# Table of Contents

**About this Guide** ........................................................................................................... 4  
About Qualys ...................................................................................................................... 4  
Qualys Support ................................................................................................................... 4  

**CloudView Overview** .................................................................................................... 5  
Qualys Subscription and Modules required ................................................................. 5  
Concepts and Terminologies ............................................................................................ 5  
CloudView API .................................................................................................................... 7  

**Get Started** .................................................................................................................. 8  
Create AWS Connector ................................................................................................... 8  
Create Azure Connector .................................................................................................. 12  
Run Your Connector ......................................................................................................... 17  

**Securing Cloud Resources** .......................................................................................... 18  
Dashboard ....................................................................................................................... 18  
Resources Details ............................................................................................................ 19  
Resources Misconfigurations ......................................................................................... 24  

**Appendix** ..................................................................................................................... 27  
IAM Permissions for Custom AWS Policy ..................................................................... 27
About this Guide

Welcome to Qualys CloudView! We’ll help you get acquainted with the Qualys solutions for securing your AWS resources using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.
CloudView Overview

Qualys CloudView provides visibility and continuous security across all of your cloud environments.

With CloudView you’ll get these features:

- Discover and inventory assets and resources across all regions from multiple accounts and multiple cloud platforms
- Search resource metadata, view resource details and show associations across resources
- Out-of-box CIS Amazon Web Services Foundations Benchmark policy & AWS Best Practices policy to identify misconfigurations of S3 Buckets
- Continuously assess and report on resource misconfigurations by checking against the controls from out-of-box policies
- Ability to search misconfigurations by Account-ID, Regions

Qualys Subscription and Modules required

Check that you have these modules available in your subscription:

- CloudView
- Vulnerability Management (only if you want to view host vulnerability information)
- AssetView
- Cloud Agents for VM

If you need a module, please contact your Qualys Technical Account Manager (TAM).

Concepts and Terminologies

Get familiar with common terms used in CloudView.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>A set of configuration checks that will assess different resources collected from your cloud account.</td>
</tr>
<tr>
<td>Control</td>
<td>A configuration check. Each check applies to a specific service/resource. Here are some examples: - MFA should be enabled for console user - applies to AWS IAM Service and IAM User Resource - Password policy should have upper case letter enforced - applies to AWS IAM Service - Security group should not allow inbound access on port 22 from 0.0.0.0 - applies to EC2/VPC services and Security Group Resource</td>
</tr>
<tr>
<td>Service</td>
<td>A service is the high level grouping by functional area. Each service consists of different entities or resources.</td>
</tr>
<tr>
<td>Concept</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resource</td>
<td>A resource is an entity that you can work with. Examples include an Amazon EC2 instance, IAM User, Security Group.</td>
</tr>
<tr>
<td>Control Passed</td>
<td>Each control is applicable to a specific resource type. For each control, applicable resources are collected. The control checks whether the particular attribute of a resource is configured as per best practices. The control is passed when the attribute that the control is checking is found configured as per the desired configuration for all the applicable resources collected.</td>
</tr>
<tr>
<td>Control Failed</td>
<td>Control is considered failed when an attribute of the control being checked is not configured as per the desired configuration for any of the applicable resources collected.</td>
</tr>
<tr>
<td>Resource Passed</td>
<td>Resource is considered passed for a control if it’s attribute is configured as per the desired configuration in the control.</td>
</tr>
<tr>
<td>Resource Failed</td>
<td>Resource is considered failed for a control if it’s attribute is not configured as per the desired configuration in the control.</td>
</tr>
</tbody>
</table>
CloudView API

Many CloudView features are available through REST APIs.

You can directly access the Swagger UI from the following URL:
http://<QualysURL>/cloudview-api/swagger-ui.html

For example, if your account is on US Platform 2

For information on what API Server URL to use, see the section “API Server URL” in the Qualys API Quick Reference Guide.

Do I need to Authenticate?

Authentication to the Qualys Cloud Platform is necessary before you try out the APIs.

Simply, click Authorize and provide the user name and password. You can now use the APIs!
Get Started

Just set up a connector for your cloud environment and that’s it! We’ll start discovering resources that are present in your cloud account. You can create AWS connectors and Azure connectors. We’ll walk you through the steps.

Create AWS Connector

Go to the Configuration tab and select Create Connector > Amazon Web Services.

Provide a name and description (optional) for your connector. Then copy settings from the connector details: Qualys AWS Account ID and External ID. You’ll need these for creating your IAM role in AWS in the next step.
Launch your AWS console, and go to IAM > Roles and click Create Role. In the Create role window, choose “Another AWS account”. Paste in the Qualys account ID and the External ID that you copied in the previous step. Click Next: Permissions.

Choose AWS policy to attach to role. Find the policy “SecurityAudit” and select the check box next to it. A custom policy may be used instead (Learn more). Click Next: Review.
Save AWS role and get the ARN. Enter a role name (e.g. QualysEC2Role), click Create role. Then click on the saved role to view role details and copy the ARN value.

Go back to your AWS connector in Qualys CloudView and paste the Role ARN value into the connector details. Then click Create Connector.

That’s it! The connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies.
Want to create a role using CloudFormation?
Download the CloudFormation template from the Create AWS Connector window.

Follow the steps on the screen to create a stack and upload the template. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.
Create Azure Connector

On the Configuration tab, select Create Connector > Microsoft Azure.

Provide a name and description (optional) for your connector.

Next we’ll describe how to configure the application ID, directory ID, authentication key and subscription ID from the Microsoft Azure console to paste into your connector details.
Application ID

Create an application in Azure Active Directory. Log on to the Microsoft Azure console and go to Azure Active Directory in the left navigation pane, then App registrations. Click New application registration.

Provide these details:

Name: A name for the application (e.g. Azure connector)

Application type: Select Web app/API

Sign-on URL: Enter any valid URL. You can enter a URL that does not exist, but it must be in valid format.

Click Create. The newly created app is displayed in the list of applications.
Copy the Application ID and paste it into the connector details.

Copy the Directory ID and paste it into the connector details.
Authentication Key
You must provide permission to the new application to access the Windows Azure Service Management API and create a secret key.

Provide permission: Select the application that you created and go to Settings > Required permissions. Click Add > Select an API > Windows Azure Service Management API, and click Select.

Select required Delegated Permissions and click Select.

Create secret key: Select the application that you created and go to Settings > Keys. Add a description and expiry duration for the new key and click Save. The value of the key appears in the Value field.

Copy the key value at this time. You won’t be able to retrieve the key later. Note down the secret key and store it securely with you. You’ll need to provide the key value with the application ID to log on as the application.
**Subscription ID**

Grant permission for the application to access subscriptions. Assign a role to the new application. The role defines the permissions for the new application to access subscriptions. Repeat these steps to add more subscriptions.

On the Microsoft Azure portal, navigate to Subscriptions.

Select the subscription for which you want to grant permission to the application, and choose Access Control (IAM). Go to Add > Select a role. Pick the role you want to give to the user. For example, the Reader role. A Reader can view everything, but cannot make any changes to the resources of a subscription.

Select Azure AD user, group, or application in Assign Access to drop-down. Search for your application, and select it. Then click Save to finish assigning the role. You’ll see your application in the list of users assigned to a role for that scope.
Run Your Connector

Once you create a connector, the connector will start discovering the resources and misconfigurations in your account. To fetch the updated resources, you need to select Run from the quick actions menu.
Securing Cloud Resources

Upon setting up your connector, it starts discovering the resources that are present in your cloud account. The resources inventory and the metadata of the resources is pushed to Qualys portal. You can navigate to the Resources tab to view the resources getting collected along with their details.

Dashboard

The Qualys CloudView application provides out-of-the-box default AWS Security Overview Dashboard providing a summary of inventory and security posture across resources.

The default dashboard provides:
- Resource inventory - Route Tables, EC2 Instances, VPC, Subnets, IAM Users, etc
- Total evaluation failures i.e. the resources misconfigurations by control criticality
- Security posture at each region level showing resources and failures
- Top 5 Accounts with maximum control failures
- Top 5 Failed controls

Check out this sample dashboard
Resources Details

The Resources tab displays the information about various resources collected. It helps you to identify the number of resources for each type and the number of resources that have one or more control failures. You can click on a row to view the number of resources of a specific type. You can click on an individual resource to view the details. For each resource you will view the following information.

Resources Summary

The List View provides a summary of your resources, including the total resources and the number of failed resources for each resource type.

Let us consider an example of Instance (EC2 Instance) and Security Group resource type to view the resource details and information.
Instance Details

Click Instance type to drill-down into your AWS EC2 instances.

Then click on any EC2 Instance ID to see the number of detected vulnerabilities, resource associations, location and network information.
Vulnerability Details
Click on the Vulnerabilities count to get information about detected vulnerabilities.

The vulnerability related data is populated only if you are using a scanner appliance or Cloud Agent.
**View Security Group Information**

You could view more details about a security group resource. Go to Resources > Security Group, and then click the security group ID to view additional details about it.

![Security Group Information](image)

**View Security Group Associations**

You can view various details about the associations such as the ID, region, state and so on.

![Security Group Associations](image)
View Controls Evaluated

You can view the controls that are evaluated for the resource and if the controls have passed or failed.

<table>
<thead>
<tr>
<th>ID</th>
<th>Control</th>
<th>Criticality</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>41</td>
<td>Ensure no security groups allow ingress from 0.0.0.0/0 to port 22</td>
<td>Low</td>
<td>Fail</td>
</tr>
<tr>
<td>42</td>
<td>Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389</td>
<td>Low</td>
<td>Fail</td>
</tr>
</tbody>
</table>
Resources Misconfigurations

CloudView compares controls from the out-of-box policies that define the desired configuration of a resource against the current configuration of the resource. If it finds a difference, then it marks the resource as failed for that particular control. Each control is evaluated against the applicable resources. If all the applicable resources are configured as per the desired configuration of the control, then the control is marked as Pass. If at least one of the applicable controls doesn’t comply with the control, then it is marked as failed. The Monitor tab will display all such misconfigurations.

Controls Evaluation View

(1) Total Resources - The unique number of resources evaluated against all the controls.
(2) Security Posture - How many control evaluations have passed and failed.
(3) Failures By Critically - Control evaluation failures by control criticality.

Each control is evaluated against the applicable resources which is represented by Total Resources. Number represented by green represents the number of pass resources that have the desired configuration as per the control. Number represented by red represents the number of failed resources.

Click on any control to get details of all the resources evaluated against the control.
Control Evaluation Details
Control details screen shows the number of resources evaluated against the control. For each resource it shows Unique Resource ID, Account ID, Region, etc. You can use the search filter to view pass/failed resources.

Resource Evidence
To get more details on why a resource failed, click the Evidence link to see actual values for the resource attributes.
View Remediation Steps
Click the Remediation Steps tab to learn the steps needed to fix the failure.

View Control Evaluation Results per Account
Quickly view how many controls are passed/failed by clicking the account filter.
Appendix

IAM Permissions for Custom AWS Policy

You may choose to create a custom policy in AWS and associate it to the cross-account role. Here is a list of permissions required.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:ListAttachedUserPolicies",
                "iam:GetCredentialReport",
                "iam:ListUserPolicies",
                "iam:ListGroupsForUser",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAddresses",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "s3:GetBucketLogging",
                "s3:GetBucketTagging",
                "s3:ListBucket*",
                "s3:GetBucketPolicy",
                "s3:GetBucketVersioning",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "logs:DescribeMetricFilters",
                "cloudwatch:DescribeAlarmsForMetric",
                "kms:GetKeyRotationStatus",
                "kms:ListKeys",
                "sns:ListSubscriptionsByTopic",
                "autoscaling:DescribeLoadBalancers",
                "config:DescribeConfigurationRecorderStatus"
            ]
        }
    ]
}
```
"elasticloadbalancing:Describe*",
"s3:GetBucket*",
"s3:ListAllMyBuckets",
"ec2:Describe*",
"autoscaling:Describe*",
"cloudtrail:DescribeTrails",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"iam:GenerateCredentialReport",
"iam:Get*",
"iam:List*"
},

"Resource": "*",
"Effect": "Allow",
"Sid": "VisualEditor0"
}]
}