

vRealize Automation 8.1

로드 밸런싱 가이드

2020년 4월 14일

vRealize Automation 8.1



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2020 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

1	vRealize Automation 8.0 로드 밸런싱	5
2	로드 밸런싱 개념	6
	SSL 패스스루	6
	로드 밸런서에 대한 이메일 알림	6
	단일 암 및 다중 암 토폴로지	7
3	vRealize Automation에 대한 로드 밸런서 구성을 위한 사전 요구 사항	8
	초기 설치 완료	9
4	NSX-V 구성	10
	글로벌 설정 구성	10
	애플리케이션 프로파일 구성	12
	서비스 모니터링 구성	13
	서버 풀 구성	15
	가상 서버 구성	17
5	NSX-T 구성	19
	NSX-T 애플리케이션 프로파일 구성	19
	Workspace ONE Access에 대한 지속성 프로파일 구성	20
	NSX-T 액티브 상태 모니터 구성	20
	NSX-T 서버 풀 구성	23
	NSX-T 가상 서버 구성	24
	로드 밸런서 구성	26
	로드 밸런서에 가상 서버 추가	26
6	F5 Big-IP LTM 구성	28
	Workspace ONE Access에 대한 사용자 지정 지속성 프로파일 구성	28
	모니터 구성	29
	F5 서버 풀 구성	30
	F5 가상 서버 구성	32
7	Citrix ADC(NetScaler ADC) 구성	34
	Citrix 모니터 구성	34
	Citrix 서비스 그룹 구성	37
	Citrix 가상 서버 구성	38

Workspace ONE Access에 대한 지속성 그룹 구성 40

8 문제 해결 41

OneConnect를 F5 BIG-IP와 함께 사용하는 경우 프로비저닝 실패 41

F5 BIG-IP 라이선스 제한 네트워크 대역폭 41

vRealize Automation 8.0 로드 밸런싱

1

이 문서는 분산 및 고가용성 배포에서 vRealize Automation, vRealize Orchestrator 및 Workspace ONE Access용 F5 Networks BIG-IP 소프트웨어(F5), Citrix NetScaler 및 NSX로드 밸런서의 로드 밸런싱 모듈 구성에 대해 설명합니다.

이 문서는 설치 가이드가 아니며 [VMware vRealize Automation 제품 설명서](#)와 [VMware vRealize Orchestrator 제품 설명서](#)에 제공되는 vRealize Automation 및 vRealize Orchestrator 설치 및 구성 설명서를 보충하는 로드 밸런싱 구성 가이드입니다.

이 정보는 다음 제품 및 버전용입니다.

표 1-1.

제품	버전
F5 BIG-IP LTM	11.x, 12.x, 13.x, 14.x, 15.x
NSX-V	6.2.x, 6.3.x, 6.4.x(자세한 내용은 VMware 제품 상호 운용성 매트릭스 를 참조하십시오.)
NSX-T	2.4
Citrix NetScaler ADC	10.5, 11.x, 12.x, 13.x
vRealize Automation	8.0
vRealize Orchestrator	8.0
Workspace ONE Access(이전 이름: VMware Identity Manager)	3.3.1

자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

로드 밸런싱 개념

2

로드 밸런서는 고가용성 배포에서 서버 간에 작업을 분산시킵니다. 시스템 관리자는 다른 구성 요소와 동시에 로드 밸런서를 정기적으로 백업합니다.

네트워크 토폴로지 및 VMware 제품 백업 계획 유지를 고려하면서 로드 밸런서 백업에 대한 사이트 정책을 따르십시오.

본 장은 다음 항목을 포함합니다.

- [SSL 패스스루](#)
- [로드 밸런서에 대한 이메일 알림](#)
- [단일 암 및 다중 암 토폴로지](#)

SSL 패스스루

SSL 패스스루는 로드 밸런싱 구성과 함께 사용됩니다.

SSL 패스스루는 다음과 같은 이유로 사용됩니다.

- **순쉬운 배포**
 - vRealize Automation, vRealize Orchestrator 또는 Workspace ONE Access 인증서를 로드 밸런서에 배포하지 않아도 되기 때문에 배포가 간소화되고 복잡성이 줄어듭니다.
- **운영비 부담 없음**
 - 인증서 갱신 시 로드 밸런서에 대한 구성 변경이 필요하지 않습니다.
- **순쉬운 통신**
 - 로드 밸런싱된 구성 요소의 개별 호스트 이름이 인증서의 주체 대체 이름 필드이기 때문에 클라이언트가 로드 밸런싱된 노드와 쉽게 통신할 수 있습니다.

로드 밸런서에 대한 이메일 알림

vRealize Automation, vRealize Orchestrator 또는 Workspace ONE Access 노드가 다운될 때마다 시스템 관리자에게 이메일을 보내는 로드 밸런서에 대한 이메일 알림을 설정하는 것이 좋습니다.

현재 NSX-V/T는 이러한 시나리오에 대한 이메일 알림을 지원하지 않습니다.

NetScaler의 경우 특정 SNMP 트랩 및 SNMP 관리자가 경고를 보내도록 구성합니다. SNMP 구성에 대한 자세한 내용은 NetScaler 설명서를 참조하십시오.

다음 방법으로 F5 키를 사용하여 이메일 알람을 설정할 수 있습니다.

- 로컬로 생성된 이메일 메시지를 전달하도록 BIG-IP 시스템 구성
- 사용자 지정 SNMP 트랩 구성
- 이메일 알람을 보내도록 경고 구성

단일 암 및 다중 암 토폴로지

단일 암 및 다중 암 배포는 로드 밸런서 트래픽을 다르게 라우팅합니다.

단일 암 배포의 경우 로드 밸런서가 물리적으로 트래픽 라인에 있지 않습니다. 즉, 로드 밸런서의 수신 및 송신 트래픽이 동일한 네트워크 인터페이스를 통과합니다. 로드 밸런서를 통한 클라이언트의 트래픽은 로드 밸런서를 소스 주소로 사용하는 NAT(네트워크 주소 변환)입니다. 노드는 클라이언트로 다시 전달되기 전에 반환 트래픽을 로드 밸런서로 보냅니다. 이러한 역방향 패킷 흐름이 없으면 반환 트래픽이 클라이언트에 직접 연결하려고 시도하기 때문에 연결이 실패합니다.

다중 암 구성에서는 트래픽이 로드 밸런서를 통해 라우팅됩니다. 최종 디바이스는 일반적으로 로드 밸런서를 기본 게이트웨이로 사용합니다.

가장 일반적인 배포는 단일 암 구성입니다. 동일한 원칙이 다중 암 배포에도 적용되며, F5 및 NetScaler와 모두 작동합니다. 이 문서에서는 vRealize Automation, vRealize Orchestrator 또는 Workspace ONE Access 구성 요소가 단일 암 구성으로 배포됩니다. 다중 암 배포도 지원되며 해당 구성은 단일 암 구성과 유사해야 합니다.

단일 암 구성:



vRealize Automation에 대한 로드 밸런서 구성을 위한 사전 요구 사항

3

vRealize Automation에 대한 로드 밸런서를 구성하기 전에 다음 사전 요구 사항을 수행합니다.

- **NSX-V/T** — NSX-V/T를 로드 밸런서로 사용하여 vRealize Automation, vRealize Orchestrator 또는 Workspace ONE Access의 HA 구현을 시작하기 전에 NSX-V/T 토폴로지가 구성되어 있고 사용 중인 NSX-V/T 버전이 지원되는지 확인합니다. 이 문서는 NSX-V/T 구성의 로드 밸런싱 측면을 다루며 NSX-V/T가 대상 환경 및 네트워크에서 올바르게 작동하도록 구성되고 검증되었다고 가정합니다.

사용 중인 버전이 지원되는지 확인하려면 현재 릴리스의 vRealize Automation 지원 매트릭스를 참조하십시오.

- **F5 BIG-IP LTM** — F5 LTM 로드 밸런서를 사용하여 vRealize Automation, vRealize Orchestrator 또는 Workspace ONE Access의 HA 구현을 시작하기 전에 로드 밸런서가 설치되고 라이선스가 부여되고 DNS 서버 구성이 완료되었는지 확인합니다.
- **NetScaler** — NetScaler 로드 밸런서를 사용하여 vRealize Automation, vRealize Orchestrator 또는 Workspace ONE Access의 HA 구현을 시작하기 전에 NetScaler가 설치되어 있고 Standard Edition 라이선스 이상을 구성했는지 확인합니다.
- **인증서** — SubjectAltNames 섹션에 클러스터 노드의 호스트 이름 및 로드 밸런서의 FQDN(정규화된 도메인 이름)이 포함된 CA(인증 기관) 서명 인증서를 요청합니다. 이 구성을 사용하면 로드 밸런서가 SSL 오류 없이 트래픽을 처리할 수 있습니다.
- **ID 제공자** — vRealize Automation 8.0부터 기본 ID 제공자는 vRealize Automation 장치 외부에 있는 Workspace ONE Access입니다.

설치 및 구성에 대한 자세한 내용은 docs.vmware.com에서 vRealize Automation 설명서를 참조하십시오.

필요한 경우 외부 vRealize Orchestrator 클러스터를 vRealize Automation 시스템과 작동하도록 구성할 수 있습니다. 이 작업은 vRealize Automation 시스템이 가동되어 실행된 후에 수행할 수 있습니다. 단, vRealize Automation 고가용성 설정에는 내장형 vRealize Orchestrator 클러스터가 이미 포함되어 있습니다.

본 장은 다음 항목을 포함합니다.

- 초기 설치 완료

초기 설치 완료

vRealize Automation, vRealize Orchestrator 또는 VMware Identity Manager 초기 설치를 완료하기 전에 로드 밸런서를 구성해야 합니다.

절차

- 1 F5, NSX 또는 NetScaler 로드 밸런서를 구성합니다. 자세한 내용은 F5 BIG-IP 구성, NSX 구성 및 Citrix NetScaler 구성을 참조하십시오.
- 2 vRealize Automation, vRealize Orchestrator 및 VMware Identity Manager [설치 및 구성 설명서](#)에 나와 있는 지침에 따라 모든 시스템 구성 요소를 설치하고 구성합니다.
- 3 설치 후 로드 밸런서에서 상태 모니터를 사용하도록 설정된 상태로 모든 노드가 예상 상태인지 확인합니다. 가상 장치 노드의 풀, 서비스 그룹 및 가상 서버를 사용할 수 있고 실행할 수 있어야 합니다. 모든 가상 장치 노드는 사용이 가능하고 실행 중이며 사용하도록 설정되어 있어야 합니다.

NSX-V 구성

4

새로운 NSX-V Edge Services Gateway를 배포하거나 기존 게이트웨이를 다시 사용할 수 있습니다. 하지만 로드 밸런싱되는 vRealize 구성 요소와의 네트워크 연결이 있어야 합니다.

본 장은 다음 항목을 포함합니다.

- 글로벌 설정 구성
- 애플리케이션 프로파일 구성
- 서비스 모니터링 구성
- 서버 풀 구성
- 가상 서버 구성

글로벌 설정 구성

다음 단계를 사용하여 전역 설정을 구성합니다.

절차

- 1 NSX-V에 로그인하여 **Manager > 설정**을 클릭하고 **인터페이스**를 선택합니다.
- 2 목록에서 **Edge** 디바이스를 선택합니다.
- 3 가상 IP 주소를 호스팅하는 외부 인터페이스에 대해 **vNIC#**을 클릭하고 **편집** 아이콘을 클릭합니다.

- 4 NSX-V Edge에 적합한 네트워크 범위를 선택하고 **편집** 아이콘을 클릭합니다.

Edit Interface | nic0

Basic Advanced

vNIC# 0

Name * nic0

Type ☐ Internal ☒ Uplink ☐ Trunk

Connected To * Prod-01

Connectivity Status ☒ Connected

Configure Subnets

+ ADD DELETE Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/>	192.168.208.102		24

1 items

CANCEL SAVE

- 5 가상 IP에 할당된 IP 주소를 추가하고 **저장**을 클릭합니다.
- 6 **확인**을 클릭하여 인터페이스 구성 페이지를 종료합니다.
- 7 로드 밸런서 탭으로 이동한 후 **편집** 아이콘을 클릭합니다.
- 8 필요한 경우 로드 밸런서 사용 및 로깅을 선택하고 **저장**을 클릭합니다.

Edit Load Balancer Global Configuration

Load Balancer ☒ Enable

Acceleration ☐ Disable

Logging ☒ Enable

Log Level

CANCEL SAVE

애플리케이션 프로파일 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 애플리케이션 프로파일을 추가해야 합니다.

절차

- 1 왼쪽 창에서 **애플리케이션 프로파일**을 클릭합니다.
- 2 **추가** 아이콘을 클릭하고 특정 제품에 필요한 애플리케이션 프로파일을 이 표에 설명된 대로 생성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 4-1. 애플리케이션 프로파일

이름	유형	지속성	만료 시간
vRealize Automation	SSL 패스스루	없음	없음
vRealize Orchestrator	SSL 패스스루	없음	없음
참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.			
VMware Identity Manager	SSL 패스스루	소스 IP	36000

결과

완료된 구성은 다음 화면과 유사합니다.

New Application Profile [X]

Application Profile Type SSL Passthrough ⓘ

General Client SSL Server SSL

Name * vRealize Automation / vRealize Orchestrator VA Web

HTTP Redirect URL

Persistence None

Cookie Name

Mode

Expires in (Seconds)

Insert X-Forwarded-For HTTP header Disable

CANCEL **ADD**

서비스 모니터링 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 서비스 모니터를 추가해야 합니다.

절차

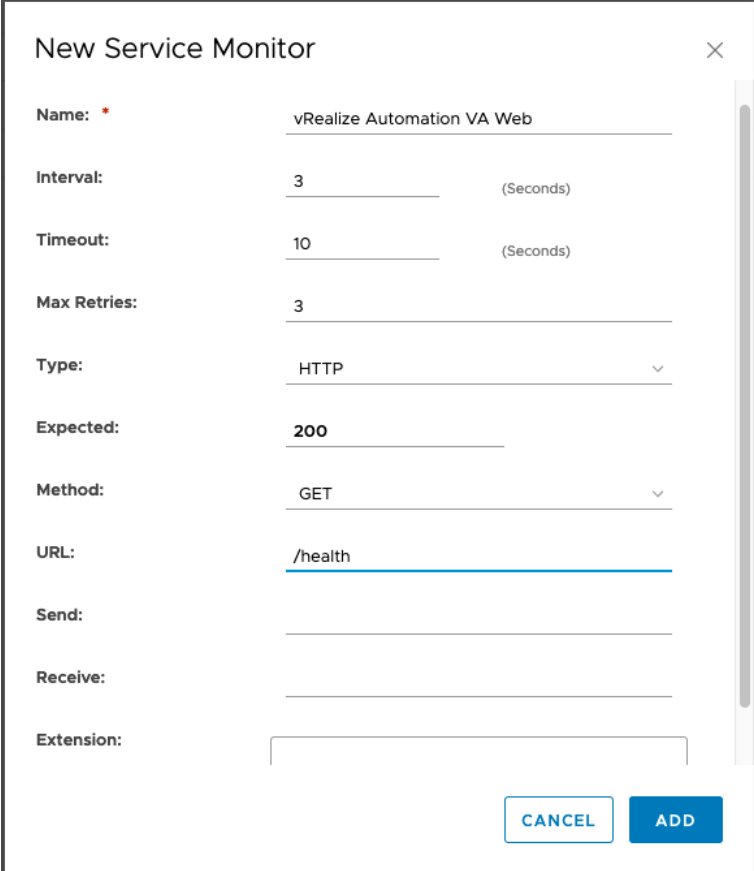
- 1 왼쪽 창에서 **서비스 모니터링**을 클릭합니다.

- 2 추가** 아이콘을 클릭하고 특정 제품에 필요한 서비스 모니터를 이 표에 설명된 대로 생성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 4-2. 서비스 모니터링

이름	간격	시간 초과	재시도 횟수	유형	메서드	URL	수신	예상
vRealize Automation	3	10	3	HTTP	GET	/health		200
vRealize Orchestrator <small>참고 외부 vRealize Orchestrator 인스턴스에 만 사용됩니다.</small>	3	10	3	HTTP	GET	/health		200
VMware Identity Manager	3	10	3	HTTPS	GET	/SAAS/API/1.0/REST/system/health/heartbeat	OK	200

결과



The image shows a 'New Service Monitor' dialog box with the following fields and values:

Field	Value	Unit/Note
Name *	vRealize Automation VA Web	
Interval	3	(Seconds)
Timeout	10	(Seconds)
Max Retries	3	
Type	HTTP	
Expected	200	
Method	GET	
URL	/health	
Send		
Receive		
Extension		

Buttons: CANCEL, ADD

완료된 구성은 다음 화면과 유사합니다.

서버 풀 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 서버 풀을 생성해야 합니다.

절차

- 1 왼쪽 창에서 **풀**을 클릭합니다.

2 추가 아이콘을 클릭하고 특정 제품에 필요한 풀을 이 표에 설명된 대로 생성합니다.

표 4-3. 서버 풀

풀 이름	알고리즘	모니터	멤버 이름	IP 주소/ vCenter 컨테이너	포트	모니터 포트
vRealize Automation	최소 연결	vRealize Automation	VA1 VA2 VA	IP 주소	443	8008
vRealize Orchestrator 참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.	최소 연결	vRealize Orchestrator	VA1 VA2 VA3	IP 주소	443	8008
VMware Identity Manager	최소 연결	VMware Identity Manager	VA1 VA2 VA3	IP 주소	443	8008

결과

완료된 구성은 다음 화면과 유사합니다.

New Pool

General

Members

+ ADD

EDIT

DELETE

	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
<input type="radio"/>	vRA_VA_1	10.10.10.10	1	8008	443		
<input type="radio"/>	vRA_VA_3	10.10.10.12	1	8008	443		
<input type="radio"/>	vRA_VA_2	10.10.10.11	1	8008	443		

1 - 3 of 3 items

CANCEL

ADD

가상 서버 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 가상 서버를 구성해야 합니다.

절차

- 1 왼쪽 창에서 **가상 서버**를 클릭합니다.

- 2 추가** 아이콘을 클릭하고 다른 제품에 필요한 가상 서버를 이 표에 설명된 대로 생성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 4-4. 가상 서버

이름	가속	IP 주소	프로토콜	포트	기본 풀	애플리케이션 프로파일
vRealize Automation	사용 안 함	IP 주소	HTTPS	443	vRealize Automation	vRealize Automation
vRealize Orchestrator 참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.	사용 안 함	IP 주소	HTTPS	443		
VMware Identity Manager	사용 안 함	IP 주소	HTTPS	443	VMware Identity Manager	VMware Identity Manager

결과

완료된 구성은 다음 화면과 유사합니다.

New Virtual Server

Virtual Server *

Enable

Acceleration *

Disable

Application Profile:

vRealize Automation VA Web

Name: *

vs_vra-va-web_443

Description:

IP Address: *

10.10.10.8

Select IP Address

Protocol:

HTTPS

Port / Port Range: *

443

e.g.: 9000,9010-9020

Default Pool:

pool_vra-va-web_443

CANCEL

ADD

NSX-T 구성

5

구성하기 전에 NSX-T가 환경에 배포되어야 하고 로드 밸런서가 있는 Tier-1 게이트웨이가 네트워크를 통해 vRealize 구성 요소에 액세스할 수 있어야 합니다.

참고 NSX-T 버전 2.3은 빠른 TCP 가상 서버 풀에 대한 HTTPS 모니터를 지원하지 않습니다. HTTPS 모니터는 NSX-T 버전 2.4 이상에서 지원됩니다.

본 장은 다음 항목을 포함합니다.

- NSX-T 애플리케이션 프로파일 구성
- Workspace ONE Access에 대한 지속성 프로파일 구성
- NSX-T 액티브 상태 모니터 구성
- NSX-T 서버 풀 구성
- NSX-T 가상 서버 구성
- 로드 밸런서 구성
- 로드 밸런서에 가상 서버 추가

NSX-T 애플리케이션 프로파일 구성

HTTPS 요청을 위해 NSX-T에서 애플리케이션 프로파일을 추가할 수 있습니다.

절차

- 1 네트워크 > 로드 밸런싱 > 프로파일로 이동합니다.
- 2 프로파일 유형으로 애플리케이션을 선택합니다.
- 3 애플리케이션 프로파일 추가를 클릭하고 빠른 TCP 프로파일을 선택합니다.
- 4 프로파일의 이름을 입력합니다.

결과

HTTPS 요청에 대해 완성된 애플리케이션은 다음 화면과 유사합니다.

The screenshot shows the 'PROFILES' configuration page in vRealize Automation 8.1. The 'Select Profile Type' dropdown is set to 'APPLICATION'. Below this, there is a table of profiles. The first profile, 'vRA_HTTPS', is selected. Its configuration is as follows:

Name	Type	Idle Timeout (sec)	HA Flow Mirroring
vRA_HTTPS	Fast TCP	1800	Disabled

Below the table, the 'Description' field is empty. The 'Tags' section shows a 'Tag (Required)' field and a 'Scope (Optional)' field with a checkmark. A note states 'Maximum 30 tags are allowed.' At the bottom are 'SAVE' and 'CANCEL' buttons.

Workspace ONE Access에 대한 지속성 프로파일 구성

Workspace ONE Access에 대한 지속성 프로파일을 구성하려면 다음 단계를 수행합니다.

절차

- 1 네트워크 > 로드 밸런싱 > 프로파일로 이동합니다.
- 2 프로파일 유형으로 **지속성**을 선택합니다.
- 3 프로파일의 이름을 입력합니다.
- 4 지속성 항목 시간을 초과를 36000초로 설정합니다.

NSX-T 액티브 상태 모니터 구성

NSX-T에 대한 액티브 상태 모니터를 구성하려면 다음 단계를 수행합니다.

절차

- 1 네트워크 > 로드 밸런싱 > 모니터로 이동합니다.
- 2 액티브 모니터 추가를 클릭하고 **HTTP**를 선택합니다.
- 3 상태 모니터의 이름을 입력합니다.

4 다음 표에 설명된 대로 상태 모니터를 구성합니다.

표 5-1. 상태 모니터 구성

이름	모니터링 포트	간격	시간 초과	Fall Count	유형	메서드	URL	응답 코드	응답 본문
vRealize Automation	8008	3	10	3	HTTP	GET	/health	200	없음
vRealize Orchestrator 참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.	8008	3	10	3	HTTP	GET	/health	200	없음
VMware Identity Manager	443	3	10	3	HTTPS	GET	/SAAS/API/1.0/REST/system/health/heartbeat	200	OK

결과

완료된 구성은 다음 화면과 유사합니다.

LOAD BALANCERS VIRTUAL SERVERS SERVER POOLS PROFILES **MONITORS** [About](#)

Select Monitor Type **ACTIVE** ▾

[ADD ACTIVE MONITOR](#) ▾ [COLLAPSE ALL](#)

Name	Protocol	Monitoring Port	Monitoring Interval	Timeout Period (sec)	Server Pools
vRealize Automation VA *	HTTP	8008	3	10	

Description Fall Count

Tags ☒ Rise Count

Maximum 30 tags are allowed.

Additional Properties ▾

HTTP Request [Configure](#) HTTP Response [Configure](#)

[SAVE](#) [CANCEL](#)


HTTP Request and Response Configuration ×

Active Health Monitor -

HTTP Request Configuration

HTTP Response Configuration

HTTP Method Get ▼HTTP Request URL /healthHTTP Request Version 1.1 ▼ADD

Header Name	Header Value
 <p>Request Header not found</p>	

HTTP Request Body

CANCELAPPLYHTTP Request and Response Configuration ×

Active Health Monitor -

HTTP Request Configuration

HTTP Response ConfigurationHTTP Response Code 200 ×

1 or more response codes

HTTP Response Body

NSX-T 서버 풀 구성

vRealize Automation, vRealize Orchestrator, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 서버 풀을 구성해야 합니다.

절차

- 1 **네트워킹 > 로드 밸런싱 > 서버 풀**로 이동합니다.
- 2 **서버 풀 추가**를 클릭합니다.
- 3 풀의 이름을 입력합니다.
- 4 다음 표에 설명된 대로 풀을 구성합니다.

표 5-2. 서버 풀 구성

풀 이름	알고리즘	액티브 모니터	이름	IP	포트
vRealize Automation	최소 연결	vRealize Automation	VA1 VA2 VA3	IP	443
vRealize Orchestrator <u>참고</u> 외부 vRealize Orchestrator 인스턴스에만 사용합니다.	최소 연결	vRealize Orchestrator	VA1 VA2 VA3	IP	443
VMware Identity Manager	최소 연결	VMware Identity Manager	VA1 VA2 VA3	IP	443

결과

완료된 구성은 다음 화면과 유사합니다.

Configure Server Pool Members

Server Pool - pool_iaas-manager_443

☒ Enter individual members ☐ Select a group

ADD MEMBER

Name	IP	Port	Weight	State	Backup Member	Max Concurrent Connections
...	<input type="text"/>	443	1	Enabled	<input checked="" type="radio"/> Disabled	
...	<input type="text"/>	443	1	Enabled	<input checked="" type="radio"/> Disabled	

CANCEL **APPLY**

NSX-T 가상 서버 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 가상 서버를 구성해야 합니다.

절차

- 1 **네트워킹 > 로드 밸런싱 > 가상 서버**로 이동합니다.

2 가상 서버 추가를 클릭하고 계층을 선택합니다.

3 다음 표에 설명된 대로 가상 서버를 구성합니다.

표 5-3. 가상 서버 구성

이름	유형	애플리케이션 프로파일	IP 주소	포트	서버 풀	지속성 프로파일
vRealize Automation	L4 TCP	vRealize Automation	IP	443	vRealize Automation	없음
vRealize Orchestrator	L4 TCP	vRealize Orchestrator	IP	443	vRealize Orchestrator	없음
참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.						
VMware Identity Manager	L4 TCP	VMware Identity Manager	IP	443	VMware Identity Manager	VMware Identity Manager

결과

완료된 구성은 다음 화면과 유사합니다.

The screenshot shows the 'VIRTUAL SERVERS' tab in the vRealize Automation console. A virtual server named 'vs_vra-va-web_443' is selected, and its configuration details are displayed in a form. The form includes fields for Name, IP Address, Ports, Type, Load Balancer, and Server Pool. The 'Ports' field is set to 443, and the 'Type' is L4 TCP. The 'Load Balancer' is set to r34r3r4. The 'Server Pool' is set to pool_... The form also includes sections for Description, Persistence, Additional Properties, Max Concurrent Connections, Max New Connection Rate, Default Pool Member Ports, Admin State, and Tags. The 'Admin State' is set to Enabled, and the 'Tags' section shows a required tag and an optional scope. The 'SAVE' and 'CANCEL' buttons are at the bottom.

로드 밸런서 구성

각 vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항) 인스턴스에 대한 로드 밸런서를 지정합니다.

절차

- 1 **네트워킹 > 로드 밸런싱 > 로드 밸런서**로 이동합니다.
- 2 **로드 밸런서 추가**를 클릭합니다.
- 3 이름을 입력하고 적절한 **로드 밸런서 크기**(vRealize Automation 클러스터 크기에 따라 다름)를 선택합니다.
- 4 **Tier 1 논리적 라우터**를 선택합니다.

참고 NSX-T 버전 2.4에서는 모든 로드 밸런서 서버 풀에 대해 **Tier 1** 업링크의 IP 주소(또는 **Tier-1** 독립형 SR의 첫 번째 서비스 포트)를 사용하여 모니터 상태 점검이 수행됩니다. 이러한 IP 주소에서 서버 풀에 액세스할 수 있는지 확인하십시오.

결과

구성은 다음 화면과 유사해야 합니다.

The screenshot displays the 'LOAD BALANCERS' configuration interface. At the top, there's a navigation bar with tabs: 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS', 'PROFILES', 'MONITORS', and 'About'. Below the navigation bar is a button labeled 'ADD LOAD BALANCER'. The main form area contains several fields: 'Name' (vra75_lb), 'Size' (Small), and 'Tier-1 Gateway' (vRA-LB-Tier-1-Router). Below these are 'Description' (Enter Description), 'Tags' (Tag (Required), Scope (Optional)), 'Error Log Level', and 'Admin State' (toggle switch). At the bottom, there are 'SAVE' and 'CANCEL' buttons.

로드 밸런서에 가상 서버 추가

로드 밸런서를 구성한 후에는 가상 서버를 추가할 수 있습니다.

절차

- 1 **네트워킹 > 로드 밸런싱 > 가상 서버**로 이동합니다.
- 2 구성된 가상 서버를 편집합니다.

3 이전에 구성한 로드 밸런서를 **로드 밸런서**로 할당합니다.

결과

구성은 다음 화면과 유사해야 합니다.

Name	IP Address	Ports	Type	Load Balancer	...
vs_vra-va-web_443 *	192.168.205.10 * <small>e.g. 10.10.10.10</small>	443 x Enter Ports or Port Rang	L4 TCP	vRA_LB (x) v	p
<hr/> <div> <div>Description</div> <div>Enter Description</div> </div> <div> <div>Persistence</div> <div>Disabled v</div> </div> <div> <div>> Additional Properties</div> </div> <div> <div>SAVE</div> <div>CANCEL</div> </div>					
<div>Application Profile * vRA_HTTPS</div>					

F5 Big-IP LTM 구성

6

F5 디바이스를 구성하기 전에 네트워크를 통해 vRealize 구성 요소에 액세스할 수 있는 환경에 배포해야 합니다.

구성하려면 F5 디바이스가 다음 요구 사항을 충족해야 합니다.

- F5 디바이스는 물리적 또는 가상 디바이스일 수 있습니다.
- F5 LTM(Local Traffic module) 로드 밸런서를 단일 암 또는 다중 암 토폴로지에 배포할 수 있습니다.
- LTM이 명목상, 최소 또는 전용으로 구성되고 라이선스가 부여되어야 합니다. **시스템 > 리소스 프로비저닝**으로 이동하여 LTM을 구성할 수 있습니다.

11.x 이전의 F5 LTM 버전을 사용하는 경우 전송 문자열과 관련된 상태 모니터 설정을 변경해야 할 수도 있습니다. 다양한 버전의 F5 LTM에 대한 상태 모니터 전송 문자열을 설정하는 방법에 대한 자세한 내용은 [노드가 올바르게 응답하더라도 HTTP 상태 점검이 실패할 수 있음](#)을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Workspace ONE Access](#)에 대한 사용자 지정 지속성 프로파일 구성
- [모니터 구성](#)
- [F5 서버 풀 구성](#)
- [F5 가상 서버 구성](#)

Workspace ONE Access에 대한 사용자 지정 지속성 프로파일 구성

F5 로드 밸런서에 대한 지속성 프로파일을 구성할 수 있습니다.

절차

- 1 F5 디바이스에 로그인하고 **로컬 트래픽 > 프로파일 > 지속성**으로 이동합니다.
- 2 **생성**을 클릭합니다.
- 3 이름을 입력하고 드롭다운 메뉴에서 **소스 주소 선호도**를 선택합니다.
- 4 사용자 지정 모드를 사용하도록 설정합니다.
- 5 **시간 초과**를 36,000초로 설정합니다.

6 마침을 클릭합니다.

모니터 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 모니터를 추가해야 합니다.

절차

- 1 F5 로드 밸런서에 로그인하여 **로컬 트래픽 > 모니터**로 이동합니다.
- 2 **생성**을 클릭하고 이 표에 설명된 대로 모니터를 구성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 6-1. 모니터 구성

이름	유형	간격	시간 초과	전송 문자열.	수신 문자열.	별칭 서비스 포트
vRealize Automation	HTTP	3	10	GET/health HTTP/1.0\r\n\r\n	HTTP/1.(0 1) (200)	8008
vRealize Orchestrator <small>참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.</small>	HTTP	3	10	GET/health HTTP/1.0\r\n\r\n	HTTP/1.(0 1) (200)	8008
VMware Identity Manager	HTTPS	3	10	GET/ SAAS/API/1.0/ REST/system/ health/ heartbeat	ok\$	443

결과

구성은 다음 화면과 유사해야 합니다.

Local Traffic » Monitors » **New Monitor...**

General Properties

Name	vra_http_va_web
Description	
Type	HTTP
Parent Monitor	http

Configuration: Basic

Interval	3 seconds
Timeout	10 seconds
Send String	GET /health HTTP/1.0\r\n\r\n
Receive String	HTTP/1\.(0 1) (200)
Receive Disable String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	8008 Other: <input type="text"/>
Adaptive	<input type="checkbox"/> Enabled

Cancel Repeat Finished

F5 서버 풀 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 서비스 풀을 구성해야 합니다.

절차

- 1 F5 로드 밸런서에 로그인하여 **로컬 트래픽 > 풀**로 이동합니다.

- 2 **생성**을 클릭하고 이 표에 설명된 대로 풀을 구성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 6-2. 서버 풀 구성

이름	상태 모니터	로드 밸런싱 방법	노드 이름	주소	서비스 포트
vRealize Automation	vRealize Automation	최소 연결(멤버)	VA1 VA2 VA3	IP 주소	443
vRealize Orchestrator 참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.	vRealize Orchestrator	최소 연결(멤버)	VA1 VA2 VA3	IP 주소	443
VMware Identity Manager	VMware Identity Manager	최소 연결(멤버)	VA1 VA2 VA3	IP 주소	443

- 3 각 풀 멤버를 **새 노드**로 입력하고 **새 멤버** 그룹에 추가합니다.

결과

구성은 다음 화면과 유사해야 합니다.

Local Traffic » Pools : Pool List » **pl_vra-va-00_443**

⚙ Properties **Members** Statistics

Load Balancing

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

Update

Current Members

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group
<input type="checkbox"/>		dz-vra8-node1.sof-mbu.eng.vmware.com:443	192.168.10.30	443		No	1	0 (Active)
<input type="checkbox"/>		dz-vra8-node2.sof-mbu.eng.vmware.com:443	192.168.10.31	443		No	1	0 (Active)
<input type="checkbox"/>		dz-vra8-node3.sof-mbu.eng.vmware.com:443	192.168.10.32	443		No	1	0 (Active)

Enable Disable Force Offline Remove

F5 가상 서버 구성

vRealize Automation, VMware Identity Manager 및 외부 vRealize Orchestrator(선택 사항)에 대한 가상 서버를 구성해야 합니다.

절차

- 1 F5 로드 밸런서에 로그인하여 **로컬 트래픽 > 가상 서버**로 이동합니다.
- 2 **생성**을 클릭하고 이 표에 설명된 대로 가상 서버를 구성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 6-3. 가상 서버 구성

이름	유형	대상 주소	서비스 포트	소스 주소 변환	기본 풀	기본 지속성 프로파일
vRealize Automation	성능(계층 4)	IP 주소	443	자동 맵	vRealize Automation	없음
vRealize Orchestrator <small>참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.</small>	성능(계층 4)	IP 주소	443	자동 맵	vRealize Orchestrator	없음
VMware Identity Manager	성능(계층 4)	IP 주소	443	자동 맵	VMware Identity Manager	VMware Identity Manager

- 3 전체 보기 및 가상 서버의 상태를 보려면 **로컬 트래픽 > 가상 서버**를 선택합니다.

결과

구성은 다음 화면과 유사합니다.

General Properties

Name	vs_vra-v-a-00_443
Description	
Type	Performance (Layer 4)
Source Address	<input checked="" type="radio"/> Host <input type="radio"/> Address List
Destination Address/Mask	<input checked="" type="radio"/> Host <input type="radio"/> Address List 192.168.10.33
Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List 443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	fastL4
HTTP Profile (Client)	None
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Acceleration: Basic

iSession Profile	None
Rate Class	None

Resources

iRules	Enabled	Available
		/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtimAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Default Pool	+ pl_vra-v-a-00_443	
Default Persistence Profile	None	
Fallback Persistence Profile	None	

Cancel Repeat Finished

● vs_vra-v-a-00_443

STATS DIAGRAM

☐ List other virtual servers that share these pools ☐ List other pools that use these nodes

Virtual Server

Pools

Pool Members

● vs_vra-v-a-00_443
192.168.10.33:443

● pl_vra-v-a-00_443

● dz-vra8-node1.sof-mbu.er
192.168.10.30

● dz-vra8-node2.sof-mbu.er
192.168.10.31

● dz-vra8-node3.sof-mbu.er
192.168.10.32

Citrix ADC(NetScaler ADC) 구성

7

Citrix ADC를 구성하기 전에 vRealize 구성 요소에 액세스할 수 있는 환경에 NetScaler 디바이스가 배포되어 있는지 확인합니다.

구성하려면 Citrix ADC가 다음과 같은 요구 사항을 충족해야 합니다.

- 가상 또는 물리적 NetScaler를 사용할 수 있습니다.
- Citrix 로드 밸런서를 단일 암 또는 다중 암 토폴로지에 배포할 수 있습니다.
- **NetScaler > 시스템 > 설정 > 구성 > 기본 기능**으로 이동하여 로드 밸런서 및 SSL 모듈을 사용하도록 설정합니다.

본 장은 다음 항목을 포함합니다.

- Citrix 모니터 구성
- Citrix 서비스 그룹 구성
- Citrix 가상 서버 구성
- Workspace ONE Access에 대한 지속성 그룹 구성

Citrix 모니터 구성

다음 단계를 수행하여 Citrix 모니터를 구성할 수 있습니다.

절차

- 1 NetScaler 로드 밸런서에 로그인하여 **NetScaler > 트래픽 관리 > 로드 밸런싱 > 모니터**로 이동합니다.

- 2 **추가**를 클릭하고 이 표에 설명된 대로 모니터를 구성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 7-1. Citrix 모니터 구성

이름	유형	간격	시간 초과	재시도 횟수	성공 재시도 횟수	HTTP 요청/전송 문자열	응답 코드	수신 문자열	대상 포트	보안
vRealize Automation	HTTP	5	4	3	1	GET / health	200	없음	8008	아니요
vRealize Orchestrator	HTTP	5	4	3	1	GET / health	200	없음	8008	아니요
참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.										
VMware Identity Manager	HTTP-ECV	5	4	3	1	GET / SAAS/API/1.0/REST/system/health/heartbeat	200	ok	443	예

결과

구성은 다음 화면과 유사해야 합니다.

← Create Monitor

Name*
 ⓘ

Type*
 > ⓘ

Basic Parameters

Interval
 ▼

Response Time-out
 ▼ ⓘ

Response Codes

+

×

Custom Header

HTTP Request
 ⓘ

☐ Secure

Advanced Parameters

Destination IP

Destination Port
 ⓘ

Down Time
 ▼

TROFS Code

TROFS String

Dynamic Time-out
 ⓘ

Deviation
 ▼

Dynamic Interval

Retries
 ⓘ

Citrix 서비스 그룹 구성

다음 단계를 수행하여 서비스 그룹을 구성할 수 있습니다.

절차

- 1 NetScaler 로드 밸런서에 로그인하여 **NetScaler > 트래픽 관리 > 로드 밸런싱 > 서비스 그룹**으로 이동합니다.
- 2 **추가**를 클릭하고 이 표에 설명된 대로 서비스 그룹을 구성합니다.

표 7-2. 서비스 그룹 구성

이름	상태 모니터	프로토콜	SG 멤버	주소	포트
vRealize Automation	vRealize Automation	SSL 브리지	VA1 VA2 VA3	IP 주소	443
vRealize Orchestrator <small>참고 외부 vRealize Orchestrator 인스턴스에만 사용됩니다.</small>	vRealize Orchestrator	SSL 브리지	VA1 VA2 VA3	IP 주소	443
VMware Identity Manager	VMware Identity Manager	SSL 브리지	VA1 VA2 VA3	IP 주소	443

결과

구성은 다음 화면과 유사해야 합니다.

← Load Balancing Service Group

Basic Settings			
Name	pl_vra-va-00_443	Cache Type	SERVER
Protocol	SSL_BRIDGE	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

Service Group Members	
3 Service Group Members	>

Settings	
SureConnect	
Surge Protection	OFF
Use Proxy Port	YES
Down State Flush	ENABLED
Use Client IP	NO
Client Keep-alive	NO
TCP Buffering	YES
Client IP	DISABLED
Header	
AutoScale Mode	DISABLED

Monitors	
1 Service Group to Monitor Binding	>

Done

Citrix 가상 서버 구성

다음 단계를 수행하여 가상 서버를 구성할 수 있습니다.

절차

- 1 NetScaler 로드 밸런서에 로그인하여 **NetScaler > 트래픽 관리 > 로드 밸런싱 > 가상 서버**로 이동합니다.

- 2 **추가**를 클릭하고 이 표에 설명된 대로 가상 서버를 구성합니다. 아무것도 지정하지 않은 경우 기본값을 사용합니다.

표 7-3. 가상 서버 구성

이름	프로토콜	대상 주소	포트	로드 밸런싱 방법	서비스 그룹 바인딩
vRealize Automation	SSL 브리지	IP 주소	443	최소 연결	vRealize Automation
vRealize Orchestrator 참고 외부 vRealize Orchestrator 인스턴스에만 사용합니다.	SSL 브리지	IP 주소	443	최소 연결	vRealize Orchestrator
VMware Identity Manager	SSL 브리지	IP 주소	443	최소 연결	VMware Identity Manager

결과

구성은 다음 화면과 유사해야 합니다.

← Load Balancing Virtual Server

Load Balancing Virtual Server [Export as a Template](#)

Basic Settings

Name

vs_vra-va-00_443

Protocol

SSL_BRIDGE

State

● UP

IP Address

10.71.226.23

Port

443

Traffic Domain

0

Listen Priority

-

Listen Policy Expression

NONE

Redirection Mode

IP

Range

1

IPset

-

RHI State

PASSIVE

AppFlow Logging

ENABLED

Retain Connections on Cluster

NO

Services and Service Groups

No Load Balancing Virtual Server Service Binding

1 Load Balancing Virtual Server ServiceGroup Binding

Traffic Settings

Health Threshold

0

Client Idle Time-out

180

Minimum Autoscale Members

0

Maximum Autoscale Members

0

ICMP Virtual Server Response

PASSIVE

Priority Queuing

Sure Connect

Down State Flush

ENABLED

Layer 2 Parameters

OFF

Trofs Persistence

ENABLED

Done

Workspace ONE Access에 대한 지속성 그룹 구성

VMware Identity Manager에 대한 지속성 그룹을 구성하려면 다음 단계를 수행합니다.

절차

- 1 NetScaler에 로그인하고 **NetScaler > 트래픽 관리 > 로드 밸런싱 > 지속성 그룹**으로 이동합니다.
- 2 **추가**를 클릭합니다.
- 3 **시간 초과**를 36,000초로 설정합니다.
- 4 모든 관련 가상 서버를 VMware Identity Manager에 추가합니다.

참고 vRealize Automation 또는 vRealize Orchestrator 가상 서버는 추가하지 마십시오.

- 5 **확인**을 클릭합니다.

본 장은 다음 항목을 포함합니다.

- **OneConnect**를 **F5 BIG-IP**와 함께 사용하는 경우 프로비저닝 실패
- **F5 BIG-IP** 라이선스 제한 네트워크 대역폭

OneConnect를 F5 BIG-IP와 함께 사용하는 경우 프로비저닝 실패

가상 서버에 **F5 BIG-IP**와 함께 **OneConnect** 기능을 사용하면 프로비저닝 작업이 실패하는 경우가 있습니다.

OneConnect는 로드 밸런서에서 백엔드 서버로의 연결이 멀티플렉싱되고 재사용되도록 합니다. 이렇게 하면 서버의 로드가 줄어들고 복원력이 향상됩니다.

F5에서는 **SSL** 패스스루가 있는 가상 서버에서 **OneConnect**를 사용하지 않는 것이 좋으며, 프로비저닝 시도가 실패할 수 있습니다. 이 문제는 로드 밸런서가 기존 세션에서 새로운 **SSL** 세션을 설정하려고 시도하지만 백엔드 서버는 클라이언트가 기존 세션을 닫거나 재협상할 것으로 예상하며 이로 인해 연결이 끊어지기 때문에 발생합니다. 이 문제를 해결하려면 **OneConnect**를 사용하지 않도록 설정합니다.

- 1 **F5** 로드 밸런서에 로그인하고 **로컬 트래픽 > 가상 서버 > 가상 서버 목록**으로 이동합니다.
- 2 수정할 가상 서버의 이름을 클릭합니다.
- 3 **가속** 섹션에서 **OneConnect 프로파일**에 대해 **없음**을 선택합니다.
- 4 **마침**을 클릭합니다.

F5 BIG-IP 라이선스 제한 네트워크 대역폭

F5 BIG-IP 라이선스 제한을 초과하는 로드 밸런서 네트워크 트래픽으로 인해 프로비저닝 실패 또는 **vRealize Automation** 콘솔 페이지를 로드하는 데 문제가 발생할 수 있습니다.

BIG-IP 플랫폼에 이 문제가 발생하는지 확인하려면 **BIG-IP VE 시스템이 라이선스가 부여된 처리량 속도를 적용하는 방식**을 참조하십시오.