NetScaler Authentication

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts the most accurate results. This document provides tips and best practices for setting up NetScaler authentication.

NetScaler Authentication for VM

Why use authentication?

With authentication, we can remotely log in to each target system with credentials that you provide, and because we're logged in, we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? It's recommended for vulnerability scans.

What privileges are needed for vulnerability scans?

The account you provide must be able to perform certain commands like 1) execute "uname" to detect the platform for packages, 2) read /etc/redhat-release and execute "rpm" (if the target is running Red Hat), and 3) read /etc/debian_version and execute "dpkg" (if the target is running Debian).

There are many more commands that must be performed. The *NIX Authenticated Scan Process and Commands article describes the types of commands run and gives you an idea of the breadth and scope of the commands executed. It includes a list of commands that a Qualys service account might run during a scan. Not every command is run every time, and *nix distributions differ. This list is neither comprehensive nor actively maintained.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

What are the steps?

First, set up a NetScaler user account and privileges on target hosts (we'll help you with this below). Then, using Qualys Vulnerability Management, complete these steps: 1) Add Unix authentication records (NetScaler uses Unix Authentication record for authentication. Use new Authentication and select Unix Authentication). 2) Launch a vulnerability scan. 3) Run the Authentication Report to view the detailed report for each scanned host. For vulnerability scans, you must enable authentication in an option profile and then select the profile at scan time. Go

to Scans > Option Profiles. Edit an option profile (or create a new one), go to the Scan section and select each type of authentication you want to use.

Can I have multiple records?

Yes. You can create multiple records with different IP addresses. Each IP address may be included in one Unix type record.

NetScaler Authentication for PC

Why use authentication?

With authentication, we can remotely log in to each target system with credentials that you provide, and because we're logged in, we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? It's required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

What are the steps?

First, set up a NetScaler user account and privileges on target hosts (we'll help you with this below). Then, using Qualys Policy Compliance, complete these steps: 1) Add Unix authentication records (NetScaler uses Unix Authentication record for authentication and assessment of controls, please use new Authentication and select Unix Authentication). 2) Launch a compliance scan. 3) Run the Authentication Report to view the authentication status for each scanned host.

Can I have multiple records?

Yes. You can create multiple records with different IP addresses. Each IP address may be included in one Unix type record.

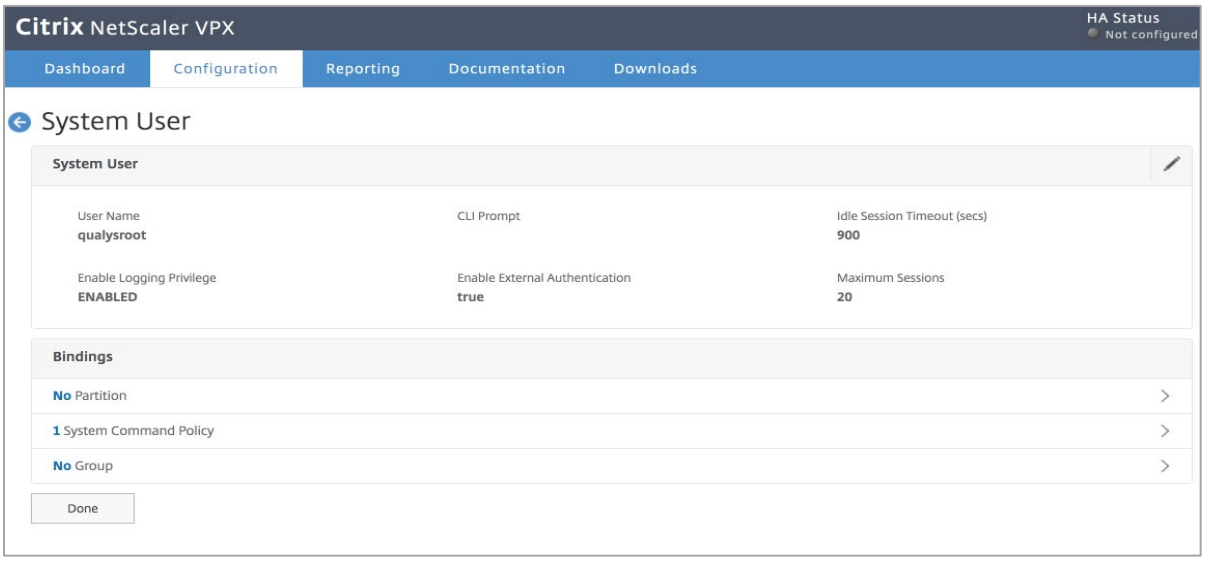
NetScaler Setup

In order for scans to work properly, the following account and privileges must exist prior to running the scan.

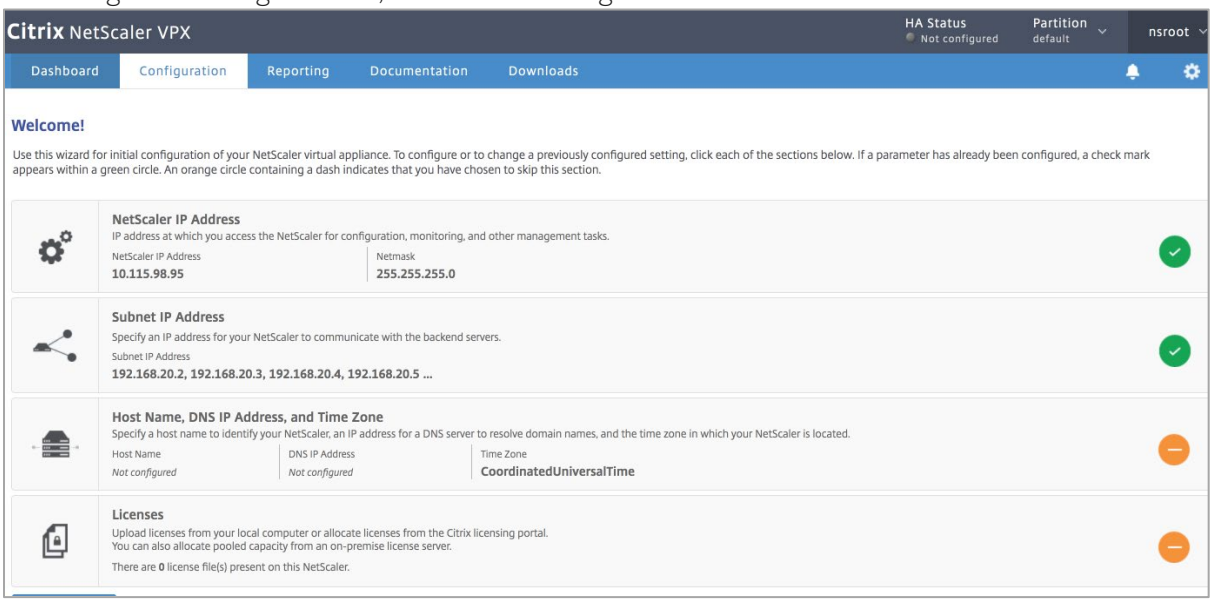
1) Create a User Account on NetScaler Instance

Create a user account called **scanuser** which is a category created by the user for scanning the NetScaler devices.

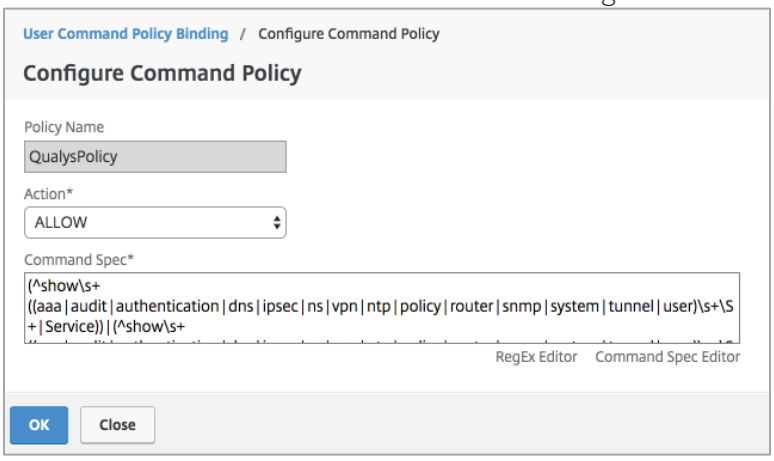
a. You can use any user name string for the user name. You'll need to provide the same user name in the Unix Authentication record in the Qualys UI.



b. To change the configurations, use the following screen:



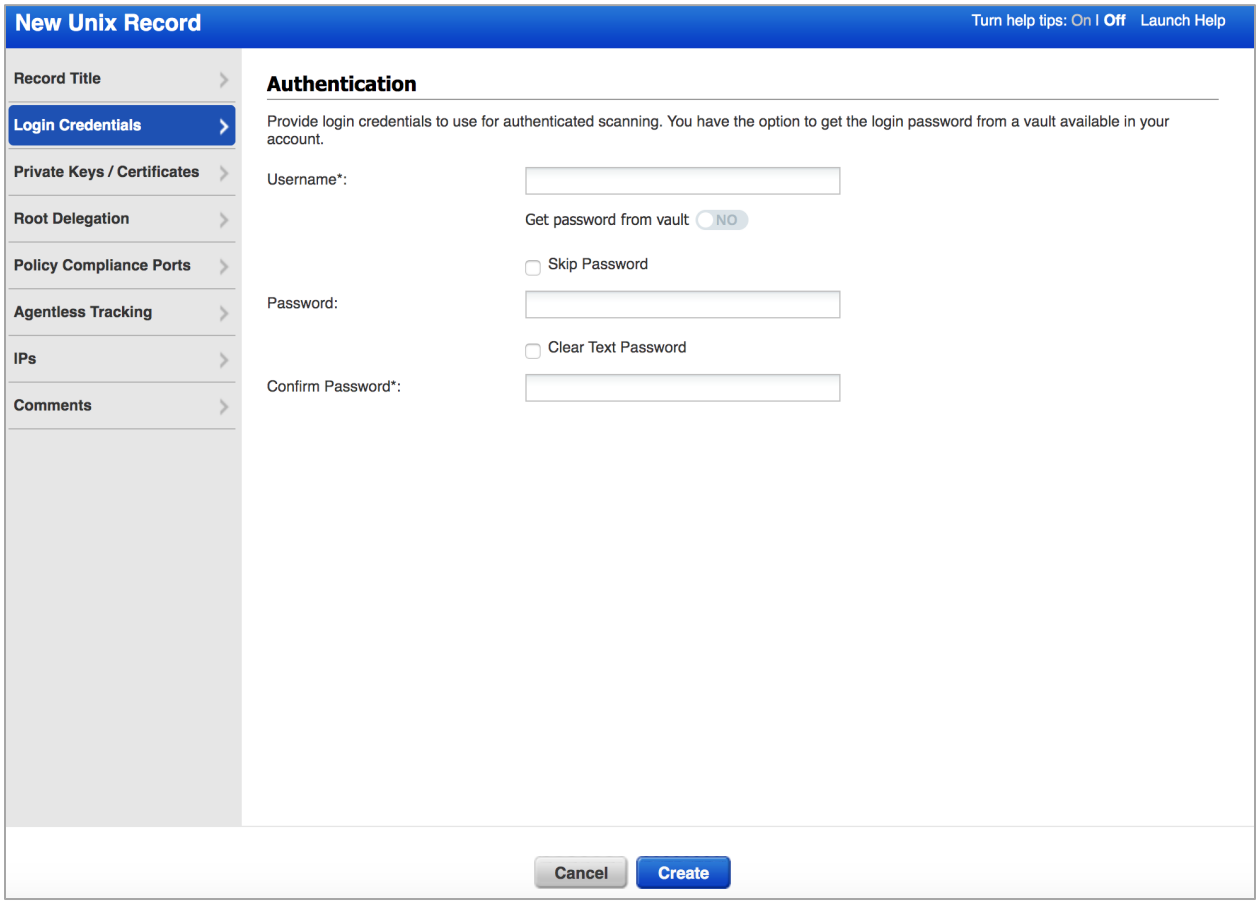
c. Once the user is created, assign a “read-only” policy directly or via the group to this user, which will be used to assess the controls during the scan.



Command Specification

```
(^man.*)|(^show\s+(?!system)|(?!configstatus)|(?!ns ns\.conf)|(?!ns
savedconfig)|(?!ns runningConfig)|(?!gslb runningConfig)|(?!audit
messages)|(?!techsupport).*)|(^stat.*)
```

2) NetScaler uses Unix Authentication record for authentication and assessment of controls so, please use new Authentication and select Unix Authentication.



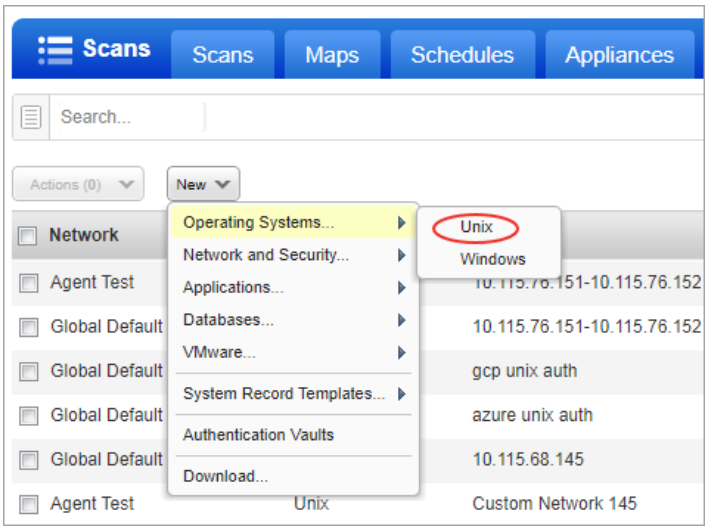
3) Following are the list of commands that are executed on the device to assess compliance controls. Supported Versions are 10.x, 11.x and 12.x.

```
shell cat /etc/sshd_config | grep "AllowTcpForwarding"
shell 'nsconmsg -d stats | grep "small_window" | sed -E "s/ +/|:|/g"'
shell cat /etc/issue
show aaa ldapParams
Show aaa radiusParams
Show aaa tacacsParams
show audit nslogParams
show iptunnel | grep "Name"
show ns feature
show ns mode
show ns mode | grep -w BridgeBPDUs
show ns mode | grep -w DRADV
show ns mode | grep -w DRADV6
show ns mode | grep -w IRADV
show ns mode | grep -w SRADV
show ns mode | grep -w SRADV6
show ns tcpbufParam
show ntp server | grep NTP
show ntp sync
show run | grep "authentication ldapPolicy"
show run | grep "authentication radiusPolicy"
show run | grep "bind system group"
show run | grep "bind system user"
show snmp alarm | grep UNSET
show snmp community -level verbose -format INPUT
show snmp manager | grep "IP"
show ssl parameter
show system user | grep "User name"
show tcpParam
show vpn parameter
show vpn parameter -level verbose -format OLD | grep "splitTunnel"
show vpn sessionAction
show aaa preauthenticationpolicy
show acl -level verbose -format OLD
show authentication ldapAction -level verbose -format OLD | grep serverIP
show authentication radiusAction -level verbose -format OLD | grep serverIP
```

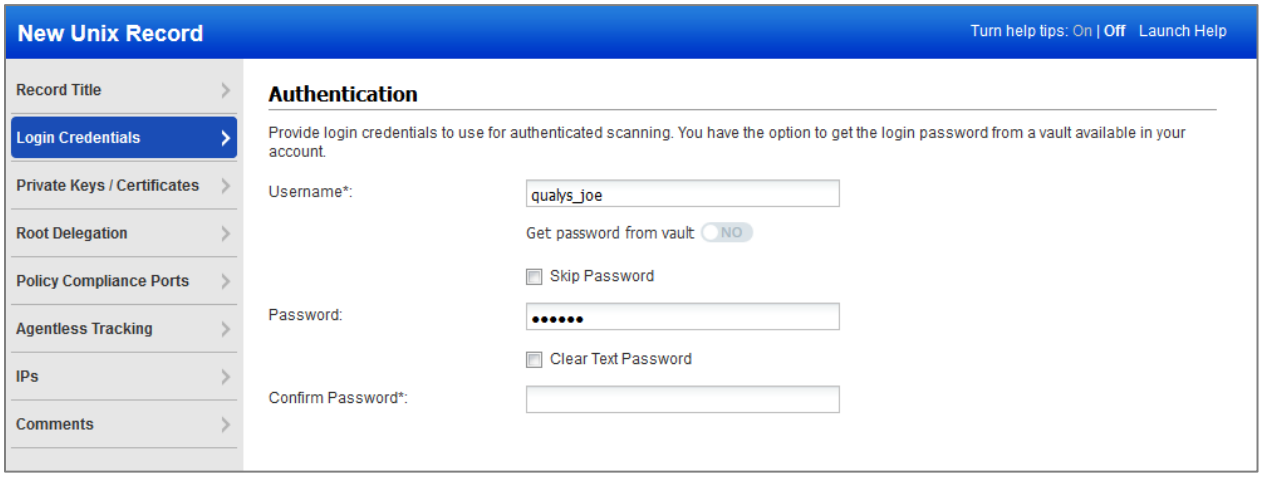
```
show authentication tacacsAction -level verbose -format OLD | grep serverIP
show authentication vserver -level verbose -format OLD
show interface -level verbose -format OLD
show ns httpProfile
show ns ip6 -level verbose -format OLD
show ns ip -level verbose -format OLD
show ns ip -type NSIP -level verbose -format OLD
show ns version
show responder action | grep 'Name|Operation|Target'
show responder global
show responder policy | grep 'Name|Active|^ *$'
show rewrite policy | grep 'Name|Active'
show rpcNode -level verbose -format OLD
show run | grep "add vpn sessionAction"
show run | grep "authentication Policy"
show run | grep "bind ssl cipher"
show run | grep "bind ssl service" | grep "certkeyName"
show run | grep "bind ssl service" | grep "nshttps-127.0.0.1-443 -
certkeyName"
show service -level verbose -format OLD | grep "TCPB YES"
show snmp alarm -level verbose -format OLD
show snmp option -level verbose -format OLD | grep "set snmp"
show snmp user -level verbose -format OLD
show ssl profile -level verbose -format OLD
show ssl service -level verbose -format OLD
show ssl service -level verbose -format OLD | grep "sessTimeout"
show ssl vserver -level verbose -format OLD
show syslogAction
show syslogAction -level verbose -format OLD | grep "syslogAction"
show syslogPArams -level verbose -format OLD | grep syslogParams
show system parameter -level verbose -format OLD | grep "system parameter"
show vpn vserver -level verbose -format OLD
```

Unix Authentication Record

Go to Scans > Authentication. Then select New > Operating Systems > Unix. You might be interested in Unix subtypes. You'll see records for Cisco authentication and Checkpoint Firewall authentication under Network and Security.

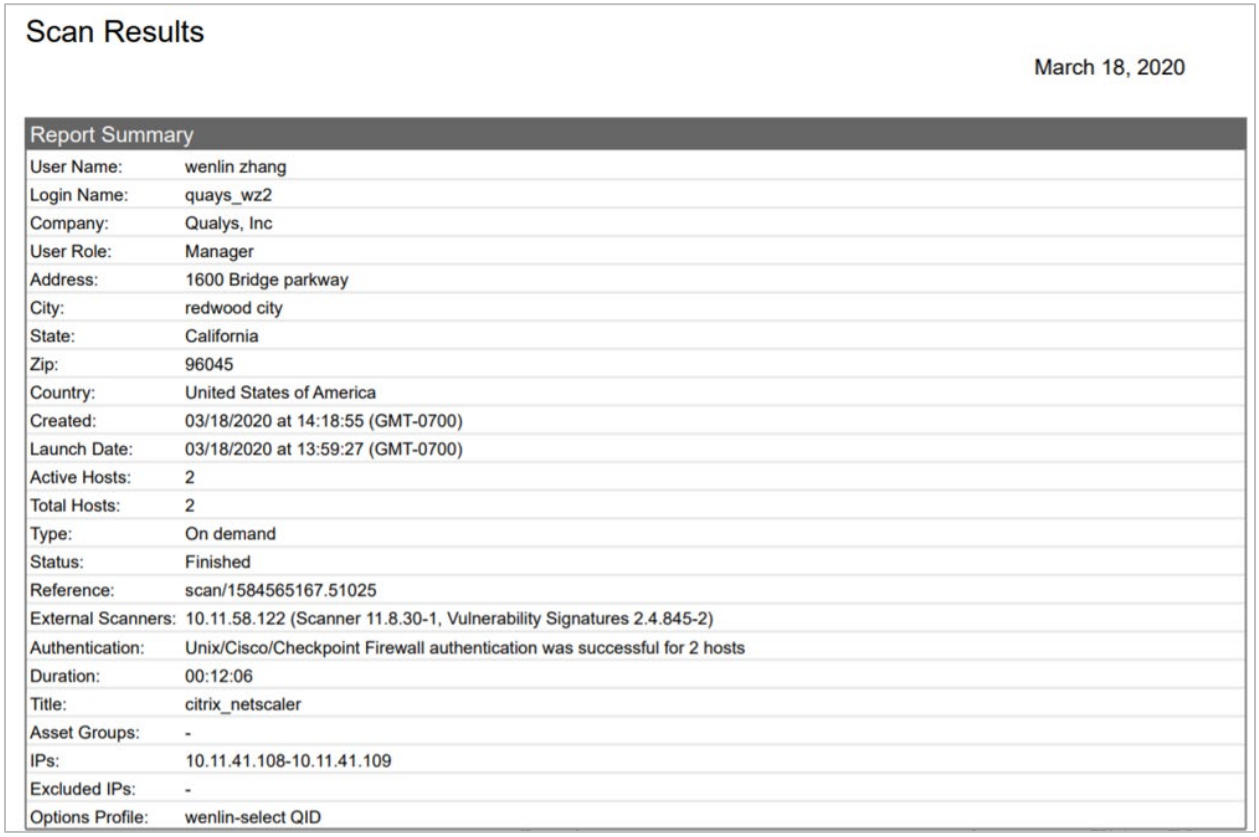


Enter the Unix login credentials (user name, password) our service will use to log in to Unix hosts at scan time. Then walk thru our wizard to select the options you want for private keys, root delegation, policy compliance and target IPs. Our online help is always available to assist you.



Reports

Sample VM Report

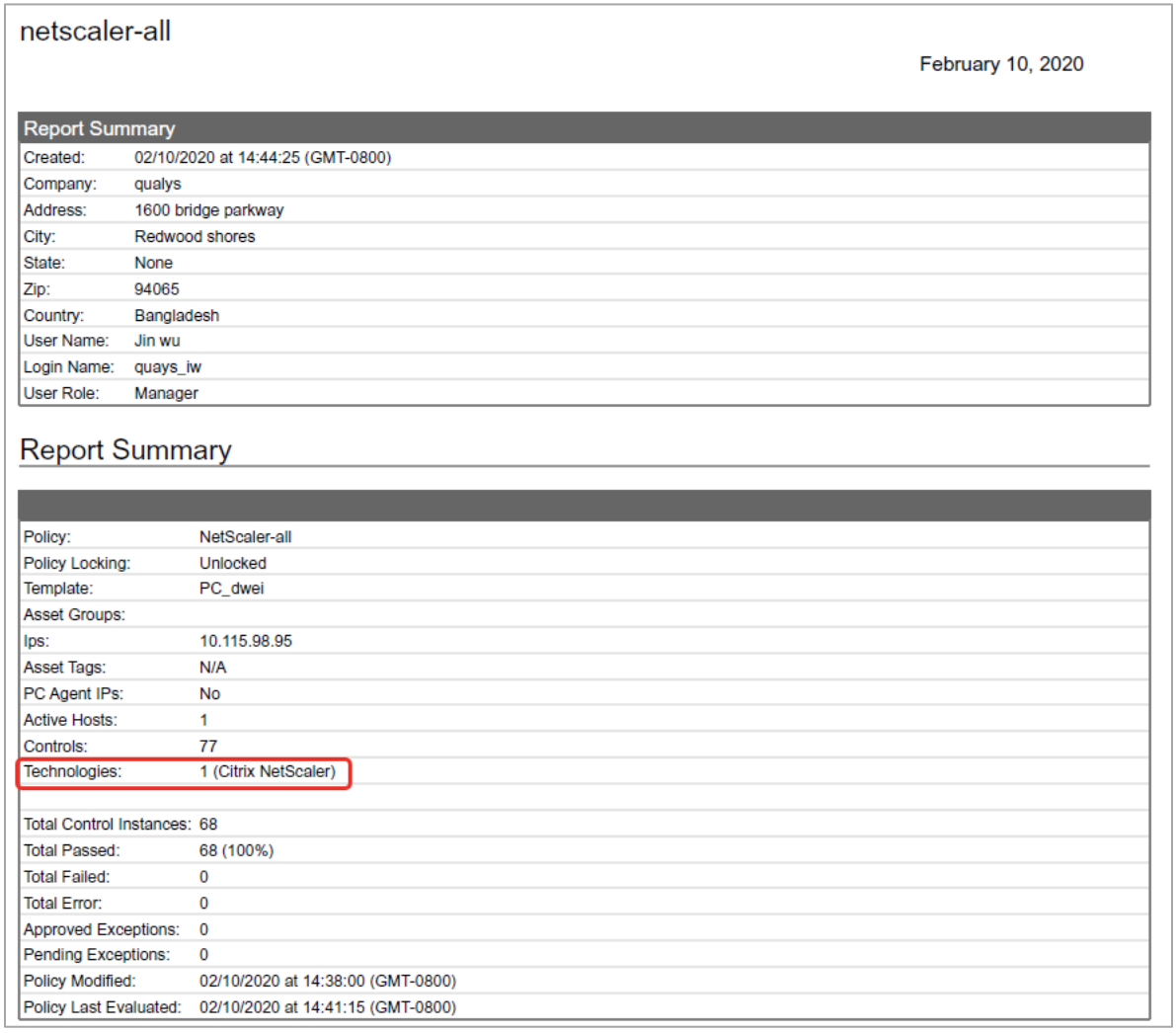


Scan Results

March 18, 2020

Report Summary	
User Name:	wenlin zhang
Login Name:	quays_wz2
Company:	Qualys, Inc
User Role:	Manager
Address:	1600 Bridge parkway
City:	redwood city
State:	California
Zip:	96045
Country:	United States of America
Created:	03/18/2020 at 14:18:55 (GMT-0700)
Launch Date:	03/18/2020 at 13:59:27 (GMT-0700)
Active Hosts:	2
Total Hosts:	2
Type:	On demand
Status:	Finished
Reference:	scan/1584565167.51025
External Scanners:	10.11.58.122 (Scanner 11.8.30-1, Vulnerability Signatures 2.4.845-2)
Authentication:	Unix/Cisco/Checkpoint Firewall authentication was successful for 2 hosts
Duration:	00:12:06
Title:	citrix_netscaler
Asset Groups:	-
IPs:	10.11.41.108-10.11.41.109
Excluded IPs:	-
Options Profile:	wenlin-select QID

Sample PC Report



netscaler-all

February 10, 2020

Report Summary	
Created:	02/10/2020 at 14:44:25 (GMT-0800)
Company:	qualys
Address:	1600 bridge parkway
City:	Redwood shores
State:	None
Zip:	94065
Country:	Bangladesh
User Name:	Jin wu
Login Name:	quays_iw
User Role:	Manager

Report Summary

Policy:	NetScaler-all
Policy Locking:	Unlocked
Template:	PC_dwei
Asset Groups:	
Ips:	10.115.98.95
Asset Tags:	N/A
PC Agent IPs:	No
Active Hosts:	1
Controls:	77
Technologies:	1 (Citrix NetScaler)
Total Control Instances:	68
Total Passed:	68 (100%)
Total Failed:	0
Total Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Policy Modified:	02/10/2020 at 14:38:00 (GMT-0800)
Policy Last Evaluated:	02/10/2020 at 14:41:15 (GMT-0800)

Last updated: May 27, 2022