

1Y0-351^{Q&As}

Citrix NetScaler 10.5 Essentials and Networking

Pass Citrix 1Y0-351 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/1y0-351.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Citrix Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

- 😳 365 Days Free Update
- 800,000+ Satisfied Customers





QUESTION 1

Which statement is true about interface link-state on the NetScaler?

- A. Interface link-state is controlled by ifconfig in BSD.
- B. Interface link-state is dependent on the HAMON setting.
- C. Interface link-state CANNOT be brought down from the NetScaler.
- D. Interface link-state on both appliances is unaffected by the force failover command.

Correct Answer: C

QUESTION 2

Which step is required to ensure that SSL traffic is passed through the NetScaler to backend services without processing SSL on the NetScaler appliance?

- A. Create a service group of type SSL.
- B. Create a service group of type HTTP.
- C. Bind an SSL certificate to a service group.
- D. Bind an SSL certificate to the virtual server
- E. Create a service group of type SSL_BRIDGE.

Correct Answer: E

QUESTION 3

Scenario: An engineer has three subnets configured on a NetScaler appliance. The engineer must only allow a certain group of users to access a virtual server on the appliance. The IT Manager requires that all rules are flexible and can be easily modified for ease of administration.

How could the engineer allow certain groups to access the virtual server while still being able to modify the setting in the future?

A. Add a Simple ACL.

- B. Disable USNIP Mode.
- C. Create an Extended ACL.
- D. Add a Host Route to the virtual server.

Correct Answer: C



QUESTION 4

Which type of authentication server could an engineer configure in order to provide the use of RSA token authentication as a permitted authentication method to access a AAA Virtual Server?

A. LDAP

- B. SAML
- C. RADIUS
- D. Negotiate

Correct Answer: C

http://support.citrix.com/article/CTX127543

This document describes how to configure Access Gateway 5.0 for authentication against an RSA SecureID Authentication server. It describes the configuration required in both the Access Gateway and the RSA server for various deployment topologies.



Name:	cag5a.support.net							
Network address:	twork address: 172.16.18.40							
Site:			Select					
Agent type:	UNIX Agent Communication S Single-Transactio							
Encryption Type:	○ SDI ④ DES							
Г	Node Secret Crea	ted						
	Open to All Local	y Known Users						
Г	Search Other Rea	lms for Unknown Users						
Г	Requires Name L	ock						
v	Enable Offline Aut	thentication						
	Enable Windows	Password Integration						
Г	Create Verifiable	Authentications						
Group Act	ivations	User Activations	1					
Secondary Nodes Delete Agent Host								
Edit Agent Host I	Extension Data	Configure RADIUS Connection]					
8	ng Servers	Create Node Secret File	7					

Within the RSA Authentication Manager console, choose Agent Host > Generate Configuration Files and select for One Agent Host, and choose the Agent Host created in step 1 and save the generated sdconf.rec file.



Eile	System	User	Token	Group	Agent Host	<u>R</u> ealm	Site	RADIUS	Log	Report	Heb	
					<u>A</u> dd Agen <u>E</u> dit Agen <u>C</u> opy Age List Agenl <u>D</u> elete Ag <u>S</u> erver As	t Host ert Host. : Hosts ient Host	 , ; 5					
					Generate	Configu	ration	Files				

If using RSA 7.1

Open the RSA Security Console and navigate to Access > Authentication Agents > Add New. Enter the name and IP Address of the Access Gateway, and set Agent type to Standard Agent.

Save this new agent.

Hostname:	Cag5.support.net Resolve IP
	C Existing node: Choose One
IP Address:	Resolve Hostname
I Protect IP Address:	I Prevent auto registration from unassigning IP address
I Alternate IP Addresses:	IP Address Add Dipdate Dipdate
	Remove X
Notes:	
Authentication Agent Attributes	
Authentication Agent Attributes	Standard Agent 👻
Authentication Agent Attributes	Standard Agent 👻
Authentication Agent Attributes	
Authentication Agent Attributes Agent Type: Disabled: Agent May be Accessed by:	Apent is disabled All users
Authentication Agent Attributes Agent Type: Disabled: Agent May be Accessed by: Authentication Manager Contact List:	Apent is disabled All users O Doly members of user groups granted access to this agent Automatically assign automatic contact list from instance that responds first
Authentication Agent Attributes AgentType: Disabled: Agent May be Accessed by: Authentication Manager Contact List: Trusted Realm Settings	Apent is disabled All users O Doly members of user groups granted access to this agent Automatically assign automatic contact list from instance that responds first
Authentication Agent Attributes AgentType: Disabled: Agent May be Accessed by: Authentication Manager Contact List: Trusted Realm Settings	Apent is disabled All users Only members of user groups granted access to this agent Automatically assign automatic contact list from instance that responds first Manually assign contact list: rea7Liapac.leb (outomatic) -

Select Access > Authentication Agents > Generate Configuration File and generate the configuration file. There is no option to generate a configuration file for a single host in RSA 7.1. Save and extract the sdconf.rec from the generated zip file.



RS/	🔨 Secu	rity Conso	ole						
Home	Identity 🔻	Authentication *	Access 🔻	Reporting *	RADIUS -	Administration *	Se		
N			Session Life	etimes 🕨 🕨					
	🖀 🔪 Realm: SystemDoma			Sessions					
	Welcome .	Authentica	tion Agents 🕨	Manage Existing					
			Test Acces	S	Add New				
	My Conso	ble		Generate Configuration File					
	> My Permi	ssions		Download Server Certificate File					
	> My Prefe	rences			Authentication Manager Contact List 🕨				

Log on to the Access Gateway AdminLogonPoint and go to Authentication Profiles to create an RSA authentication profile. Browse to the generated sdconf.rec file on your computer to upload it on the Appliance, and save the profile.

System Administration	Authentication Profile	5				
Networking						
Appliance Failover	RADUS, and RSA Se	e authentication profiles on Acces: curiD.	s Gateway, The ava-	ladie autrientication types	are LUAP	
Name Service Providers						
Static Routes		10.6%				
Address Pools	Profile Name	Description		Туре		
Deployment Mode	ctxang	ctxang		LDAP		
Password	RSA	ų.		RSA SecuriD		
Date and Time			RSA SecuriD	Configuration		×
licensing						
Logging				General Pro	operties	
			Name	* 754		
Access Control	Add	Edit Remove	Descriptio	n.		
Global Options			J	755		
Authentication Profiles				-	5	
Network Resources			Configura	ton file: a ketcred>	-4	Browse
Device Profiles	1		· Instantes	required field	1	[]
Logon Points			maroates	Nederica Hela		
SmartGroups	1				1.000	- 14 M

Additional Notes for Creating the Agent Record in RSA. The details entered into the Agent Host configuration are specific, and depend on the deployment configuration of your Access Gateway. The following are the different deployment methods and the associated configuration within the RSA Agent:

Access Gateway is a non-HA deployment in one-arm mode. Network Address: IP address of Access Gateway Access Gateway is a non-HA deployment in two-arm mode, traffic to the RSA server is through the

interface with the Internal role

Network Address: IP address of the interface with the Internal role Access Gateway is a non-HA deployment in two-arm mode, traffic to the RSA server is through the interface with the External role. Network Address: IP address of the



interface with the Internal role Secondary Nodes: IP address of the

interface with the External role Access Gateway is in an HA deployment in one-arm mode Network

Address: The HA Virtual IP address Secondary Nodes: The physical IP addresses of both Access Gateways Access Gateway is in an HA deployment in two-arm mode, traffic to the RSA server is through the interface marked as INTERNAL

Network Address: The HA Internal virtual IP address

Secondary Nodes: The physical IP addresses of the interfaces with the Internal role on both Access Gateways Access Gateway is in an HA deployment in two-arm mode, traffic to the RSA server is through the

interface marked as EXTERNAL Network Address: The HA Internal virtual IP address

Secondary Nodes: The physical IP addresses of the interfaces with the External role on both Access Gateways

*In RSA 7.1 Secondary Nodes have been renamed to Alternate IP Addresses in the Authentication Agent configuration.

QUESTION 5

Traffic to which destination is sourced from the NetScaler IP (NSIP) by default?

A. NTP servers

- B. Clients on the Internet
- C. Load-balanced web services
- D. Load-balanced authentication services

Correct Answer: A

Latest 1Y0-351 Dumps

1Y0-351 Practice Test

1Y0-351 Exam Questions