Modern best practices for Citrix ADC implementations

6th October 2021

Contact details

Steven Wright
Email: steven@stevenwright.co.uk
Twitter: https://twitter.com/stevenwrightuk

All feedback gratefully received.

Overview

This draft Tech Paper aims to convey what someone skilled in ADC would configure as a generic implementation and will shortly be submitted to Citrix's TechZone.

> **Note:** As no single configuration will suit all, it is essential to note that a consultant or administrator with better knowledge of your specific needs may deviate from these defaults and record the rationale for such changes in their design documentation.

Table of Contents

        - 7. Configure all of the routes that the ADC will require within System, Network, Routes.
        - 8. Create any Policy Based Routes required.
        - 9. Verify that you can ping each SNIP with MBF disabled or that you understand why you cannot.
        - 10. You have installed a new SSL certificate and key for the management GUI within Traffic Management, SSL, Certificates.
    - Base configuration settings
        - 1. Set the timezone and enable NTP.
        - 2. Create a Key Encryption Key.
        - 3. Set a non-default nsroot password.
        - 4. Add an account for ADM with external authentication disabled.
        - 5. Restrict non-management applications access to the NSIP and only HTTPS access.
        - 6. Set a non-default RPC node password.
        - 7. HA failsafe mode is enabled to ensure the last healthy node continues to provide service.
        - 8. Restrict HA failovers to 3 in 1200 seconds.
        - 9. Disable SSLv3 for management services.
        - 10. Set generic modes and features.
        - 11. Configure one or more DNS nameserver.
        - 12. Set TCP and HTTP parameters.
        - 13. Restrict SNMP queries to select servers.
        - 14. Set SNMP alarms and traps.
        - 15. Set a remote syslog server.
        - 16. You should set a timeout and prompt for management sessions.
        - 17. Centralized authentication for management accounts.
        - 18. Disable LDAP authentication for the nsroot user.
        - 19. TLS/SSL Best practices.

Power and Lights Out management settings

If you have purchased a Citrix ADC appliance, you should ensure:

1. The Citrix ADCs are deployed in locations separate enough to meet your high availaiblity requirements.

2. The redundant Power Supply Units on each ADC (if you have purchased such) are connected to separate electrical supplies.

3. The Lights Out Management card (if you have purchased appliances with such a card) are configured.

You can find more information on configuring Lights Out Management Cards here: https://docs.citrix.com/en-us/citrix-hardware-platforms/mpx/netscaler-mpx-lights-out-management-port-lom.html

Physical network cabling, VLANs, and connectivity

1. All physical interfaces connecting the Citrix ADC to your network(s) should be redundant.

To ensure that data continues to flow during a cable, switch, or interface failure, you should connect your ADC to each network with redundant cables.

To combine the interfaces connecting each network into a single link (known as a channel), you must configure link aggregation on your ADC. Ideally, you should use Link Aggregation Control Protocol (LACP) but, manual aggregated links are possible in the rare event that your network switches do not support LACP.

Instructions for configuring Link Aggregation on your Citrix ADC can be found here: https://docs.citrix.com/en-us/citrix-adc/13/networking/interfaces/configuring-link-aggregation.html

In a virtualised or Cloud environment, your provider will likely have already completed this step for you and is not required.

2. All redundant physical interfaces should be unmonitored for HA within System, Network, Interfaces.

As each network has redundant connections, it is not usually desirable that the ADC initiates an HA failover when a single link fails. Instead, the ADC should continue to provide business services without interruption by using a surviving link and only trigger a failover to the secondary ADC node if all links become unavailable.

To ensure that the ADC does not initiate an HA failover when a single physical interface comprising an aggregated redundant channel fails, you should mark the channel's component interfaces as unmonitored.

To mark an interface as unmonitored, select System, Network, Interfaces. Then, select each interface that will form a part of each redundant channel and set the "HA Monitoring" radio button to "OFF".

In a virtualised or Cloud environment, you will not have physical interfaces and this step is not required as your provider will already have ensured the virtual interfaces presented to the ADC failover correctly.

3. All channels comprising redundant physical interfaces should be monitored for HA within System, Network, Channels.

The failure of all aggregated links connecting the ADC to a particular network will cause the channel representing those links to enter a failed/DOWN state.

By ensuring that the Citrix ADC has HA monitoring enabled for the channel, we ensure that the ADC will initiate an HA failover if all redundant links between the ADC and a network fail.

To mark a channel as monitored, select System, Network, Channels. Then, select each channel and set the "HA Monitoring" radio button to "ON".

4. All channels are bound to a separate VLAN and, you have taken care that no untagged channels are accidentally still in VLAN 1.

Each redundant channel ordinarily represents the aggregate physical links connecting the ADC to a particular logical network.

In a virtualised or Cloud environment, each interface likely represents aggregate physical links with your provider having completed the aggregation work for you.

By default, the ADC considers all interfaces, channels, and IP addresses as being in VLAN 1 and treats these as the same logical network. As such, if you were to overlook VLAN configuration, you would find that each IP address assigned to the ADC was available from every directly-connected network.

To prevent this behaviour, you should configure VLANs on the ADC to represent your logic networks and appropriately isolate traffic.

You can find instructions to create VLANs here: https://docs.citrix.com/en-us/citrix-adc/current-release/networking/interfaces/configuring-vlans.html

5. Create an HA pair between your ADCs within System, High Availability.

You should deploy Citrix ADCs redundantly. You can achieve redundancy by implementing an HA pair of ADCs, creating a cluster of up to thirty-two nodes, or using a technology such as GSLB to split requests between instances. For a generic implementation, Citrix recommends the creation of a two-node HA pair.

You can find instructions for configuring an HA pair here: https://docs.citrix.com/en-us/citrix-adc/current-release/getting-started-with-citrix-adc/configure-ha-first-time.html

6. Create and bind one SNIP to every VLAN, ensuring that each SNIP is in the subnet of the connected network.

Citrix ADC will initiate communication from a Subnet IP (usually called a SNIP) with limited exceptions.

You must create one Subnet IP/SNIP for every directly connected logical network. As you have already isolated each network using VLANs, you must bind each SNIP to its respective VLAN. Please take care to ensure that no VLANs are missing a SNIP.

As each Subnet IP/SNIP includes a netmask, the ADC silently identifies any current or future Virtual IPs (usually called VIPs) within that subnet and attaches these to the same VLAN, thereby isolating vServers to their intended network.

You can find instructions for configuring SNIPs here: https://docs.citrix.com/en-us/citrix-adc/current-release/networking/ip-addressing/configuring-citrix-adc-owned-ip-addresses/configuring-subnet-ip-addresses-snips.html

7. Configure all of the routes that the ADC will require within System, Network, Routes.

If you have connected multiple logical networks, you will likely have routers in each. Therefore, you must now configure all the routes that the ADC will require to reach its clients and backend servers.

Please note that the ADC has a single routing table for all interfaces.

You can find instructions for configuring routes here: https://docs.citrix.com/en-us/citrix-adc/current-release/networking/ip-routing/configuring-static-routes.html

8. Create any Policy Based Routes required.

Occasionally, it is impossible to configure a static route that allows for the behaviour you require.

The most common example is an ADC with separate ingress, egress, and dedicated management networks, and with management clients on the egress network.

Here, static rules would not be sufficient. Instead, you would require a Policy Based Route (PBR) to cause traffic from the ADC's management IP addresses to go via the management router and override the static routing table that would otherwise have sent data to the router in the egress network.

You can find instructions for configuring Policy Based Routes here: https://docs.citrix.com/en-us/citrix-adc/current-release/networking/ip-routing/configuring-policy-based-routes/configuring-policy-based-routes-pbrs-for-ipv4-traffic.html

However, if you have the scenario described above, you need the following PBR:

```
add ns pbr Management ALLOW -srcIP = <NSIP_of_first_HA_node>-
<NSIP_of_second_HA_node> -destIP "!=" <first_IP_management_subnet>-
<last_IP_management_subnet> -nextHop <management_subnet_router> - priority
1
apply pbrs
```

9. Verify that you can ping each SNIP with MBF disabled or that you understand why you cannot.

Citrix ADC has a mode called Mac Based Forwarding (MBF) that causes it to ignore the routing table and instead send replies to the MAC address from which it received the traffic.

MBF is of great use where you cannot define your routes. For example, suppose the ADC has multiple Internet connections and must reply using the Internet router through which traffic arrived. Here, MBF would cause the ADC to record the source MAC address of each connection (the source MAC being that of the Internet router) and would use this as the destination MAC in its reply.

However, having MBF override the routing table can make troubleshooting more complex. With MBF, you cannot understand traffic flows from the ADC's configuration file alone as MBF overrides the routing table, and traffic may not flow as you intended. The result is that MBF, while crucial to some implementations, can also lead to misconfigurations in the supporting network remaining undetected.

To ensure that your routing table and PBRs are correct, you should disable Mac Based Forwarding and verify that each SNIP remains reachable or that you understand why it does not.

The command to disable MBF is

```
disable ns mode mbf
```

The command to enable MBF is

```
enable ns mode mbf
```

If you do not require MBF, you should leave it disabled.

You can find more information of Mac Based Forwarding here: https://support.citrix.com/article/CTX132952

10. You have installed a new SSL certificate and key for the management GUI within Traffic Management, SSL, Certificates.

The Citrix ADC's default SSL certificate is not trusted and will cause your web browser to display a warning message when accessing the ADC's management services.

So that management users do not become accustomed to accepting warning messages that would otherwise already them to a Man In The Middle Attack, Citrix recommends that you replace the default SSL certificate.

You can find details of how to replace the management SSL certificate here: https://support.citrix.com/article/CTX122521

Base configuration settings

1. Set the timezone and enable NTP.

Having accurate and easily understood timestamps in your log files is vital when troubleshooting or handling a security issue.

First, you should set the timezone to something that makes sense to you. For example, if you have any devices logging to a central syslog server and need to cross-reference data from each, you will likely want to use the same timezone as your existing servers.

The command to set the timezone is:

```
set ns param –timezone CoordinatedUniversalTime
```

The command to add NTP servers and enable time synchronization is:

```
add ntp server pool.ntp.org
enable ntp sync
```

You can find details of how to the timezone using the ADC's GUI here: https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/manage-system-settings.html

You can find details of how to add NTP servers here: https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/configure/configure-ntp-server.html

2. Create a Key Encryption Key.

A Key Encryption Key (commonly known as a KEK) is used to encrypt and decrypt credentials that the ADC must store in a reversible form. For example, the ADC must keep its LDAP bind password reversible to retrieve it at authentication time.

The ADC will automatically create a KEK from Citrix ADC firmware 13.0-76.31, and the command below will return an error message that you can safely ignore.

On older releases, you can create a KEK with the command:

```
create kek <RANDOMSTRING>
```

3. Set a non-default nsroot password.

Recent releases of Citrix ADC firmware have the "-forcePasswordChange" system parameter enabled and will prompt you to change the default password for the "nsroot" account when you first log in to the CLI or GUI.

For older releases, you must change the "nsroot" password with the command:

```
set system user nsroot –password <NSROOTPASSWORD>
```

4. Add an account for ADM with external authentication disabled.

Ideally, you will connect all of your Citrix ADCs to ADM for centralised licensing and management. That connection to ADM will require a username and password, which we should now add.

```
add system user admuser <ADMPASSWORD> –externalAuth DISABLED –timeout 900
bind system user admuser superuser 100
set system user admuser –externalAuth DISABLED
```

5. Restrict non-management applications access to the NSIP and only HTTPS access.

We should prevent non-management services from accessing the management IP and set the management IP to require secure communication access (HTTPS rather than HTTP).

```
set ns ip NSIP -restrictAccess enabled -gui SECUREONLY
```

You can find more details on restricting access to the NSIP: https://support.citrix.com/article/CTX126736

6. Set a non-default RPC node password.

You should set RPC communication (used for HA and GSLB) to use a non-default password.

```
set rpcNode <NSIP_OF_SECONDARY_NODE> -password <RPC_SECONDARY_PASSWORD> -
secure YES

set rpcNode <NSIP_OF_PRIMARY_NODE> -password <RPC_PRIMARY_PASSWORD> -
secure YES
```

7. HA failsafe mode is enabled to ensure the last healthy node continues to provide service.

In the unlikely event that both ADCs enter an unhealthy state, by their HA interface or route monitors indicating an error, HA fail-safe mode ensures that the last surviving node will continue attempting to provide business services.

```
set HA node -failSafe ON
```

You can find more details on HA fail-safe mode here: https://docs.citrix.com/en-us/citrix-adc/current-release/system/high-availability-introduction/configuring-fail-safe-high-availability.html

8. Restrict HA failovers to 3 in 1200 seconds.

In the unlikely event that HA failovers repeatedly occur, there will come the point where you wish them to stop and for the ADC to attempt to continue providing business services.

Here, we define a limit of three HA failovers within a 1200 second (20 minutes) period.

```
set ha node -maxFlips 3
set ha node -maxFlipTime 1200
```

9. Disable SSLv3 for management services.

The Citrix ADC management GUI has SSLv3 and TLS1.0 enabled by default. However, to ensure secure communication, you should disable SSLv3.

```
set ssl service nshttps-::1l-443 -ssl3 disabled
set ssl service nshttps-127.0.0.1-443 -ssl3 disabled
```

Depending on your company's internal security policy, you may also wish to disable TLS1.0.

```
set ssl service nshttps-::1l-443 -ssl3 disabled -tls1 disabled
set ssl service nshttps-127.0.0.1-443 -ssl3 disabled -tls1 disabled
```

10. Set generic modes and features.

Citrix ADC has Layer 3 mode enabled by default. Layer 3 mode causes the ADC to act as a router and should usually be disabled.

```
disable ns mode l3 edge
```

You can find more details on Layer 3 mode here: https://docs.citrix.com/en-us/citrix-adc/current-release/getting-started-with-citrix-adc/configure-system-settings/configure-modes-packet-forwarding.html

The specific modes and features that you will need depend on your use case. However, we can select a list of options that would apply to most installations.

```
enable ns feature lb ssl rewrite responder cmp
```

You can find more details about modes and features here: https://support.citrix.com/article/CTX122942

11. Configure one or more DNS nameserver.

The Citrix ADC needs to have access to one or more nameservers for DNS resolution. As the Citrix ADC checks if the DNS servers are online using ICMP, it is usual to implement a local load balancing vServer both to distribute load and to allow DNS based monitoring.

You should configure nameservers using the following commands:

```
add lb vserver DNS DNS 0.0.0.0 0 -persistenceType NONE -cltTimeout 120

add serviceGroup DNSSVG DNS -maxClient 0 -maxReq 0 -cip DISABLED -usip NO
-useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO
bind lb vserver DNS DNSSVG

add lb monitor DNS-monitor DNS -query . -queryType Address -LRTM DISABLED
-interval 6 -resptimeout 3 -downTime 20 -destPort 53
bind serviceGroup DNSSVG -monitorName DNS-monitor

bind serviceGroup DNSSVG <DNSSERVERIP1> 53
bind serviceGroup DNSSVG <DNSSERVERIP2> 53

add dns nameserver DNS
```

12. Set TCP and HTTP parameters.

While Window Scaling (WS) and Selective Acknowledgement (SACK) now default to enabled in ADC 13.0 firmware, you should enable these TCP settings in earlier firmware versions.

```
set ns tcpparam -WS ENABLED
set ns tcpparam -SACK ENABLED
```

Nagle will cause the Citrix ADC to combine data to send a smaller number of larger packets and should be enabled.

```
set ns tcpparam -nagle ENABLED
```

By default, Citrix ADC will forward HTTP requests that arrive at a load balancer but do not conform to the RFC standard. You should configure the ADC to drop invalid requests and allow them on a case by case basis by changing the HTTP options on an individual vServer after discussions with your security team.

Additionally, you should disable support for the HTTP/0.9 protocol, which has been obsolete for over twenty years. For reference, Mosaic 2.0 on Windows 3.1 includes support for HTTP/1.0.

```
set ns httpparam –dropInvalReqs ENABLED –markHttp09Inval ON
```

Cookie version 0 includes absolute timestamps, whereas version 1 cookies have a relative time. If the ADC and client's clock differ, cookies with an absolute timestamp may not expire at the time expected but, those with a relative time giving an expiry of +X minutes will.

Internet Explorer 2 included support for version 1 cookies in 1995, and you should not experience issues by enabling this option.

```
set ns param –cookieversion 1
```

13. Restrict SNMP queries to select servers.

It is good practice that the ADC should only answer SNMP queries from hosts supposed to make such queries. You should limit the hosts that the ADC will allow SNMP queries from using the command:

```
set snmp manager SNMPMANAGERIP
```

You can find more details on configuring SNMP here: https://docs.citrix.com/en-us/citrix-adc/current-release/getting-started-with-citrix-adc/configure-system-settings/configure-snmp.html

14. Set SNMP alarms and traps.

It is usually helpful for the ADC to raise alerts when high CPU or memory usage occurs and send these via SNMP trap configuration to your SNMP server. You can implement such configuration with the following commands:

```
set snmp alarm CPU-USAGE -state ENABLED -normalValue 35 -thresholdValue 95
-logging ENABLED -severity Informational
set snmp alarm MEMORY -state ENABLED -normalValue 35 -thresholdValue 95 -
logging ENABLED -severity Critical

add snmp trap generic SNMPTRAPDSTIP -communityName public
```

15. Set a remote syslog server.

In addition to allowing monitoring platforms to poll the ADC using SNMP, it is generally helpful to configure audit logging via Syslog and direct this to an existing server where the logs can be retained and analysed.

You can configure the Citrix ADC to send audit logs to a remote Syslog server using the following commands:

```
add audit syslogAction RemoteSyslogServerAction SYSLOGSERVERIP -loglevel
ALL
add audit syslogpolicy RemoteSyslogServerPolicy true
RemoteSyslogServerAction
bind audit syslogGlobal -policyName RemoteSyslogServerPolicy -priority 100
```

You can find more details about audit logging here: https://docs.citrix.com/en-us/citrix-adc/current-release/system/audit-logging.html

16. You should set a timeout and prompt for management sessions.

Citrix ADC 13.0 allows a default of 900 seconds (15 minutes) before disconnecting idle management sessions. On older firmware versions, you should ensure that you have configured an appropriate timeout.
set system parameter -timeout 900

As an administrator may have SSH sessions open to multiple ADCs simultaneously, it is helpful to change the ADC's CLI prompt to display their username, the ADC's hostname, and the HA state of the instance.

```
set system parameter -promptString %u@%h-%s
```

17. Centralized authentication for management accounts.

Security teams generally consider it better to control management accounts from a central platform such as Active Directory and grant users permissions with group memberships rather than create accounts on each device.

The usual rationale for centralised authentication and authorisation is that managing accounts on each device is time-consuming and prone to error. Additionally, there is the risk that management users will not change their passwords frequently and that IT may forget to remove ex-employees' accounts.

To configure centralised authentication, you should use the following commands while noting the LDAP filter controlling which users will be able to login.

```
add authentication ldapAction LDAP_mgmt_auth -serverIP
<LDAPMANAGEMENTSERVERIP> -serverPort 636 -ldapBase "
<dc=mycoolcompany,dc=local>" -ldapBindDn "
<serviceaccount@mycoolcompany.local>" -ldapBindDnPassword <LDAPPASSWORD> -
ldapLoginName <sAMAccountName> -searchFilter "&(|
(memberOf:1.2.840.113556.1.4.1941:<cn=Citrix-ADC-
FullAccess,ou=groups,dn=mycoolcompany,dc=local>)
(memberOf:1.2.840.113556.1.4.1941:<cn=Citrix-ADC-
ReadOnly,ou=groups,dn=mycoolcompany,dc=local>))" -groupAttrName memberOf -
subAttributeName cn -secType SSL -passwdChange ENABLED -
nestedGroupExtraction ON -maxNestingLevel 5 -groupNameIdentifier
samAccountName -groupSearchAttribute memberOf -groupSearchSubAttribute CN

add authentication Policy LDAP_mgmt_pol -rule true -action LDAP_mgmt_auth
bind system global LDAP_mgmt_pol -priority 100
```

While the commands above control authentication, they do not control authorization and, by default, the authenticated user will not be able to perform any actions.

To grant the user (or more accurately, the group of which they are a member) the right to perform actions on the ADC, you should use these commands:

```
add system group Citrix-ADC-FullAccess -timeout 900
add system group Citrix-ADC-ReadOnly -timeout 900
bind system group Citrix-ADC-FullAccess -policyName superuser 100
bind system group Citrix-ADC-ReadOnly -policyName read-only 110
```

You can find more information about centralised authentication and authorisation here:
https://support.citrix.com/article/CTX123782

You can also find information about the LDAP filter string used above here:
https://support.citrix.com/article/CTX201948

Further, from ADC firmware version 12.1.51.16 you can configure multi-factor authentication for management users by following the steps here: https://docs.citrix.com/en-us/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/two-factor-authentication-for-system-users-and-external-users.html

18. Disable LDAP authentication for the nsroot user.

As the Citrix ADC processes authentication and authorisation separately, users can authenticate using LDAP, and the ADC will grant permissions based on their group membership.

In the same manner, while it would be bad practice, you could create a list of user accounts with permissions on the ADC and authenticate using the password of an Active Directory user with that exact case sensitive name.

To prevent an Active Directory administrator from creating a "nsroot" user and being able to authenticate, you should disable external authentication for the "nsroot" user account.

```
set system user nsroot -externalAuth DISABLED
```

19. TLS/SSL Best practices.

While not included here to prevent duplication, you should now follow the TLS/SSL Best Practice document to define a secure cipher suite that can be used to protect your vServers.

You can find the TLS/SSL best practice document here: https://docs.citrix.com/en-us/tech-zone/build/tech-papers/networking-tls-best-practices.html