

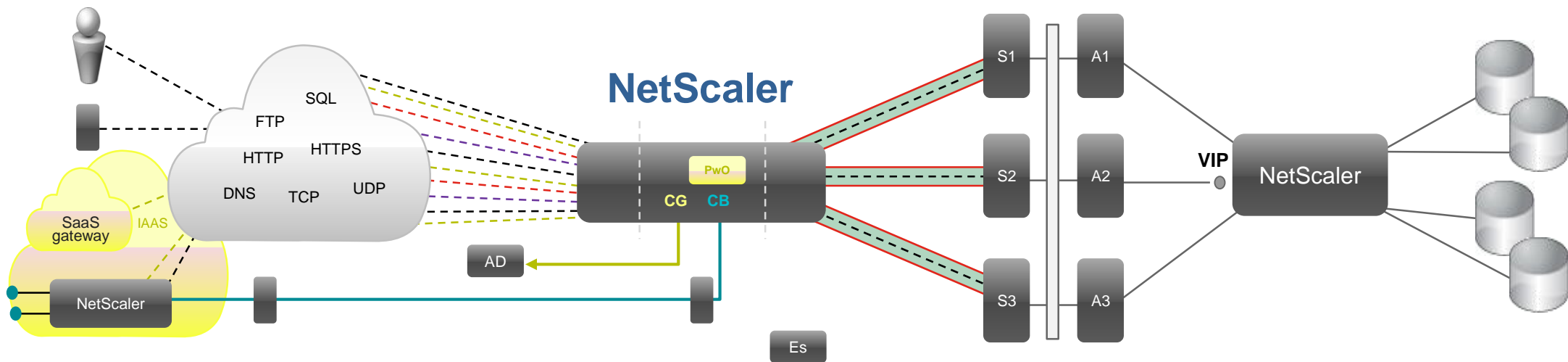


Citrix NetScaler Best Practices

Claudio Mascaro
Senior Systems Engineer
BCD-Sintrag AG

Agenda

- Deployment
- Initial Konfiguration
- Load Balancing
- NS Wizards, Unified GW, AAA Feature
- SSL



Acceleration

- TCP Offload
- HTTP Compression
- Caching (HTTP, SQL)
- TCP Optimization
- Rate Limiting
- SSL Offload
- Surge Protection
- Web 2.0 Push

Security

- Web Application Firewall
- L4-7 ACL
- DDoS Protections
- Rewrite + Responder
- SSL VPN
- NetScaler Gateway
- AAA TM-Auth. & SSO
- SAML 2.0 & Kerberos

Availability

- Server Loadbalancing (IPv4+6)
- Layer 7 Content Switching
- Advanced Health Check
- GSLB
- Traffic Domains & PBR
- Dyn. Routing, VLAN, LACP
- HTTP Callout
- CloudBridge
- DataStream

Management

- CLI/GUI/SNMP/Syslog
- API XML,NITRO,SOAP,REST
- AppFlow
- Command Center
- Web Logging (NSWL)
- Inbox Monitoring/Reporting
- Action Analytics
- NetScaler Insight Center
- Visualizer
- ACE Migration Tool**

Platforms

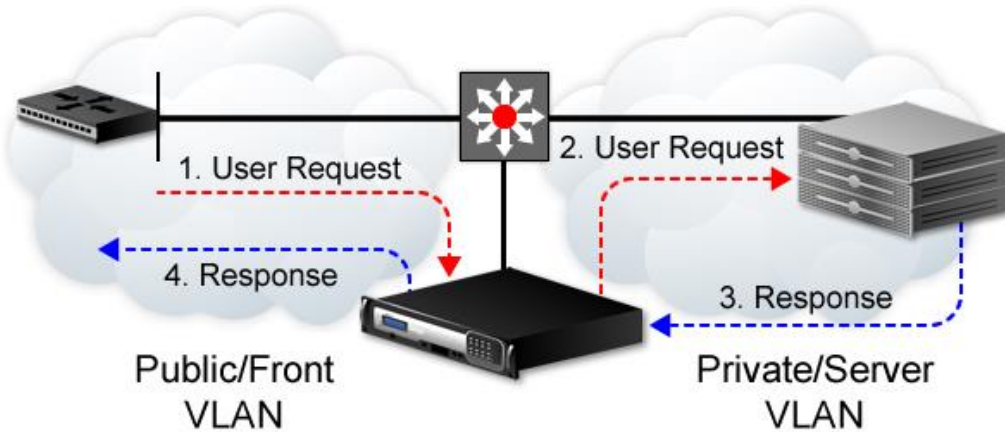
- VPX **XenServer**
VMWare
Hyper V
10, 200, 1G, 3G
- MPX & SDX
- Editions: Standard, Enterprise and Platinum, Express, Developer



Deployment

NetScaler Deployment

One-Arm Mode

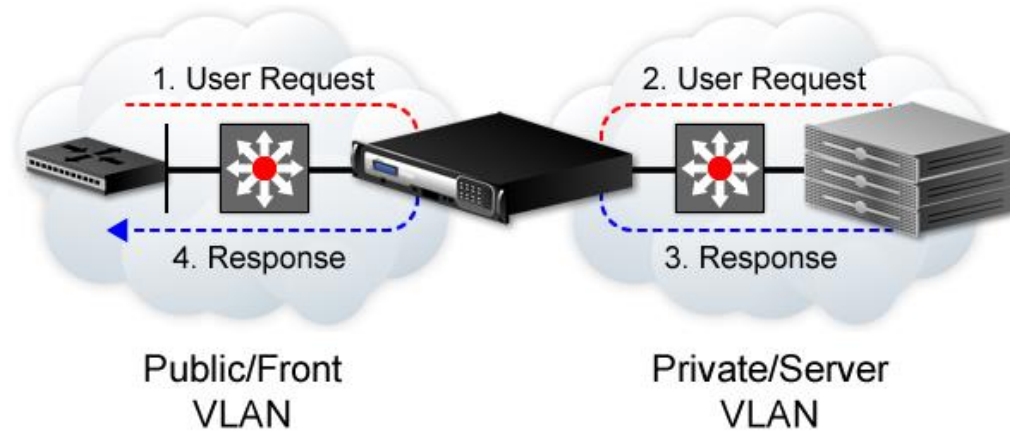


3 IP's im Minimum (Standalone)

- 1x NetScaler IP (NSIP)
- 1x Subnet IP (SNIP)
- 1x Virtual IP (VIP)

+ 1x NSIP im High Availability Mode

Two-Arm Mode



4 IP's im Minimum (Standalone)

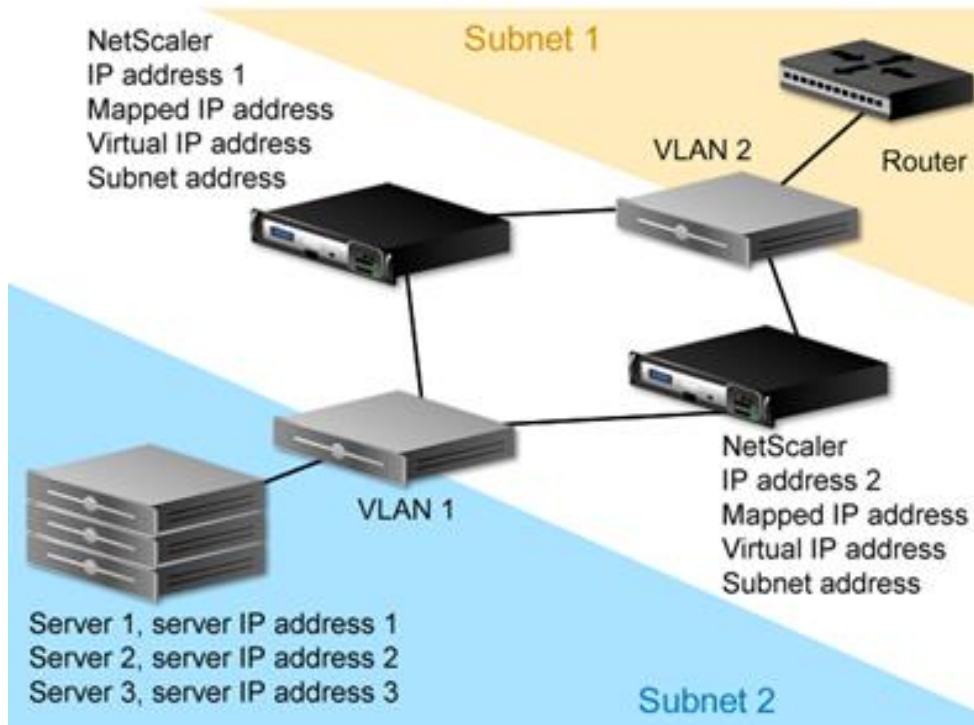
- 1x NetScaler IP (NSIP)
- 2x Subnet IP (SNIP, 1 pro Netz)
- 1x Virtual IP (VIP)

STATIC ROUTES zu Backend Server !!!

+ 1x NSIP im High Availability Mode

NetScaler High Availability

Typical Two-Arm Configuration



Beide NetScaler wie Eineiige Zwillinge !

- VPX – VPX or MPX – MPX
- Gleiche MPX Hardware
- Gleiche Platform Lizenz
- Gleiche Firmware Version
- Gleiche Interfaces und gleich gepatched

Arbeiten im Active/Passive Mode



Initial Configuration

Configuration

NetScaler VPX (1000) HA Status: Not Configured Info: NS11.0 63.16.nc Logout Citrix

Dashboard Configuration Reporting Documentation Downloads

NetScaler IP Address
IP address at which you access the NetScaler for configuration, monitoring, and other management tasks.
NetScaler IP Address: 172.27.140.65 Netmask: 255.255.252.0

Subnet IP Address
Specify an IP address for your NetScaler to communicate with the backend servers.
Subnet IP Address: 192.168.13.85, 172.27.140.66

Host Name, DNS IP Address, and Time Zone
Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located.
Host Name: socnsdmzprod DNS IP Address: 172.27.141.100, 172.27.141.101 Time Zone: GMT+01:00-CET-Europe/Zurich

Licenses
Upload licenses from your local computer or allocate licenses from the Citrix licensing portal.
There are 2 license file(s) present on this NetScaler.

NetScaler > System > NTP Servers

Add Edit Delete Action

Server Name	Minimum Poll Interval	Maximum Poll Interval	Preferred
172.27.141.100	6 (64 secs)	10 (1024 secs)	YES

← Back

Configure NTP Synchronization

Synchronization State*
 ENABLED DISABLED ?

OK Close

Licensing

NetScaler > System > System Information

System Information | System Sessions

System Upgrade | Reboot | Statistics | Call Home

System Information

NetScaler IP Address	172.27.140.65
Netmask	255.255.252.0
Node	Standalone
Time Zone	GMT+01:00-CET-Europe/Zurich
System Time	Fri, 6 Nov 2015 16:29:13 CET
Last Config Changed Time	Wed, 4 Nov 2015 17:04:38 CET
Last Config Saved Time	Wed, 4 Nov 2015 17:04:57 CET

Hardware Information

Platform	NetScaler Virtual Appliance 450000
Manufactured on	2/17/2009
CPU	1995 MHZ
Host Id	aaa226bc0ae1
Serial no	HE2H91SCZ6
Encoded serial no	98310000cb254307ee78

License Log File bei Troubleshooting:
`/var/log/license.log`

HA Status: Not Configured | Info: NS11.0 63.16.nc | Logout | CITRIX

User: nsroot

IP Address (Host Name): 172.27.140.65 (socnsdmzprod)

Version: NS11.0: Build 63.16.nc, Date: Oct 4 2015

Lizenz Server Host für:
NetScaler Gateway & Universal License

Lizenz Server Host für:
NetScaler Standard, Enterprise, Platinum, Options License

System Settings

System

- Licenses
- Settings**
- Diagnostics
- High Availability
- NTP Servers

NetScaler > System > Settings

Modes and Features

Configure Modes

Configure Basic Features

Configure Advanced Features

NetScaler > System > Licenses

Manage Licenses...

License type	Platinum
Load Balancing	✓
Content Switching	✓
Global Server Load Balancing	✓
Authentication, Authorization and Auditing	✓

Maximum NetScaler Gateway Users Allowed 45

- NetScaler Gateway License
- NetScaler Standard License
- NetScaler Enterprise Lic.
- NetScaler Platinum Lic.
- SSLVPN Universal License

Configure Basic Features

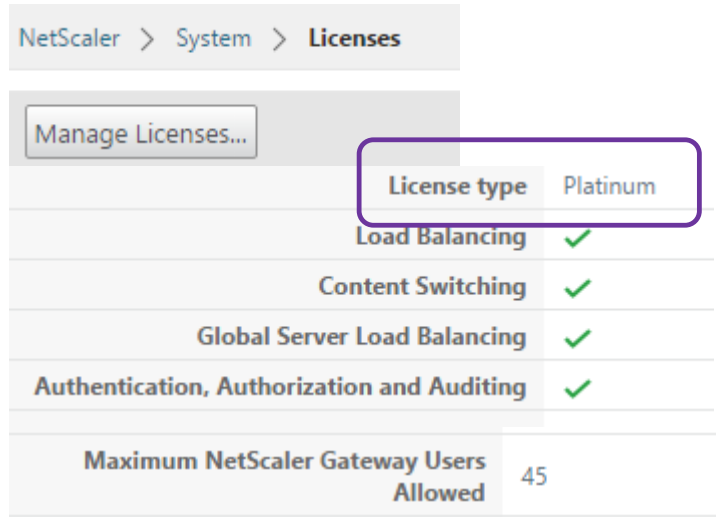
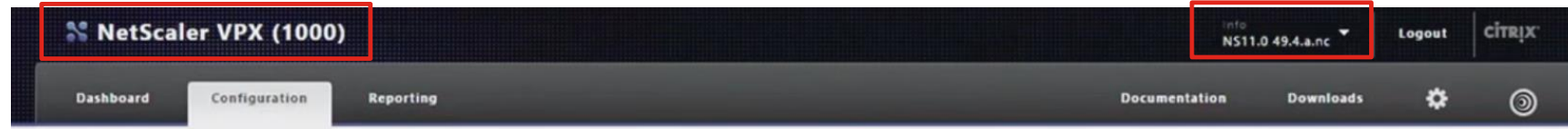
- SSL Offloading
- Load Balancing
- Content Filter
- Rewrite
- Authentication, Authorization and Auditing
- HTTP Compression
- Content Switching
- Integrated Caching
- NetScaler Gateway
- Application Firewall

Configure Advanced Features

- Surge Protection
- Priority Queuing
- Cache Redirection
- Web Logging
- RIP Routing
- IPv6 Protocol Translation
- EdgeSight Monitoring (HTML Injection)
- AppFlow
- ISIS Routing
- AppQoS
- Content Accelerator
- vPath
- Sure Connect
- Http Dos Protection
- Global Server Load Balancing
- OSPF Routing
- BGP Routing
- Responder
- NetScaler Push
- Cloud Bridge
- Callhome
- Front End Optimization
- Large Scale NAT
- RDP Proxy

https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet.pdf

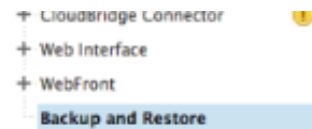
Version



1 Download Firmware

Firmware
NetScaler Release 11.0 Build 63.16 F
Oct 8, 2015

2 Backup



Backup

NetScaler Version
NS11.0: Build 62.10.nc, Date: Aug 8 2015, 23:00:46

File Name*

Type*

Comment

3 HA-Disable

```
set node -hasync disable
```

4 Upload Firmware

5 Update

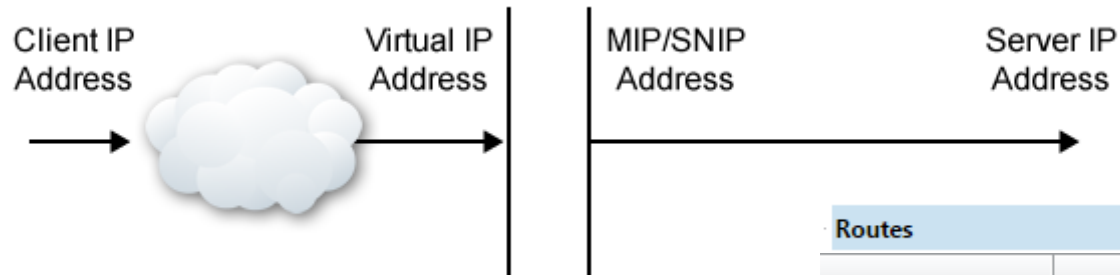
```
shell  
cd /var/install/  
tar -zxvf yourfile  
./installns
```

NetScaler Architektur



2 separate TCP Sessions !

- Client zu Virtual IP
- Subnet IP zu Backend Server



Routes

Network	Netmask	Gateway/Owned IP/Name	State	Distance	Flags
0.0.0.0	0.0.0.0	192.168.13.1	UP	1	STATIC
127.0.0.0	255.0.0.0	127.0.0.1	UP	0	PERMANENT
172.27.140.0	255.255.252.0	172.27.140.65	UP	0	DIRECT

Network

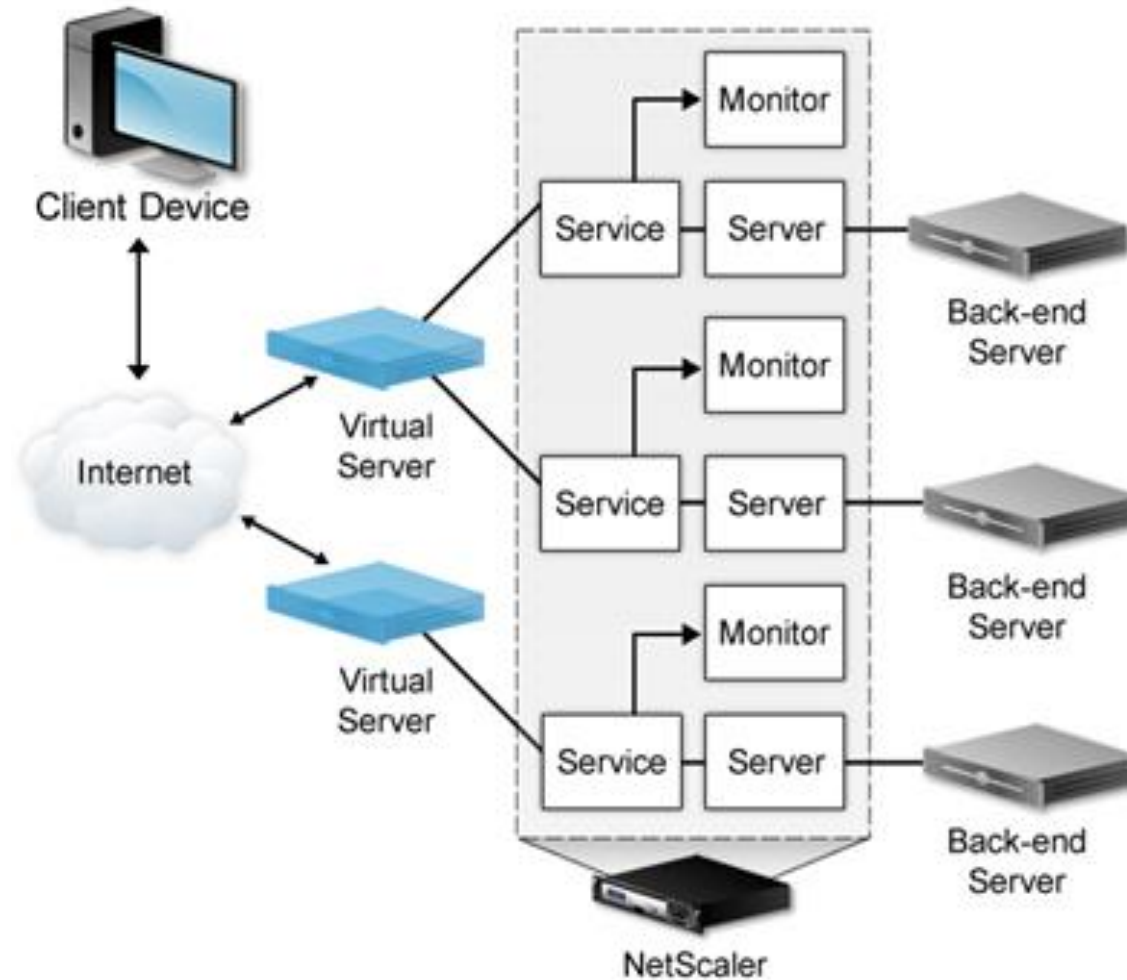
IPs

▶ 172.27.140.61	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED
▶ 172.27.140.65	Enabled	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.27.140.66	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-



Load Balancing

Loadbalancing und Entities



Loadbalancing vServer, Services, Servers

Steps

Load Balancing	▶ SOCXDC01	● Enabled	172.27.141.110
Virtual Servers	▶ SOCXDC02	● Enabled	172.27.141.111
Services	▶ SOCXAX01	● Enabled	172.27.141.113
Service Groups	▶ SOCXAX02	● Enabled	172.27.141.114
Monitors			
Metric Tables			
Servers			
Persistency Groups			

1

Load Balancing	▶ SVC-XDXML-1	● Up	172.27.141.110	443	SSL
Virtual Servers	▶ SVC-XDXML-2	● Up	172.27.141.111	443	SSL
Services	▶ SVC-XAXML-1	● Up	172.27.141.113	80	HTTP
	▶ SVC-XAXML-2	● Up	172.27.141.114	80	HTTP

NS über Firewall zum Backend ist offen (SubnetIP)
 😊 😊 😊

2

Load Balancing	▶ LB-vsrv-XDXML-2	● Up	● Up	192.168.168.111	443	SSL	LEASTCONNECTION
Virtual Servers	▶ LB-vsrv-XDXML-1	● Up	● Up	192.168.168.110	443	SSL	LEASTCONNECTION
	▶ LB-vsrv-XAXML-2	● Up	● Up	192.168.168.114	80	HTTP	LEASTCONNECTION
	▶ LB-vsrv-XAXML-1	● Up	● Up	192.168.168.113	80	HTTP	LEASTCONNECTION

3

Loadbalancing vServer

Load Balancing	▶ LB-vsrv-XDXML-2	● Up	● Up	192.168.168.111	443	SSL	LEASTCONNECTION
Virtual Servers	▶ LB-vsrv-XDXML-1	● Up	● Up	192.168.168.110	443	SSL	LEASTCONNECTION
	▶ LB-vsrv-XAXML-2	● Up	● Up	192.168.168.114	80	HTTP	LEASTCONNECTION
	▶ LB-vsrv-XAXML-1	● Up	● Up	192.168.168.113	80	HTTP	LEASTCONNECTION

Load Balancing Method*

LEASTCONNECTION ▼

ROUNDROBIN
LEASTCONNECTION
LEASTRESPONSETIME
DESTINATIONIPHASH
SOURCEIPHASH
LEASTBANDWIDTH
LEASTPACKETS
SRCIPDESTIPHASH
LRTM
SRCIPSRCPORHASH
CUSTOMLOAD
LEASTREQUEST
URLHASH
DOMAINHASH
CALLIDHASH
TOKEN

Persistence*

SOURCEIP ▼

NONE
SOURCEIP
COOKIEINSERT
SSLSESSION
RULE
URLPASSIVE
CUSTOMSERVERID
DESTIP
SRCIPDESTIP

Alle Zugriffe von Netscaler auf Backend Server, sollten Loadbalanced werden.

- DNS Server
- AD / Radius Server
- Citrix Webinterface
- Citrix Storefront
- Citrix Datacollector
- Citrix Delivery Controller
- Citrix XenMobile
- Citrix ShareFile
- Microsoft Exchange Server
- Etc.

Loadbalancing Monitors

Load Balancing

- Virtual Servers
- Services
- Service Groups
- Monitors**

▶ XDXML-Mon	● Enabled	HTTP
▶ XAXML-Mon	● Enabled	CITRIX-XML-SERVICE

← Back

Configure Monitor

Name
XAXML-Mon

Type
CITRIX-XML-SERVICE ▼

Standard Parameters | Special Parameters

Custom Header

Application Name
XA65

Type*

- PING
- LDAP
- POP3
- CITRIX-XML-SERVICE**
- CITRIX-WEB-INTERFACE
- DNS-TCP
- RTSP
- ARP
- CITRIX-AG
- CITRIX-AAC-LOGINPAGE
- CITRIX-AAC-LAS
- CITRIX-XD-DDC
- ND6
- CITRIX-WI-EXTENDED
- CITRIX-XNC-ECV
- CITRIX-XDM
- DIAMETER
- RADIUS_ACCOUNTING
- STOREFRONT
- APPC**
- SMPP

Auswahl

HTTP to HTTPS Redirection with Responder Policy

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

Basic Settings

Name **VSRV-HTTPtoHTTPS**
Protocol **HTTP**
State **Up**
IP Address **192.168.13.54**
Port **80**
Traffic Domain **0**

Services and Service Groups

1 Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

Policies

Request Policies

1 Responder Policy

Configure Responder Policy

Name

Action*
 +

Log Action
 +

AppFlow Action
 +

Undefined-Result Action*

Expression*

Ist die Verbindung nicht SSL

Configure Responder Action

Name

Type

Expression*

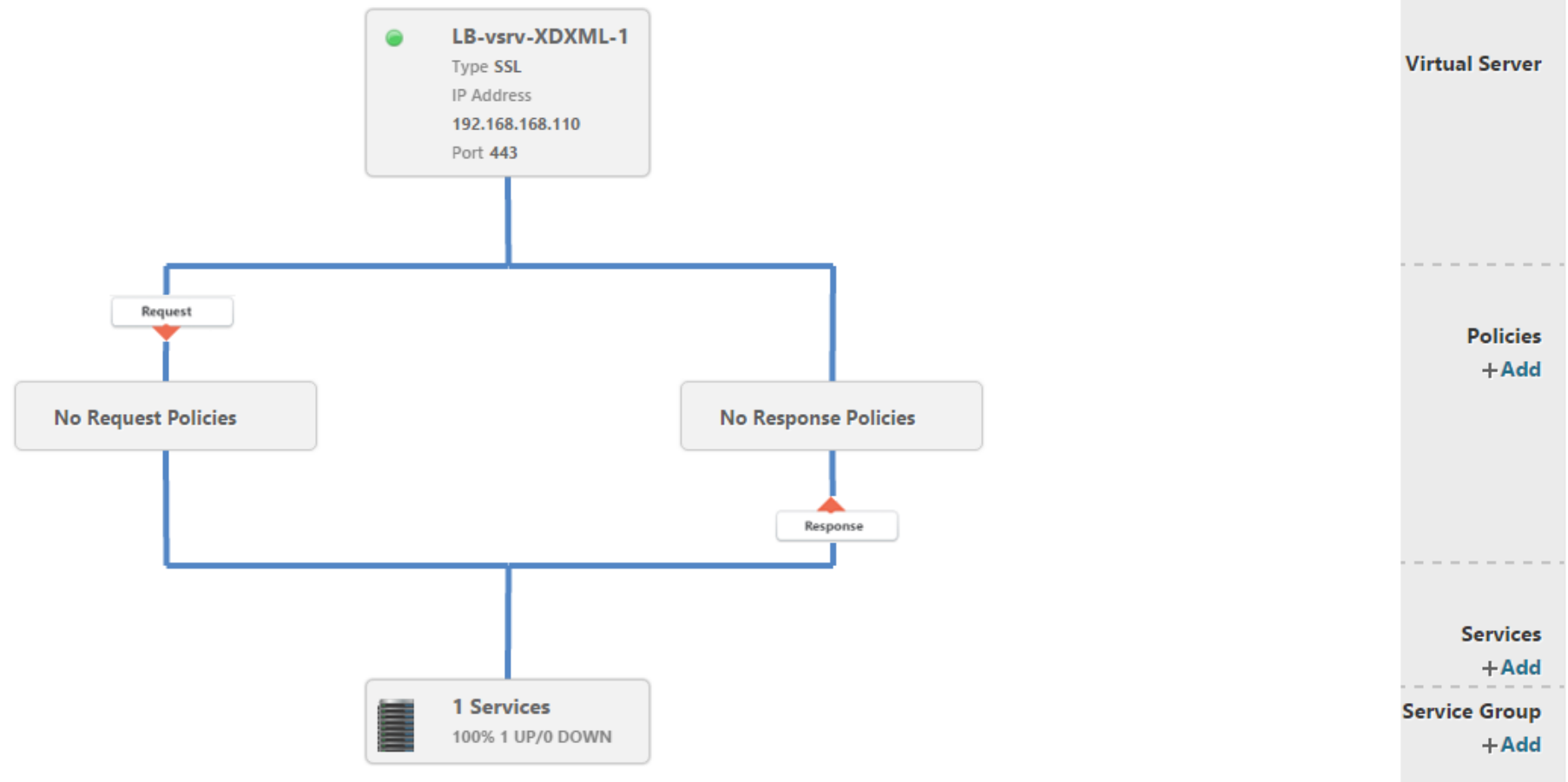
Redirect Expression zu HTTPS

Loadbalancing Visualizer

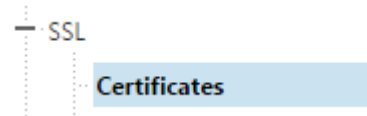
LB Visualizer

The visualizer for load balancing displays a graphical view of the configuration of the selected virtual server. Click an entity to display details and, if necessary, change them. You can also add new entities.

Visualizer - LB-vsrv-XDXML-1



Zertifikate



Name	Days to Expire	Status
wild-so-2017-cert	512	Valid
socxmdeviceCA,pem_CERT_KEY_ic1	8135	Valid
socxmdeviceCA,pem_CERT_KEY	8135	Valid
RapidSSL-SHA256-CA-G3-cert	2383	Valid
ns-server-certificate	5720	Valid
Geotrust-Global-CA-cert	1014	Valid
Equifax-cert	1016	Valid

Server Zertifikat mit Private Key

Intermediate und Root CA Zertifikate

Configure Certificate-key pair	
Certificate-Key Pair Name	CA Certificate Name
RapidSSL-SHA256-CA-G3-cert	Geotrust-Global-CA-cert
wild-so-2017-cert	RapidSSL-SHA256-CA-G3-cert

Cert Links !!

Tools

- Create Diffie-Hellman (DH) key
- Import PKCS#12
- Export PKCS#12
- Manage Certificates / Keys / CSRs
- Start SSL certificate, key file synchronization for HA
- Start SSL certificate, key file synchronization for Cluster
- OpenSSL interface



NetScaler Wizards Unified Gateway AAA Feature

NetScaler Wizards

Wizards

- + System
- + AppExpert
- + Traffic Management
- + Optimization
- + Security
- + NetScaler Gateway
- + Authentication
- [Show Unlicensed Features](#)

Integrate with Citrix Products

- XenMobile
- XenApp and XenDesktop
- Unified Gateway

NetScaler > System > System Information

System Information | System Sessions

System Upgrade | Reboot | Statistics | Call Home

System Information

NetScaler IP Address	172.27.140.65
Netmask	255.255.252.0
Node	Standalone
Time Zone	GMT+01:00-CET-Europe/Zurich
System Time	Tue, 10 Nov 2015 10:46:30 CET
Last Config Changed Time	Tue, 10 Nov 2015 10:26:29 CET
Last Config Saved Time	Wed, 4 Nov 2015 17:04:57 CET

Hardware Information

Platform	NetScaler Virtual Appliance 450000
Manufactured on	2/17/2009
CPU	1995 MHZ
Host Id	aaa226bc0ae1
Serial no	HE2H91SCZ6

XenMobile Wizard

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action

Name	State	IP Address	Port	Protocol
UG_VPN_myUnifiedGateway	Up	0.0.0.0	0	SSL
_XM_XenMobileGateway	Up	192.168.13.49	443	SSL
_XM_XenMobileGateway_CB	Up	172.27.140.60	443	SSL

Wizard erstellt:

- 3x LB vServer
- 1x GW vServer
- 3x Session Policies
- Authentication Server

Gateway vServer (MAM)
Externer Zugriff

Load Balancing

Virtual Servers

_XM_MAM_LB_172.27.140.61_8443	Up	Up	172.27.140.61	8443	SSL
_XM_LB_MDM_XenMobileMDM_192.168.13.48_443	Up	Up	192.168.13.48	443	SSL
_XM_LB_MDM_XenMobileMDM_192.168.13.48_8443	Up	Up	192.168.13.48	8443	SSL

Mobile App Mgmt. (MAM)
Interner Zugriff von GW Session Pol.

Mobile Device Mgmt. (MDM)
Externer Zugriff

NetScaler > NetScaler Gateway > Policies > NetScaler Gateway Session Policies and Profiles > Session Policies

Session Policies Session Profiles

PL_OS_192.168.13.49	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && RE...	AC_OS_192.168.13.49_A_
PL_WB_192.168.13.49	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver &...	AC_WB_192.168.13.49_A_
PL_AG_PLG_192.168.13.49	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver &...	AC_AG_PLG_192.168.13.49_A_

NetScaler > NetScaler Gateway > Policies > Authentication > LDAP > Policies

Name	Expression	Request Server
soadc01	ns_true	soadc01-srv

Unified Gateway

Eine IP für mehrere Zugriffe

- Exchange 2013
- Citrix Insight
- Datanow
- NetScaler Gateway
- Etc.

Content Switching

Virtual Servers

NetScaler > Traffic Management > Content Switching > Content Switching Virtual Servers

Add Edit Delete Statistics Action

Name	State	IP Address	Port	Protocol
myUnifiedGateway	Up	192.168.13.54	443	SSL

1 IP für 4 oder mehr verschiedene Backend LB vServer

Content Switching Virtual Server Content Switching Policy Binding

Content Switching Virtual Server Content Switching Policy Binding

Add Binding Unbind Edit

Priority	Policy Name	Expression	Action
110	UG_CSPOL_EXCH_AUTODISCOVER	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_AUTODISCOVER
120	UG_CSPOL_EXCH_ECP	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_ECP
130	UG_CSPOL_EXCH_EAS	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_EAS
140	UG_CSPOL_EXCH_OA	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_OA
150	UG_CSPOL_EXCH_OAB	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_OAB
160	UG_CSPOL_EXCH_EWS	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_EWS
170	UG_CSPOL_EXCH_OWA	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_EXCH_OWA
200	UG_CSPOL_Datanow	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_Datanow
210	UG_CSPOL_Insight	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_LBPOL_Insight
63000	UG_CSPOL_myUnifiedGateway	HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE)...	UG_CSACT_myUnifiedGateway

Loadbalanced vServer

Exchange 2013

Datanow Webserver

Insight Webserver

NetScaler GW

Action von Content Switching zeigt auf LB vServer & NS Gateway

NetScaler > Traffic Management > **Load Balancing > Virtual Servers**

Add Edit Delete Enable Disable Statistics Action

Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence
▶ VSRV-HTTPtoHTTPS	Up	Up	192.168.13.54	80	HTTP	LEASTCONNECTION	NONE
▶ VSRV-EXCH-OWA-FOR-GW	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	NONE
▶ VSRV-EXCH-OWA	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	COOKIEINSERT
▶ VSRV-EXCH-OAB	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	NONE
▶ VSRV-EXCH-OA	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	NONE
▶ VSRV-EXCH-EWS	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	NONE
▶ VSRV-EXCH-ECP	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	COOKIEINSERT
▶ VSRV-EXCH-EAS	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	NONE
▶ VSRV-EXCH-AUTODISCOVER	Up	Up	0.0.0.0	0	SSL	LEASTCONNECTION	NONE

NetScaler > NetScaler Gateway > **NetScaler Gateway Virtual Servers**

Add Edit Delete Statistics Visualizer Action

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
UG_VPN_myUnifiedGateway	Up	0.0.0.0	0	SSL	0	0

Die Expression definiert wohin...

Expression* **Outlook Web Access**

Operators Saved Policy Expressions Frequently Used Expressions

```
HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH("mail") && HTTP.REQ.HEADER("User-Agent").SET_TEXT_MODE(IGNORECASE).CONTAINS("Mozilla")
```

Expression* **Outlook Anywhere**

Operators Saved Policy Expressions Frequently Used Expressions

```
HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH("mail") && HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS("/rpc")
```

Expression* **NetScaler Gateway**

Operators Saved Policy Expressions Frequently Used Expressions

```
HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH("cloud") && (is_vpn_url || HTTP.REQ.URL.PATH.SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Citrix/Store"))
```

AAA Feature (z.B. NS als TMG Ersatz für Exch.2013)

NetScaler > Security > AAA - Application Traffic > Authentication Virtual Servers

Add Edit Delete Statistics Visualizer Action

Name	State	IP Address	Port
AAA-VSRV-EXCH	Up	192.168.13.58	443

Basic Settings

Name: AAA-VSRV-EXCH
Authentication Domain: aaa.s[redacted]e.ch
IP Address: 192.168.13.58
Port: 443

Session Policies | Session Profiles

Add Edit Delete Action

Name	Expression	Request Profile
SETTMSSESSPARAMS_POL	ns_true	SETTMSSESSPARAMS_ACT
owa-session-pol	ns_true	owa-session-prof

Primary Authentication

2 LDAP Policies

Configure Session Profile

Name: owa-session-prof

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

Setting	Value	Override Global
Session Time-out (mins)	30	<input checked="" type="checkbox"/>
Default Authorization Action*	ALLOW	<input checked="" type="checkbox"/>
Single Sign-on to Web Applications*	ON	<input checked="" type="checkbox"/>
Credential Index*	PRIMARY	<input checked="" type="checkbox"/>
Single Sign-on Domain	software-online.ch	<input checked="" type="checkbox"/>
HTTPOnly Cookie*	NO	<input checked="" type="checkbox"/>
Enable Persistent Cookie*	ON	<input checked="" type="checkbox"/>
Persistent Cookie Validity	30	<input checked="" type="checkbox"/>

User – NS – CSW – LB – AAA – LB – Exchange Server

NetScaler > Traffic Management > Load Balancing > Virtual Servers

Add Edit Delete Enable Disable Statistics Action

Name	State	Effective State	IP Address	Port	Protocol
VSRV-EXCH-OWA 3	Up	Up	0.0.0.0	0	SSL

Authentication

Form Based Authentication **ON** Authentication FQDN **aaa. domain.ch**
 Authentication Virtual Server - Authentication Profile

AAA vServer

NetScaler > Security > AAA - Application Traffic > Authentication Virtual Servers

Add Edit Delete Statistics Visualize Action **5**

Name	State	IP Address	Port	Protocol
AAA-VSRV-EXCH	Up	192.168.13.58	443	SSL

Basic Settings

Name **AAA-VSRV-EXCH** IP Address **192.168.13.58**
 Authentication Domain **aaa. domain.ch** Port **443**

Session Policies Session Profiles

Add Edit Delete Action

Name	Expression	Request Profile
SETTMSESSPARAMS_POL	ns_true	SETTMSESSPARAMS_ACT
owa-session-pol	ns_true	owa-session-prof

Primary Authentication
 2 LDAP Policies

NetScaler > Traffic Management > Content Switching >

Add Edit Delete Statistics

Name	State
myUnifiedGateway 2	Up



https://Mail.domain.com

Exchange 2013 Backend Server

9
Publish Mail Content

AD Auth

7
True

8



6

Single Sign On



SSL

SSL A-Rating Konfiguration

- Traffic Management
 - + Load Balancing
 - + Content Switching
 - + Cache Redirection 
 - + DNS
 - + GSLB 
 - + **SSL**
 - + Subscriber
 - + Service Chaining
- + Optimization
- + Security
- + NetScaler Gateway
- + Authentication

Getting Started

- Server Certificate Wizard
- Client Certificate Wizard
- Intermediate-CA Certificate Wizard
- Root-CA Certificate Wizard
- CRL Management

SSL Keys

- Create RSA Key
- Create DSA Key

Policy Manager

- SSL Policy Manager

SSL Certificates

- Create Certificate Signing Request (CSR) Certificate
- Create and Install a Server Test Certificate
- Install Certificate (HSM)

Tools

- Create Diffie-Hellman (DH) key
- Import PKCS#12
- Export PKCS#12
- Manage Certificates / Keys / CSRs
- Start SSL certificate, key file synchronization for HA
- Start SSL certificate, key file synchronization for Cluster
- OpenSSL interface

Settings

- Change advanced SSL settings

Configure SSL DH Param

DH Filename (with path)

DH Parameter Size (Bits)

DH Generator

2 5



SSL Renegotiation

SSL

SSL Keys

[Create RSA Key](#)

[Create DSA Key](#)

Policy Manager

[SSL Policy Manager](#)

Tools

[Create Diffie-Hellman \(DH\) key](#)

[Import PKCS#12](#)

[Export PKCS#12](#)

[Manage Certificates / Keys / CSRs](#)

[Start SSL certificate, key file synch](#)

[Start SSL certificate, key file synch](#)

[OpenSSL interface](#)

Settings

[Change advanced SSL settings](#)

Change Advanced SSL Settings

SSL quantum size (KBytes)

8

Max CRL memory size (MBytes)

256

Encryption trigger timeout (10 ms ticks)

100

Encryption trigger packet count

45

Deny SSL Renegotiation

FRONTEND_CLIENT

NO
FRONTEND_CLIENT
FRONTEND_CLIENTSERVER
ALL
NONSECURE
Unicode

PUSH encryption trigger timeout (ms)

1

Crypto Device Disable Limit

0

Undefined Control Action

CLIENTAUTH

Undefined Data Action

NOOP

Strict CA checks

Drop requests for SNI enabled SSL sessions if host header is absent

Send Close-Notify

vServer SSL Settings

SSL Parameters

Enable DH Param

Refresh Count

File Path*
 ▼

Enable DH Key Expire Size Limit
 Enable Ephemeral RSA
 Enable Session Reuse

Time-out

Enable Cipher Redirect
 SSLv2 Redirect
 Client Authentication

SSL Redirect
 SNI Enable
 Send Close-Notify

Clear Text Port

PUSH Encryption Trigger
 ▼

Protocol

SSLv2 SSLv3 TLSv1 TLSv11 TLSv12

NS 11.0 auch bei VPX TLSv11 und TLS12 verfügbar

SSL Ciphers

Configured (3)

Remove All

TLS1-ECDHE-RSA-AES256-SHA	—
TLS1-DHE-RSA-AES-256-CBC-SHA	—
TLS1-AES-256-CBC-SHA	—

ECC Curve

4 ECC Curves

SSL Rating A 😊

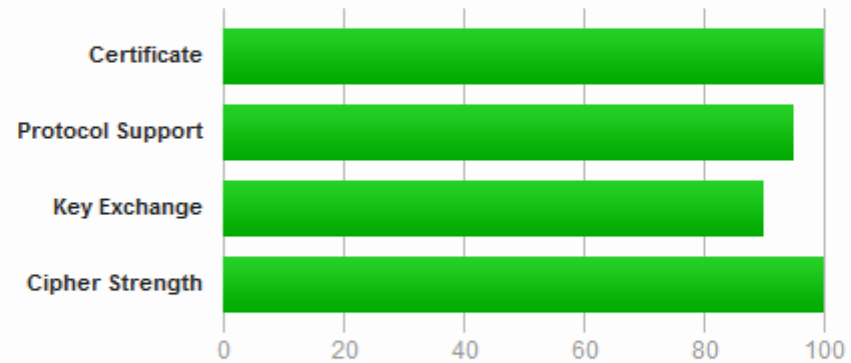
SSL Report: cloud.██████████.ch (██████████54)

Assessed on: Tue, 10 Nov 2015 09:29:11 UTC | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. [MORE INFO »](#)

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

Vielen Dank

