



- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

Scenario: A Citrix Engineer created the policies in the attached exhibit.

Click the Exhibit button to view the list of policies.

Policy name	Priority	Expression	Profile	Goto Expression
Policy_A	100	CLIENT.IP.SRC.IN_SUBNET(192.168.10.0/24)	Policy_A	END
Policy_B	110	HTTP.REQ.HEADER("User-Agent").CONTAINS("Safari")	Policy_B	END
Policy_C	120	HTTP.REQ.URL.PATH.CONTAINS("password")	Policy_C	END
Policy_D	130	true	Policy_D	END

HTTP Request:

GET /resetpassword.htm HTTP/1.1 -

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:64.0) Gecko/20100101 Firefox/64.0

Host: www.citrix.com -

Accept-Language: en-us -

Accept-Encoding: gzip, deflate -

Connection: Keep-Alive -

Which profile will be applied to the above HTTP request?

A. Profile\_C

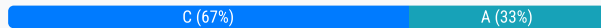
B. Profile\_D

C. Profile\_A

D. Profile\_B

**Suggested Answer: A**

Community vote distribution



**diskman** Highly Voted 3 years, 2 months ago

Choice A (Profile C) is correct since the http request header matches the policy C expression then hit it (neither policy A or B are mismatched).  
upvoted 6 times

**3a0f5fb** Most Recent 1 year, 3 months ago

**Selected Answer: A**

Policy\_C

upvoted 1 times

**dante\_2k5** 2 years, 5 months ago

Profile C

upvoted 1 times

**flabiola** 2 years, 10 months ago

**Selected Answer: C**



Profile C

upvoted 2 times

How can a Citrix Engineer monitor the Citrix ADC appliances to check that all SSL certificates have a key strength of at least 2048 bits from the SSL Dashboard Settings?

- A. Delete 512, 1024, and 4096 on the Enterprise Policy tab.
- B. Delete 512 and 1024 on the Enterprise Policy tab.
- C. Select 2048 and 4096 on the Enterprise Policy tab.
- D. Select 2048 on the Enterprise Policy tab.

**Suggested Answer:** C

  **Mr\_Marcus** 1 year, 3 months ago

Correct answer is C. Reference: <https://docs.citrix.com/en-us/citrix-application-delivery-management-service/networks/ssl-certificate-dashboard/how-to-configure-enterprise-policy.html>

upvoted 1 times

Scenario: A Citrix Engineer notices that a web page takes a long time to display. Upon further investigation, the engineer determines that the requested page consists of a table of high-resolution pictures which are being displayed in table cells measuring 320 by 180 pixels. Which Front End Optimization technique can the engineer enable on the Citrix ADC to improve time to display?

- A. Shrink to Attributes
- B. Make Inline
- C. Extend Page Cache
- D. Minify

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗨️ 👤 **Mr\_Marcus** 1 year, 3 months ago

**Selected Answer: A**

Correct answer is really Image Optimization, which includes Image Shrink-to Attributes. <https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html>

upvoted 1 times

A Web Application Engineer is reviewing log files and finds that a large number of bad HTTP requests are being sent to the web application servers.

What can the Citrix ADC Engineer do to prevent bad HTTP requests from getting to the web application?

- A. Create an HTTP profile and select 'Drop invalid HTTP requests'.  
Assign the HTTP profile to the virtual server.
- B. Create an HTTP profile and select 'Drop invalid HTTP requests'.  
Assign the HTTP profile to the Web App Firewall policy.
- C. Modify the default HTTP profile and select 'Drop invalid HTTP requests'.  
Bind the default HTTP profile globally.
- D. Select 'Change HTTP Parameters' under System > Settings.  
Select 'Drop invalid HTTP requests'.

**Suggested Answer: D**

*Community vote distribution*

D (100%)

🗳️ 👤 **thedelph** 1 year, 1 month ago

**Selected Answer: D**

with it saying web application servers (i.e. plural), applying this at a global level may be the way to go.  
upvoted 1 times

🗳️ 👤 **lexmen** 1 year, 2 months ago

I'm agree with bengie but the aswer D is more specific A is to global level  
upvoted 1 times

🗳️ 👤 **Rink76** 1 year, 4 months ago

**Selected Answer: D**

<https://support.citrix.com/article/CTX227979/faq-strict-http-validation-on-netScaler-application-delivery-controller-and-netScaler-gateway>  
upvoted 1 times

🗳️ 👤 **bengie** 1 year, 9 months ago

A or D should both work  
upvoted 1 times

🗳️ 👤 **Mr\_Marcus** 1 year, 9 months ago

**Selected Answer: D**

Reference - <https://www.carlstalhood.com/system-configuration-citrix-adc-13/#profiles>  
upvoted 1 times

Which syntax is used to write a StyleBook?

- A. JSON
- B. LISP
- C. YAML
- D. XML

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗳️ 👤 **bengie** 1 year, 3 months ago

**Selected Answer: C**

YAML is correct

upvoted 1 times

🗳️ 👤 **Rafateka** 1 year, 5 months ago

**Selected Answer: C**

StyleBooks use a declarative syntax, written in YAML, components of a StyleBook can be specified in any order

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/stylebooks.html>

upvoted 1 times

🗳️ 👤 **JandroFR** 1 year, 5 months ago

**Selected Answer: C**

Correct answer, C: YAML

upvoted 2 times



Scenario: A Citrix Engineer wants to protect a web application using Citrix Web App Firewall. After the Web App Firewall policy afweb\_protect is bound to the virtual server, the engineer notices that pages are displaying in plain text with graphics included. What is the likely cause of this?

- A. The Safe Objects protection is NOT properly configured.
- B. The Start URL list does NOT include CSS files.
- C. The Web App Firewall feature is disabled.
- D. The policy expression allows for HTML files only.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **bengie** 1 year, 3 months ago

**Selected Answer: B**

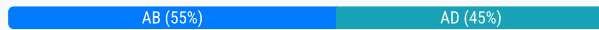
If the Design is missing it is likely that the css is missing  
upvoted 2 times

Which two protections ensure that the correct data is returned by the client? (Choose two.)

- A. Form Field Consistency.
- B. Field Formats
- C. HTML Cross-Site Scripting (XSS)
- D. Cross-Site Request Forgeries (CSRF)

**Suggested Answer:** AB

Community vote distribution



**kirshad** 3 weeks, 5 days ago

**Selected Answer:** AB

Form Field Consistency and Formats are correct answers

upvoted 1 times

**3a0f5fb** 1 year, 3 months ago

**Selected Answer:** AB

A. Form Field Consistency: This ensures that the data submitted by the client matches the expected format and values, preventing tampering or manipulation of form fields.

B. Field Formats: This involves validating that the data conforms to the expected format, such as ensuring email addresses are correctly formatted or dates are in the proper format.

upvoted 1 times

**thedelfh** 2 years, 1 month ago

A. Form Field Consistency - This ensures that the client has not altered the structure of the web forms and that data submitted adheres to HTML restrictions for length and type.

B. Field Formats - This validates the type and length of user-submitted data in web forms to ensure they are appropriate for the intended fields.

upvoted 2 times

**thedelfh** 2 years, 1 month ago

**Selected Answer:** AB

The question is asking about data returned by the client. XSS and CSRF are with regard to preventing malicious data from being sent to the server rather than ensuring the correct data is returned by the client.

upvoted 2 times

**RVR** 2 years, 5 months ago

**Selected Answer:** AD

A & D are fine

CSRF meaning CSRF form tagging check (<https://docs.netScaler.com/en-us/citrix-adc/current-release/application-firewall/form-protections/cross-site-request-forgery-check.html>) where data from web forms returned by users are checked.

upvoted 4 times

**bengie** 2 years, 9 months ago

**Selected Answer:** AB

A and B check the form of the input

upvoted 2 times

**Mr\_Marcus** 2 years, 9 months ago

**Selected Answer:** AD

Reference - <https://docs.citrix.com/en-us/citrix-adc-secure-deployment.html> See "Third Tier of Security."

upvoted 1 times

**Binomimus** 3 years ago



B (Field Formats) should also be correct, since it validates users' forms input as well

Field Formats: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/form-protections/field-formats-check.html>

Form Field Consistency Check: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/form-protections/form-field-consistency-check.html>

CSRF: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/form-protections/cross-site-request-forgery-check.html>

upvoted 1 times

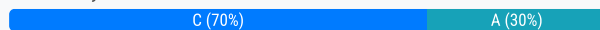
Scenario: A Citrix Engineer is asked to implement multi-factor authentication for Citrix Gateway. The engineer creates the authentication policies and binds the policies to the appropriate bind points. The engineer creates a custom form using Notepad++ to format the page which will capture the user's credentials.

To which folder on the Citrix ADC will the engineer need to upload this form?

- A. /flash/nsconfig/loginschema/LoginSchema
- B. /var/netscaler
- C. /flash/nsconfig/loginschema
- D. /var

**Suggested Answer: C**

Community vote distribution



🗨️ 👤 **kirshad** 3 weeks, 5 days ago

**Selected Answer: A**

nsconfig/loginschema/LoginSchema correct folder  
upvoted 1 times

🗨️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: A**

of course nsconfig/loginschema/LoginSchema  
upvoted 2 times

🗨️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: C**

If the engineer creates a custom form for multi-factor authentication, they would need to upload the XML scheme that describes this form to the /nsconfig/loginschema/LoginSchema directory on the Citrix NetScaler.  
upvoted 1 times

🗨️ 👤 **bengie** 2 years, 9 months ago

**Selected Answer: C**

as JandroFR writes C should be correct. <https://docs.citrix.com/de-de/citrix-adc/current-release/aaa-tm/authentication-methods/multi-factor-nfactor-authentication/nfactor-extensibility.html>  
upvoted 3 times

🗨️ 👤 **Mr\_Marcus** 2 years, 9 months ago

<https://www.carlstalhood.com/system-configuration-citrix-adc-13/#mgmttwofactor>  
upvoted 1 times

🗨️ 👤 **JandroFR** 2 years, 11 months ago

**Selected Answer: C**

I think that should be C. Built-in schema files are stored in /nsconfig/loginschema/LoginSchema, but when editing one to create a custom schema, the new one is automatically saved to the upper folder: /nsconfig/loginschema.  
Therefore, built-in schema files are in /nsconfig/loginschema/LoginSchema, and custom schema files go into /nsconfig/loginschema  
upvoted 3 times

Scenario: A Citrix Engineer used Learning to establish the HTML SQL Injection relaxations for a critical web application. The engineer now wishes to begin working on the protections for a different web application. The name of the Web App Profile is appfw\_prof\_customercare. Which CLI command can the engineer use to empty the Learn database?

- A. set appfw learningsettings appfw\_prof\_customercare -SQLInjectionMinThreshold 0
- B. set appfw learningsettings appfw\_prof\_customercare -startURLMinThreshold 0
- C. reset appfw learningdata
- D. export appfw learningdata appfw\_prof\_customercare

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗲️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: C**

reset appfw learningdata

Remove all databases. Make transaction count zero

<https://docs.netScaler.com/en-us/citrix-adc/current-release/application-firewall/profiles/learning.html>

upvoted 1 times

🗲️ 👤 **Rafateka** 2 years, 11 months ago

**Selected Answer: C**

<https://developer-docs.citrix.com/projects/netScaler-command-reference/en/12.0/appfw/appfw-learningdata/appfw-learningdata/#reset-appfw-learningdata>

upvoted 4 times

Which Citrix Application Delivery Management (ADM) Analytics page allows a Citrix Engineer to monitor web application traffic?

- A. Web Insight
- B. WAN Insight
- C. HDX Insight
- D. Gateway Insight

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: A**

The correct Citrix Application Delivery Management (ADM) Analytics page that allows a Citrix Engineer to monitor web application traffic is: A. Web Insight

<https://docs.netScaler.com/en-us/netScaler-console-service/analytics.html>

upvoted 1 times

🗳️ 👤 **bengie** 2 years, 8 months ago

**Selected Answer: A**

A is correct, HDX insight is only for HDX

upvoted 2 times

🗳️ 👤 **flabiolo** 2 years, 10 months ago

**Selected Answer: A**

Web Insight

upvoted 2 times

🗳️ 👤 **Rafateka** 2 years, 11 months ago

**Selected Answer: A**

"The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and Citrix ADC instances."

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/application-analytics-and-management/web-insight.html>

upvoted 2 times

🗳️ 👤 **Binomimus** 3 years ago

**Selected Answer: A**

"The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and Citrix ADC instances."

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/application-analytics-and-management/web-insight.html>

upvoted 3 times

🗳️ 👤 **diskman** 3 years, 2 months ago

I think A should be correct rather than C, web application should involve web insight instead of hdx insight

upvoted 3 times

Which report can a Citrix Engineer review to ensure that the Citrix ADC meets all PCI-DSS requirements.

- A. Generate Application Firewall Configuration
- B. PCI-DSS Standards
- C. Application Firewall Violations Summary
- D. Generate PCI-DSS

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer:** D

Correct answer: D

upvoted 1 times

🗨️ 👤 **JandroFR** 2 years, 11 months ago

**Selected Answer:** D

Correct answer: D - <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/stats-and-reports.html>

upvoted 4 times

Scenario: A Citrix Engineer manages Citrix Application Delivery Management (ADM) for a large holding company. Each division maintains its own ADC appliances. The engineer wants to make Citrix ADM features and benefits available to each group independently. What can the engineer create for each division to achieve this?


- A. A site
- B. A role
- C. A tenant
- D. A dashboard
- E. A group

**Suggested Answer: A**

Community vote distribution


C (67%)

E (33%)

  **d6294d0** 1 year, 5 months ago

**Selected Answer: C**

"Multitenancy is no longer supported for ADM on-premises and service deployments." No tenant has visibility into the instances and applications of the other tenants. Only the system admin has visibility into all instances, applications, and reports of all tenants. <https://docs.netScaler.com/en-us/netScaler-application-delivery-management-software/current-release/access-control/multi-tenancy.html>  
upvoted 2 times

  **thedelph** 1 year, 7 months ago

Having said that, "Multitenancy is no longer supported for ADM on-premises and service deployments."  
upvoted 1 times

  **thedelph** 1 year, 7 months ago

<https://docs.netScaler.com/en-us/citrix-application-delivery-management-software/current-release/access-control/multi-tenancy.html>  
upvoted 1 times

  **thedelph** 1 year, 7 months ago

**Selected Answer: C**

While roles (B) and groups (E) are important for defining access within Citrix ADM, it is the tenant (C) feature that enables the Citrix Engineer to provide a completely exclusive management environment to each division. Multitenancy allows each division to operate independently within the ADM platform, which is precisely the engineer's goal.  
upvoted 2 times

  **CoreyHawk** 2 years, 4 months ago

I would say group: <https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/access-control/role-based-access-control/rbac-configuring-groups.html>  
upvoted 2 times

  **Binomimus** 2 years, 6 months ago

**Selected Answer: E**

Should be E: a group

"In Citrix ADM, a group can have both feature-level and resource-level access. For example, one group of users might have access to only selected Citrix ADC instances; another group with only a selected few applications, and so on."  
<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/setting-up/configuring-role-based-access-control.html>  
upvoted 2 times

  **Binomimus** 2 years, 6 months ago

Since the question already talks about existing groups, those groups must be assigned roles: B  
upvoted 1 times

  **diskman** 2 years, 8 months ago

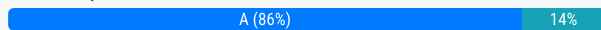
Should be C: A tenant that involves multi-tenancy solution provisioned by ADM  
upvoted 3 times

Scenario: During application troubleshooting, a Citrix Engineer notices that response traffic received from a protected web application is NOT matching what the web server is sending out. The engineer is concerned that someone is trying to disrupt caching behavior. Which action is the Citrix Web App Firewall performing that would trigger this false positive?

- A. Removing the Last-Modified header
- B. Inserting a hidden form field
- C. Removing the Accept-Encoding header
- D. Modifying and adding cookies in the response

**Suggested Answer: A**

Community vote distribution



🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: A**

A. Removing the Last-Modified header

Removing the Last-Modified header can disrupt caching behavior, as this header is used by browsers and proxies to determine if the content has changed since it was last cached. This can lead to discrepancies between what the web server sends and what the client receives.

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: A**

Changing my answer to A:

A. Removing the Last-Modified header.

This action can affect the caching behavior because the "Last-Modified" header is used by caches to understand if the content has changed since the last time it was retrieved. If the Web App Firewall removes this header, it can disrupt the caching mechanism, leading to a false positive regarding caching behavior.

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: C**

why not C?

The documentation (<https://docs.netScaler.com/en-us/citrix-adc/13-1/application-firewall/introduction-to-citrix-web-app-firewall>) refers to the Accept-Encoding header being dropped but doesn't list "Last-Modified" but rather "If-Modified-Since" header.

upvoted 1 times

🗳️ 👤 **bengie** 2 years, 8 months ago

**Selected Answer: A**

without Header pages get wrongly cached; should be A

upvoted 2 times

🗳️ 👤 **Binomimus** 3 years ago

**Selected Answer: A**

Please ignore my previous comment, A makes more sense in this case, same article: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html>

upvoted 2 times

🗳️ 👤 **Guntrrr** 3 years, 1 month ago

Should be A

upvoted 3 times

Scenario: A Citrix Engineer configures Citrix Web App Firewall to protect an application. Users report that they are NOT able to log on. The engineer enables a Start URL relaxation for the path //login.aspx.  
What is the effect of the Start URL relaxation on the application?

- A. Access to the path /login.aspx is unblocked.
- B. Access to the path /login.aspx is blocked.
- C. External users are blocked from the path /login.aspx.  
Internal users are permitted to the path /login.aspx.
- D. Non-administrative users are blocked from the path /login.aspx.  
Administrative users are permitted to the path /login.aspx.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: A**

A. Access to the path /login.aspx is unblocked.  
upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: A**

This is the correct answer. The Start URL check is designed to block connections if the URL does not meet the specified criteria, which includes matching an entry in the Start URL list. By adding a relaxation for //login.aspx, the Citrix Engineer is allowing this URL to be accessed, which would enable users to reach the login page that they were previously unable to access due to the firewall's restrictions.  
upvoted 1 times

🗳️ 👤 **Rink76** 2 years, 4 months ago

**Selected Answer: A**

<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/url-protections/starturl-check.html>  
upvoted 1 times



Which setting in the Cookie Consistency protection feature does a Citrix Engineer need to configure to ensure that all a cookie is sent using TLS only?

- A. Encrypt Server Cookies > Encrypt All
- B. Flags to Add in Cookies > Secure
- C. Encrypt Server Cookies > Encrypt Session Only
- D. Proxy Server Cookies > Session Only

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: B**

Flags to Add in Cookies > Secure: Add the Secure flag to cookies that are to be sent only over an SSL connection. Browsers that support the Secure flag do not send the flagged cookies over an insecure connection.

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: B**

When the Secure flag is set, browsers that support this flag will not send the flagged cookies over an insecure connection.

upvoted 1 times

🗳️ 👤 **Rink76** 2 years, 4 months ago

**Selected Answer: B**

Secure. Add the Secure flag to cookies that are to be sent only over an SSL connection. Browsers that support the Secure flag do not send the flagged cookies over an insecure connection.

upvoted 1 times

🗳️ 👤 **CoreyHawk** 2 years, 10 months ago

I stand corrected; I'd say A now

upvoted 1 times

🗳️ 👤 **CoreyHawk** 2 years, 10 months ago

B: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/cookie-protection/cookie-consistency-check.html>

upvoted 2 times

Which security model should a Citrix Engineer implement to make sure that no known attack patterns pass through Citrix Web App Firewall?

- A. Hybrid
- B. Static
- C. Positive
- D. Negative

**Suggested Answer:** D

Community vote distribution

D (78%)

C (22%)

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

The negative security model, also known as the signature-based model, is designed to block known attack patterns by using predefined signatures and rules. This model is effective in identifying and preventing known threats.

upvoted 1 times

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: D**

To ensure that no known attack patterns pass through Citrix Web App Firewall, a Citrix Engineer should implement the:

D. Negative security model

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: D**

The Negative security model is designed to block known vulnerabilities and attack patterns based on a database of signatures, which makes it suitable for this particular requirement.

upvoted 1 times

🗳️ 👤 **Rink76** 2 years, 4 months ago

**Selected Answer: D**

<https://docs.citrix.com/en-us/tech-zone/learn/poc-guides/citrix-waf-deployment.html>

The negative security model employs vulnerability signatures to prevent known attacks.

upvoted 2 times

🗳️ 👤 **bengie** 2 years, 8 months ago

**Selected Answer: D**

D negative security model; keyword is "known"

upvoted 3 times

🗳️ 👤 **bengie** 2 years, 8 months ago

D negative security model; keyword is "known"

upvoted 2 times

🗳️ 👤 **CoreyHawk** 2 years, 10 months ago

Correction; should be D: Negative; Negative security model uses a rich set signatures to protect against L7 and HTTP application vulnerabilities. That is, looking for patterns in known attacks, which is what the signature update does.

upvoted 3 times

🗳️ 👤 **Binomimus** 3 years ago

**Selected Answer: C**

C: Positive

<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/deploymentguide.html>

upvoted 2 times

Scenario: A Citrix Engineer has configured Integrated Caching to improve application performance. Within hours, the Citrix ADC appliance has run out of memory.

Which Content Group setting can the engineer configure to show the caching process until a need is demonstrated?

- A. Maximum memory usage limit
- B. Quick Abort Size
- C. Do not cache – if hits are less than
- D. Do not cache – if size exceeds

**Suggested Answer: A**

*Community vote distribution*



🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: A**

A

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: C**

This setting directly addresses the issue of caching objects based on demonstrated need. By setting a minimum number of hits before an object is cached, the cache will only store items that are frequently requested, which helps to conserve memory and could prevent the out-of-memory issue. However, this does not address the immediate problem of the cache having already run out of memory.

upvoted 1 times

🗳️ 👤 **ShowMe** 2 years, 7 months ago

C: <https://docs.netScaler.com/en-us/citrix-adc/current-release/optimization/integrated-caching/improve-cache-performance.html#requiring-a-minimum-number-of-server-hits-before-caching>

upvoted 2 times

🗳️ 👤 **CoreyHawk** 2 years, 10 months ago

Changing it to C: <https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/integrated-caching/improve-cache-performance.html>

upvoted 4 times

🗳️ 👤 **CoreyHawk** 2 years, 10 months ago

A: <https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/integrated-caching.html>

upvoted 1 times

A Citrix Engineer reviews the App Dashboard and notices that three of the monitored applications have an App Score of less than 50. The engineer can interpret the App Score as a metric of application \_\_\_\_\_. (Choose the correct option to complete the sentence.)

- A. security, with a lower score indicating better security
- B. performance and availability, with a higher score indicating better health
- C. performance and availability, with a lower score indicating better health
- D. security, with a higher score indicating better security

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: B**

B. performance and availability, with a higher score indicating better health  
upvoted 1 times

🗳️ 👤 **thedelfh** 2 years, 1 month ago

**Selected Answer: B**

A score between 0 and <40 is considered critical, between 40 and <75 is fair, and a score greater than 75 is good. Thus, a higher app score reflects better performance and availability of the monitored applications.  
upvoted 1 times

🗳️ 👤 **Rink76** 2 years, 4 months ago

**Selected Answer: B**

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/application-analytics-and-management/dashboard/application-management.html>  
upvoted 1 times

🗳️ 👤 **CoreyHawk** 2 years, 10 months ago

B: <https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/application-analytics-and-management/dashboard/application-management.html>  
upvoted 1 times



Which Front End Optimization technique causes the Citrix ADC to resize images before sending them to the client?

- A. Minify
- B. Shrink to Attributes
- C. Compression
- D. Inlining

**Suggested Answer:** B

*Community vote distribution*

B (100%)

  **Rink76** 1 year, 4 months ago

**Selected Answer:** B

<https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html>

upvoted 1 times

  **CoreyHawk** 1 year, 11 months ago

B: <https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html>

upvoted 1 times

A review of purchases made at an online retailer shows that several orders were processed for items at an unpublished price.

Which protection can a Citrix Engineer implement to prevent a site visitor from modifying the unit price of a product on the shopping cart page?

- A. Cross-Site Request Forgeries (CSRF)
- B. Form Field Consistency
- C. HTML Cross-Site Scripting (XSS)
- D. HTML SQL Injection

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗲️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: B**

B. Form Field Consistency

upvoted 1 times

🗲️ 👤 **Rink76** 2 years, 4 months ago

**Selected Answer: B**

<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/form-protections/form-field-consistency-check.html>

upvoted 1 times

🗲️ 👤 **CoreyHawk** 2 years, 10 months ago

B: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/form-protections/form-field-consistency-check.html>

upvoted 1 times

Scenario: A Citrix Engineer configures Citrix Web App Firewall to protect an application. Upon reviewing the log files, the engineer notices a pattern of forceful browsing toward the configuration page for the application. To protect against this, the engineer enforces Start URL and enables Enforce URL Closure.

What is the effect of enforcing Start URL and enabling Enforce URL Closure on the application?

- A. Access to the path /config.aspx is unblocked when a user clicks a referring link elsewhere on the website.
- B. Non-administrative users are blocked from the path /config.aspx.  
Administrative users are permitted to the path /config.aspx.
- C. External users are blocked from the path /config.aspx.  
Internal users are permitted to the path /config.aspx.
- D. Access to the path /config.aspx is blocked.

**Suggested Answer: A**

*Community vote distribution*

A (100%)


 **thedelph** 1 year, 1 month ago

**Selected Answer: A**

A. Access to the path /config.aspx is unblocked when a user clicks a referring link elsewhere on the website.

This is because Enforce URL Closure allows users to access any webpage on the website by clicking a hyperlink on any other page on the website, as long as the URL is configured as a Start URL. If /config.aspx is a Start URL and the user navigates there by clicking a link within the site, they will be allowed access. If it is not a Start URL, even navigating there by clicking a link within the site would be blocked.


upvoted 1 times

 **ShowMe** 1 year, 7 months ago

**Selected Answer: A**


A: Access to the URL is blocked (D) when browsing forcefully. But, if you click on a link from a valid web page, access is allowed (A).

upvoted 1 times

 **bengie** 1 year, 8 months ago

D and A are both correct, I think

upvoted 1 times

 **oztech** 1 year, 11 months ago

**Selected Answer: A**

Agree, it's A

upvoted 1 times

 **Binomimus** 2 years ago

**Selected Answer: A**

i agree, it's A

<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/url-protections/starturl-check.html>

Enforce URL Closure. Allow users to access any web page on your website by clicking a hyperlink on any other page on your website.

upvoted 3 times

 **achen** 2 years, 1 month ago

it should be A

upvoted 3 times

A Citrix Engineer needs to set up access to an internal application for external partners.  
Which two entities must the engineer configure on the Citrix ADC to support this? (Choose two.)

- A. SAML Policy
- B. SAML IdP Profile
- C. SAML IdP Policy
- D. SAML Action

**Suggested Answer:** AD

Community vote distribution

AD (100%)

🗲️ 👤 **diskman** Highly Voted 3 years, 2 months ago

Should be A and D to act ADC as a SAML SP (Service Provider) that redirects the requests from external users to an SAML IDP to do authentication prior to authorizing them applying the internal services

upvoted 7 times

🗲️ 👤 **3a0f5fb** Most Recent 1 year, 3 months ago

**Selected Answer:** AD

- A. SAML Policy
- D. SAML Action

upvoted 1 times

🗲️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer:** AD

A. SAML Policy - This is needed to apply the SAML action to all traffic.

D. SAML Action - This is required to define the behavior of the NetScaler when it redirects unauthenticated user requests and processes SAML assertions from the IdP.

upvoted 1 times

🗲️ 👤 **Binomimus** 3 years ago

**Selected Answer:** AD

I agree A and D

<https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm/authentication-methods/saml-authentication/citrix-adc-saml-sp.html>

upvoted 4 times



Scenario: A Citrix Engineer implements Application-level Quality of Experience (AppQoE) to protect a web application. The engineer configures the AppQoE action to deliver a custom response from a backup server once the maximum number of concurrent connection is reached. To achieve this, the engineer should set the Action Type to \_\_\_\_\_ and specify the \_\_\_\_\_. (Choose the correct option to complete the sentence.)

- A. NS; Alternate Content Server Name
- B. ACS; Custom File
- C. ACS; Alternate Content Server Name
- D. NS; Custom File


**Suggested Answer:** C

Community vote distribution

C (100%)

 **Guntrrr** Highly Voted 2 years, 1 month ago

Should be C - question specifies response comes from a backup server, not the NS itself  
upvoted 6 times

 **thedelph** Most Recent 1 year, 1 month ago

**Selected Answer: C**

C. ACS; Alternate Content Server Name

In the context of Citrix NetScaler's Application-level Quality of Experience (AppQoE), ACS stands for "Alternate Content Service", which is used to specify an action that serves alternate content from a different server when certain conditions are met (like reaching the maximum number of concurrent connections). The "Alternate Content Server Name" would be the specification of the backup server from which the custom response is delivered.

upvoted 1 times

 **Binomimus** 2 years ago

**Selected Answer: C**

I agree, it's C

upvoted 3 times

Scenario: A Citrix Engineer wants to configure the Citrix ADC for OAuth authentication. The engineer uploads the required certificates, configure the actions, and creates all the necessary policies. After binding the authentication policy to the application, the engineer is unable to authenticate.

What is the most likely cause of this failure?

- A. The log files are full.
- B. The Redirect URL is incorrect.
- C. The certificates have expired.
- D. The policy bindings were assigned incorrect priorities.

**Suggested Answer: B**

Community vote distribution

B (67%)

D (33%)


  **diskman**  2 years, 8 months ago

Should be B: incorrect redirect URL that fails user authentication, whereas incorrect policy binding priority value doesn't cause this kind of failure  
upvoted 5 times

  **caioninaut**  1 year, 6 months ago



**Selected Answer: B**

B. The Redirect URL is part of OAuth Configuration profile, and If isn't correctly configured the auth will fail.  
upvoted 1 times

  **thedelph** 1 year, 7 months ago

**Selected Answer: B**

B. The Redirect URL is incorrect: The Redirect URL is a critical component in the OAuth flow. It's where the authorization server sends the user after they have approved the application. If this URL is not correctly configured to match the application's expected URL, the authorization process will fail.  
upvoted 2 times

  **lexmen** 1 year, 8 months ago

**Selected Answer: B**

B is the most likely I agree with diskman  
upvoted 1 times

  **ShowMe** 2 years, 1 month ago

**Selected Answer: D**

D is most likely. The question gives the impression that the engineer is able to enter credentials but authentication fails. So the logon form was displayed.

Log files being full isn't a reason for authentication to stop.

It's not an incorrect URL otherwise an authentication attempt won't happen in the first place.

Certificates possibly, but this may have presented differently than unable to authenticate.

Incorrect bindings seem most likely since the engineer is presented with the option to authenticate, but no policy is hit to allow the process to succeed.

upvoted 2 times

  **Citrix\_Guru** 1 year, 1 month ago

If bindings were incorrect, he wouldn't hit that policy in the first place. Although the question in general is silly, I would lean towards B.  
upvoted 1 times

What is required for connecting a data center to the Citrix Application Delivery Management (ADM) Service?

- A. Instance
- B. Configuration Job
- C. Agent
- D. Syslog

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗳️ 👤 **thedelfh** 1 year, 1 month ago

**Selected Answer: C**

NetScaler ADM is available as a service on the Citrix Cloud.

After signing up for Citrix Cloud and starting the service, you install agents in your network environment or initiate the built-in agent in the instances. An agent enables communication between the NetScaler ADM and the managed instances in your data center, collecting data from the managed instances and sending it to NetScaler ADM.

upvoted 1 times

🗳️ 👤 **robholgate** 1 year, 4 months ago

**Selected Answer: C**

An agent enables communication between the NetScaler ADM and the managed instances in your data center. The agent collects data from the managed instances in your network and sends it to the NetScaler ADM.

upvoted 1 times

🗳️ 👤 **RVR** 1 year, 7 months ago

Its a citrix cloud question, <https://docs.netScaler.com/en-us/citrix-application-delivery-management-service/overview.html> "After you sign up for Citrix Cloud and start using the service, install agents in your network environment or initiate the built-in agent in the instances. Then, add the instances you want to manage to the service."

upvoted 2 times

🗳️ 👤 **fabbe81** 1 year, 9 months ago

**Selected Answer: C**

The agent works as an intermediary between the Citrix ADM and the discovered instances in the data center.

upvoted 2 times

A Citrix Engineer needs to create a configuration job to clone a configuration from an existing Citrix ADC to a new Citrix ADC.  
Which configuration source can the engineer use to accomplish this?

- A. Master Configuration
- B. Inbuilt Template
- C. Instance
- D. Configuration Template

**Suggested Answer: C**

*Community vote distribution*

C (100%)

 **diskman** Highly Voted 1 year, 8 months ago

Should be C: instance

<https://docs.citrix.com/en-us/citrix-application-delivery-management-software/13/networks/configuration-jobs/replicate-configuration.html>

upvoted 6 times

 **Binomimus** Most Recent 1 year, 6 months ago

**Selected Answer: C**

I agree C: instance

<https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/networks/configuration-jobs/replicate-configuration.html>

upvoted 4 times

Scenario: A Citrix Engineer is asked to help improve the performance of a web application. After capturing and analyzing a typical session, the engineer notices a large number of user requests for the stock price of the company.

Which action can the engineer take to improve web application performance for the stock quote?

- A. Enable the Combine CSS optimization.
- B. Create a static content group.
- C. Create a dynamic content group.
- D. Enable the Minify JavaScript optimization.

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗲️ 👤 **diskman** Highly Voted 2 years, 2 months ago

Should be C: create a dynamic content group  
upvoted 8 times

🗲️ 👤 **Binomimus** Highly Voted 2 years ago

**Selected Answer: C**

I agree C: dynamic content group  
<https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/integrated-caching/configure-selectors-basic-content-groups.html#content-groups>  
upvoted 5 times

🗲️ 👤 **thedelph** Most Recent 1 year, 1 month ago

**Selected Answer: C**

A. Enable the Combine CSS optimization: This approach combines multiple CSS files into one to reduce requests, which is beneficial for static content optimization but not directly useful for dynamic content like stock prices.

B. Create a static content group: Static content groups are used for content that does not change often, which does not apply to stock prices that frequently update.

C. Create a dynamic content group: Dynamic content groups are designed for content that is frequently updated. This would allow the engineer to cache the stock price data temporarily, serving it quickly to multiple users without repeatedly querying the backend systems, thus improving the performance for this particular content.

D. Enable the Minify JavaScript optimization: Minifying JavaScript optimizes the size of JavaScript files but does not affect the server-side performance related to dynamic content fetching like stock prices.

upvoted 2 times

Which Citrix Application Delivery Management (ADM) Analytics page allows a Citrix Engineer to monitor the metrics of the optimization techniques and congestion control strategies used in Citrix ADC appliances?

- A. Gateway Insight
- B. TCP Insight
- C. HDX Insight
- D. Web Insight

**Suggested Answer: B**

Community vote distribution

B (100%)

Binomimus Highly Voted 3 years ago

**Selected Answer: B**

B TCP Insight

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/analytics/tcp-insight.html>

upvoted 6 times

3a0f5fb Most Recent 1 year, 3 months ago

B. TCP Insight

<https://docs.netScaler.com/de-de/netScaler-application-delivery-management-software/current-release/analytics/tcp-insight.html>

upvoted 1 times

thedelph 2 years, 1 month ago

**Selected Answer: B**

B. TCP Insight

This is the page within Citrix ADM Analytics that allows a Citrix Engineer to monitor metrics for optimization techniques and congestion control strategies, as it directly relates to monitoring TCP optimization performance on the network.

upvoted 1 times

What can a Citrix Engineer implement to protect against the accidental disclosure of personally identifiable information (PII)?

- A. Form Field Consistency
- B. HTML Cross-Site Scripting
- C. Safe Object
- D. Cookie Consistency

**Suggested Answer:** C

Community vote distribution

C (100%)

 **Binomimus** Highly Voted 3 years ago

**Selected Answer: C**

I agree C: safe object

<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/dataleak-prevention/safeobject-check.html>

upvoted 6 times

 **diskman** Highly Voted 3 years, 2 months ago

Should be C: safe object that protects PII

upvoted 5 times

 **3a0f5fb** Most Recent 1 year, 3 months ago

**Selected Answer: C**

Sensitive data can be configured as Safe objects in Safe Commerce protection to avoid exposure.

upvoted 1 times

 **thedelph** 2 years, 1 month ago

**Selected Answer: C**

The Citrix Engineer can implement the Safe Object check (C) to protect against the accidental disclosure of PII, as it allows for configurable protection rules that can mask or remove sensitive information from the responses served to users.

upvoted 1 times

Which Front End Optimization technique can a Citrix Engineer enable on the Citrix ADC to remove all excess whitespace from a file?

- A. Shrink to Attributes
- B. Minify
- C. Lazy Load
- D. Inlining

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: B**

B. Minify

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: B**

B. Minify: Minification is the process of removing unnecessary characters such as whitespace, comments, and newline characters from code files.

According to the provided information, NetScaler FEO feature performs minification for CSS, JavaScript, and HTML, which matches the requirement to remove all excess whitespace from a file.

upvoted 2 times

🗳️ 👤 **Binomimus** 3 years ago

**Selected Answer: B**

B Minify

<https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html>

upvoted 4 times

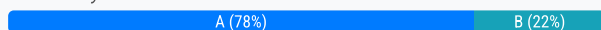


Which data populates the Events Dashboard?

- A. Syslog messages
- B. SNMP trap messages
- C. API calls
- D. AppFlow IPFIX records

**Suggested Answer: A**

*Community vote distribution*



🗳️ 👤 **3a0f5fb** 1 year, 3 months ago

**Selected Answer: A**

Syslog messages are commonly used for logging system events and can provide detailed information about various activities and issues within the system.

upvoted 1 times

🗳️ 👤 **thedelfh** 2 years, 1 month ago

**Selected Answer: A**

A. Syslog messages: The Events Dashboard typically displays events and alerts generated within the system, which are often captured as syslog messages. Syslog is a standard for message logging, and in the context of Citrix ADM, it would collect information about the system, network, and devices.

upvoted 1 times

🗳️ 👤 **MG\_KIM** 2 years, 10 months ago

syslog messages B

upvoted 1 times

🗳️ 👤 **flabiolq** 2 years, 10 months ago

**Selected Answer: A**

Syslog messages

upvoted 2 times

🗳️ 👤 **JandroFR** 2 years, 11 months ago

**Selected Answer: B**

I think that should be B, SNMP trap messages: <https://docs.citrix.com/en-us/citrix-application-delivery-management-service/networks/events/how-to-display-event-severities-snmp-traps.html>

upvoted 2 times

🗳️ 👤 **Binomimus** 3 years ago

**Selected Answer: A**

A syslog

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/networks/events/how-to-use-the-events-dashboard.html>

upvoted 3 times

Scenario: A Citrix Engineer is notified that improper requests are reacting the web application. While investigating, the engineer notices that the Citrix Web App Firewall policy has zero hits.

What are two possible causes for this within the Citrix Web App Firewall policy? (Choose two.)

- A. The expression is incorrect.
- B. It has been assigned an Advanced HTML profile.
- C. It is NOT bound to the virtual server.
- D. It has been assigned the built-in APPFW\_RESET profile.

**Suggested Answer:** AC

*Community vote distribution*

AC (100%)

  **thenetscalerguy** 1 year, 3 months ago

**Selected Answer:** AC

A and C

upvoted 1 times

  **thedelph** 1 year, 7 months ago

**Selected Answer:** AC

A. The expression is incorrect: If the policy expression does not correctly identify the traffic it is supposed to catch, then it will not trigger when that traffic is encountered. This is a common reason for a policy to have zero hits, indicating that the policy logic does not match the nature of the traffic.

C. It is NOT bound to the virtual server: For a Web App Firewall policy to be evaluated, it must be bound to the virtual server handling the traffic for the web application. If it is not bound, the policy will not be applied, and no hits will be registered regardless of the traffic.

upvoted 2 times

Which feature of Learning should a Citrix Engineer configure to direct Citrix Web App Firewall to learn from specific sessions?

- A. Advanced policy expression filter
- B. Default policy expression filter
- C. Trusted Learning Clients list
- D. Manage Content Types for Safe Commerce

**Suggested Answer: C**

*Community vote distribution*

C (100%)

  **thenetscalerguy** 1 year, 3 months ago

C Trusted Learning Clients list  
upvoted 1 times

  **thedelph** 1 year, 7 months ago

**Selected Answer: C**

C. Trusted Learning Clients list

This list is used to specify the IP addresses from which the learning feature can generate recommendations, thereby allowing learning from specific sessions that are considered trusted.

upvoted 2 times

  **Binomimus** 2 years, 6 months ago

**Selected Answer: C**

C Trusted Learning Clients list

<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/profiles/learning.html>

upvoted 2 times

A Citrix Engineer has defined an HTTP Callout, `hc_authorized_location`, to return the value "Authorized" if client's IP address is on a list of authorized external locations.

Which advanced expression should the engineer use in a policy for testing this condition?

- A. `SYS.HTTP_CALLOUT(hc_authorized_location).IS_TRUE`
- B. `SYS.HTTP_CALLOUT(hc_authorized_location).EQ("Authorized")`
- C. `SYS.HTTP_CALLOUT(hc_authorized_location).IS_VALID`
- D. `SYS.HTTP_CALLOUT(hc_authorized_location).EQUALS_ANY("Authorized")`

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ **3a0f5fb** 1 year, 3 months ago

**Selected Answer: B**

Answer B

upvoted 1 times

🗳️ **thenetscalerguy** 1 year, 9 months ago

Should be B

upvoted 1 times

🗳️ **vipjason** 2 years, 1 month ago

**Selected Answer: B**

B. The specific response they are looking for is "authorized" so the expression must equal authorized. Pretty cut and dry.

upvoted 1 times

🗳️ **Binomimus** 3 years ago

**Selected Answer: B**

I agree, B

upvoted 4 times

🗳️ **Guntrrr** 3 years, 1 month ago

Should be B - see <https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/http-callout/invoking-http-callout.html>

upvoted 4 times

Scenario: A Citrix Engineer configured signature protections for Citrix Web App Firewall. Signature Auto-Update has been enabled. Upon reviewing the log files, the engineer notices that the auto update process has an error. In the settings for Signature Auto Update the engineer notices that the URL is blank.

Which URL should the engineer enter to restore the update process?

- A. <https://s3.amazonaws.com/NSAppFwSignatures/SignaturesMapping.xml>
- B. <https://download.citrix.com/NSAppFwSignatures/SignaturesMapping.xml>
- C. <https://www.citrix.com/NSAppFwSignatures/SignaturesMapping.xml>
- D. <https://citrix.azure.com/NSAppFwSignatures/SignaturesMapping.xml>

**Suggested Answer: A**

Community vote distribution

A (100%)

 **Binomimus** Highly Voted 2 years, 6 months ago

**Selected Answer: A**

A


<https://support.citrix.com/article/CTX138858/signature-auto-update-feature-of-application-firewall>

upvoted 5 times

 **thenetscalerguy** Most Recent 1 year, 3 months ago

Should be A

upvoted 1 times

 **thedelfh** 1 year, 7 months ago

**Selected Answer: A**

A. <https://s3.amazonaws.com/NSAppFwSignatures/SignaturesMapping.xml>

This URL is typically used by Citrix Web App Firewall to retrieve the latest signature updates. If the URL is blank, entering this specific URL should allow the auto-update process to resume and fetch the latest signature updates.

upvoted 1 times

 **vipjason** 1 year, 7 months ago

**Selected Answer: A**

A. Citrix mentions that the list is hosted at amazon in the training on [learning.citrix.com](https://learning.citrix.com) and if you look at the actual URL in the ADC it says amazon. Just search for signatures in the top left of your adc and look for the auto update setting.

upvoted 1 times

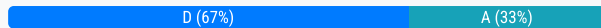
Scenario: A Citrix Engineer is reviewing the Citrix Web App Firewall log files using the GUI. Upon further analysis, the engineer notices that legitimate application traffic is being blocked.

What can the engineer do to allow the traffic to pass through while maintaining security?

- A. Note the protection blocking the traffic in the log entry. Edit the profile and deselect the Block action for the protection.
- B. Select the check box in the log entry. Choose Dismiss to allow the traffic to pass through from the Action menu.
- C. Note the protection blocking the traffic in the log entry. Create a new profile and policy and bind it with a larger priority number.
- D. Select the check box in the log entry. Choose Edit & Deploy to create a relaxation rule from the Action menu.

**Suggested Answer: A**

*Community vote distribution*



🗲️ 👤 **Guntrrr** Highly Voted 👍 2 years, 7 months ago

Answer should be D since security needs to be maintained.

upvoted 5 times

🗲️ 👤 **thenetscalerguy** Most Recent 🕒 1 year, 3 months ago

**Selected Answer: D**

Should be D

upvoted 1 times

🗲️ 👤 **thedelph** 1 year, 7 months ago

**Selected Answer: D**

D. Select the checkbox in the log entry. Choose Edit & Deploy to create a relaxation rule from the Action menu.

By selecting "Edit & Deploy," the engineer can modify the Web App Firewall rule that is blocking legitimate traffic, turning it into a relaxation rule that allows the traffic while keeping other security measures in place. This is supported by the standard practices for managing false positives in security appliances like Citrix Web App Firewall.

upvoted 1 times

🗲️ 👤 **vipjason** 1 year, 7 months ago

**Selected Answer: A**

I'm pretty sure you have to cut and paste the url or partial url from the log into the relaxation policy. I really need a relaxation policy myself.

upvoted 1 times

Scenario: A Citrix Engineer has enabled the IP Reputation feature. The engineer wants to protect a critical web application from a distributed denial of service attack.

Which advanced expression can the engineer write for a Responder policy?

- A. CLIENT.IP.SRC.IPREP\_THREAT\_CATEGORY(SPAM\_SOURCES)
- B. CLIENT.IP.SRC.IPREP\_THREAT\_CATEGORY(BOTNETS)
- C. CLIENT.IP.SRC.IPREP\_THREAT\_CATEGORY(WEB\_ATTACKS)
- D. CLIENT.IP.SRC.IPREP\_THREAT\_CATEGORY(WINDOWS\_EXPLOITS)

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗲️ 👤 **thenetscalerguy** 1 year, 3 months ago

Should be B

upvoted 1 times

🗲️ 👤 **thedelfh** 1 year, 7 months ago

**Selected Answer: B**

B. CLIENT.IP.SRC.IPREP\_THREAT\_CATEGORY(BOTNETS)

This is because botnets are commonly used to perform DDoS attacks, and selecting this category would help in creating a policy that focuses on preventing traffic that is likely to be part of such an attack. If a more specific category related to DDoS attacks is available in the actual Citrix system, that would be the ideal choice.

upvoted 1 times

🗲️ 👤 **vipjason** 1 year, 7 months ago

**Selected Answer: B**

The correct answer should be DOS but its not here. The closest thing is probably botnet. Another crappy question.

upvoted 1 times

🗲️ 👤 **Binomimus** 2 years, 6 months ago

**Selected Answer: B**

I agree, but would go for B (botnets) unless DOS is not listed

upvoted 3 times

🗲️ 👤 **Guntrrr** 2 years, 7 months ago

Correct answer doesn't seem to be in the list, the most appropriate here would be CLIENT.IP.SRC.IPREP\_THREAT\_CATEGORY(DOS) - see <https://docs.citrix.com/en-us/citrix-adc/13/reputation/ip-reputation.html>

upvoted 3 times

A Citrix Engineer wants to delegate management of Citrix Application Delivery Management (ADM) to a junior team member. Which assigned role will limit the team member to view all application-related data?

- A. readonly
- B. appReadonly
- C. admin
- D. appAdmin

**Suggested Answer: D**

Community vote distribution

D (50%)

B (50%)

🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: D**

switched to D. appAdmin. A Citrix Engineer wants to delegate management of...  
upvoted 2 times

🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: B**

To limit a junior team member to view all application-related data in Citrix Application Delivery Management (ADM), the appropriate role to assign would be:

B. appReadonly  
upvoted 3 times

🗳️ 👤 **thenetscalerguy** 1 year, 9 months ago

Should be B  
upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: B**

B. appReadonly

This role typically implies that the user can view application data but not make any changes to the configuration or settings.  
upvoted 1 times

🗳️ 👤 **robholgate** 2 years, 4 months ago

**Selected Answer: B**

appreadonly\_policy. Grants read-only permission for application features. A user bound to this policy can view the applications, but cannot perform any add, modify, or delete, enable, or disable operations.  
upvoted 1 times

🗳️ 👤 **fabbe81** 2 years, 9 months ago

**Selected Answer: D**

I would take appAdmin, as the Junior Admin needs Management permission and not only read permission.  
upvoted 3 times

🗳️ 👤 **robholgate** 2 years, 4 months ago

limit the team member to view all application-related data... look but dont allow changes  
upvoted 1 times



A Citrix Engineer wants the Citrix Web App Firewall to respond with a page stored on the Citrix ADC when a violation is detected. Which profile setting accomplishes this?

- A. Redirect URL
- B. RFC Profile
- C. Default Request
- D. HTML Error Object

**Suggested Answer: D**

Community vote distribution

D (100%)

🗲️ 👤 **thenetscalerguy** 1 year, 3 months ago

Should be D

upvoted 1 times

🗲️ 👤 **thedelph** 1 year, 7 months ago

**Selected Answer: D**

D. HTML Error Object

This setting allows the engineer to specify a custom HTML page to be presented when a policy violation occurs.

upvoted 1 times

🗲️ 👤 **vipjason** 1 year, 7 months ago

**Selected Answer: D**

D is correct. I remember this from Citrix course CNS-320 at learning.citrix.com. That guy really loves his chalk board.

upvoted 1 times

🗲️ 👤 **robholgate** 1 year, 10 months ago

**Selected Answer: D**

CTX140293

How to Create a Customized Error Page with Variables for NetScaler Application Firewall

upvoted 1 times

Scenario: A Citrix Engineer implements Application-level Quality of Experience (AppQoE) to protect a web application. Shortly after that, users call to complain that nearly every request is being met with a Captcha.

What can the engineer do to improve the user experience?

- A. Disable the Captcha.
- B. Increase the DOS Attack Threshold.
- C. Increase the Policy Queue Depth.
- D. Increase the Session Life.

**Suggested Answer: D**

Community vote distribution

D (50%)

B (50%)

🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: B**

higher number of connections are queued before activating DoS protection measures like presenting a Captcha. This is likely to improve user experience because fewer legitimate users will be presented with a Captcha under normal traffic conditions, but it still maintains a level of protection against potential DoS attacks.

upvoted 3 times

🗳️ 👤 **thenetscalerguy** 1 year, 9 months ago

Should be D

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: B**

B. Increase the DOS Attack Threshold.

Increasing the DOS Attack Threshold means that the system will wait until a higher number of connections are queued before activating DoS protection measures like presenting a Captcha. This is likely to improve user experience because fewer legitimate users will be presented with a Captcha under normal traffic conditions, but it still maintains a level of protection against potential DoS attacks.

D. Increase the Session Life.

Session Life is the duration for which the system remembers a user after displaying alternate content, like a Captcha. Increasing this time means once a user has completed a Captcha, they wouldn't be prompted again for a longer period. While this could reduce the frequency of Captcha challenges for individual users, it wouldn't prevent the initial challenge from occurring, so it might not be the most effective solution if almost every request is being met with a Captcha.

upvoted 1 times

🗳️ 👤 **vipjason** 2 years, 1 month ago

**Selected Answer: D**

I think D is the best answer

upvoted 1 times

🗳️ 👤 **fabbe81** 2 years, 9 months ago

**Selected Answer: D**

I would take D: <https://norz.at/?p=534>

upvoted 3 times

🗳️ 👤 **Binomimus** 3 years ago

B & D seem valid, I would go for B as well. A is most likely wrong, since we do not want to disable the security measure completely

upvoted 2 times

🗳️ 👤 **breakpoint0815** 3 years, 1 month ago

I would suggest answer B because of <https://support.citrix.com/article/CTX250221/appqoe-http-dos-protection-enabled-clients-were-not-getting-the-hic-response-challenge>

upvoted 2 times

  **Guntrrr** 3 years, 1 month ago

Answer D seems more appropriate - see <https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/appqoe/appqoe-parameters.html>  
upvoted 3 times

Which build-in TCP profile can a Citrix Engineer assign to a virtual server to improve performance for users who access an application from a secondary campus building over a fiber optic connection?

- A. nstcp\_default\_tcp\_lfp
- B. nstcp\_default\_tcp\_lan
- C. nstcp\_default\_tcp\_interactive\_stream
- D. nstcp\_default\_tcp\_lnp

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ **thenetscalerguy** 1 year, 3 months ago

Should be B

upvoted 1 times

🗨️ **thedelph** 1 year, 7 months ago

**Selected Answer: B**

B. nstcp\_default\_tcp\_lan

This built-in TCP profile is designed for back-end server connections where the servers reside on the same LAN as the appliance. It's optimized for environments with low latency and high bandwidth, which is characteristic of a fiber optic connection within a campus setting.

upvoted 1 times

🗨️ **Binomimus** 2 years, 6 months ago

**Selected Answer: B**

no reason to choose interactive\_stream over lan according to the citrix docs, i'd choose B

<https://docs.citrix.com/en-us/citrix-adc/current-release/system/tcp-configurations.html#built-in-tcp-profiles>

upvoted 2 times

Scenario: A Citrix Engineer wants to protect a web application using Citrix Web App Firewall. The engineer enables the Learn action for the Start URL, HTML, Cross-Site Scripting, and HTML SQL Injection protections. The engineer assigns this profile to a policy, which is then bound to the virtual server.

Which two items can the engineer check to determine that the Learn action is NOT capturing any rules? (Choose two.)

- A. The HTML Error Object is configured for the profile.
- B. Enough space is left on the /flash file system.
- C. The aslearn process is running on the Citrix ADC appliance.
- D. The Learn database is less than 20 MB.

**Suggested Answer:** CD

Community vote distribution

CD (100%)

  **thedelph** 1 year, 1 month ago

**Selected Answer:** CD

C. The aslearn process is running on the Citrix ADC appliance.

The aslearn process is responsible for the learning functionality of the Citrix Web App Firewall. If this process is not running, learning will not occur. The engineer can verify the process status using the command line on the ADC appliance.

D. The Learn database is less than 20 MB.

The Learn database has a size limit, and if it exceeds 20 MB, it will stop capturing new rules. The engineer should check the size of this database to ensure it has not reached its limit and that there is enough space to capture additional rules. If the database size is at the limit, no new learning data will be captured until the database is managed to bring it below the threshold.

upvoted 1 times

  **vipjason** 1 year, 1 month ago

**Selected Answer:** CD

C and D only make sense here.

upvoted 1 times

  **Binomimus** 2 years ago

**Selected Answer:** CD

I agree, C&D according to Guntrrr's article

upvoted 1 times

  **Guntrrr** 2 years, 1 month ago

Should be C & D - see <https://support.citrix.com/article/CTX223403/how-to-troubleshoot-netcaler-appfirewall-aslearn-issues>

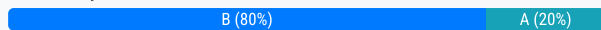
upvoted 2 times

Scenario: A Citrix Engineer wants to use Citrix Application Delivery Management (ADM) to monitor a single Citrix ADC VPX with eight web applications and one Citrix Gateway. It is important that the collected data be protected.  
Which deployment will satisfy the requirements?

- A. A single Citrix ADM with database replication to a secondary storage repository.
- B. A pair of Citrix ADM virtual appliances configured for High Availability.
- C. A single Citrix ADM imported onto the same hypervisor as the Citrix ADC VPX.
- D. A pair of Citrix ADM virtual appliances, each working independently.

**Suggested Answer: B**

Community vote distribution



caioninaut 1 year ago

**Selected Answer: A**

As the statement only says satisfy, both options will satisfy. But if you think about the resources and for ex. can't afford an HA. A single instance of ADM and a store on another host would be sufficient.

I would go with A.

upvoted 1 times

vipjason 1 year, 1 month ago

**Selected Answer: B**

ADM can run in an HA pair in which the database on the primary will be replicated to the secondary. It can also run in a DR setup with database replication, but the DR will not come online until a script is run on it. When failing over back to prod the script must be run there.

upvoted 1 times

Binomimus 2 years ago

**Selected Answer: B**

I agree, B

upvoted 3 times

Guntrrr 2 years, 1 month ago

Should be B - see <https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/deploy/high-availability-deployment.html>

upvoted 3 times

A manager for a hospital billing system wants to display the last four digits of a credit card number when printing invoices. Which credit card security action does this?

- A. X-Out
- B. Log
- C. Transform
- D. Block

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ **3a0f5fb** 1 year, 2 months ago

<https://docs.netScaler.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html>

upvoted 1 times

🗳️ **3a0f5fb** 1 year, 2 months ago

**Selected Answer: A**

Credit card protection

The Application Firewall offers an option to inspect the headers and body of the response and either removes or x-outs the Credit Card numbers before forwarding the response to the client. Currently Application Firewall offers protection for the following major credit cards: American Express, Diners Club, Discover, JCB, MasterCard, and Visa. The x-out action works independent of the Block action.

upvoted 1 times

🗳️ **thedelph** 2 years, 1 month ago

**Selected Answer: A**

A. X-Out

X-Out is typically used to mask or hide sensitive information, such as credit card numbers, by replacing part of the data with "X" characters, except for the last few digits. This helps protect sensitive information while still providing some information for reference purposes.

upvoted 1 times

🗳️ **robholgate** 2 years, 4 months ago

**Selected Answer: A**

The number of X'd out digits depends on the length of the credit card numbers. Ten digits are X'd out for credit cards that have 13 through 15 digits. Twelve digits are X'd out for credit cards that have 16 digits. If your application does not require sending the entire credit card number in the response, Citrix recommends that you enable this action to mask the digits in the credit card numbers.

upvoted 2 times

Which protection can a Citrix Engineer implement to prevent a hacker from extracting a customer list from the company website?

- A. Cross-Site Request Forgeries (CSRF)
- B. Form Field Consistency
- C. HTML Cross-Site Scripting (XSS)
- D. HTML SQL Injection

**Suggested Answer:** D

*Community vote distribution*

D (100%)

  **thedelph** 1 year, 1 month ago

**Selected Answer: D**

D. HTML SQL Injection

This type of protection is designed to prevent SQL injection attacks, where an attacker could exploit vulnerabilities in the web application's database interaction to execute malicious SQL statements. This could lead to unauthorized viewing of data, such as a customer list, or even worse, database modification or control over the database server. The other protections listed are for different types of attacks:

upvoted 1 times

  **Binomimus** 2 years ago

**Selected Answer: D**

I agree, should be D

upvoted 3 times

  **Guntrrr** 2 years, 1 month ago

Answer should be D

upvoted 2 times



Scenario: A Citrix Engineer needs to forward the Citrix Web App Firewall log entries to a central management service. This central management service uses an open log file standard.

Which log file format should the engineer use in the Citrix Web App Firewall engine settings to designate the open log file standard?

- A. CEF
- B. IIS
- C. W3C
- D. TLA

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗲️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: A**

CEF enables customers to use a common event log format so that data can be easily collected and aggregated for analysis by an enterprise management system.

<https://docs.netScaler.com/en-us/citrix-adc/current-release/application-firewall/logs.html>

upvoted 1 times

🗲️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: A**

A. CEF

The Common Event Format (CEF) is an open log management standard that facilitates interoperability between security-related information from different security and network devices and applications. It's designed to allow easy integration and aggregation of logs from different systems into a central management service.

upvoted 1 times

🗲️ 👤 **robholgate** 2 years, 4 months ago

**Selected Answer: A**

The Web App Firewall also supports CEF logs. CEF is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications.

<https://docs.netScaler.com/en-us/citrix-adc/current-release/application-firewall/logs.html>

upvoted 2 times

Scenario: A Citrix Engineer is monitoring the environment with Citrix Application Delivery Management (ADM). Management has asked for a report of high-risk traffic to protected internal websites.

Which dashboard can the engineer use to generate the requested report?

- A. App Security
- B. Transactions
- C. Users & Endpoints
- D. App

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: A**

A. App Security

<https://docs.netScaler.com/en-us/netScaler-console-service/analytics/security/app-security-dashboard.html>

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: A**

A. App Security

The App Security dashboard in Citrix ADM is designed to provide insights into security threats and risks within the environment. The engineer can utilize this dashboard to generate reports detailing high-risk traffic to protected internal websites, as it would typically include metrics and data related to security events and violations, including web application firewall (WAF) events, which are indicative of high-risk traffic.

upvoted 2 times

🗳️ 👤 **robholgate** 2 years, 4 months ago

**Selected Answer: A**

The App Security dashboard provides you the overview of security metrics for the discovered/licensed applications. This dashboard displays the security attack information for the discovered/licensed applications, such as sync attacks, small window attacks, DNS flood attacks, and so on.

upvoted 1 times

🗳️ 👤 **fabbe81** 2 years, 9 months ago

**Selected Answer: A**

I think it is A, as transactions displays the user behavior. App Security shows communication to Webserver: <https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/application-analytics-and-management/app-security-dashboard.html>

upvoted 2 times

Scenario: A Citrix Engineer has a pair of Citrix ADC VPX appliances configured as a High-Availability (HA) pair and hosted on a Citrix Hypervisor. The engineer wants to use Citrix Application Delivery Management (ADM) to monitor and manage the 35 web applications on the appliances. The engineer has imported Citrix ADM virtual appliance to Citrix Hypervisor. The engineer has also configured the management IP address settings and has added the 35 instances. However, some of the instances are NOT reporting any data. Which two areas can the engineer check to determine the cause of the issue? (Choose two.)

- A. A Premium platform license must be configured on each instance.
- B. AppFlow must be enabled on each instance.
- C. The Citrix ADM license must be installed.
- D. An SSL certificate must be installed on the Citrix ADM appliance.

**Suggested Answer: BC**

Community vote distribution

BC (100%)

🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: BC**

- B. AppFlow must be enabled on each instance.
- C. The Citrix ADM license must be installed.

upvoted 1 times

🗳️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: BC**

- B. AppFlow must be enabled on each instance.

AppFlow is the feature on Citrix ADC appliances that collects application traffic data and forwards it to Citrix ADM for analysis and reporting. If AppFlow is not enabled on an instance, Citrix ADM will not receive any application traffic data from that instance. The engineer should ensure that AppFlow is enabled and properly configured on all instances that are not reporting data.

- C. The Citrix ADM license must be installed.

For Citrix ADM to monitor and manage instances, the appropriate licenses must be installed on the ADM appliance. Without a valid license, the functionality of Citrix ADM can be restricted, which might result in some instances not reporting any data. The engineer should verify that Citrix ADM is properly licensed to manage the number of instances and the features required for monitoring and managing the web applications.

upvoted 1 times

🗳️ 👤 **vipjason** 2 years, 1 month ago

**Selected Answer: BC**

ADM can monitor up to 30 vservers without requiring a license. In order for a vServer to be monitored, it must have app flow enabled.

upvoted 1 times

🗳️ 👤 **Guntrrr** 3 years, 1 month ago

Should be B&C

upvoted 4 times

Which Front End Optimization technique overcomes the parallel download limitation of web browsers?

- A. Domain Sharding
- B. Minify
- C. Extend Page Cache
- D. Lazy Load

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: A**

A. Domain Sharding  
upvoted 1 times

🗳️ 👤 **thedelfh** 2 years, 1 month ago

**Selected Answer: A**

Domain Sharding:

"Overcomes the connection limitation, which improves page-rendering time by enabling client browsers to download more resources in parallel."

<https://docs.netScaler.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html#optimizations-performed-by-the-feo-feature>  
upvoted 3 times

🗳️ 👤 **robholgate** 2 years, 4 months ago

**Selected Answer: A**

Domain sharding

Many browsers set limits on the number of simultaneous connections that can be established to a single domain. This can cause browsers to download webpage resources one at a time, resulting in higher browsers time.

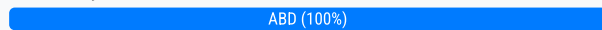
<https://docs.netScaler.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html>  
upvoted 1 times

Statistics for which three types of violations are presented on the App Security Dashboard? (Choose three.)

- A. Web App Firewall protection
- B. IP Reputation
- C. SSL Enterprise Policy
- D. Signature
- E. AAA

**Suggested Answer:** ABD

*Community vote distribution*



 **thedelfh** 1 year, 1 month ago

**Selected Answer:** ABD

The App Security Dashboard presents statistics for the following three types of violations:

- A. Web App Firewall protection
  - B. IP Reputation
  - D. Signature
- upvoted 1 times

Which Citrix Web App Firewall profile setting can a Citrix Engineer configure to provide a response when a violation occurs?

- A. Default Request
- B. Redirect URL
- C. Return URL
- D. Default Response

**Suggested Answer:** D

*Community vote distribution*

D (100%)

  **thedelph** 1 year, 1 month ago

**Selected Answer:** D

A Citrix Engineer can configure the Default Response setting in a Citrix Web App Firewall profile to provide a response when a violation occurs. This setting determines the action the Web App Firewall takes when a request matches a Web App Firewall rule and is considered a violation.  
upvoted 1 times

A Citrix Engineer wants to quietly track attempts that cause a web application to display a list of all user accounts. Which action should the engineer enable to achieve this?

- A. Stats
- B. Block
- C. Log
- D. Learn

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗲️ 👤 **3a0f5fb** 1 year, 2 months ago

**Selected Answer: C**

C. Log

upvoted 1 times

🗲️ 👤 **thedelph** 2 years, 1 month ago

**Selected Answer: C**

The Citrix Engineer should enable the "Log" action to quietly track attempts that cause a web application to display a list of all user accounts. This action will record the attempts in the logs without blocking the user or impacting the user experience.

upvoted 2 times


Which protection ensures that links to sensitive pages can only be reached from within an application?

- A. Form Field Consistency Check
- B. Buffer Overflow Check
- C. URL Closure
- D. Deny URL

**Suggested Answer:** C

*Community vote distribution*

C (100%)

  **thedelph** 1 year, 1 month ago

**Selected Answer: C**

C. URL Closure

The URL Closure protection ensures that links to sensitive pages can only be reached from within the application. It helps prevent forceful browsing to sensitive pages without proper navigation from within the site, by restricting direct access to URLs that are only meant to be accessed as part of the application's flow.

upvoted 1 times

  **RVR** 1 year, 7 months ago

**Selected Answer: C**

Think it should be (c) Enforce URL Closure <https://docs.netScaler.com/en-us/citrix-adc/current-release/application-firewall/url-protections/starturl-check.html>

upvoted 2 times