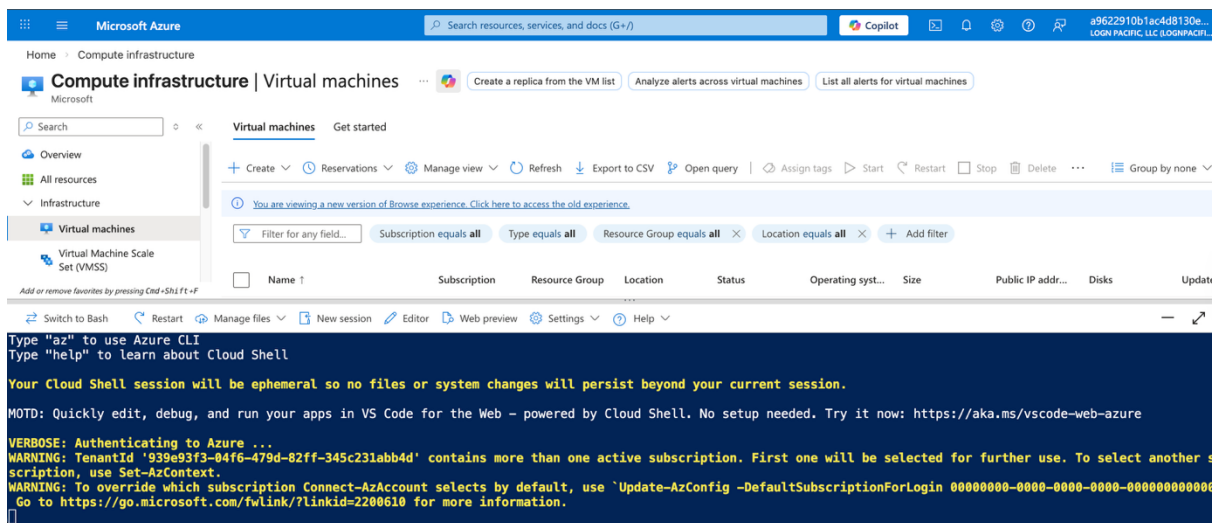


Used Azure Cli to export the details of VMs



The screenshot shows the Azure portal interface for Virtual machines. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user's profile. The main content area displays the 'Virtual machines' page with a table of resources. The table has columns for Name, Subscription, Resource Group, Location, Status, Operating system, Size, Public IP address, Disks, and Update. Below the table, there is a terminal window showing the output of the Azure CLI command 'az vm list'.

```
Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

MOTD: Quickly edit, debug, and run your apps in VS Code for the Web - powered by Cloud Shell. No setup needed. Try it now: https://aka.ms/vscode-web-azure

VERBOSE: Authenticating to Azure ...
WARNING: TenantId '939e93f3-04f6-479d-82ff-345c231abb4d' contains more than one active subscription. First one will be selected for further use. To select another subscription, use Set-AzContext.
WARNING: To override which subscription Connect-AzAccount selects by default, use `Update-AzConfig -DefaultSubscriptionForLogin 00000000-0000-0000-0000-000000000000`
Go to https://go.microsoft.com/fwlink/?linkid=2200610 for more information.
```

1. Get all subscriptions you have access to

```
$subs = Get-AzSubscription
```

2. Prepare an empty list

```
$report = @()
```

```
foreach ($sub in $subs) {
```

```
    Write-Host "Scanning Subscription: $($sub.Name)..." -ForegroundColor Cyan
```

```
    # Switch context to that subscription
```

```
    Set-AzContext -SubscriptionId $sub.Id | Out-Null
```

```
    # Get VMs for this subscription
```

```
    $vms = Get-AzVM -Status
```

```
    # Process them
```

```
    $currentSubVMs = $vms | ForEach-Object {
```

```
        $nic = Get-AzNetworkInterface -ResourceId $_.NetworkProfile.NetworkInterfaces[0].Id
```

```
        [PSCustomObject]@{
```

```
            name      = $_.Name
```

```
            object_id = $_.VmId
```

```
            ip_address = $nic.IpConfigurations[0].PrivateIpAddress
```

```
            dns_domain = "azure.lab"
```

```

os      = $_StorageProfile.OsDisk.OsType

cpu_count  = $_HardwareProfile.VmSize

state     = ($_PowerState -replace 'PowerState/',)

location  = $_Location

classification= "Production"
}
}

# Add to the master list

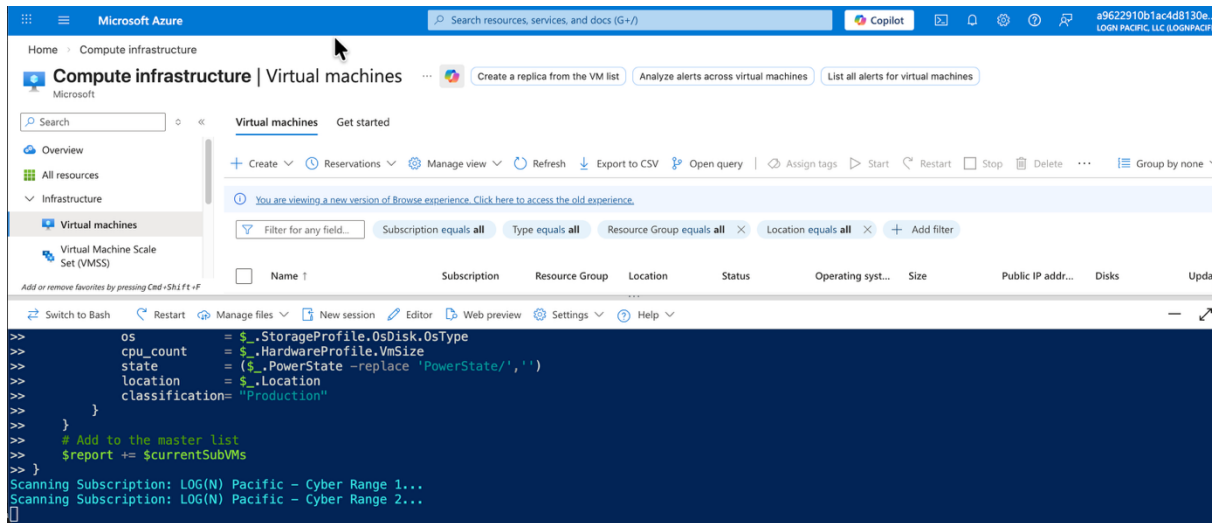
$report += $currentSubVMs
}

# 3. Export the final combined list

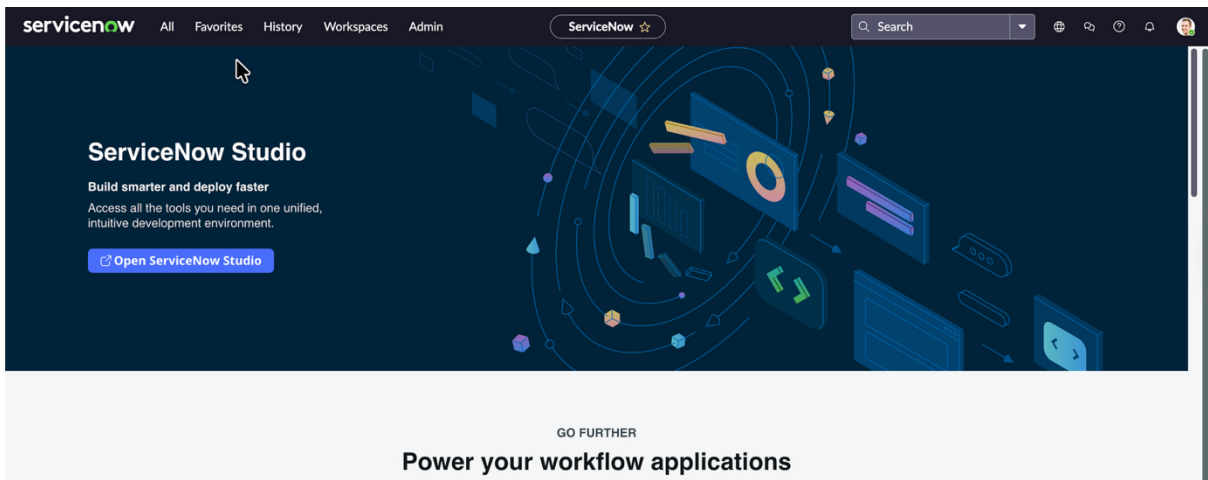
$report | Export-Csv -Path ".\azure_assets_v2.csv" -NoTypeInformation

Write-Host "Success! Found $( $report.Count ) VMs across all subscriptions." -ForegroundColor Green

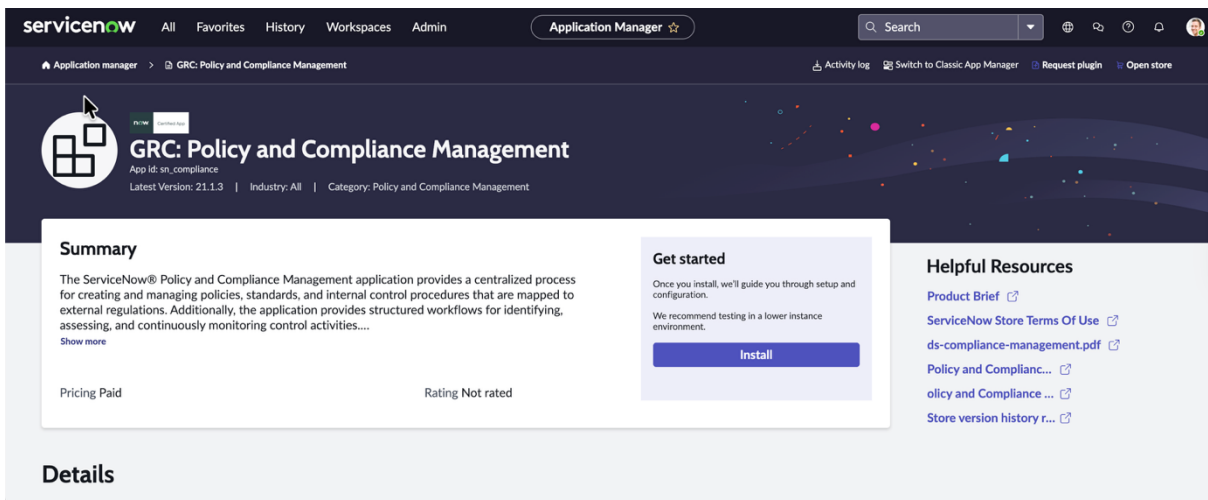
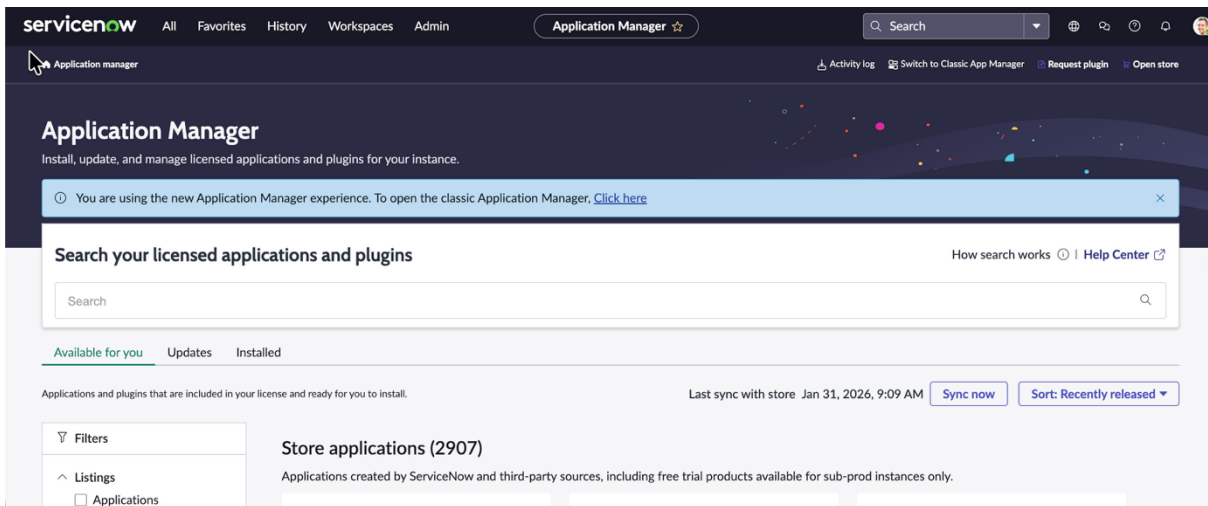
```



Created a Servicenow developer pdi profile and made an instant



Logged into the Xanadu version of servicenow and installed the GRC plugin



servicenow | All | Favorites | History | Workspaces | Admin | Application Manager

Application manager > GRC: Policy and Compliance Management

GRC: Policy and Compliance Management

App Id: sn_compliance
Latest Version: 21.1.3 | Industry: All | Category: Policy and Compliance Management

Summary

The ServiceNow® Policy and Compliance Management application provides a centralized process for creating and managing policies, standards, and internal control procedures that are mapped to external regulations. Additionally, the application provides structured workflows for identifying, assessing, and continuously monitoring control activities...

Pricing Paid | Rating Not rated

Get started

Once you install, we'll guide you through setup and configuration.

We recommend testing in a lower instance environment.

Installing: 91%

View Details

Helpful Resources

- Product Brief
- ServiceNow Store Terms Of Use
- ds-compliance-management.pdf
- Policy and Compliance...
- olicy and Compliance ...
- Store version history r...

Details

Imported the Data

servicenow | All | Favorites | History | Workspaces | Admin | Table Transform Map - Azure Map

Table Transform Map - Azure Map

Field maps created

* Name: Azure Map

* Source table: Computer [imp_computer]

Active:

Run business rules:

Enforce mandatory fields: No

Copy empty fields:

Create new record on empty coalesce fields:

Application: Global

Created: 2026-02-02 17:56:10

* Target table: Virtual Machine Instance [cmdb_ci_vm_ins...]

Order: 100

Run script:

Copy | Update | Delete

Related Links

- Auto Map Matching Fields
- Mapping Assist
- Validate Coalesce Fields
- Transform
- Index Coalesce Fields
- Run Point Scan

servicenow | All | Favorites | History | Workspaces | Admin | Table Transform Map - Azure Map

Table Transform Map - Azure Map

Transform

Index Coalesce Fields

Run Point Scan

Field Maps (9) | Transform Scripts | Unindexed reference fields (1) | Empty reference fields (3)

Source field	Target field	Coalesce
u_dns_domain	dns_domain	false
u_name	name	false
serial_number	serial_number	false
u_location	location	false
u_ip_address	ip_address	false
model_id	model_id	false
u_state	state	false
u_object_id	object_id	false
manufacturer	manufacturer	false

1 to 9 of 9

Set the coalesce for object id to true as it is the name and the distinguishing thing of the set

Source field	Target field	Coalesce
u_dns_domain	dns_domain	false
u_name	name	false
serial_number	serial_number	false
u_location	location	false
u_ip_address	ip_address	false
model_id	model_id	false
u_state	state	false
u_object_id	object_id	true
manufacturer	manufacturer	false

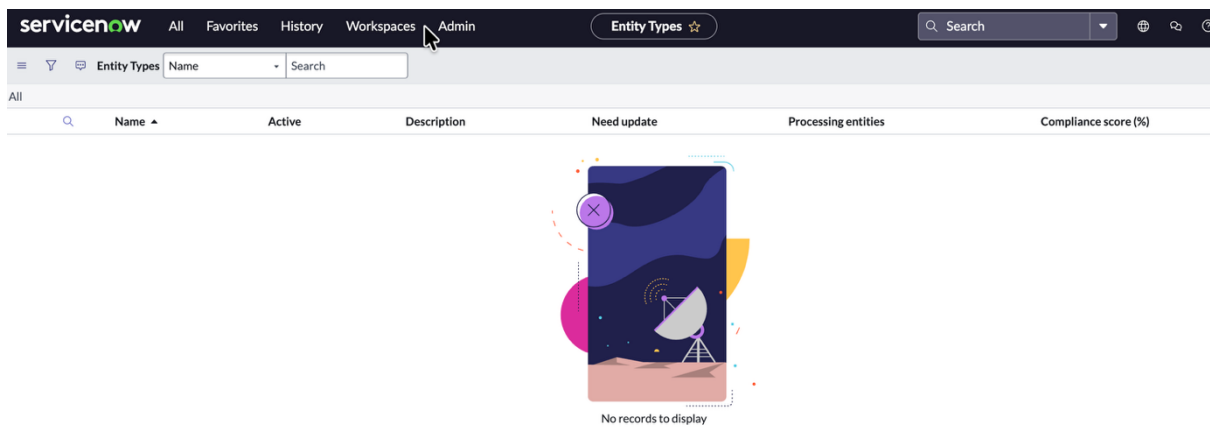
Import successful

Number: ISET0010003
 State: Processed
 Data source: azure_assets_v2.csv (Uploaded)
 Import set table: azure import 2 [u_azure_import_2]
 Short description: Type: File
 Format: CSV

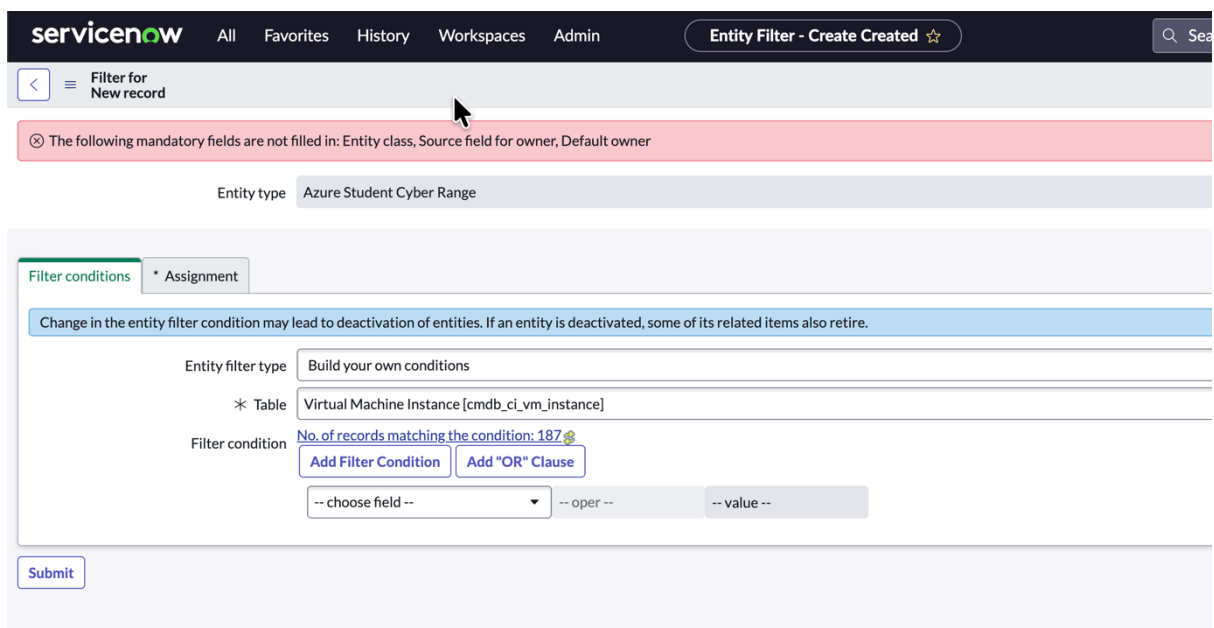
Created	Row	State	Target record	Error	Comment	Transform Map
2026-02-02 18:06:06	0	Inserted	Virtual Machine Instance: linux-target-1	(empty)		Azure import 2-2

Created	Row	State	Target record	Error	Comment	Transform Map
2026-02-02 18:06:06	0	Inserted	Virtual Machine Instance: linux-target-1	(empty)		Azure import 2-2
2026-02-02 18:06:06	1	Inserted	Virtual Machine Instance: windows-target-1	(empty)		Azure import 2-2
2026-02-02 18:06:06	2	Inserted	Virtual Machine Instance: LOCAL-SCAN-ENGINE-01	(empty)		Azure import 2-2
2026-02-02 18:06:06	3	Inserted	Virtual Machine Instance: sky-vm	(empty)		Azure import 2-2
2026-02-02 18:06:06	4	Inserted	Virtual Machine Instance: RMS-VM-To-MDE	(empty)		Azure import 2-2
2026-02-02 18:06:06	5	Inserted	Virtual Machine Instance: Mosh-Oct-28-2025stlg	(empty)		Azure import 2-2
2026-02-02 18:06:06	6	Inserted	Virtual Machine Instance: WinVMjbTest	(empty)		Azure import 2-2
2026-02-02 18:06:06	7	Inserted	Virtual Machine Instance: toni-stig-test	(empty)		Azure import 2-2
2026-02-02 18:06:06	8	Inserted	Virtual Machine Instance: Milton-Test	(empty)		Azure import 2-2
2026-02-02 18:06:06	9	Inserted	Virtual Machine Instance: FPhillip-Win11-EDR	(empty)		Azure import 2-2
2026-02-02 18:06:06	10	Inserted	Virtual Machine Instance: GdsVM	(empty)		Azure import 2-2
2026-02-02 18:06:06	11	Inserted	Virtual Machine Instance: Drea-test-scan	(empty)		Azure import 2-2
2026-02-02 18:06:06	12	Inserted	Virtual Machine Instance: WIN-11-Kolff	(empty)		Azure import 2-2
2026-02-02 18:06:06	13	Inserted	Virtual Machine Instance: threathunt-vm	(empty)		Azure import 2-2
2026-02-02 18:06:06	14	Inserted	Virtual Machine Instance: Saul-VM-Project	(empty)		Azure import 2-2
2026-02-02 18:06:06	15	Inserted	Virtual Machine Instance: EDR-VM	(empty)		Azure import 2-2
2026-02-02 18:06:06	16	Inserted	Virtual Machine Instance: Bigone	(empty)		Azure import 2-2
2026-02-02 18:06:06	17	Inserted	Virtual Machine Instance: vuln-machine	(empty)		Azure import 2-2

Went into entities types



Created a filter



servicenow All Favorites History Workspaces Admin Entity Filter - Create Created ☆ Search

Filter for New record

⊗ The following mandatory fields are not filled in: Source field for owner

Entity type Azure Student Cyber Range

Filter conditions Assignment

* Entity class VM

* Default owner System Administrator

Use owner field

* Source field for owner Assigned to

Auto-update owner

* Empty owner Use Default

Submit

servicenow All Favorites History Workspaces Entity Type - Azure Student Cyber Range ☆ Search

Entity Type Azure Student Cyber Range Update Delete

Entities (187) Entity Filters (1) Policies Control Objectives Policy Exceptions Content References

Entity Search


Entity type = Azure Student Cyber Range

Entity	Created Manually	Compliance score (%)
cyberranger-Pro-25	false	0
Ebtest	false	0
windows-target-1	false	0
GdsVM	false	0
Abdiaziz	false	0
Harken-test-vm	false	0
windows11-ana	false	0
Drea-test-scan	false	0
Alexander-Win11-STIG-Test	false	0
win-11-2026	false	0
kjvm1	false	0
Jan30test	false	0
Brian-VM	false	0
vm-final-lab-vmone	false	0

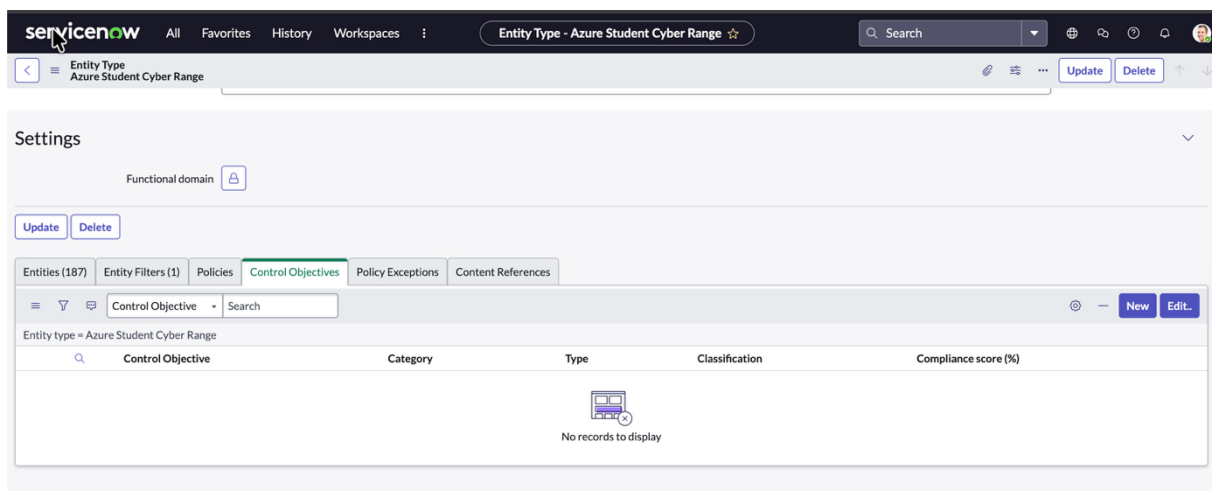
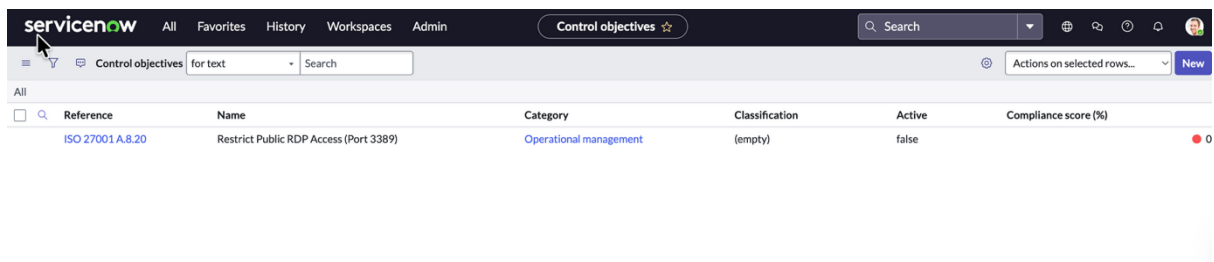
Went to control objectives

servicenow All Favorites History Workspaces Admin Control objectives ☆ Search

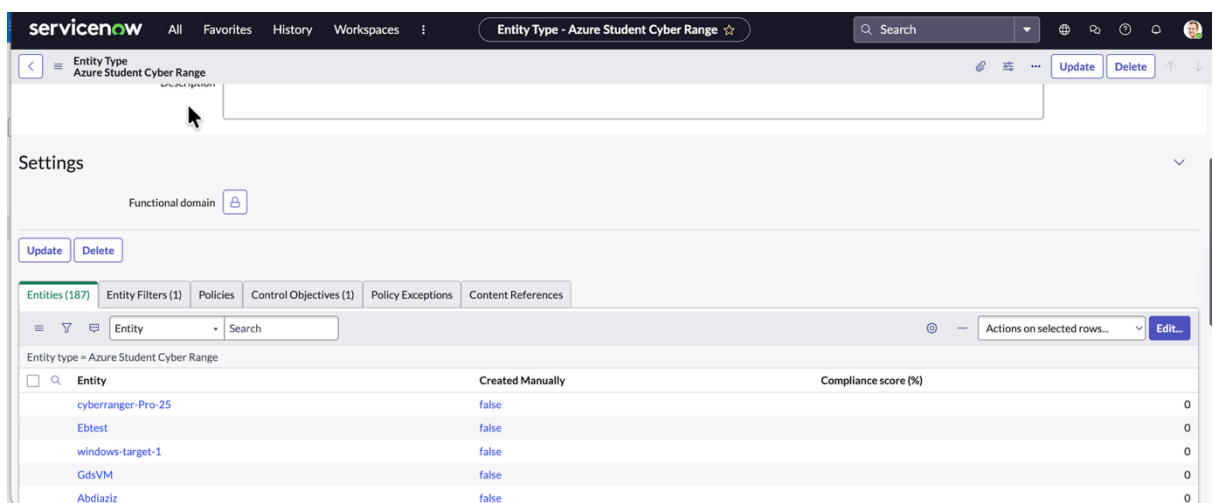
Control objectives for text Search New

Reference	Name	Category	Classification	Active	Compliance score (%)
 <p>No records to display</p>					

Created a new control objective. Restrict public RDP access



Went into entity type



Ended up creating the control objective from there and set it to active

servicenow All Favorites History Workspaces Admin Control objectives

Control objectives for text Search

Reference	Name	Category	Classification	Active	Compliance score (%)
ISO 27001 A.8.20	Restrict Public RDP Access (Port 3389)	Operational management	(empty)	true	0
ISO 27001 A.8.20	Restrict Public RDP Access (Port 3389)	Operational management	(empty)	false	0
ISO 27001 A.8.20	Restrict Public RDP Access (Port 3389)	Operational management	(empty)	false	0

Vms show up under control tab

servicenow All Favorites History Admin Control objective - Restrict Public RDP Access (Port 3389)

Control objective Restrict Public RDP Access (Port 3389)

Entity types (1) Additional entities Policies Citations Control objectives Controls (187) Policy exceptions Issues Indicator templates Content references

Entity Search

Control objective = Restrict Public RDP Access (Port 3389)

Number	Name	Entity	Function	State	Status	Exempt	Owner	Description
CTRL0020087	Restrict Public RDP Access (Port 3389)	ThreatHuntingScenarioAustin	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020183	Restrict Public RDP Access (Port 3389)	ThreatHuntShad	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020099	Restrict Public RDP Access (Port 3389)	toni-stig-test	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020084	Restrict Public RDP Access (Port 3389)	TP--tp--TP	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020138	Restrict Public RDP Access (Port 3389)	trevor-mde-test	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020170	Restrict Public RDP Access (Port 3389)	UpskillsDani	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020172	Restrict Public RDP Access (Port 3389)	UserSTIGVIEW	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020153	Restrict Public RDP Access (Port 3389)	Vary-AM	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020069	Restrict Public RDP Access (Port 3389)	VirtualTest3	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020154	Restrict Public RDP Access (Port 3389)	vm-final-lab-anas	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020064	Restrict Public RDP Access (Port 3389)	VM-Final-Lab-JJ	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020126	Restrict Public RDP Access (Port 3389)	vm-final-lab-saif	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020014	Restrict Public RDP Access (Port 3389)	vm-final-lab-symone	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020062	Restrict Public RDP Access (Port 3389)	VM-Lionel	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020184	Restrict Public RDP Access (Port 3389)	vm-mde	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020094	Restrict Public RDP Access (Port 3389)	vm-mde-gumball	Standard control	Draft	Status	false	System Administrator	Automated check to ensure port 3389 is n...

Went to tenable scanner

tenable Workspace

Your Tenable Products

Vulnerability Management

Scan assets for vulnerabilities, view and refine results and related data, and share this information with an unlimited set of users or groups.

Utilization 44%

[See More](#)

Enhance Your Security Program

Exposure Management

Aggregating data from multiple sources to present a unified contextual view of your risks, enabling...

AI Exposure

Gain full visibility into AI usage, including prompts, agents, and risky interactions within your AI platforms. Derived from data received at infrastructure and...

Attack Surface Management

Understand your external attack surface.

Scanned a honeypot Linux VM

tenable Vulnerability Management | Scans

Quick Actions

Scans

Create Scan Create Scan Template Tools

Search by scan name, scan status

1 to 14 of 14 Page 1 of 1

14 Items

NAME	SCHEDULE	LAST RUN	STATUS	ACTIONS
vm-final-lab-symone3 Shared	On Demand	02/03/2026	Completed	
vm-final-lab-symone2 Rollover Shared	On Demand	02/03/2026	Canceled	
HD_STIG-DISA1232PolicyScan	On Demand	01/26/2026	Completed	
HD-vul-linux	On Demand	01/26/2026	Completed	
Windows 11 STIG scan Gideon Shared	On Demand	01/20/2026	Completed	
Brown-Win11-AgentScan Shared	Triggered	N/A	Enabled	
J-linuxAgentScan-J Shared	Triggered	N/A	Enabled	
Windows10-Basic agent Scan Shared	Triggered	N/A	Disabled	
GD - Windows 10 Agent Based Mo... Shared	Triggered	N/A	Enabled	
linux-pc-Shadowboss Shared	Triggered	N/A	Enabled	
Copy of DISA-STIG implementatio... Shared	On Demand	N/A	Empty	
Linux_vm_Sam_Scan Shared	Triggered	N/A	Enabled	
Base-Agent Scan-Larnes Shared	Triggered	N/A	Disabled	
Linux_vm_Sam_Scan Shared	Triggered	N/A	Enabled	

Basic network scan ran on the VM using public ip and cloud instance of tenable on the linux vm

tenable Vulnerability Management | Scans > Scan Details

Quick Actions

Compliance Audit - linux-target-1

VULNERABILITY MANAGEMENT SCANS

Edit Trash

Vulns by Asset History

Filters 1 Result

1 Item

1 to 1 of 1 Page 1 of 1

	START TIME	END TIME	DURATION	STATUS	ACTIONS
Current	02/03/2026 at 2:12 PM		1min	Running	

CRITICAL VULNERABILITIES: 0

HIGH VULNERABILITIES: 0

MEDIUM VULNERABILITIES: 0

LOW VULNERABILITIES: 0

Scan Details

STATUS: Running

START TIME: 02/03/2026 at 2:12 PM

TEMPLATE: Basic Network Scan

SCANNER: US Cloud Scanner

TARGETS: 20.57.2.159

SCANNER GROUPS: US Cloud Scanner

Created an issue on service now


servicenow All Favorites History Workspaces Admin

Issues

Search

Issues Number Search

All > Control/Risk Class = Control.or.Control/Risk is empty > Is group = false > Task type != label > or Classification = Compliance.or.Classification = (empty) > Is group = false

Number	Priority	State	Assigned to	Name	Due date
 <p>No records to display</p>					

servicenow All Favorites History Workspaces Admin Issues

Issue New record

New Analyze Respond Review Closed

Number IPT0020001 State New

Assignment group Substate --None--

Assigned to Priority 4 - Low

Issue source Issue rating --None--

Issue type --None-- Configuration item

Classification --None-- Location

Issue manager group Watch list

Issue manager

* Name

Description

Went into controls for the linux vm

servicenow All Favorites History Admin Control objective - Restrict Public RDP Access (Port 3389)

Control objective Restrict Public RDP Access (Port 3389)

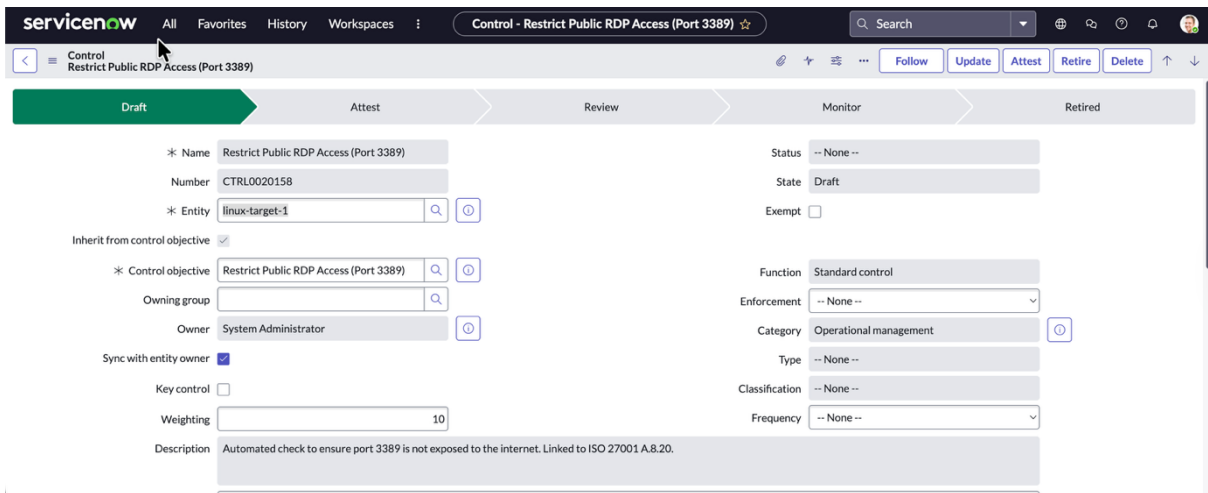
Entity types (1) Additional entities Policies Citations Control objectives Controls (104) Policy exceptions Issues Indicator templates Content references

Entity Search

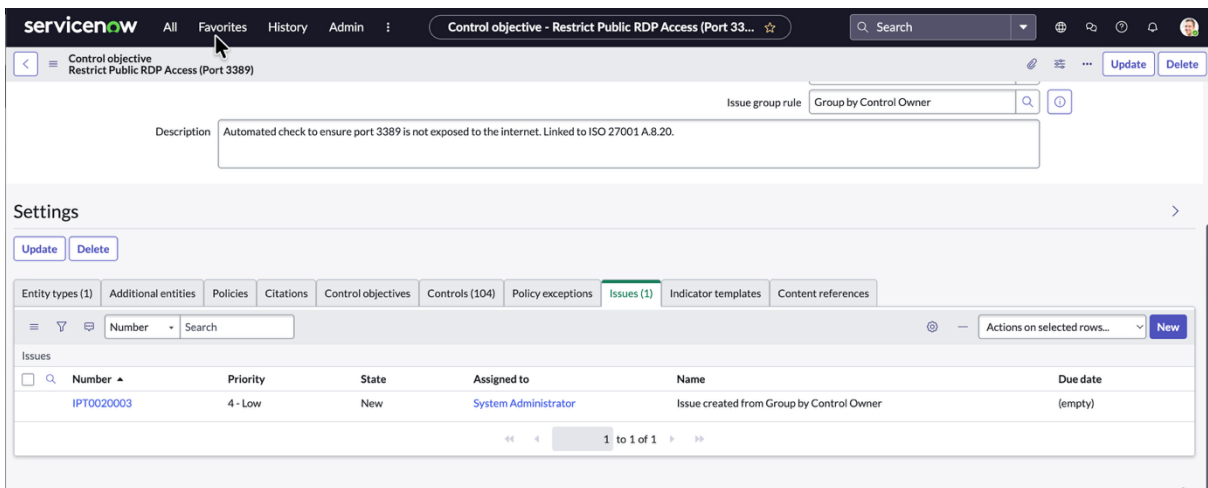
Control objective = Restrict Public RDP Access (Port 3389) Entity Name >= linux

Number	Name	Entity	Function	State	Status	Exempt	Owner	Description
CTRL0020073	Restrict Public RDP Access (Port 3389)	Linux-M1	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020181	Restrict Public RDP Access (Port 3389)	Linux-Programmatic-fx-Michael	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020158	Restrict Public RDP Access (Port 3389)	linux-target-1	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020027	Restrict Public RDP Access (Port 3389)	local-agent-win-11-test-clay	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020017	Restrict Public RDP Access (Port 3389)	LOCAL-SCAN-ENGINE-01	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020047	Restrict Public RDP Access (Port 3389)	Made-by-DGT	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...
CTRL0020097	Restrict Public RDP Access (Port 3389)	mads	Standard control	Draft		false	System Administrator	Automated check to ensure port 3389 is n...

Issue filled



Issue turns up under issues tab



Tenable vm did not show any vulnerabilities but decided to say it does have the RDP access vulnerability for the lab.

tenable Vulnerability Management | Scans > Scan Details

Quick Actions

Compliance Audit - linux-target-1

VULNERABILITY MANAGEMENT SCANS

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES | 0 MEDIUM VULNERABILITIES | 1 LOW VULNERABILITIES

Scan Details

STATUS: Completed
 START TIME: 02/03/2026 at 2:12 PM
 TEMPLATE: Basic Network Scan
 SCANNER: US Cloud Scanner

TARGETS: 20.57.2.159

SCANNER GROUPS: US Cloud Scanner

Vulns by Plugin | Vulns by Asset | History

Filters | 1 Result

	START TIME	END TIME	DURATION	STATUS	ACTIONS
1 Item	02/03/2026 at 2:12 PM	02/03/2026 at 2:23 PM	10min	Completed	

tenable Vulnerability Management | Scans > Scan Details

Quick Actions

Compliance Audit - linux-target-1

VULNERABILITY MANAGEMENT SCANS

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES | 0 MEDIUM VULNERABILITIES | 1 LOW VULNERABILITIES

Scan Details

STATUS: Completed
 START TIME: 02/03/2026 at 2:12 PM
 TEMPLATE: Basic Network Scan
 SCANNER: US Cloud Scanner

TARGETS: 20.57.2.159

SCANNER GROUPS: US Cloud Scanner

Vulns by Plugin | Vulns by Asset | History

Filters | Search | 19 Results

SEVERITY	NAME	FAMILY	INSTANCES
Low	ICMP Timestamp Request Remote Date Disclosure	General	1
Info	SSH Server Type and Version Information	Service detection	1
Info	SSH Protocol Versions Supported	General	1
Info	Nessus SYN scanner	Port scanners	1
Info	OS Identification	General	1
Info	Nessus Scan Information	Settings	1
Info	Service Detection	Service detection	1
Info	TCP/IP Timestamps Supported	General	1
Info	Backported Security Patch Detection (SSH)	General	1
Info	Common Platform Enumeration (CPE)	General	1
Info	Device Type	General	1
Info	SSH Algorithms and Languages Supported	Misc	1

Changed priority to High

servicenow All Favorites History Workspaces | Issue - Issue created from Group by Control Owner

Search

Issue created from Group by Control Owner

Discuss Follow Update Delete

New Analyze Respond Review Closed

Number: IPT0020003 | State: New

Assignment group: | Substate: -- None --

Assigned to: System Administrator | Priority: 2 - High

Issue source: Ad-Hoc | Issue rating: -- None --

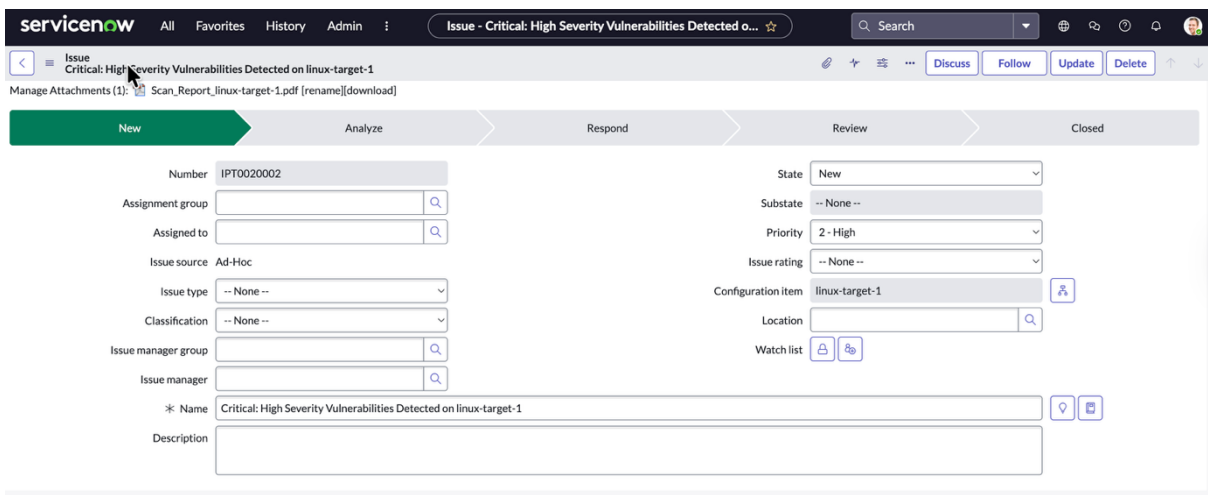
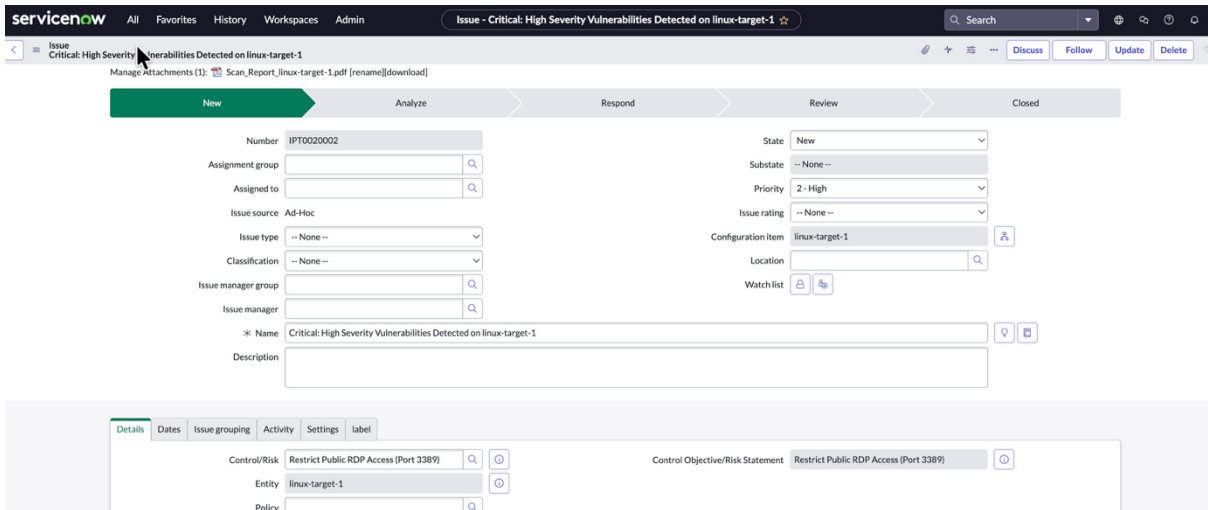
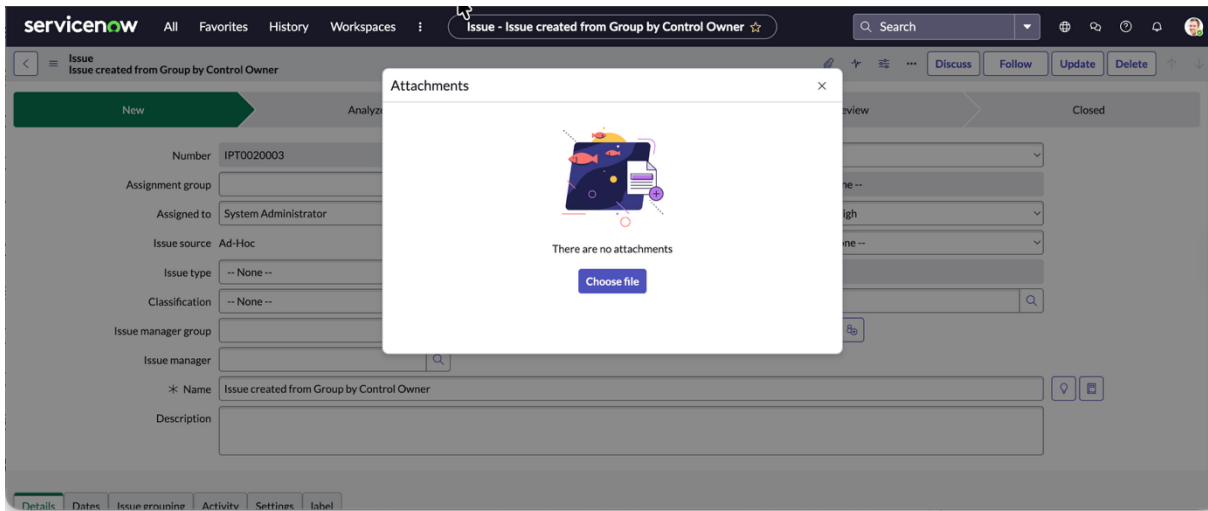
Issue type: -- None -- | Configuration item: | Location: | Watch list: [lock] [refresh]

Classification: -- None --

Issue manager group: | Issue manager: | Name: Issue created from Group by Control Owner

Description:

Attached the scan to the issue



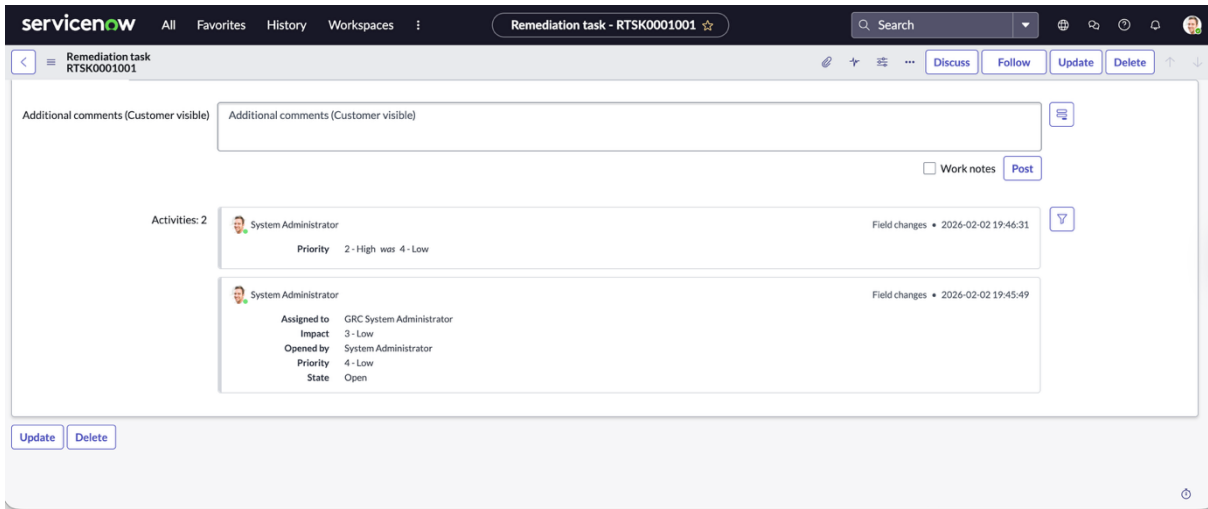
Added a remediation task

The screenshot shows the ServiceNow interface for an issue titled "Issue created from Group by Control Owner". The breadcrumb trail includes "Workspaces". Below the issue title, there are "Update" and "Delete" buttons. Under the "Related Links" section, there is a link for "Repair SLAs". A tabbed interface shows "Remediation tasks" as the active tab. Below the tabs is a search bar with "Number" selected and a search icon. The main content area is a table with columns: "Number", "Name", "Assigned to", "Priority", "State", and "Updated". The table is empty, displaying "No records to display" with a small icon.

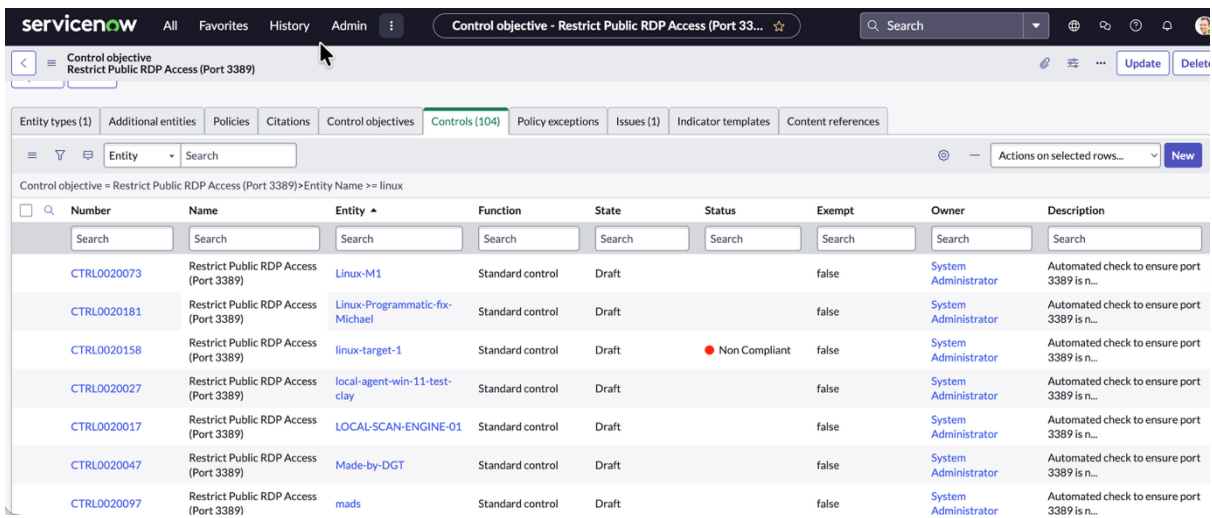
The screenshot shows the "Remediation task - Create RTSK0001001" form. At the top, there is a "Submit" button. Below it is a progress bar with stages: "Open" (highlighted in green), "Response", "Work in Progress", "Review", and "Closed". The form fields include: "Number" (RTSK0001001), "Assigned to" (GRC System Administrator), "Issue" (Issue created from Group by Control Own), "State" (Open), "Priority" (4 - Low), "Watch list" (lock and refresh icons), "Created" and "Updated" (empty fields), "* Name" (fix), and "Description" (Patch OpenSSL on linux-target-1). Below the form are tabs for "Notes and Comments" and "Task Schedule". A text area for "Additional comments (Customer visible)" is present.

The screenshot shows the ServiceNow interface for the same issue. The "Remediation tasks" tab is active, and the table now contains one record. The table has columns: "Number", "Name", "Assigned to", "Priority", "State", and "Updated". The record is: RTSK0001001, fix, GRC System, 2 - High, Open, 2026-02-02 19:45:50. Below the table, there are navigation arrows and "1 to 1 of 1".

Number	Name	Assigned to	Priority	State	Updated
RTSK0001001	fix	GRC System	2 - High	Open	2026-02-02 19:45:50



Checked the status under the controls tab



Closed the remediation by saying it is complete

servicenow All Favorites History Workspaces Remediation task - RTSK0001002

Remediation task
RTSK0001002

Open Response Work in Progress Review Closed

Number: RTSK0001002 State: Closed Complete
 Assigned to: [Search] Priority: 2 - High
 Issue: Critical: High Severity Vulnerabilities Detz [Search] [Info]
 Watch list: [Add] [Remove]
 Created: 2026-02-02 19:50:38
 Updated: 2026-02-02 19:53:36

* Name: Patch OpenSSL on linux-target-1 [Info] [Copy]
 Description: fixed

Notes and Comments Task Schedule

Additional comments (Customer visible): [Text Area]

servicenow All Favorites History Admin Issue - Critical: High Severity Vulnerabilities Detected o...

Issue
Critical: High Severity Vulnerabilities Detected on linux-target-1

[Update] [Delete]

Related Links
Repair SLAs

Policy exceptions Remediation tasks (1) Indicator results Task SLAs

Issue = Critical: High Severity Vulnerabilities Detected on linux-target-1

Number	Name	Assigned to	Priority	State	Updated
RTSK0001002	Patch OpenSSL on linux-target-1	(empty)	2 - High	Closed Complete	2026-02-02 19:54:39

1 to 1 of 1

servicenow All Favorites History Admin Control objective - Restrict Public RDP Access (Port 33...

Control objective
Restrict Public RDP Access (Port 3389)

Description: Automated check to ensure port 3389 is not exposed to the internet. Linked to ISO 27001 A.8.20.

Settings

[Update] [Delete]

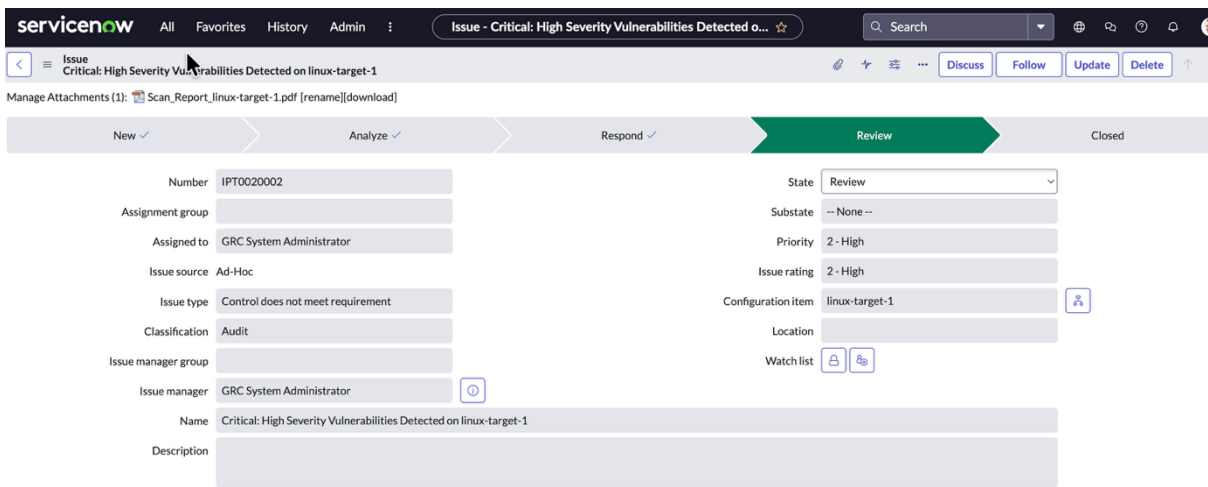
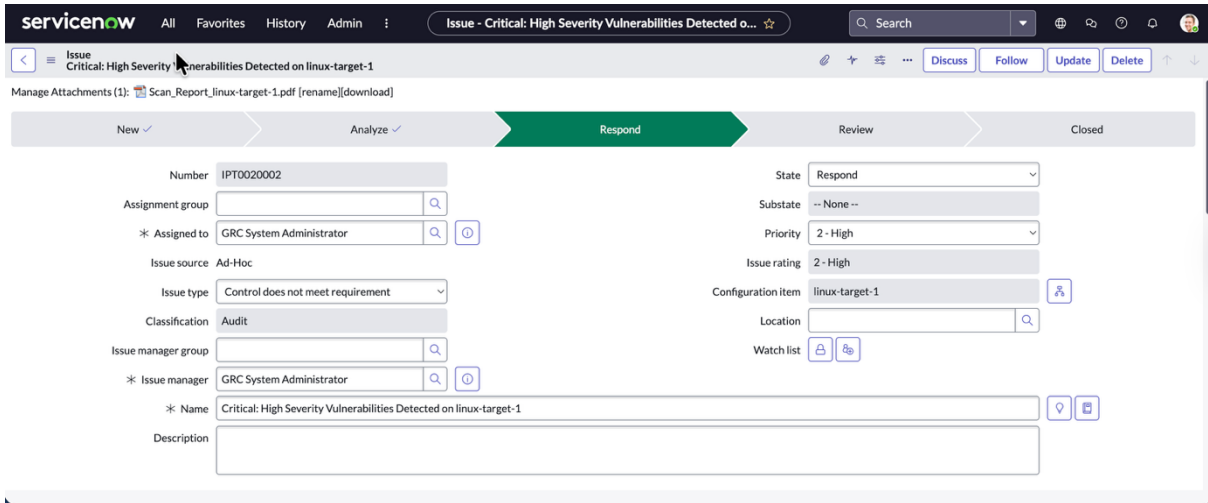
Entity types (1) Additional entities Policies Citations Control objectives Controls (104) Policy exceptions Issues (1) Indicator templates Content references

Issues

Number	Priority	State	Assigned to	Name	Due date
IPT0020002	2 - High	Analyze	GRC System Administrator	Critical: High Severity Vulnerabilities Detected on linux-target-1	2026-02-06 20:01:33

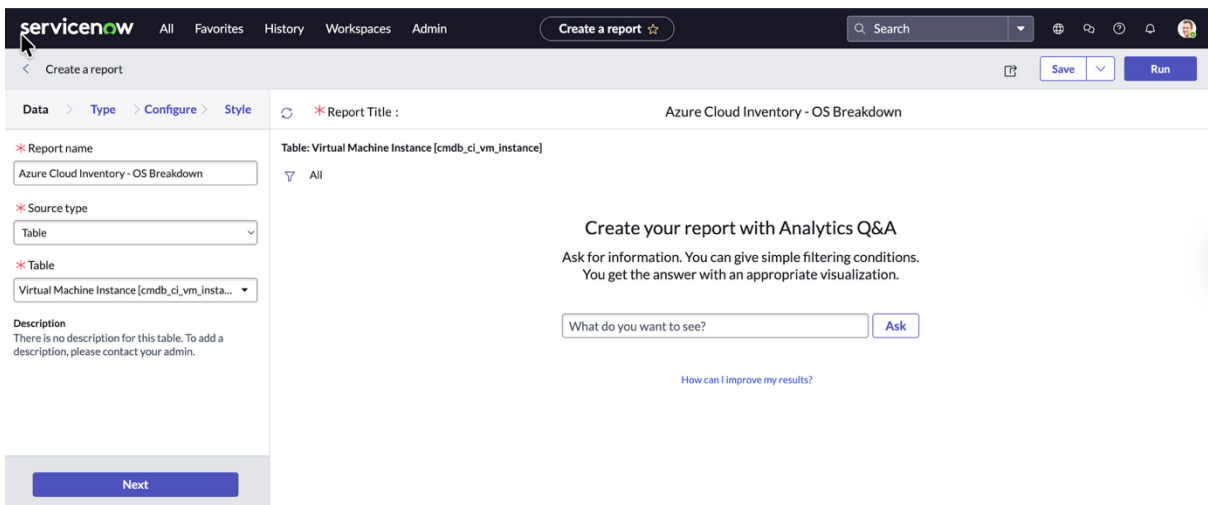
1 to 1 of 1

Went through the lifecycle of the issue



Closed the issue saying it is complete

Decided to create a table



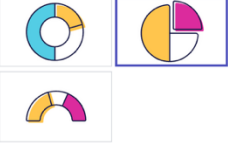
servicenow All Favorites History Workspaces Admin Create a report ☆ Search

Create a report Save Run

Data > Type > Configure > Style

Filter the visualizations

Pies and Donuts
Pies and Donuts show the proportions that make up a whole.



Time series

Back Next

* Report Title : Azure Cloud Inventory - OS Breakdown

Type a question about your data
What do you want to see? Ask How can I improve my results?

To modify the current report, use the left panel or Edit Condition.

Table: Virtual Machine Instance [cmdb_ci_vm_instance]

All

Name	Object ID	Class	State	CPU	Memory (MB)	Disks	Disks size (GB)	Network adapters
aafbc1288	bffa9e5-0a1b-4683-bdb4-af8160c80995	Virtual Machine Instance	VM deallocated					
aaron-vm-test	bfcdfb5d-de43-4419-917f-655b13c8db25	Virtual Machine Instance	VM deallocated					
Abdiaziz	50e2dc3d-58a9-46b9-a63c-3fed5a93b7a9	Virtual Machine Instance	VM deallocated					
Alex-mde-test	553a5a64-e552-480a-9912-b3bad2e9726f	Virtual Machine Instance	VM deallocated					
Alexander-Win11-	7f89f5d6-14d0-4b0c-9a10-	Virtual Machine	VM					

servicenow All Favorites History Workspaces Admin Create a report ☆ Search

Edit report Save Run

Data > Type > Configure > Style

General Title

Show chart title Report only

Chart title

Size of the chart title 16 px

Chart title color Black

Title horizontal alignment Center

Title vertical alignment Top

Back Share

* Report Title : Azure Cloud Inventory

Ask another question

Table: Virtual Machine Instance [cmdb_ci_vm_instance]

All

Azure Cloud Inventory
187

Sharing

Share

Add to Dashboard

End of lab.