Welcome to Nutanix Security Bootcamp!

The Story

Blips and Chitz Inc. is a hugely popular entertainment arcade that supports gaming machines, a payment application, desktops for corporate staff, and a customer information database.

From a strategic perspective, properly protecting this data helps maintain the company's competitive advantages. All of the collected customer information and payment card details must be kept confidential due to strict regulatory guidelines including, but not limited to:

- PCI DSS - The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.
- CCPA - The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.
- GDPR - The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

Blips and Chitz Inc. have just purchased a Nutanix cluster to support production workloads.

You are the sole Security Engineer, and your responsibilities are both varied and numerous. You don't have a lot of time to learn new security tools and operating systems, let alone spend weeks or longer on dedicated training in order to deploy these tools in production. Simply put, you need security to just work.

In terms of your background, you have some familiarity with the Linux command line, but would likely need help with certain commands. You understand basic networking security principles, but you're unfamiliar with new technologies like micro-segmentation. Lastly, you have zero experience with analytics platforms, and data archiving technologies like object based write-one ready-many (WORM) enabled data protection.

You forward all logs to a syslog server, then use a SIEM (Security Incident Event Management) which is used by an outsourced SOC (Security Operations Center). For audit purposes, you have to be able to show evidence of log collection for the platform and for the virtual infrastructure powering Blips and Chitz Inc. Your boss Roy has requested that the Nutanix cluster be ready to support production workloads by the end of the week. This tight timeline is driven in part because a new Qualified Security Assessor (QSA) will be visiting next week to begin to conduct the annual Blips and Chitz Inc. security audit for PCI DSS. While you immediately voiced your concerns that this time frame isn't feasible, Roy knows you'll try your best to implement this new platform ahead of the audit.

While you drank this morning's coffee, you read about a new variant of ransomware known as Krombopulous. It is gaining notoriety, and has recently been effective at disrupting the local hospital. This new malware variant is highly adaptable and pervasive, which is what prompted Blips and Chitz Inc. to purchase additional Nutanix products to further protect the company's sensitive data on this cluster. Rick Sanchez, the Systems Architect, sent you a **Tech Brief** which outlines the benefits to utilizing these products.

If all this wasn't enough, Roy wants you to demonstrate to the board how these tools can be used to limit the exposure of ransomware within the Nutanix cluster, thus giving the board members peace of mind when considering expansion of this environment. The board meeting is at the end of the week.

Last Updated: 5/26/2023, 1:44:20 PM

Getting Started →

Getting Started

Welcome to the Nutanix Security Bootcamp!

This bootcamp highlights the intrinsic security benefits of our core platform, and the data plane security enhancements available via microsegmentation, analytics, and any automation that can be leveraged to prevent, detect, and recover from malware attacks such as ransomware.

What's New

Last updated 2023-05-25

Labs are updated for the following software versions:

- AOS: 6.5.2.5 LTS
- PC : pc.2022.6.0.3
- Files: 4.2.1.1
- Files Analytics: 3.2.1

Agenda

- Introductions
- Lab Setup

Security Labs

- Prevent
  - Secure Access & System Hardening
  - Authentication
  - Security Technical Implementation Guides (STIGs)
- Detect - Networking
  - Securing the Virtual Infrastructure
  - Categorization
  - Securing Applications
  - Isolate Environments
- Detect - Data Services
  - Monitoring Data Services
  - File Analytics
  - File Analytics Ransomware Protection
  - Nutanix Objects
- Protect and Recover
  - Preparing For Disaster
  - Protecting Your Environment

Optional Labs (Instructor Led)

- Simulating An Attack
- Configuring A Syslog Server

Last Updated: 5/26/2023, 1:44:20 PM

← The Story

Environment Details →

Environment Details

Nutanix Bootcamps are intended to run within the Nutanix Hosted POC (HPOC) environment. Your cluster contains all the necessary images, networks, and VMs to complete the exercises.

> **Danger**
>
> Do not perform any upgrades to the environment, including but not limited to Prism Element (PE), Prism Central (PC), Acropolis Operating System (AOS), Nutanix Cluster Check (NCC), Foundation, any hardware-specific updates (ex. firmware), and any software within any remote sessions (ex. Graylog, Linux packages, PuTTY, Sublime Text).
>
> Doing so will negatively impact your lab experience and potentially any other attendees using this cluster.

Remote Connection

Your instructor will provide you with username and passwords to get connected to our remote environment. Visit the **Accessing the Environment** section in the Appendix for more details on each of the connection methods provided.

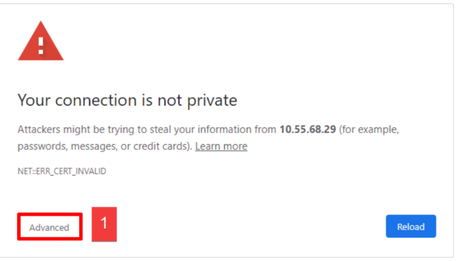
> **Warning!**
>
> Always use applications within the remote session. Otherwise, the version you use may look or operate differently, negatively impacting your ability to complete the lab in the allotted time. Additionally, this aids with handling downloaded files, as all files would be within the remote session.

Know Before You Go

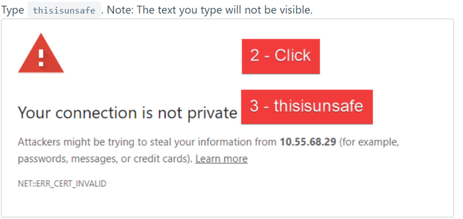
- Never use the information within screenshots in your environment (ex., IP addresses.) Screenshots are shown for illustration purposes only.
- Ignore any IP addresses that resemble **169.254.###.###**.
- Throughout the lab, you will see the usage of **##**. Replace the **##** with your assigned user number (ex., User01).

  For example:

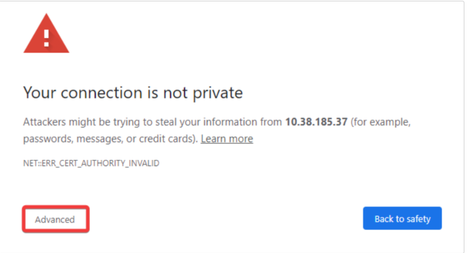
  - Active Directory user - adminuser**01**@ntnxlab.local
  - Windows Tools VM: User**01**-WinTools
  - VDI/VPN: DM3-POC020-User**04**
- Anywhere you see `<CVM-PASSWORD>` please use the password provided by the instructor.
  - This is the same password as you used to access the remote environment.
- The cluster's time zone is UTC (previously GMT).
- If instructed to:
  - SSH (Secure Shell): Use PuTTY within your desktop's *Tools* folder.
  - Remote Desktop, Remote Desktop Protocol (RDP), or Remote Desktop Connection (RDC): **Remote Desktop Connection** via **Start Menu** > **Remote Desktop Connection**.
- If you are presented with a security warning in Chrome, use one of the following methods to proceed.
  - Method 1
    1. Click **Advanced**.



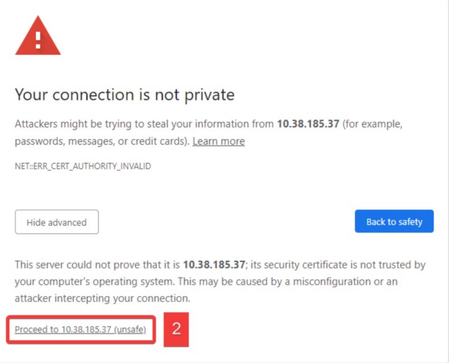
    2. Click on any blank section within the main browser window.
    3. Type `thisisunsafe` . Note: The text you type will not be visible.



  - Method 2
    1. Click **Advanced**



    2. Click **Proceed to *IP-ADDRESS* (unsafe)**.



Last Updated: 5/26/2023, 1:44:20 PM

Secure Access & System Hardening

You have just been informed that the deployment of the cluster has completed, and the access details have been emailed to you. Your first job is to ensure that the platform is hardened according to **NIST SP800-53** guidelines, and that all system default passwords are changed from the vendor-supplied defaults.

When trying to get acquainted with Nutanix, you received a **Tech Note: TN-2026** from your Nutanix Account team.

You think back to all the time and effort you've previously poured into hardening and maintaining alignment to a secure baseline for the previous infrastructure. If all that is truly no longer required to make this Nutanix cluster production-ready, it could mean shaving off a considerable amount of time.

STIGs (Security Technical Implementation Guide) are a hardening guide, used to perform the process of system and security hardening, each Nutanix node in a cluster is covered by these STIGs, to harden both the hypervisor (AHV) and the Controller VM (CVM) which provides all of the Nutanix services. To satisfy the compliance requirements, you can now provide evidence of this system state via the STIG report of the nodes.

Last Updated: 5/2/2023, 11:07:35 AM

Authentication →

Authentication

Changing Vendor Default Passwords

Changing vendor default passwords is an essential first step in the adoption of new platforms, and is often tested and measured in many compliance assessments. Failure to address this early critical step in system configuration can result in effectively leaving an open door to an attacker.

In a Nutanix deployment, there are several default passwords that we'll demonstrate how to change.

Even though the Nutanix cluster you are using is dedicated to the Bootcamp, all of our automation is based on the current configured passwords. Changing those passwords will break our internal automation system. Instead, we are providing you with a video describing the process.

The first of which is Prism Element. Upon first log in, you are required to create a new, secure password for the local *Admin* account.

AHV is protected with a local account, with credentials **hashed** and **salted** for further protection from potential **brute force** or **dictionary attacks**.

How to Change the AHV Passwords Video

The CVM has two local accounts: *Nutanix* and *Admin*.

How to Change the CVM Passwords Video

The Intelligent Platform Management Interface (IPMI) is a way for remote administrators to ascertain the hardware state of the infrastructure Nutanix is running upon. In compliance with **California statute SB-327**, these are set using a unique password.

- Username - `admin`
- Password - `<NODE-SERIAL-NUMBER>`

How to Change the IPMI Password Video

Cluster Lockdown

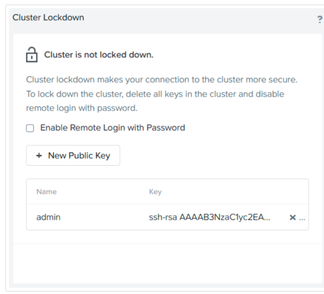
There are several options available within *Cluster Lockdown* section. You can enable or disable remote login via password, SSH key, or both. Disabling both remote login methods will enable *Cluster Lockdown*.

To further protect access to your cluster, you have the option of introducing a layer of **non-repudiation** to your access method. You can replace SSH password-based authentication with a public SSH key. Only the holder of the corresponding private key will be able to login.

1. Open `https://<PRISM-CENTRAL-IP>/` in a new browser tab, and log in.
2. Within Prism Central, select ☰ > **Prism Central Settings** > **Security** > **Cluster Lockdown**.

   From this screen you could provide the name, along with your public key for key based authentication. To ensure full protection, you would uncheck the *Enable Remote Login with Password* box to disable remote login via password.

   > **Note**
   > You'll notice your cluster is pre-configured to prevent password authentication and instead has provided an SSH key for the admin user.



3. Click the `Enable Remote Login with Password` checkbox and click **OK** to enable SSH access for steps later in this guide.

Directory Services and Identity Providers

The local *admin* user account should be protected via SSH keys, rather than a password. For regular day-to-day access by team members and end-users, a more secure way to provide member access to Prism is with the use of *Directory Services*. No passwords or hashes are stored on the cluster for directory services users, as authentication is passed through to the directory.

> **Note**
> While the Active Directory server (AutoAD) is already included, we've provided the below steps to illustrate what would be required to use an Active Directory (AD) environment.

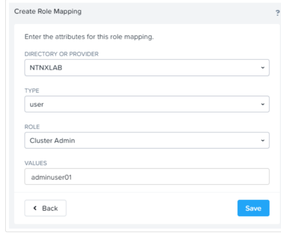
1. Within Prism Central, select ☰ > **Prism Central Settings** > **Users and Roles** > **Authentication**, and then click **+ New Directory**.

   > **Note**
   > As you may have noticed in Prism Central, if you visit the *Authentication Configuration* menu, you have the option to connect to an Identity Provider (IdP), this further enhances access protocols by leveraging technologies like Single Sign On (SSO) and Multi-Factor Authentication (MFA).
   >
   > Currently Prism Central only supports Active Directory Federation Services (ADFS) as part of the SAML protocol. But you can register your appropriate account metadata in the same *Authentication Configuration* menu used above.

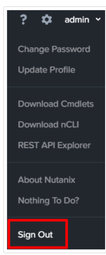
2. Once you are finished reviewing the *Authentication Configuration* section, click **Back**.

   To complete Active Directory configuration, you must map AD users to Prism Central roles.

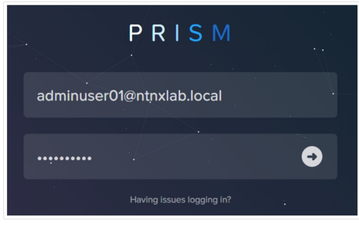
3. Under *Users and Roles*, select **Role Mapping**, and then click **+ New Mapping**.
4. Specify `adminuser##` within the *Values* field, select **Cluster Admin** from the *ROLE* drop-down, and then click **Save**.



5. Log out of Prism Central.



6. Log in to Prism Central as *adminuser##*. (ex. `adminuser01@ntnxlab.local`).



> **Note**
> Continue to use *adminuser##* for Prism Central throughout the rest of the labs.

Last Updated: 5/26/2023, 1:44:20 PM

Nutanix Security Bootcamp

The Story

Getting Started

Environment Details

Prevent

Secure Access & System Hardening

Authentication

Security Technical Implementation Guides (STIGs)

STIG Reports on Nutanix Nodes

Analyzing the STIG Report

Security Configuration Management Automation (SCMA) Self-Healing Lab

Testing Automation

Takeaways

Security Technical Implementation Guides (STIGs)

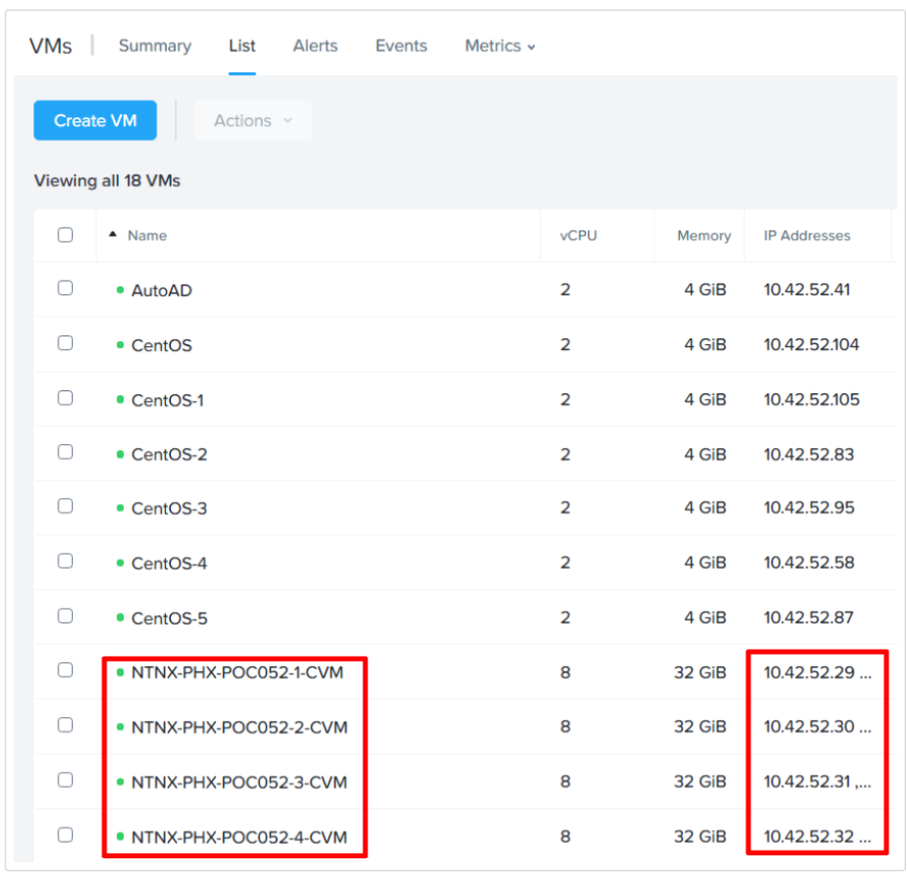
Security is in the DNA of the Nutanix platform. As a result, a significant portion of our business is from sectors of industry that care deeply about security, including federal, local, and state governments, financial services, healthcare, retail, and beyond. Security is automatically part of every configuration and deployment, enabled by default, and continuously monitored for compliance against the security baselines. Nutanix doesn't just have a single STIG, we apply multiple STIGs automatically, and continuously verify against them.

> **Note**
>
> What is a STIG?
>
> The description of a STIG is publicly available on the Defense Information Systems Agency, Information Assurance Support Environment web site:
>
> The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, Defense Information Systems Agency (DISA) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to lock down information systems and software that might otherwise be vulnerable to a malicious computer attack.

STIG Reports on Nutanix Nodes

You can run a STIG report, which will check on all the individual STIG controls, and verify which are compliant with your system, and which are not.

1. Within *Prism Central*, select ☰ > **Compute & Storage** > **VMs**.
2. If there are any filters listed in the search bar in the top left-hand corner, click the ✕ to clear them.
3. Observe the IP address of any CVM, which will be named as *NTNX-<DATACENTER>-<CLUSTER>-#-CVM* as shown below.



4. SSH into any CVM via Terminal, PuTTy, or similar using the following credentials:

- **User Name** - `nutanix`
- **Password** - `<CVM-PASSWORD>`

5. Change to the root directory of the CVM:

```
cd /
```

6. List the files available to the root user within the `/root` directory:

```
sudo -u root ls -l /root
```

Executable files contain *x* in the permission string, as shown in this sample output:

```
nutanix@NTNX-16SM6B260127-A-CVM:10.42.13.29:/$ sudo -u root ls -l /root
total 260
-rw-------. 1 root root   3416 Nov 13  2020 anaconda-ks.cfg
drwxr-x---. 2 root root   4096 Oct 18 16:07 filesystems
-rw-r-----. 1 root root   1132 Sep 16 07:32 homeaudit.pp
-rw-r-----. 1 root root   1510 Sep 16 07:32 inimfile.pp
-rw-r-----. 1 root root    489 Sep 16 07:32 inimfile.te
-rw-r-----. 1 root root   1231 Sep 16 07:32 my-runcon.pp
-rw-r-----. 1 root root    464 Sep 16 07:32 my-runcon.te
-rwxr-x---. 1 root root  12048 Sep 16 07:32 report_open_jre8_stig.sh
-rwx------. 1 root root 135482 Oct  7 21:05 report_stig.sh
-rwxr-x---. 1 root root  71039 Sep 16 07:32 report_web_stig.sh
-rwx------. 1 root root   1264 Sep 16 07:34 scap_report.sh
drwxr-x---. 2 root root   4096 Oct 18 16:12 sretools
-rw-r-----. 1 root root    840 Sep 16 07:32 sshdlocal.pp
```

There are three files that end in `\_stig.sh`, where its name corresponding to the output format it will display.

7. In this example, we'll run the generic text output:

```
sudo -u root ./root/report_stig.sh
```

The output will be written to the root user log folder.

8. List the files in the folder, and note the name of the report.

```
sudo -u root ls -l /home/log | grep STIG
```

9. Copy the report to the Nutanix home directory, substituting the actual file name for the asterisks.

```
sudo -u root cp /home/log/STIG-report-**-**-****-**-**-** /home/nutanix
```

10. List the files in the /home/nutanix folder.

```
ls -l ~
```

11. Change the owner of the report file to be the Nutanix user, substituting the actual file name for the asterisks.

```
sudo -u root chown nutanix:nutanix /home/nutanix/STIG-report-**-**-****-**-**-**
```

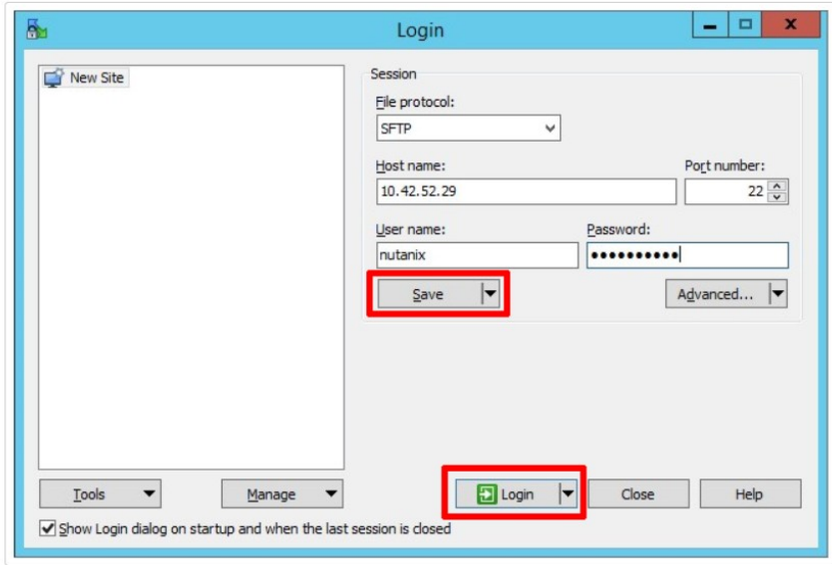
12. Log in to your *USER##*-WinTools VM using the following credentials:

- **User Name** - `adminuser##@ntnxlab.local`
- **Password** - `nutanix/4u`

13. Open **WinSCP** from within the *Tools* folder on the desktop.

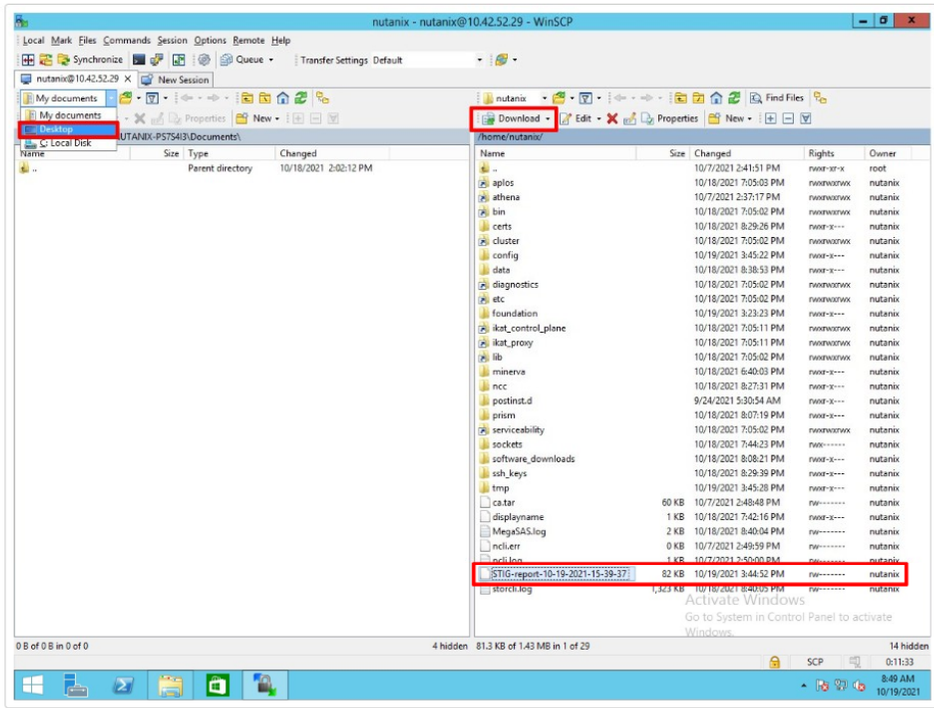
14. Fill out the following fields, click **Save**, and then click **Login**.

- **Host name** - `<CVM-IP-ADDRESS>`
- **User name** - `nutanix`
- **Password** - `<CVM-PASSWORD>`



15. Within *WinSCP*, select **Desktop** from the top left-hand corner drop-down.

16. Select the `STIG-report-<date>` file, click **Download**, and then click **OK**.



17. Close *WinSCP* and the *Tools* folder window.

Analyzing the STIG Report

You now have the STIG report, and can use it to evaluate the current compliance state of the system, or for validation and accreditation requirements for security compliance.

This will report the results of all elements that make up the Nutanix STIG, and the report will show the compliance result for each of the checks contained within the STIG.

1. Right-click on the `STIG-report-<date>` file on your *USER##*-WinTools VM desktop, and choose either **Open with Code** or **Open with Sublime Text**.

Report Format

```
The first sentence says the check name
The second sentence is an explanation of the check
The third sentence is the legend for the result of the check
The fourth sentence is the result of the check
The fifth sentence is the completion status of the check
```

Example of a Finding

```
CAT I RHEL-07-021710 SRG-OS-000095-GPOS-00049 CCI-000381 CM-7 a, CM-7 b
The telnet-server package must not be installed.
The result of the check should be yes.  If no, then it's a finding
no
Completed.
```

Example of a Non-Finding

```
CAT II RHEL-07-021030 SRG-OS-000480-GPOS-00227 CCI-000366 CM-5 (1)
All world-writable directories must be group-owned by root, sys, bin, or an application group.
The result of the check should be yes.  If no, then it's a finding
yes
Completed.
```

Security Configuration Management Automation (SCMA) Self-Healing Lab

To make a system truly scalable, it must address security misconfigurations automatically, whether you're managing four nodes or four hundred.

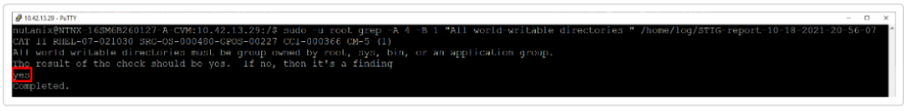
With Nutanix, Security Configuration Management is automated with SCMA. SCMA is a **saltstack daemon** that runs as a scheduled **cron** job. If the daemon spots an inconsistency, it both corrects and logs the event. The CVM self-heals deviations to the secure state. This state is established according to industry best practices, along with information we've gathered over the years from our customers.

Testing Automation

From the report you generated in **STIG Reports on Nutanix Nodes** download it or access it from the console in order to get the state of the check *All world-writable directories must be group-owned by root, sys, bin, or an application group*. The result of the check should be *yes*.

1. Return to your SSH session.
2. We will now test to confirm the system is self-healing from security violations via SCMA. The result of the check should be *yes*, as shown below.

   `sudo -u root grep -A 4 -B 1 "All world-writable directories " /home/log/STIG-report-**-**-****-**-**-**`

   Now we'll compromise the system, so that the result of this check is *no*, and then manually fix the issue.

3. Verify the current ownership.

   `sudo -u root ls -l / | grep tmp`

   ```
   nutanix@NTNX-16SM6B260127-A-CVM:10.42.13.29:/$ sudo -u root ls -l / | grep tmp
   drwxrwxrwt.  12 root root  4096 Oct 19 16:37 tmp
   ```

4. Change the group ownership.

   `sudo -u root chown root:nutanix /tmp`

5. Verify the ownership change:

   `sudo -u root ls -l / | grep tmp`

   ```
   nutanix@NTNX-16SM6B260127-A-CVM:10.42.13.29:/$ sudo -u root chown root:nutanix /tmp
   nutanix@NTNX-16SM6B260127-A-CVM:10.42.13.29:/$ sudo -u root ls -l / | grep  tmp
   drwxrwxrwt.  12 root nutanix  4096 Oct 19 16:38 tmp
   ```

6. Re-run the report to see if this change has been detected.

   `sudo -u root ./root/report_stig.sh`

   `sudo -u root grep -A 4 -B 1 "All world-writable directories " /home/log/STIG-report-**-**-****-**-**-**`

   The result of the check is *no*, indicating a finding.

```
nutanix@NTNX-16SM6B260127-A-CVM:10.42.13.29:/$ sudo -u root grep -A 4 -B 1 "All world-writable directories " /home/log/STIG-report-10-19-2021-16-41-39
CAT II RHEL-07-021030 SRG-OS-000480-GPOS-00227 CCI-000366 CM-5 (1)
All world-writable directories must be group-owned by root, sys, bin, or an application group.
The result of the check should be yes. If no, then it's a finding.
no
Completed.
```

7. Run the *salt-call* command to fix this vulnerability.

```
sudo -u root salt-call state.sls security/CVM/fdpermsownerCVM
```

8. List the directory again, and note that the "compromise" has been reverted.

```
sudo -u root ls -l / | grep tmp
```

```
nutanix@NTNX-16SM6B260127-A-CVM:10.42.13.29:/$ sudo -u root ls -l / | grep tmp
drwxrwxrwt.  12 root root  4096 Oct 19 16:53 tmp
```

In this example, we manually ran the *salt-call* command. It is set to automatically run all checks on a daily basis by default. You can adjust the cadence of this check to run hourly, if so desired.

9. Close your SSH session.

Takeaways

- Nutanix uses STIGs to verify compliance.
- Nutanix uses daily checks to self-remediate issues.

Last Updated: 5/26/2023, 1:44:20 PM

← Authentication

Securing the Virtual Infrastructure

Your first hands-on experience with Nutanix was productive. You were impressed that it was all accomplished in less than a day. The automation helped alleviate much of the "grunt work" you used to complete on a quarterly basis, if not more often.

As you sit down at your desk, sipping your coffee, you log in to the Nutanix console to notice that VMs are already starting to be created. Your peers don't waste any time, do they?

This gives you pause. This cloud-like consumption method, while great for end-users, could quite easily get out of hand if the VMs they create aren't appropriately (and automatically!) protected. You recall a session that Rick gave on Flow micro-segmentation. It began by assigning categories to VMs, so they could later be acted upon as a logical group, such as being protected with policies for security and backup.

Nutanix Flow provides:

- Multiple system categories out of the box that are used to quickly group virtual machines. Security policies can then be applied using these categories. You can choose the existing categories, or add your own.
- A detailed visualization of communications between VMs, which can aid in categorizing and grouping workloads, making it simple and straight-forward to set the right policies for the environment.

> **Note**
>
> Nutanix Flow has already been enabled for this environment, however we've include the steps required below.

1. Within Prism Central, select ☰ > **Prism Central Settings**.
2. Under *Flow*, select **Microsegmentation**.
3. Select the **Enable Microsegmentation** check box, and then click **Save**.

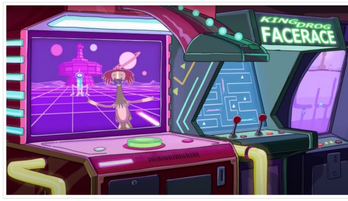
Last Updated: 5/2/2023, 11:07:35 AM

Categorization →

Categorization

You observe that VMs are already being created to support one of the most popular gaming apps, King Drog FaceRace. This workload is supported centrally by the Nutanix cluster, and delivered via the gaming machines on the game floor via the following VMs:

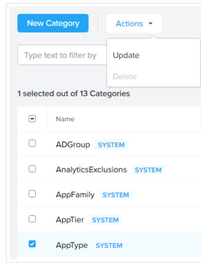
- `User##` -FaceRace-Web
- `User##` -FaceRace-DB



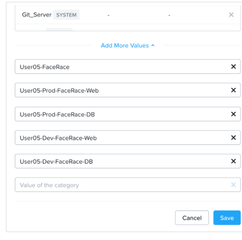
Customers swipe their payment cards for access to game credits, and log in to track high scores. These machines collect cardholder data (CHD) such as the primary account number (PAN) and other personally identifiable information (PII). These VMs need to be isolated from the rest of the network in order to meet PCI DSS guidelines for segmentation of the cardholder data environment (CDE). The payment and user information must be protected from unauthorized access.

Prism Central uses categories as metadata to tag VMs to determine how policies will be applied. We need to add categories to identify all of our *King Drog FaceRace* application VMs.

1. Within *Prism Central*, select ☰ > **Administration** > **Categories**.
2. Select the checkbox for **AppType**, and then click **Actions** > **Update**.



3. Click the `Add More Values` link to add additional category values.
4. We need to add multiple category values to manage the app along with the different tiers of the FaceRace application. Enter each of the category values liste below. As you add each value, a new input box will appear for you to enter another value.
   - **User ##** -FaceRace
   - **User ##** -Prod-FaceRace-Web (*Production* Web tier)
   - **User ##** -Prod-FaceRace-DB (*Production* Database tier)
   - **User ##** -Dev-FaceRace-Web (*Development* Web tier)
   - **User ##** -Dev-FaceRace-DB (*Development* Database tier)

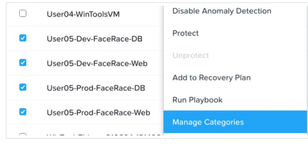


   Once you have entered all the values, click **Save**.
5. Deselect the checkbox for **AppType**, select the checkbox for **AppTier**, and then click **Actions** > **Update**.
6. Click the `Add More Values` link and add each of the additional category values:
   - **User ##** -Web
   - **User ##** -Database
7. Click **Save**.

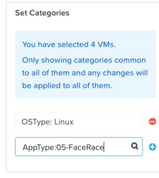
Assigning Categories to VMs

In this exercise, you'll assign your custom categories to the VMs supporting *King Drog FaceRace*. This will help align access to the proper resources, security, and protection policies within the environment.

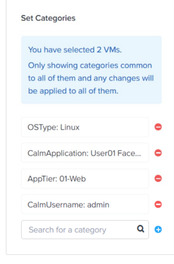
1. Select ☰ > **Compute & Storage** > **VMs**.
2. Select all four of your **User##-FaceRace** VMs, and then click **Actions** > **Manage Categories**.



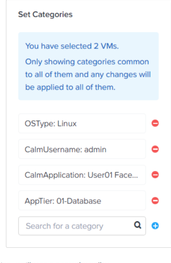
   By selecting more than one VM, we're simultaneously defining categories values that will be common to them: the AppType category value that we defined earlier.
3. In the search bar, enter **AppType:User##-FaceRace**, click ⊕, and then click **Save**.



   We now need to assign the appropriate tier category value to each of the VMs.
4. Deselect both **User##-FaceRace-DB** VMs, and then click **Actions** > **Manage Categories**.
5. In the search bar, type **AppTier:User##-Web**, click the ⊕, and then click **Save**.



6. De-select the **User##-FaceRace-Web** VMs, select the **##-FaceRace-DB** VMs, and then click **Actions** > **Manage Categories**.
7. In the search bar, type **AppTier:User##-Database**, click the ⊕, and then click **Save**.



Next, we'll create a security policy.

Securing Applications

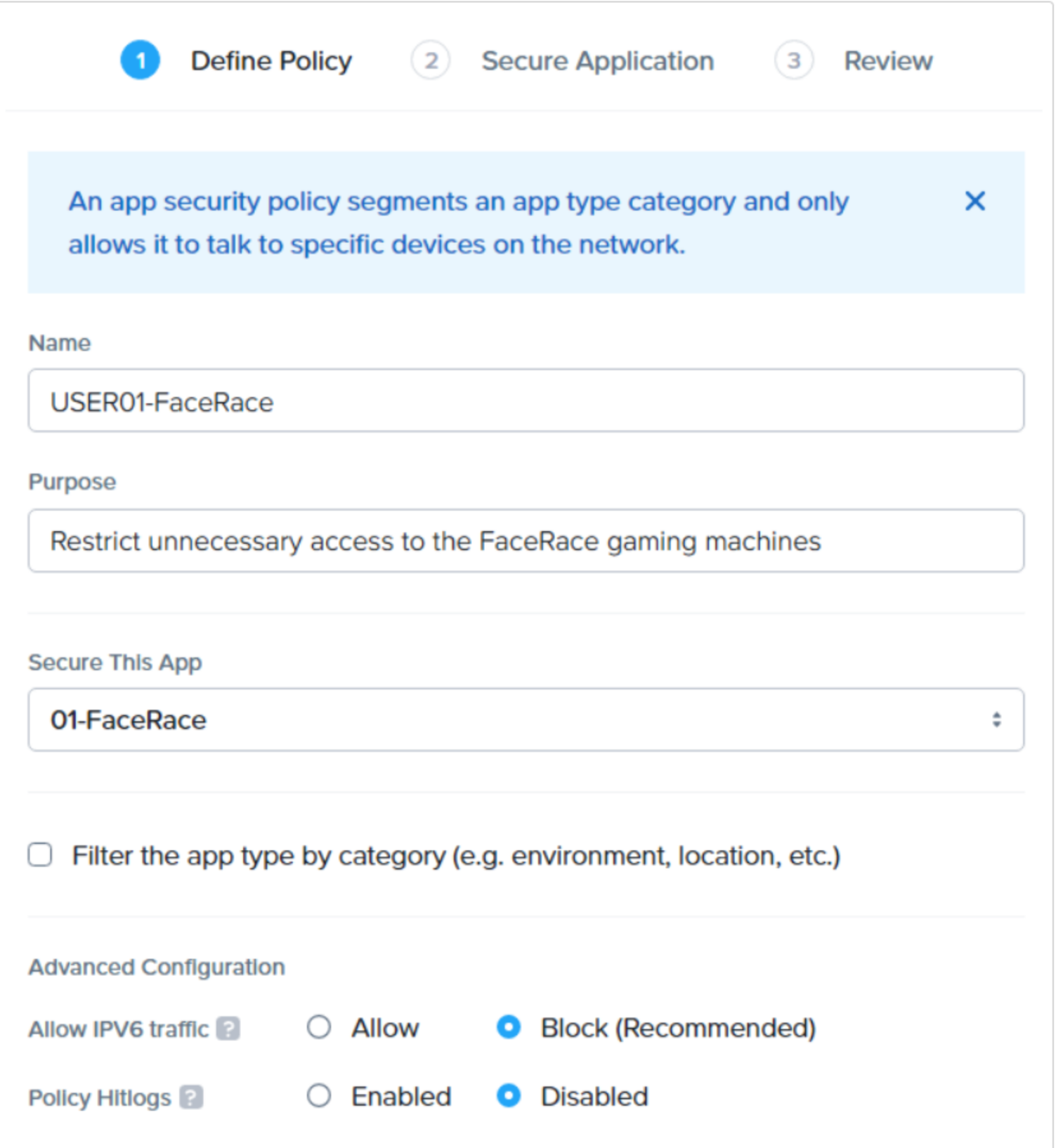
Creating Security Policy

Now that we've defined some categories, and assigned them to the respective VMs, we can begin to use those categories to form security policies that will be used to control traffic amongst these VMs. This capability is part of Flow micro-segmentation.

Flow is an application-centric network security product, which is tightly integrated into Nutanix AHV and Prism Central. Flow provides rich network traffic visualization, automation, and security for VMs running on AHV.

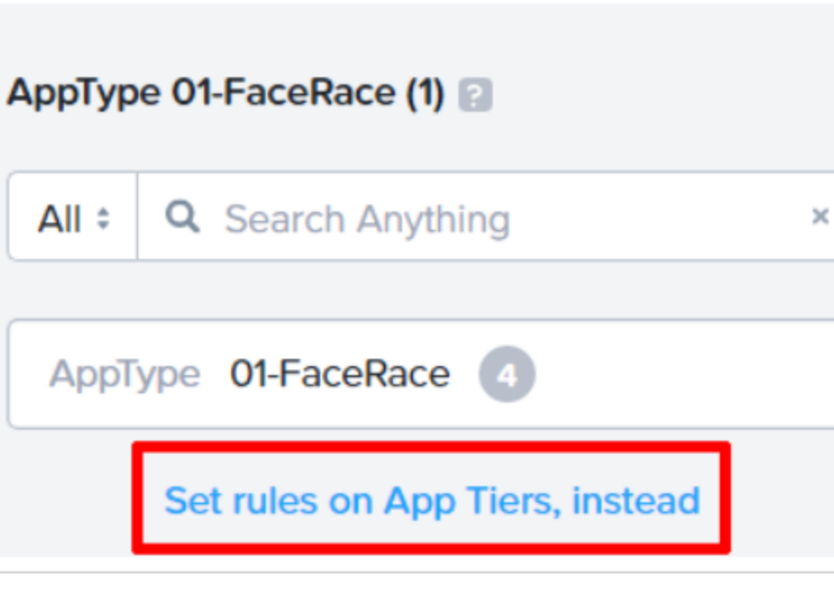
Microsegmentation is a component of Flow that uses simple policy-based management to secure VM networking. Using Prism Central categories, you can create a powerful distributed firewall.

1. Within *Prism Central*, select ☰ > **Network & Security** > **Security Policies**.
2. Click **Create Security Policy** > **Secure Applications (App Policy)** > **Create**.
3. Fill out the following fields, and then click **Next**.
   - **Name** - `USER##` -FaceRace
   - **Purpose** - Restrict unnecessary access to the FaceRace gaming machines
   - **Secure This App** - Apptype: `##` -FaceRace

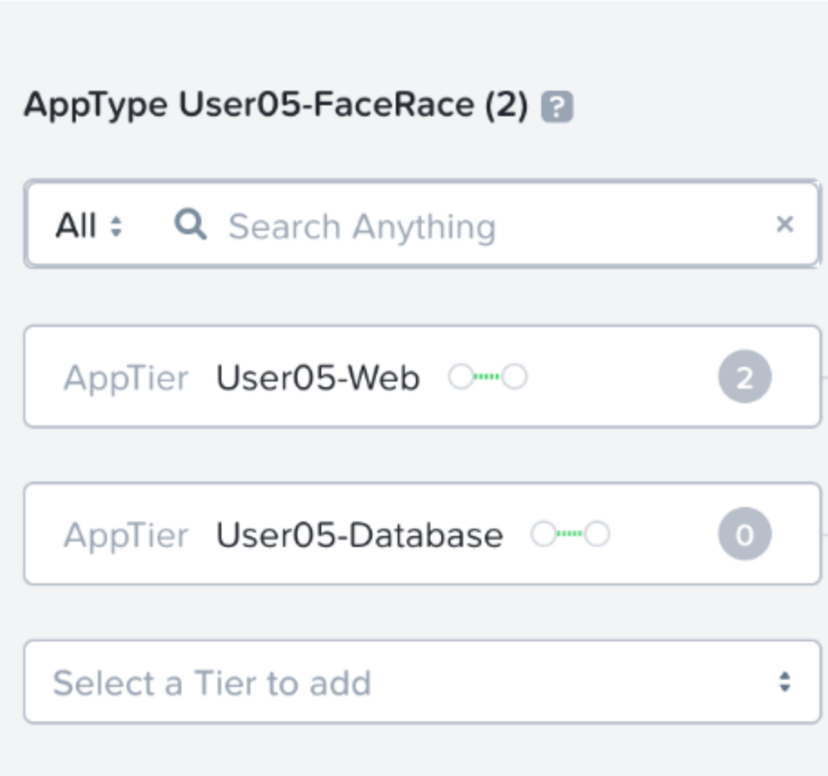


> **Note**
>
> If prompted, click *OK, Got it!* on the tutorial diagram of the *Create App Security Policy* wizard.

4. To allow for a more granular configuration of the security policy, click **Set rules on App Tiers, instead**, rather than applying the same rules to all components of the application.



5. Select **User** `##` **-Web** from the drop-down.
6. Select **User** `##` **-DataBase** from the drop-down.



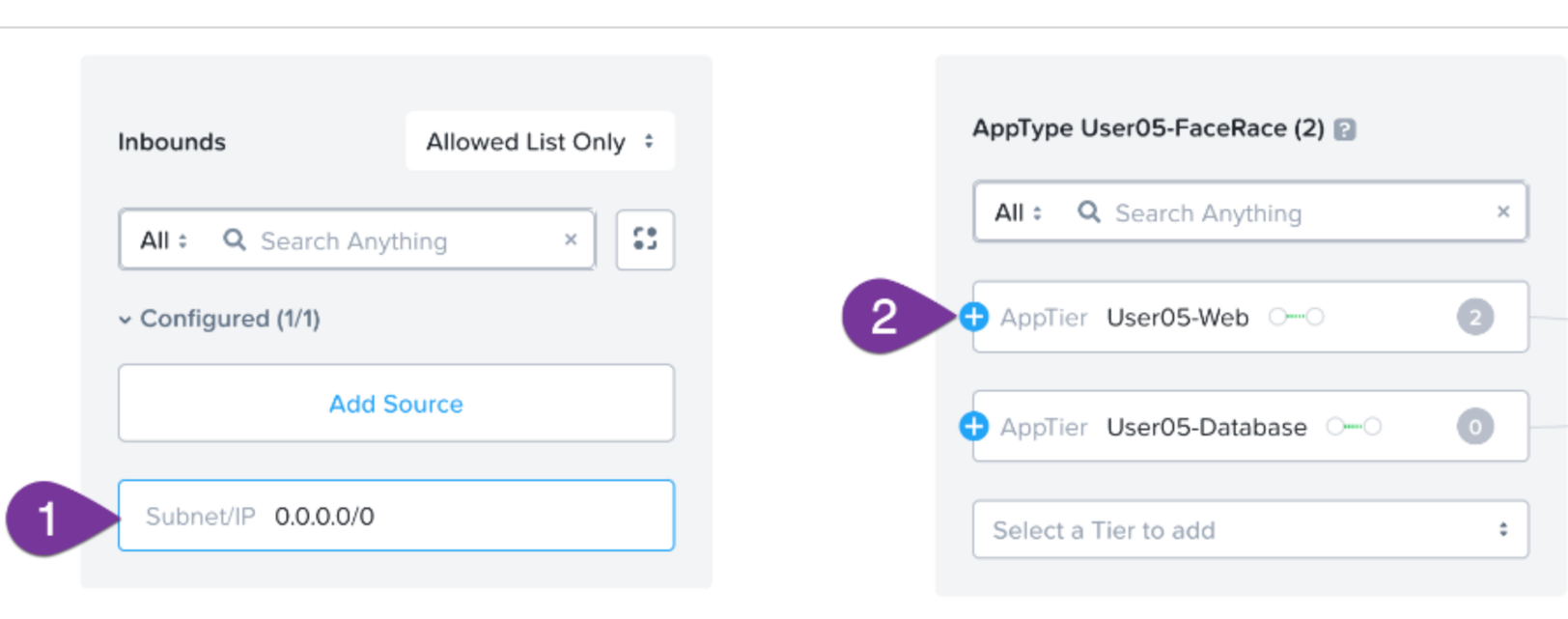
Next, you will define the *Inbounds* rules, which control which sources you will allow to communicate with the FaceRace VMs. You can allow all inbound traffic, or define whitelisted sources. By default, the security policy is set to deny all incoming traffic.

In this scenario, we will allow inbound TCP traffic to the FaceRace web tier on TCP port 80 from all clients.

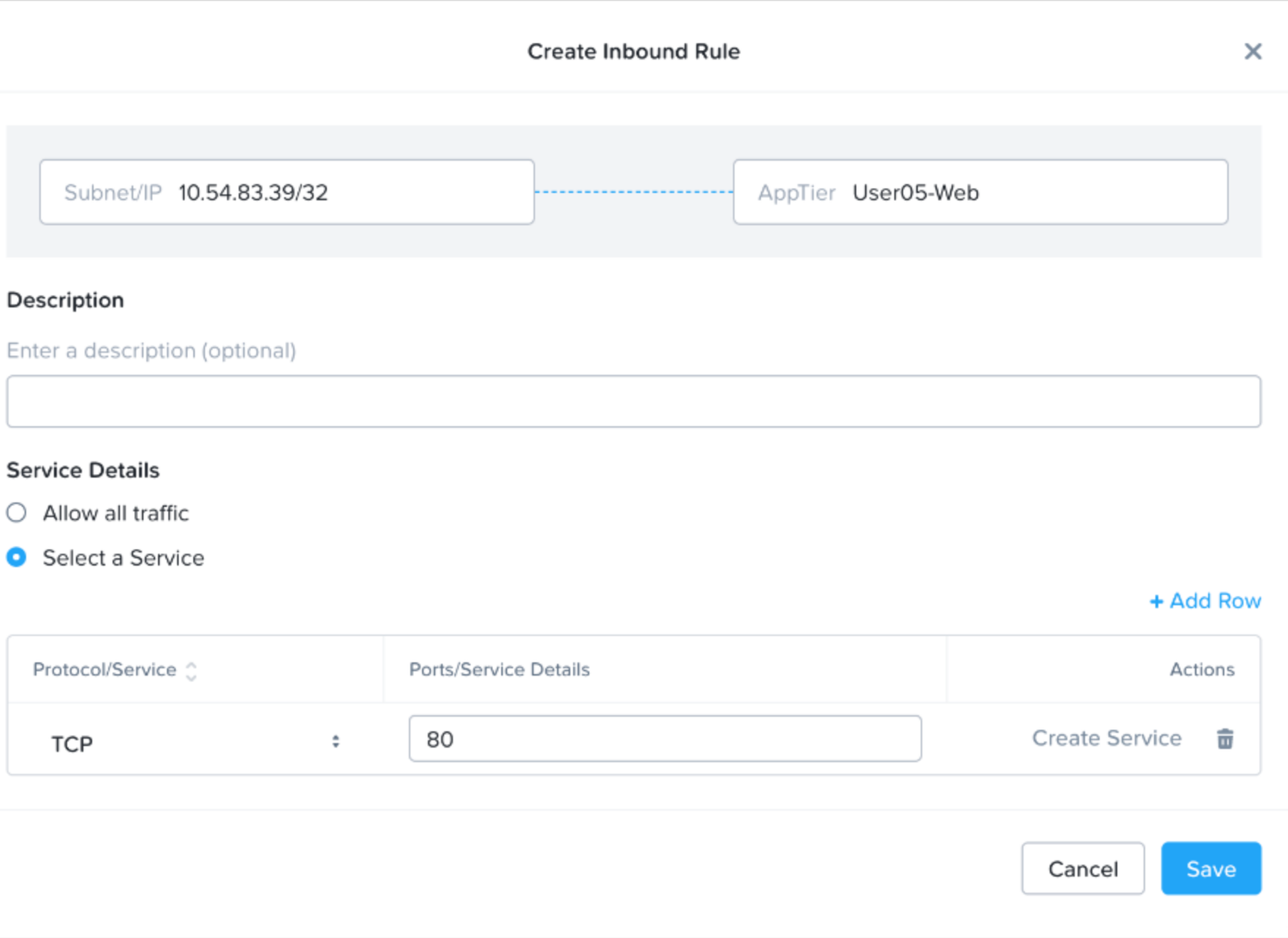
7. Under **Inbounds**, click **Add Source**.
8. Fill out the following fields to allow all inbound IP addresses, and then click **Add**.
   - **Add source by:** - Subnet/IP
   - **Enter a subnet.** - `0.0.0.0/0`

> **Note**
>
> Sources can also be specified by category, allowing for greater flexibility as this data can follow a VM regardless of changes to its network location.

9. To create an inbound rule, click **Subnet/IP 0.0.0.0/0**, and then select ⊕ to the left of **AppTier User** `##` **-Web**.



10. Choose **Select a Service**, fill out the following fields, and then click **Save**:
    - **Protocol/Service** - TCP
    - **Ports/Service Details** - 80

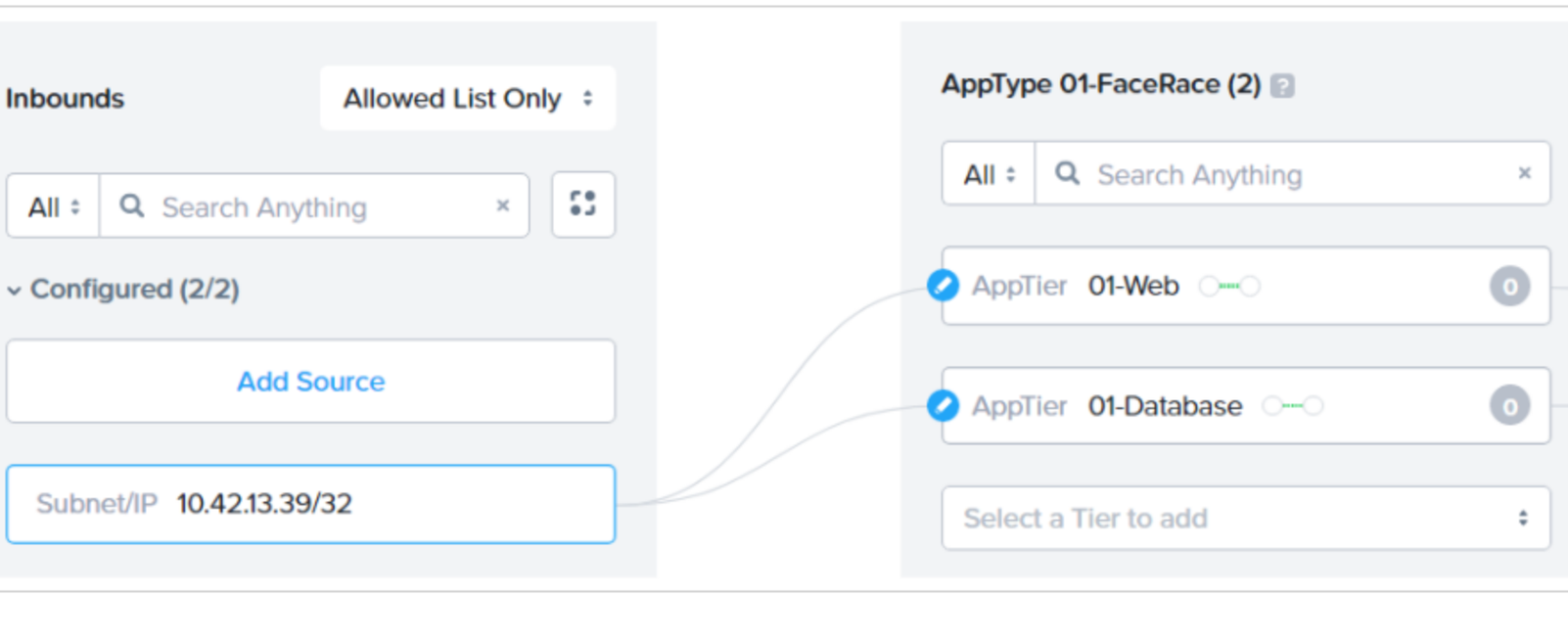


> **Note**
>
> Multiple protocols and ports can be added to a single rule.

11. Under **Inbounds**, click ⊕ **Add Source**.
12. Fill out the following fields, and then click **Add**.
    - **Add source by:** - Subnet/IP
    - **Enter a subnet.** - `<PRISM-CENTRAL-IP-ADDRESS>/32` (ex. [10.42.52.39/32])

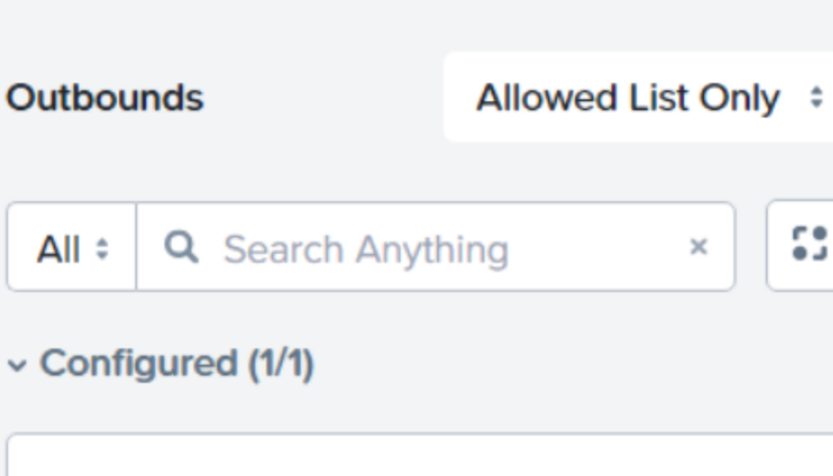
> **Note**
>
> The /32 denotes a single IP address, as opposed to a subnet range.

13. To create an inbound rule, click **Subnet/IP** `<PRISM-CENTRAL-IP-ADDRESS>/32`, and then select ⊕ to the left of **AppTier User** `##` **-Web**.
14. Choose **Select a Service**, fill out the following fields, and then click **Save**:
    - **Protocol/Service** - TCP
    - **Ports/Service Details** - 22
15. Repeat previous step for **AppTier User** `##` **-Database** to allow communication with the database VM.

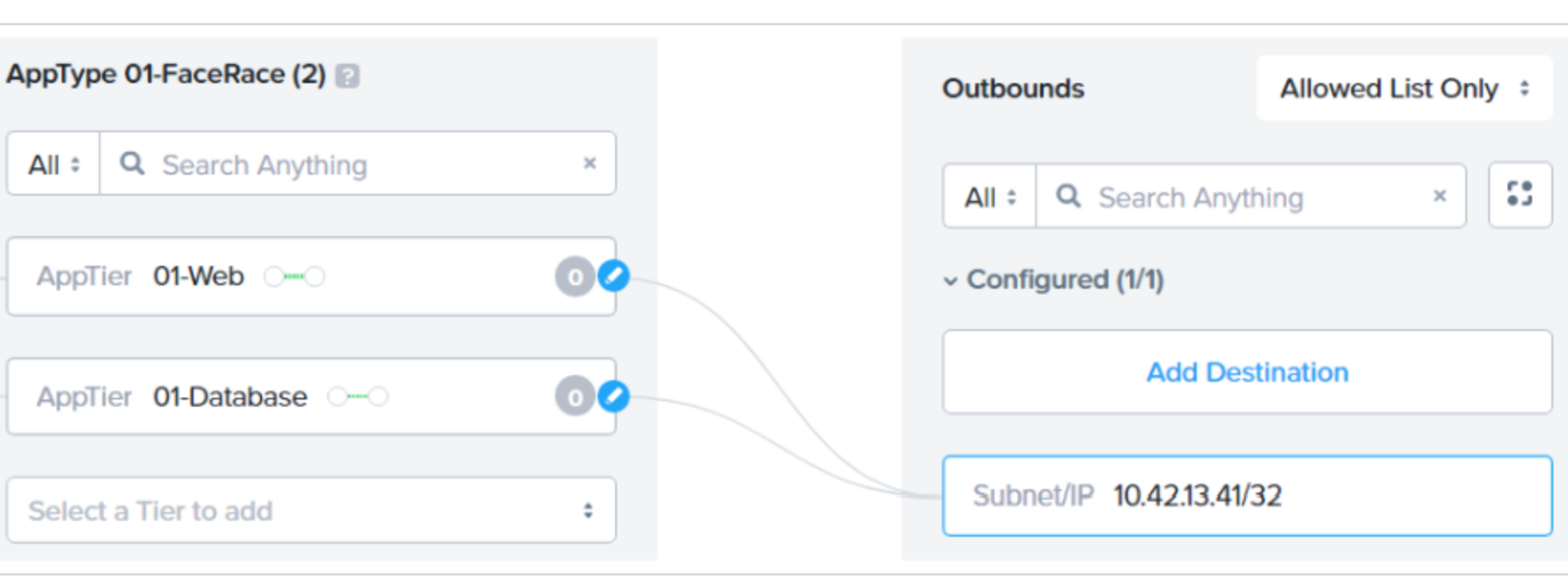


By default, the security policy allows the application to send all outbound traffic to any destination. The only outbound communication required for your application is to communicate with your DNS server.

16. Under **Outbounds**, select **Allowed List Only** from the drop-down menu, and then click **Add Destination**.
17. Fill out the following fields, and then click **Add**:
    - **Add destination by:** - Subnet/IP (default)
    - **Enter a subnet.** - `<AUTOAD-IP-ADDRESS>/32` (ex. `10.42.52.41/32`)

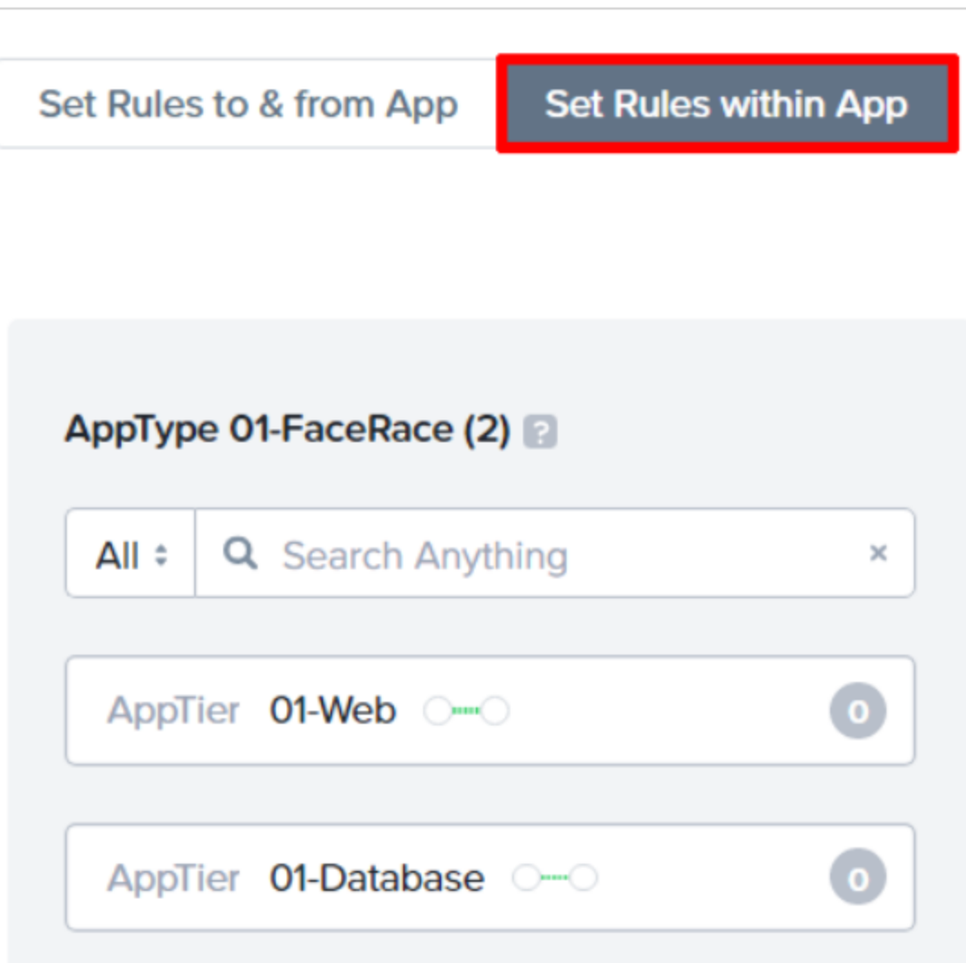


18. To create an outbounds rule, click **Subnet/IP** `<PRISM-CENTRAL-IP-ADDRESS>/32`, and then select ⊕ to the right of **AppTier User** `##` **-Web**.
19. Choose **Select a Service**, fill out the following fields, and then click **Save**:
    - **Protocol/Service** - UDP
    - **Ports/Service Details** - 53
20. Repeat this for **AppTier User** `##` **-Database**.



Each tier of the application communicates with other tiers, and as such, the policy must allow this traffic. Some tiers, such as the web tier, do not require communication within the same tier.

21. To define intra-app communication, click **Set Rules within App**.



22. Click **AppTier User** `##` **-Web** > **Edit**, and under *Can VMs in this tier talk to each other?* select **No** to prevent communication between VMs in this tier.

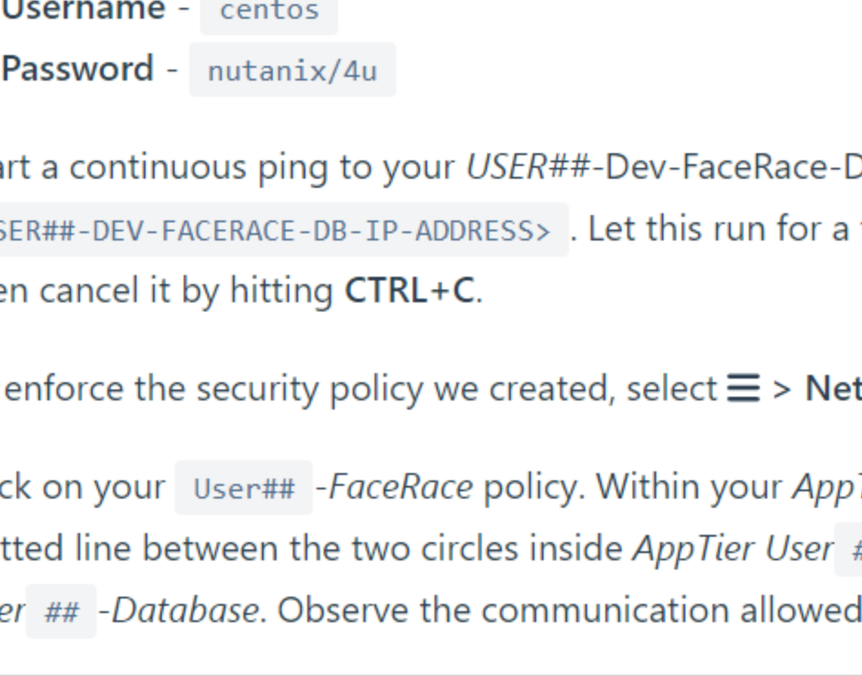
    There are only two VMs (Prod and Dev) within the tier currently, but scale-out operations will apply this policy to all VMs in this category preventing their ability to communicate with one another - regardless of how many VMs are deployed.

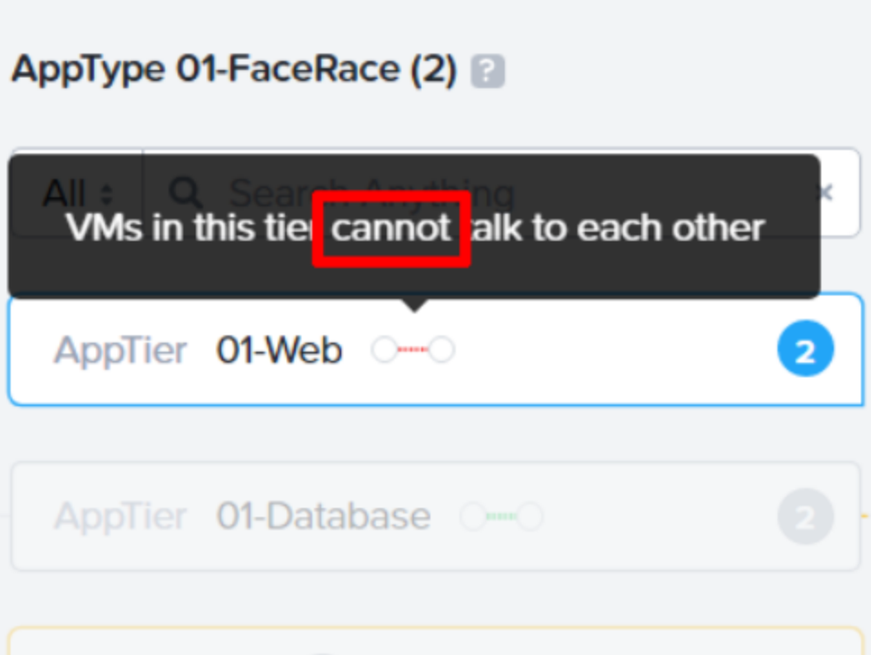
23. While **AppTier: User** `##` **-Web** is still selected, click ⊕ to the right of **AppTier User** `##` **-Database** to create a tier-to-tier rule.
24. Choose **Select a Service**, fill out the following fields, and then click **Save**:
    - **Protocol/Service** - TCP
    - **Ports/Service Details** - 3306
25. Click **Next** to review the security policy.
26. Click **Save and Monitor** to save the policy.

Testing Security Policy

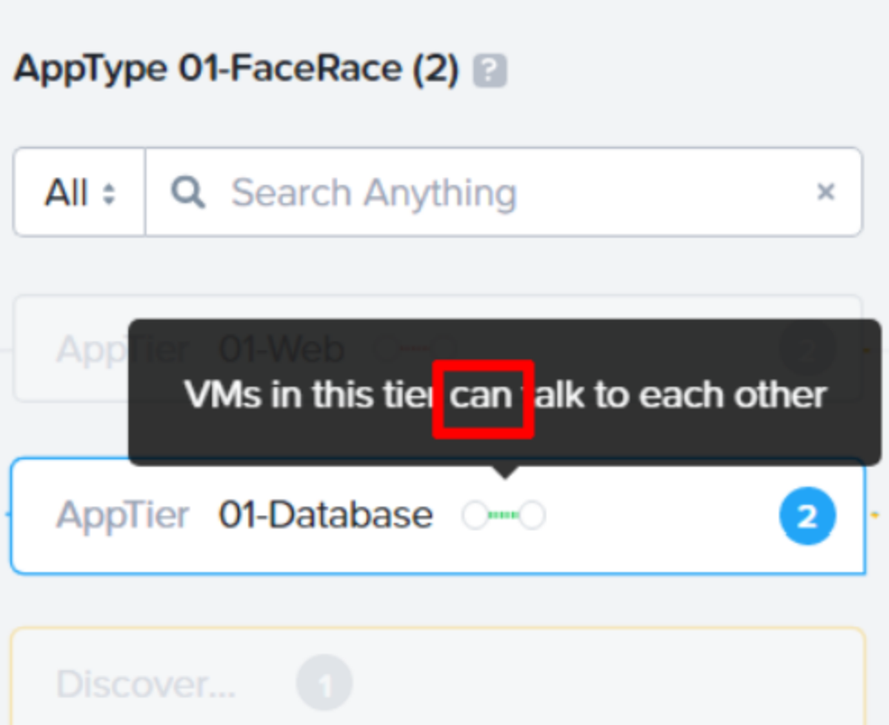
Now that we have created our first security policy, we need to test it. Note that we configured our policy in *Monitor* mode, which means that we are not yet enforcing any inbound and outbound traffic rules.

1. Select ☰ > **Compute & Storage** > **VM**.
2. Note the IP address for *USER##*-Dev-FaceRace-Web, and *USER##*-Dev-FaceRace-DB.
3. Right-click on *USER##*-Prod-FaceRace-Web, and then select **Launch Console**.
4. Login using the following credentials:
   - **Username** - `centos`
   - **Password** - `nutanix/4u`
5. Start a continuous ping to your *USER##*-Dev-FaceRace-Web VM IP by entering the command `ping <USER##-DEV-FACERACE-WEB-IP-ADDRESS>`. Let this run for a few moments to confirm communication, and then cancel it by hitting **CTRL+C**.
6. Note the IP address for *USER##*-Dev-FaceRace-DB.
7. Right-click on *USER##*-Prod-FaceRace-DB, and then select **Launch Console**.
8. Login using the following credentials:
   - **Username** - `centos`
   - **Password** - `nutanix/4u`
9. Start a continuous ping to your *USER##*-Dev-FaceRace-DB VM IP by entering the command `ping <USER##-DEV-FACERACE-DB-IP-ADDRESS>`. Let this run for a few moments to confirm communication, and then cancel it by hitting **CTRL+C**.
10. To enforce the security policy we created, select ☰ > **Network & Security** > **Security Policies**.
11. Click on your `User##` *-FaceRace* policy. Within your *AppType User* `##` *-FaceRace*, hover over the dotted line between the two circles inside *AppTier User* `##` *-Web*, and then again for *AppTier User* `##` *-Database*. Observe the communication allowed within these application tiers.

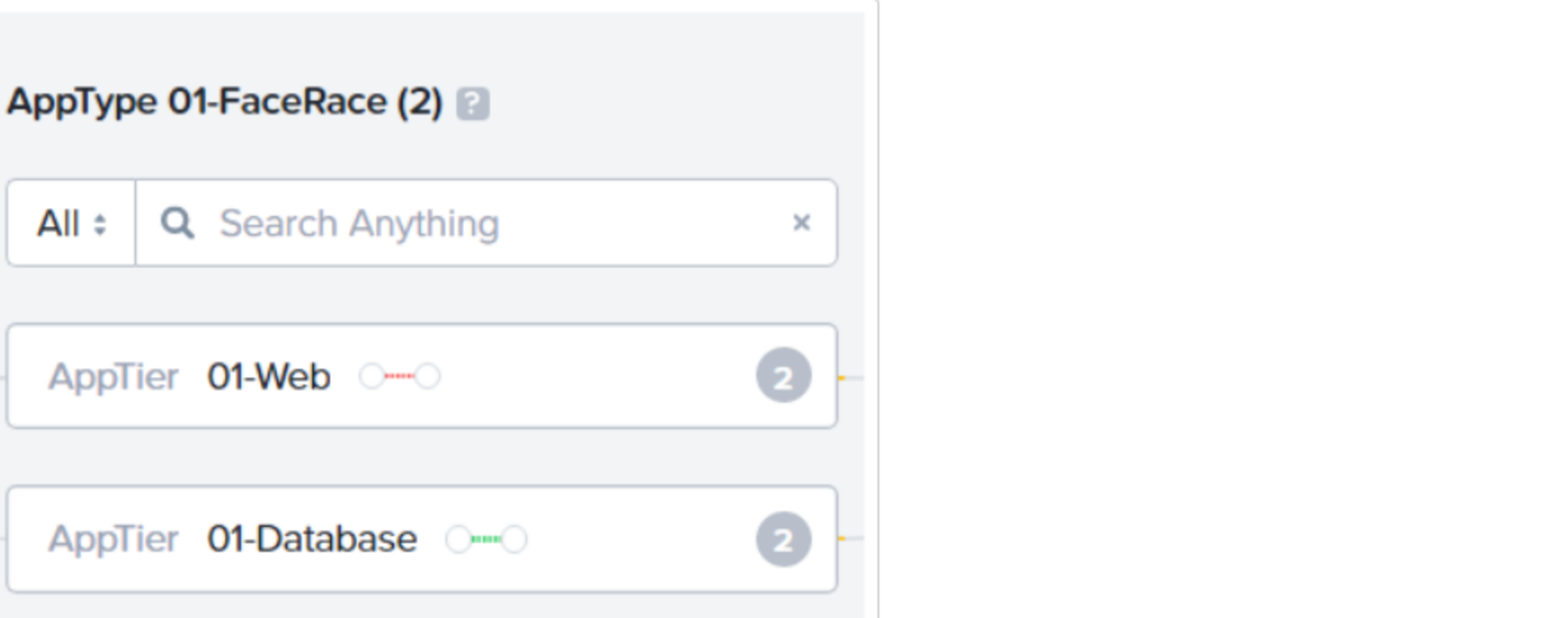




12. Click on the *Discovered* box. Note that Flow is observing the traffic between the VMs in the policy.

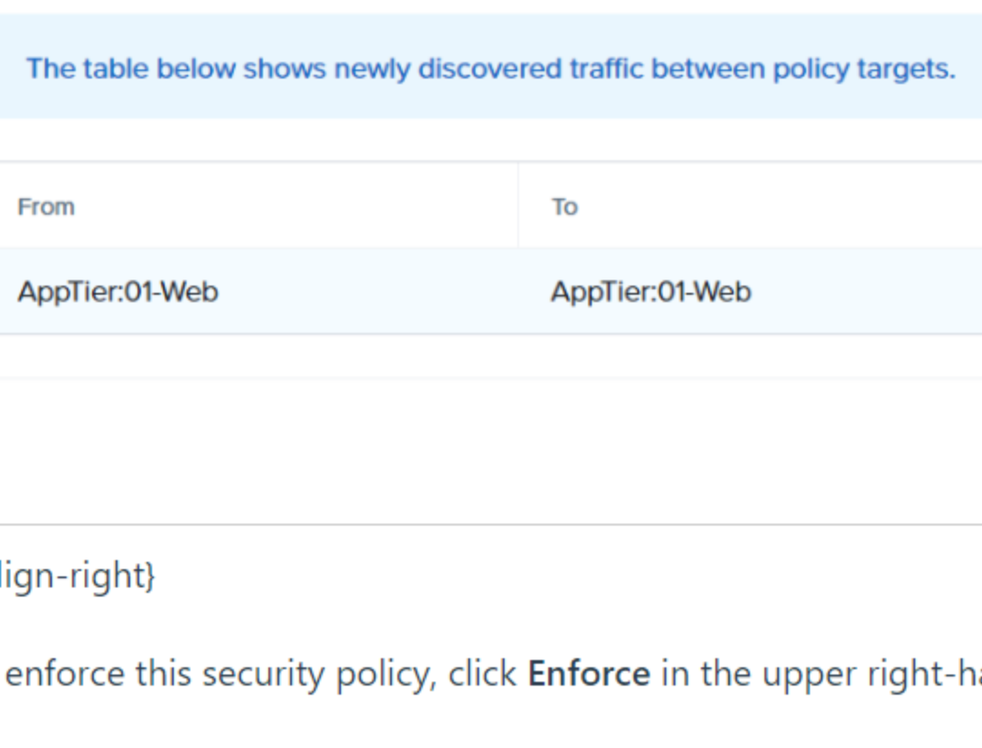


{.align-left}

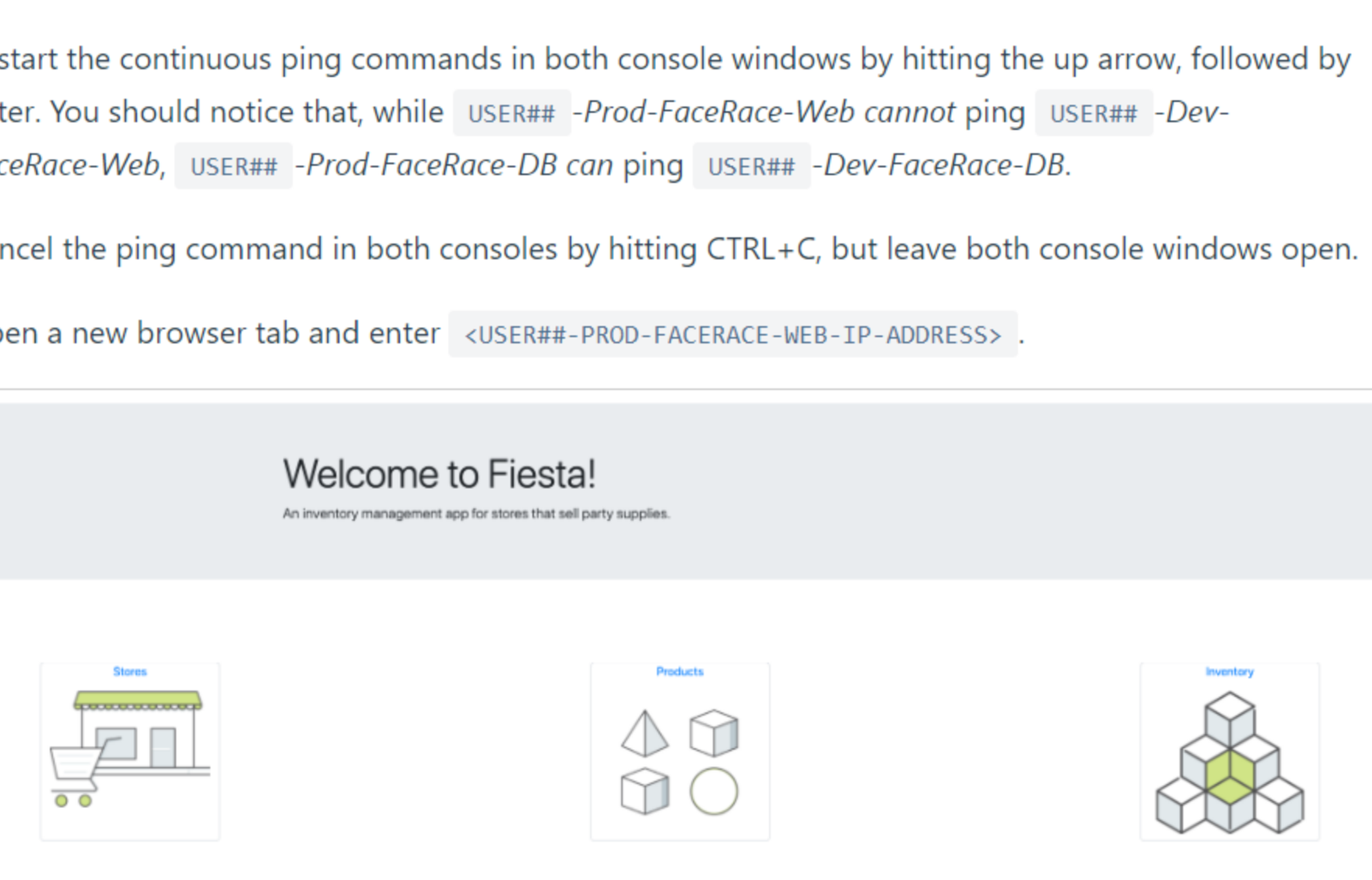


{.align-right}

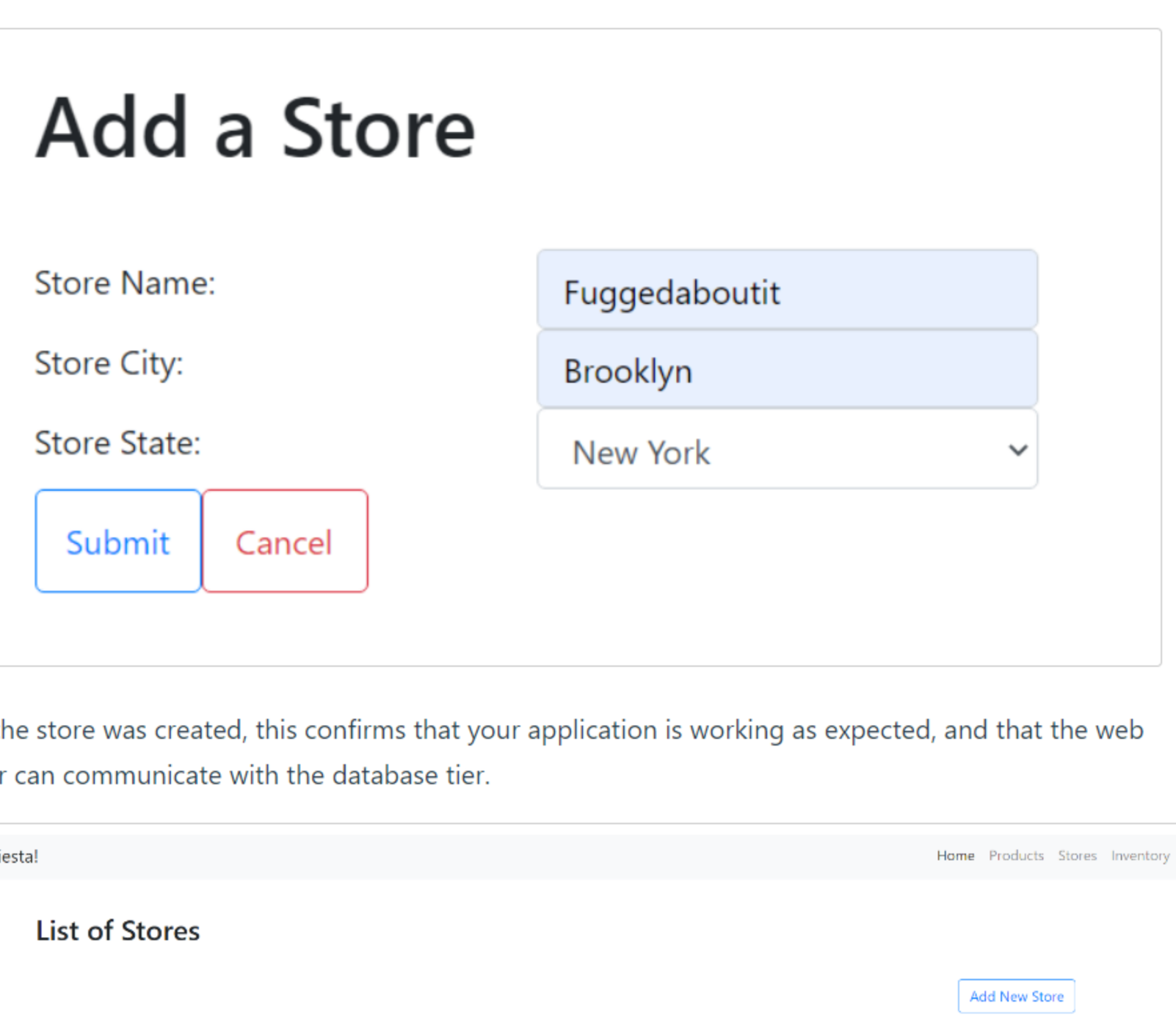
13. To enforce this security policy, click **Enforce** in the upper right-hand corner.
14. Type **ENFORCE**, and then click **Confirm**.



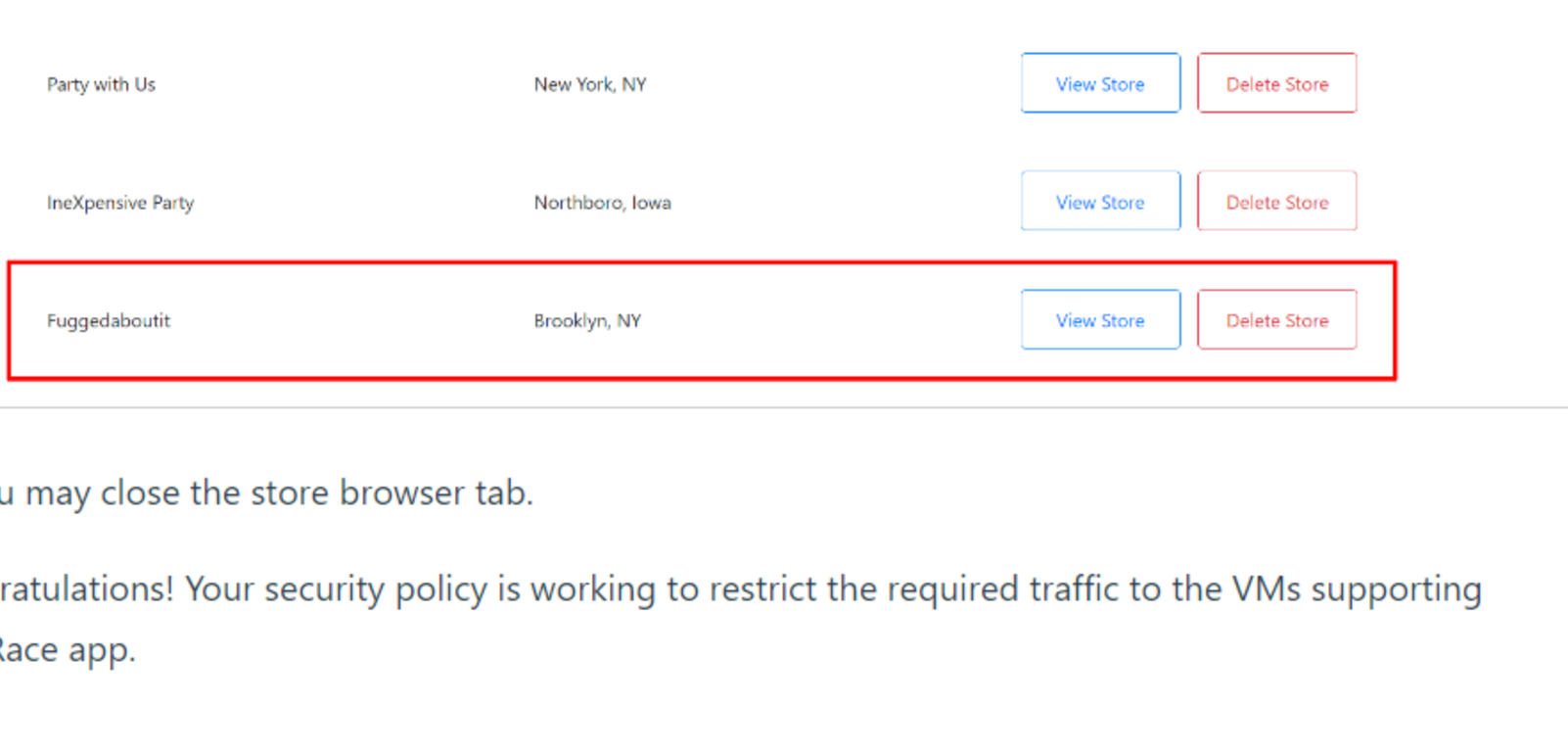
15. Return to the consoles of *USER##*-Prod-FaceRace-Web and *USER##*-Prod-FaceRace-DB.
16. Restart the continuous ping commands in both console windows by hitting the up arrow, followed by enter. You should notice that, while `USER##` *-Prod-FaceRace-Web cannot* ping `USER##` *-Dev-FaceRace-Web*, `USER##` *-Prod-FaceRace-DB can* ping `USER##` *-Dev-FaceRace-DB*.
17. Cancel the ping command in both consoles by hitting CTRL+C, but leave both console windows open.
18. Open a new browser tab and enter `<USER##-PROD-FACERACE-WEB-IP-ADDRESS>`.



19. Select **Stores** > **Add New Store**.
20. Fill out the information, and then click **Submit**.



21. If the store was created, this confirms that your application is working as expected, and that the web tier can communicate with the database tier.



22. You may close the store browser tab.

Congratulations! Your security policy is working to restrict the required traffic to the VMs supporting FaceRace app.

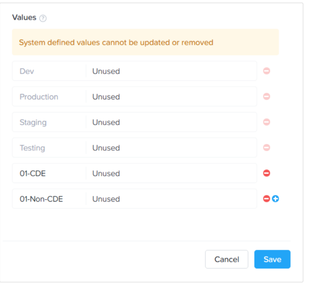
Last Updated: 5/26/2023, 1:44:20 PM

Isolate Environments

Our FaceRace gaming machines are now properly secured from network activity outside the cluster. We want to ensure that we prevent access from other VMs from within the cluster. To achieve this, we can provide isolation policies to all the VMs in our environment.

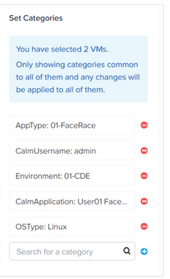
The environments we will create enable isolation between the cardholder data environment (CDE) and the non-CDE (i.e. everything else). Similar to the previous section, we will add two more environmental categories: *CDE* and *Non-CDE*.

1. Within *Prism Central*, select ☰ > **Administration** > **Categories**.
2. Select **Environment** > **Actions** > **Update**.
3. Click `Add More Values` to display the value text box, create **User ## -CDE** and **User ## -Non-CDE** entries, and then click **Save**.

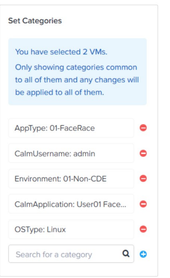


Next we will assign the *CDE* category value to the **User ## -Prod-FaceRace** VMs, and the *Non-CDE* category value to "everything else".

4. Select ☰ > **Compute & Storage** > **VMs**.
5. Select both the *USER##*-Prod-FaceRace-Web and *USER##*-Prod-FaceRace-DB VMs, and then click **Actions** > **Manage Categories**.
6. Specify **Environment:User##-CDE** (ex. `Environment:User01-CDE`) as the value name, and then click **Save**.

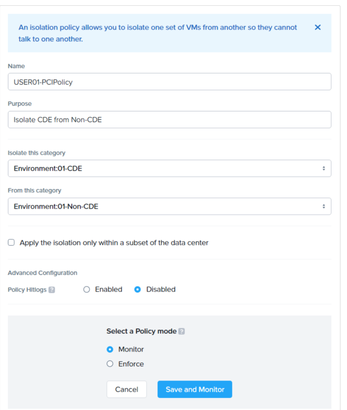


7. Deselect both the `USER##` -*Prod-FaceRace-Web* VMs, select both the *User##-Dev-FaceRace-Web* and *User ## -Dev-FaceRace-DB* VMs, and click **Actions** > **Manage Categories**.
8. Specify **Environment:User##-Non-CDE** (ex. `Environment:User01-Non-CDE`) as the value name, and then click **Save**.



Now that category values have been created and appropriately assigned to the VMs, we can create an isolation policy.

9. Select ☰ > **Network & Security** > **Security Policies**.
10. Click **Create Security Policy** > **Isolate Environments (Isolation Policy)** > **Create**.
11. In the fields enter the following information:
    - **Name** - `User##` -PCIPolicy
    - **Purpose** - Isolate CDE from Non-CDE
    - **Isolate this category** - Environment:User `##` -CDE
    - **From this category** - Environment:User `##` -Non-CDE
12. Click **Save and Monitor**.

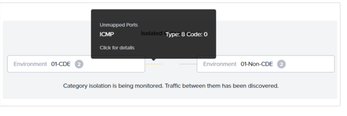


This type of policy is a simple and effective way to achieve the desired isolation between sensitive environments that might contain personal customer data, or for the creation of network security best practices (i.e. creating a DMZ, or honeypots).

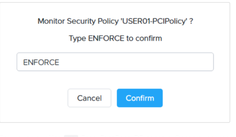
Testing the Isolation Policy

As we did during our security policy testing, we will enforce the new isolation policy, and confirm it is working as expected.

1. Return to the consoles of *USER##*-Prod-FaceRace-DB, and restart the continuous ping command by hitting the up arrow, followed by enter.
2. Click on your `USER##` -**PCIPolicy**.
3. Hover your mouse over the dotted line to the right of *Environment User##-CDE*. You'll notice that Flow is observing the traffic between the VMs in the policy.



4. To activate the isolation policy, click **Enforce** in the upper right-hand corner of your screen.
5. Type **ENFORCE**, and then click **Confirm**.



6. Return to your **User ## -Prod-FaceRace-DB** console. Observe that the pings now fail, as we are blocking the Production (CDE) environment from Development (Non-CDE).
7. You may cancel the ping command, log out of both console sessions, and then close the console windows.

Congratulations for going above and beyond and isolate your production application environment.

Last Updated: 5/26/2023, 1:44:20 PM

← Securing Applications

Monitoring Data Services

After just two days, you've managed to secure the Nutanix platform basic features by changing all the default passwords, and securing mission-critical applications. It can't be this simple. Can it?

But if it is, you're ready to start leveraging more tools to help in the monitoring and alerting of potentially malicious activity.

Jerry, who oversees storage and data services, has told you that he has deployed Nutanix Files, which includes an analytics dashboard. He thinks you'd like to explore it, as it will store users saved games files and departmental shares of the company. He also mentioned it has an *anti-ransomware* component to it. He had your curiosity, but now he has your attention.

We'll now move on to protecting the company's data, and making sure you have the means to recover and take action upon suspicious activities.

On the surface, File Analytics seems to be a very powerful, very useful tool in the effort to detect and prevent ransomware execution at its most likely ingress: the endpoint. Detecting that activity in the file systems could be critical to the continued smooth operation of Blips and Chitz, Inc.

Last Updated: 5/2/2023, 11:07:35 AM

File Analytics →

File Analytics

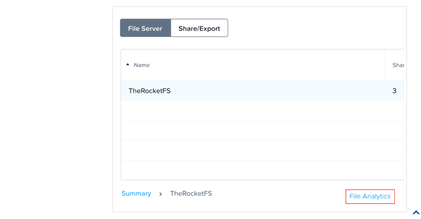
Defining Anomalies

1. Within *Prism Central*, select ☰ > **Services** > **Files**.

2. Click on **File Servers** from the left-hand menu, and then click on **Manage** within the **Actions** column for **TheRocketFS**.

A new browser tab will open.

3. Click on **TheRocketFS**, and then select **File Analytics**.

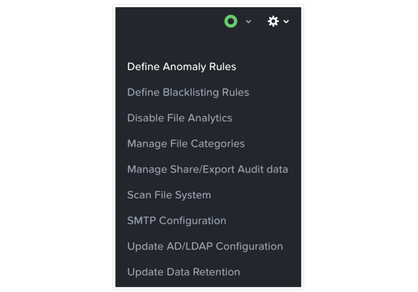


Your File Analytics dashboard will show metrics for *Top 5 active users*, *Top 5 accessed files*, *File Operations*, and more.

Everything looks normal right now. These widgets are essential to detect unusual or anomalous behavior, such as repeated failed authentications, an increase in network traffic, or a large volume of file updates and touch-points.

Let's create an *Anomaly Rule* to detect suspicious activity based on action.

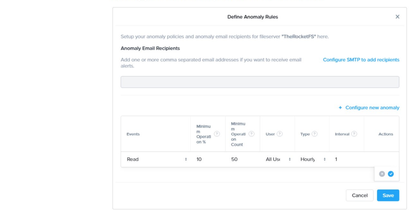
4. Click on the ⚙ > **Define Anomaly Rules** > **+ Define Anomaly Rules**.



5. Fill out the following information, click ✔, and then click **Save**.

- **Events** - Read
- **Minimum Operation %** - 10
- **Minimum Operation Count** - 50
- **User** - All Users
- **Type** - Hourly
- **Interval** - 1

Optionally, you can send an *Anomaly Alert* to one or more email addresses



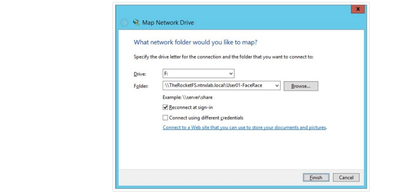
> **Note**
> This is a one time configuration. If you see this step already performed, proceed to the next step.

In this next step, we are mimicking what an attack or deliberately malicious behavior could look like. For example, a malicious script repeatedly accessing data, or someone trying to steal private information from the company.

6. Within *Prism Central*, identify the IP address for your *USER##*-WinTools VM, and utilizing Windows Remote Desktop, log in using the following credentials:

- **User Name** - adminuser `##` @ntnxlab.local (ex. adminuser01@ntnxlab.local)
- **Password** - `nutanix/4u`

7. Open *Windows Explorer*, right click on **This PC** > **Map Network Drive** > **\\TheRocketFS.ntnxlab.local\User##-FaceRace**. From the *Drive:* drop-down, select **F:**.



8. Within your `USER##` -*WinTools* VM, copy and paste the following link into Chrome to download the sample data (https://peerresources.blob.core.windows.net/sample-data/SampleData_Small.zip). Once downloaded, click on it to open, and copy/paste the *Sample Data* folder to **F:**.

9. Open **PowerShell**, and run the command:

```
cd F:\\Sample Data\\Technical PDFs
```

10. Run the command:

```
Get-ChildItem *.pdf | foreach {start-process $_.fullname}
```

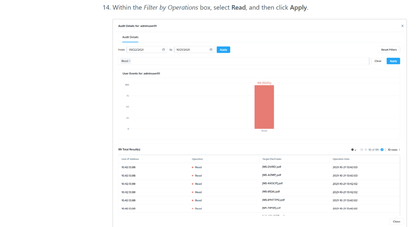
This will open 99 PDF files within your browser.

11. Return to *File Analytics*, and then select ☰ > **Audit Trails**.

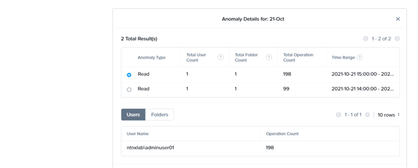
12. Select *Users* and search for **adminuser##**.

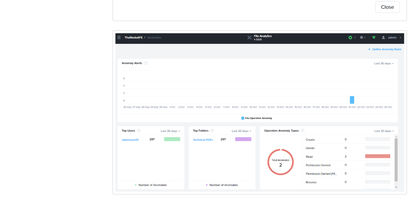
13. Under the *Action* column, click **View Audit**.

14. Within the *Filter by Operations* box, select **Read**, and then click **Apply**.



15. Since you have already defined this behavior as an anomaly, close this window, and then navigate to ☰ > **Anomalies**. Click on the *Anomaly Alerts* timeline.





This may take up to one hour, so you may wish to move on, and circle back to check on this at a later time. This is expected behavior when your environment is being attacked, and *File Analytics* helps identify anomaly trends in your environment.

File Analytics Ransomware Protection

File Analytics scans files for ransomware in real-time, and notifies you via email in the event of a ransomware attack. By using the Nutanix Files file blocking mechanism, File Analytics prevents files with signatures of potential ransomware from carrying out malicious operations. Ransomware Protection automatically scans for ransomware based on a curated list of signatures that frequently appear in ransomware files. Optionally, you can add additional signatures to the list.

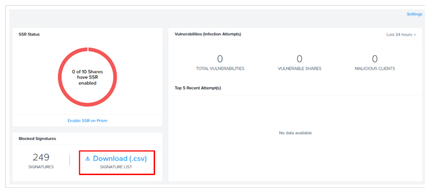
File Analytics also monitors file shares for self-service restore (SSR) policies, and identifies shares that do not have SSR enabled in the ransomware dashboard. You can enable SSR through the ransomware dashboard by selecting shares identified by File Analytics.

Enabling Ransomware Protection

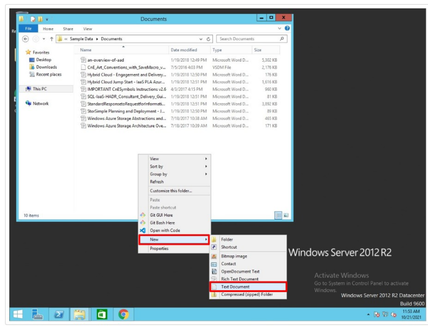
1. Within the *Files Analytics* dashboard, click ☰ > **Ransomware**.
2. Click **Enable Ransomware Protection**, and then click **Enable**.

> **Note**
>
> This is a one-time setting. If you see that *Ransomware Protection* is enabled, you can review the options but no action is required.

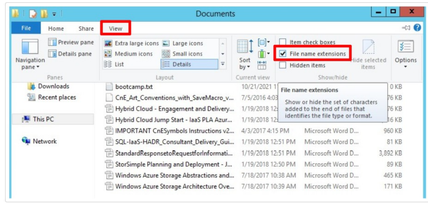
3. Click **Download (.csv)**, and then open the *.csv* file. It lists which file extensions File Analytics will block by default.



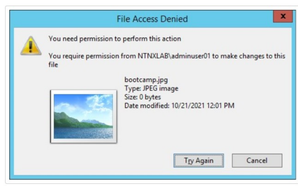
4. Within your *USER##*-WinTools VM, navigate to the *F:\Sample Data\Documents* folder.
5. Create a new *.txt* file by right-clicking in an empty space, choosing **New** ▸ **Text Document**, and then hitting **Enter**. The file will be created with the name *New Text Document.txt*.



6. Rename the file to *bootcamp.txt*.
7. Click the **View** menu, and then check the box for **File name extensions**.

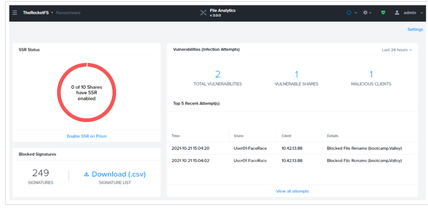


8. Change the file extension to **.jpg**, and then click **Yes**.
9. Change the file extension to **.Valley**, and then click **Yes**.



This operation fails, as **.Valley** is one of the extensions that are blocked by Ransomware Protection, listed in the *.csv* file.

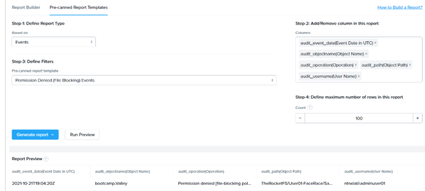
10. Click **Cancel** on the *File Access Denied* dialogue box.
11. Return to the *File Analytics* dashboard. Within the *Vulnerabilities* section, observe that this now displays the malicious attempt of creating a **.Valley** file.



Custom Reports

Let's explore how to build a report in File Analytics.

1. Click on the ☰ > **Reports** > **+ Create a new report**.
2. Select **Pre-canned Report Templates**.
3. Select **Events** from the *Based on* drop-down.
4. Under *Define Filters*, select **Permission Denied (File Blocking) Events** from the *Pre-canned report template* drop-down.
5. Click on **Run Preview**.



> **Note**
>
> Feel free to customize and explore the reports in other ways, in this example we are targeting the actions that resulted in preventing a user (or script) from altering the file in a malicious way.

Last Updated: 5/2/2023, 11:07:35 AM

Nutanix Objects

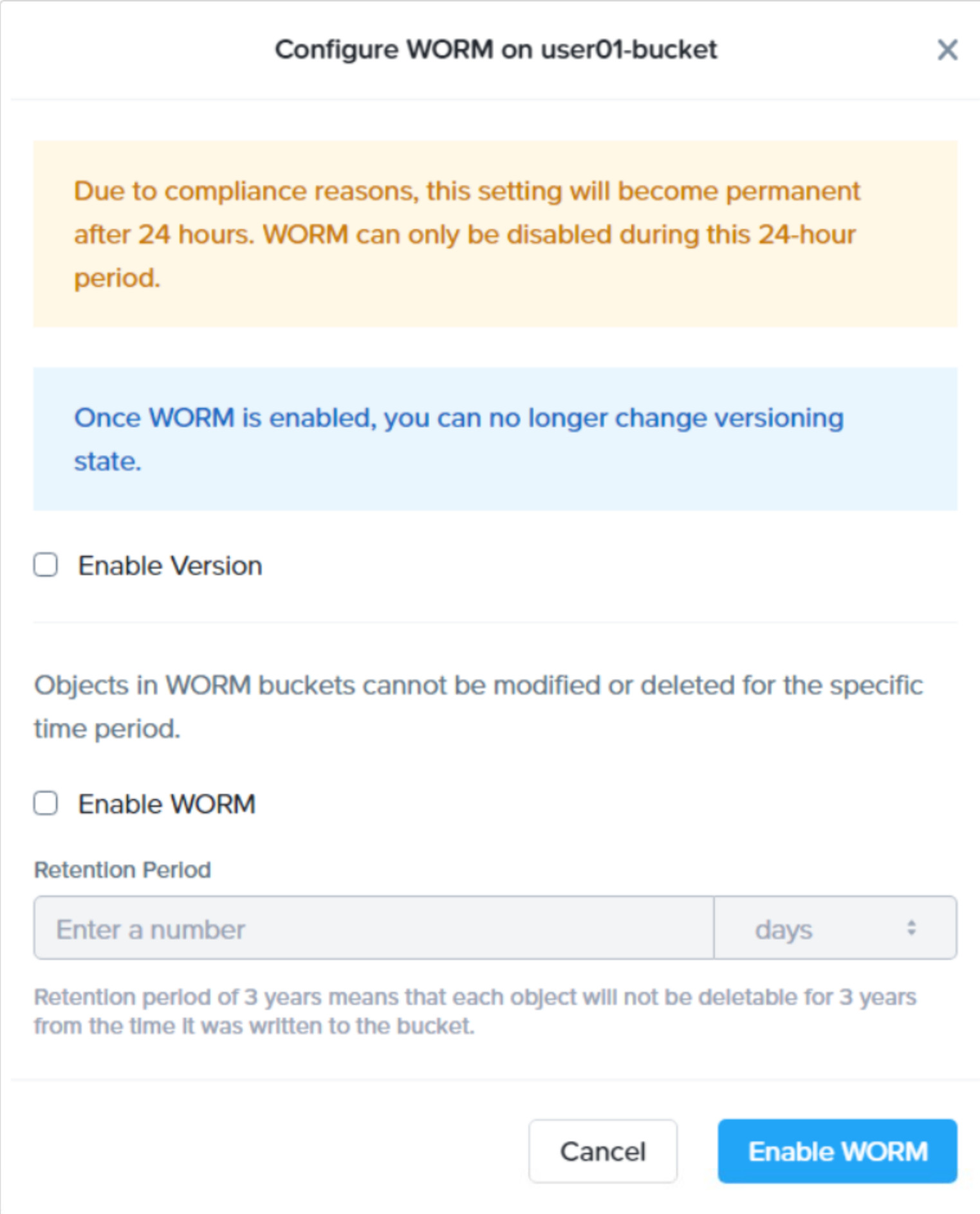
Configuring WORM

The storage administrators for Blips and Chitz, Inc. have created an object storage for *Mortynight Run*, the video surveillance system. It needs to retain archive data for regulatory purposes, and improved security. Your task will be to guarantee that the policies set for the repository adhere to the company's security guidelines.

Create Bucket

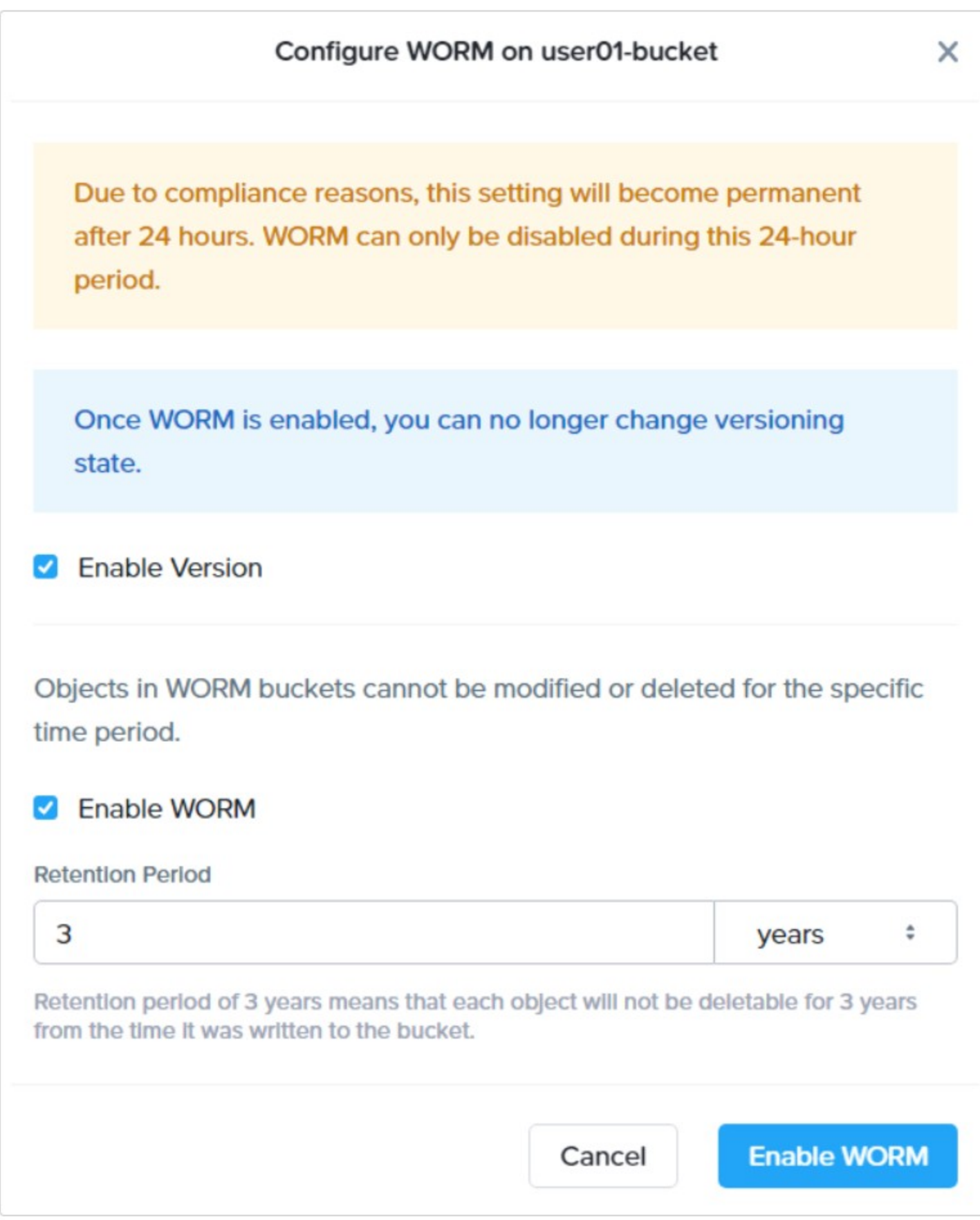
A bucket is a repository within an object store that can have policies applied to it, such as versioning, and WORM (Write Once, Read Many). By default, a newly created bucket is a private resource to the creator. By default, the creator of the bucket has read/write permissions, and can grant permissions to other users.

1. Within Prism Central, select ☰ > **Services** > **Objects**.
2. Click on the existing Object Store name **mortynightrun** to manage it.
3. Select checkbox to the left of **user** `##` **-bucket**, and then click **Actions** > **Configure WORM** to view its settings.

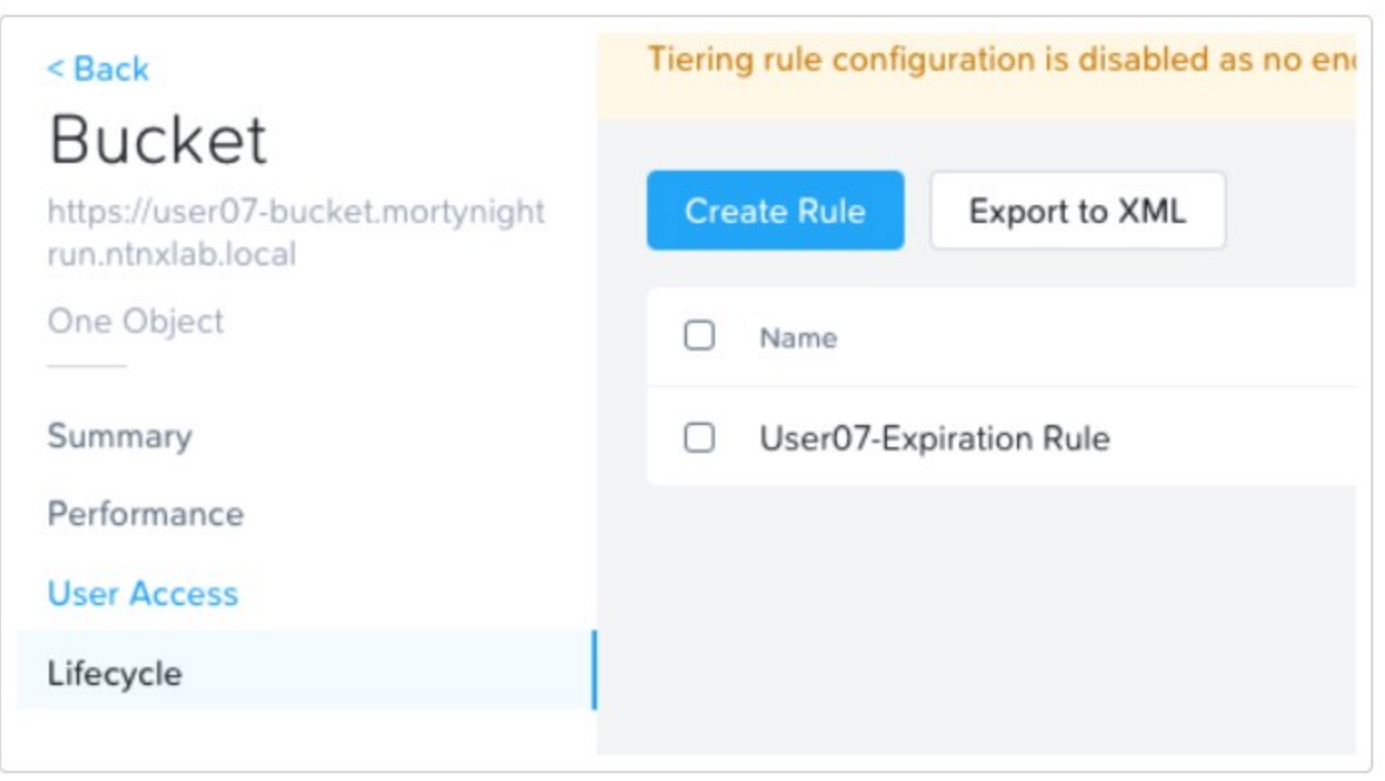


You realize your colleagues didn't enable *WORM* and *Expiration* settings, so you will now proceed with those modifications in order to protect the company's data from attackers and for audit purposes.

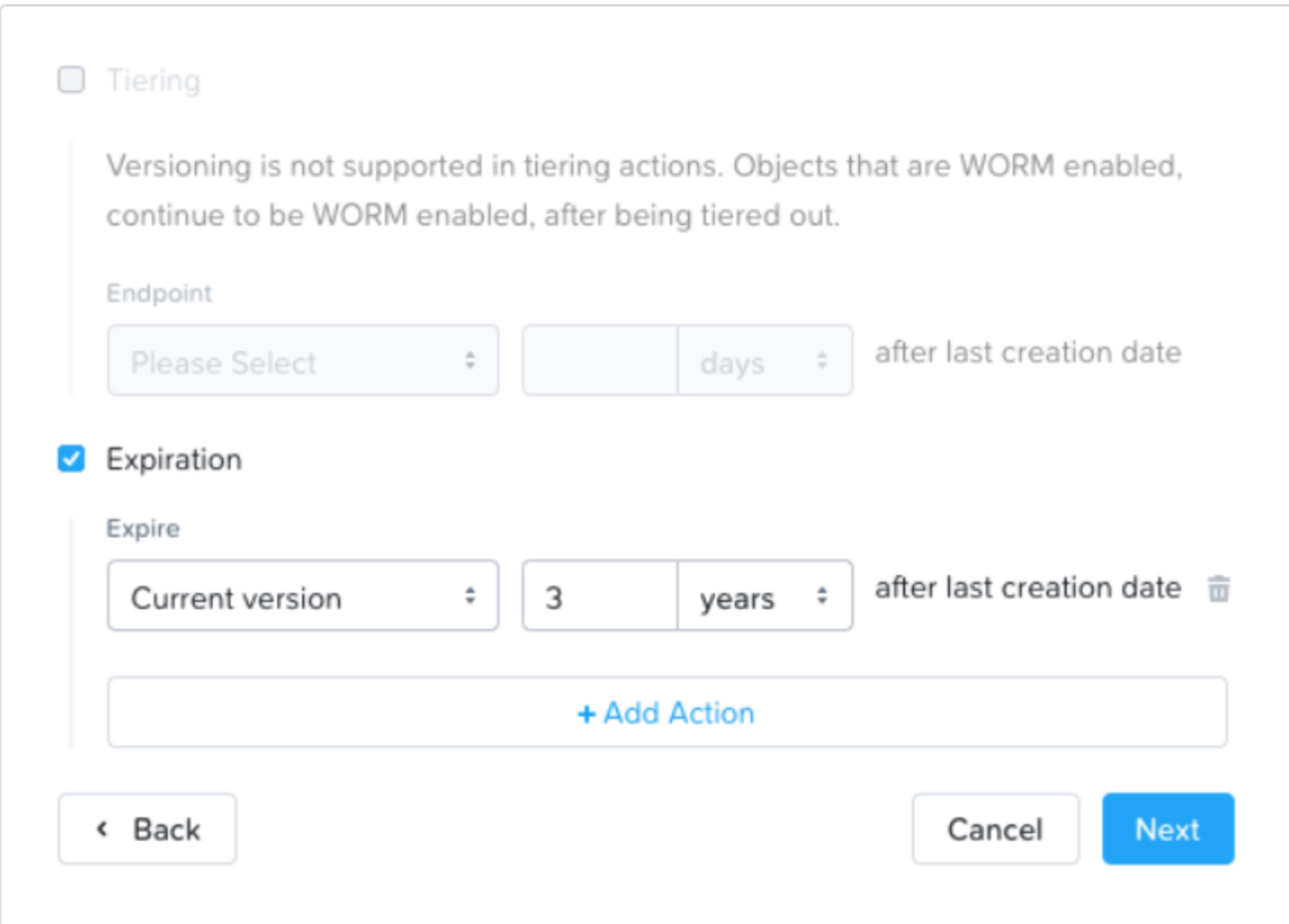
4. Click **Enable Version**.
5. Click **Enable WORM**, and set the *Retention Period* to **3 years**.
6. Click **Enable WORM** to save the changes.



7. Click on **user** `##` **-bucket**, and then select **Lifecycle** from the left-hand menu.



8. Click **Create Rule**, and fill out the following information:
   - **Name** - `User##` -Expiration Rule
   - **Scope** - All Objects
9. Click **Next**.
10. Click **Expiration**, and within the *Expire* section, set **Current Version 3 years** after last creation date.



> **Note**
>
> After you save the WORM configuration, you will have a 24-hour grace period window where you can disable its settings. After that time, you can no longer change it, and the system will permanently follow this behavior. Not even Nutanix support can modify it.

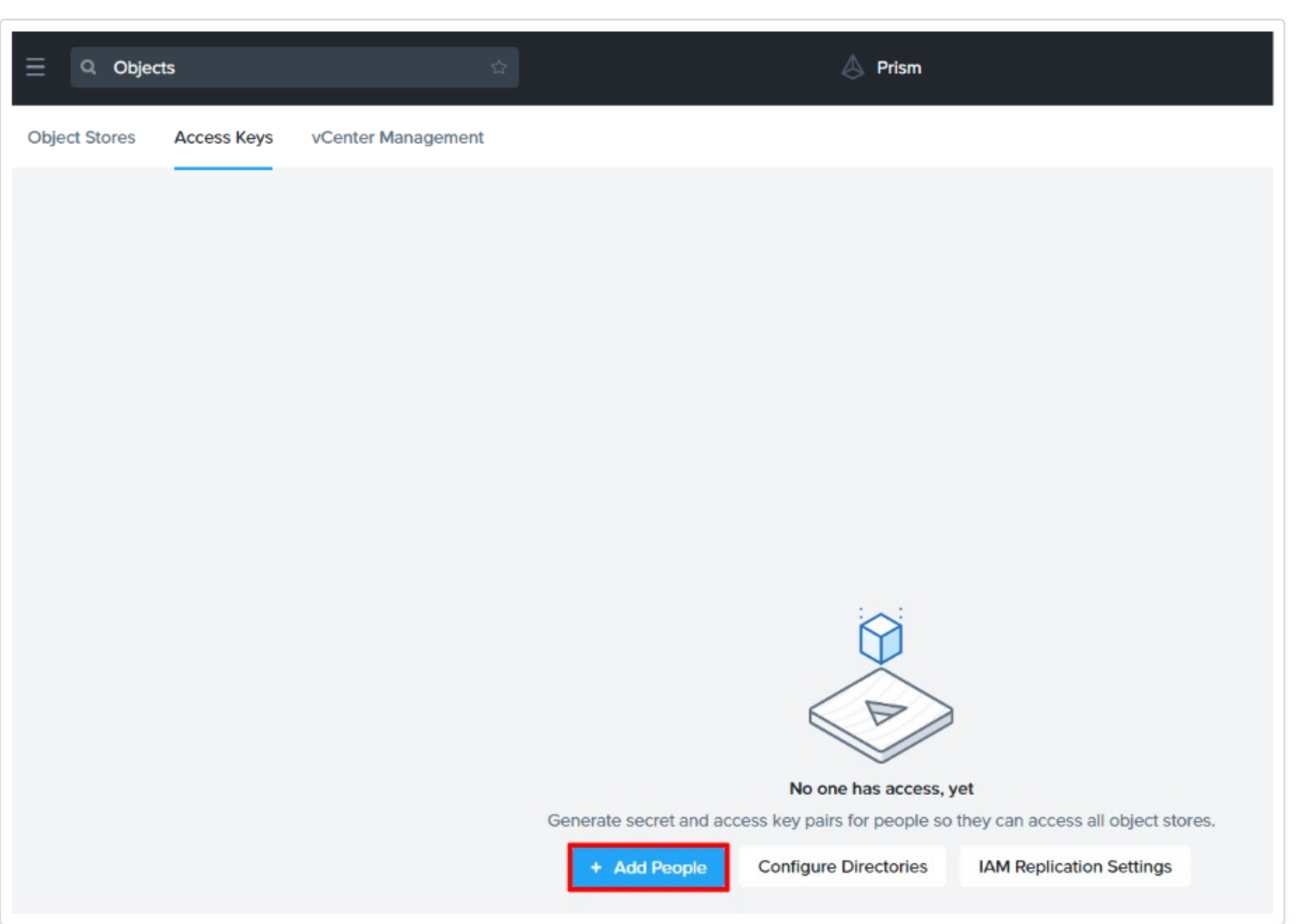
11. Click **Next** > **Done**.

> **WORM**
>
> WORM storage prevents the editing, overwriting, renaming, or deleting of data and is crucial in heavily regulated industries (finance, healthcare, public agencies, etc.) where sensitive data is collected and stored. Examples include emails, account information, voice mails, and more.
>
> If WORM is enabled on the bucket, this will supersede any lifecycle expiration policy.

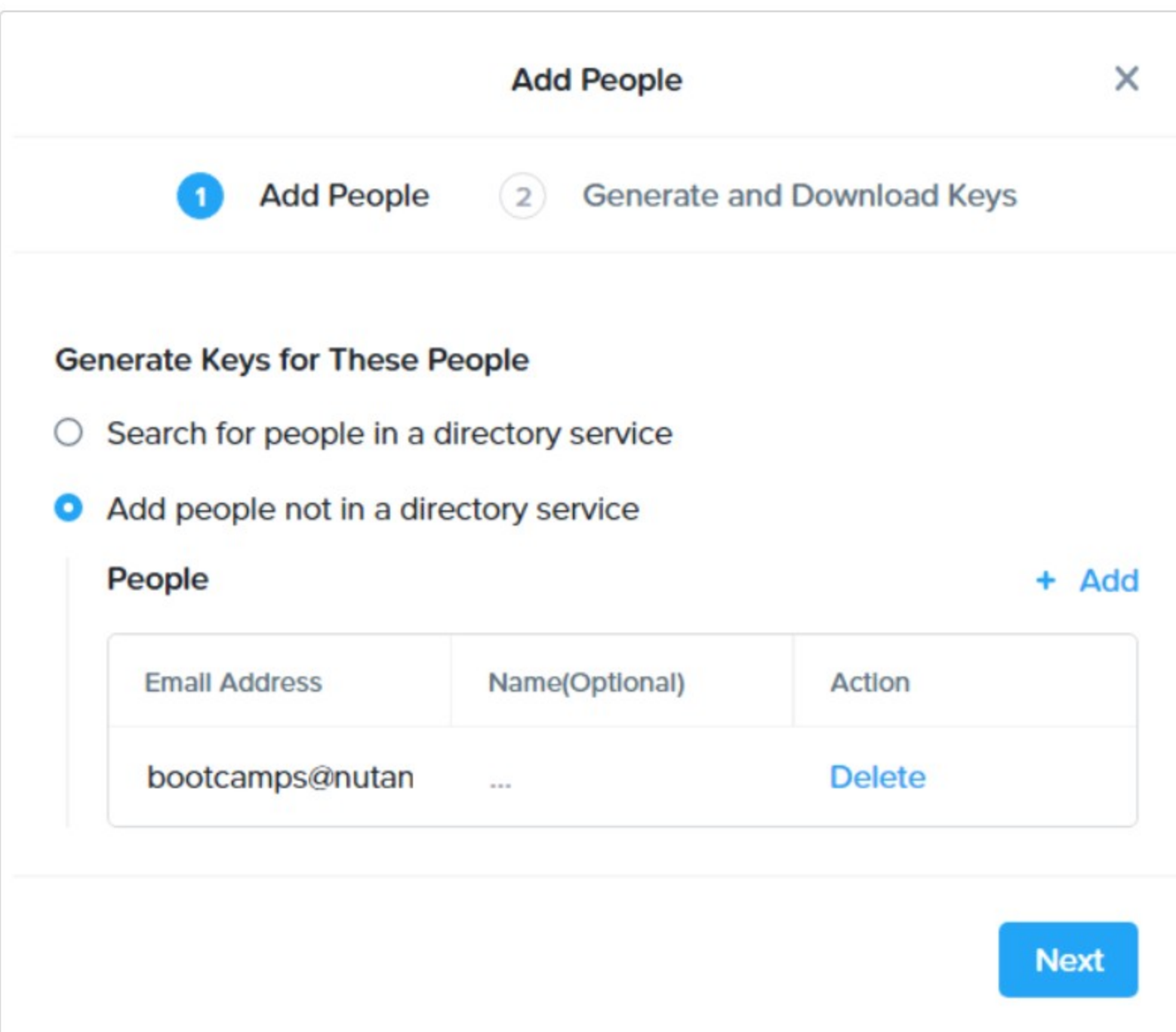
User Management

In this exercise, you will generate access and secret keys to access the Object store that will be used throughout the lab.

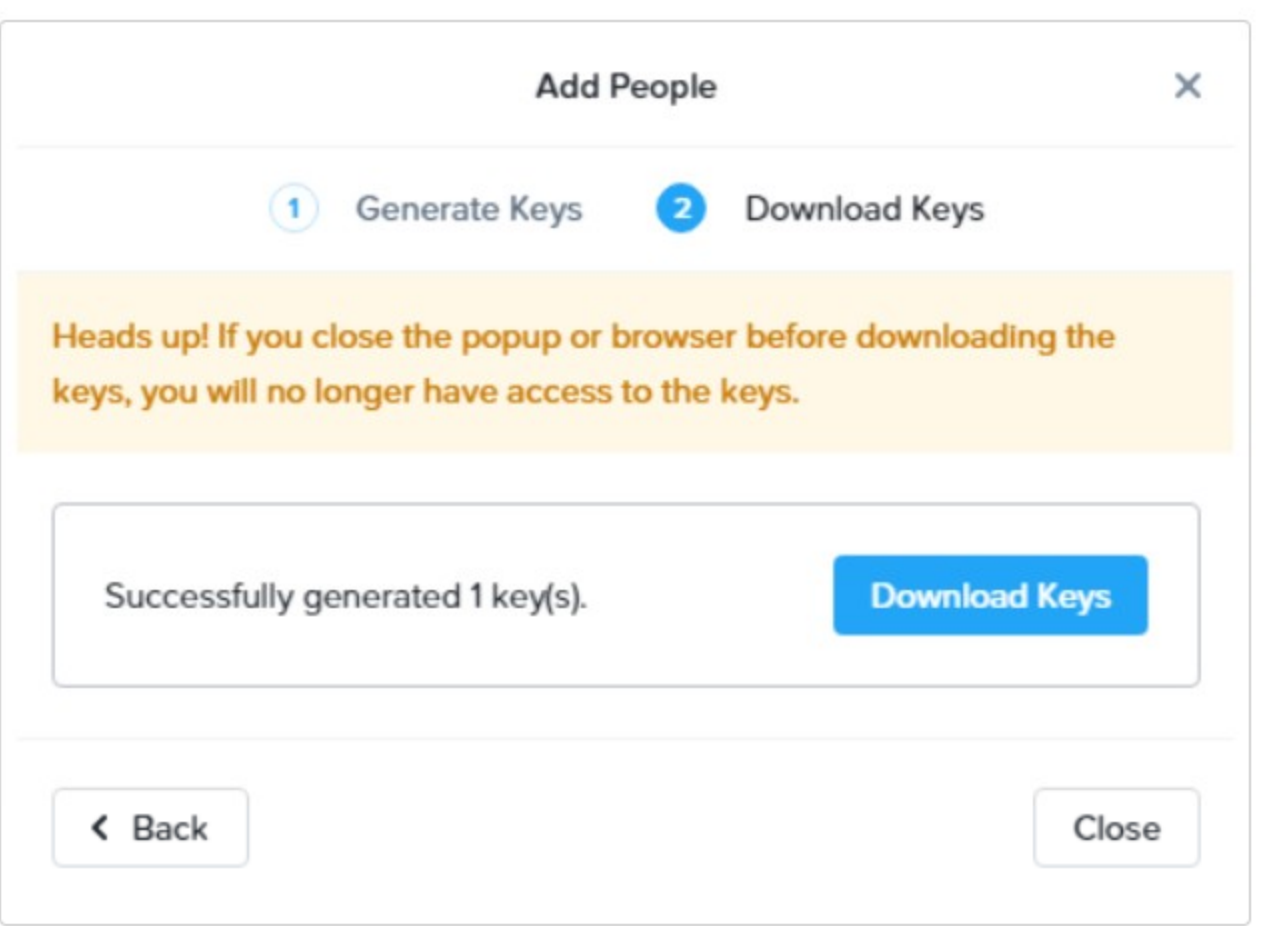
1. Within *Prism Central*, select ☰ > **Services** > **Objects**.
2. Click on **Access Keys** and then **+ Add People**.



3. Select **Add people not in a directory service**, and enter your work or personal e-mail address.



4. Click **Next**, and then click **Generate Keys**.
5. Click **Download Keys** to download a .txt file containing the *Access Key* and *Secret Key*.



6. Click **Close**.
7. Open the file with a text editor.

```
Username: bootcamps@nutanix.com
Access Key: KpWEnU0wSuuTGpPM5piCT9d13k2kTFKT
Secret Key: 0BRH4BKt_7T19nZrU1u_Mdg1L8_0I-VA
```

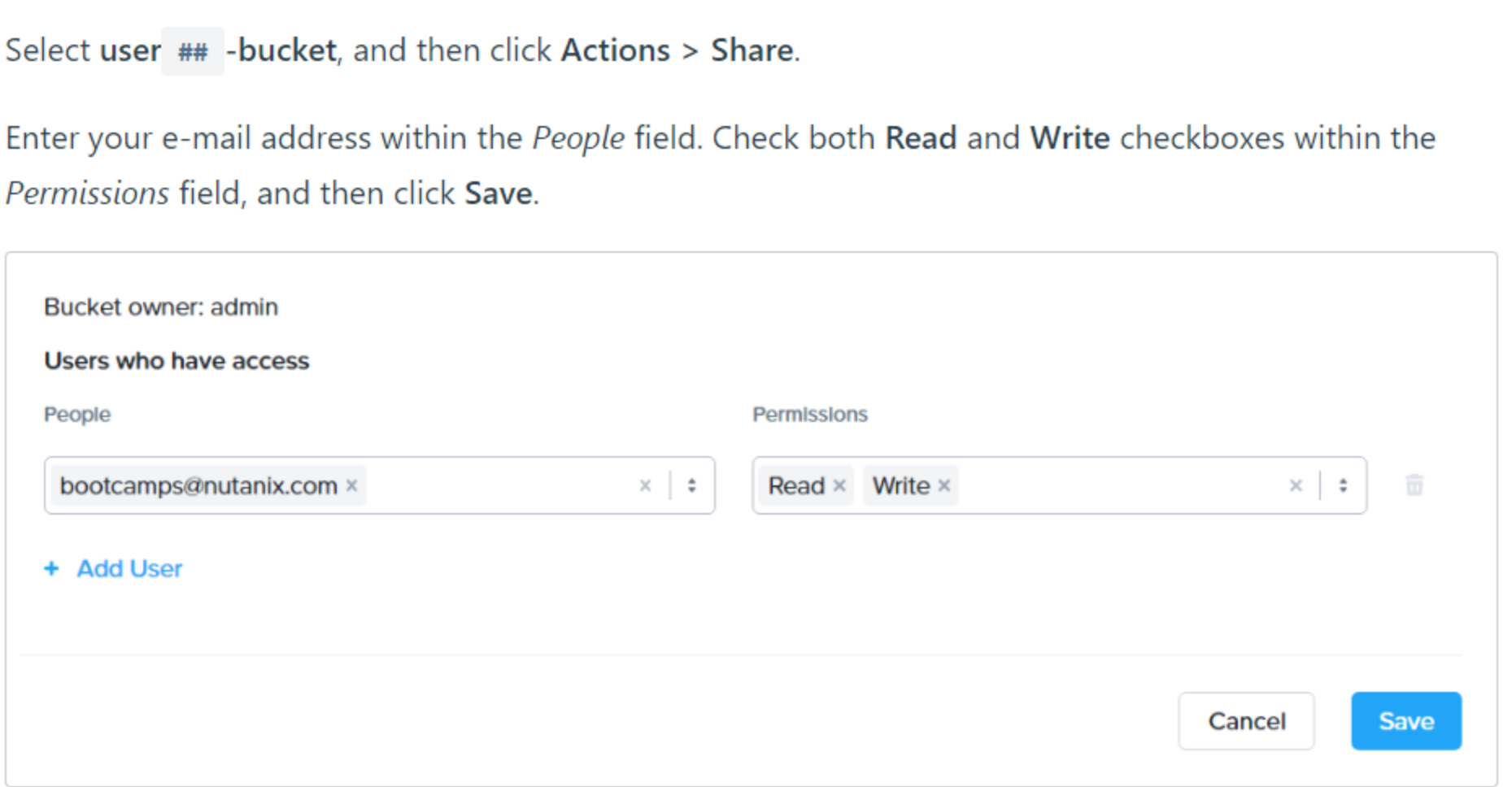
Keep the text file open, to have the access and secret keys readily available for future labs.

> **Note**
>
> You can always revoke or renew access keys.

Granting Bucket Access

Next, you will grant other users access to your bucket. You can configure read/write access on a per user basis.

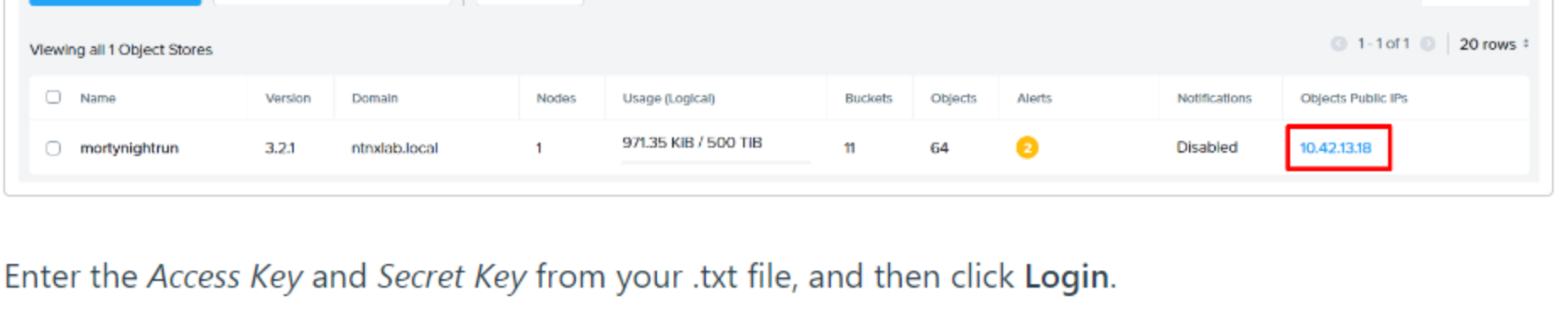
1. Click on **Object Stores** > **mortynightrun**.
2. Select **user** `##` **-bucket**, and then click **Actions** > **Share**.
3. Enter your e-mail address within the *People* field. Check both **Read** and **Write** checkboxes within the *Permissions* field, and then click **Save**.



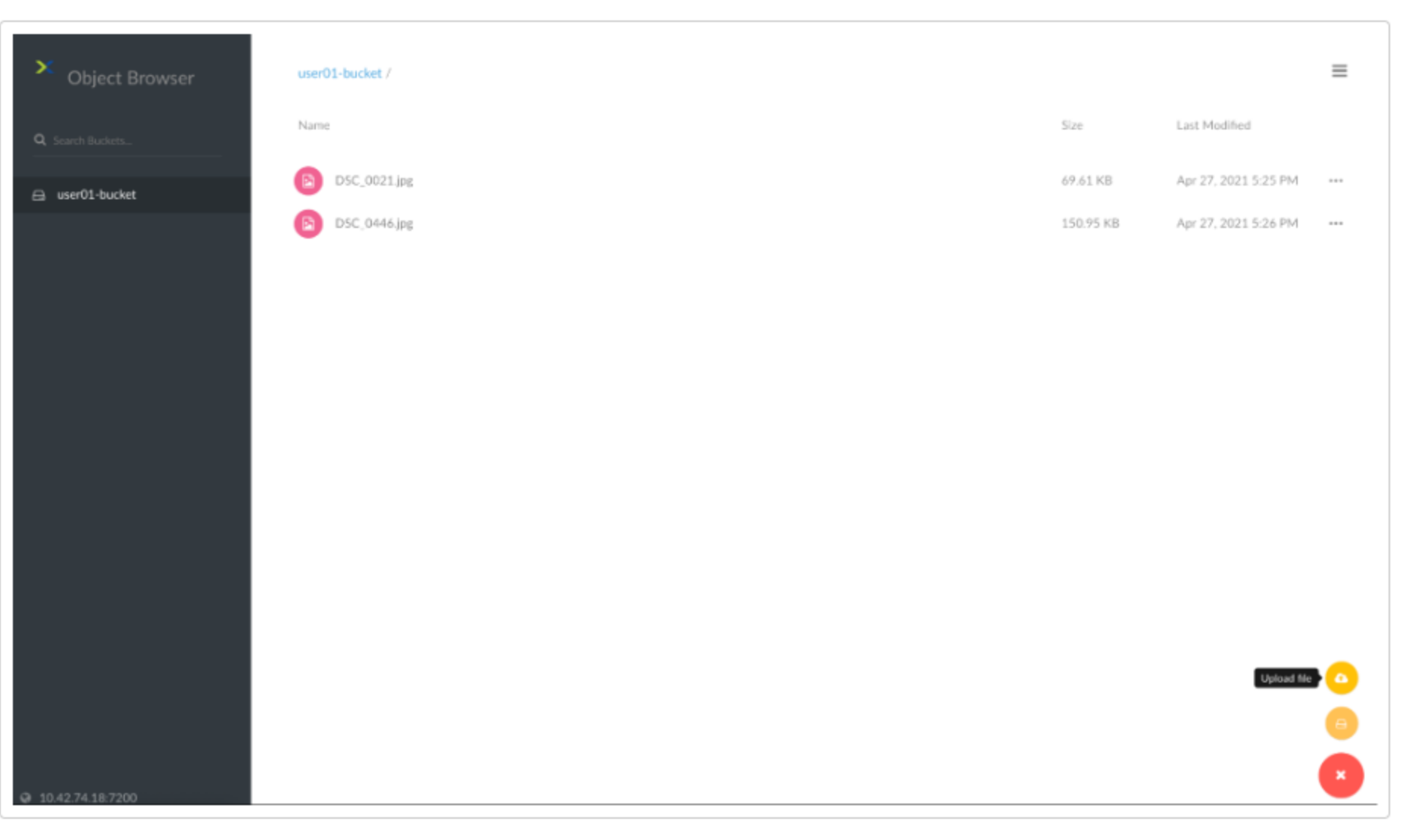
Objects Browser

In this exercise, you will use the *Objects Browser* to create and access buckets in the object store.

1. Within your *USER##*-WinTools VM, download sample images using **this** link, and extract it to your desktop.
2. Within your `USER##` **-WinTools** VM, open *Prism Central* and select ☰ > **Services** > **Objects**.
3. Click on **Objects Public IPs**.



4. Enter the *Access Key* and *Secret Key* from your .txt file, and then click **Login**.
5. Click on *user##*-bucket. From the *Upload Objects* drop-down, select **Select Files**.
6. Navigate to the *sample-pictures* directory on your desktop, and upload one picture to your bucket. You may optionally repeat this process to upload multiple pictures.



Object Versioning

Object versioning allows the upload of new versions of the same object, while retaining the original data. Versioning can be used to preserve, retrieve, and restore every version of every object stored within a bucket. This allows for easy recovery situations such as unintended user action, or application failures.

1. Within your *USER##*-WinTools VM, open *Notepad*.
2. Enter `version 1.0` , and then save the file on your desktop as **user##.txt**.
3. Within *Objects Browser*, upload the text file to **user** `##` **-bucket**, and then click **Close** once the upload has completed.
4. Open *user##.txt*, modify the file to now contain `version 2.0` , and then save the file.
5. Upload *user##.txt* once again to your bucket.
6. Return to *Prism Central*. Within *Object Stores*, click on **mortynightrun**, and then user `##` **-bucket**.
7. Look at the *Total number of objects* entry.

Properties

Name	Status
Link	https://user01-bucket.mortynightrun.ntnxlab.local
Total number of objects	2
Used Capacity (logical)	22 byte(s)
Versioning	Enabled
WORM	Yes (3 years)

You will see that there is an object created for every version of your test file. By keeping multiple versions of the same file, Nutanix Objects makes it possible to restore old versions at any point in time. Additionally, S3 compatible third-party tools can access previous versions of any given file.

Last Updated: 5/26/2023, 1:44:20 PM

← File Analytics Ransomware Protection

Preparing For Disaster

Nicely done! In just three days, you managed to protect Blips and Chitz, Inc.'s critical applications using Nutanix best practices, helping prevent or reduce the fallout of a security breach or data loss.

After your daily report to Roy, you being creating a disaster recovery strategy, to ensure your critical systems return to operation after an outage.

For that, you'll configure a consistent protection policy, a DR site, and a backup system that is reliable enough against the ransomware *Krombopulos*.

This will put Nutanix to the test. It's only a matter of (ever-decreasing) time until Roy expects the new infrastructure to be fully production-ready.

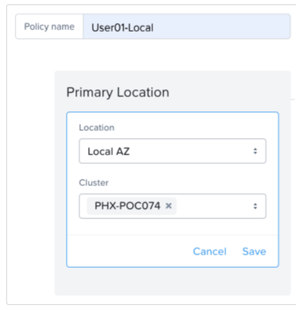
Last Updated: 5/2/2023, 11:07:35 AM

Protecting Your Environment →

Protecting Your Environment

Creating a Protection Policy

1. Within *Prism Central*, select ☰ > **Data Protection and Recovery** > **Protection Policies**.
   - If DR is not enabled, click the link to `Enable Disaster Recovery`
2. Click **Create Protection Policy**. Fill out the following fields, and then click **Save**.
   - **Policy name** - `USER##` -Local (ex. USER01-Local)
   - **Primary Location** > **Location** - Local AZ
   - **Cluster** - `<YOUR-CLUSTER>` (ex. PHX-POC074)



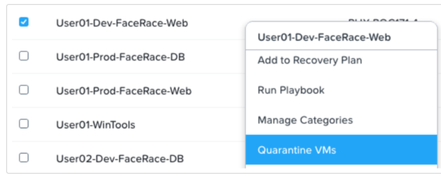
3. Click **Add Local Schedule**. Fill out the following fields, and then click **Save Schedule**:
   - **Take Snapshot Every** - Hour(s) 1
   - **Retention Type** - Linear (default)
   - **Retention on Local AZ** : `<CLUSTER>` - 5 Recover Points
4. Within the **Recovery Location** click **Cancel**, and then click **Next**.
5. Within the *Search for a category* field, select **AppType:** `##` **-FaceRace** (ex: Apptype:01-FaceRace), and then click **Add** > **Create**.

You now have a continuous stream of snapshots protecting these VMs, making it possible to roll back your FaceRace application to a previous point in time.

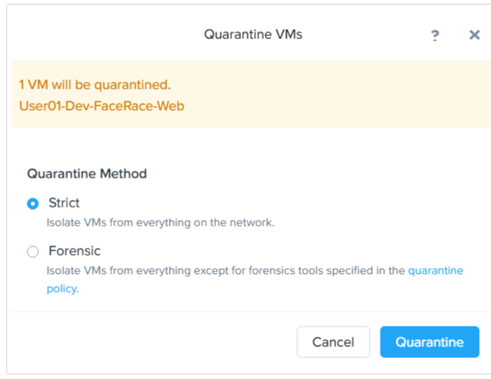
Recovery Of A Compromised VM

You've identified that your *User##-Dev-FaceRace-Web* VM has been compromised by ransomware. You'll need to act quickly to prevent this VM from sending or receiving traffic by quarantining it.

1. Within Prism Central, select ☰ > **Compute and Storage** > **VMs**.
2. Select **User** `##` **-Dev-FaceRace-Web**, and then click **Actions** > **Quarantine VMs**.



3. Select **Strict**, and then click **Quarantine**.



> **Note**
>
> Quarantining a VM using *Strict* mode will prevent the VM from sending or receiving traffic. While not used here, there is also *Forensics* mode, which restricts the VM to only being able to communicate with specified VMs. This enables investigation of the VM, while still preventing all other traffic.
>
> The red icon next to the VM name means that it has been quarantined.
>
>
>
>
> If you were now to ping the *User##-Dev-FaceRace-Web* VM from any other VM, you would observe that the ping would fail.

Bring an infected VM back to a stable state

We will now restore your compromised VM to the previous known-good state, and confirm it is operating as expected.

1. Within *Prism Central*, select ☰ > **Compute and Storage** > **VMs**.
2. Click on **User** `##` **-Dev-FaceRace-Web** > **Recovery Points**.
3. Select the latest snapshot, click **Restore** from the *Actions* drop-down, and then click **Restore**.
4. Return to ☰ > **Compute and Storage** > **VMs**, and open the console for the restored copy of the VM (ex: User01-Dev-FaceRace-Web_clone1).
5. Confirm you are able to communicate with other VMs by performing a ping test to them.

Within seconds you were able to not only avert a potential disaster by immediately quarantining an infected VM, but restore the VM to normal operation.

Last Updated: 5/26/2023, 1:44:20 PM

Simulating An Attack

You're impressed so far, but like the old Russian proverb states: Доверяй, но проверяй (Trust, but verify). How can you simulate an attack against Blips and Chitz, Inc.? You don't have the necessary experience to conduct a penetration test yourself, so you go about trying to find a tool that can simulate an Advanced Persistent Threat (APT).

What is Infection Monkey?

Infection Monkey by Guardicore, is a tool that can be used to simulate and automate many of the same actions a penetration test would typically perform. While penetration tests by skilled professionals are more thorough and accurate, this can serve as an initial attempt to expose potential critical vulnerabilities in this new system.

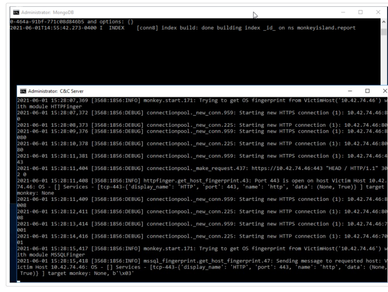
Infection Monkey is an open source breach and attack simulation (BAS) platform that allows you to discover security gaps and fix them. It uses various methods to self propagate across a data center, and reports success to a centralized *Monkey Island* server. You can simulate credential theft, compromised machines and other security flaws, and mimic the what is commonly observed in ransomware attacks, albeit non-destructively. Infection Monkey is executed from a user-friendly, web-based GUI.

The Infection Monkey is comprised of two parts:

- *Monkey* - A tool which infects other machines and propagates to them.
- *Monkey Island* - A dedicated server to control and visualize the Infection Monkey's progress inside the data center.

Installing Infection Monkey

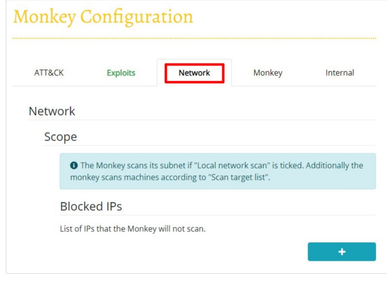
1. Log in to your `USER##` -**WinTools** VM using the following credentials:
   - **User Name** - `administrator`
   - Password - `nutanix/4u`
2. Download Infection Monkey, and the required Microsoft Visual C++ package. Both are found **here**.
3. You will first install the Microsoft Visual C++ package *VC_redist.x64*, followed by *InfectionMonkey*.
4. Open *File Explorer*, navigate to `C:\Program Files\Guardicore\Monkey Island\vmonkey_island\MonkeyIsland.exe` , and execute it.
5. Two terminal screens will open. These terminal sessions are for the *MongoDB* instance, and *C&C Server* (Command and Control). Minimize, but do not close these windows.



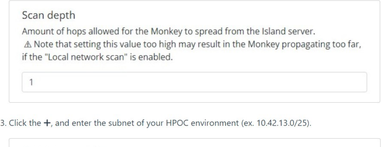
6. Additionally, Chrome will launch. This session may initially time-out, as it takes a few minutes for the *MongoDB* and *C&C Server* services to start. Once they are ready, you can refresh Chrome, and continue.
7. When connecting to the web interface for the first time, you will be prompted to setup a username and password, or continue without a username/password. Click the link that says **I want anyone to access this island**.

Configuring Infection Monkey

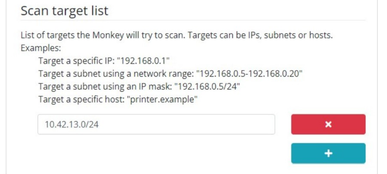
1. Click **Configure Monkey**, and then the **Network** tab.



2. Set the *Scan depth* to **1**. This will prevent Infection Monkey from scanning outside of the local subnet.



3. Click the **+**, and enter the subnet of your HPOC environment (ex. 10.42.13.0/25).



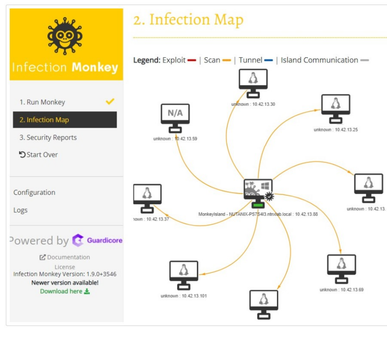
4. Click **Submit**.

Run Infection Monkey

1. Click **Run Monkey** from the left-hand menu, and then click on **Run on Monkey Island Server**.

Infection Monkey will require approximately 10 minutes to discover machines on the network.

2. Click on **Infection Map**. This provides a visual map of the discovered machines, exploits, etc. You can also view the *Security Reports* while it is running, once the scan has completed. This will provide more complete information on the findings.



Last Updated: 5/2/2023, 11:07:35 AM

Configuring a Syslog Server →

Configuring a Syslog Server

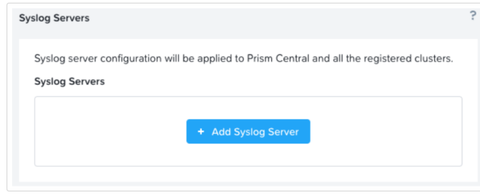
The last task in this section is observe the setup of a syslog server to collect all the system logs that will be generated by AOS, AHV and Prism. The following are the steps they will demonstrate.

1. Within *Prism Central*, select ☰ > **Compute & Storage** > **VMs**. Find the *KiwiSyslog* VM, and note its IP address.

> **Note**
>
> While you are here, open the console, and then the Kiwi Syslog Service Manager and observe that there is no data collection being performed.

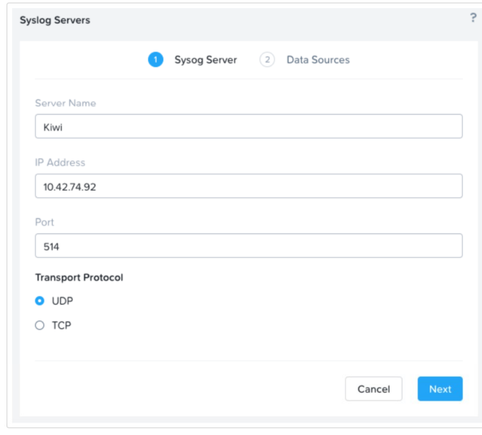
2. Select ☰ > **Prism Central Settings** > **Syslog Server**.

3. Click **+ Add Syslog Server**.

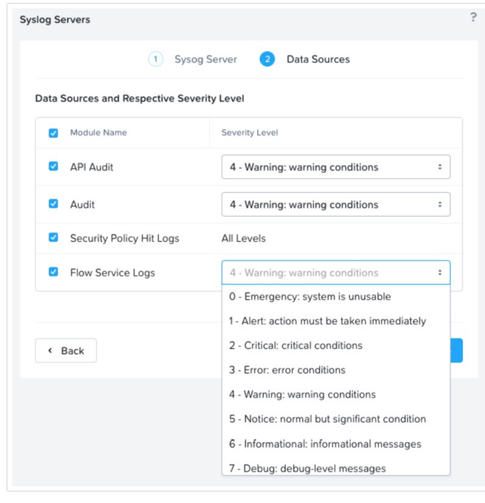


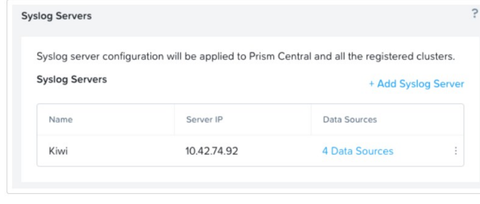
4. Fill out the following fields, and then click **Next**.

- **Server Name** - Kiwi
- **IP Address** - `<KIWISYSLOG-IP-ADDRESS>`
- **Port** - 514
- **Transport Protocol** - UDP

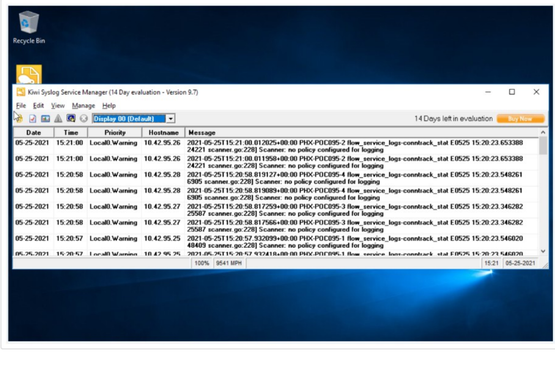


5. Select the modules and associated severity level to capture, and then click **Save**.





6. Select ☰ > **Compute & Storage** > **VMs**. Open the *KiwiSyslog* console. Observe that logs are now being collected.



Glossary

Nutanix Core

AOS

AOS stands for Acropolis Operating System, and it is the OS running on the Controller VMs (CVMs).

Pulse

Pulse provides diagnostic system data to Nutanix customer support teams so that they can deliver proactive, context-aware support for Nutanix solutions.

Prism Element

Prism Element is the native management plane for Nutanix. Because its design is based on consumer product interfaces, it is more intuitive and easier to use than many enterprise application interfaces.

Prism Central

Prism Central is the multi-cloud control and management interface for Nutanix. Prism Central can manage multiple Nutanix clusters and serves as an aggregation point for monitoring and analytics.

Node

An industry-standard x86 server with server-attached SSD and optional HDD (All-Flash & Hybrid Options).

Block

2U rackmount chassis contains 1, 2, or 4 nodes with shared power and fans and no shared backplane.

Storage Pool

A storage pool is a group of physical storage devices, including PCIe SSD, SSD, and HDD devices for the cluster.

Storage Container

A container is a subset of available storage used to implement storage policies.

Anatomy of a Read I/O

Performance and Availability

- Data is read locally
- Remote access only if data is not locally present

Anatomy of a Write I/O

Performance and Availability

- Data is written locally
- Replicated on other nodes for high availability
- Replicas are spread across the cluster for high performance

Nutanix Flow

Application Security Policy

Use an application security policy to secure an application by specifying allowed traffic sources and destinations.

Isolation Environment Policy

Use an isolation environment policy when you want to block all traffic, regardless of direction, between two groups of VMs identified by their category. VMs within a group can communicate with each other.

Quarantine Policy

Use a quarantine policy when you want to isolate a compromised or infected VM and optionally wish to subject it to forensics. You cannot modify this policy, and the two modes to quarantine a VM are Strict or Forensic.

Strict: Use this value when you want to block all inbound and outbound traffic.

Forensic: Use this value when you want to block all inbound and outbound traffic except the traffic to and from categories that contain forensic tools.

AppTier

Add values for the tiers in your application (ex. web, application_logic, and database) to this category and use the values to divide the application into tiers when configuring a security policy.

AppType

Associate the VMs in your application with the appropriate built-in application type such as Exchange and Apache_Spark. You can also update the category to add values for applications not listed in this category.

Environment

Add values for environments that you want to isolate from each other and then associate VMs with the values.

Last Updated: 5/2/2023, 11:07:35 AM

Accessing the Environment

Nutanix employees are able to access the Hosted POC environment with the **corporate GlobalProtect VPN**, or via either method covered below.

Partners and customers can gain access to the Hosted POC environment using the following:

Lab Access User Credentials

PHX Based Clusters:

- Username: PHX-POC###-User## (User01 through User20. Ex. PHX-POC123-User15)
- Password: *<PROVIDED BY INSTRUCTOR>*

RTP Based Clusters:

- Username: RTP-POC-User (User01 through User20. Ex. RTP-POC123-User15)
- Password: *<PROVIDED BY INSTRUCTOR>*

Frame VDI

Users can also access the HPOC through a Frame on AHV session.

Log in to: **https://console.nutanix.com/x/labs**

Access From	Type	Credentials
Nutanix	Internal	NUTANIXDC
Prospect/Customer/Partner	External	Lab Access User Credentials

Parallels VDI

Users can also access the HPOC through a non-persistent Windows 10 virtual desktop.

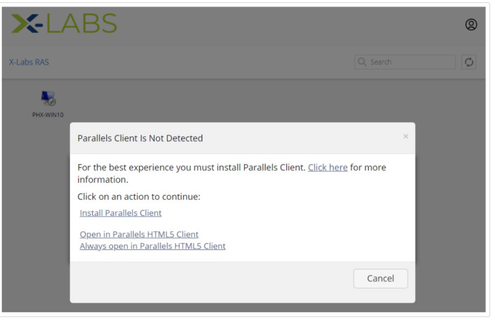
PHX Based Clusters Login to: **https://phx-vpn.xlabs.nutanix.com**

RTP Based Clusters Login to: **https://dm3-vpn.xlabs.nutanix.com**

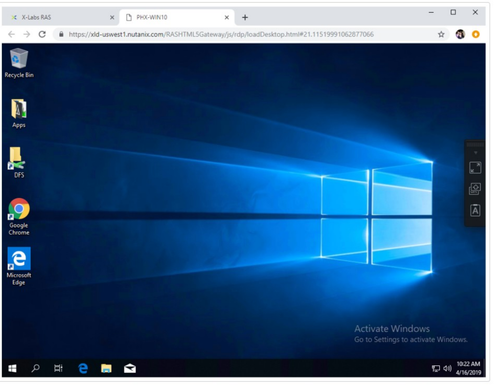
BLR Based Clusters Login to: **https://xlv-blr.xlabs.nutanix.com**

Access From	Type	Credentials
Nutanix	Internal	NUTANIXDC
Prospect, Customer, Partner	External	Lab Access User Credentials

The WIN10 desktop can be accessed through a locally installed Parallels client or via HTML5.



The local client is recommended, but the HTML5 client is a great option for users unable to install applications on their device.



Pulse Secure VPN

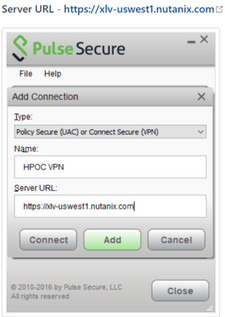
> **Note**
>
> Use of the VPN solution requires attendees to install the Pulse agent on their device. Attendees may not have local administrator access to their device to allow for installation.

Refer to your **automation@nutanix.com** *Reservation Confirmation* e-mail for the *Lab Access User Credentials* associated with the reservation.

Each reservation receives 20 accounts in the format of <Cluster \Name>-User<01-20>, using the same password associated with the reservation.

1. Log in to **https://xlv-uswest1.nutanix.com** (for PHX clusters) or **https://xlv-useast1.nutanix.com** (for RTP clusters) using one of the provided accounts.
2. Under *Client Application Sessions*, click **Start** to the right of *Pulse Secure* to download the client.
3. Install and open **Pulse Secure**.
4. Add connection:

- **Type** - Policy Secure (UAC) or Connection Server
- **Name** - HPOC VPN
- **Server URL** - **https://xlv-uswest1.nutanix.com** or **https://xlv-useast1.nutanix.com**



1. Connect using the provided credentials.

Last Updated: 5/2/2023, 11:07:35 AM

Network Configuration

The following tables detail the network IP Address assignments for multi-node and single-node environments.

Multi-Node Reservations

IP Range	Service	Comments
10.x.x.7	Hyper-V Failover IP	
10.x.x.8 - 10.x.x.14	Files	
10.x.x.15	File Analytics	
10.x.x.16 - 10.x.x.21	Objects	
10.x.x.22		
10.x.x.23	Beam	
10.x.x.25 - 10.x.x.28	Hosts	
10.x.x.29 - 10.x.x.32	CVMs	
10.x.x.33 - 10.x.x.36	IPMI	
10.x.x.37	Cluster IP	
10.x.x.38	Data Services IP	
10.x.x.39	Prism Central	
10.x.x.40	VCSA	vCenter
10.x.x.41	AutoAD	Windows Domain Controller
10.x.x.42	PrismOpsLabUtilityServer	Used for Prism Ops Labs
10.x.x.44	Era	
10.x.x.45	Citrix DDC	
10.x.x.50 - 10.x.x.125	Primary Network IPAM	VLAN 0
10.x.x.126 - 10.x.x.254	Secondary Network IPAM	Secondary VLAN

Single Node Reservations

Partition 1	Partition 2	Partition 3	Partition 4	Service	Comments
10.38.x.1	10.38.x.65	10.38.x.129	10.38.x.193	Gateway	
10.38.x.5	10.38.x.69	10.38.x.133	10.38.x.197	AHV Host	
10.38.x.6	10.38.x.70	10.38.x.134	10.38.x.198	CVM	
10.38.x.7	10.38.x.71	10.38.x.135	10.38.x.199	Cluster IP	
10.38.x.8	10.38.x.72	10.38.x.136	10.38.x.200	Data Services	
10.38.x.9	10.38.x.73	10.38.x.137	10.38.x.201	Prism Central	
10.38.x.11	10.38.x.75	10.38.x.139	10.38.x.203	AUTOAD	Windows Domain Controller
10.38.x.12	10.38.x.76	10.38.x.140	10.38.x.204	Utility Server	Prism Ops Lab
10.38.x.14	10.38.x.78	10.38.x.142	10.38.x.206	Era	
10.38.x.15	10.38.x.79	10.38.x.143	10.38.x.207	Citrix DDC	
10.38.x.32 - 10.38.x.37	10.38.x.96 - 10.38.x.101	10.38.x.160 - 10.38.x.165	10.38.x.224 - 10.38.x.229	Objects	
10.38.x.38 - 10.38.x.58	10.38.x.102 - 10.38.x.122	10.38.x.166 - 10.38.x.186	10.38.x.230 - 10.38.x.250	Primary Network IPAM	6 IPs free for static assignment

Last Updated: 5/2/2023, 11:07:35 AM

← Accessing the Environment

Active Directory User and Groups →

Active Directory User and Groups

Each cluster has a dedicated domain controller VM - AUTOAD - responsible for providing Active Directory services for the *ntnxlab.local* domain. The domain is pre-populated with the following users and groups:

Group	Username(s)	Password
Administrators	Administrator	nutanix/4u
SSP Admins	adminuser01 - adminuser25	nutanix/4u
SSP Developers	devuser01 - devuser25	nutanix/4u
SSP Consumers	consumer01 - consumer-25	nutanix/4u
SSP Operators	operator01 - operator-25	nutanix/4u
SSP Custom	custom01 - custom25	nutanix/4u
Bootcamp Users	user01 - user25	nutanix/4u

Last Updated: 5/2/2023, 11:07:35 AM

← Network Configuration

Getting Help →

Getting Help

The cluster (ex. RX, password not working, Foundation failed, cluster in a degraded state, etc.). **#rx-and-hpoc**

The lab content (ex. instructions incorrect or unclear, typos, feedback, etc.) or staging (ex. images or blueprints are missing). **#technology-bootcamps**

Frame, Parallels VDI, or Pulse VPN access. **#x-labs**

Feedback and suggestions can also be submitted to **bootcamps@nutanix.com**.

Last Updated: 5/2/2023, 11:07:35 AM

← Active Directory User and Groups