instructions for a successful login and logout may be found in section 3.8 “Configuring an SSH server” of this document.
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed). Instructions for configuration changes may be found in section 5 “Administration and Management Security” of this document.
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). Instructions for cryptographic key management may be found in sections 3.8 “Configuring an SSH Server”, 3.9 “Cryptographic Keys”, and 5.1 “Configuring a vserver” of this document.
- Resetting passwords (name of related user account shall be logged). Instructions on password management may be found in section 5.4 “Configuring Password Policy” of this document.

6.2 Example Logs

The following table identifies example audit logs for NDcPP Auditable Events.

| Requirement | Auditable Events | Additional Audit Record Contents | Sample Audit Records |
|------------------------------|------------------|----------------------------------|----------------------|
| FAU_GEN.1 | None | None | NA |
| FAU_GEN.2 | None | None | NA |
| FAU_STG_EXT.1 | None | None | NA |
| FCS_CKM.1 | None | None | NA |
| FCS_CKM.2 | None | None | NA |
| FCS_CKM.4 | None | None | NA |
| FCS_COP.1/ DataEncryption | None | None | NA |
| FCS_COP.1/SigGen | None | None | NA |
| FCS_COP.1/Hash | None | None | NA |
| FCS_COP.1/ KeyedHash | None | None | NA |
| FCS_RBG_EXT.1 | None | None | NA |

| | | | |
|----------------|--|--|--|
| FCS_SSHS_EXT.1 | Failure to establish an SSH session | Reason for failure | 9) 02/16/2021:23:04:49 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 105 0 : User test1 - Remote_ip 10.1.2.171 - Command "login test1 "*****" - Status "ERROR: Invalid username or password" |
| FCS_TLSC_EXT.1 | Failure to establish a TLS Session | Reason for failure | 13) 05/21/2021:15:18:00 GMT Debug 0-PPE-0 : default SSLLOG SSL_HANDSHAKE_FAILURE 2673 0 : Backend SPCBId 1364 - ServerIP 10.1.2.171 - ServerPort 1514 - ProtocolVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session New - SERVER AUTHENTICATED - Reason "Handshake failure-Internal Error" 14) 05/21/2021:15:18:05 GMT Debug 0-PPE-0 : default SSLLOG SSL_HANDSHAKE_FAILURE 2674 0 : Backend SPCBId 1365 - ServerIP 10.1.2.171 - ServerPort 1514 - ProtocolVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session New - SERVER AUTHENTICATED - Reason "Handshake failure-Internal Error" |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded | Origin of the attempt (e.g., IP address) | 17) 02/14/2021:23:16:28 GMT Error 0-PPE-0 : default AAA Message 131 0 : "user: test1 is locked down, max login attempt 3 within 1 min(s) has been reached." |
| FIA_PMG_EXT.1 | None | None | NA |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism | Origin of the attempt (e.g., IP address) | 15) 02/19/2021:23:18:36 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 977 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "*****" - Status "ERROR: Invalid username or password" 19) 02/19/2021:23:20:09 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 981 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "*****" - Status "Success" |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism | Origin of the attempt (e.g., IP address) | 15) 02/19/2021:23:18:36 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 977 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "*****" - Status "ERROR: Invalid username or password" 19) 02/19/2021:23:20:09 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 981 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "*****" - Status "Success" |
| FIA_UAU.7 | None | None | NA |

| | | | |
|-------------------------|--|--|--|
| FIA_X509_EXT.1/Rev | · Unsuccessful attempt to validate a certificate | · Reason for failure of certificate validation | <pre>18) 09/21/2021:07:16:22 GMT Debug 0-PPE-0 : default SSLLOG SSL_HANDSHAKE_FAILURE 397 0 : Backend SPCBID 482 - ServerIP 10.1.2.171 - ServerPort 1514 - ProtocolVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session New - SERVER AUTHENTICATION FAILED - Reason "Invalid server certificate"</pre> |
| | · Any addition, replacement or removal of trust anchors in the TOE's trust store | · Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store | <pre>19) 09/23/2021:01:27:25 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 185 0 : User nsroot - Remote_ip 192.168.254.155 - Command "rm ssl certKey_ica_ec" - Status "Success"</pre> |
| FIA_X509_EXT.2 | None | None | NA |
| FMT_MOF.1/Manual Update | Any attempt to initiate a manual update | None | <pre>17) 11/03/2021:18:42:54 GMT citrixmpx Informational 0-PPE-5 : default CLI CMD_EXECUTED 180 0 : User Test1 - Remote_ip 10.1.2.155 - Command "shell /var/nsinstall/12.1_5-258/build-12.1-55-258_nc_64.tgz" - Status "ERROR: Not authorized to execute this command" 18) 11/03/2021:18:42:54 GMT citrixmpx Debug 0-PPE-5 : default AAA Message 181 0 : " No active policy with accounting Enabled" 19) 11/03/2021:18:43:06 GMT citrixmpx Informational 0-PPE-5 : default CLI CMD_EXECUTED 182 0 : User Test1 - Remote_ip 10.1.2.155 - Command "show audit messages -numOfM esgs 20" - Status "ERROR: Not authorized to execute this command"</pre> |
| FMT_MTD.1/CoreData | None. | None | NA |
| FMT_SMF.1 | All management activities of TSF data. | None | <pre>15) 02/03/2021:16:26:58 GMT Informational 0-PPE-1 : default CONSOLE CMD_EXECUTED 934 0 : User admin - Remote_ip 127.0.0.1 - Command "login admin "*****" - Status "ERROR: Invalid username or password"</pre> |
| FMT_SMR.2 | None | None | NA |
| FPT_SKP_EXT.1 | None | None | NA |
| FPT_APW_EXT.1 | None | None | NA |
| FPT_TST_EXT.1 | None | None | NA |
| FPT_STM_EXT.1 | Discontinuous changes to time - either Administrator actuated or changed via an automated process. | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address). | <pre>6) 09/23/2021:01:32:55 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 191 0 : User nsroot - Remote_ip 192.168.254.155 - Command "shell date" - Status "Success" 7) 09/23/2021:01:33:19 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 193 0 : User nsroot - Remote_ip 192.168.254.155 - Command "shell date 202108151300" - Status "Success" 8) 08/15/2021:13:00:05 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 195 0 : User nsroot - Remote_ip 192.168.254.155 - Command "shell date" - Status "Success"</pre> |
| | (Note that no continuous changes to time need to be logged. See also | | |

| | | | |
|--|---|---|--|
| | application note on FPT_STM_EXT.1) | | |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success or failure) | None | <pre>COLLECTOR::INFOA::Tue Nov 2 22:03:54 2021:Successfully loaded configuration(NS12.1-55.258) root@ns#</pre> <pre>Jan 20 08:16:41 <user.notice> citrixmpx installns: [99339]: Error: Can't find checksum of build ns-12.1-55.258 Jan 20 08:16:41 <user.notice> citrixmpx backforntns: not done (User: test, ip: 10.1.2.171, code: 9951)</pre> |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism | None | <pre>15) 09/23/2021:16:35:19 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 5671 0 : User acumensec - Remote_ip 10.1.2.171 - Command "login acumensec *****" - Status "Success" 16) 09/23/2021:16:35:19 GMT Debug 0-PPE-0 : default AAA Message 5672 0 : " No active policy with accounting Enabled" 17) 09/23/2021:16:36:19 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 5673 0 : User acumensec - Remote_ip 10.1.2.171 - Command "logout" - Status "Success"</pre> |
| FTA_SSL.4 | The termination of an interactive session | None | <pre>13) 02/19/2021:23:49:16 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 1083 0 : User test1 - Remote_ip 127.0.0.1 - Command "login test1 *****" - Status "Success" 14) 02/19/2021:23:49:16 GMT Debug 0-PPE-0 : default AAA Message 1084 0 : " No active policy with accounting Enabled" 15) 02/19/2021:23:50:49 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 1085 0 : User test1 - Remote_ip 127.0.0.1 - Command "logout" - Status "Success"</pre> |
| FTA_SSL_EXT.1 (if "terminate the session" is selected) | The termination of a local session by the session locking mechanism | None | <pre>17) 09/23/2021:16:20:42 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 5640 0 : User acumensec - Remote_ip 127.0.0.1 - Command "login acumensec *****" - Status "Success" 18) 09/23/2021:16:20:42 GMT Debug 0-PPE-0 : default AAA Message 5641 0 : " No active policy with accounting Enabled" 19) 09/23/2021:16:22:42 GMT Informational 0-PPE-0 : default CONSOLE CMD_EXECUTED 5642 0 : User acumensec - Remote_ip 127.0.0.1 - Command "logout" - Status "Success"</pre> |
| FTA_TAB.1 | None | None | NA |
| FTP_ITC.1 | Initiation of the trusted channel | Identification of the initiator and target of failed trusted channels establishment attempt | <pre>16) 07/27/2021:23:53:44 GMT Informational 0-PPE-0 : default AAA Message 904 0 : "In update_aaa_cntr: Succeeded policy for user cctester1 = ldapserver" 17) 07/27/2021:23:53:44 GMT Debug 0-PPE-0 : default AAA Message 905 0 : "rba_server_handler Authentication complete for user cctester1"</pre> <pre>19) 07/27/2021:23:53:44 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 907 0 : User cctester1 - Remote_ip 10.1.2.171 - Command "login cctester1 *****" - Status "Success"</pre> |
| | Termination of the trusted channel | | <pre>10) 07/27/2021:23:57:26 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 269 0 : User cctester1 - Remote_ip 10.1.2.171 - Command "logout" - Status "Success"</pre> |
| | Failure of the trusted channel functions | | <pre>19) 07/27/2021:23:59:45 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 315 0 : User cctester1 - Remote_ip 10.1.2.171 - Command "login cctester1 *****" - Status "ERROR: Invalid username or password"</pre> |

| | | | |
|---------------------|--|------|---|
| FTP_TRP.1 /Admin | <ul style="list-style-type: none"> Initiation of the trusted path | None | <pre> 18) 02/15/2021:01:21:45 GMT Informational 0-PPE-0 : default CLI CMD_EXECUT ED 173 0 : User test1 - Remote_ip 10.1.2.171 - Command "login test1 "***** ***" - Status "Success" 19) 02/15/2021:01:21:48 GMT Informational 0-PPE-0 : default CLI CMD_EXECUT ED 174 0 : User test1 - Remote_ip 10.1.2.171 - Command "logout" - Status " Success" 9) 02/16/2021:23:04:49 GMT Informational 0-PPE-0 : default CLI CMD_EXECUTED 105 0 : U ser test1 - Remote_ip 10.1.2.171 - Command "login test1 "*****" - Status "ERROR: In valid username or password" </pre> |
| | <ul style="list-style-type: none"> Termination of the trusted path. | | |
| | <ul style="list-style-type: none"> Failure of the trusted path functions. | | |

7 Backup Current Configuration

Depending on the type of data to be backed up and the frequency at which you create a backup, you can create a basic backup or a full backup.

- **Basic backup:** Backs up only configuration files. You might want to perform this type of backup frequently, because the files it backs up change constantly. The files that are backed up are:

Directory Sub-Directory of Files

/nsconfig

- ns.conf
- ZebOs.conf
- rc.netscaler
- snmpd.conf
- nsbefore.sh
- nsafter.sh
- monitors

/var/

- download/*
- log/wicmd.log
- wi/tomcat/webapps/*
- we/tomcat/logs/*
- wi/tomcat/conf/catallina/localhost/*
- nslw.bin/etc/krb.conf
- netscaler/locdb/*
- lib/likewise/db/*
- vpn/bookmark/*
- netscaler/crl
- nstemplates/*
- learnt_data/*

/netscaler/

- custom.html
- vsr.htm

- **Full backup:** In addition to the files that are backed up by a basic backup, a full backup backs up some less frequently updated files. The files that are backed up when using the full backup option are:

Directory Sub-Directory or Files

/nsconfig/

- ssl/*
- license/*
- fips/*

/var/

- netscaler/ssl/*
- wi/java_home/jre/lib/security/cacerts/*
- wi/java_home/lib/security/cacerts/*

/nsconfig

- ssh/*
- sshd_config

The backup is stored as a compressed TAR file in the `/var/ns_sys_backup/` directory. To avoid issues due to non-availability of disk space, you can store a maximum of 50 backup files in this directory. You can use the `rm` system backup command to delete existing backup files so that you can create new ones.

Note:

- While the backup operation is in progress, do not execute commands that affect the configuration.
- If a file that is required to be backed up is not available, the operation skips that file.

To back up the ADC appliance by using the ADC command line interface:

At the command prompt, do the following:

1. Save the ADC configurations.

```
save ns config
```

2. Create the backup file.

```
create system backup [<filename>] -level <basic|full> -comment<string>
```

Note: If the file name is not specified, the appliance creates a TAR file with the following naming convention: `backup_<level>_<nsip_address>_<date-timestamp>.tgz`.

Example: The following command backs up the full appliance, using the default naming convention for the backup file.

```
> create system backup -level full
```

3. Verify that the backup file was created.

```
show system backup
```

You can view properties of a specific backup file by including the **fileName** parameter.

8 Reverting to Factory Defaults

You can clear the configuration on your ADC appliance to revert the settings to factory defaults. At the ADC command prompt, type:

```
clear ns config <level>
```

where level is one of the following:

- Basic: Clears everything except NSIP, SNIPs, network settings, HA node definitions, features and mode settings, and the nsroot account.
- Extended: Clears everything except NSIP, SNIPs, network settings, and HA node definitions.
- Full: All settings except the NSIP and default gateway are reset to their factory default values. The NSIP address is left unchanged so that the appliance does not lose network connectivity.

9 References

The following documents were created and evaluated as part of the Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 evaluation:

- Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Security Target [ST] version 1.2
- Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Common Criteria Configuration Guide [AGD] version 1.0