

# Introducing NetScaler

## Student Guide

NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on Introducing the NetScaler, was designed to:

- Capture essential job-related information, including On the Job Application.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Contents and click the question of interest.



# Table of Content

## Skills covered in this course

[What is true about NetScaler's role in handling client and server communication?](#)

[What is the purpose of network link aggregation?](#)

[When determining the system throughput of a NetScaler physical appliance, what factors are involved in this decision?](#)

[An administrator is investigating a network issue and has identified that incoming client requests are not reaching the backend servers. What could be the possible explanation for this issue?](#)

[An administrator configured a new VPX NetScaler following the initial IP address setup that appears during the initial installation, NSIP, Netmask, and Gateway. After conducting some tests, the Administrator observed that the NetScaler could only be accessed from IP addresses located within the same subnet as its NSIP. What is a possible explanation for this behavior?](#)

[If you want to access the NetScaler management interface and configure the appliance, which IP address should you use?](#)

[Given a situation where you need to use NetScaler in a two-arm mode deployment with multiple subnets, what should you do to leverage this configuration effectively?](#)

[An administrator is configuring a NetScaler for the first time. They need to establish communication between the NetScaler and servers on a specific subnet. What should they do to achieve this?](#)

[An administrator is investigating the loss of the most recent configuration on the production NetScaler appliance after a power outage. What might be the cause of this incident?](#)

# Clip: Introducing NetScaler Networking

---

## Scenario/Challenge:

What is true about NetScaler's role in handling client and server communication?

---

Within the NetScaler environment, it situates itself as an intermediary, intercepting client requests, and routing them to the backend server. In this dual communication flow, NetScaler assumes the roles of both the client and the server. Understanding this concept is essential for comprehending NetScaler's contributions to client and server communication.

## Understanding NetScaler's Role in Client and Server Communication

This section explains NetScaler's involvement in client and server communication through a comprehensive understanding of its role.

### Handling Client and Server Communication

- Layers of Focus:
  - Traditional networking typically revolves around layers 2 and 3 of the Open Systems Interconnection (OSI) model, dealing with switching and routing.
    - NetScaler, on the other hand, primarily focuses on layers 4 through 7, emphasizing the transport layer through the application layer.
- Layer 7 Dynamics:
  - At layer 7, we encounter client/server requests and responses, especially in scenarios like viewing a web page after entering a URL.
    - The client initiates a request to the server service, and the server responds, indicating success or an error.
- NetScaler's Role:
  - NetScaler positions itself in the middle of the traffic to intercept and capture requests sent by the client.

- It forwards these requests to the backend server, effectively serving as both the client and the server for two distinct communication flows.
  - Reverse Proxy Concept:
    - This configuration, where NetScaler acts as an intermediary between client requests and server responses, is commonly referred to as a reverse proxy.
      - The NetScaler assumes the role of a go-between, facilitating communication without the client directly interacting with the backend server.
- 

## On the Job Application

- NetScaler utilizes Virtual Servers to efficiently mediate between client requests and server responses.
  - Virtual Servers play a key role in various NetScaler features, contributing to its effectiveness in managing and optimizing communication flows.
  - By default, NetScaler utilizes its subnet IP (SNIP) for communication with the backend server. However, this behavior can be modified, either at the service level or globally.
-

# Clip: NetScaler VLANs and Link Aggregation

---

## Scenario/Challenge

What is the purpose of network link aggregation?

---

Understanding the purpose of network link aggregation, especially in the context of aggregating interfaces for bandwidth requirements, is crucial for optimizing network performance. By referring to the provided source and grasping the concepts outlined in this guide, you will be well-prepared to answer questions related to this topic.

## Understanding Network Link Aggregation

This section explores the details of network link aggregation.

### Introduction

- Network link aggregation, also known as NIC teaming or bonding, is a technique used to combine multiple physical network links into a single logical link.
    - The purpose of this technique is to enhance performance, improve fault tolerance, and meet bandwidth requirements.
  - Aggregating Interfaces for Bandwidth Requirements:
    - The primary purpose of network link aggregation is to address bandwidth requirements. When a single network link is not sufficient to meet the data transfer demands, multiple interfaces can be aggregated to work as a unified channel.
      - This also allows for the simultaneous use of multiple links, significantly increasing the available bandwidth.
  - Source Reference:
    - In the provided source, the phrase "Link aggregation, often referred to as NIC teaming or NIC bonding, can be done to aggregate interfaces into channels to satisfy bandwidth requirements" emphasizes the goal of combining interfaces to fulfill increased bandwidth needs.
-

## On the Job Application

- Link aggregation not only enhances bandwidth but also improves network reliability. If one link fails, the traffic is automatically redirected to the remaining active links, minimizing downtime.
- It is essential to configure link aggregation properly, considering compatibility with network devices and ensuring support from the network infrastructure.
- After adding interfaces to a channel, it loses its Virtual Local Area Networks (VLAN) configuration and is returned to the default VLAN. Nevertheless, these channels can be subsequently bound back to their original VLAN.
- The NetScaler supports both port-based VLANs and 802.1q tagged VLAN

# Clip: Introducing NetScaler Networking

---

## Scenario/Challenge

When determining the system throughput of a NetScaler physical appliance, what factors are involved in this decision?

---

Understanding the factors influencing the system throughput of a NetScaler physical appliance, particularly the emphasis on the platform being used, is crucial for making informed decisions in network deployments.

## Understanding NetScaler Physical Appliance System Throughput

This section explains about the NetScaler Physical Appliance System Throughput.

### Introduction

- System throughput is a crucial metric when assessing the performance of a NetScaler physical appliance. It refers to the amount of data that the appliance can process within a given time frame.
  - The primary factor influencing the system throughput of a NetScaler physical appliance is the platform being used.
    - The platform encompasses the hardware specifications, processing power, and other physical attributes of the NetScaler appliance.
- The provided source highlights that for NetScaler physical appliances, the system throughput is determined by the platform in use. This emphasizes the importance of considering the hardware specifications when evaluating the appliance's performance.
  - It's important to note the distinction between virtual platforms (VPX) and physical appliances.
    - For virtual platforms, the system throughput is determined by the VPX license purchased, indicating a software-based limitation rather than hardware specifications.



---

## On the Job Application

- While the platform is a key factor, other considerations such as network bandwidth requirements and the overall network deployment plan should also be considered.
  - Different NetScaler models may have varying throughput capacities, so it's essential to choose a model that aligns with the network's demands.
  - Always refer to the NetScaler hardware datasheet to choose the hardware that best suits your requirements.
-

# Clip: NetScaler Initial IP Addressing

---

## Scenario/Challenge

If you want to access the NetScaler management interface and configure the appliance, which IP address should you use?

---

As a learner, understanding how to access the NetScaler management interface is crucial for configuring the appliance. By mastering the NSIP configuration and understanding its role in accessing the NetScaler management interface, you set the foundation for effective management and configuration of the NetScaler appliance.

## Accessing NetScaler Management Interface

This section explains the process of accessing the NetScaler Management Interface.

### Initial IP Addressing

- When setting up NetScaler, the initial step involves configuring the IP address for management purposes.
    - After turning on the NetScaler, be patient as the boot process unfolds. It might take a couple of minutes to reach the console.
  - NSIP Configuration
    - Once prompted, you will need to enter the NetScaler's IP address. This is referred to as the NSIP (NetScaler IP).
      - Along with the NSIP, provide the Netmask for the NSIP and the Gateway IP. This information is essential for network connectivity.
      - Input the required information and choose whether to make changes or save and continue with the boot process.
  - Patience during Boot
    - During the interface activation phase, it is common to see a significant amount of text. Use this time to be patient or take a break.
      - The boot process may take some time, especially during the activation of interfaces. Avoid unnecessary concerns if the device seems to take a while to complete.
-



## On the Job Application

- Ensure accurate input of the NSIP, Netmask, and Gateway IP during the initial setup to establish proper network connectivity.
  - Understand that the boot process may take some time. Avoid unnecessary concerns and let the NetScaler complete its initialization.
  - Once configured, the NSIP allows persistent access to the NetScaler management interface for ongoing configuration and management tasks.
  - Implement secure practices when configuring the NSIP, such as using strong passwords and adhering to security guidelines.
-

# Clip: Introducing NetScaler Networking

---

## Scenario/Challenge

An administrator is investigating a network issue and has identified that incoming client requests are not reaching the backend servers. What could be the possible explanation for this issue?

---

Understanding the potential causes of network issues, especially the impact of VLAN misconfigurations on client requests reaching backend servers, is crucial for administrators.

## Understanding Network Connectivity Issues

This section explains common network connectivity issues, offering insights into potential challenges and their solutions.

### Introduction

- Network connectivity issues can manifest in various ways, affecting the flow of data between clients and backend servers.
    - An administrator investigating a network issue notices that incoming client requests are not reaching the backend servers.
  - Potential Explanation: VLAN Misconfiguration:
    - The source highlights that IPs owned by the NetScaler can be used on any available interface.
      - If there is a failure to associate an IP address with an interface, it might be due to VLAN misconfiguration.
      - The provided source emphasizes the role of VLAN configuration in associating IP addresses with interfaces and logically managing data flow within the NetScaler.
-

## On the Job Application

- VLAN 1 is the default VLAN on NetScaler.
  - It is a best practice not to use the default VLAN 1 for user traffic. Instead, create dedicated VLANs for specific purposes to enhance security and organization.
  - For scenarios where multiple VLANs need to be carried over a single interface, implement VLAN trunking.
  - Every subnet should be linked to a corresponding VLAN.
-

# Clip: NetScaler Initial IP Addressing

---

## Scenario/Challenge

An administrator configured a new VPX NetScaler following the initial IP address setup that appears during the initial installation, NSIP, Netmask, and Gateway. After conducting some tests, the Administrator observed that the NetScaler could only be accessed from IP addresses located within the same subnet as its NSIP. What is a possible explanation for this behavior?

---

Understanding the relationship between NSIP, Netmask, Gateway, and subnet configuration is crucial for ensuring proper network access to the NetScaler. In this case, troubleshooting the gateway configuration can resolve the issue of limited accessibility to the NetScaler from addresses outside its local subnet.

## Understanding NetScaler IP Configuration

This section explains the configuration of NetScaler IP, providing insights into its setup and management.

### IP Configuration Process

- Initial Setup:
  - During the initial installation of the VPX NetScaler, the administrator is prompted to configure key parameters, including the NetScaler IP (NSIP), Netmask, and Gateway IP.
- NSIP Configuration:
  - The NSIP is a crucial element in this setup, serving as the primary IP address through which the NetScaler can be accessed.
- Gateway Configuration:
  - The administrator also configures the Gateway IP, which is essential for directing traffic beyond the local subnet.
- Possible Explanation for Behavior:
  - In the scenario described, the NetScaler is only accessible from IP addresses within the same subnet as its NSIP.
  - The likely explanation for this behavior is that the configured default gateway is unable to direct traffic to other subnets.

---

## On the Job Application

- Ensure that the gateway is properly configured to route traffic to external subnets, allowing broader accessibility to the NetScaler.
  - Confirm the accuracy of the subnet netmask.
  - DNS is also important if leading with name resolution.
-

# Clip: NetScaler Deployments

---

## Scenario/Challenge

Given a situation where you need to use NetScaler in a two-arm mode deployment with multiple subnets, what should you do to leverage this configuration effectively?

---

NetScaler deployment in a two-arm mode with multiple subnets is a strategic choice for scenarios requiring the NetScaler to be inline with both the client and server networks. This configuration allows for more control and flexibility, but it requires careful consideration and proper setup.

## Understanding Two-Arm Modes

This section explains the concepts behind Two-Arm Modes.

### Considerations for Two-Arm Mode

- **Interface Requirements:** Two-arm mode necessitates multiple interfaces on the NetScaler to handle communication between the client and server networks.
  - **Communication Flow:** All communication is directed through the NetScaler in two-arm mode, providing control over the traffic flow.
  - **VLAN and Subnet Support:** Two-arm mode supports the use of multiple subnets and VLANs, offering greater flexibility in network design.
  - **Redundancy:** Similar to one-arm mode, redundancy considerations apply to networking equipment to prevent downtime. However, with multiple interfaces, there is potential for increased resilience.
-

## On the Job Application

- Understand one-arm and two-arm deployment modes for NetScaler. Choose the appropriate mode based on network architecture and communication flow.
- Leverage VLANs to efficiently organize and manage network traffic, ensuring proper segmentation.
- Ensure that NetScaler has the necessary interfaces available to support two-arm mode.
- Plan for switch redundancy to mitigate downtime risks, ensuring continuous communication flow in case of switch failures.



# Clip: NetScaler IPs

---

## Scenario/Challenge

An administrator is configuring a NetScaler for the first time. They need to establish communication between the NetScaler and servers on a specific subnet. What should they do to achieve this?

---

When configuring a NetScaler for the first time, it's essential to establish communication between the NetScaler and servers on a specific subnet. One crucial step in achieving this is setting up Subnet IP (SNIP) addresses.

## Set Up SNIPs for Server Communication

This section explains the process of setting up Subnet IP addresses (SNIPs) for server communication, outlining the necessary configurations and steps.

### Configuration Steps

1. Access NetScaler Configuration:
  - Use the NSIP (NetScaler IP) to access the NetScaler's management interface and configuration settings.
2. Navigate to SNIP Configuration:
  - Locate the SNIP configuration section within the NetScaler settings.
3. Add SNIP for Specific Subnet:
  - Add a new SNIP address for the subnet where the servers are located.
  - Specify the IP address that represents the NetScaler on the chosen subnet.
4. Configure Subnet Communication:
  - Associate the newly added SNIP with the appropriate settings to enable communication with servers on the specific subnet.
5. Validate Configuration:
  - Confirm that the SNIP configuration is accurate and matches the subnet requirements.



- Test communication between the NetScaler and servers to ensure successful connectivity.
- 

## On the Job Application

- Gain a comprehensive understanding of key NetScaler IP addresses, including NSIP, SNIP, and VIP.
  - Before configuring, identify the specific subnet where communication needs to be established between the NetScaler and servers.
  - Test and verify communication between the NetScaler and servers on the specific subnet after configuring SNIPs.
  - Concentrate on subnet-specific configuration by leveraging SNIPs, ensuring seamless communication within the targeted network environment.
-

# Clip: NetScaler Initial Configuration

---

## Scenario/Challenge

An administrator is investigating the loss of the most recent configuration on the production NetScaler appliance after a power outage. What might be the cause of this incident?

---

When facing a situation where the most recent configuration on the production NetScaler appliance is lost after a power outage, it's crucial to understand potential causes and preventive measures.

## Preventing Configuration Loss: Key Steps to Follow

This section provides the key steps to avoid configuration loss.

### Steps to Avoid Configuration Loss

1. Access the NetScaler Configuration Interface:
  - Use a web browser to connect to the NetScaler appliance's management interface.
2. Make Configuration Changes:
  - Implement any necessary changes or updates to the NetScaler configuration.
3. Save Configuration Changes:
  - Navigate to the configuration management section of the interface.
  - Look for an option to save or apply changes. This might involve clicking a "Save" or "Apply" button.
4. Verify Configuration Persistence:
  - Confirm that the configuration changes have been successfully saved by checking for any confirmation messages or status indicators.
5. Regular Backups:
  - Establish a routine for backing up the NetScaler configuration to an external location. This ensures that even if a power outage occurs, you can restore the configuration from a recent backup.
6. Scheduled Saves:

- Some NetScaler appliances allow you to schedule automatic saves of the configuration at specified intervals. Consider configuring scheduled saves to minimize the risk of configuration loss.
- 

## On the Job Application

- schedule routine backups of the NetScaler configuration to safeguard against data loss, enabling quick restoration after incidents like power outages.
  - Utilize automation tools or scripts to automatically save configurations at specified intervals, reducing the risk associated with manual oversight and forgetfulness.
  - Set up monitoring tools to track the NetScaler environment, including alerts for pending configuration changes that have not been saved, enabling administrators to take prompt action.
-



**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# Deploying NetScaler Common Traffic Management Features

Student Guide

NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on Deploying NetScaler Common Traffic Management Features, was designed to:

- Capture essential job-related information, including On the Job Application.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Content and click on the question of interest.

# Table of Content

## Skills covered in this course:

What is the name of the SSL deployment scenario where the NetScaler handles all SSL-encrypted communication between the client and the web servers?

What is the key difference between SSL Offload and SSL Bridge deployments on NetScaler?

Your organization is concerned about optimizing SSL communications and reducing the load on backend servers, what would you recommend based on the leading practices?

In the context of maintaining session persistence for a shopping cart application, what is the recommended method to ensure that connections are part of the same persistence session?

The IT administrator at a medium-sized e-commerce company is tasked with planning SSL on a NetScaler for their public-facing website. They need to ensure that the SSL deployment is secure and efficient. What is the recommended approach for obtaining an SSL certificate for securing their public-facing website?

Which SSL deployment scenario places more load on the backend servers due to the absence of SSL decryption and limited traffic control by the NetScaler?

An administrator is investigating a NetScaler issue and notices that incoming client requests are not being distributed correctly. What is the possible cause of this situation?

A NetScaler administrator is investigating an issue with a website's SSL certificate. Users are reporting security warnings when trying to access the site. What is the most likely explanation in this case?

What is the principal function of the NetScaler probe monitor?

What happens to the load balancing virtual server if a server within a service group becomes unresponsive?

In a scenario where users are experiencing SSL certificate errors when accessing a



website through NetScaler, what is the next step to resolve this issue effectively?

Given a scenario in a NetScaler load balancing setup where a specific service member consistently experiences higher traffic than others, analyze the following strategies to optimize the distribution of traffic and ensure fairness among service members. Which of these strategies would most effectively address the issue?

When configuring a load balancing virtual server, what would be the appropriate step to ensure that the load balancing virtual server is able to receive connection requests from clients effectively?

Which of the following accurately represents the primary use of load balancing?

What is the main advantage of SSL Offload in a NetScaler deployment?

In the context of the SSL offload scenario described, what is the primary advantage of configuring the NetScaler to handle SSL-encrypted communication?

Given a SSL handshake scenario, what changes would you make to ensure the successful establishment of a secure connection between the client and the server?



# Clip: SSL Deployments

---

## Scenario/Challenge

What is the name of the SSL deployment scenario where the NetScaler handles all SSL-encrypted communication between the client and the web servers?

---

In NetScaler, Secure Sockets Layer (SSL) deployment scenarios play a crucial role in managing encrypted communication between clients and web servers. In this section, we will cover the SSL Offload scenario.

## Managing Encrypted Communication Between Clients and Web Servers

This section explains the management of encrypted communication between clients and web servers.

### SSL Offload Deployment Scenario

- SSL Offload is a deployment scenario that optimizes the SSL-encrypted communication flow between clients and web servers. It enhances server performance by alleviating the burden of SSL processes from the backend servers, allowing them to operate more efficiently.
  - In this scenario, the NetScaler takes on the responsibility of handling all SSL-encrypted communication between the client and the web servers. In this setup, the communication between the NetScaler and the backend servers remains unencrypted.
- Enabling SSL Offload offers several advantages:
  - Load Reduction on Servers: By offloading SSL encryption and decryption processes to the NetScaler, backend servers experience reduced load. This allows servers to focus on their primary role of performing application tasks.
    - Enhanced Server Efficiency: With SSL Offload, servers can concentrate on application-specific functions rather than managing SSL processes contributing to improved overall server efficiency.

## On the Job Application

- To leverage SSL Offload and enjoy its benefits, ensure that the SSL Offload feature is enabled on your NetScaler device.
  - There are other SSL deployment scenarios on NetScaler, such as End-to-End SSL and SSL Bridge. Each serves different purposes, and the choice depends on specific requirements.
-

# Clip: Planning SSL on NetScaler

---

## Scenario/Challenge

What is the key difference between SSL Offload and SSL Bridge deployments on NetScaler?

---

As you embark on configuring SSL deployment scenarios on NetScaler, it's essential to grasp the key differences between SSL Offload and SSL Bridge. This knowledge will guide you in making informed decisions based on your specific environment and requirements.

## SSL Offload vs. SSL Bridge

This section compares SSL Offload and SSL Bridge, highlighting the distinctions between these approaches to secure socket layer (SSL) processing.

### SSL Offload

- Definition: SSL Offload is a deployment scenario where the NetScaler handles SSL-encrypted communication between the client and server.
  - Key Characteristics:
    - The NetScaler takes on the responsibility of decrypting SSL traffic from clients.
    - It handles the SSL decryption and encryption processes, reducing the load on backend servers.
    - The communication between the NetScaler and the backend servers is unencrypted.

### SSL Bridge

- Definition: SSL Bridge is a deployment scenario where the NetScaler forwards encrypted traffic to the target server without decrypting it.
  - Key Characteristics:
    - Encrypted traffic from clients is forwarded directly to the backend servers without decryption.
    - SSL termination and encryption are performed by the backend servers.
- When deciding between SSL Offload and SSL Bridge, consider the following factors:
  - Determine if your environment or manager requires end-to-end SSL.
    - Yes: If you want to leverage additional features on the NetScaler, choose SSL Offload.

- No: Opt for SSL Bridge.
- 

## On the Job Application

- Remember that SSL Offload handles SSL-encrypted communication between the client and server, while SSL Bridge forwards encrypted traffic to the target server without decryption.
  - The communication between NetScaler and backend servers is unencrypted when SSL offload is in place.
  - If you want to leverage additional features on the NetScaler, consider SSL Offload. If not, and end-to-end SSL is not required, choose SSL Bridge.
  - Consider SSL Offload if additional NetScaler features are desired.
-

# Clip: Planning SSL on NetScaler

---

## Scenario/Challenge

Your organization is concerned about optimizing SSL communications and reducing the load on backend servers. What would you recommend based on the leading practices?

---

Understanding and implementing SSL Offload on NetScaler is a strategic approach to optimize SSL communications. This practice aligns with leading industry standards and can significantly improve the overall performance and efficiency of your organization's SSL-encrypted communication.

## Optimizing SSL Communications with SSL Offload

This section explores the optimization of SSL communications through SSL Offload.

### Introduction

- Optimizing SSL communications is a key concern for organizations aiming to reduce the load on backend servers. In the context of NetScaler, one leading practice is to implement SSL Offload. This guide will help you understand and recommend SSL Offload based on best practices.
  - Definition: SSL Offload is a practice where the NetScaler takes on the responsibility of handling SSL-encrypted communication between clients and servers.
    - Objective: The primary goal of SSL Offload is to optimize SSL communications by offloading the SSL decryption and encryption processes from backend servers to the NetScaler.
  - Reducing Backend Server Load: SSL Offload significantly reduces the computational load on backend servers by handling SSL decryption and encryption centrally on the NetScaler.
- Implementation Benefits:
  - By implementing SSL Offload, your organization can experience enhanced performance, improved response times, and better utilization of backend server resources. Therefore, recommending SSL Offload is a sound choice in response to concerns about optimizing SSL communications and reducing backend server load.

---

## On the Job Application

- Based on leading practices and real-world examples, it is advisable to enable SSL Offload to optimize SSL-encrypted communication and reduce the load on backend servers.
  - SSL Offload involves NetScaler handling SSL-encrypted communication between clients and servers.
  - By offloading SSL decryption and encryption to NetScaler, backend servers can focus on other essential tasks, enhancing overall efficiency.
-



# Clip: Load Balancing Decision Making

---

## Scenario/Challenge

In the context of maintaining session persistence for a shopping cart application, what is the recommended method to ensure that connections are part of the same persistence session?

---

Maintaining session persistence is crucial for applications like shopping carts, ensuring a seamless user experience. This section will help you understand and recommend the advised method to ensure connections are part of the same persistence session on NetScaler.

## Choosing the Persistence Method

This section guides you through the process of choosing the persistence method.

### Session Persistence Methods

- In the context of a shopping cart application, two common session persistence methods are used:
    - Cookie Insert: In the Cookie Insert method, the NetScaler Cookie is inserted into the HTTP header.
    - How It Works: Connections that have the same NetScaler Cookie in the HTTP header are considered part of the same persistence session.
      - In the SourceIP method, connections from the same client IP address are considered part of the same persistence session.
  - Shopping Cart Example:
    - Consider a shopping cart application where it's essential to maintain a session with the same backend server for the user's shopping journey.
      - For maintaining session persistence in a shopping cart scenario, the recommended method is Cookie Insert.
      - Based on the nature of a shopping cart application and the need for maintaining a continuous session with the same backend server, it is advisable to utilize Cookie Insert as the preferred method for session persistence.
-

## On the Job Application

- Understanding the importance of session persistence, especially in applications like shopping carts, is crucial for delivering a seamless user experience.
  - NetScaler Cookie is inserted into the HTTP header for session persistence.
  - Connections with the same NetScaler Cookie in the HTTP header are treated as part of the same persistence session.
  - By choosing the recommended method of Cookie Insert, where the NetScaler Cookie is inserted into the HTTP header, you can ensure that connections remain part of the same persistence session, enhancing the overall performance and consistency of your application.
-



# Clip: SSL Certificates

---

## Scenario/Challenge

The IT administrator at a medium-sized e-commerce company is tasked with planning SSL on a NetScaler for their public-facing website. They need to ensure that the SSL deployment is secure and efficient. What is the recommended approach for obtaining an SSL certificate for securing their public-facing website?

---

Planning SSL deployment on NetScaler for a public-facing website involves crucial decisions for security and efficiency. Careful planning, from pre-work to SSL deployment, is essential for meeting the specific needs of your environment.

## SSL Certificate Overview

This section provides an overview of SSL certificates.

### Introduction

- Private Key Generation: Generate a private key on the NetScaler, ensuring a secure asymmetric key (public-private key pair) is created.
  - CSR Creation: Create a Certificate Signing Request (CSR) on the NetScaler. The CSR contains public information about the company and domain for which the certificate is required.
    - CSR Submission to CA: Send the CSR to an authorized Certificate Authority (CA), such as VeriSign. This step is necessary for the CA to process and validate the request, ensuring its authenticity.
    - CA Processing: Once the CA processes the CSR, it issues both the public SSL certificate and the intermediate CA certificate.
- Certificate-Key Pair Configuration: Configure the Certificate-Key Pair on the NetScaler, linking it to the intermediate CA certificate. Both files are installed on the NetScaler during this process.
  - SSL Virtual Server Binding: Bind the certificate-key pair to the SSL virtual server on the NetScaler. Until this step is completed, the SSL virtual server remains in a DOWN state.
  - Trust: Browsers trust certificates from well-known CAs, preventing security warnings for users.
  - Pre-Work: Perform pre-work, including certificate generation and determining the optimal SSL deployment.

---

## On the Job Application

- The recommended approach for obtaining an SSL certificate is to request it from an authorized Certificate Authority. This ensures a secure and trusted connection for your users, enhancing the overall reliability and reputation of your e-commerce platform.
  - Before obtaining a certificate, plan the SSL deployment on NetScaler based on your environment's needs.
  - Enhance the overall reliability and reputation of your e-commerce platform by prioritizing secure connections.
-

# Clip: SSL Deployments

---

## Scenario/Challenge

Which SSL deployment scenario places more load on the backend servers due to the absence of SSL decryption and limited traffic control by the NetScaler?

---

For efficient SSL deployment on NetScaler, understanding the impact of different scenarios on backend servers is crucial. This section aims to clarify which SSL deployment scenario the NetScaler supports and the capabilities of these deployments.

## Understanding the SSL deployments on the NetScaler

This section delves into understanding SSL deployments on the NetScaler.

### SSL Bridging Overview

- SSL Bridging is a deployment scenario that introduces considerations for managing SSL traffic between the client and the target server. Unlike other scenarios, SSL Bridging does not involve SSL decryption by the NetScaler, potentially impacting backend server performance.
  - SSL Bridging places more load on backend servers as traffic remains encrypted, bypassing NetScaler decryption capabilities.
    - In this scenario, the NetScaler primarily forwards traffic to the target server without actively managing SSL sessions or applying features and policies.
    - Instead of two separate SSL tunnels, SSL Bridging sends encrypted traffic directly through the NetScaler to the target server without decryption.
    - The absence of SSL decryption limits the NetScaler's ability to control and optimize traffic, potentially leading to poor performance on backend servers.

### SSL Offload Overview:

- In SSL Offload, the NetScaler handles SSL decryption, reducing the load on backend servers and allowing for effective traffic management.
  - Communication between the NetScaler and the backend server is unencrypted.
    - Unencrypted communication reduces the load on the backend server.
    - SSL certificate is installed on the NetScaler appliance.
    - Allows the server to focus on its application role rather than managing SSL encryption and decryption processes.

## SSL End-to-End overview

- End-to-end SSL involves maintaining separate SSL tunnels from the client to the NetScaler and from the NetScaler to the target server.
    - Clear text data is re-encrypted, and secure SSL sessions are used for communication with back-end web servers.
      - These handshakes can be CPU-intensive on the backend servers.
      - NetScaler utilizes SSL session multiplexing for backend SSL transactions.
      - SSL session multiplexing helps in reusing existing SSL sessions with back-end web servers.
      - Avoids the CPU-intensive SSL handshake process on the backend servers.
- 

## On the Job Application

- It is important to note that for all SSL deployment scenarios to be leveraged, the SSL Offload feature must be enabled on the NetScaler.
  - When SSL Bridge deployment is chosen, NetScaler cannot decrypt traffic.
  - Certain NetScaler features are unsupported in the presence of SSL Bridge deployment.
-

# Clip: Introduction to Load Balancing

---

## Scenario/Challenge

An administrator is investigating a NetScaler issue and notices that incoming client requests are not being distributed correctly. What is the possible cause of this situation?

---

For administrators handling NetScaler configurations, comprehending the complexities of incoming client request distribution is essential. This overview aims to provide insights into load balancing algorithms on NetScaler, enabling administrators to make informed decisions and maintain optimal performance.

## Overview of Load Balancing on NetScaler

This section provides an overview of load balancing on NetScaler.

### Introduction

- Load balancing evenly distributes workloads across multiple servers, optimizing resource usage and minimizing response time. There are several reasons why you might want to use load balancing in your environment:
  - Improved performance, redundancy, scalability, security, and cost-efficiency.
    - NetScaler offers various methods for decision-making on incoming load balancing traffic.
    - The virtual server makes load-balancing decisions based on the configured algorithm, load-balancing method, and service monitor results.
- Most used Load Balancing methods:
  - Least Connection:
    - Selects the service with the fewest active connections, optimizing resource usage.
    - Example Scenario:
      - Server 1: 3 active connections
      - Server 2: 15 active connections
      - Server 3: No active connections
    - Request Distribution:
      - Server 3 receives the 1st, 2nd, and 3rd requests.
      - Server 1 receives the 4th request.

- Round Robin:
  - Maintains a running queue of active services, distributing each connection to the next service in the queue.
  - Example Scenario:
    - Server 1: 3 active connections
    - Server 2: 15 active connections
    - Server 3: No active connections
  - Request Distribution:
    - Server 1 receives the 1st request.
    - Server 2 receives the 2nd request.
    - Server 3 receives the 3rd request.
    - Rotation continues for subsequent requests.
- Additional Consideration when the Slow Start feature is enabled.
  - Slow Start:
    - During the start-up of a virtual server or when the state changes, the round-robin method is initially used.
    - After the initial phase, the virtual server switches to the specified load-balancing method to prevent unnecessary load on a single server.

---

## On the Job Application

- Incorrect configurations of load balancing settings, persistence, or health monitors can lead to unexpected behavior.
  - When troubleshooting issues related to load balancing or session management, consider the impact of persistence.
  - Misconfigured algorithms may result in some servers becoming overloaded while others are underutilized.
-



# Clip: SSL Certificates

---

## Scenario/Challenge

A NetScaler administrator is investigating an issue with a website's SSL certificate. Users are reporting security warnings when trying to access the site. What is the most likely explanation in this case?

---

Understanding SSL certificates and their role in secure communication is crucial for troubleshooting and resolving issues. This section will help you address common issues related to SSL certificates.

## Investigating SSL Certificate Issues on NetScaler

This section guides you through investigating SSL certificate issues on NetScaler.

### SSL Communication Overview

- SSL
  - It is a protocol that ensures privacy and integrity in communications over TCP/IP. It relies on encryption using symmetric and public-key algorithms, such as Data Encryption Standard (DES), Rivest Cipher 4 (RC4), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Digital Signature Algorithm (ECDSA) to establish a secure connection between a client and a server.
- SSL Handshake Process:
  - Client "Hello" Message
    - Lists client capabilities and preferences.
    - Includes version, cipher suites, and compression methods.
    - Contains a 28-byte random number.
  - Server "Hello" Message:
    - Selects cipher suite and compression method.
    - Provide session ID and another random number.
    - Ensures at least one common cipher suite.
  - Server Sends Certificate:
    - Contains the server's digital certificate.
    - Optionally includes a "digital certificate request" for client authentication.
  - Client Verification:
    - Verifies the server's digital certificate.
    - Validates server "hello" parameters.

- Key Exchange:
  - Client sends a "client key exchange" message.
  - Includes the pre-master secret encrypted with the server's public key.
- Master Secret Derivation:
  - Client converts the pre-master secret into a master secret.
  - Generates key material for encryption and message authentication.
- Cipher Suite Change:
  - Client sends a "change cipher spec" message.
  - Switches the server to the negotiated cipher suite.
- Finished Messages:
  - Client sends the first encrypted "finished" message.
  - Server responds with its "change cipher spec" and "finished" messages.
  - SSL handshake concludes, and encrypted application data can be exchanged.

### **Troubleshooting Steps:**

1. Certificate Expiry Check:
    - Verify the expiration date of the SSL certificate. Certificates have a validity period, and if this period has lapsed, browsers will display warnings to users.
    - Renew or replace the certificate before it expires to avoid disruptions.
  2. Certificate Installation:
    - Ensure that the SSL certificate is correctly installed on the NetScaler Load Balancing Virtual Server, Content Switching Virtual Server, or VPN Virtual Server.
    - Check for any installation errors that might affect its functionality.
  3. Browser Certificate Store:
    - Confirm that the root certificate is installed in the browser's certificate store.
    - The lack of a valid root certificate can trigger security warnings.
-

## On the Job Application

- Obtain SSL certificates from reputable and trusted Certificate Authorities
  - Keep the private key secure to prevent unauthorized access and potential security breaches.
  - Promptly revoke and replace compromised certificates to maintain security.
  - Utilize wildcard or Subject Alternative Name (SAN) certificates for versatile use.
-

# Clip: Load Balancing Decision Making

---

## Scenario/Challenge

What is the principal function of the NetScaler probe monitor?

---

NetScaler users must comprehend the functionality of probe monitors to ensure the health and availability of backend servers. Probe monitors play a vital role in maintaining the optimal performance of services and service group members by periodically probing backend servers. Understanding their purpose is essential for efficient network management.

## Understanding the Principal Function of NetScaler Probe Monitors

This section explores the principal function of NetScaler Probe Monitors.

### Built-in Monitors

- NetScaler comes equipped with two default monitors, namely tcp-default and ping-default. These monitors are automatically bound to services during creation to facilitate immediate usability if the service is UP.
  - tcp-default monitor functionality:
    - Initiates a TCP 3-way handshake to ensure communication readiness at the server's port.
    - Validates the ability of TCP connections to be established.
  - ping-default monitor functionality:
    - Utilizes a simple ICMP request-response mechanism to validate network reachability.
    - Verifies basic connectivity with backend servers.

### Additional Pre-built Monitors

- Custom Monitors.
  - Creation:
    - Admins have the flexibility to create custom monitors.
    - Customization includes adjusting communication parameters sent to backend servers.

### Importance of Probe Monitors:

- Understanding the diverse capabilities of NetScaler probe monitors is instrumental in identifying the health state of backend servers. This knowledge aids in distinguishing between NetScaler and server-side issues during traffic assessments.

- By exploring the intricacies of probe monitors, users can enhance their ability to manage network health effectively, contributing to a robust and reliable infrastructure.

---

## On the Job Application

- NetScaler offers a variety of pre-built monitors designed for specific protocols, allowing users to tailor monitoring based on their application requirements.
  - Adjust monitoring parameters to align with specific application requirements to minimize false alerts.
  - Ensure probes align with backend server capabilities.
  - Regularly update monitors to reflect server-side changes.
-

# Clip: Load Balancing Process

---

## Scenario/Challenge

What happens to the load balancing virtual server if a server within a service group becomes unresponsive?

---

Understanding the intricacies of load balancing virtual server behavior and health states is crucial for effective NetScaler ADC administration. This section provides insights into how the virtual server behaves in response to service health changes, including the impact of a server going down in a load balancing deployment.

## Understanding Load Balancing Virtual Server Behavior

This section delves into understanding the behavior of Load Balancing Virtual Servers.

### Load Balancing Virtual Server Overview

- Traffic Distribution:
  - Distribution Across Services:
    - Incoming load is distributed across available services.
  - Balancing Methods:
    - Distribution method varies based on configured load balancing methods.

### Health Verification

- Pre-Connection Health Checks:
  - TCP Connection Checks:
    - TCP connections to target ports are tested for server responsiveness.
    - The NetScaler appliance establishes a 3-way handshake with the monitor destination and then closes the connection.
  - ICMP Pings:
    - NetScaler ADC can send ICMP pings to verify server health.
    - The NetScaler appliance sends an ICMP echo request to the destination of the monitor and expects an ICMP echo response.

### Service States

- Service Health Status
  - UP: Successful probes from all bound monitors.
  - DOWN: Probes fail to receive responses within configured time limits.



- OUT OF SERVICE (OFS): Administratively disabled service or gracefully shut down service.
- GOING OUT OF SERVICE (TROFS): Service administratively disabled with delay or gracefully shut down with active transactions.
- DOWN WHEN GOING OUT OF SERVICE (TROFS\_DOWN): Monitoring probe fails during GOING OUT OF SERVICE state.

## Virtual Server States

- Virtual Server Health Status:
  - UP: At least one bound service is UP.
  - DOWN: All bound services are DOWN, or the load balancing feature is not enabled.
  - OUT OF SERVICE (OFS): Administratively disabled virtual server, entering OFS state with effective state DOWN.

## Server Failure in Load Balancing Deployment

- Impact on Load Balancing:
  - Exclusion of Unresponsive Server: When a server becomes unresponsive, the virtual server continues to route traffic but excludes the unresponsive server.
  - Dynamic Adaptation: Load balancing adapts dynamically to server health changes to ensure uninterrupted service.

---

## On the Job Application

- Adjust health threshold parameters to balance responsiveness and accuracy.
  - Enable logging for health check results to track historical patterns.
  - Implement graceful shutdown procedures for backend servers to avoid abrupt service interruptions.
-

# Clip: SSL Process

---

## Scenario/Challenge

In a scenario where users are experiencing SSL certificate errors when accessing a website through NetScaler, what is the next step to resolve this issue effectively?

---

By understanding the SSL certificate lifecycle, obtaining certificates from authorized CAs, and addressing additional considerations, administrators can ensure secure and error-free SSL communication for users accessing websites through NetScaler.

## Resolving SSL Certificate Errors on the NetScaler

This section addresses the process of resolving SSL certificate errors on the NetScaler.

### SSL Certificate Overview

- SSL Certificate Basics: Importance of using a public signed certificate from an authorized Certificate Authority (CA) for public communication.

### SSL Certificate Configuration

- Certificate-Key Pair Configuration: Linking the Certificate-Key Pair to the intermediate CA certificate.

### SSL Entity

- SSL Virtual Server Binding:
  - Binding the certificate-key pair to the SSL entity (SSL Load Balancing Virtual Server, Content Switching Virtual Server, or VPN Virtual Server).
  - Addressing the DOWN state of the SSL virtual server by completing the binding process.

### SSL Validation

- SSL Certificate Validation
    - Verifying the validity of the SSL certificate and common name
    - Confirming the correct installation of the SSL certificate on NetScaler and linking.
    - Utilizing available tools on NetScaler to troubleshoot SSL-related issues, such as OpenSSL.
-

## On the Job Application

- Keep NetScaler software and SSL libraries up to date to address potential vulnerabilities.
  - Enable auditing features to capture relevant SSL-related events.
  - Check SSL/TLS protocol and cipher suite configurations.
-

# Clip: Load Balancing Process

---

## Scenario/Challenge

Given a scenario in a NetScaler load balancing setup where a specific service member consistently experiences higher traffic than others, analyze the following strategies to optimize the distribution of traffic and ensure fairness among service members. Which of these strategies would most effectively address the issue?

---

By understanding load balancing methods, the significance of weight settings, and the strategy of adjusting weights, administrators can effectively optimize traffic distribution in NetScaler load balancing setups, ensuring fairness and efficiency among service members.

## Optimizing Traffic Distribution in NetScaler Load Balancing

This section explores strategies for optimizing traffic distribution in NetScaler Load Balancing.

### Analyzing Strategies for Traffic Optimization

- Load Balancing Configuration Overview:
    - Load Balancing Methods: Exploring various load balancing methods, such as least connection and round robin, to influence traffic distribution based on different algorithms.
    - Weight Settings for Traffic Distribution: Analyzing the concept of assigning weights to services and its impact on determining the percentage of traffic each service member can handle.
    - Importance of Weights: Understanding how weights indicate the capacity of service members to handle requests, allowing for a more effective balance of load.
    - Weight Settings for Traffic Distribution: Analyzing the concept of assigning weights to services and its impact on determining the percentage of traffic each service member can handle
-

## On the Job Application

- By leveraging load balancing methods, adjusting weight settings, and fine-tuning configurations, administrators can effectively optimize traffic distribution in NetScaler load balancing setups.
  - Explore various load balancing methods, such as least connection and round robin, to influence traffic distribution using different algorithms.
  - Adjusting weights strategically can ensure fairness and efficiency in traffic distribution, addressing the challenges posed by uneven traffic among service members.
-

# Clip: Introduction to Load Balancing

---

## Scenario/Challenge

When configuring a load balancing virtual server, what would be the appropriate step to ensure that the load balancing virtual server is able to receive connection requests from clients effectively?

---

As a learner, understanding the key steps to configure a load balancing virtual server on NetScaler is essential for optimizing the performance, availability, and scalability of applications.

## Configuring Load Balancing Virtual Server Effectively

This section guides you through the effective configuration of Load Balancing Virtual Servers.

### Introduction to Load Balancing

- Load Balancing Overview:
    - Load balancing is a crucial feature on NetScaler designed to enhance the performance, availability, and scalability of various applications, including HTTP, HTTPS, and TCP-based applications.
      - NetScaler employs two fundamental object types for defining load balancing relationships:
        - Service: Represents the backend server's IP, port, and protocol.
        - Virtual Server: Represents the front-end server hosted on NetScaler with its own IP, port, and protocol. This is what DNS resolves to on the client side.
  - Configuring Load Balancing Virtual Server
    - When configuring a load balancing virtual server, the appropriate step is to ensure a unique combination of:
      - IP Address: Assign a distinct IP address to the load balancing virtual server.
      - Port: Specify a unique port for communication.
      - Protocol: Define the protocol to be used for load balancing.
-



## On the Job Application

- Explore additional configuration features to enhance load balancing functionality, such as protecting the configuration against failure, managing client traffic, monitoring servers, and handling large-scale deployments.
  - Customize settings as needed, including persistence for connections, to align with specific application requirements.
  - When configuring a load balancing virtual server, ensure a unique combination of IP address, port, and protocol to effectively receive connection requests from clients.
  - Regularly refer to NetScaler documentation for up-to-date information on load balancing configuration and best practices.
-

# Clip: Introduction to Load Balancing

---

## Scenario/Challenge

Which of the following accurately represents the primary use of load balancing?

---

Load balancing is a critical technique used in enterprise environments to optimize resource usage and enhance the performance, availability, and scalability of applications.

## Load Balancing Overview

This section provides an overview of load balancing.

### Primary Uses of Load Balancing

- **Improving Performance:** Distributing workloads evenly across multiple resources boosts overall application performance.
  - **Ensuring Redundancy:** Load balancing redirects traffic to available servers if one or more servers fail, ensuring continuous service.
  - **Scalability:** Load balancing allows adding additional servers to handle increased traffic, ensuring scalability.
  - **Security Enhancement:** Load balancing hides the IP addresses of backend servers and controls traffic through specific ports, enhancing security.
  - **Cost Efficiency:** Load balancing across multiple servers is often more cost-effective than using a single, large, expensive server.
- 

## On the Job Application

- Emphasize the primary use of load balancing, which is to improve application performance by evenly distributing workloads across multiple resources.
  - Recognize load balancing as a solution for scalability, allowing for the addition of servers to handle increased traffic as the user base grows.
  - Evaluate the security benefits of load balancing, including the added layer of security by concealing backend server IP addresses and controlling traffic through specific ports.
-

# Clip: SSL Deployments

---

## Scenario/Challenge

In the context of the SSL offload scenario described, what is the primary advantage of configuring the NetScaler to handle SSL-encrypted communication?

---

SSL offload is a critical configuration in the NetScaler environment that can significantly impact server load and application performance. By understanding and implementing SSL offload effectively, administrators can enhance the overall efficiency of their application delivery, providing a smoother experience for end-users while efficiently managing server resources.

## SSL Offload Scenario Overview

This section offers an overview of the SSL Offload scenario.

### Streamlining Server Load

- **Load Reduction on Backend Servers:** By offloading SSL processing to the NetScaler, the backend servers experience a reduction in load. This is because they no longer need to handle the resource-intensive SSL encryption and decryption processes.
- **Focusing on Application Roles:** With SSL offload, backend servers can dedicate more resources to performing their primary application roles. This specialization improves overall server efficiency and contributes to better application performance.

### Optimizing Application Performance

- **Avoiding SSL Handshake Overhead:** SSL handshakes, which typically occur every two minutes for security purposes, can be CPU-intensive on backend servers. SSL offload eliminates the need for repeated handshakes, contributing to a more streamlined and optimized communication process.
  - **SSL Multiplexing for Session Reuse:** NetScaler utilizes SSL multiplexing to reuse existing SSL sessions with backend web servers. This efficient reuse avoids the overhead of repeated handshakes, further enhancing application performance.
-

## On the Job Application

- Ensure that the SSL offload feature is activated on the NetScaler to take advantage of the primary benefit – streamlined server load and optimized application performance.
  - Confirm that the NetScaler has the required license for SSL offload functionality, ensuring that the SSL-encrypted communication is effectively managed.
  - Evaluate your organization's security requirements to determine whether front-end SSL, end-to-end SSL, or SSL bridge is the most suitable deployment, keeping in mind the trade-offs between security and performance.
-

# Clip: SSL Process

---

## Scenario/Challenge

Given an SSL handshake scenario, what changes would you make to ensure the successful establishment of a secure connection between the client and the server?

---

By focusing on the SSL handshake process you can contribute to the smooth and secure establishment of connections between a client and a server. Understanding the intricacies of SSL communication is essential for making informed decisions in configuring and maintaining secure network environments.

## SSL Handshake Steps

This section details the SSL handshake steps.

### Key SSL Handshake Steps

- **Root Certificate Installation:** For a client to establish a secure connection, a root certificate must be installed in the browser certificate store and on the client.
- **Client Hello Message:** The client initiates the SSL handshake by sending a Client Hello message containing cryptographic capabilities, version preferences, cipher suites, and a random number.
- **Server Hello Response:** The server responds with a Server Hello message, selecting cryptographic methods, a session ID, and another random number. Both client and server must support at least one common cipher suite for the handshake to proceed.
- **Server Digital Certificate:** The server sends its digital certificate, allowing the client to verify the server's identity.
- **Certificate Request (Optional):** If required, the server may send a digital certificate request message specifying supported certificate types and acceptable certificate authorities.
- **ServerHelloDone and Client Verification:** The server sends a ServerHelloDone message, and upon its receipt, the client verifies the server's digital certificate and checks the server's hello parameters.
- **ClientKeyExchange:** The client sends a ClientKeyExchange message containing a premaster secret, encrypted with the server's public key.
- **Key Material Derivation:** The client uses cryptographic operations to derive key material for encryption and message authentication from the premaster secret.
- **ChangeCipherSpec:** The client sends a ChangeCipherSpec message, indicating the switch to the newly negotiated cipher suite.
- **Finished Messages:** Both client and server exchange Finished messages, signaling the end of the SSL handshake, and encrypted application data can be transmitted securely.

---

## On the Job Application

- Thoroughly validate the authenticity of the server's digital certificate during the SSL handshake process.
  - Ensure that both the client and server support at least one common cipher suite to avoid handshake failures.
  - Stay updated on SSL/TLS protocol developments and versions.
-



# Clip: Planning SSL on NetScaler

---

## Scenario/Challenge

What is the main advantage of SSL Offload in a NetScaler deployment?

---

Understanding SSL deployment options and the advantages they offer is crucial for optimizing NetScaler performance. SSL Offload stands out for its ability to offload SSL-encrypted communication, thereby reducing the server load and improving overall efficiency in a NetScaler deployment.

## Advantage of SSL Offload

This section explores the advantages of SSL Offload.

### Main Advantage of SSL Offload

- Offloads SSL-Encrypted Communication:
    - SSL Offload shifts the responsibility of SSL encryption and decryption from backend servers to NetScaler.
    - When using SSL Offload, the NetScaler device handles the SSL encryption and decryption tasks, reducing the burden on backend servers.
    - This results in a significant reduction in server load, allowing backend servers to focus on processing application logic and data rather than SSL-related tasks.
  - Implementing SSL Offload:
    - Certificate Acquisition:
      - Obtain a public certificate from a Certificate Authority (CA) for your website.
    - Decision-Making:
      - Confirm that end-to-end SSL is not required for your environment.
      - If leveraging additional features on NetScaler is not a priority, choose SSL Offload.
    - Implementation:
      - Create a new virtual server using the same IP, selecting SSL as the protocol, and applying the acquired certificate.
      - Utilize the existing backend services and custom monitoring configurations.
-

## On the Job Application

- Before implementing SSL Offload, determine the specific SSL deployment needs for your environment.
  - Perform a thorough analysis of your environment, considering factors like load balancing, to determine if SSL Offload is the most suitable solution.
  - Create a new virtual server, maintaining the same IP, and configure it with SSL as the protocol, applying the acquired certificate.
  - Utilize existing back-end services and custom monitoring configurations for a seamless transition to SSL Offload.
-



**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# Leveraging NetScaler Policy Engine to Control Traffic

Student Guide

NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on Leveraging NetScaler Policy Engine to Control Traffic, was designed to:

- Capture essential job-related information, including On the Job Application.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Content and click on the question of interest.

# Table of Content

## Skills covered in this course:

[What is the main purpose of the NetScaler Policy Engine?](#)

[What tool is available for converting classic policies in older NetScaler versions to the latest version?](#)

[What is one of the built-in actions available for Rewrite?](#)

[Which built-in action allows NetScaler to forward messages without actually rewriting the traffic?](#)

[What is the purpose of the "state update" option on Content Switching Virtual Servers in NetScaler?](#)

[An administrator is configuring a Content Switching virtual server and policies on a NetScaler appliance. However, they encounter an issue where traffic is not matching any of the defined policies, resulting in HTTP 503 errors for unmatched requests. What would you do to correct this situation and ensure proper Content Switching for these requests?](#)

[An Administrator needs to set up policies for controlling and manipulating traffic on a NetScaler appliance. However, they are unsure about whether to use the Rewrite feature or the Responder feature for specific tasks. Given this problem, what is the solution?](#)

[An Administrator needs to configure Content Switching for a web application. The web application consists of dynamic content like web scripts and static content like JPEG files. They want to ensure that one load balancing virtual servers handles the web scripts, while another handles the static images. Which of the following components are necessary for this Content Switching configuration?](#)

[A NetScaler administrator is in the process of deploying an application utilizing Content Switching. During testing, the administrator consistently notices that the Content Switching VIP status remains UP, irrespective of the status of the associated Load Balancing VIP. What actions can the administrator take to modify this behavior?](#)

[What would you do to improve the performance and efficiency of the Content Switching](#)



Virtual Server when dealing with international traffic?

Given the differences between the Rewrite and Responder features in NetScaler, what action would you take if you wanted to modify the URL on the Response phase of an HTTP transaction?

In a NetScaler environment, you have identified a scenario where incoming requests to a specific web application need to be redirected to an alternative URL. How would you configure NetScaler policies to redirect the traffic effectively?

# Clip: Introducing NetScaler Policy Engine

---

## Scenario/Challenge

What is the main purpose of the NetScaler Policy Engine?

---

Understanding the NetScaler Policy Engine empowers administrators to effectively control and optimize network traffic. Whether enforcing simple access rules or implementing complex routing decisions, this tool plays a pivotal role in shaping the behavior of the network.

## Understanding the NetScaler Policy Engine

This section delves into understanding the NetScaler Policy Engine.

### Role and Features

- The NetScaler Policy Engine serves as the central hub for creating and enforcing network policies.
  - Its primary purpose is to control and manage the flow of information, enabling administrators to dictate how traffic is handled and routed within their network.
  - Explore features such as Content Switching, Rewrite, and Responder, highlighting their significance in optimizing network traffic.
- Policy Creation:
  - Simple rules control access to specific resources.
  - Complex expressions dictating traffic handling and routing.
  - Create policies by specifying the policy expression and desired actions.
- Policy Application:
  - Easily apply created policies to specific Virtual Servers or globally at the NetScaler level.
  - Binding policies to selected objects or groups for efficient enforcement.
  - As traffic enters NetScaler, the Policy Engine evaluates if the specified conditions are met.
- Real-world Examples:
  - Blocking all traffic to specific ports.
  - Redirecting traffic to a different server based on content type.

---

## On the Job Application

- Clearly define policies with specific conditions and actions to ensure effective network governance.
- Explore advanced features like Content Switching, Rewrite, and Responder for enhanced traffic management.
- Regularly evaluate the effectiveness of policies and adjust them as network requirements evolve.
- Opt for Advanced policies to maximize effectiveness and ensure comprehensive support.

# Clip: Introducing NetScaler Policy Engine

---

## Scenario/Challenge

What tool is available for converting classic policies in older NetScaler versions to the latest version?

---

NetScaler, a powerful application delivery controller, has evolved over time, transitioning from Classic policies to Advanced policies. From the NetScaler version 13.1, Classic policies have been deprecated. To assist admins of older NetScaler versions in converting Classic policies to the latest version, the NetScaler Policy Engine provides a useful tool called NSPEPI.

## Converting Classic Policies

This section provides guidance on classic policies.

### Understanding Classic Policies

- Classic policies, present in older NetScaler versions, evaluate basic characteristics of traffic.
  - Use simplistic policy expressions.

### Understanding Advanced Policies

- Utilize expressions with a more detailed syntax.
  - Enable a deeper examination of HTTP headers or bodies for thorough traffic analysis.
  - With the introduction of Advanced policies, admins gain the ability to use more detailed syntax for evaluating HTTP headers or bodies, allowing for a more thorough analysis of incoming traffic.

### The NSPEPI Tool

- The NetScaler Policy Engine provides the NetScaler Policy Engine Programming Interface (NSPEPI) tool for users seeking to convert Classic policies to the latest version. This tool serves as a bridge between older NetScaler versions and the NetScaler 13.1+ release. By utilizing NSPEPI, admins can seamlessly transition their policies to the updated framework.
    - NSPEPI includes a pre-configuration check tool to validate if any Classic policies are still in use before updating. This ensures a smooth transition without disrupting existing configurations.
      - You can convert either a single policy expression or the entire ns.conf file.
-

## On the Job Application

- NSPEPI facilitates a smooth transition from Classic to Advanced policies, ensuring compatibility with the latest NetScaler version. Following best practices minimizes the risk of disruptions.
- You have the option to utilize the `check_invalid_config` tool to examine whether any feature configuration still employs invalid, removed, or deprecated functionality.
- You can run the NSPEPI tool only on NetScaler version 12.1, 13.0, and later versions.
- A reboot of the NetScaler instance is necessary after successfully converting the `ns.conf` file, and this should be done without saving the configuration changes.

# Clip: Introduction to Rewrite

---

## Scenario/Challenge

What is one of the built-in actions available for Rewrite?

---

In the realm of NetScaler, the Rewrite feature plays a crucial role in tasks such as altering request destinations, modifying URL formats, or managing HTTP headers. As part of configuring Rewrite actions, there are built-in actions that simplify common tasks.

## Understanding Built-In Actions for Rewrite in NetScaler

This section focuses on understanding the built-in actions for rewrite in NetScaler.

### Built-In Actions:

- When working with Rewrite, it is essential to understand the purpose of built-in actions, as they provide predefined functionalities for specific scenarios. Here are some key details about the built-in actions:
  - NoRewrite: Forwards the message without any alteration, essentially letting the traffic pass through without rewriting.
  - Reset: Aborts connections at the TCP level. This is particularly useful for scenarios where a connection needs to be forcefully terminated.
  - Drop: Messages on either side of the communication are dropped. The "Drop" action is employed when you want to discard messages in transit.

### Configuration and Binding:

#### Rewrite Policy

- Action Creation: After enabling Rewrite, actions need to be configured. You can either create custom actions or utilize built-in actions like "Drop."
  - Binding to Policies: Once an action is created, it needs to be bound to a policy. Policies define the conditions under which the action will be applied.
  - Policy Binding to Objects: Policies, with their associated actions, must be bound to specific objects like Virtual Servers or applied globally.
-



## On the Job Application

- While it is necessary to bind actions to policies, exercise caution in binding Rewrite globally. Opt for selective binding to specific objects to avoid potential loss of control over traffic.
- As a best practice, be mindful of the CPU impact when binding a policy.
- Periodically review and update your Rewrite configurations to ensure they align with changing network requirements.

# Clip: Introduction to Rewrite

---

## Scenario/Challenge

Which built-in action allows NetScaler to forward messages without actually rewriting the traffic?

---

In the realm of NetScaler, the Rewrite feature plays a crucial role in tasks such as altering request destinations, modifying URL formats, or managing HTTP headers. As part of configuring Rewrite actions, there are built-in actions that simplify common tasks.

## Understanding Built-In Actions for Rewrite in NetScaler

This section aims to facilitate the user's understanding of the built-in actions for rewrite in NetScaler.

### Built-In Actions:

- When working with Rewrite, it is essential to understand the purpose of built-in actions, as they provide predefined functionalities for specific scenarios. Here are some key details about the built-in actions:
  - NoRewrite: Forwards the message without any alteration, essentially letting the traffic pass through without rewriting.
  - Reset: Aborts connections at the TCP level. This is particularly useful for scenarios where a connection needs to be forcefully terminated.
  - Drop: Messages on either side of the communication are dropped. The "Drop" action is employed when you want to discard messages in transit.

### Configuration and Binding:

#### Rewrite Policy

- Action Creation: After enabling Rewrite, actions need to be configured. You can either create custom actions or utilize built-in actions like "Drop."
  - Binding to Policies: Once an action is created, it needs to be bound to a policy. Policies define the conditions under which the action will be applied.
  - Policy Binding to Objects: Policies, with their associated actions, must be bound to specific objects like Virtual Servers or applied globally.
-

## On the Job Application

- While it is necessary to bind actions to policies, exercise caution in binding Rewrite globally. Opt for selective binding to specific objects to avoid potential loss of control over traffic.
- As a best practice, be mindful of the CPU impact when binding a policy.
- Periodically review and update your Rewrite configurations to ensure they align with changing network requirements.

# Clip: Content Switching Process

---

## Scenario/Challenge

What is the purpose of the "State Update" option on Content Switching Virtual Servers in NetScaler?

---

Understanding the "State Update" option empowers administrators to manage the state of Content Switching Virtual Servers dynamically. This feature enhances flexibility and responsiveness in directing traffic based on the real-time status of associated Load Balancing Virtual Servers.

## Understanding the "State Update" Option on Content Switching Virtual Server

This section is dedicated to understanding the 'State Update' option.

### Purpose of "State Update"

- The "State Update" option serves a specific purpose related to the state of the Content Switching Virtual Server:
  - Change the state of the Content Switching Virtual Server based on target Load Balancing Virtual Servers (LB Vservers).

### Understanding "State Update" Option

#### Default State of CS Virtual Server

- By default, the Content Switching Virtual Server does not require a bound LB Vserver for its status to be UP. Even with no LB Vservers bound, its default state is UP.
  - If there is a need for the Content Switching Virtual Server to dynamically change its state based on the status of associated LB Vservers, the "State Update" option is utilized.
- Initial Status and Binding:
  - Upon the addition of a new Content Switching Virtual Server, its status is initially shown as DOWN.
  - When binding a Load Balancing Virtual Server with a UP status, the status of the Content Switching Virtual Server becomes UP.
- Handling Multiple LB Vservers:
  - If multiple LB Vservers are bound, and one is specified as the default, the status of the Content Switching Virtual Server mirrors the status of the default LB Vserver.

- If no default is specified and multiple LB Vservers are bound, the Content Switching Virtual Server's status is UP only if all the bound LB Vservers are UP.
  - Configuration Location:
    - The "State Update" option can be configured under the Traffic Settings specific to the Content Switching Virtual Server.
- 

## On the Job Application

- Enable "State Update" selectively based on the specific requirements of your network configuration.
- If using multiple LB Vservers, consider specifying a default LB Vserver to determine the Content Switching Virtual Server's status.
- Periodically review and adjust the "State Update" configuration to align with changes in LB Vserver statuses.

# Clip: Content Switching Process

---

## Scenario/Challenge

An administrator is configuring a Content Switching virtual server and policies on a NetScaler appliance. However, they encounter an issue where traffic is not matching any of the defined policies, resulting in HTTP 503 errors for unmatched requests. What would you do to correct this situation and ensure proper Content Switching for these requests?

---

Understanding the priority of policies and implementing a default virtual server for unmatched traffic are key elements in achieving a well-functioning Content Switching setup.

## Resolving Content Switching Virtual Server Issues

This section guides users on resolving issues related to Content Switching Virtual Server.

### Issue Resolution Steps

- **Policy Evaluation Order:** Understand that when a request reaches the Content Switching virtual server, policies associated with that virtual server are applied based on their priority. The policy priority defines the order in which policies are evaluated.
- **Priority Assignment:** If you have assigned priorities to your policies, they are evaluated in the specified order. If not, policies are evaluated in the order they were created.
- **Default Virtual Server Binding:** Bind a default virtual server for all traffic not matched by the previous policy expressions and actions. This ensures that unmatched requests have a designated destination.
- **Default Virtual Server Status:** Ensure that the configured default virtual server is in a UP state. If the default virtual server is DOWN or not configured, it results in an HTTP 503 Not Found error for unmatched requests.
- **Error Handling:** Understand that an HTTP 503 error is sent to the client by the default virtual server when there is no match for the incoming request.

### Additional Considerations

#### Content Switching Scope

- Content Switching can be deployed for various types of connections, including HTTP, HTTPS, TCP, and UDP.
  - Ensure that SSL Offload is enabled if handling HTTPS or SSL connections.



- Dependency on Load Balancing Virtual Servers:
    - Note that Content Switching Virtual Server policies require existing Load Balancing Virtual Servers that are up and running to point to as the action on the matching expression.
- 

## On the Job Application

- It is a best practice to set up the Load Balancing Deployment and validate its proper functioning before introducing Content Switching. This ensures a stable foundation for Content Switching configurations.
- Validate that each policy accurately matches the intended criteria and directs traffic as expected.
- Maintain comprehensive documentation of the Content Switching configuration, including policies, priorities, and virtual server bindings. Ensure that knowledge about the setup is shared among team members for efficient troubleshooting and management.

# Clip: Comparing Rewrite vs Responder

---

## Scenario/Challenge

An administrator needs to set up policies for controlling and manipulating traffic on a NetScaler appliance. However, the administrator is unsure about whether to use the Rewrite feature or the Responder feature for specific tasks. Given this problem, what is the solution?

---

When configuring policies to control and manipulate traffic on a NetScaler appliance, administrators may face a common dilemma: whether to use the Rewrite feature or the Responder feature for specific tasks. To resolve this uncertainty, understanding the key differences and best practices for each feature is crucial.

## Choosing Between Rewrite and Responder Features on NetScaler

This section assists users in making informed decisions when choosing between the Rewrite and Responder features on NetScaler.

### Differentiating Rewrite and Responder

- The primary distinction between the Rewrite and Responder features lies in their capabilities and use cases.
  - Responder cannot be used for response or server-based expressions.
  - Responder is specifically designed for scenarios such as redirecting an HTTP request, responding with a custom message, or dropping/resetting a connection at the request level based on client parameters.
- Rewrite, on the other hand, is recommended for manipulating data on both HTTP requests and responses.
  - It allows the NetScaler to examine requests from clients or responses from servers, take actions based on applicable policies, and forward the traffic accordingly.

### Use Rewrite for Data Manipulation

#### HTTP Requests

- For tasks involving the manipulation of data on HTTP requests and responses, the recommended approach is to use the Rewrite feature.
  - Rewrite provides a more versatile and comprehensive set of actions for modifying content and structure.
- Identify Task Requirements:

- Clearly define the requirements of the task at hand. Determine whether the goal is to reset or drop connections based on client parameters, redirect traffic, respond with custom messages, or manipulate data on HTTP requests and responses.

---

## On the Job Application

- The best practice is to use Responder when the intention is to reset or drop a connection based on client or request-based parameters.
- Responder is ideal for tasks like redirecting traffic or responding with custom messages.
- Utilize the Expression Evaluator to test and verify that your expression functions correctly and meets your specified criteria before applying it.

# Clip: Introduction to Content Switching

---

## Scenario/Challenge

An administrator needs to configure Content Switching for a web application. The web application consists of dynamic content like web scripts and static content like JPEG files. The administrator wants to ensure that one load balancing Virtual Servers handles the web scripts, while another handles the static images. Which of the following components are necessary for this Content Switching configuration?

---

When tasked with configuring Content Switching for a web application, administrators aim to efficiently direct traffic to specific servers based on the content of incoming requests. This section will outline the necessary components for this Content Switching configuration.

## Configuring Content Switching for Web Applications on NetScaler

This section provides a comprehensive guide to configuring Content Switching for web applications on NetScaler.

### Necessary Components

- Content Switching Virtual Server: The Content Switching Virtual Server serves as the central component for directing traffic. It acts as a decision point, analyzing incoming requests and determining the appropriate course of action.
- Load Balancing Virtual Servers: Multiple Load Balancing Virtual Servers are required to handle different types of content, such as web scripts and static images. Each Load Balancing Virtual Server is responsible for serving a specific category of content.
- Content Switching Policies: Content Switching is achieved through the configuration of policies. These policies define the criteria based on which traffic is directed. Criteria can include requested web pages, URL suffixes, client attributes, or any other relevant factors.

### Implementation Steps:

#### Configuration

- Define Virtual Servers: Create the necessary Load Balancing Virtual Servers to handle the different types of content in the web application. For example, set up one virtual server for web scripts and another for static images.
- Configure Content Switching Virtual Server: Set up the Content Switching Virtual Server, specifying the criteria or conditions that will be used to direct traffic. This could be based on the requested web pages, URL suffixes, or client attributes.

- **Create Content Switching Policies:** Develop Content Switching policies that align with the criteria defined for directing traffic.
  - **Associate Policies with Virtual Servers:** Associate the created Content Switching policies with the Content Switching Virtual Server. This ensures that the configured criteria are applied to incoming requests, allowing the Content Switching Virtual Server to make informed decisions.
- 

## On the Job Application

- Develop Content Switching policies with exact expressions to guarantee precise matching of traffic.
- Prioritized policies are evaluated in the specified order, providing more control over traffic redirection.
- Conduct load testing to assess the scalability of your Content Switching setup.

## Clip: Content Switching Process

---

### Scenario/Challenge

A NetScaler administrator is in the process of deploying an application utilizing Content Switching. During testing, the administrator consistently notices that the Content Switching VIP status remains UP, irrespective of the status of the associated Load Balancing VIP. What actions can the administrator take to modify this behavior?

---

Understanding and utilizing the "State Update" parameter is crucial for NetScaler administrators dealing with Content Switching. By modifying this parameter, administrators can ensure that the Content Switching VIP status accurately reflects the health of associated load balancing virtual servers, providing a more reliable and responsive application deployment.

### Modifying Content Switching VIP Status Behavior

This section explores the modification of Content Switching VIP (Virtual IP) status behavior.

#### Default UP Status

- The Content Switching Virtual Server (CS vServer) defaults to an UP status, even without an associated Load Balancing Virtual Server (LB vServer). This means that, by default, the CS vServer remains UP.
    - If an administrator desires the Content Switching VIP status to reflect the state of the associated LB vServers, the "State Update" option becomes crucial.
  - Enabling State Update:
    - Initially, when a new CS vServer is added, its status is DOWN. Binding an LB vServer with a UP status results in the CS vServer status changing to UP.
    - The status of the CS vServer reflects the state of the default LB vServer if specified. If multiple LB vServers are bound without specifying a default, the CS vServer's status is UP only if all bound LB vServers are UP.
- 

### On the Job Application

- Consider specifying a default LB vServer if applicable.
- Be mindful of the impact on status when multiple LB vServers are involved.
- Testing the configuration in a staging environment before deployment is a recommended practice.



# Clip: Introduction to Content Switching

---

## Scenario/Challenge

What would you do to improve the performance and efficiency of the Content Switching Virtual Server when dealing with international traffic?

---

When dealing with international traffic on a Content Switching Virtual Server, administrators may encounter challenges related to language attributes and overall traffic management. This guide outlines effective strategies to improve the performance and efficiency of the Content Switching Virtual Server in such scenarios.

## Enhancing Content Switching Virtual Server Performance

This section focuses on enhancing the performance of Content Switching Virtual Server.

### Leverage Language Attributes

- Create policies based on client language attributes. For instance, examine the Accept-Language HTTP header in the client request to determine the language preference of the user's browser.
  - Use the identified language to route requests to servers that serve content in the corresponding language. This ensures a personalized user experience based on language preferences.
- Implement Content Switching Protections:
  - If the Content Switching Virtual Server is handling a substantial volume of traffic, consider implementing Content Switching Protections. This can include Backup Content Switching Virtual Servers or Content Switch Spillover to manage and protect incoming requests effectively.
  - Utilize advanced content switching options such as pattern matching and regular expressions. These features offer more granular control over traffic management, allowing organizations to optimize application performance and allocate resources based on specific criteria.

### Implementation Steps:

1. Define Language-Based Policies:
  - Create Content Switching policies that focus on language attributes. This involves specifying criteria based on the Accept-Language header in client requests.
2. Configure Routing to Language-Specific Servers: Set up routing mechanisms that direct traffic to servers serving content in the identified language. This creates a targeted and language-specific user experience.
3. Implement Content Switching Protections:

- Depending on traffic volume, configure Content Switching Protections like Backup Virtual Servers or Spillover to efficiently manage incoming requests and prevent overload.
- 

## On the Job Application

- Steer clear of excessively general expressions that could inadvertently direct traffic.
- Implement resilient load balancing configurations for Load Balancing Virtual Servers to ensure high availability and fault tolerance. This minimizes the risk of service disruptions.
- Implementing logging and monitoring proactively identifies traffic patterns, policy hits, and potential issues, enabling timely interventions.

## Clip: Planning NetScaler URL Transformation

---

### Scenario/Challenge

Given the differences between the Rewrite and Responder features in NetScaler, what action would you take if you wanted to modify the URL on the Response phase of an HTTP transaction?

---

Understanding how to modify URLs during the Response phase of an HTTP transaction is crucial when working with NetScaler. In this guide, we will explore the specific features and actions needed to achieve this task.

### Modifying URLs in NetScaler

This section provides guidance on modifying URLs in NetScaler.

#### URL Transformation Feature

- Given the differences between the Rewrite and Responder features in NetScaler, if you aim to modify the URL during the Response phase of an HTTP transaction, the recommended action is to utilize the URL Transformation feature.
  - URL Transformation is an advanced feature designed explicitly for modifying URLs during both the Request and Response phases of an HTTP transaction.
  - URL Transformation is similar to Rewrite but is more efficient, especially for large transactions. It is important to note that URL Transformation requires the Rewrite feature to be enabled, and a NetScaler standard license is also necessary.

#### Implementation Steps

1. Client Request: A client initiates a request to an external web site address, which is resolvable to a virtual server hosted on the NetScaler.
  2. Policy Evaluation and URL Transformation: The NetScaler checks for a policy match and evaluates the expression by transforming the URL during the Response phase.
  3. Request to Backend Web Server: The transformed URL is then sent to the backend web server, which processes the request based on the modified URL.
  4. Response from Backend Web Server: The backend web server sends the Response back to the NetScaler.
  5. Policy Evaluation and URL Transformation (Reverse): The NetScaler, during the Response phase, checks for a policy match and evaluates the expression by transforming the URL back to its original form.
  6. Response to Client: The NetScaler sends the response back to the client with the original URL, completing the modification cycle.
-

## On the Job Application

- URL Transformation rewrites URLs specifically in the HTML response body. It is not applied to JavaScript and other variables.
- If URL Transformation is expected to handle large transactions, perform load testing to assess the scalability and performance impact.
- If URL Transformation is applied to HTTPS traffic, manage SSL certificates efficiently.

# Clip: Introducing to Responder

---

## Scenario/Challenge

In a NetScaler environment, you have identified a scenario where incoming requests to a specific web application need to be redirected to an alternative URL. How would you configure NetScaler policies to redirect the traffic effectively?

---

In a NetScaler environment, redirecting incoming requests to a specific web application to an alternative URL can be efficiently accomplished using the AppExpert feature. This section provides step-by-step instructions on configuring NetScaler policies to redirect traffic effectively.

## Redirecting Traffic with NetScaler

This section delves into the strategies and configurations for redirecting traffic with NetScaler.

### Understanding NetScaler Responder

- NetScaler's Responder feature offers a powerful tool for intercepting incoming traffic and responding with pre-configured actions.
  - These actions can include redirecting traffic to a different URL, presenting custom error pages, or denying access to specific resources. Responder supports various protocols, including TCP, DNS (UDP), and HTTP.

### Benefits of Using Responder

- Simplicity and Efficiency:
  - Responder is a straightforward and efficient feature. Its simplicity reduces CPU cycles and processing time, making it ideal for tasks that do not require complex processing.
  - Create Responder policies based on criteria relevant to the redirection scenario. This may include specific URLs, source information, or other criteria based on your requirements.

### Configure Actions

- After enabling Responder, configure one or more actions unless using a built-in action. Built-in actions include:
  - Respond with: Forwards the message without rewriting the traffic.
  - Respond with HTML page: Aborts connections at the TCP level.
  - Redirect: Drops messages on either side of the communication.

- Choose the "Redirect" Action:
    - Specifically, for redirecting traffic, choose the "Redirect" action. This action is designed for scenarios where incoming requests need to be redirected to an alternative URL.
    - Define the alternative URL to which the traffic should be redirected. Ensure the URL is accurate and aligns with the redirection requirements for the web application.
- 

## On the Job Application

- Before implementing Responder policies in a production environment, conduct thorough testing in a staging environment.
- Clearly define the conditions under which traffic should be redirected.
- Ensure that redirection does not compromise security and consider potential security implications based on the redirection criteria.





**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# Managing NetScaler

## Student Guide

NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on Managing NetScaler, was designed to:

- Capture essential job-related information, including On the Job Application.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Content and click on the question of interest.

# Table of Content

## Skills covered in this course:

What is a platform that operates as a virtual appliance on a hypervisor or in a cloud environment?

Which tool automates the notification process for software or hardware failures?

What term describes the process when configuration changes made on the primary are synchronized to the secondary?

Which NetScaler platform is ideal for supporting multiple virtual NetScaler instances, allowing for complete isolation and independence?

Which statement accurately describes NetScaler backups?

What tool is used for capturing network traffic on a NetScaler and saving trace files in the native NetScaler format with a .cap extension for use with network analyzers?

What is the primary purpose of performing a forced failover in a NetScaler High-Availability configuration?

In the context of attempting to failover from the primary to the secondary node, how can an Administrator resolve the following error message? Error: Cannot failover as Node State set to STAYPRIMARY

An Administrator is concerned about the management of expiring SSL certificates on the NetScaler and wants to implement a proactive solution to ensure that certificate renewals are handled efficiently. What would you do to address this situation?

You are an administrator responsible for maintaining a NetScaler deployment, and you want to ensure that your system is proactively monitored and optimized for performance. You have encountered a situation where you need to address potential known issues, apply necessary updates, and receive recommendations for best

practices. What action should you take to rectify this scenario?

While setting up NetScaler High Availability, an Administrator encountered a scenario where the other node took on the primary role, leading to the loss of all NetScaler configurations. What might have caused this situation?

A company is planning to deploy a NetScaler appliance as a critical part of their network infrastructure. The network administrator is tasked with ensuring the physical and appliance security of the NetScaler. Given the scenario, which of the following measures would provide the highest level of protection against unauthorized access and potential security breaches?

Given a scenario where a NetScaler upgrade is planned, but issues are encountered during the process, what could be the most likely explanation for the following problem: "The upgrade process was initiated, but the NetScaler appliance rebooted unexpectedly and is now stuck in a continuous boot loop, making it inaccessible."

A network administrator is planning to upgrade the NetScaler device to the latest firmware version for performance improvements and security updates. They want to ensure a smooth and successful upgrade process. What should they analyze and take into consideration?

In a scenario where one of the NetScaler appliances in a high-availability configuration fails, what is the next step to ensure uninterrupted service and maintain high availability?

What term is commonly used to describe the practice of configuring failover and redundancy on a NetScaler to ensure uninterrupted operation?

# Clip: Planning NetScaler VPX Deployments

---

## Scenario/Challenge

What is a platform that operates as a virtual appliance on a hypervisor or in a cloud environment?

---

NetScaler VPX is a powerful networking platform that can be deployed as a virtual appliance in various virtualization environments and cloud platforms. This guide will help you understand NetScaler VPX and its compatibility with different virtualization platforms.

## Understanding NetScaler VPX as a Virtual Appliance

This section is dedicated to understanding NetScaler VPX as a virtual appliance.

### Key Features of NetScaler VPX

- Virtualization Platforms:
    - Citrix Hypervisor
    - VMware ESX or ESXi
    - Linux-KVM
    - Microsoft Hyper-V
  - Cloud Environments:
    - AWS (Amazon Web Services)
    - Azure (Microsoft Azure)
    - Google Cloud
  - Deployment Flexibility:
    - NetScaler VPX can be deployed on-demand, anywhere in the datacenter, providing flexibility to IT organizations, cloud service providers, and telecom service providers of any size.
    - NetScaler VPX, as a software-based virtual appliance, enables rapid on-demand provisioning in both public and private cloud infrastructures. This means that resources can be quickly allocated or de-allocated as needed.
-



## On the Job Application

- Before selecting NetScaler VPX, have a clear understanding of your application workload, traffic patterns, and performance requirements. Different workloads may have varying demands, and choosing the right VPX model is crucial.
- If you plan to extend your applications to the cloud, verify that NetScaler VPX is compatible with your chosen cloud provider.
- Assess the performance requirements of your applications. NetScaler VPX models come with different throughput and resource allocations.
- Understand the licensing models and editions available for NetScaler VPX. Choose the licensing structure that best fits your organization's requirements and be aware of any limitations or feature variations between editions.

# Clip: Introducing NetScaler System Maintenance

---

## Scenario/Challenge

Which tool automates the notification process for software or hardware failures?

---

NetScaler, like any other technology, may encounter software or hardware issues that can affect its performance. In such cases, it's crucial to identify and resolve these issues promptly to prevent potential impacts on the customer site. The "Call Home" feature in NetScaler automates the notification process, allowing for proactive issue identification and faster resolution.

## Understanding NetScaler Automated Notifications

This section focuses on understanding NetScaler automated notifications.

### Key information

- "Call Home" is a feature in NetScaler, when enabled, automates the notification process for software or hardware failures.
    - It allows Cloud Software Group (CSG) to collect data and resolve issues before they can impact the customer site.
    - The feature periodically monitors the appliance and automatically uploads data to Citrix Insight Services at [cis.citrix.com](https://cis.citrix.com).
    - "Call Home" is enabled by default on all platforms of NetScaler.
  - Benefits of "Call Home":
    - Monitor Hardware and Software Error Conditions: "Call Home" actively monitors both hardware and software error conditions, providing a comprehensive view of the NetScaler's health.
    - Notify Critical Events: The feature automatically notifies critical events that could impact your network, allowing for quick response and issue mitigation.
    - Proactive Issue Identification: By automating the notification process, "Call Home" contributes to proactive issue identification. This allows support teams to address potential problems before they escalate.
-

## On the Job Application

- Take advantage of the default setting where "Call Home" is enabled on all platforms of NetScaler. This ensures that proactive monitoring and data collection are in place from the beginning.
- Establish a routine for reviewing the notifications generated by the "Call Home" feature. Regular reviews help in identifying and addressing issues promptly.
- Unless there are specific reasons to disable it temporarily, keep "Call Home" enabled to ensure that CSG receives up-to-date information about your NetScaler deployment. This contributes to better support and troubleshooting.
- Keep your NetScaler software up to date with the latest releases and patches. This ensures that "Call Home" is optimized with the latest features, improvements, and security enhancements.

# Clip: Introducing High Availability

---

## Scenario/Challenge

What term describes the process when configuration changes made on the primary are synchronized to the secondary?

---

Understanding the term "Propagation" is crucial for NetScaler administrators implementing High Availability. Propagation ensures that any configuration changes made on the primary NetScaler are synchronized to the secondary, maintaining consistency and reliability in the HA pair. This knowledge is essential for optimizing the performance and resilience of NetScaler deployments in enterprise environments.

## NetScaler High Availability Overview

This section provides an overview of NetScaler High Availability.

### Understanding Propagation

- Definition of Propagation: Propagation refers to the process where configuration changes made on the primary NetScaler are synchronized to the secondary NetScaler.
  - Synchronization vs. Propagation:
    - Sync occurs after the secondary restarts or after the primary becomes secondary during a failover or a first afore synchronization.
    - Propagation specifically addresses changes made on the primary being applied to the secondary.
  - Common Processes in HA: Outside of failover and heartbeat processes, synchronization and propagation are crucial for maintaining consistency between primary and secondary NetScaler.
-

## On the Job Application

- Ensure that both NetScalers in the HA pair have consistent configurations to guarantee smooth failover and uninterrupted operation.
- Implement a regular monitoring schedule for health checks and heartbeats to quickly identify any issues in the primary NetScaler, triggering failover if necessary.
- After making configuration changes on the primary NetScaler, administrators should validate the synchronization process by ensuring the secondary reflects the changes through proper propagation.

# Clip: Planning NetScaler SDX Deployments

---

## Scenario/Challenge

Which NetScaler platform is ideal for supporting multiple virtual NetScaler instances, allowing for complete isolation and independence?

---

NetScaler Service Delivery Controller (SDX) is a powerful platform designed to efficiently support multiple virtual NetScaler instances, providing complete isolation and independence for each instance. This section will help you understand the unique features of NetScaler SDX and how it facilitates the deployment of multiple virtual instances on a single appliance.

## Key Features of NetScaler SDX

This section outlines the key features of NetScaler SDX.

### Complete Isolation

- NetScaler SDX offers fully isolated and independent NetScaler instances, each functioning as its own entity.
  - Isolation is achieved through virtualization technologies using Citrix XenServer and a management service called the SDX Service Virtual Machine.
- Dedicated Resources for Each Instance:
  - Each NetScaler instance on SDX has its own dedicated:
    - Kernel
    - Memory and CPU
    - Routing stack
- Scalability:
  - NetScaler SDX supports multiple virtual NetScaler instances on a single platform, providing scalability to meet various deployment needs.
- Per-Tenant Isolation:
  - SDX ensures complete per-tenant isolation, allowing for instances to be utilized for dedicated customers or shared among multiple customers.
- Version and Lifecycle Independence:



- Instances on NetScaler SDX benefit from firmware version independence and lifecycle independence, providing flexibility in managing and updating each instance.
  - Throughput and Rate Limits:
    - Administrators can impose throughput and packets-per-second rate limits on VPX instances, providing control over the network usage of each instance.
- 

## On the Job Application

- The platform's features, such as per-tenant isolation, dedicated resources, and scalability, make it an ideal choice for various deployment scenarios.
- Citrix XenServer provides the SDX per-tenant isolation.
- Utilize the dedicated resources provided for each NetScaler instance on SDX, including the dedicated kernel, memory, CPU, and routing stack. This ensures optimal performance and independence.
- Take advantage of the version and lifecycle independence offered by NetScaler SDX. This flexibility allows for the management and updating of each instance independently, accommodating diverse deployment scenarios.
- Leverage the completely isolated networks for each instance to enhance security. Ensure that instances operate independently in terms of networking to prevent interference between different instances.

# Clip: Introducing NetScaler System Maintenance

---

## Scenario/Challenge

Which statement accurately describes NetScaler backups?

---

NetScaler backups are crucial for ensuring the integrity and availability of configurations, certificates, and licenses. This guide will help you understand the backup options available for NetScaler, with a focus on the statement that accurately describes Full Backups.

## Understanding NetScaler Backups

This section is dedicated to understanding NetScaler backups.

### Key Backup Options

- High Availability:
  - When High Availability is set up, both NetScaler appliances will have copies of the configuration and important system files. This provides redundancy and ensures that critical data is available on both appliances.
- NetScaler Application Delivery Management (ADM):
  - NetScaler ADM can be leveraged to automatically back up the NetScaler's configuration, certificates, and licenses. When a NetScaler instance is added, NetScaler ADM runs backup jobs by default.
- Manual Backup using Backup and Restore Feature:
  - NetScaler provides a manual backup option accessible through the System -> Backup and Restore feature.
  - This feature allows the creation of backup files stored in the `/var/ns_sys_backup` directory, which can be copied and moved to another server using Secure Control Protocol (SCP).
- Backup and Restore Options:
  - Basic Backup:
    - Focuses on backing up configuration files only, including frequently changing files such as `/nsconfig/`, `/var/`, `/netscaler/`, and `ns.conf`.
    - Suitable for capturing configurations that change most often.

- Full Backup:
    - Captures the same data as a basic backup but includes additional files that are less frequently updated.
    - Backs up folders and files such as `/nsconfig/`, `/var/`, certificates, and license files.
    - Suitable for comprehensive backup, ensuring less frequently updated but critical data is included.
- 

## On the Job Application

- Establish a routine for performing backups, ensuring that critical data is consistently backed up to prevent data loss in the event of a failure.
- Understand the differences between Basic and Full backups. Choose the appropriate backup type based on the frequency of changes and the importance of the data being backed up.
- When using manual backup options, ensure that backup files are securely copied and moved to another server using protocols like SCP to maintain the confidentiality and integrity of the backup data.
- Regularly monitor backup jobs, especially when using automated backup solutions like NetScaler ADM. Ensure that backups are running as scheduled and review any reported issues.
- Periodically test the restoration procedures to ensure that backups can be successfully restored. This practice helps verify the integrity of backup files and the effectiveness of the restoration process.

# Clip: Taking NetScaler Logs and Trace

---

## Scenario/Challenge

What tool is used for capturing network traffic on a NetScaler and saving trace files in the native NetScaler format with a .cap extension for use with network analyzers?

---

## Capturing Network Traffic on NetScaler

This section provides an explanation on capturing network traffic on NetScaler.

### NetScaler Trace (Nstrace)

- Accessing Diagnostics in the GUI:
    - Navigate to System -> Diagnostics in the NetScaler GUI to access diagnostic tools, including network trace options.
  - Utilizing Nstrace:
    - Nstrace is the primary tool for capturing network traffic on NetScaler. It dumps packets in the native NetScaler format, and the resulting trace files have a .cap extension.
    - To initiate a network trace using Nstrace, click on the icon represented by a laptop cursor in blue. This action starts capturing packets and generating trace files.
  - Location of Trace Files:
    - Nstrace stores captured trace files in the directory `/var/nstrace` on the NetScaler appliance. These files have a .cap extension and can be used with common network analyzers like Wireshark.
  - Additional Network Trace Tools:
    - While Nstrace is the primary tool for capturing NetScaler traffic, other tools like Nstcpdump and Tcpcdump are available for low-level troubleshooting. However, Nstrace is recommended for its comprehensive information capture.
-

## On the Job Application

- Nstrace is a NetScaler packet capture tool designed to capture network traffic in the native NetScaler format.
- When capturing traces with Nstrace, it is recommended to set a filter size of 0 if possible. This helps prevent data truncation and ensures a comprehensive capture of relevant information.
- When using network analyzers like Wireshark, apply specific filters to analyze captured data effectively. Filters can also be specified using the NetScaler CLI during the capture process.
- Periodically review captured trace files to stay informed about network activity. Regular reviews can help identify patterns, anomalies, or potential issues that require attention.
- When utilizing network analyzers like Wireshark, make use of specific filters to focus on relevant data. This practice enhances the efficiency of data analysis and troubleshooting.

# Clip: Managing NetScaler High Availability Failovers

---

## Scenario/Challenge

What is the primary purpose of performing a forced failover in a NetScaler High-Availability configuration?

---

NetScaler High-Availability (HA) configuration is critical for ensuring uninterrupted service in case of a node failure. This section will help you understand the primary purpose of performing a forced failover and when it should be initiated.

## Understanding the Purpose of Forced Failover

This section delves into understanding the purpose of forced failover.

### Forced Failover for Testing HA Functionality

- **Accessing Forced Failover:** Forced failover is a deliberate action taken by administrators to test the functionality of the HA setup. It can be initiated from either the primary or the secondary node.
- **Testing HA Regularly:** Administrators should regularly test their HA functionality to ensure it works properly. Forced failover serves as a proactive measure to assess the failover process and verify that the backup node can seamlessly take over if needed.
- **Not Propagated or Synchronized:** Unlike automatic failovers triggered by system events, a forced failover is not propagated or synchronized. It is an intentional and controlled action initiated by administrators for testing purposes.
- **Viewing Synchronization Status:** After a forced failover, administrators can view the synchronization status by checking the status of the nodes. This helps assess whether the forced failover had the intended effect and whether the backup node is functioning as the new primary.
- **Circumstances of Forced Failover Failure:** Forced failover is designed to work in specific circumstances. It may fail under the following conditions:
  - Attempting a forced failover on a standalone system.
  - The secondary node is disabled.
  - The secondary node is configured to remain secondary.
  - Heartbeat failure occurs, the secondary reaches the lost heartbeat threshold, and promotes itself to primary status.



---

## On the Job Application

- Implement a regular testing schedule for High-Availability functionality using forced failover. Regular testing ensures that the failover process works as intended and allows administrators to identify and address issues proactively.
- Avoid unnecessary forced failovers to prevent disruption to normal operations.
- After performing a forced failover, assess the synchronization status by checking the status of the nodes. Ensure that the backup node has seamlessly taken over as the new primary and is functioning properly.
- Plan forced failover tests during low-traffic periods to minimize the impact on users and operations. Avoid conducting tests during peak hours to prevent potential disruptions.
- Communicate forced failover testing plans to relevant stakeholders, including IT teams and users. Ensure that all parties are aware of the testing schedule to manage expectations and avoid unnecessary concerns.

# Clip: Managing NetScaler High Availability States

---

## Scenario/Challenge

In the context of attempting to failover from the primary to the secondary node, how can an Administrator resolve the following error message? Error: Cannot failover as Node State set to STAYPRIMARY

---

In NetScaler High Availability setups, administrators may encounter errors preventing failover attempts. If you face the "Cannot failover as Node State set to STAYPRIMARY" error, this section will provide you with the steps to resolve it.

## Error in NetScaler High Availability

This section addresses errors in NetScaler High Availability.

### Resolving the Error

- Identify STAYPRIMARY Configuration:
  - The error indicates that the primary node is configured with the STAYPRIMARY command, meaning it prefers to stay in the primary state even during failover events.
- Navigate to High Availability Settings:
  - Locate and navigate to the High Availability settings within the NetScaler configuration.
    - In the High Availability Status configuration, set it to "ENABLED (Active participate in HA)."
    - This modification ensures that the primary node actively participates in failover events.
    - Save the configuration.
- Understand STAYPRIMARY Considerations:
  - Recognize that configuring a node with STAYPRIMARY keeps it in the primary state if it remains healthy, even if the peer node was initially the primary.
  - If the primary node was configured with STAYPRIMARY and experienced a failure, it will automatically fail back to the primary state when it recovers.
  - This adjustment allows the primary node to actively engage in failover events, enabling the secondary node to assume the primary state when

necessary. Understanding the impact of the STAYPRIMARY configuration is vital for effective NetScaler High Availability management.

---

## On the Job Application

- Recognize that the STAYPRIMARY command configures a node to prefer staying in the primary state during failover events, even if it initially wasn't the primary node.
- Periodically review and understand the High Availability configuration settings. Stay informed about any specific configurations, such as STAYPRIMARY, that may impact failover behavior.
- Conduct regular failover tests to ensure that the High Availability configuration functions as expected. Include scenarios where the primary node has the STAYPRIMARY configuration to validate failover and failback processes.
- Set up a regular schedule for failover testing, considering the overall network and system usage patterns. Conduct tests during periods of low traffic to minimize potential impact.

# Clip: Introducing NetScaler System Maintenance

---

## Scenario/Challenge

An Administrator is concerned about the management of expiring SSL certificates on the NetScaler and wants to implement a proactive solution to ensure that certificate renewals are handled efficiently. What would you do to address this situation?

---

SSL certificates play a crucial role in securing communication on NetScaler, and their expiration needs to be proactively managed to avoid disruptions. This section will help you understand and implement a solution to efficiently handle SSL certificate renewals.

## Proactive Management of SSL Certificate Expirations on NetScaler

This section focuses on the proactive management of SSL certificate expirations on NetScaler.

### Proactive Management of SSL Certificate Expirations

- Understanding SSL Certificate Expirations: SSL certificates have an expiration date set by the Certificate Authority. It's crucial to stay aware of certificate expirations to ensure secure and uninterrupted operations.
- Options for Proactive Management: To address administrator concerns, there are proactive options for managing expiring SSL certificates, such as:
  - Email alerts
  - SNMP traps
- Configure Email Alerts: Utilize NetScaler's capability to configure email alerts for SSL certificate expiration. Set up notifications to be sent to administrators well in advance of the expiration date.
- Configure SNMP Traps: SNMP (Simple Network Management Protocol) traps are another effective way to receive notifications. Configure NetScaler to send SNMP traps when SSL certificates are nearing expiration. SNMP traps provide real-time alerts.
- Utilize NetScaler ADM: NetScaler ADM offers Event Rules that can trigger actions based on specific events, such as SNMP traps. Configure Event Rules to send email notifications when ADM receives SNMP traps related to SSL certificate expirations.

---

## On the Job Application

- Proactively managing expiring SSL certificates on NetScaler is crucial for maintaining a secure environment.
- Regularly monitor SSL certificate expiration dates to stay ahead of potential issues. Automated alerts and traps can assist in proactive monitoring.
- Define notification thresholds for SSL certificate expirations based on your organization's policies. Ensure that alerts are triggered with enough lead time to allow for the renewal process.
- Periodically test the email alert and SNMP configurations to ensure that notifications are being sent as expected. Testing helps confirm the effectiveness of the alerting system.
- Integration with Citrix ADM further enhances central management capabilities, providing a comprehensive solution for SSL certificate lifecycle management.

# Clip: Introducing NetScaler System Maintenance

---

## Scenario/Challenge

You are an administrator responsible for maintaining a NetScaler deployment, and you want to ensure that your system is proactively monitored and optimized for performance. You have encountered a situation where you need to address potential known issues, apply necessary updates, and receive recommendations for best practices. What action should you take to rectify this scenario?

---

As a NetScaler administrator, ensuring the optimal performance of your deployment is crucial. This section will help you take proactive steps to identify and rectify potential issues, apply updates, and implement best practices for enhanced system performance.

## Proactive Monitoring and Optimization of NetScaler Deployment

This section explains proactive monitoring and optimization strategies for NetScaler deployment.

### Proactive Monitoring and Optimization Steps

- **Generate a Tech Support Bundle:** A Tech Support bundle is a comprehensive collection of logs, configurations, and system information. To generate it:
  - Log in to the NetScaler configuration interface.
  - Navigate to System > Diagnostics > Generate Tech Support.
  - Follow the prompts to create the Tech Support bundle.
- **Utilize Citrix Insight Services:** Citrix Insight Services is a platform that analyzes the Tech Support bundle for known issues, recommends updates, and provides best practices advice.
  - Access Citrix Insight Services at [cis.citrix.com](https://cis.citrix.com).
  - Upload the generated Tech Support bundle for analysis.
  - Explore the detailed report provided by Citrix Insight Services.
  - Take note of identified issues, recommended updates, and best practices advice.
- **Analyze Citrix Insight Services Report:** The report from Citrix Insight Services will:
  - Identify any known issues in your NetScaler environment.



- Suggest hot fixes, patches, and updates with prioritization (red/yellow/green).
  - Analyze your configuration and provide best practices advice.
  - Include links to relevant articles or white papers for further information.
- 

## On the Job Application

- Regularly perform this proactive monitoring process to stay ahead of potential issues.
- Consider integrating this procedure into routine system maintenance practices.
- Use the provided links in the report to access additional resources for in-depth understanding and resolution.
- By following these steps, administrators can maintain a healthy and optimized NetScaler deployment, ensuring a reliable and high-performance application delivery environment.

# Clip: Planning NetScaler High Availability

---

## Scenario/Challenge

While setting up NetScaler High Availability, an administrator encountered a scenario where the other node took on the primary role, leading to the loss of all NetScaler configurations. What might have caused this situation?

---

Setting up NetScaler High Availability is crucial for ensuring continuous and uninterrupted operation. This section will help you understand HA node states and configuration parameters, specifically addressing scenarios where the other node unexpectedly becomes the primary, resulting in the loss of configurations.

## Understanding NetScaler High Availability Node States and Configuration Parameters

This section is dedicated to understanding NetScaler High Availability node states and configuration parameters.

### Understanding HA Node States

- **UP - Node Accessible:** Indicates that the node is accessible and can function as either a primary or secondary node.
- **DISABLED - Manual Disablement:** Indicates that the high availability status of the node has been manually disabled. Synchronization and propagation cannot occur between peer nodes.
- **INIT - Node Initialization:** Indicates that the node is in the process of becoming part of the high availability configuration.
- **PARTIALFAIL - Interface Failure:** Indicates that one of the high availability monitored interfaces has failed due to a card or link failure. Triggers a failover.
- **COMPLETEFAIL - All Interfaces Unusable:** Indicates that all interfaces of the node are unusable, triggering a failover. This could be due to disconnected or manually disabled interfaces.

### HA Sync States

- **ENABLED - Normal HA Operation:** Signifies normal HA operation without constraints or preferences.
- **STAYPRIMARY - Node Preference:** Keeps the node in the primary state if it is healthy, even if the peer node was the primary initially.

- STAYSECONDARY - Forced Secondary:
    - Forces the secondary device to stay as secondary, independent of the primary device's state.
    - When configuring NetScaler High Availability, explicitly set the status of the secondary node to "STAYSECONDARY."
  - DISABLED - HA Operation Disabled: Disables the normal HA operation of the node.
  - Prevent Unexpected Role Reversals:
    - Failure to set the "STAYSECONDARY" parameter may lead to an unexpected scenario where the other node becomes the primary, and your system transitions to the secondary role.
    - If the secondary node inadvertently becomes the primary without the "STAYSECONDARY" setting, any configurations present on that node could be lost. This emphasizes the critical nature of this configuration parameter.
- 

## On the Job Application

- When configuring NetScaler High Availability, explicitly set the "STAYSECONDARY" parameter for the secondary node to prevent unexpected role changes.
- When using the graphical user interface (GUI) for HA configuration, ensure to designate the "other" unit as "stay secondary" during the setup. GUI misconfigurations can lead to unintended primary and secondary role reversals.
- Configuring "STAYSECONDARY" helps mitigate the risk of losing configurations. Without this setting, an unexpected role change could result in data loss on the secondary node.
- Prior to deployment in a live environment, perform simulation tests to validate the HA setup. Simulate failover scenarios to confirm that configurations are retained as expected.

# Clip: Planning NetScaler Physical Security

---

## Scenario/Challenge

A company is planning to deploy a NetScaler appliance as a critical part of its network infrastructure. The network administrator is tasked with ensuring the physical and appliance security of the NetScaler. Given the scenario, which of the following measures would provide the highest level of protection against unauthorized access and potential security breaches?

---

Deploying a NetScaler appliance is a critical step in ensuring secure and reliable network infrastructure. This guide provides insights into physical and appliance security best practices, emphasizing measures that offer the highest level of protection against unauthorized access and potential security breaches.

## Ensuring Physical and Appliance Security for NetScaler Deployment

This section focuses on ensuring physical and appliance security for NetScaler deployment.

### Physical and Appliance Security Best Practices

- **Secure Location Deployment:** Deploy the NetScaler appliance in a secure location with strict physical access controls. This ensures protection against unauthorized access.
  - **Access Controls:** Control access to the server room where the NetScaler is deployed. Utilize methods such as locks, electronic card readers, or other physical access control mechanisms to restrict entry.
  - **Electronic Surveillance System:** Implement an electronic surveillance system, such as Closed-Circuit Television (CCTV), to continuously monitor the server room. In case of unauthorized intrusion, the system should notify security personnel.
  - **Protection Against Power Spikes:** An uninterruptible power supply not only safeguards against power outages but also provides protection against power spikes, contributing to the longevity of the NetScaler appliance.
-

## On the Job Application

- Deploy NetScaler appliances in physically secure locations with controlled access to the server room. This is the foundational step for ensuring the overall security of the appliance.
- Regular monitoring, maintenance, and adherence to security protocols contribute to a robust and secure network environment.
- If employing CCTV, ensure that recorded footage is not only stored securely but is also readily accessible for audit purposes. Regularly reviewing the footage contributes to maintaining a vigilant security stance.
- Establish a routine for monitoring and reviewing both physical security measures and electronic surveillance data. Regular checks ensure that security protocols are consistently enforced and any anomalies are promptly addressed.
- By following these best practices, the highest level of protection against unauthorized access and potential security breaches can be achieved.



# Clip: Planning NetScaler Physical Security

---

## Scenario/Challenge

Given a scenario where a NetScaler upgrade is planned, but issues are encountered during the process, what could be the most likely explanation for the following problem: "The upgrade process was initiated, but the NetScaler appliance rebooted unexpectedly and is now stuck in a continuous boot loop, making it inaccessible."

---

Upgrading NetScaler software is a critical task to ensure the appliance's optimal performance and security. However, encountering issues, such as unexpected reboots and continuous boot loops, can disrupt the upgrade process. This section provides an understanding of common issues and troubleshooting steps.

## Understanding and Troubleshooting NetScaler Upgrade Issues

This section is dedicated to understanding and troubleshooting NetScaler upgrade issues.

### Identifying the Problem:

- **Verify Firmware Version:** Check and verify that the firmware version used for the upgrade is correct. Ensure compatibility with the NetScaler appliance model and the upgrade process.
  - **High Availability Considerations:** If the NetScaler is part of a high availability setup, ensure that both appliances are running the same NetScaler software release. Upgrade both appliances to the same version to maintain synchronization.
  - **Upgrade Procedure:** Follow the recommended upgrade procedure for NetScaler appliances. Configure the secondary node to be in a STAYSECONDARY HA state before initiating the upgrade. Upgrade the secondary node first to ensure a smooth process.
  - **Note on Code Builds:** During the upgrade process, the two nodes in a high-availability pair can run on different NetScaler code builds. However, automatic configuration sync will be disabled until both NetScalers are on the same build versions.
-



## On the Job Application

- Before initiating a NetScaler upgrade, verify that the selected firmware version is compatible with the NetScaler appliance model. Ensure compatibility to prevent unexpected reboots and issues during the upgrade.
- In a high availability setup, both NetScaler appliances must run the same software release. Maintain synchronization by upgrading both appliances to the same version to avoid compatibility issues and disruptions.
- In a high availability pair, configure the secondary node to be in a STAYSECONDARY HA state before initiating the upgrade. This helps in controlling the upgrade sequence and avoiding unexpected role changes.
- After upgrading the secondary node, validate the functionality of the upgraded version. Change the HA State back to ENABLED and force a HA failover to make the original secondary node the primary. Validate the primary node's behavior.
- Before initiating any upgrade, perform regular backups of critical configurations. This ensures that in case of unforeseen issues, configurations can be restored to a known working state.

# Clip: Upgrading NetScalers in a High Availability Pair

---

## Scenario/Challenge

A network administrator is planning to upgrade the NetScaler device to the latest firmware version for performance improvements and security updates. They want to ensure a smooth and successful upgrade process. What should they analyze and take into consideration?

---

Upgrading the NetScaler firmware is crucial for performance improvements and security updates. To guarantee a successful upgrade, administrators must carefully analyze various factors, including the physical location of the NetScaler appliance. This section outlines essential considerations for a seamless firmware upgrade.

## Essential Considerations for a Successful NetScaler Firmware Upgrade

This section explains essential considerations for a successful NetScaler firmware upgrade.

### Physical Location of the NetScaler Appliance

- **Impact of Physical Location:** The physical location of the NetScaler appliance can significantly impact the upgrade process. Consider factors such as the accessibility of the appliance, proximity to other network components, and potential environmental conditions.
- **Accessibility and Security:** Ensure that the NetScaler appliance is easily accessible during the upgrade process. Physical security measures should be in place to prevent unauthorized access and disruptions. Choose a location with controlled access to minimize the risk of interference.
- **Network Connectivity:** Assess the network connectivity of the NetScaler appliance in its current location. A stable and reliable network connection is essential for downloading firmware updates and ensuring a smooth upgrade process. Address any network issues beforehand.
- **Redundancy and High Availability:** If the NetScaler is part of a high-availability setup, analyze the redundancy mechanisms in place. Ensure that the secondary

appliance is adequately prepared for the upgrade to maintain a seamless failover in case of any issues.

- **Testing and Rollback Procedures:** Before initiating the upgrade, establish testing procedures to validate the firmware on a test environment. Additionally, have rollback procedures in place in case the upgrade encounters unexpected issues or compatibility issues with the physical setup.

---

## On the Job Application

- Analyzing the physical location of the NetScaler appliance is a critical component of ensuring a successful firmware upgrade.
- Collaborate with relevant stakeholders, including network administrators, security teams, and IT personnel. Communicate the importance of the upgrade, potential impacts, and the measures in place to ensure a smooth process.
- Document the entire upgrade plan, including considerations related to the physical location. This documentation serves as a reference for future upgrades and troubleshooting scenarios.
- After the upgrade is complete, perform post-upgrade validation to ensure that the NetScaler appliance is functioning as expected. Monitor performance, check configurations, and address any post-upgrade issues promptly.

# Clip: Managing NetScaler High Availability Failovers

---

## Scenario/Challenge

In a scenario where one of the NetScaler appliances in a high-availability configuration fails, what is the next step to ensure uninterrupted service and maintain high availability?

---

In a high-availability configuration, it's crucial to have a plan in place to handle appliance failures and maintain continuous service. This section outlines the necessary steps to take when one of the NetScaler appliances in a high-availability setup experiences a failure.

## Ensuring High Availability with NetScaler Failover

This section is dedicated to ensuring high availability with NetScaler Failover.

### Next Steps After NetScaler Appliance Failure

- **Identify the Cause of Failure:** When a NetScaler appliance in a high-availability configuration fails, the first step is to identify the root cause of the failure. Common triggers include interface failure, SSL card failure, or a lack of response to heartbeat packets on UDP Port 3003.
- **Initiate Failover to Standby Appliance:** In response to the failure, initiate a failover to the standby appliance. The secondary appliance, which is in standby mode, will be promoted to the primary role to ensure uninterrupted service. This failover mechanism is automatic and helps maintain high availability.
- **Investigate the Root Cause:** Once failover has been initiated and service is restored, investigate the root cause of the failure. Examine logs, monitor system health, and perform diagnostics to determine why the primary appliance became unavailable. Understanding the cause is essential for preventing future incidents.
- **Perform GARP on NetScaler ADC IPs:** After the failover, the new primary appliance performs a Gratuitous ARP (GARP) on all NetScaler ADC IPs. This step is crucial for updating the ARP tables across the network, ensuring that traffic is now directed to the new primary appliance.
- **Regular Testing of HA Functionality:** Regularly test the high-availability functionality to ensure proper operation. Administrators can force a failover in a controlled environment to verify that the failover process works as expected. Testing helps identify any potential issues before they impact live operations.

- Circumstances for Forced Failover: Understand that forced failover should only be conducted in controlled scenarios, such as testing high-availability functionality. Forced failover is not propagated or synchronized and should not be performed in circumstances where it could impact live operations.

---

## On the Job Application

- Ensuring high availability with NetScaler involves a proactive approach to handling appliance failures.
- By initiating failover to the standby appliance, investigating the root cause, and performing necessary actions, administrators can maintain uninterrupted service and uphold the reliability of the network infrastructure.
- Regular testing and a comprehensive understanding of failover mechanisms contribute to a robust high-availability setup.

# Clip: Introducing High Availability

---

## Scenario/Challenge

What term is commonly used to describe the practice of configuring failover and redundancy on a NetScaler to ensure uninterrupted operation?

---

Understanding High Availability on NetScaler is crucial for administrators to ensure close to 100% uptime in enterprise environments. Learners should grasp the HA configuration process, failover mechanisms, and key terms like synchronization and propagation to confidently address questions related to uninterrupted operation in a NetScaler environment.

### High Availability (HA) on NetScaler

- High Availability, commonly abbreviated as HA, refers to the practice of configuring failover and redundancy on a NetScaler to ensure uninterrupted operation in enterprise environments.
- In enterprise environments leveraging NetScaler, redundancy is not a luxury but a requirement to achieve close to 100% uptime.

### Communication and Authentication in HA

- Knowledge of Opposite System: Effective communication between NetScalers in an HA pair requires knowledge of the opposite system, including authentication details.
  - Role of RPC Nodes: Remote Procedure Calls (RPC) nodes maintain essential information for communication, such as IP addresses and authentication passwords.
  - RPC Node Passwords: Initially, all NetScalers are configured with the same RPC node password, crucial for authentication during communication.
-



## On the Job Application

- recognize the necessity of redundancy in enterprise environments leveraging NetScaler and prioritize configurations to ensure high availability.
- Configure High Availability (HA) by setting up two NetScalers in an active-passive pair, with one serving as the primary and the other as the secondary, maintaining identical configurations.
- Guarantee uniformity in configurations between the primary and secondary NetScalers, apart from their unique NSIP addresses, to facilitate smooth failover processes.
- Establish a routine for monitoring heartbeat processes, ensuring that periodic messages and health checks are consistently exchanged between HA-paired NetScalers to detect and respond to issues promptly.



**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# Optimizing NetScaler

## Student Guide

NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on Optimizing the NetScaler, was designed to:

- Capture essential job-related information, including On the Job Application.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Content and click on the question of interest.

# Table of Content

## Skills covered in this course:

[What is the primary purpose of Authentication in the NetScaler AAA system?](#)

[What is the purpose of NetScaler Application Delivery Management \(ADM\) Pooled Capacity licensing?](#)

[Which LDAP entity is responsible for intercepting incoming user traffic in the LDAP authentication setup on a NetScaler?](#)

[Which component of GSLB evaluates configured algorithms to select the best-performing service, ensuring efficient traffic distribution across multi-site data centers?](#)

[A company has recently implemented NetScaler ADC to secure access to its intranet for employees in the office and remotely. Despite the implementation, some employees report difficulty accessing the Intranet application when working from home. What steps would you take to troubleshoot the issue?](#)

[When using a Service Provider \(SP\) to host multiple applications, companies may face issues due to traditional user authentication methods. What is the advantage of SAML authentication?](#)

[Your company faces performance issues with its web applications due to high bandwidth usage and slow response times. As the IT administrator, you implement NetScaler Integrated Caching to address these challenges. While planning the implementation, you encounter a scenario where certain dynamic content needs to be cached but with specific conditions. Which components and configurations would you utilize to achieve this specific caching requirement?](#)

[Your organization is transitioning to NetScaler ADM Pooled Capacity Licensing. As the IT administrator, you need to ensure the correct setup for licensing and allocation of resources. A new NetScaler VPX instance running on Microsoft Azure needs to be added to the pooled capacity. What steps should you take to ensure proper licensing and resource allocation?](#)

A network administrator is tasked with integrating LDAP for user authentication. They want to ensure seamless authentication and group extraction using Active Directory. Which of the following actions is a necessary step for the administrator to successfully implement LDAP authentication on the NetScaler appliance?

What are the two major benefits of using NetScaler ADM Pooled Capacity as mentioned in the source?

How does the ADM Agent function within the NetScaler Application Delivery Management Pooled Capacity licensing system?

A company is planning to deploy Global Server Load Balancing (GSLB) to ensure High Availability and load balancing for its global users. Which would be most suitable if the company needs to distribute traffic across multiple active data centers for global distribution, ensuring that all sites are actively serving traffic?



# Clip: Intro to NetScaler AAA

---

## Scenario/Challenge

What is the primary purpose of Authentication in the NetScaler AAA system?

---

NetScaler ADC employs the AAA framework to enhance security and control over access to corporate resources.

## Authentication in NetScaler AAA System

This section focuses on Authentication, the first pillar of AAA, and its primary purpose in verifying client credentials and ensuring that only authorized users can access protected servers.

### What is NetScaler AAA?

- Authentication is the initial step in the AAA process. It involves verifying the client's credentials to establish their identity. This verification can occur either locally on the NetScaler or through an external authentication server. The primary goal is to ensure that users are who they claim to be.
  - The primary purpose of authentication is to ensure secure access to protected servers. By verifying user credentials, the NetScaler system acts as a gatekeeper, allowing only approved users to proceed further in the access process.
    - Consider a scenario where a company has a large workforce accessing corporate resources remotely. The company aims to establish secure access to sensitive data and applications while maintaining strict control over user authorization and maintaining robust auditing capabilities.
- Verification of Client Credentials:
  - During the authentication process, the NetScaler system checks the client's provided credentials, such as usernames and passwords. This verification ensures that only users with valid and approved credentials are granted access to protected servers.

- NetScaler offers flexibility in authentication methods. It can authenticate users locally based on credentials stored within the NetScaler system. Alternatively, it can leverage external authentication servers, enhancing scalability and centralizing user management.
  - User Authorization (Next AAA Pillar)
    - While authentication focuses on verifying identity, the next pillar in AAA, Authorization, determines what content or resources a user is allowed to access. Authentication sets the stage for subsequent authorization checks based on the user's identity.
      - Authentication is not only about permitting or denying access but also about maintaining a record of user activity. The AAA system's auditing capabilities log and track each user's actions on protected servers, contributing to comprehensive security monitoring.
- 

## On the Job Application

- Authentication is a fundamental component of the NetScaler AAA system, establishing the identity of users by verifying their credentials.
  - Authentication serves as the first line of defense in ensuring secure access to corporate resources.
  - NetScaler provides flexibility by supporting authentication either locally within the NetScaler system or through external authentication servers. Choose the method that aligns with security and scalability requirements.
  - Rigorous verification is essential to prevent unauthorized individuals from accessing sensitive corporate data remotely.
  - Periodically test the authentication system to ensure its effectiveness. Conduct security audits to identify vulnerabilities and address them promptly, enhancing the overall resilience of the authentication process.
-

# Clip: Introducing Pooled Capacity

---

## Scenario/Challenge

What is the purpose of NetScaler Application Delivery Management (ADM) Pooled Capacity licensing?

---

Imagine being responsible for managing licenses across numerous NetScaler appliances hosted in different data centers or cloud platforms. Traditionally, each NetScaler instance required its own individual license, leading to complexity in license management. NetScaler ADM Pooled Capacity licensing addresses this challenge by offering centralized license management through the ADM Service.

## Understanding NetScaler ADM Pooled Capacity Licensing

This section is dedicated to understanding NetScaler ADM Pooled Capacity Licensing.

### Key Features of Pooled Capacity Licensing

- **Flexibility:** NetScaler ADM Pooled Capacity licensing provides flexibility in allocating licenses dynamically. This ensures that the right number of licenses is available for each NetScaler instance when needed.
  - **Optimizing License Usage:** The dynamic allocation of licenses allows organizations to optimize their license usage. Licenses are utilized efficiently, and unnecessary costs associated with over-provisioning are minimized.
  - **Cost Reduction:** By efficiently managing licenses and avoiding the need for individual licenses for each NetScaler instance, organizations can achieve cost reductions. Pooled Capacity licensing enables a more cost-effective approach to license management.
  - **Centralized Management:** One of the primary advantages of NetScaler ADM Pooled Capacity licensing is centralized license management. Instead of managing licenses for individual NetScaler appliances separately, organizations can leverage ADM's centralized capabilities to manage licenses across multiple appliances simultaneously.
  - **Timesaving and Consistency:** Centralized license management not only saves time but also ensures consistency across the entire application delivery infrastructure. Changes and updates can be applied uniformly, streamlining administrative tasks.
-

## On the Job Application

- NetScaler ADM Pooled Capacity licensing provides a solution to the challenges associated with managing licenses across multiple NetScaler instances.
  - The flexibility, optimization of license usage, cost reduction, and centralized management capabilities make it a valuable feature for organizations seeking efficient license management in their application delivery infrastructure.
  - Pooled Capacity licensing enables organizations to optimize license usage, reducing unnecessary costs associated with over-provisioning.
  - Include license management in backup and disaster recovery planning. Ensure that license information is backed up regularly to avoid data loss and facilitate quick recovery in case of unforeseen events.
-

# Clip: Planning Lightweight Directory Access Protocol (LDAP)

---

## Scenario/Challenge

Which LDAP entity is responsible for intercepting incoming user traffic in the LDAP authentication setup on a NetScaler?

---

## LDAP Authentication Setup on NetScaler

This section guides users through the setup of LDAP authentication on NetScaler.

### Understanding LDAP Authentication

- LDAP (Lightweight Directory Access Protocol) authentication is a common method used by NetScaler to validate user credentials against an LDAP server. To set up LDAP authentication on NetScaler, several entities and configurations come into play. Let's break down the key components:
  - LDAP Action:
    - The LDAP action is the initial configuration step, defining the connection parameters to the LDAP server.
    - LDAP IP or FQDN, port number, Base Distinguished Name (Base DN) of the LDAP server, bind credentials, and a user login attribute (e.g., samAccountName or UserPrincipalName).
    - It establishes the connection details and attributes required for communication with the LDAP server.
  - The LDAP policy, mapped to this action, plays a crucial role in intercepting and managing incoming user traffic based on specified conditions.
    - LDAP Policy:
      - The LDAP policy is created with an expression that intercepts incoming user traffic based on specified criteria.
      - It is mapped to the LDAP action, associating the defined action with specific conditions or attributes.
      - The LDAP policy is then bound to a bind point, such as an Authentication virtual server or a global bind point, with an assigned priority number.



- Bind Points:
    - Authentication Virtual Server:
      - A specific virtual server dedicated to handling authentication requests.
    - Global Bind Point:
      - A broader configuration that can be applied globally to the NetScaler.
    - System Authentication:
      - In the case of system authentication, privileges are assigned to system users. This involves applying privileges either on a group level or individually for each user.
- 

## On the Job Application

- In the context of intercepting incoming user traffic during LDAP authentication setup on a NetScaler, the LDAP action takes center stage. It serves as the configuration entity that establishes the connection to the LDAP server and defines the attributes necessary for the user.
  - The LDAP policy, mapped to this action, plays a crucial role in intercepting and managing incoming user traffic based on specified conditions.
  - Use LDAP group extraction for efficient privilege management.
  - Regularly review and update these configurations to align with changes in LDAP settings or organizational requirements.
-



# Clip: Introducing NetScaler GSLB Entities

---

## Scenario/Challenge

Which component of GSLB evaluates configured algorithms to select the best-performing service, ensuring efficient traffic distribution across multi-site data centers?

---

In this section, we will explore the key component of GSLB (Global Server Load Balancing) that evaluates configured algorithms to select the best-performing service.

## Introduction to Global Server Load Balancing (GSLB)

This section serves as an introduction to GSLB.

### GSLB Methods in NetScaler

- GSLB is a crucial feature in NetScaler ADC, designed to intelligently distribute traffic across multiple sites or data centers for optimal performance, disaster recovery, and efficient resource utilization.
    - GSLB Sites: Represents individual data centers or locations participating in GSLB.
    - GSLB Services/Service Groups: Define the services or groups of services available at GSLB sites.
    - GSLB Virtual Servers: Provide the entry point for client requests and act as the decision-making entity.
    - ADNS Services: Advanced Domain Name System services play a role in resolving GSLB domain names to IP addresses.
  - Focus on GSLB Methods: GSLB methods are algorithms employed by the GSLB virtual server to select the best performing GSLB service.
    - NetScaler ADC offers a range of GSLB methods, each with its unique criteria for service selection.
  - Available GSLB Methods: GSLB methods are algorithms employed by the GSLB virtual server to select the best performing GSLB service.
    - NetScaler provides a variety of GSLB methods, including Round Robin, Least Response Time, Static Proximity, and others, each with distinct criteria for selecting services.
-

## On the Job Application

- Understanding GSLB methods is essential for configuring efficient traffic distribution in a multi-site environment.
  - Regularly review and adjust GSLB methods based on traffic patterns.
  - By default, the GSLB virtual server is set to the "Least Connections" method.
  - Consider the specific needs of your application when choosing GSLB methods.
  - Test GSLB configurations to ensure optimal service selection.
-

# Clip: Intro to NetScaler AAA

---

## Scenario/Challenge

A company has recently implemented NetScaler to secure access to its intranet for employees in the office and remotely. Despite the implementation, some employees report difficulty accessing the Intranet application when working from home. What steps would you take to troubleshoot the issue?

---

In a scenario where a company has recently deployed NetScaler to secure access to its intranet for both office and remote employees, troubleshooting may be necessary if some employees face difficulties accessing the intranet application from home.

## Troubleshooting Remote Access Issues with NetScaler

This section addresses troubleshooting remote access issues with NetScaler.

### Authentication Policies Check

- Verify the authentication policies configured on NetScaler.
  - Ensure that authentication policies are correctly set up for remote access.
  - Confirm that employees working remotely have the appropriate authentication credentials and are authorized to access the intranet application.
- NetScaler AAA Implementation:
  - Ensure that NetScaler AAA is implemented correctly to secure access to sensitive data and applications.
  - Verify that employees working remotely are required to provide appropriate authentication factors beyond just a username and password.
- Granular Access Control:
  - Leverage the AAA feature for granular access control, defining detailed access policies based on user roles, groups, or attributes.
  - Tailor access permissions to specific departments or teams, ensuring users have access only to resources necessary for their roles.
  - Understand how fine-grained control with NetScaler AAA helps reduce the risk of unauthorized access and data breaches.
- Secure Remote Access:
  - Emphasize the importance of secure remote access using NetScaler AAA.
  - Highlight that employees can securely access corporate resources from anywhere, using various devices, without compromising security.

---

## On the Job Application

- Authentication policies play a crucial role in securing access to applications.
  - Proper configuration of authentication policies is essential for both on-site and remote access.
  - Authentication verifies user credentials, authorization controls access, and auditing maintains detailed activity records.
  - Implementing NetScaler AAA mitigates risks associated with unauthorized access, ensuring a secure environment for corporate resources.
  - Implement multi-factor authentication to enhance the security of remote access.
  - Follow NetScaler AAA implementation guidelines for optimal results.
-

# Clip: Introducing SAML

---

## Scenario/Challenge

When using a Service Provider (SP) to host multiple applications, companies may face issues due to traditional user authentication methods. What is the advantage of SAML authentication?

---

When companies utilize a Service Provider (SP) to host multiple applications, traditional user authentication methods can lead to various challenges. One solution to address these challenges is Security Assertion Markup Language (SAML) authentication.

## Understanding the Advantages of SAML Authentication

This section explores the advantages of SAML authentication in the context of hosting multiple applications through a Service Provider.

### Understanding the Challenge

- SAML authentication emerges as a powerful solution for companies utilizing Service Providers to host multiple applications.
  - Elimination of User Database Maintenance:
    - Traditional Challenge: Service Providers usually need to maintain a separate database for the company's users.
    - The advantage of SAML: SAML eliminates the need for the Service Provider to manage a database for the company's users. This allows the Service Provider to focus on delivering better services rather than identity management.
  - Service Provider Security:
    - Ensuring the security of user data becomes a critical responsibility.
    - The company must validate users and maintain up-to-date user data, both in its database and the Service Provider's database.
    - Users are required to log in individually to each hosted application, leading to a cumbersome login process.
- Synchronization Burden Alleviation:
  - Traditional Challenge:

- Companies typically bear the responsibility of ensuring synchronization between their user database and the Service Provider's database. SAML alleviates the burden on the company by removing the need to synchronize user databases. The company can maintain its user data independently.
  - Single Sign-On (SSO) Capability:
    - Traditional Challenge:
      - Users often need to log in separately to each application hosted by the Service Provider. SAML enables Single Sign-On (SSO), allowing users to log in once to one application and gain automatic access to other hosted applications. This significantly improves the user
- 

## On the Job Application

- By eliminating the need for separate user databases, easing synchronization challenges, and enabling SSO, SAML contributes to a more streamlined and secure authentication process.
  - Understanding the advantages of SAML is crucial for companies seeking efficient and user-friendly authentication solutions in a Service Provider-hosted environment.
  - SAML enables SSO, allowing users to log in once to one application and gain automatic access to other hosted applications.
-



# Clip: Implementing NetScaler IC

---

## Scenario/Challenge

Your company faces performance issues with its web applications due to high bandwidth usage and slow response times. As the IT administrator, you implement NetScaler Integrated Caching to address these challenges. While planning the implementation, you encounter a scenario where certain dynamic content needs to be cached but with specific conditions. Which components and configurations would you utilize to achieve this specific caching requirement?

---

As an IT administrator addressing performance issues with web applications, implementing NetScaler Integrated Caching can significantly enhance your company's web application delivery by reducing bandwidth usage and improving response times. This guide will walk you through the key components involved in NetScaler Integrated Caching and how to implement caching for dynamic content with specific conditions.

## Implementing NetScaler Integrated Caching for Dynamic Content

This section provides guidance on implementing NetScaler Integrated Caching for dynamic content.

### Components Involved

- Content Groups:
  - Content Groups act as logical containers for cached content, organizing data based on criteria like URLs, file extensions, or other attributes.
  - Two types of Content Groups: Static and Dynamic.
    - Static Content Groups: Match exact URL stem and hostname in requests and responses.
    - Dynamic Content Groups: Look for objects with specific parameter-value pairs, arbitrary strings, or string patterns, suitable for frequently updated data.
- Cache Selector:
  - Cache Selector acts as a filter to locate specific objects within a Content Group.
  - Specify whether the selector identifies cache requests or objects to be invalidated.
  - Configuration of Cache Selectors is a best practice for effective caching.

- Caching Policies:
    - Each Content Group is associated with one or more Caching Policies, defining caching rules.
    - Policies determine how content is cached, allowing for granular control over caching behavior.
    - Examples include caching all '.jpg' images for 24 hours or specifying conditions for not caching certain HTML files.
    - Policies are crucial for the Integrated Cache to decide whether to serve a response from the cache or the origin.
  - Policy Bank:
    - Policies bound to a particular bind point collectively form a policy bank.
    - Binding policies to specific processing points in the request-response flow ensures effective caching based on defined rules.
- 

## On the Job Application

- Implementing NetScaler Integrated Caching with a focus on Content Groups, Cache Selectors, and Caching Policies allows for efficient caching of dynamic content under specific conditions.
- Expiration can be configured for entire content groups or selected entries.
- Create Caching Policies for each Content Group, specifying caching rules and conditions.
- Thoroughly test the caching setup to ensure dynamic content caching meets the specified conditions.
- By following these steps, you can address performance challenges and optimize web application delivery for enhanced user experience.

---

## Clip: Planning Pooled Capacity

---

### Scenario/Challenge

Your organization is transitioning to NetScaler ADM Pooled Capacity Licensing. As the IT administrator, you need to ensure the correct setup for licensing and allocation of resources. A new NetScaler VPX instance running on Microsoft Azure needs to be added to the pooled capacity. What steps should you take to ensure proper licensing and resource allocation?

---

As your organization transitions to NetScaler ADM Pooled Capacity Licensing, ensuring the correct setup for licensing and resource allocation is crucial. This section outlines the steps an IT administrator should take to transition to pooled capacity, focusing on proper licensing and resource allocation.

### NetScaler ADM Pooled Capacity

This section elaborates on NetScaler ADM Pooled Capacity.

#### Steps for Proper Licensing and Resource Allocation

- Prepare Pooled Capacity Files:
  - Acquire the necessary Pooled Capacity files, specifically the Bandwidth and Instance Pool license files.
  - Ensure these files are associated with the unique HOST ID of the ADM service.
- Match HOST IDs:
  - Verify that the HOST ID of the license files matches the HOST ID of your NetScaler ADM service.
  - Any mismatch between HOST IDs will result in license issues, so meticulous matching is essential.
- Upload License Files to ADM Service:
  - Once HOST IDs are verified and matched, upload the Bandwidth and Instance Pool license files to the NetScaler ADM service.
  - The ADM service acts as the Licensing server, managing the allocation of licenses from the pool.

- Allocate Bandwidth and Instance License:
    - Within the NetScaler ADM service, allocate the required bandwidth and an instance license from the respective license pools.
    - This step ensures that the new NetScaler VPX instance on Microsoft Azure receives the appropriate licensing.
  - Apply Licenses On-Demand:
    - The ADM service, now configured as the Licensing server, allocates licenses from the pool to NetScaler instances on-demand.
    - This dynamic allocation optimizes resource utilization and ensures efficient licensing distribution.
  - Understand Bandwidth Pool:
    - The Bandwidth pool represents the total bandwidth available for sharing among NetScaler instances, including both physical and virtual.
    - Separate pools exist for different software editions like Standard, Advanced, and Premium.
- 

## On the Job Application

- Transitioning to NetScaler ADM Pooled Capacity enhances the scalability and flexibility of the NetScaler deployment.
  - The careful matching of HOST IDs, uploading of license files, and dynamic allocation of licenses through the ADM service contribute to an efficient and optimized licensing environment.
  - Acquire the Bandwidth and Instance Pool license files for NetScaler ADM Pooled Capacity.
  - Understand the Bandwidth pool, representing the total shared bandwidth for NetScaler instances, categorized by software editions.
-

# Clip: Planning LDAP

---

## Scenario/Challenge

A network administrator is tasked with integrating LDAP for user authentication. They want to ensure seamless authentication and group extraction using Active Directory. Which of the following actions is a necessary step for the administrator to successfully implement LDAP authentication on the NetScaler appliance?

---

In a scenario where seamless authentication and group extraction from Active Directory are essential, NetScaler ADC provides a robust solution. This section outlines the necessary steps for a network administrator to successfully implement LDAP authentication on the NetScaler appliance.

## Implementing LDAP Authentication on NetScaler

This section provides comprehensive guidance on implementing LDAP authentication on NetScaler.

### Define LDAP Action

- Begin by defining an LDAP action on the NetScaler appliance.
  - Include essential parameters such as LDAP IP or FQDN, port number, Base Distinguished Name (DN) of the LDAP server, bind credentials, and a user logon attribute (e.g., samAccountName or UserPrincipalName).
- Create LDAP Policy:
  - Map the LDAP action to an LDAP policy.
  - The LDAP policy is constructed using an expression that intercepts incoming user traffic.
- Choose Bind Point:
  - Bind the LDAP policy to an appropriate bind point.
  - Common bind points include an Authentication virtual server or a global bind point.
- Assign Priority:
  - Specify a priority number when binding the LDAP policy.
  - Priority determines the sequence in which policies are evaluated, allowing precise control over policy execution.

- System Authentication Configuration:
    - If LDAP authentication is for system administration, configure privileges for system users.
    - Assign privileges based on LDAP group memberships or individual user configurations.
- 

## On the Job Application

- Define LDAP action with essential parameters.
  - Map LDAP action to LDAP policy for traffic interception.
  - Bind LDAP policy to an appropriate bind point with a specified priority.
  - Configure privileges for system users if LDAP authentication is for system administration.
  - Create local users or groups matching LDAP names for group extraction.
  - Utilize LDAP group extraction to determine and utilize user group memberships on NetScaler ADC.
-



# Clip: Introducing Pooled Capacity

---

## Scenario/Challenge

What are the two major benefits of using NetScaler ADM Pooled Capacity as mentioned in the source?

---

NetScaler ADM Pooled Capacity offers significant advantages in managing licenses for multiple NetScaler appliances.

## Benefits of NetScaler ADM Pooled Capacity

In this section, we will explore the two major benefits of using the ADM Pooled Capacity.

### Simplified Management

- **Traditional Licensing Challenges:** In traditional licensing models, each NetScaler instance requires its own individual license. Managing licenses across multiple instances can become complex and inefficient.
- **ADM Pooled Capacity Solution:** NetScaler ADM Pooled Capacity simplifies license management by providing a centralized approach. Instead of handling individual NetScaler appliances separately, ADM's centralized management capabilities allow simultaneous.
- **Time and Consistency Savings:** This centralized approach saves time and ensures consistency in managing licenses and streamlining administrative tasks for NetScaler administrators.

### Flexible Resource Allocation

- **Dynamic License Allocation:** ADM Pooled Capacity offers flexibility by allowing dynamic allocation of licenses. This ensures that the right number of licenses is available for each NetScaler instance when needed.
- **Optimized License Usage:** The flexibility provided by ADM Pooled Capacity optimizes license usage, reducing costs associated with over-provisioning. Licenses can be allocated based on demand, adapting to the changing needs of the infrastructure.

- Efficient Application Delivery Infrastructure: Organizations can efficiently manage their application delivery infrastructure, allocating and reallocating licenses as required. This adaptability enhances resource utilization and scalability.
- 

## On the Job Application

- NetScaler ADM Pooled Capacity offers simplified license management and flexible resource allocation, contributing to increased flexibility, scalability, and efficiency in NetScaler ADC deployments.
  - By decoupling software from the underlying hardware, organizations can achieve better resource utilization, reduce administrative overhead, and streamline the license renewal process, leading to cost savings and improved operational effectiveness.
  - ADM Agent: Installed on the on-premise data center, the ADM Agent acts as an intermediary between the NetScaler instances and the cloud-based license server.
  - Built-in Agent: Available on NetScaler SDX, MPX, and VPX instances, facilitating communication between NetScaler instances and ADM Service.
-

# Clip: Introducing ADM Pooled Capacity

---

## Scenario/Challenge

How does the ADM Agent function within the NetScaler ADM Pooled Capacity licensing system?

---

Understanding the role of the ADM Agent in NetScaler ADM Pooled Capacity licensing is crucial for administrators seeking efficient, centralized license management across diverse NetScaler instances, ultimately enhancing operational effectiveness and reducing costs.

## Key Concepts

- **Traditional Licensing Challenges:** In traditional licensing models, each NetScaler instance requires individual licenses, leading to complexity and inefficiency in managing licenses across multiple instances.
  - **Flexibility and Dynamic Allocation:** Pooled capacity licensing offers flexibility by allowing dynamic allocation of licenses, ensuring the right number of licenses are available for each instance when needed.
  - **Centralized Management with ADM:** Instead of managing individual NetScaler appliances separately, ADM's centralized management capabilities enable simultaneous license management across multiple appliances, saving time and ensuring consistency.
  - **Role of ADM Agent:** The ADM Agent, installed on the on-premise data center, acts as an intermediary between the NetScaler ADM service and discovered NetScaler instances. It serves as a network proxy to a cloud-based license server.
  - **Built-In Agent on NetScaler Instances:** NetScaler SDX, MPX, and VPX instances come with a built-in agent facilitating communication between instances and the ADM service. Ideal for smaller ADC standalone or HA pair deployments.
  - **Benefits of Pooled Licensing:** NetScaler ADM Pooled Licensing streamlines license management, offering organizations increased flexibility, scalability, efficiency, better resource utilization, reduced administrative overhead, simplified license renewal, cost savings, and improved operational effectiveness.
-

## On the Job Application

- Utilize the centralized management capabilities of NetScaler ADM to efficiently manage licenses across multiple NetScaler appliances simultaneously, saving time and ensuring consistency.
  - Ensure the installation of the ADM Agent on your on-premise data center to act as a vital intermediary between the NetScaler ADM service and discovered NetScaler instances.
  - Recognize that the ADM Agent functions as a network proxy to a cloud-based license server, facilitating crucial communication between the NetScaler ADM service and NetScaler instances.
-

# Clip: Planning NetScaler GSLB Deployments

---

## Scenario/Challenge

A company is planning to deploy GSLB to ensure High Availability and load balancing for its global users. Which would be most suitable if the company needs to distribute traffic across multiple active data centers for global distribution, ensuring that all sites are actively serving traffic?

---

Selecting the right GSLB deployment type depends on the company's requirements. Whether it's active-active for load balancing, active-passive for disaster recovery, or parent-child topology for scalability, GSLB offers flexibility for global traffic distribution and High Availability across multiple data centers.

## Understanding GSLB Deployment Types

This section aims to enhance understanding of GSLB deployment types.

### Choosing the Right Deployment

- Consider Active-Active for Global Traffic Distribution:
    - Choose active-active deployment when global traffic needs to be distributed across multiple active data centers.
    - Ensure all sites actively participate in serving client requests for optimal performance.
  - Opt for Active-Passive for Disaster Recovery:
    - Consider active-passive deployment when disaster recovery is a primary concern.
    - Designate an active GSLB site and one or more standby sites for failover during disaster events.
  - Explore Parent-Child Topology for Large Deployments:
    - For large deployments beyond 32 sites, explore the parent-child topology to efficiently manage traffic flow.
    - Designate parent nodes for DNS proxying and MEP traffic management, ensuring scalability without exponential traffic growth.
-

## On the Job Application

- Ensure a comprehensive understanding of GSLB deployment principles, including site identifiers, virtual servers, and GSLB services configuration.
  - Assess the company's needs and select the most suitable GSLB deployment type, with a specific emphasis on "Active-Active" for distributing traffic across multiple active data centers globally.
  - Understand the limitations of MEP synchronization, particularly the maximum of 32 GSLB sites in active-active or active-passive scenarios, and plan accordingly for larger deployments.
-





**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# Introducing Citrix and StoreFront

## Student Guide

NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on Introducing Citrix and StoreFront, was designed to:

- Capture essential job-related information, including On the Job Application.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Content and click on the question of interest.

# Table of Content

## Skills covered in this course:

What is the correct order of the four high-level phases involved in launching a Citrix resource, such as a published app or desktop?

Which Citrix technology allows administrators to have more control over network bandwidth consumption?

Which component in a Citrix Desktop as a Service (DaaS) deployment serves as the relay point of communications between customer-managed components and the infrastructure components in Citrix Cloud?

A Citrix administrator is experiencing issues in delivering published applications to users in a Citrix Virtual Apps and Desktops environment. A master image, machine catalog, and delivery group have been created, but users can't access them. Investigation reveals a configuration issue. How can the administrator troubleshoot it?

A Citrix administrator has received reports from users who are experiencing issues with authentication when attempting to access applications through StoreFront. Upon investigation, it was discovered that StoreFront is unable to authenticate users with Active Directory. What could be the possible reason for this issue?

What is the first step in the installation process of the Citrix Delivery Controller on Windows Server 2019?

During which resource launch phase are applications and desktops identified and presented to the user, based on their group memberships and assigned resources in the Citrix environment?

Which of the following best describes the role of the Delivery Controller in the Resource

## Enumeration phase?

You are an IT administrator responsible for managing Citrix Virtual Apps and Desktops within your organization. One of your tasks is to ensure that users can successfully launch their Citrix resources. You have a new user who is trying to access a published app for the first time using the Citrix system. Considering the phases of the Citrix resource launch process, identify the appropriate steps you would instruct them to follow in order to launch the published app.

Which of the following statements accurately reflects their relationship and function during the User Authentication and Resource Enumeration phases?

An IT administrator is responsible for managing Citrix Virtual Apps and Desktops deployment in a large organization. A user reports that they are unable to access their virtual desktop from their laptop, even though they have the Citrix Workspace app installed. What approach would you use to troubleshoot and resolve the user's inability to access their virtual desktop?

# Clip: Understanding Internal Apps and Desktops Launch Process

---

## Scenario/Challenge

What is the correct order of the four high-level phases involved in launching a Citrix resource, such as a published app or desktop?

---

This section was designed to help you understand the correct order of the four high-level phases involved in launching a Citrix resource, such as a published app or desktop.

## Understanding the Launch Phases of Citrix Resources

This section delves into understanding the launch phases of Citrix resources.

### Introduction to Citrix Resource Launch

- Launching a Citrix resource involves a structured process comprising four distinct high-level phases. These phases collectively ensure a seamless user experience. Let's explore the correct order of these phases.
  - The correct order of the four high-level phases is as follows:
    1. User Authentication: This phase involves verifying the user's identity, ensuring secure access to Citrix resources.
    2. Resource Enumeration: After authentication, the system enumerates available resources, identifying the published apps or desktops accessible to the authenticated user.
    3. Resource Launch: Once the resources are identified, the launch phase is initiated, allowing the user to access the intended published app or desktop.
    4. Session Initialization: The final phase involves setting up the user session, configuring the environment for optimal use, and ensuring a smooth start to the Citrix resource session.
  - Shared Phases Across Deployments
    - It is important to note that Citrix Virtual Apps and Desktops, as well as Citrix DaaS deployments, share the same high-level session launch



phases. This standardization simplifies the understanding of the launch process.

- While each of the four phases involves several smaller steps, encompassing tickets, tokens, checks, and validations, our focus will be on the major steps within each phase for a clearer understanding.

---

## On the Job Application

- By familiarizing yourself with the correct order of the four high-level phases - User Authentication, Resource Enumeration, Resource Launch, and Session Initialization - you gain insight into the structured process that ensures secure and efficient Citrix resource launch.
  - Remember, within each of these phases, numerous intricacies contribute to a secure and seamless user experience.
  - Both Citrix Virtual Apps and Desktops, as well as Citrix DaaS deployments, follow the same high-level session launch phases, promoting standardization.
  - Emphasize robust user authentication to ensure secure access to Citrix resources.
-

# Clip: The evolution of Citrix and Remote Computing

---

## Scenario/Challenge

Which Citrix technology allows administrators to have more control over network bandwidth consumption?

---

In this section, we will delve into the Citrix technology to understand the Independent Computing Architecture protocol (ICA) and its role in optimizing user experiences, drawing insights from the provided source.

## Understanding Citrix Technology and Network Bandwidth Control

This section delves into understanding Citrix technology and network bandwidth control.

### Introduction to Citrix Technology

- Citrix offers a solution that goes beyond the limitations of the Remote Desktop Protocol (RDP) through the development of the Independent Computing Architecture protocol (ICA). This advancement provides administrators with enhanced control over network bandwidth consumption.
  - Citrix Components Overview:
    - Citrix Workspace App (CWA): Installed on client machines, CWA is a specialized software optimizing the user experience, managing outbound connections to the server.
    - Virtual Delivery Agent (VDA): Installed on the remote server, the VDA manages user connections and facilitates access to the full desktop or specific published applications.
  - ICA Protocol: Enabling Control
    - The ICA protocol is the key to Citrix's network bandwidth control. Unlike traditional protocols like RDP, ICA empowers administrators by allowing them to regulate how much network bandwidth is consumed by remote users.

- Citrix's vision extends beyond conventional device connections. The ICA protocol enables any device, irrespective of the OS platform, to connect to any business application. This means users can remotely access resources seamlessly, even across different types of client devices.
  - Real-World Examples:
    - Consider scenarios where a Linux-based computer in a local office launches a Windows desktop remotely or an Android phone runs Microsoft Word while the user is in the cafeteria. This exemplifies the flexibility and reach achieved through the ICA protocol.
- 

## On the Job Application

- ICA is the Citrix protocol that grants administrators enhanced control over network bandwidth consumption.
  - Prioritize the use of the ICA protocol to benefit from enhanced control over network bandwidth consumption and optimize user experiences.
  - Citrix Workspace App (CWA) on client machines and Virtual Delivery Agent (VDA) on remote servers are crucial components enabling the efficient functioning of Citrix technology.
  - Leverage the capabilities of CWA to customize and optimize user experiences, tailoring them to specific organizational needs and preferences.
  - Regularly monitor network bandwidth usage and performance to identify potential issues and optimize network resources accordingly.
-

# Clip: Introducing Citrix DaaS

---

## Scenario/Challenge

Which component in a Citrix Desktop as a Service (DaaS) deployment serves as the relay point of communications between customer-managed components and the infrastructure components in Citrix Cloud?

---

In Citrix Desktop as a Service (DaaS) deployments, the Citrix Cloud Connector plays a pivotal role as the relay point for communications between customer-managed components and infrastructure components in Citrix Cloud.

## Understanding Citrix Desktop as a Service (DaaS) Components

In this section, we will understand the key components of the Citrix Cloud connector.

### Introduction to Citrix DaaS

- Citrix Desktop as a Service (DaaS) is a solution that facilitates the delivery of virtual desktops and applications from the cloud. In a DaaS deployment, various components work together to ensure seamless communication and functionality.
  - The component central to relaying communications between customer-managed components and infrastructure components in Citrix Cloud is the Citrix Cloud Connector.
    - Communication Relay Point: The Citrix Cloud Connector serves as the essential relay point, facilitating communication between customer-managed components (like Virtual Delivery Agents or VDAs) and infrastructure components in Citrix Cloud.
    - Connectivity with Active Directory: It enables VDAs to communicate with Citrix Cloud and establishes communication channels between Citrix Cloud and Active Directory.
  - Infrastructure in Citrix DaaS Deployment: The infrastructure for a Citrix DaaS deployment is hosted in the Citrix Cloud platform, providing the necessary infrastructure and services to deliver virtual desktops and applications to users.
    - Citrix Workspace, a Citrix Cloud-managed component, functions as the equivalent of StoreFront in the cloud. Users can log into Citrix Workspace, whether they are within their company network or external users.

---

## On the Job Application

- The Citrix Cloud Connector serves as a critical relay point for communications in Citrix Desktop as a Service (DaaS) deployments.
  - Ensure proper configuration of the Citrix Cloud Connector to guarantee efficient relay of communications between customer-managed components and Citrix Cloud infrastructure.
  - Implement security best practices when configuring and managing the Citrix Cloud Connector to protect communication channels and sensitive data.
  - Stay informed about updates and changes to Citrix Cloud Connector functionality, and implement regular monitoring to identify and address potential issues promptly.
-

# Clip: Resources Published with Citrix Virtual Apps and Desktops

---

## Scenario/Challenge

A Citrix administrator is experiencing issues in delivering published applications to users in a Citrix Virtual Apps and Desktops environment. A master image, machine catalog, and delivery group have been created, but users can't access them. Investigation reveals a configuration issue. How can the administrator troubleshoot it?

---

This section was designed to help you troubleshoot issues related to delivering published applications in a Citrix Virtual Apps and Desktops environment. If you are experiencing difficulties even after creating a master image, machine catalog, and delivery group, the below steps will help to identify and resolve configuration issues.

## Troubleshooting Citrix Virtual Apps and Desktops Application Delivery Issues

This section is dedicated to troubleshooting Citrix Virtual Apps and Desktops application delivery issues.

### Confirm Machine Catalog and Delivery Group Configuration

- In Citrix Studio, verify the configuration of the machine catalog and delivery group created. Ensure that the master image is correctly associated with the machine catalog.
  - Access the Citrix Studio interface and navigate to the delivery group settings. Confirm that users or user groups have been added to the delivery group to grant access to the published applications.
    - If users are unable to access published applications, the issue may be related to user permissions. Add users or user groups to the delivery group specifically for application access. This is done through the Citrix Studio interface.
    - Confirm that the integration with the customer's user directory, typically Microsoft Active Directory, is functioning correctly. Ensure



that the users or user groups added to the delivery group are valid and exist in the directory.

- Review Application Publishing.
    - Check the Citrix Studio settings for the delivery group to verify that the applications and desktops have been correctly published and made available to users. Ensure that the desired resources are configured for access.
      - Monitor the Citrix Delivery Controller for any error messages or alerts related to the delivery group. Investigate any logged issues that might provide insights into the configuration problem.
      - Review the master image configuration to ensure that it includes the necessary components and settings for the intended applications. Confirm that the master image is updated and compatible with the delivery group.
  - Consider Resource Provisioning Steps.
    - Reflect on the entire process of provisioning resources, starting from creating the master image, machine catalog, and delivery group. Ensure that each step has been accurately completed, as outlined in Citrix Studio.
      - Consult Citrix documentation or support resources for specific troubleshooting steps related to the Virtual Apps and Desktops environment. Citrix provides comprehensive documentation for administrators.
-

## On the Job Application

- Ensure users or user groups are added to the delivery group in Citrix Studio to grant them access to published applications.
  - Verify the configuration of the machine catalog and delivery group in Citrix Studio, ensuring correct association with the master image.
  - Keep user groups up-to-date in the delivery group, adding or removing users as needed. This ensures that the right individuals have access to the published applications.
  - Regularly review and update the master image configuration to include necessary components and settings for the intended applications. Ensure compatibility with the delivery group.
-

# Clip: Integrating Storefront with Citrix

---

## Scenario/Challenge

A Citrix administrator has received reports from users who are experiencing issues with authentication when attempting to access applications through StoreFront. Upon investigation, it was discovered that StoreFront is unable to authenticate users with Active Directory. What could be the possible reason for this issue?

---

This section was designed to help you address authentication issues reported by users attempting to access applications through StoreFront in a Citrix environment. If you have discovered that StoreFront is unable to authenticate users with Active Directory, follow these steps to identify the potential reason for the issue.

## StoreFront Authentication Issues with Active Directory

This section addresses StoreFront authentication issues with Active Directory.

### Understanding StoreFront and Active Directory Communication:

- When users sign on to StoreFront to launch applications or desktops, StoreFront handles the authentication process. This is known as Direct Authentication, where StoreFront communicates directly with an Active Directory domain controller using Lightweight Directory Access Protocol (LDAP) or secure LDAP over port 389 or port 636.
  - If users are experiencing authentication failures, it's crucial to investigate the communication between StoreFront and Active Directory to pinpoint the root cause.
    - The possible reason for the authentication issue could be that StoreFront is using an incorrect port for LDAP communication with Active Directory. This misconfiguration can lead to authentication failures.
- Check LDAP Port Configuration
  - Access the StoreFront server configuration and verify the LDAP port settings. Ensure that StoreFront is configured to communicate with Active Directory over the correct port, either 389 for LDAP or 636 for secure LDAP.

- Citrix recommends securing communications between StoreFront and critical components, including Active Directory, by using HTTPS and encrypting the data with SSL certificates. Confirm that HTTPS is enabled, and SSL certificates are properly configured.
  - Check the validity of SSL certificates used in the communication between StoreFront and Active Directory. Expired or invalid certificates can disrupt secure communication.
- 

## On the Job Application

- Familiarize yourself with Citrix's best practices for secure communication in a Citrix environment.
  - Ensure that StoreFront follows these best practices to guarantee the confidentiality and integrity of the communication.
  - Review StoreFront logs for any error messages or warnings related to LDAP communication. These logs can provide valuable insights into the authentication issue.
  - Collaborate with your IT security team to ensure that the communication between StoreFront and Active Directory aligns with security policies and standards.
-

# Clip: Installing Citrix Delivery Controller

---

## Scenario/Challenge

What is the first step in the installation process of the Citrix Delivery Controller on Windows Server 2019?

---

This section was designed to walk you through the first step in the installation process of the Citrix Delivery Controller on Windows Server 2019. Following these steps ensures a smooth initiation of the installation process.

## Installing Citrix Delivery Controller on Windows Server 2019

This section provides a step-by-step guide to installing Citrix Delivery Controller on Windows Server 2019.

### Pre-installation Preparation

- Before starting the installation process, ensure that your machines are already joined to the Active Directory (AD) domain. This is a prerequisite for the installation.
- Initiating the Installation: Navigate to the Citrix website by entering the URL [www.citrix.com](http://www.citrix.com) in your browser's address bar.
  - Once on the Citrix website, locate and click on the "Customers" section.
  - In the dropdown menu, select "Downloads" to access the Citrix product downloads.
  - Choose "Citrix Virtual Apps and Desktops" from the available options.
  - A list of the latest versions of Citrix Virtual Apps and Desktops will be displayed. Select the version you intend to use. For example, click on version 7.2308.
  - Scroll down to find the "Download file" option associated with the chosen version and click on it.
  - Accept the download agreement, and the download process will commence. Note that the file size can be substantial, up to 3 GB, so be patient during the download.
- Opening the Downloaded File: Once the download is complete, open the downloaded file.
  - Select the "Auto Select" option, which will initiate the installation window.

- Look for and click on the "Start" button next to "Virtual Apps and Desktops."
- Subsequently, click on "Delivery Controller" to proceed with the installation of the Citrix Delivery Controller.

---

## On the Job Application

- The first step involves navigating to the Citrix website ([www.citrix.com](http://www.citrix.com)) to download the latest Citrix Virtual Apps and Desktops (CVAD) installer ISO.
- Choose the version of Citrix Virtual Apps and Desktops that you intend to use. Consider compatibility and any specific features offered by the selected version.
- Ensure that the machines where Citrix Delivery Controller is being installed are running on the latest updates and patches for the Windows Server 2019 operating system.
- Confirm that the machines meet the system requirements specified by Citrix for running the Delivery Controller. This includes hardware specifications and software prerequisites.
- Periodically check the Citrix website for the latest versions of Citrix Virtual Apps and Desktops to stay informed about updates, features, and potential security enhancements.



# Clip: Understanding Internal Apps and Desktops Launch Process

---

## Scenario/Challenge

During which resource launch phase are applications and desktops identified and presented to the user, based on their group memberships and assigned resources in the Citrix environment?

---

This section was designed to help you understand the resource launch phases in the Citrix environment. We will focus on the phase where applications and desktops are identified and presented to the user based on their group memberships and assigned resources.

## Understanding Citrix Resource Enumeration


This section delves into understanding Citrix resource enumeration.

### Resource Enumeration

- The process of launching a Citrix resource, whether it's a published app or published desktop, consists of four high-level phases: User Authentication, Resource Enumeration, Resource Launch, and Session Initialization.
  - The specific phase where applications and desktops are identified and presented to the user is known as Resource Enumeration.
    - The process begins with StoreFront passing the user's credentials to a Delivery Controller.
    - The Delivery Controller, in turn, takes these credentials and submits them to Active Directory (AD). However, this is not for authentication but to retrieve the list of AD security groups to which the user belongs.
    - The Delivery Controller queries the site database on the SQL server. This database maintains records of all applications and desktops assigned to individual users and groups.

- The user's AD account details and group information are submitted to SQL, and in return, SQL provides the list of applications and desktops assigned to that user, along with application icons.
  - The Delivery Controller sends this list and app icons to the StoreFront server.
  - StoreFront takes this information and renders it in HTML format, creating a graphical list of application and desktop icons.
  - On the StoreFront page, the user can now view and interact with the displayed applications and desktops, launching them as needed.
  - Resource Launch Phase
    - As the user decides to launch an app or desktop by clicking on the corresponding icon, this action initiates the subsequent phase known as the Resource Launch phase.
- 

## On the Job Application

- Resource Enumeration is the phase where applications and desktops are identified and presented to the user based on their group memberships and assigned resources.
  - Ensure that the machines involved in the Citrix environment, including Delivery Controllers and StoreFront servers, are regularly updated with the latest operating system patches and Citrix software updates.
  - Efficiently manage user groups in Active Directory, ensuring that users are appropriately assigned to security groups. This practice streamlines the Resource Enumeration phase and enhances overall system organization.
- 

# Clip: Understanding Internal Apps and Desktops Launch Process

---

## Scenario/Challenge

Which of the following best describes the role of the Delivery Controller in the Resource Enumeration phase?

---

## Understanding the Role of Delivery Controller in Resource Enumeration

This section was designed to help you comprehend the essential role of the Delivery Controller in the Resource Enumeration phase within the Citrix environment. This knowledge contributes to a comprehensive understanding of the Citrix resource launch process.

### Authentication Phase Overview

- Before delving into Resource Enumeration, it's essential to briefly recap the Authentication phase. Users enter credentials on the StoreFront page, initiating a process that involves authentication with the AD domain controller.
  - Once the Authentication phase is successfully completed, we transition to the second phase: Resource Enumeration. StoreFront passes the user's credentials to the Delivery Controller to initiate this phase.
    - The Delivery Controller takes these credentials and submits them to Active Directory, not for authentication but to retrieve the list of AD security groups the user belongs to.
    - Simultaneously, the Delivery Controller queries the site database on the SQL server. This database maintains records of applications and desktops assigned to individual users and groups.
    - Beyond Resource Enumeration, the process concludes with the Session Initialization phase, where the user connects to the VDA session and begins working in the launched app.

- Role of Delivery Controller
    - The entire session launch process can be grouped into two parts:
      - Authentication and Enumeration: When the user logs on, and the apps and desktops assigned to them are displayed.
      - Launch: When the user can launch any app or desktop from the icons displayed, and a Virtual Delivery Agent (VDA) is selected to host the session.
- 

## On the Job Application

- Understanding the role of the Delivery Controller in the Resource Enumeration phase is pivotal for grasping how Citrix efficiently identifies and presents applications and desktops to users based on their group memberships and assigned resources.
  - Implement regular monitoring of the Citrix environment, including Delivery Controllers and SQL servers, to identify any performance issues or potential bottlenecks in the Resource Enumeration phase.
  - Regularly review logs generated by Delivery Controllers to identify and address any errors or warnings promptly. Proactive log monitoring contributes to maintaining a healthy Citrix environment.
  - Efficiently manage user groups in AD to streamline the Resource Enumeration phase, ensuring that users are appropriately assigned to security groups.
-

# Clip: Understanding Internal Apps and Desktops Launch Process

---

## Scenario/Challenge

You are an IT administrator responsible for managing Citrix Virtual Apps and Desktops within your organization. One of your tasks is to ensure that users can successfully launch their Citrix resources. You have a new user who is trying to access a published app for the first time using the Citrix system. Considering the phases of the Citrix resource launch process, identify the appropriate steps you would instruct them to follow in order to launch the published app.

---

As an IT administrator managing Citrix Virtual Apps and Desktops, ensuring a seamless experience for users launching their Citrix resources is crucial. If you have a new user trying to access a published app for the first time, consider the following steps based on the phases of the Citrix resource launch process.

## Launching Citrix Resources

This section guides users through the process of launching Citrix resources.

### Accessing the StoreFront Page

1. Open a web browser on your device.
2. Navigate to the StoreFront page, either by entering the StoreFront URL directly or accessing it through Citrix Workspace.
3. On the StoreFront page, enter your credentials (username and password) to authenticate and gain access to Citrix resources.
4. Once authenticated, you will see a list of published applications and desktops on the StoreFront page. Select the published app you wish to launch from the displayed list.
5. Click on the corresponding app icon to initiate the request to launch the selected resource. This request is then sent to StoreFront, indicating your intention to launch the chosen app.

### Delivery Controller Interaction

- StoreFront forwards the launch request to the Delivery Controller, a critical component in the Citrix environment. The Delivery Controller, based on its



configuration, selects the Virtual Delivery Agent (VDA) best suited to host the session for the user.

- The information about the selected VDA is stored in the site database on the SQL server. The site database plays a key role in maintaining records of the Citrix environment's configurations, including VDA assignments.

### **Seamless Resource Launch**

- Thanks to the efficient process, the user experiences a quick and seamless launch of the selected app. This entire process, from entering credentials to launching apps and desktops, takes only a couple of seconds.
  - To connect to the Virtual Delivery Agent (VDA) and launch the published app successfully, the user can use the ICA file generated during the process.
- 

### **On the Job Application**

- Provide training to users, especially newcomers, on the process of accessing and launching Citrix resources. Clear instructions can contribute to a positive user experience.
  - Implement regular monitoring of logs generated by Citrix components, including the Delivery Controller and StoreFront. Proactive log checks help identify and address potential issues promptly.
  - Continuously assess and plan for the capacity of the Citrix environment to accommodate growing user demands. Consider hardware requirements and potential scalability.
-



# Clip: Understanding Internal Apps and Desktops Launch Process

---

## Scenario/Challenge

Which of the following statements accurately reflects their relationship and function during the User Authentication and Resource Enumeration phases?

---

Citrix session launch involves several critical phases, including User Authentication and Resource Enumeration. This section breaks down these phases to provide a comprehensive understanding of their relationship and functions.

## Understanding User Authentication and Resource Enumeration Phases

This section explains the user authentication and resource enumeration phases.

### User Authentication

- Resource Enumeration Phase:
  - StoreFront forwards the user's credentials to the Delivery Controller, marking the beginning of the Resource Enumeration phase.
    - The Delivery Controller, instead of authenticating, retrieves the user's AD security group information from the Active Directory.
    - The Delivery Controller queries the site database on the SQL server, storing records of assigned applications and desktops for each user and user group.
    - The user's AD account and group details are submitted to SQL, retrieving a list of apps and desktops along with application icons.
    - The Delivery Controller sends the list and app icons to StoreFront for user display in HTML format.
    - On the StoreFront page, the user can launch any displayed application or desktop, marking the completion of Resource Enumeration.

- User Authentication verifies the user's identity through StoreFront and AD, completing the initial phase of the session launch.
    - Resource Enumeration involves the Delivery Controller retrieving user group information, querying the site database, and presenting available resources on StoreFront.
- 

## On the Job Application

- Understanding the User Authentication and Resource Enumeration phases is crucial for a smooth and efficient Citrix session launch experience.
  - Regularly monitor logs to address potential issues promptly.
  - Maintain detailed documentation for troubleshooting and training purposes.
  - Prioritize secure communication practices, especially concerning user credentials.
-

# Clip: The Evolution of Citrix and Remote Computing

---

## Scenario/Challenge

An IT administrator is responsible for managing Citrix Virtual Apps and Desktops deployment in a large organization. A user reports that they are unable to access their virtual desktop from their laptop, even though they have the Citrix Workspace app installed. What approach would you use to troubleshoot and resolve the user's inability to access their virtual desktop?

---

As an IT administrator managing Citrix Virtual Apps and Desktops in a large organization, it's crucial to be equipped with troubleshooting skills. When a user reports an inability to access their virtual desktop despite having the Citrix Workspace app installed, a systematic approach is essential to identify and resolve the issue.

## Troubleshooting Approach

- Verify System Requirements:
  - Check Operating System Compatibility: Verify if the laptop's operating system is compatible with the version of Citrix Workspace app installed.
  - Review Hardware Specifications: Ensure that the laptop's hardware meets the minimum requirements specified by Citrix for optimal performance.
  - Check for Updates: Confirm that the Citrix Workspace app on the user's laptop is up-to-date. Citrix regularly releases updates to address compatibility issues and enhance performance.
- Update Citrix Workspace App:
  - Update Citrix Workspace App: Direct the user to update their Citrix Workspace app to the latest version available. This can usually be done through the app store or by downloading the latest installer from the Citrix website.
  - Restart the Laptop: After updating the app, instruct the user to restart their laptop to ensure that the changes take effect.
- Test Virtual Desktop Access:
  - Launch Citrix Workspace App: Instruct the user to launch the Citrix Workspace app on their laptop.
  - Attempt Virtual Desktop Access: Guide the user to attempt accessing their virtual desktop again. Monitor for any error messages or issues during the

connection process.

---

## On the Job Application

- Before troubleshooting, ensure the user's laptop meets the system requirements specified for the Citrix Workspace app.
  - Check the installed version of the Citrix Workspace app on the user's laptop and update it to the latest version if necessary.
  - Check the status of the Citrix Virtual Apps and Desktops deployment to ensure it is operational, examining server logs for any errors related to the user's connection.
  - Verify the stability of the user's internet connection and check for any potential firewall or network issues that may be affecting the Citrix connection.
-



**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# NetScaler Gateway

## Student Guide



NetScaler, a comprehensive application delivery controller (ADC), excels in advanced traffic management, load balancing, and security features. This guide, with a focus on NetScaler Gateway, was designed to:

- Capture essential information, including On the Job Application, that will assist you in performing job-related tasks.
- Enhance your learning experience by reducing note taking tasks while taking the course.

For a faster guide navigation, scroll down to the Table of Content and click on the question of interest.

# Table of Content

## Skills covered in this course:

[What is the primary role of NetScaler Gateway in providing remote access to an organization's network resources?](#)

[What is the purpose of the Full VPN Deployment option in Netscaler Gateway?](#)

[What is the role of STA in Citrix Virtual Apps and Desktops access through NetScaler Gateway?](#)

[Which statement accurately describes the purpose of RDP Proxy in Netscaler Gateway deployment options?](#)

[What key component is necessary to securely handle ICA traffic to ensure secure access for external clients in a Citrix Virtual Apps and Desktops \(CVAD\) environment through Netscaler Gateway?](#)

[What is the purpose of the Resource Enumeration phase in launching a Citrix resource through Netscaler Gateway?](#)

[When a user clicks on a specific application icon, what action does it initiate in the Citrix resource launch through Netscaler Gateway?](#)

[Which of the following accurately describes the role of pre-authentication policies in NetScaler Gateway's access control process?](#)

[A remote worker needs to access web-based applications and virtual desktops without installing any additional client software. Which Netscaler Gateway deployment option would be most suitable for this situation?](#)

[An IT administrator is responsible for setting up remote access to Citrix Virtual Apps and Desktops using Netscaler Gateway. They want to ensure that users accessing the gateway via the Workspace app have a smooth experience. What action should they take to achieve this?](#)

[A company implemented nFactor authentication with NetScaler Gateway for](#)

security, but some employees are experiencing issues during the authentication process and are unable to proceed past a certain step. What should IT support do to address this issue?

You have set up the integration between ADM and Netscaler Gateway. The Insight column in ADM indicates "Enabled"; however, you do not see any data on the NetScaler ADM dashboard. What aspect of the configuration should you investigate to diagnose the issue?

An organization is using NetScaler Gateway's EPA feature to enhance its network security. An employee's laptop fails the Endpoint Analysis scan due to outdated antivirus software and an inadequate OS patch level. What should the organization do to address this issue effectively?

An organization is using NetScaler Gateway to provide remote access to their internal resources. They have configured a Virtual Server (vServer) to handle HTTPS traffic, utilized SSL certificates for secure communication, and set up various authentication methods. They also customized the portal theme for a consistent user experience and defined specific rules for application access and traffic management. Given this setup, analyze which of the following scenarios would most likely require a change in the existing configuration of the NetScaler Gateway?

What is the specified IP Address Type for the AAA Vserver used for internal communication in the Netscaler Gateway Virtual Server configuration?

What is the purpose of setting up a server certificate for the Gateway Virtual Server in the Netscaler admin console?

As a network administrator, you are reviewing the steps that one of the IT specialists is planning to take when setting up a Gateway Virtual Server in the NetScaler admin console. Identify the mistake in the setup process.

Scenario: You are a network administrator tasked with setting up a NetScaler Gateway Virtual Server following the steps outlined in the video. You named the Virtual Server "external\_gateway," configured it with an IP address, set up a server certificate, and added LDAP authentication. After completing the basic configuration, you are considering additional security measures. Question: Based on the current setup of the NetScaler Gateway Virtual Server, which of the following actions would most effectively enhance the security of the server?

Considering the configuration process for Netscaler Gateway Virtual Server outlined

in the video, analyze the potential consequences of omitting the step related to setting up a server certificate.

Which statement accurately describes the purpose of the traffic policy for Single Sign-on (SSO) in the NetScaler configuration?

Which step is crucial for the configuration of the session policy for web browsers in the NetScaler Gateway setup?

As a network administrator, you configured a session policy for web browsers and a traffic policy for Single Sign-On (SSO) on NetScaler Gateway. You also set up and bound an STA server to the Gateway Virtual servers and ensured that the session policy for web browsers evaluates to true for clients using any web browser, and the traffic policy for SSO is applicable for all users. Which of the following scenarios would most likely require additional adjustments to the existing setup of the NetScaler Gateway?

What action should be taken in the "Security" tab of the session profile configuration for Citrix Workspace App users in Netscaler Gateway?

As an IT administrator, you are in the process of configuring session policies on NetScaler Gateway for different types of users. What step should you take to correctly set up the session policy for users accessing via the Citrix Workspace App (CWA)?

As an IT specialist, you created a session policy for users accessing the NetScaler Gateway via the Citrix Workspace App. You named the policy "Session\_policy\_CWA," set up various parameters like Split Tunnel, Clientless Access, and Plugin-in Type, and configured the policy to apply when the "CitrixReceiver" user-agent is detected. Now, you are preparing to deploy this configuration in your organization's network. Given the specifics of the "Session\_policy\_CWA" configuration, which of the following situations would most likely require a review or modification of this policy?

What information is entered in the "Single Sign-on domain" field under the session profile for Netscaler Gateway?

As a network administrator, you have successfully configured session policies for Citrix Workspace App (CWA) and web browsers, as well as a traffic policy for Single Sign-On (SSO) on the NetScaler Gateway. You have also bound an STA server to the Gateway Virtual servers. This setup is intended to streamline user access and enhance security. After implementing these configurations, which of the following

scenarios would most likely require further modifications to the NetScaler Gateway's session and traffic policies?

What is one of the key functionalities of Application Delivery Management (ADM) HDX Insight?

Which statement best captures the role and capabilities of Application Delivery Management (ADM) HDX Insight in enhancing application performance?

You are an IT administrator tasked with integrating ADM HDX with the NetScaler Gateway to monitor Citrix Virtual Apps and Desktops traffic. Which actions would you take in this situation?

As an IT Security Manager, you have been tasked with utilizing the Endpoint Analysis (EPA) feature of NetScaler Gateway to enhance the network security of your organization. Which of the following actions would you take to apply EPA effectively in your network environment?

You have tasked an IT administrator with setting up a NetScaler Gateway VPN connection.. Select the statement that will best demonstrate their understanding about the functions and considerations involved in setting up a NetScaler Gateway VPN connection for remote access?

As a network administrator, you are setting up a NetScaler Gateway VPN for your organization to facilitate secure remote access for employees. Which of the following actions would you take to effectively apply these principles in your setup?



# Clip: Introducing NetScaler Gateway

---

## Scenario/Challenge

What is the primary role of NetScaler Gateway in providing remote access to an organization's network resources?

---

This section was designed to help you understand the primary role of NetScaler Gateway in providing remote access to an organization's network resources. Let's delve into the key concepts and gain insights from the provided source.

## Understanding the Primary Role of NetScaler Gateway

This section focuses on understanding the primary role of NetScaler Gateway.

### Introduction to NetScaler Gateway

- Imagine you are working from home, and the need arises to access your company's applications and data. However, connecting directly to your office network from your home is not a straightforward process. This is where NetScaler Gateway becomes essential.
  - NetScaler Gateway serves as a virtual door connecting users outside the organization's network with the internal resources they need to access. Its primary role is to securely provide remote access to network resources.
    - NetScaler Gateway utilizes various security protocols to establish a secure connection between your device and the internal network. It acts as a middleman, encrypting data traffic during transit. The encryption is crucial for safeguarding sensitive information from unauthorized access, especially when dealing with confidential data like customer records or financial information.
- Importance of Encryption
  - The provided source emphasizes that one of the key benefits of NetScaler Gateway is its ability to encrypt data traffic. Encryption ensures that sensitive information remains protected from prying eyes, enhancing the overall security of remote connections.
    - NetScaler Gateway offers flexibility by allowing secure access to applications and data regardless of the user's location or the device they are using. Whether it's a laptop, smartphone, or tablet, NetScaler Gateway supports a wide range of client devices. This adaptability enables users to work from their preferred devices



while maintaining a secure connection, promoting productivity and facilitating a mobile workforce

---

## On the Job Application

- NetScaler Gateway plays a pivotal role in securely connecting remote users to an organization's network resources.
  - Remember, NetScaler Gateway acts as more than just a gateway—it's a virtual door ensuring authorized access while keeping unauthorized users at bay.
  - Conduct regular security audits to assess the effectiveness of NetScaler Gateway configurations, identify potential vulnerabilities, and apply necessary adjustments.
  - Educate users on secure practices, including the importance of strong passwords, secure connection practices, and awareness of phishing threats.
-

# Clip: Panning Gateway VPN Connection

---

## Scenario/Challenge

What is the purpose of the Full VPN Deployment option in NetScaler Gateway?

---

## Understanding the Purpose of Full VPN Deployment in NetScaler Gateway

This section is dedicated to understanding the purpose of full VPN deployment in NetScaler Gateway.

### Purpose of Full VPN Deployment

- NetScaler Gateway offers a Full VPN Deployment option that plays a crucial role in providing secure remote access to an organization's network resources. Understanding its purpose is essential for grasping the significance of this feature.
  - The purpose of the Full VPN Deployment option in NetScaler Gateway is to create a virtual private network concentrator. This concentrator facilitates remote access for users from various locations, including their homes or other remote sites via the Internet.
- Key Components of Full VPN Deployment:
  - Before implementing NetScaler Gateway Full VPN, it's imperative to consider specific prerequisites to ensure a secure and seamless remote access experience for users. Here are the key components to understand:
    - Before deploying a Full VPN, assess your organization's requirements.
    - Consider factors such as the number of remote users, network architecture, types of applications/resources needing access, and existing security policies.
    - This assessment ensures that the Full VPN Deployment aligns with the specific needs of your organization.
    - Typically, NetScaler is placed in a Demilitarized Zone (DMZ) to enhance security.
    - DMZ acts as an additional layer of protection between the internet and your internal network, safeguarding sensitive information from potential threats.

---

## On the Job Application

- A NetScaler Gateway VPN connection is a secure and remote access solution that enables users to connect to their organization's network from outside locations.
  - Full VPN Deployment in NetScaler Gateway serves to create a virtual private network concentrator and its primary goal is to facilitate secure remote access for users connecting from various locations via the Internet.
  - Consider factors such as the number of remote users, network architecture, types of applications/resources needing access, and existing security policies.
  - Place NetScaler in a DMZ to provide an additional layer of security.
-

# Clip: Integrating NetScaler with Citrix

---

## Scenario/Challenge

What is the role of STA in Citrix Virtual Apps and Desktops access through NetScaler Gateway?

---

In the realm of Citrix Virtual Apps and Desktops, the Secure Ticket Authority (STA) plays a crucial role in ensuring secure access for users through NetScaler Gateway. This section will help you comprehend the significance of STA and its function in the authentication process.

## Understanding the Role of STA in Citrix Virtual Apps and Desktops Access

This section is dedicated to understanding the role of STA in Citrix Virtual Apps and Desktops access.

### Introduction

- Role of STA in Citrix Virtual Apps and Desktops Access.
  - Definition of STA:
    - The STA is an XML web service that performs a vital function in the Citrix environment.
    - Its primary role is to exchange Citrix Virtual Apps and Desktops (CVAD) server information for randomly generated tickets.
- Ticket Exchange for Secure Access
  - STA facilitates the exchange of CVAD server information for randomly generated secure tickets.
    - As users attempt to access resources through NetScaler Gateway, STA generates these secure tickets containing session details.
- Authentication Process:
  - The secure tickets generated by STA are presented to Citrix servers during the authentication process.
  - This ensures that access to resources is both secure and authenticated.

- Configuration of STA
    - Setting up STA involves configuring the NetScaler Gateway with information about one or more STA servers.
      - STA servers can be physical or virtual machines running Citrix Secure Ticket Authority software.
      - This ensures that access to resources is both secure and authenticated.
- 

## On the Job Application

- Each component, from Virtual Server setup to STA optimization and Storefront configuration, plays a vital role in ensuring a user-friendly and well-managed Citrix environment.
  - It is crucial that the STA server information specified in both Storefront and NetScaler Gateway matches perfectly for seamless functionality.
  - Verify that the STA is functioning optimally by configuring NetScaler Gateway with accurate information about one or more STA servers.
  - Configure Session Policy and Profile for user access, ensuring that the policies align with security requirements.
-

# Clip: Planning NetScaler Deployment

---

## Scenario/Challenge

Which statement accurately describes the purpose of RDP Proxy in NetScaler Gateway deployment options?

---

In the NetScaler Gateway deployment, understanding the purpose of RDP Proxy is crucial for ensuring secure access to Remote Desktop Services (RDS) or Virtual Desktop Infrastructure (VDI) resources using the Remote Desktop Protocol (RDP). This section will help you comprehend the accurate statement regarding the purpose of RDP Proxy.

## Understanding the Purpose of RDP Proxy in the NetScaler Gateway Deployment

This section delves into understanding the purpose of RDP Proxy in the NetScaler Gateway deployment.

### Purpose of RDP Proxy

- Definition of RDP Proxy
    - RDP Proxy is a specific deployment type within NetScaler Gateway that serves a distinct purpose.
      - RDP Proxy acts as a proxy for Remote Desktop Protocol (RDP) traffic.
      - Its primary role is to enhance security and control over remote access to RDS and Virtual Desktop Infrastructure (VDI) resources.
  - Secure Access to RDS and VDI
    - The key function of RDP Proxy is to enable users to securely access Remote Desktop Services (RDS) or VDI resources using RDP.
      - By acting as a proxy, RDP Proxy enhances security and control over RDP traffic, ensuring that remote access is both secure and managed effectively.
-



## On the Job Application

- Understanding the role of RDP Proxy is integral to leveraging Netscaler Gateway effectively for secure remote access to RDS and VDI resources.
  - NetScaler Gateway offers various deployment types to cater to diverse organizational needs.
  - Choosing a NetScaler Gateway deployment type depends on factors such as security requirements, types of applications for remote access, and the desired level of control.
  - NetScaler Gateway's versatility empowers organizations to securely enable remote access while customizing the solution to their specific needs.
-

# Clip: Introducing NetScaler Gateway Entities

---

## Scenario/Challenge

What key component is necessary to securely handle ICA traffic to ensure secure access for external clients in a Citrix Virtual Apps and Desktops (CVAD) environment through NetScaler Gateway?

---

In a Citrix Virtual Apps and Desktops (CVAD) environment, ensuring secure access for external clients is paramount. One key component plays a crucial role in securely handling ICA traffic through NetScaler Gateway.

## Key Component for Secure Handling of ICA Traffic

This section explores a key component for the secure handling of ICA (Independent Computing Architecture) traffic.

### Understanding the Virtual Server (vServer)

- A Virtual Server, often abbreviated as vServer, is a fundamental component within NetScaler Gateway.
  - It serves as the access point for users, providing a secure entryway to internal resources, applications, and desktops.
    - The Virtual Server acts as a network endpoint that listens for incoming connections from external clients.
    - It plays a pivotal role in directing traffic based on configured policies, ensuring that the traffic is handled securely and efficiently.
- Secure Handling of Independent Computing Architecture (ICA) Traffic
  - In the context of Citrix Virtual Apps and Desktops, the Virtual Server is crucial for securely handling ICA traffic.
    - ICA is the protocol used by Citrix for communication between the client device and the Citrix Virtual Apps or Desktops servers. The Virtual Server ensures that this traffic is managed and secured effectively.
- Configuration Examples
  - You can configure a Virtual Server to handle specific types of traffic, such as HTTPS, on designated ports (e.g., 443).
    - By configuring policies, you can route ICA traffic securely to the appropriate backend servers, providing a seamless and secure user experience.

---

## On the Job Application

- The Virtual Server acts as the access point for users, directing incoming connections and ensuring the secure handling of ICA traffic between external clients and internal resources.
  - The Virtual Server is essential for securely handling ICA (Independent Computing Architecture) traffic in a Citrix Virtual Apps and Desktops environment.
  - Regularly update SSL/TLS certificates to maintain a secure connection.
-

# Clip: Understanding External Application Enumeration

---

## Scenario/Challenge:

What is the purpose of the Resource Enumeration phase in launching a Citrix resource through NetScaler Gateway?

---

Launching Citrix resources through NetScaler Gateway involves several phases, each playing a crucial role in providing users with secure and efficient access to assigned apps and desktops.

## The Purpose of Resource Enumeration Phase in Launching Citrix Resources through NetScaler Gateway

In this section, we will focus on the Resource Enumeration phase and its purpose in the overall process.

### Overview of Launch Phases

- Launching Citrix resources through NetScaler Gateway involves four main phases: User Authentication, Resource Enumeration, Resource Launch, and Session Initialization.
  - These phases can be divided into two parts: Enumeration and Launch.
    - The Enumeration phase allows users to view their assigned apps and desktops, while the Launch phase enables them to access and use the desired resources.
- Key Steps in Enumeration Phase
  - The Resource Enumeration phase is initiated after successful authentication.
    - During this phase, the client requests a list of resources from NetScaler Gateway.
- Purpose of Resource Enumeration
  - The specific purpose of the Resource Enumeration phase is for the client to receive a list of assigned apps and desktops from Netscaler Gateway.
    - This list contains all the resources that have been assigned to the user.

- Efficiency of Enumeration Process
    - While the authentication and enumeration steps may seem detailed, they are efficiently executed, taking only a few seconds from credential input to the display of accessible apps and desktops.
- 

## On the Job Application

- The purpose of the Resource Enumeration phase in launching a Citrix resource through NetScaler Gateway is for the client to request a list of assigned apps and desktops.
  - During this phase, NetScaler Gateway communicates with StoreFront, which consults the Delivery Controller to determine the available resources based on the user's roles and permissions.
  - StoreFront consults the Delivery Controller (DDC) to determine the available apps and desktops based on the user's roles and permissions
  - NetScaler Gateway, in turn, communicates with StoreFront to retrieve the list of available resources for the user.
-

# Clip: Understanding External Application Launch

---

## Scenario/Challenge

When a user clicks on a specific application icon, what action does it initiate in the Citrix resource launch through NetScaler Gateway?

---

The Citrix resource launch through Netscaler Gateway involves a series of steps that ensure a secure and seamless user experience.

## Understanding the Action Initiated in Citrix Resource Launch through NetScaler Gateway

In this section, we will focus on the specific action initiated when a user clicks on a specific application icon.

### Action Initiated in Citrix Resource Launch

- Resource Launch Phase Overview
    - The resource launch phase begins when a user clicks on a specific application icon.
      - Clicking on the application icon triggers a request for the ICA file from the NetScaler Gateway.
  - Request Flow to Delivery Controller (DDC)
    - The request is relayed from the Netscaler Gateway to StoreFront (SF), which further forwards it to the Delivery Controller (DDC).
      - The DDC responds with critical Virtual Delivery Agent (VDA) information, including IP, port, and session key.
  - STA Ticket Generation and ICA File Creation
    - SF, aware of external user connections, contacts the Secure Ticket Authority (STA) server for STA ticket information.
      - The STA server generates a ticket for the session and sends it back to SF.
      - SF then generates the ICA file, substituting VDA information with STA ID and STA ticket details to secure internal server information.
      - The NetScaler Gateway transmits the ICA file back to the client after receiving a response.
-



## On the Job Application

- When a user clicks on a specific application icon, it initiates the action of the NetScaler Gateway downloading the ICA file to the client endpoint
  - Once the ICA file is downloaded, the Citrix Workspace on the client endpoint triggers the connection to the NetScaler Gateway Virtual server.
  - Utilizing the data in the ICA file, the NetScaler Gateway verifies the STA ticket with the STA server.
  - Upon receiving a valid response from the STA server, including VDA server information (IP and port), NetScaler Gateway establishes a connection with the VDA's port.
  - Once the connection is established, the NetScaler Gateway assumes the role of a "proxy" between the client and the VDA.
-

# Clip: Planning EPA

---

## Scenario/Challenge

Which of the following accurately describes the role of pre-authentication policies in NetScaler Gateway's access control process?

---

NetScaler Gateway offers robust security features, including the powerful Endpoint Analysis (EPA) feature, to enhance network security.

## Understanding the Role of Pre-Authentication Policies

This section will focus on understanding the role of pre-authentication policies in NetScaler Gateway's access control process.

### Overview of EPA and Access Control

- EPA is a crucial feature that ensures secure remote access by analyzing endpoints and enforcing security requirements before granting access to applications and resources.
  - EPA can be configured either before or after authentication, and both pre-authentication and post-authentication policies play distinct roles in the access control process.
    - Pre-authentication policies specifically focus on evaluating incoming requests to assess the security and compliance of the device.
    - These policies perform checks on various aspects of the device, including antivirus software, patches, firewall settings, and other security configurations.
- Purpose of Pre-Authentication Policies
  - The primary purpose of pre-authentication policies is to ensure that only compliant and secure devices can proceed with the authentication process.
    - Devices that do not meet the specified security criteria might either be denied access or redirected to remediation steps, such as updating antivirus definitions or applying necessary patches.
- Device Compliance Assessment
  - Pre-authentication policies act as a gatekeeper, assessing the device's compliance with security standards before allowing it to progress to the authentication phase.

- This proactive evaluation enhances the overall security posture of the remote access environment.
- 

## On the Job Application

- Pre-authentication policies in NetScaler Gateway's access control process evaluate incoming requests to assess the security and compliance of the device.
  - These policies check elements such as antivirus software, patches, firewall settings, and other security configurations. The primary purpose is to ensure that only compliant and secure devices can proceed with authentication.
  - Devices not meeting the criteria might be denied access or redirected to remediation steps, such as updating antivirus definitions or applying necessary patches.
-

# Clip: Planning NetScaler Deployment

---

## Scenario/Challenge

A remote worker needs to access web-based applications and virtual desktops without installing any additional client software. Which NetScaler Gateway deployment option would be most suitable for this situation?

---

When it comes to remote access, selecting the appropriate NetScaler Gateway deployment is crucial to meet specific user needs.

## Choosing the right NetScaler Gateway Deployment for Remote Access

In this section, we will focus on a scenario where a remote worker needs to access web-based applications and virtual desktops without installing any additional client software.

### Clientless Access Deployment

- The most suitable deployment option for this situation is the Clientless Access Deployment.
  - In this deployment, users can access applications and resources without the need to install any additional client software.
    - Users simply use a standard web browser and log in through NetScaler Gateway's user-friendly portal.
- Accessing Web-Based Applications and Virtual Desktops
  - Clientless Access Deployment is particularly useful when users need to access web-based applications or virtual desktops without the hassle of installing specific software.
    - It provides a convenient and straightforward solution for remote workers who prefer accessing resources through a web browser.
- Key Features - Clientless Access Policies
  - Clientless Access Policies are integral to this deployment option.
    - These policies allow users to access certain applications and resources without the need to install any client software.
    - This is especially beneficial in scenarios where users require remote access from unmanaged devices.

---

## On the Job Application

- The most suitable NetScaler Gateway deployment option for a remote worker needing to access web-based applications and virtual desktops without installing additional client software is the Clientless Access Deployment.
  - This deployment allows users to access resources using a standard web browser, eliminating the need for additional client software installations.
  - Clientless Access Policies further enable users to access specific applications and resources without installing any client software, making it ideal for scenarios where remote access is required from unmanaged devices.
  - Implement strong authentication methods, such as multi-factor authentication (MFA), to enhance user verification.
-

# Clip: Integrating Netscaler with Citrix

---

## Scenario/Challenge

An IT administrator is responsible for setting up remote access to Citrix Virtual Apps and Desktops using NetScaler Gateway. They want to ensure that users accessing the gateway via the Workspace app have a smooth experience. What action should they take to achieve this?

---

Setting up remote access to Citrix Virtual Apps and Desktops using NetScaler Gateway requires careful configuration to ensure a smooth experience for users, especially those accessing the gateway via the Workspace app.

## Ensuring a Smooth Experience for Workspace App Users on NetScaler Gateway

In this section, we will focus on the action an IT administrator should take to ensure a smooth experience for Workspace App users on NetScaler Gateway.

### Action to Ensure a Smooth Experience

- Configure Session Policies
  - The key action to ensure a smooth experience for users accessing the gateway via the Workspace app is to configure Session Policies.
    - Session policies play a crucial role in controlling and customizing user sessions based on various parameters.
- Different Expressions for User Connection Evaluations
  - Within Session Policies, IT administrators can create different expressions for user connection evaluations.
    - For example, specific policies can be designed specifically for users accessing the gateway via the Workspace app, tailoring the experience for this user group.
- Customized Policies for Workspace App Users
  - By creating customized policies for Workspace app users, administrators can define specific rules and configurations that optimize the user experience for this connection method.
    - This may include adjusting settings to accommodate features unique to the Workspace app.



- Triggering Session Profiles
    - Session policies, once configured, trigger session profiles.
      - Session profiles define various settings related to user experience, including Single Sign-On (SSO) configurations and the Storefront base URL.
- 

## On the Job Application

- By configuring Session Policies with tailored expressions for user connection evaluations, IT administrators can optimize the user experience for Workspace app users accessing NetScaler Gateway.
  - The session profile can be configured to specify the Storefront base URL for NetScaler Gateway to redirect connections to the Citrix Virtual Apps and Desktops (CVAD) environment.
  - These session policies enable the customization and control of user sessions, allowing the creation of specific policies tailored for users accessing the gateway via the Workspace app.
  - IT administrators can leverage session policies to optimize Single Sign-On (SSO) configurations for Workspace app users.
-

## Clip: Utilizing NetScaler nFactor for Authentication

---

### Scenario/Challenge

A company implemented nFactor authentication with NetScaler Gateway for security, but some employees are experiencing issues during the authentication process and are unable to proceed past a certain step. What should IT support do to address this issue?

---

Implementing nFactor authentication with NetScaler Gateway is a powerful security measure, but sometimes, users may encounter issues during the authentication process.

### Addressing Authentication Issues in nFactor Authentication

In this section, we will explore the steps IT support should take to address authentication issues in nFactor Authentication.

#### Review Authentication Policies

- When users experience issues during the authentication process, the first step for IT support is to review the authentication policies associated with the AAA (Authentication, Authorization, and Auditing) vServer.
    - Identify the specific step in the authentication process where users are getting stuck.
      - Understand the point in the process where users are unable to proceed.
  - Evaluate Authentication policies
    - Authentication policies associated with the AAA vServer are evaluated based on the defined criteria.
      - Examine the policies to ensure they align with the intended authentication flow and security requirements.
  - Modify Policies if necessary
    - If necessary, IT support should modify the authentication policies to address the issues users are facing.
      - Adjust the policies to resolve any conflicts or misconfigurations causing the authentication process to stall.
-

## On the Job Application

- IT support should review the authentication policies bound to the AAA vServer, identify the specific step in the authentication process where users are getting stuck, and modify the policies if necessary. This involves evaluating the policies associated with the authentication policy label, ensuring they align with the intended authentication flow and security requirements.
  - Effectively addressing authentication issues in nFactor authentication with NetScaler Gateway requires a thorough review of authentication policies.
  - For the policies associated with the authentication policy label, evaluate them to identify which ones are true.
  - Actions associated with true policies are executed in order of priority until one of the actions succeeds.
-

# Clip: Planning ADM HDX integration with Netscaler Gateway

---

## Scenario/Challenge

You have set up the integration between ADM and NetScaler Gateway. The Insight column in ADM indicates "Enabled"; however, you do not see any data on the NetScaler ADM dashboard. What aspect of the configuration should you investigate to diagnose the issue?

---

Encountering a situation where the Insight column in ADM indicates "Enabled" but no data is visible on the NetScaler ADM dashboard can be perplexing.

## Troubleshooting Lack of Data on NetScaler ADM Dashboard

This section will walk you through the troubleshooting process to identify and resolve lack of data on the NetScaler ADM dashboard.

### Troubleshooting Steps

- Check Analytics Activation
  - Navigate to the ADM dashboard and locate the virtual servers related to your NetScaler Gateway.
    - Ensure that the "Analytics" feature is activated for these virtual servers.
- License Verification:
  - Confirm that your virtual servers are properly licensed and running.
    - Verify the licensing status of both ADM and NetScaler Gateway.
- Review Delivery Methods
  - Understand the delivery methods for analytics data, i.e., IPFIX protocol or LogStream.
    - Ensure that the chosen method is configured correctly.
    - You can choose between using the IPFIX protocol or the LogStream method for delivery.
- Protocol Configuration
  - If using IPFIX, validate the configuration to export flow-level data for connections.
    - For LogStream, ensure that the Citrix-owned protocol is set up efficiently between NetScaler instances and ADM.

- Check Data Transfer
    - Confirm that there are no issues with data transfer between Netscaler instances and ADM.
      - Inspect logs or error messages related to data transfer.
- 

## On the Job Application

- Enable the "Analytics" feature on ADM for your NetScaler Gateway virtual servers to start collecting data.
  - Ensure that your virtual servers are properly licensed and in an operational state. Analytics can only be enabled on licensed and running virtual servers.
  - Implement a routine monitoring process for ADM and NetScaler Gateway integration. Regularly check analytics data to ensure it aligns with expectations. Update configurations as needed.
  - Ensure that licensing is up to date, and configurations align with best practices.
-

# Clip: Planning EPA

---

## Scenario/Challenge

An organization is using NetScaler Gateway's Endpoint Analysis (EPA) feature to enhance its network security. An employee's laptop fails the Endpoint Analysis scan due to outdated antivirus software and an inadequate OS patch level. What should the organization do to address this issue effectively?

---

NetScaler Gateway's EPA feature is a vital component in enhancing an organization's network security. However, situations may arise where an employee's laptop fails the EPA scan due to issues such as outdated antivirus software and an inadequate operating system (OS) patch level.

## Addressing NetScaler Gateway Endpoint Analysis Scan Failures

This section will help you understand how to effectively address NetScaler Gateway Endpoint Analysis scan failures.

### Understanding Endpoint Analysis Scan

- Before delving into the solution, it's essential to grasp the Endpoint Analysis scan process:
  - The endpoint sends a connection request to the NetScaler Gateway.
    - The NetScaler Gateway server installs the Endpoint Analysis plug-in onto the endpoint.
    - The plug-in evaluates the endpoint's compliance with defined policies.
    - If the endpoint passes all policy checks, access to requested resources is granted. Otherwise, access is denied.
- Granting Temporary Access and Remediation Steps
  - Grant Temporary Access:
    - Since the employee's laptop has failed the EPA scan, grant temporary access to ensure they can continue working.
    - This step is crucial to minimize disruptions while the necessary updates are being applied.



- Redirect to Remediation Steps
    - Direct the employee to remediation steps to update antivirus software and apply necessary OS patches.
      - Provide clear instructions on how to perform these updates to bring the laptop into compliance with security policies.
- 

## On the Job Application

- The Endpoint Analysis tool is a crucial asset in NetScaler Gateway's security strategy. By thoroughly assessing the compliance status of connecting endpoints and enforcing policies, organizations can mitigate security risks and enable secure remote work from any location.
  - When an employee's laptop fails the Endpoint Analysis scan, the organization should promptly grant temporary access to avoid disruptions.
  - Simultaneously, redirect the employee to follow remediation steps to update antivirus software and apply required OS patches. By doing so, the organization ensures that the laptop complies with security policies and remains a secure endpoint within the network.
-

# Clip: Introducing NetScaler Gateway Entities

---

## Scenario/Challenge

An organization is using NetScaler Gateway to provide remote access to their internal resources. They have configured a Virtual Server (vServer) to handle HTTPS traffic, utilized SSL certificates for secure communication, and set up various authentication methods. They also customized the portal theme for a consistent user experience and defined specific rules for application access and traffic management. Given this setup, analyze which of the following scenarios would most likely require a change in the existing configuration of the NetScaler Gateway?

---

NetScaler Gateway plays a pivotal role in providing secure remote access to an organization's internal resources.

## Analyzing NetScaler Gateway Configuration Scenarios

In this section, we will explore the key elements of a NetScaler Gateway configuration and analyze which scenario would most likely require a change in the existing setup.

### Virtual Server (vServer)

- Configured to handle HTTPS traffic, ensuring secure communication.
    - Utilizes SSL certificates for encryption to safeguard data during transmission.
  - Authentication Methods
    - Various authentication methods are supported, including LDAP, RADIUS, SAML, and more.
      - Users must provide valid credentials (username and password) for authentication before accessing internal applications.
  - Customized Portal Theme
    - Theme customization for a consistent and branded user experience.
  - Implementing Two-Factor Authentication
    - This scenario involves a significant change in the authentication method, moving from single-factor (username and password) to two-factor authentication. This change necessitates adjustments in the NetScaler Gateway configuration to accommodate the new security policy.
-

## On the Job Application

- Maintain comprehensive documentation of the NetScaler Gateway configuration, including authentication methods, SSL certificates, portal themes, and access rules. Implement proper change management procedures when modifying configurations.
  - Set up monitoring and alerts to promptly detect and respond to any anomalies or security incidents related to NetScaler Gateway. This includes monitoring authentication logs, SSL certificate status, and system performance.
  - Regular assessments and proactive measures contribute to a robust remote access solution that supports the organization's business objectives.
-

# Clip: Configuring Gateway Virtual Server

---

## Scenario/Challenge

What is the specified IP Address Type for the AAA Vserver used for internal communication in the NetScaler Gateway Virtual Server configuration?

---

In the realm of Netscaler Gateway configuration, the AAA Vserver (Authentication, Authorization, and Accounting Vserver) plays a crucial role in handling internal communication.

## Understanding NetScaler Gateway AAA Vserver Configuration

This section will help you understand the specified IP Address Type for the AAA Vserver used in the NetScaler Gateway Virtual Server configuration.

### AAA Vserver

- The AAA Vserver is a critical component responsible for Authentication, Authorization, and Accounting functions within the NetScaler Gateway.
    - It is configured to manage user access, permissions, and track user activities for internal communication purposes.
  - IP Address Type
    - When configuring the AAA Vserver, one key parameter to consider is the "IP Address Type."
      - Since this AAA Vserver will be used for internal communication, the 'IP Address Type' can be set as 'Non Addressable'.
-

## On the Job Application

- The AAA Vserver in NetScaler Gateway configuration is used for handling authentication, authorization, and accounting (AAA) functions.
  - Choose a meaningful and easily identifiable name for the AAA Vserver during configuration.
  - Familiarize yourself with the NetScaler Gateway management console to efficiently locate and configure the AAA Vserver.
  - Configure monitoring and logging features to track AAA Vserver activities. This helps in troubleshooting and security analysis.
-

# Clip: Introducing NetScaler Gateway Entities

---

## Scenario/Challenge

What is the purpose of setting up a server certificate for the Gateway Virtual Server in the NetScaler admin console?

---

In the administration console of NetScaler Gateway, establishing a server certificate for the Gateway Virtual Server is essential to guarantee a secure access point for users. This section aims to enhance your comprehension of the significance of this setup.

## Importance of Server Certificate for NetScaler Gateway Virtual Server

### Understanding the Context

- Learn about Virtual Servers: Understand that a Virtual Server (vServer) in NetScaler Gateway serves as the access point for users to securely connect to internal resources.
    - Recognize that a vServer listens for incoming connections and directs traffic based on configured policies.
  - Secure Communication with Certificates: Importance of Certificates
    - Acknowledge that certificates play a crucial role in securing the communication between users and the NetScaler Gateway.
    - Understand that NetScaler Gateway uses SSL certificates to encrypt data, ensuring a secure and encrypted communication channel between clients (users) and the gateway.
  - Certificate Configuration: Familiarize yourself with the steps to configure SSL certificates for the NetScaler Gateway Virtual Server. This may involve importing, installing, and associating the certificate with the vServer.
    - Implement security best practices in certificate management, such as using strong encryption algorithms and regularly updating certificates.
-



## On the Job Application

- SSL certificates are crucial for securing communication between users and the NetScaler Gateway. They encrypt data to ensure a secure and private connection.
  - Setting up a server certificate for the Gateway Virtual Server enables encryption, contributing to a secure communication channel between clients and the gateway.
  - Keep the NetScaler Gateway software up-to-date to benefit from the latest security enhancements and features.
  - Before making changes to certificate configurations or other settings, create backups to facilitate quick restoration in case of issues.
-

# Clip: Configuring Gateway Virtual Server

---

## Scenario/Challenge

As a network administrator, you are reviewing the steps that one of the IT specialists is planning to take when setting up a Gateway Virtual Server in the NetScaler admin console. Identify the mistake in the setup process.

---

As a network administrator, reviewing and understanding the configuration steps for setting up a Gateway Virtual Server in the NetScaler admin console is crucial.

## AAA Vserver

This section aims to assist you in grasping the context and pinpointing any errors for setting a Gateway Virtual Server.

### Review the IP Address Type

- When configuring the AAA Vserver, a key parameter to consider is the "IP Address Type."
    - Pay close attention to the configuration of the "IP Address Type" for the "AAA Vserver" during the setup process.
      - The recommended IP Address Type for the AAA Vserver used in the Netscaler Gateway Virtual Server configuration is 'Non Addressable'.
  - Additional Considerations
    - While correcting the mistake, also ensure that other configurations align with best practices and the intended use of the AAA Vserver.
    - Configuring an IP address for authentication on an AAA vServer is optional and not required.
-

## On the Job Application

- Whenever possible, conduct lab testing of configurations to validate their functionality and identify potential issues before deploying changes in a production environment.
  - When a mistake is identified, take prompt corrective action to ensure that configurations align with recommended settings.
  - Always refer to reliable sources, documentation, or best practices when reviewing or validating configuration steps.
-

# Clip: Utilizing NetScaler nFactor for Authentication

---

## Scenario/Challenge

Scenario: You are a network administrator tasked with setting up a NetScaler Gateway Virtual Server following the steps outlined in the video. You named the Virtual Server "external\_gateway," configured it with an IP address, set up a server certificate, and added LDAP authentication. After completing the basic configuration, you are considering additional security measures. Question: Based on the current setup of the NetScaler Gateway Virtual Server, which of the following actions would most effectively enhance the security of the server?

---

Now that you have completed the foundational setup tasks for a NetScaler Gateway Virtual Server, including defining an IP address, configuring a server certificate, and implementing LDAP authentication, the next step is to enhance security.

## Enhancing NetScaler Gateway Virtual Server Security

This section is intended to offer insights and guidance for effectively enhancing security.

### Identify Security Enhancement Options

- Consider Additional Security Measures: Acknowledge that there is a need for additional security measures beyond the basic setup.
    - Understand that the question is asking for the most effective action to enhance the security of the NetScaler Gateway Virtual Server.
  - Understand the Importance of Multi-Factor Authentication (MFA): Understand that NetScaler provides nFactor authentication as a flexible and extensible approach to configuring multi-factor authentication.
    - Recognize the nFactor visualizer as a GUI feature that allows administrators to link factors or policy labels together, creating dynamic authentication flows based on user profiles.
-

## On the Job Application

- Familiarize yourself with the benefits of multi-factor authentication in providing an additional layer of security beyond traditional authentication methods.
  - Explore NetScaler documentation to understand how to configure nFactor authentication and its integration with multi-factor authentication methods.
  - If possible, practice implementing multi-factor authentication in a lab environment to gain hands-on experience.
  - Regularly review NetScaler documentation for updates and best practices related to security configurations.
-

# Clip: Introducing NetScaler Gateway Entities

---

## Scenario/Challenge

Considering the configuration process for NetScaler Gateway Virtual Server outlined in the video, analyze the potential consequences of omitting the step related to setting up a server certificate.

---

In the configuration process for a NetScaler Gateway Virtual Server, the step related to setting up a server certificate is crucial for ensuring secure communication between users and the NetScaler Gateway.

## Importance of Setting up a Server Certificate for NetScaler Gateway Virtual Server

This section explores the importance of setting up a Server Certificate for NetScaler Gateway Virtual Server.

### Analyzing Consequences

- Connection Errors: Omitting the step related to setting up a server certificate may result in users encountering connection errors.
    - SSL certificates play a pivotal role in encrypting data during communication, and without a valid certificate, the connection between users and the NetScaler Gateway may fail.
  - Security Compromises: The absence of a server certificate compromises the security of login access points.
    - Certificates establish a secure and encrypted channel, preventing unauthorized access and protecting sensitive user credentials during login.
-



## On the Job Application

- Follow the configuration process diligently and ensure that setting up a server certificate is part of the NetScaler Gateway Virtual Server setup.
  - Use a valid SSL certificate obtained from a trusted Certificate Authority (CA) to enhance security.
  - Implement a practice of regularly updating and renewing SSL certificates.
  - Expired or outdated certificates may lead to disruptions in service and potential security vulnerabilities.
  - Set up monitoring mechanisms to receive alerts on impending certificate expirations.
-

# Clip: Configuration for Session policy for Web, Traffic, and STA

---

## Scenario/Challenge

Which statement accurately describes the purpose of the traffic policy for Single Sign-on (SSO) in the NetScaler configuration?

---

In the NetScaler configuration, understanding the purpose of the traffic policy for SSO is crucial for seamless user experiences.

## Understanding the Purpose of NetScaler Traffic Policy for SSO

This section provides insights into the statement that accurately describes the role of the traffic policy for SSO.

### Introduction:

- **Facilitating Secure Communication:** The traffic policy for Single Sign-on ensures secure communication between NetScaler Gateway and Storefront.
    - Security is paramount in SSO, and the traffic policy establishes a protected channel for passing user credentials.
  - **Eliminating Credential Redundancy:** The primary goal of the traffic policy is to eliminate the need for users to re-enter credentials.
    - Users connect to NetScaler Gateway, and the traffic policy facilitates the seamless transmission of their credentials to Storefront.
    - It emphasizes the role of the traffic policy in ensuring that NetScaler Gateway securely communicates with Storefront, thereby preventing the redundancy of user credential input.
-

## On the Job Application

- When creating the traffic policy for Single Sign-on, set the expression as "True" to make it applicable to all users.
- This ensures that the SSO functionality covers the entire user base.
- Periodically review and update traffic policies to align with changes in the network environment.
- Stay informed about updates and improvements in NetScaler configurations to enhance SSO capabilities.

# Clip: Configuration for Session policy for Web, Traffic, and STA

---

## Scenario/Challenge

Which step is crucial for the configuration of the session policy for web browsers in the NetScaler Gateway setup?

---

Configuring a session policy for web browsers in the NetScaler Gateway setup is a critical step for enabling seamless and secure access.

## Crucial Steps for Configuring NetScaler Gateway Session Policy for Web Browsers

This section outlines the crucial steps for configuring NetScaler Gateway Session Policy for web browsers, focusing on adding the FQDN of the StoreFront server and the Store path."

### Key Configuration Steps

- Enable ICA Proxy: Under "Session Profile > Published Applications", set "ICA Proxy" to "ON."
    - This setting is crucial for ensuring proper ICA (Independent Computing Architecture) proxy functionality.
  - Specify FQDN and Store Path: Add the FQDN (Fully Qualified Domain Name) of the Storefront server.
    - Include the path to the Store under "Published Applications," for example, <https://storefront.domain.lab/Citrix/StoreWeb>.
    - This step is essential for directing the NetScaler Gateway to the correct Store and facilitating access to published applications.
  - Configure Single Sign-On Domain: Add your domain under "single sign-on domain."
    - This setting contributes to a streamlined Single Sign-On (SSO) experience for end-users.
-

## On the Job Application

- Periodically review and update session policies to align with changes in the network environment.
  - Stay informed about updates and improvements in NetScaler configurations.
  - Validate the session policy by testing it with various web browsers to ensure compatibility.
  - Address any issues related to web browser access during the testing phase.
  - Enable "ICA Proxy" under "Published Applications" to ensure proper ICA proxy functionality.
-

# Clip: Configuration for Session policy for Web, Traffic, and STA

---

## Scenario/Challenge

What is a characteristic of the session policy created for web browsers on NetScaler Gateway?

---

Understanding the characteristics of a session policy for web browsers on NetScaler Gateway is crucial for optimizing user experience and security.

## Characteristics of NetScaler Gateway Session Policy for Web Browsers

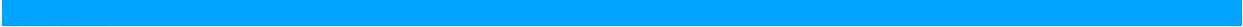
This section provides insights into the key characteristics, focusing on the settings related to "Split Tunnel" and "Clientless Access."

### Characteristic Details

- Session Profile Configuration: Navigate to the session profile configuration in NetScaler Gateway.
    - Within the session profile, find the "Client Experience" tab.
    - The session profile allows administrators to override global NetScaler Gateway parameters for specific configurations.
  - Client Experience Settings: Under the "Client Experience" tab, locate the following settings:
    - Set "Split tunnel" to "Off." This configuration choice has implications for the routing of network traffic during the VPN session.
    - With "Split Tunnel" set to "Off," all traffic, including internet-bound traffic, is routed through the VPN tunnel.
    - Set "Clientless Access" to "On." This setting enables a clientless VPN access mode, allowing users to access specific applications or resources without requiring a VPN client installation.
-



## On the Job Application

- The characteristics of the session policy for web browsers on NetScaler Gateway, particularly the settings for "Split Tunnel" and "Clientless Access," play a significant role in defining the user experience and security parameters.
  - "Split Tunnel" is set to "Off" in the session policy, directing all traffic through the VPN tunnel.
  - "Clientless Access" is set to "On," enabling a clientless VPN access mode for specific applications.
  - Evaluate security implications and align settings with organizational network policies.
- 

# Clip: Configuring policies for CWA

---

## Scenario/Challenge

As a network administrator, you are reviewing the setup of session and traffic policies on a NetScaler Gateway. Identify the issue in the process that needs correction.

---

As a network administrator, reviewing and correcting session and traffic policies on a NetScaler Gateway is a crucial task to ensure a seamless and secure user experience. In this section, we will identify and address a specific issue in the process.

## Session and Traffic Policies on NetScaler Gateway

In this section, we will identify and address a specific issue related to Session and Traffic Policies on NetScaler Gateway.

### Identifying the Issue

- Session Policy Overview: Session policies control user access, providing a customized and secure environment.
  - Expression Creation for Web Browsers: When creating session policies for web browsers, it's essential to accurately define conditions for the policy to evaluate as "TRUE."
    - In this scenario, an expression was created in the "Expression Editor" to evaluate the policy as "TRUE" for users accessing via web browsers.
  - Expression Editor Configuration: Access the "Expression Editor" and configure the expression to evaluate correctly.
    - The expression uses the "HTTP" "REQ" "HEADER" and focuses on the "User-Agent" header.
  - Identifying the Issue: The issue lies in the header value specified in the expression, which is "CitrixReceiver."
    - "CitrixReceiver" is specific to the Citrix Workspace App (CWA) and is not a standard value for web browsers.
-

## On the Job Application

- Choose appropriate values in the "User-Agent" header that are indicative of web browsers.
  - Avoid including values that are specific to Citrix Workspace App unless intended for a separate session policy.
  - After modifying the expression, thoroughly test and validate the session policy.
  - Confirm that the policy correctly identifies users accessing via web browsers.
-

# Clip: Integrating NetScaler with Citrix

---

## Scenario/Challenge

As a network administrator, you configured a session policy for web browsers and a traffic policy for Single Sign-On (SSO) on NetScaler Gateway. You also set up and bound an STA server to the Gateway Virtual servers and ensured that the session policy for web browsers evaluates to true for clients using any web browser, and the traffic policy for SSO is applicable for all users. Which of the following scenarios would most likely require additional adjustments to the existing setup of the NetScaler Gateway?

---

As a network administrator, the setup of NetScaler Gateway requires the establishment of session and traffic policies customized to needs.

## Optimizing NetScaler Gateway Policies

In this section, we will explore the essential aspects of optimizing NetScaler Gateway policies, identifying potential adjustments for enhanced configuration.

### Configuration Overview

- As a network administrator, you have undertaken the task of configuring NetScaler Gateway for secure remote access. The setup involves a session policy for web browsers, a traffic policy for Single Sign-On (SSO), and the establishment of an STA server bound to the Gateway Virtual servers.
    - In this scenario, the session policy for web browsers evaluates to true for clients using any web browser, and the traffic policy for SSO is applicable for all users. The STA server is properly configured to facilitate secure communication.
      - The most likely scenario requiring additional adjustments is when there's a need to "enforce more stringent security protocols for user authentication."
  - Learn about ICA Proxy
    - Refer to the provided source to understand how ICA Proxy in Netscaler Gateway ensures data encryption, authentication, and secure transport of ICA traffic.
      - Understand the importance of Virtual Server setup, Session Policy and Profile for user access, optimal STA functioning, and Storefront configuration in maintaining a secure Citrix environment.\
-

## On the Job Application

- Understand that while the initial setup covers essential components, fine-tuning may be necessary to meet specific security requirements.
  - Recognize that a well-configured NetScaler Gateway ensures a smooth remote access experience for users accessing virtual applications and desktops.
  - Consider implementing continuous monitoring to identify any evolving security needs and adapt the NetScaler Gateway configuration accordingly.
-

# Clip: Configuring policies for CWA

---

## Scenario/Challenge

What action should be taken in the "Security" tab of the session profile configuration for Citrix Workspace App users in NetScaler Gateway?

---

As a learner, understanding the configuration settings for Citrix Workspace App users in NetScaler Gateway is essential.

## Configuring Security Settings for Citrix Workspace App Users

This section will guide you on configuring security settings for Citrix Workspace App Users.

### Accessing Session Profile Configuration

- Access Session Profile Configuration: Look for the "Security" tab within the session profile configuration, next to "Client Experience."
    - Within the "Security" tab, find the setting related to "Default Authorization Action." This setting controls the default action taken if no specific authorization policy matches.
- 

## On the Job Application

- Configuring security settings for Citrix Workspace App users in NetScaler Gateway is crucial for maintaining a secure environment.
  - Keep NetScaler Gateway software up-to-date to benefit from the latest security enhancements and bug fixes.
  - Periodically conduct security audits to assess the effectiveness of the configured security settings and identify areas for improvement.
-



# Clip: Configuring policies for Citrix Workspace App (CWA)

---

## Scenario/Challenge

As an IT administrator, you are in the process of configuring session policies on NetScaler Gateway for different types of users. What step should you take to correctly set up the session policy for users accessing via the CWA?

---

As an IT administrator configuring session policies on NetScaler Gateway, you are tasked with setting up a session policy specifically for users accessing via the CWA.

## Configuring Session Policies for CWA Users

This session guides you on how to configure session policies for CWA users.

### Access NetScaler Console

- Open your web browser and log in to the NetScaler Gateway console using your administrator credentials.
    - In the NetScaler console, go to "NetScaler Gateway," then select "Policies," and click on "Session."
  - Initiate Session Policy Creation
    - Click on "Add" to create a new session policy. For CWA users, name it "session\_policy\_CWA" and proceed.
  - Create Session Profile
    - In the session profile configuration, name it "session\_profile\_CWA."
    - Under the "Client Experience" tab:
      - Set "Split Tunnel" to "Off."
      - Enable "Clientless Access."
      - Set "Plugin-in Type" as "Java."
      - In "Published Applications," turn on "ICA Proxy" and add the StoreFront server's FQDN under "Web Interface Address."
      - Include the NetBIOS name for the domain under "Single Sign-on domain."
      - Enter the account services address, typically the StoreFront URL.
-

## On the Job Application

- Session policies on NetScaler Gateway are rules that control how users access and interact with the gateway, allowing customization of user experiences and enforcing security measures.
  - Different session policies can be created for users accessing the gateway via Citrix Workspace App (CWA) and web browsers to cater to specific client types.
  - Understand the use of expressions for evaluating policies. In this scenario, an expression based on the User-Agent header is created to identify CitrixReceiver.
  - Anticipate the need for additional session policies for users accessing via web browsers and be prepared to create and bind these policies when required.
-

# Clip: Integrating NetScaler with Citrix

---

## Scenario/Challenge

As an IT specialist, you created a session policy for users accessing the NetScaler Gateway via the Citrix Workspace App. You named the policy "Session\_policy\_CWA," set up various parameters like Split Tunnel, Clientless Access, and Plugin-in Type, and configured the policy to apply when the "CitrixReceiver" user-agent is detected. Now, you are preparing to deploy this configuration in your organization's network. Given the specifics of the "Session\_policy\_CWA" configuration, which of the following situations would most likely require a review or modification of this policy?

---

By following this section, you are well-equipped to review and modify the session policies based on the specifics of your organization's network and user requirements. By implementing these steps and best practices, you can ensure the effective deployment and ongoing optimization of session policies for users accessing NetScaler Gateway through the Citrix Workspace App.

## Reviewing and Modifying Session Policy for Citrix Workspace App Users

This section guides users through the process of reviewing and modifying session policies for Citrix Workspace App users.

### Understand the Deployment Basics

- Key Components Overview: NetScaler Gateway, using Independent Computing Architecture (ICA) Proxy, provides secure access for users to virtual apps and desktops.
  - The Virtual Server in NetScaler Gateway represents the external-facing interface and handles ICA traffic securely. Verify details like IP address, port, and secure communication settings.
  - Session policies control user sessions, with specific expressions for connection evaluations. Confirm that the Session Policy aligns with the user experience goals, especially when users connect via Citrix Workspace App.
  - The STA exchanges CVAD server information for tickets, ensuring secure and authenticated access. Confirm that the STA setup, including information about one or more STA servers, is accurate.

- Potential Situation for Review: Mobile Device Access Issues
    - Users reporting issues in accessing resources when connecting through mobile devices using the Citrix Workspace App may indicate a need for a review or modification of the Session Policy for CWA
    - Ensure compatibility and optimal performance for users on mobile devices.
- 

## On the Job Application

- Regularly monitor user feedback and performance metrics to identify potential issues promptly.
  - Storefront manages and organizes accessible apps and desktops. Check that the NetScaler Gateway URL, authentication methods, and STA server details are correctly configured on the Storefront server.
  - Collaborate with users to gather insights into their experiences and identify specific issues related to mobile device access.
-

# Clip: Configuring policies for CWA

---

## Scenario/Challenge

What information is entered in the "Single Sign-on domain" field under the session profile for NetScaler Gateway?

---

As a learner, understanding the specific information to be entered in the "Single Sign-on domain" field under the session profile for Netscaler Gateway is crucial.

## Introduction to Session Profile Configuration

This section serves as an introduction to session profile configuration.

### Session Profile Purpose

- Session profiles in NetScaler Gateway control and customize user sessions, allowing administrators to tailor user experiences and enforce security measures.
    - Role of "Single Sign-on domain"
      - The "Single Sign-on domain" field is a critical component in the session profile configuration. It plays a significant role in facilitating Single Sign-On (SSO) to Storefront when LDAP authentication is used.
  - Entering NetBIOS Name
    - When configuring the session profile, navigate to the "Single Sign-on domain" field under the "Published Applications" section.
      - Enter the NetBIOS name for the domain in this field.
      - The NetBIOS name is essential for establishing Single Sign-On (SSO) functionality to Storefront.
-

## On the Job Application

- After entering the NetBIOS name in the "Single Sign-on domain" field, ensure to apply and save the changes to the session profile configuration.
  - Regularly consult the NetScaler Gateway documentation for comprehensive information on session profile configuration and best practices.
  - After entering the NetBIOS name, conduct testing to ensure that Single Sign-On (SSO) to Storefront is functioning as expected.
-



# Clip: Configuring policies for CWA

---

## Scenario/Challenge

As a network administrator, you have successfully configured session policies for Citrix Workspace App (CWA) and web browsers, as well as a traffic policy for Single Sign-On (SSO) on the NetScaler Gateway. You have also bound an STA server to the Gateway Virtual servers. This setup is intended to streamline user access and enhance security. After implementing these configurations, which of the following scenarios would most likely require further modifications to the NetScaler Gateway's session and traffic policies?

---

As a network administrator, you have successfully configured session policies for CWA and web browsers, along with a traffic policy for SSO on NetScaler Gateway.

## Evaluating NetScaler Gateway Session and Traffic Policies

In this section, we will explore scenarios where further modifications to the NetScaler Gateway's session and traffic policies may be required.

### Understanding the Configuration

- Session Policy Overview: Session policies control user access and interaction with NetScaler Gateway, allowing customization of user experiences and enforcing security measures.
  - Configuration for CWA Users: Create a session policy.
    - Configure specific settings for the session profile
    - Implement Single Sign-On (SSO) to web applications
  - Identifying the Need for Modification: Review and Modify Policies
    - In response to the organization's decision for additional authentication, administrators may need to review and modify existing session and traffic policies on NetScaler Gateway.
-

## On the Job Application

- Collaborate with the organization's security teams to ensure alignment with security policies when implementing additional authentication layers.
  - Regularly refer to the NetScaler Gateway documentation for comprehensive information on session and traffic policies.
  - By staying informed and proactive, network administrators can efficiently adapt NetScaler Gateway configurations to meet evolving security requirements and ensure a secure and streamlined user access experience.
-

# Clip: Introducing ADM HDX Insight

---

## Scenario/Challenge

What is one of the key functionalities of Application Delivery Management (ADM) HDX Insight?

---

ADM HDX Insight is a powerful tool that provides in-depth insights into application performance within Citrix environments. To understand one of its key functionalities, particularly in the context of network latency, let's explore the concept of L7 latency reporting.

## Understanding ADM HDX Insight Functionality

This section is dedicated to understanding the functionality of ADM HDX Insight.

### Granular ICA Traffic Monitoring

- ADM HDX Insight goes beyond just monitoring – it provides granular ICA traffic monitoring.
    - This means it captures detailed information about the Independent Computing Architecture (ICA) traffic, which is essential for Citrix environments.
  - Comprehensive Application Visibility and Control: HDX Insight ensures comprehensive application visibility and control.
    - It allows administrators to have a clear understanding of how applications are performing, ensuring a proactive approach to addressing potential issues.
  - Efficient Management Capabilities: ADM HDX Insight doesn't require expensive data collections or storage infrastructure.
    - It comes equipped with efficient management capabilities, saving both time and resources for administrators.
  - L7 Latency Reporting: ADM HDX Insight doesn't require expensive data collections or storage One of the key functionalities of ADM HDX Insight is L7 latency reporting.
    - L7 refers to Layer 7 of the OSI model, which is the application layer. L7 latency reporting provides insights into end-to-end network latency for both client and server networks.
-

## On the Job Application

- The insights provided by HDX Insight are actionable.
  - Administrators can use these insights to identify the root causes of application slowdowns or issues, enabling them to take proactive measures before they impact users.
  - HDX Insight can further enhance its capabilities by joining forces with Enlighted Data Transport (EDT) traffic reporting.
  - Even in scenarios where Receiver and Gateway are in different networks or organizations, ADM HDX Insight excels with its outbound ICA proxy deployment.
-

# Clip: Introducing ADM HDX Insight

---

## Scenario/Challenge

Which statement best captures the role and capabilities of ADM HDX Insight in enhancing application performance?

---

ADM HDX Insight plays a crucial role in navigating the complex landscape of modern app delivery. To comprehend its significance and capabilities in enhancing application performance, let's delve into its key features.

## Understanding the Role of ADM HDX Insight

This section is dedicated to understanding the role of ADM HDX Insight.

### Key Role and Capabilities:

- **Granular ICA Traffic Monitoring:** ADM HDX Insight provides granular ICA traffic monitoring, offering a detailed view of the Independent Computing Architecture (ICA) traffic within Citrix environments.
  - This level of monitoring allows organizations to gain insights into how applications are performing and identify potential issues.
- **Comprehensive Application Visibility and Control:** The tool ensures comprehensive application visibility and control.
  - Organizations can manage and optimize the performance of their applications, ensuring a seamless and delightful user experience.
- **Efficient Management Capabilities:** ADM HDX Insight is designed with efficient management capabilities, eliminating the need for expensive data collections or storage infrastructure.
  - This efficiency saves both time and resources, making it a valuable asset for organizations.
- **Actionable Insights:** The tool goes beyond mere observation; it provides actionable insights.
  - Administrators can proactively address issues by understanding the root causes of application slowdowns, fostering optimal app experiences.
- **L7 Latency Reporting:** One of the key functionalities of ADM HDX Insight is L7 latency reporting.
  - Operating at Layer 7 of the OSI model (the application layer), this reporting provides a clear picture of end-to-end network latency for both client and server networks.

- **User Experience Improvement:** By offering granular monitoring, application visibility, efficient management, and L7 latency reporting, ADM HDX Insight contributes significantly to improving the user experience.
    - It ensures that applications accessed through Citrix Virtual Apps and Desktops work seamlessly, leading to user delight.
- 

## On the Job Application

- By combining granular monitoring, application visibility, efficient management, and latency reporting, ADM HDX Insight contributes significantly to enhancing the overall user experience.
  - One of its key functionalities is L7 latency reporting, offering a clear picture of end-to-end network latency for both client and server networks.
  - Schedule regular reviews of the insights provided by ADM HDX Insight to stay proactive in addressing any potential issues affecting application performance.
  - Leverage the actionable insights gained from HDX Insight to make informed decisions about optimizing application delivery and user experiences.
-



# Clip: Planning ADM HDX integration with NetScaler Gateway

---

## Scenario/Challenge

You are an IT administrator tasked with integrating ADM HDX with the NetScaler Gateway to monitor Citrix Virtual Apps and Desktops traffic. Which actions would you take in this situation?

---

As an IT administrator tasked with integrating Citrix ADM HDX with NetScaler Gateway for monitoring Citrix Virtual Apps and Desktops traffic, you'll need to follow specific steps to ensure a seamless integration. In this section, we will list the key actions you should take in this situation.

## Integrating ADM HDX with NetScaler Gateway for Citrix Monitoring

This section provides guidance on integrating ADM HDX with NetScaler Gateway for Citrix monitoring, offering step-by-step instructions, configurations.

### Integrate ADM HDX with NetScaler Gateway

- Ensure that your Citrix Application Delivery Management (ADM) is set up and ready to manage and monitor your Citrix infrastructure.
  - Add the NetScaler instance that you want to manage within ADM. You can do this during the initial setup of the NetScaler ADM server or at a later stage.
- Create an Instance Profile
  - The crucial step in this integration is to create an instance profile. An instance profile serves as a package of information, including the necessary details for accessing the NetScaler instance.
  - These details typically include:
    - Username
    - Password
    - Communication ports
    - Authentication types

- Instance Profile Specifics
    - Consider the default profile for each instance type, such as 'nsroot' for NetScaler instances. This default profile may use the default admin credentials.
      - If you have changed the instance credentials, you will need to create custom instance profiles.
      - Keep in mind that if you change instance credentials after the initial discovery, you'll need to edit or create a profile and then rediscover the instance.
- 

## On the Job Application

- Ensure that your Citrix ADM is properly set up before attempting to integrate it with NetScaler Gateway.
  - Use ADM to add the specific NetScaler instances that you want to manage and monitor within your Citrix environment.
  - The critical step in the integration process is to create an instance profile in ADM.
  - This profile contains essential details such as username, password, communication ports, and authentication types for the NetScaler instance.
-

# Clip: Planning Endpoint Analysis

---

## Scenario/Challenge

As an IT Security Manager, you have been tasked with utilizing the EPA feature of NetScaler Gateway to enhance the network security of your organization. Which of the following actions would you take to apply EPA effectively in your network environment?

---

As an IT Security Manager tasked with enhancing the network security of your organization using the EPA feature of NetScaler Gateway, understanding how to configure and apply EPA effectively is crucial.

## Utilizing EPA in NetScaler Gateway for Enhanced Network Security

This section provides steps and recommendations to help you leverage EPA for a more secure network environment.

### Understand EPA's Role

- EPA serves as a security framework within NetScaler Gateway, analyzing endpoints to ensure they meet specific security requirements before granting access to applications and resources.
    - Focus on implementing pre-authentication policies that assess the security and compliance of devices before allowing access.
      - Criteria for assessment may include antivirus software status, firewall settings, patch levels, and other security configurations.
  - Configure Criteria for Compliance
    - Use the NetScaler Gateway's Policy Manager to define a set of policies that endpoints must adhere to before gaining access.
      - Criteria for compliance checks should cover aspects like antivirus status, OS patch level, and other security-related factors.
  - EPA Components
    - Understand the key components of EPA, including the EPA Plug-in installed on connecting endpoints, policies configured in the NetScaler Gateway's policy manager, and the Expression Editor for creating compliance criteria.
-

## On the Job Application

- Familiarize yourself with the Expression Editor, a tool that enables administrators to create and edit expressions defining criteria for compliance checks.
  - Expressions play a crucial role in specifying the conditions that endpoints must meet to be considered compliant.
  - Acknowledge the role of post-authentication policies, which come into play after successful user login.
  - Recognize that by thoroughly assessing compliance status and enforcing policies, EPA helps mitigate security risks, ensuring secure remote work from any location.
-

# Clip: Planning Gateway VPN Connection

---

## Scenario/Challenge

You have tasked an IT administrator with setting up a NetScaler Gateway VPN connection. Select the statement that will best demonstrate their understanding about the functions and considerations involved in setting up a NetScaler Gateway VPN connection for remote access?

---

Setting up a NetScaler Gateway VPN connection for remote access involves considerations and prerequisites to ensure a secure and seamless experience for users.

## Setting Up NetScaler Gateway VPN Connection for Remote Access

This section will help the IT administrator understand the functions and considerations involved in establishing a NetScaler Gateway VPN connection for remote access.

### Understanding NetScaler Gateway VPN Connection

- A NetScaler Gateway VPN connection is a secure and remote access solution enabling users to connect to the organization's network from remote locations via the Internet.
  - It provides secure access to corporate resources such as applications, files, and internal websites.
- Prerequisites for Full VPN Mode
  - Before implementing NetScaler Gateway Full VPN, consider the following prerequisites for a secure and seamless remote access experience:
    - Assess organizational requirements, including the number of remote users, network architecture, types of applications/resources needed, and existing security policies.
    - Place NetScaler in a DMZ for an additional layer of security between the internet and the internal network.
- Choosing Deployment Modes
  - NetScaler Gateway offers two deployment modes, each serving specific purposes:
    - Full VPN Mode: Routes all network traffic from the remote user's device through NetScaler Gateway, ensuring the security of all internet-bound traffic.

- Clientless VPN Mode: Allows users to access specific applications and resources without a full VPN connection. Ideal for granting access to web applications without routing all traffic through the VPN.
  - Considerations for Full VPN Mode
    - In Full VPN mode, all user traffic is routed through NetScaler Gateway, providing a comprehensive and secure connection.
      - Assess the organization's needs for full traffic routing, considering factors such as data sensitivity, security policies, and the nature of applications accessed remotely.
  - Considerations for Clientless VPN Mode
    - Clientless VPN mode is suitable for scenarios where routing all traffic through the VPN is not necessary.
      - It allows access to specific applications and resources without the need for a full VPN connection, providing a more targeted approach.
- 

## On the Job Application

- Before implementing NetScaler Gateway VPN, assess the organization's requirements, including the number of remote users, network architecture, and types of applications/resources needed.
  - Placing NetScaler in a DMZ enhances security by creating an additional layer of protection between the internet and the internal network.
  - The NetScaler Gateway VPN can operate in either Full VPN mode, routing all user traffic through the Gateway, or Clientless VPN mode, which is used for specific applications without a full VPN connection.
-



# Clip: Planning Endpoint Analysis

---

## Scenario/Challenge

As a network administrator, you are setting up a NetScaler Gateway VPN for your organization to facilitate secure remote access for employees. Which of the following actions would you take to effectively apply these principles in your setup?

---

As a network administrator tasked with setting up a NetScaler Gateway VPN for secure remote access, it is crucial to follow key principles and conduct a thorough analysis to ensure a seamless and secure deployment.

## Setting Up NetScaler Gateway VPN

This section guides users through the process of setting up NetScaler Gateway VPN.

### Steps to Effectively Apply Principles

- **Network Architecture:** Understand your organization's network architecture to determine where NetScaler Gateway should be placed. Consider implementing it in a DMZ for added security.
    - **Number of Remote Users:** Assess the number of remote users who will utilize the VPN. This information is critical for capacity planning and resource allocation.
    - **Types of Applications:** Identify the types of applications remote users need to access. This will influence the choice of VPN deployment mode.
    - **Existing Security Policies:** Review and align with existing security policies. Ensure that the chosen VPN mode complies with organizational security standards.
  - **Prerequisites:** Ensure that the organization's prerequisites are met:
    - Evaluate network requirements, such as bandwidth and latency, to provide optimal performance.
    - Verify that the organization's security policies align with the chosen VPN deployment mode.
  - **Security Measures:** Implement additional security measures as needed.
    - Configure firewall rules to restrict unauthorized access.
    - Regularly update and patch NetScaler Gateway to address potential vulnerabilities.
-

## On the Job Application

- Conduct a comprehensive analysis of network architecture, remote user numbers, application requirements, and existing security policies before implementing NetScaler Gateway VPN.
  - Understand the differences between Full VPN and Clientless VPN modes and choose the mode that aligns with the organization's security, performance, and access requirements.
  - Align authentication methods with security requirements and compliance standards. Consider multifactor authentication for enhanced security.
  - Implement regular security measures, such as firewall rules and timely updates, to enhance the overall security of the NetScaler Gateway VPN.
-



**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**

# NetScaler Lab Guide

**Disclaimer:** In partnership with Layer 8 Training, NetScaler Self-Paced Online Labs (SPO) are now available for purchase to customers and partners. These hands-on lab exercises are configured and managed by Layer 8 Training, a global provider of authorized Citrix and NetScaler training content. The lab library is designed to align with the free learning content available on Pluralsight. The SPO lab store can be found at this [site](#). Click [here](#) to access the price sheet for the NetScaler Self-Paced Online Labs.

For more details visit: <https://www.citrix.com/training-and-certifications/>

If you prefer not to purchase the SPO labs, you may proceed by following the instructions in the lab guide below to practice in your own environment setup.



Version 2.0



## Introduction to NetScaler Administrator Lab Guide

The NetScaler Administrator Lab Guide aligns with the NetScaler Administrator Academy, equipping participants with essential skills for efficient NetScaler administration. It covers core topics, enabling a deep understanding of key concepts and effective execution of configurations for optimal application delivery.

We understand that you have already chosen the type of environment for your NetScaler deployment, whether on-premises or in the public cloud. Below, you will find the minimum required NetScaler resources for your selected configuration.

---

**Note:**

1. The guide does not provide instructions for creating machines, whether on-premises or in the cloud.
  2. As a best practice, we advise using an IP tracking tool or spreadsheet to oversee and manage all the IPs required throughout the entirety of this guide.
-

NetScaler VPX for on-premises CPU and Memory requirement								
Model	Minimum Memory *	vCPUs	Minimum Disk size	Vmware ESXi	Linux KVM	Citrix XenServer	MS Hyper-V	Recommended Network Driver
VPX 200	4 GB	2	20 GB	✓	✓	✓	✓	VMXNET3 or paravirtualization
VPX 1000	4 GB	2-4	20 GB	✓	✓	✓	✓	VMXNET3 or paravirtualization
VPX 3000	4 GB	2-4	20 GB	✓	✓	✓	✓	VMXNET3 or paravirtualization
VPX 5000	4 GB	2-6	20 GB	✓	✓	✓		VMXNET3 or paravirtualization

NetScaler VPX for Public Cloud - CPU and Memory Requirement						
Model	Minimum Memory *	vCPUs *	Minimum Disk Size	AWS	Azure	GCP
VPX BYOL	4 GB	2	20 GB	✓	✓	✓
VPX 10	4 GB	2-4	20 GB	✓	✓	✓
VPX 200	4 GB	2-4	20 GB	✓	✓	✓
VPX 1000	4 GB	2-6	20 GB	✓	✓	✓

Windows environment for CVAD - CPU and Memory requirement			
Model	Minimum memory *	vCPUs *	Minimum Disk size
Windows Server 2019	8 GB	4	40 GB
Windows 10	8 GB	4	40 B

To explore details about other NetScaler models, refer to the [NetScaler data sheet](#).



## Licensing

NetScaler offers diverse product editions and licensing models designed for MPX and VPX appliances to meet your organizational specific needs. To ensure optimal functionality, a NetScaler appliance requires a license from one of the NetScaler family editions: Advanced, Premium, and Standard Edition.

It is important to note that the Standard edition has reached its End of Sale (EOS) and it is still available for renewal only.

The NetScaler includes a VPX Expression license (Freemium), requiring no license file for both on-premises and cloud deployments. VPX Express offers the following features:

- About 20 Mbps bandwidth, 20 Mbps Secure Sockets Layer (SSL) throughput and up to 250 SSL sessions
- Web Logging, Load Balancing, Content Switching, Cache Redirection, SSL Offloading, Content Filtering, Rewrite, IPv6 protocol translation, Responder, AppFlow, Clustering, and CallHome

---

**IMPORTANT NOTE:** VPX Express license is used for all exercises, except GSLB and Gateway, where a license is required. We recommend obtaining the license through your Sales Rep/Customer Service for seamless integration and enhanced functionality.

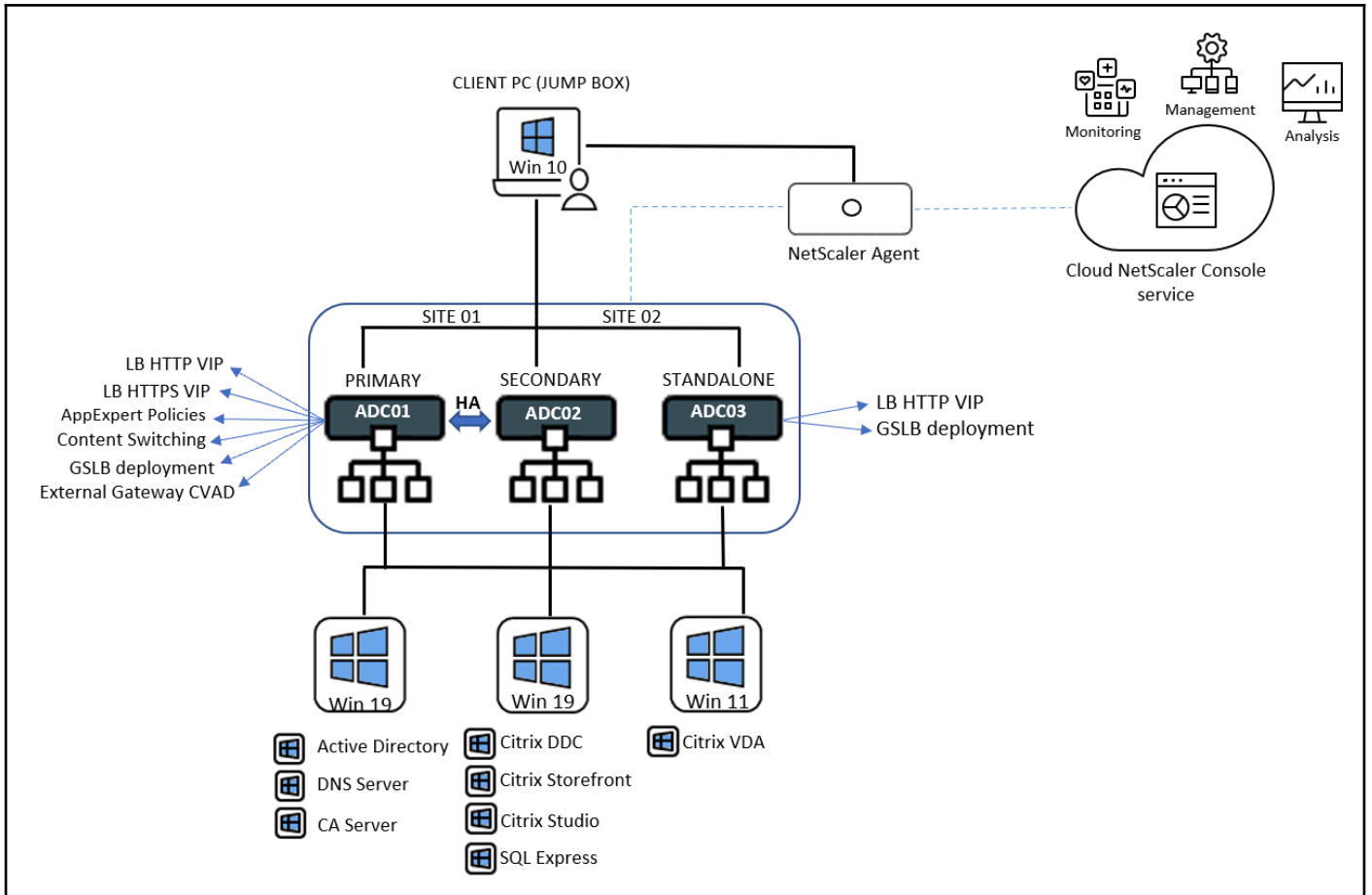
---

## Virtual Machines Covered in This Guide

- VM NetScaler ADC01 Primary
- VM NetScaler ADC02 Secondary
- VM NetScaler ADC03 Standalone for GSLB
- VM Windows Server for Active Directory, DNS, and CA
- VM Windows Server 2019 for Delivery Controller (DDC) and Storefront
- VM Windows 10 for VDA
- VM ADM Agent

## Virtual Machines and Services NOT Covered in This Guide:

- HTTP Web Server configuration
- VM Windows 10/Ubuntu Client (JumpBox)



## Table of Contents

<b>INSTALLING FIRST NETSCALER 14.1</b>	<b>8</b>
<b>Configuring an HTTP LB VIP</b>	<b>12</b>
Adding a Hostname to Your Windows Client Hosts File	17
TCP-based Application Probe	20
HTTP-based Application Monitor	21
Curl Tool and nstcpdump.sh	25
Configuring Persistence and LB method	26
Testing Persistence	28
<b>Creating a Root-CA and SSL Certificate on the NetScaler</b>	<b>31</b>
<b>Configuring an SSL Offloading LB VIP</b>	<b>40</b>
Enabling Enhanced/Default SSL Profile	40
Installing the Root CA certificate on Windows Client (Jump box)	44
Enabling TLS 1.3	49
Troubleshooting Common SSL Client Issues	52
Using OpenSSL tool to match SSL Certificate and SSL Key	53
<b>Configuring Rewrite and Responder Policies</b>	<b>55</b>
Rewrite – Removing an HTTP Header	55
Testing	58
Responder Policy to Redirect from HTTP to HTTPS	59
<b>Configuring an HTTP Content Switching VIP</b>	<b>65</b>
Configuring Non-Addressable Virtual Servers by CLI	65
Configuring the Content Switching VIP and Policies	66
Testing and Checking the Policy Hits	74
Content Switching Backup Virtual Server	76
<b>SECOND NETSCALER 14.1 (HA) INSTALL</b>	<b>81</b>
<b>NetScaler High Availability (HA) Configuration</b>	<b>86</b>
Triggering a Manual Failover	92
<b>NetScaler Console Service and NetScaler Agent Setup</b>	<b>94</b>
Configure the ADM Service License Server (Pooled Capacity)	107
Configure the Pooled License to the NetScaler	110
<b>Third NetScaler 14.1 for GSLB Install CLI</b>	<b>113</b>
Configuring an HTTP LB VIP	117
<b>Configuring GSLB Active-Active</b>	<b>119</b>
Configuring GSLB SITE 01	119
Configuring GSLB SITE 02	134
Manual Sync Between Site 01 and Site 02	139
Testing the GSLB Deployment	141
Changing Deployment Type to ACTIVE-PASSIVE	147
<b>Citrix Virtual Apps and Desktops Install</b>	<b>157</b>
Installing Active Directory Domain Services	157
Adding User Accounts and Configuring Group Membership	174

Configuring Active Directory DNS	180
Configuring Delivery Controller, Storefront, and Studio	210
Launching the CVAD installer	215
Site Configuration	228
Windows 11 Install for Virtual Delivery Agent (VDA)	233
Launching the VDA installer	238
Machine Catalog Configuration	252
Delivery Group Configuration	257
<b>StoreFront installation and configuration</b>	<b>265</b>
Configuring DNS entry for Storefront	278
Testing Internal Launching	280
Monitoring the Sessions with Citrix Director	282
Verify VDA Machine is Registered with the Delivery Controller	285
Unable to Start APP/Desktop	286
There are no apps or Desktops available to you at this time Error	288
<b>Integrating NetScaler Gateway with CVAD on-prem</b>	<b>289</b>
DNS Configuration for STA and Gateway	289
Gateway Vserver Configuration	294
Configuring Advanced Authentication	297
STA and Session Policies	306
Storefront Configuration for Gateway	317
Testing Authentication, Enumeration, Launch, and Session Via Web Browser	323
Testing Authentication, Enumeration, Launch, and Session Via CWA	329
Monitoring ICA sessions Via NetScaler GUI	332
<b>NETSCALER CONSOLE HDX INTEGRATION WITH NETSCALER GATEWAY</b>	<b>335</b>
Generating HDX Traffic and Testing	343
<b>NetScaler and NetScaler Gateway Troubleshooting</b>	<b>345</b>
Cannot Complete your Request Error	345
Cannot Start App/Desktop Error	347
Storefront Event Viewer	348
Examining ICA File	350
Checking STA Server Status – External Launch Failure	351
LDAP/Radius Authentication Issue	352
Taking VPX Network Trace on GUI (Wireshark)	354
Limitations of Using SSL Session Keys	359
Taking VPX Network Trace by Using the Command Line Interface (CLI)	359
Taking VPX Logs (Support Bundle)	360
Taking VPX Logs by Using the Command Line (CLI)	361
Download Trace Files and Support Bundles Generated by CLI	362
Taking SDX/SVM Logs (Support Bundle)	362

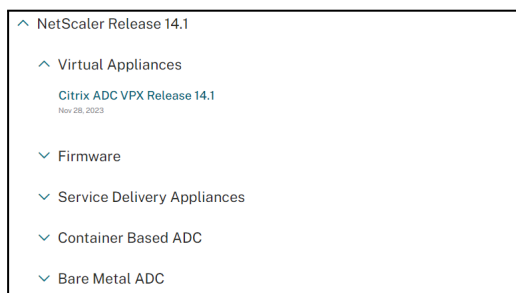
<b>Author</b>	<b>Changes</b>
Willian de Souza Oliveira	NetScaler Lab Guide Version 1.0

# Installing First NetScaler 14.1

**NOTE:** If NetScaler firmware is already downloaded and the initial NetScaler IP (NSIP), subnet mask, and gateway are configured, skip the steps 1 through 3.

1. Download the NetScaler VPX firmware from the Citrix website. Select the most recent 14.1 firmware build and the appropriate platform. If you are executing these steps on a Hypervisor (Xenserver, VMware, KVM, and others), opt the Virtual Appliance section to download the image corresponding to your hypervisor.

Download the NetScaler firmware: <https://www.citrix.com/downloads/citrix-adc/>



For steps on how to deploy the NetScaler on the supported platforms, please refer to the official documentation:

<https://docs.netScaler.com/en-us/citrix-adc/current-release/deploying-vpx>

2. After step #1, proceed to configure the **management IP (NSIP)**, **Netmask**, and your designated **Gateway** using the **NetScaler Console**.

```
-----[DSA 1024]-----+
+*****. .
0.+.0.+. .
* *000.0
.X0+00.. .
S 0E=. .
. *.0
. .0
. *0
. .0
-----[SHA256]-----+

kern.sched.idlespinthresh: 157 -> 32
Start daemons: syslogd Dec 19 13:34:40 <kern.info> ns syslogd: kernel boot file
is /flash/ns-14.1-4.42
Dec 19 13:34:40 <kern.notice> ns kernel: lo0: link state changed to UP
inetd cron httpd monit sshd /etc/sshd_config line 19: Deprecated option UsePriv
ilegeSeparation

!There is no ns.conf in the /nsconfig!

Start Netscaler software
Input: no terminal type specified and no TERM environmental variable.
Enter Citrix ADC's IPv4 address []: █
```

3. Enter the **new IP, netmask**, and **your own gateway**. If everything is correct, press 4 on the keyboard to **Save** and **quit**.



```

Citrix ADC Virtual Appliance Initial Network Address Configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([ ]).
Selecting the listed number allows the address to be changed.

After the network changes are saved, you may either login as nsroot and
use the Citrix ADC command line interface, or use a web browser to
http://10.91.69.145 to complete or change the Citrix ADC configuration.

1. Citrix ADC's IPv4 address [ 10.X.X.X ]
2. Netmask [ 255.X.X.X ]
3. Gateway IPv4 address [ 10.X.X.X ]
4. Save and quit
Select item (1-4) [4]: 4

```

At this point, the NetScaler will boot, and the login prompt will appear.

```

NetScaler initialization is still in progress; please wait
20 to 30 seconds before attempting to log in.
Jan 13 14:58:12 <local0.alert> 10.110.73.136 01/13/2023:14:57:47 GMT 0-PPE-0 :
default EVENT STATECHANGE 27 0 : Device "self node 10.110.73.136" - State UP
#####
#
# WARNING: Access to this system is for authorized users only.
# Disconnect IMMEDIATELY if you are not an authorized user!
#
#####
login:

```

4. Enter "nsroot" in the **login** field and then enter "nsroot" in the **Password** field.
5. You will be prompted to change your nsroot password. Set a new password with robust characters.
6. Save the configuration using the command "save config".

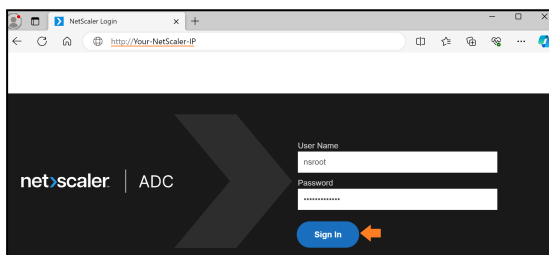
```

login: nsroot
Password:
Dec 20 10:15:25 <auth.notice> ns login: ROOT LOGIN (nsroot) ON tty00

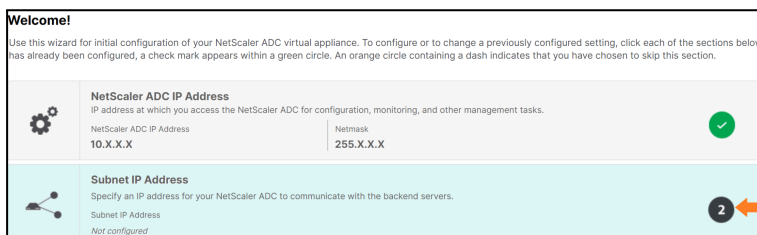
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
> save config
Done

```

7. Access the link **http(s)://YOUR-NETSCALER-IP**.
8. Enter "nsroot" in the **User Name** input field and the new password in the **Password** input field.
9. Click the **Sign In** button.



10. Click **number 2**.



11. Enter your Subnet IP Address (SNIP) + Netmask. This IP must be free in the network. Click **Done**.

12. Click **number 3**.

13. Enter **“netscaler01.repro.lab”** in the **Host Name** input field.

14. Set **Time Zone**.

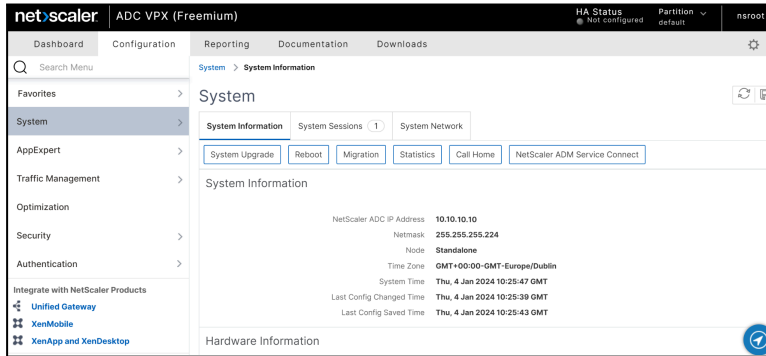
15. If you already have an internal DNS/NTP server in your network, enter the IP(s) and then click **Done**.

16. You will be prompted to save and reboot the NetScaler, click **YES**. The NetScaler GUI will be available again in about a minute.

17. Enter **nsroot** in the **User Name** input field and then enter the new password in the **Password** input field.



18. The Initial configuration is done.



# Configuring an HTTP LB VIP

**Important Note:** To create the Load Balancer Virtual Server, ensure you have at least two running Web such as Apache, IIS, and Nginx. If creating two Web Servers is unfeasible, you can proceed with only one; however, some exercises may not be fully executable in such scenarios.

The following are the official documentation links for two players that offer the necessary Web Server Installation for the upcoming exercises. Alternatively, you can explore other online sources to set up your Web Servers.

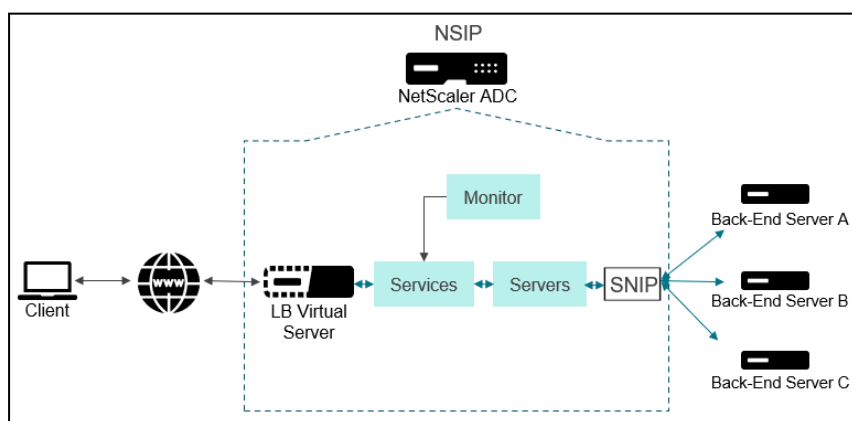
## Microsoft IIS Install

<https://learn.microsoft.com/en-us/iis/manage/creating-websites/scenario-build-a-static-website-on-iis>

## Linux Apache Server

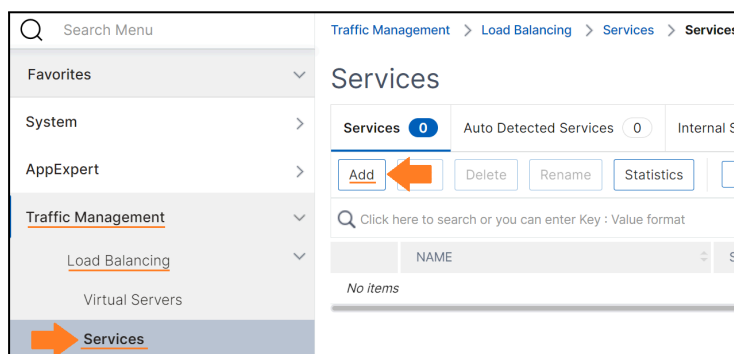
<https://httpd.apache.org/docs/2.4/install.html>

The following is a visual representation of a client's request to a backend server, including the load balancing entities.



Perform the following steps to have the same configuration set up in your environment:

1. On NetScaler, navigate to **Traffic Management > Load Balancing > Services** and click **Add** to add your Web Servers as services to be associated (bound) to the Load balance VIP.



2. Enter **svrc\_http\_01** in the **Service Name** input field.
3. Enter **Your Web Server 01 IP Address** in the **IP Address** field.

- Keep the protocol as **HTTP** and **port 80** and then Click **OK**.

**Basic Settings**

Service Name\*

New Server  Existing Server

IP Address\*

Protocol\*

Port\*

More

**OK** **Cancel**

- The **Server State** setting for the **srvc\_http\_01** service should be marked as **UP**. If yes, click **Done**.

**Load Balancing Service**

**Basic Settings**

Service Name	srvc_http_01	Traffic Domain	0
Server Name	10.X.X.X	Number of Active Connections	-
IP Address	10.X.X.X	Hash ID	-
Server State	UP	Server ID	None
Protocol	HTTP	Cache Type	SERVER
Port	80	Cacheable	NO
Comments		Health Monitoring	YES
		AppFlow Logging	ENABLED

Monitoring Connection Close Bit: NONE

**Service Settings**

Surge Protection	OFF	Use Source IP Address	NO
Use Proxy Port	YES	Client Keep-Alive	NO
Down State Flush	ENABLED	TCP Buffering	NO
Access Down	NO	Compression	NO
		Insert Client IP Address	DISABLED
		Header	client-ip

**Monitors**

1 Service to Load Balancing Monitor Binding

**Done**

- Uncheck the **“srvc\_http\_01”** checkbox and click **Add**.

**Services**

Services 1 | Auto Detected Services 0 | Internal Services 8

**Add** **Delete** **Rename** **Statistics** **No action**

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE
<input checked="" type="checkbox"/>	srvc_http_01	UP

Total 1

- Enter **srvc\_http\_02** in the **Service Name** input field.
- Enter **Your Web Server 02 IP Address**, in the **IP Address**.
- Keep the protocol as **HTTP** and **port 80** and then Click **OK**.

**Basic Settings**

Service Name\*

New Server  Existing Server

IP Address\*

Protocol\*

Port\*

More

10. The **Server State** setting for the **srvc\_http\_02** service should be marked as **UP**. If yes, click **Done**.

← Load Balancing Service

**Basic Settings**

Service Name	srvc_http_02	Traffic Domain	0
Server Name	10.X.X.X	Number of Active Connections	-
IP Address	10.X.X.X	Hash ID	-
Server State	UP	Server ID	-
Protocol	HTTP	Cache Type	SERVER
Port	80	Cacheable	NO
Comments		Health Monitoring	YES
		AppFlow Logging	ENABLED

Monitoring Connection Close Bit: NONE

**Service Settings**

Surge Protection	OFF	Use Source IP Address	NO
Use Proxy Port	YES	Client Keep-Alive	NO
Down State Flush	ENABLED	TCP Buffering	NO
Access Down	NO	Compression	NO
		Insert Client IP Address	DISABLED
		Header	client-ip

**Monitors**

1 Service to Load Balancing Monitor Binding

**Note:** If you have more than two Web Servers, please replicate the previous steps to include your additional servers.

Your Web Servers will look similar to the following screenshot. Now, you can set up the configuration for the load balancing VIP.

**Services**

Services 2 | Auto Detected Services 0 | Internal Services 8

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE
<input type="checkbox"/>	srvc_http_01	UP
<input type="checkbox"/>	srvc_http_02	UP

Total 2

11. Navigate to **Traffic Management > Load Balancing > Virtual Servers** and click **Add**.

Search Menu

Traffic Management > Load Balancing > Virtual Servers

**Virtual Servers** 0

Click here to search or you can enter Key : Value format

NAME	STATE
No items	



12. Enter **lb\_vip\_http\_repro.lab** in the Name input field.
13. Select **HTTP** from the **Protocol** drop-down list.
14. Select **IP Address** from the **IP Address Type** drop-down list.
15. Click **Create**.

**Basic Settings**

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*

Protocol\*

IP Address Type\*

IP Address\*

Port\*

More

16. Click **No Load Balancing Virtual Server Service Binding** under the Services and Service Groups section.

**Basic Settings**

Name	lb_vip_http_repro.lab	Listen Priority	-
Protocol	HTTP	Listen Policy Expression	NONE
State	DOWN	Redirection Mode	IP
IP Address	10.X.X.X	Range	1
Port	80	IPset	-
Traffic Domain	0	RHI State	PASSIVE
Toggle Order	ASCENDING	AppFlow Logging	ENABLED
Order Threshold	0	Retain Connections on Cluster	NO
		Probe Protocol	-
		Probe Success Response Code	-
		Probe Port	-

**Services and Service Groups**

A service is a logical representation of an application running on a server. A service group enables you to manage a group of services as though it were a single service. After creating a service group, you can bind it to a virtual server, and you can service groups.

Note: Bind at least one service or service group to the virtual server.

Click **Continue** to display the advanced settings and select the method, persistence type, and any other configuration detail that you might need.

No Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

17. Click **Click to select**.

**Service Binding**

Select Service\*

**Binding Details**

Weight

Order

18. Select all your services and click **Select**.

**Service 2**

Click here to search or you can enter Key : Value format

<input checked="" type="checkbox"/>	NAME	STATE
<input checked="" type="checkbox"/>	srvc_http_01	UP
<input checked="" type="checkbox"/>	srvc_http_02	UP

Total 2

19. Click **Bind** to bind all the services to your load balance VIP.

**Service Binding**

Select Service\*  
svc\_http\_01, svc\_http\_02 > Add Edit ⓘ

**Binding Details**

Weight  
1

Order

Bind Close

20. Click **Continue**.

**Services and Service Groups**

A service is a logical representation of an application running on a server.  
A service group enables you to manage a group of services as though it were a single service. After creating a service service groups.  
**Note:** Bind at least one service or service group to the virtual server.

Click **Continue** to display the advanced settings and select the method, persistence type, and any other configuration

2 Load Balancing Virtual Server Service Bindings >

No Load Balancing Virtual Server ServiceGroup Binding >

Continue

21. Click **Done**.

**Services and Service Groups**

2 Load Balancing Virtual Server Service Bindings >

No Load Balancing Virtual Server ServiceGroup Binding >

Done

LB VIP is **UP** and ready to receive connections. Additionally, you can monitor the **Service Health Percentage** with all three services currently marked as **UP** and none as **DOWN**. The default load balancing method, which is **LEASTCONNECTION**, is also displayed.

**Virtual Servers** 1

Add Edit Delete Enable Disable Rename Statistics Select Ac

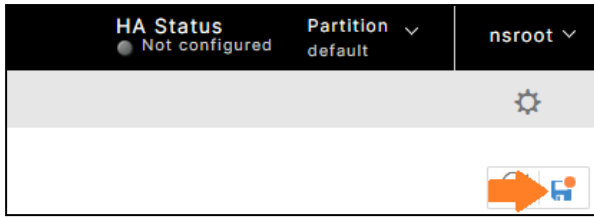
Q Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE
<input type="checkbox"/>	lb_vip_http_repro.lab	UP	UP

Total 1

Virtual Servers

22. Click the **Save** icon to save the configuration.



## Adding a Hostname to Your Windows Client Hosts File

Adding a hostname to the Windows hosts file is a way to manually map a domain name to an IP address on a Windows computer. This mapping is useful for various purposes, but for us, it will be useful for "Local Testing." We will test the HTTP Load Balancing VIP by directing a domain name "lb.repro.lab" to the LB VIP IP address, simulating how they would resolve the name if a DNS server was in place.

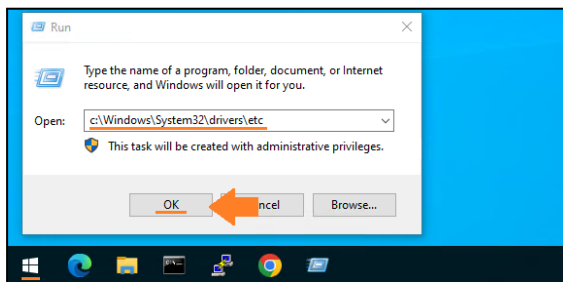
---

**Note:** If you have an existing DNS server in your environment, you have the option to append a new "A Host", mapping the new Load Balancing VIP to its corresponding IP Address. If this is the case, skip the steps from 1 through 10.

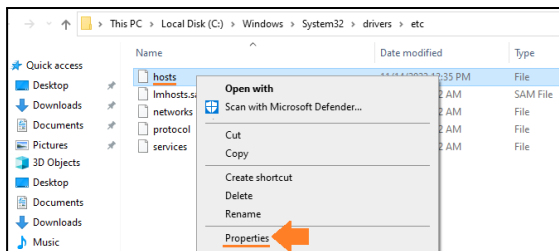
---

The following are the steps to add a hostname to your Windows Client Hosts File

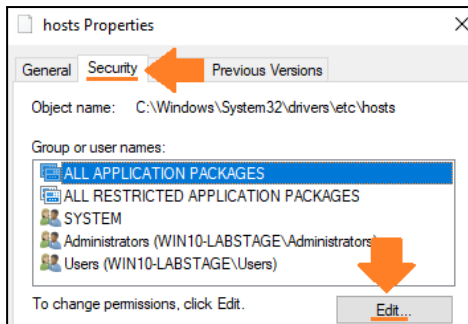
1. From your Jump Box Windows Client, either navigate to **Windows Explorer > Local Disk (C:) > Windows > System32 > Drivers > etc** or from the **Run** command, execute the following path.  
`c:\Windows\System32\drivers\etc`



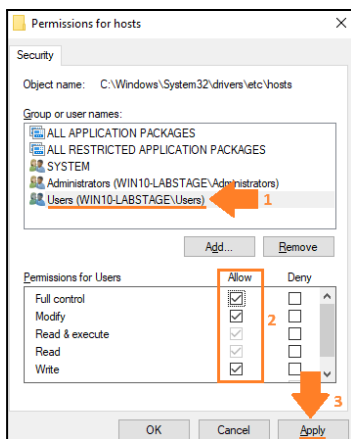
2. Right-click **hosts** and then select **Properties**.



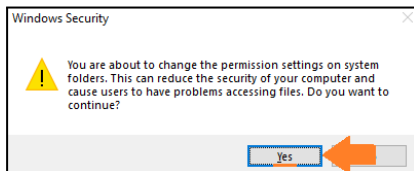
3. Click **Edit**.



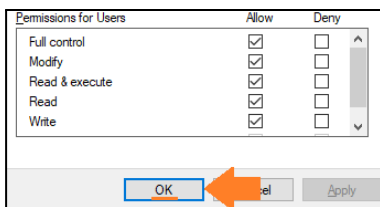
4. Select the list item that starts with the word **Users**.
5. Select all the items under the **Permission for Users** section.
6. Click **Apply**.



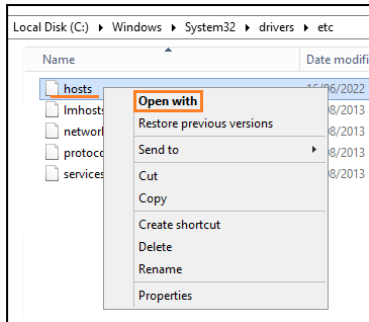
7. Click **Yes**.



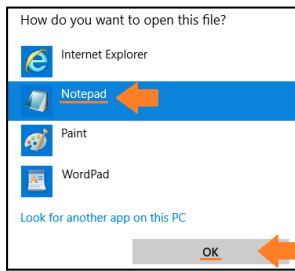
8. Click **OK**.



9. **Right-click** **hosts** and then select the **Open with** list item.



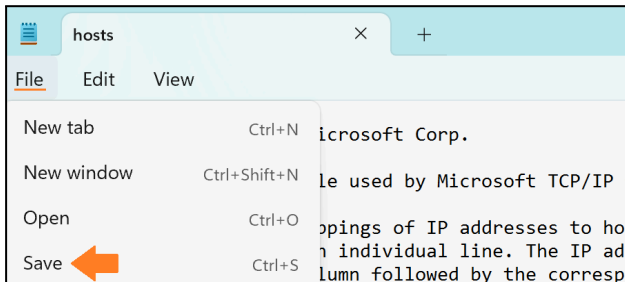
10. Select **Notepad**.



11. Add your HTTP LB Virtual Server IP followed by the hostnames **lb.repro.lab**. For example, 10.50.1.10 lb.repro.lab.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
10.X.X.X lb.repro.lab
```

12. Click the **File** menu and then click **Save** to save the changes.



13. Open a web browser and enter the HTTP LB VIP hostname (lb.repro.lab).

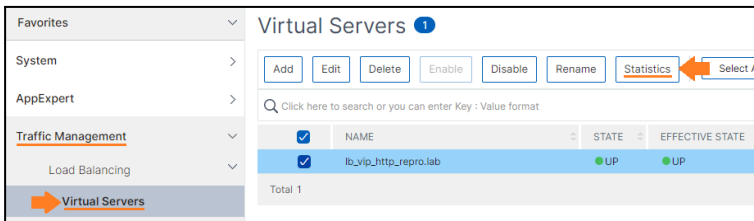


14. Refresh the browser or open a new tab and enter the <http://LB-VIP> this time. You should be redirected to the second HTTP server.



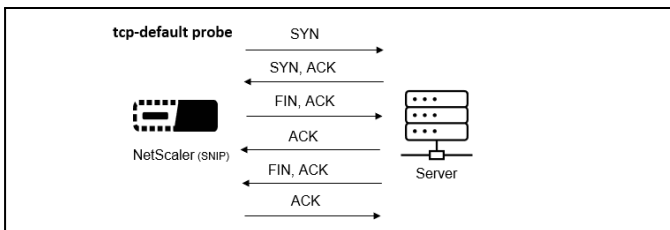
**Note:** Since no persistence has been configured, the LB VIP will continue to evenly distribute your requests among all your services.

15. Select **LB VIP** and then click **Statistics** to verify the number of hits and the load balancing.



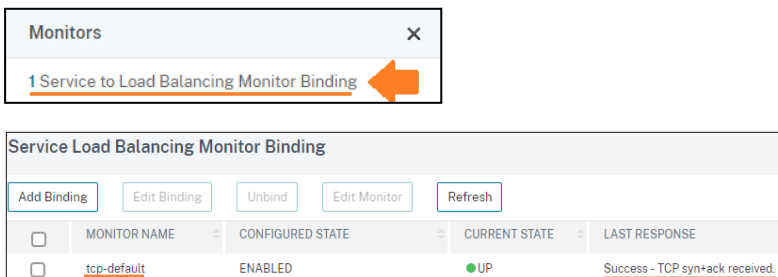
## TCP-based Application Probe

By default, when setting up a **TCP-based** service on the NetScaler, the "**tcp-default**" monitor is automatically bound to the service. The NetScaler appliance establishes a **3-way handshake** with the server destination, and then closes the connection performing a **complete TCP handshake**. It sends a "**SYN**" from its **SNIP address** and expects to receive a "**SYN-ACK**" in response. If successful, the service is marked as "**UP**," otherwise, it's marked as "**DOWN**."



The following are the steps to inspect and confirm the monitor response:

1. From **Traffic Management > Load Balancing > Services**, you can inspect and confirm the monitor response.



The following are the steps to see the real-time monitoring probe in action:



2. Open the **NetScaler CLI** using the **mRemoteNG**.
3. Run the below command to invoke the **"nstcpdump.sh"** script.

```
> shell
# nstcpdump.sh host YOUR-BACKEND-SERVER-IP and
port 80
```

**Note 1:** By default, If the NetScaler observes TCP traffic to the destination, it does not send TCP monitoring requests. Under **"Last Response"** you will notice the status **"Probe skipped – live traffic to service"** as below.

Service Load Balancing Monitor Binding				
MONITOR NAME	CONFIGURED STATE	CURRENT STATE	LAST RESPONSE	
tcp-default	ENABLED	UP	Probe skipped - live traffic to service.	

**Note 2:** You have the option to modify the **"Monitor Connection Close"** parameter at either the **LB global level** or the **Service level**. When this parameter is adjusted, instead of going through the **entire TCP handshake** process and closes the connection with **[FIN]**, the NetScaler initiates a **partial TCP handshake** and closes the connection upon receiving the **SYN-ACK** from the server with **[RESET]**. It minimizes the volume of network probe monitoring.

The screenshot shows the 'Configure Load Balancing Parameters' dialog. On the left, under 'Connection Close for Monitor', the 'FIN' radio button is selected. On the right, the 'Monitoring Connection Close Bit' dropdown menu is set to 'NONE'. Both are highlighted with orange arrows.

**Note 3:** In the NetScaler CPX, the **"Monitor Connection Close"** parameter value is set to **RESET** by default.

**Note 4:** For all **non-TCP** services, the **"ping-default"** monitor probe is applied. The NetScaler sends an **ICMP echo request** to the destination of the monitor and expects an **ICMP echo response**.

For additional details regarding the TCP-based monitor, please refer to the official documentation.

For additional details regarding the "Close Monitor Connection", please refer to the [official documentation](#).

## HTTP-based Application Monitor

In the next exercise, we will associate the **HTTP** monitor to a service. This action will result in the automatic removal of the **tcp-default** monitor from the service. The **"tcp-default"** monitor is solely focused on the **"TCP"** response and does **not** assess the proper functionality of the HTTP service. For instance, if a Webserver returns a **"500 error code"**, the **"tcp-default"** monitor will not detect that the HTTP content is unavailable and will keep delivering the **"500 error page"** to the end user, which is not the desired outcome.

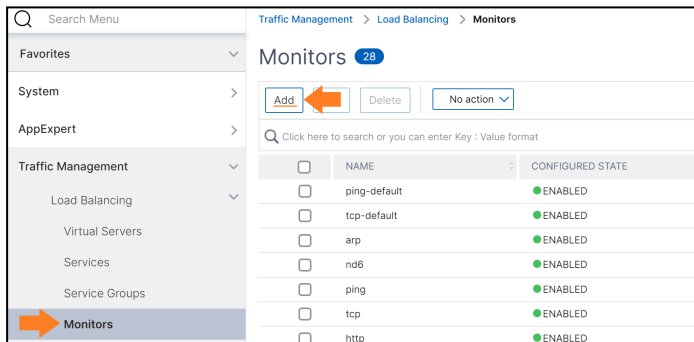
The HTTP monitor probe initiates a **TCP 3-way handshake** with the destination. After the connection is successfully established, the NetScaler sends an **HTTP request ["HEAD /"]**. It then assesses the response code by comparing it to the preset response codes in the monitor probe. By default, only a **200** code is considered acceptable. Any other response code received from the server will result in the monitor being marked as **DOWN**.

Source	Destination	Protocol	SrcPort	DestPort	Info
ADC SNIP	HTTP Server	TCP	21922	80	21922 → 80 [SYN] Seq=0 Win=8188 Len=0 MSS=1460
HTTP Server	ADC SNIP	TCP	80	21922	80 → 21922 [SYN, ACK] Seq=0 Ack=1 Win=29200 Le
ADC SNIP	HTTP Server	HTTP	21922	80	HEAD / HTTP/1.1
HTTP Server	ADC SNIP	TCP	80	21922	80 → 21922 [ACK] Seq=1 Ack=62 Win=29312 Len=0
HTTP Server	ADC SNIP	HTTP	80	21922	HTTP/1.1 200 OK
ADC SNIP	HTTP Server	TCP	21922	80	21922 → 80 [FIN, ACK] Seq=62 Ack=277 Win=7936
HTTP Server	ADC SNIP	TCP	80	21922	80 → 21922 [FIN, ACK] Seq=277 Ack=62 Win=29312
ADC SNIP	HTTP Server	TCP	21922	80	21922 → 80 [ACK] Seq=63 Ack=278 Win=7936 Len=0
HTTP Server	ADC SNIP	TCP	80	21922	80 → 21922 [ACK] Seq=278 Ack=63 Win=29312 Len=0

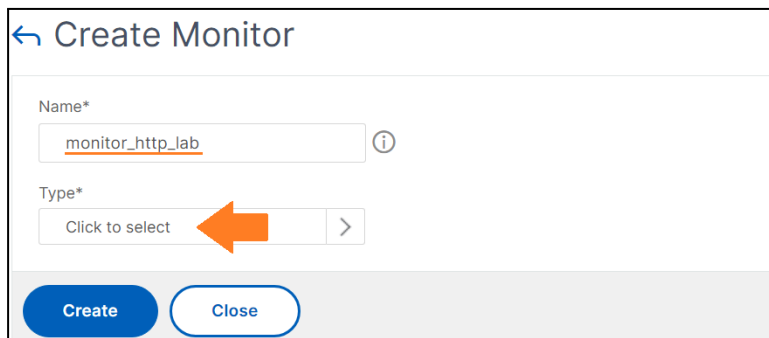
**Note:** You can utilize the existing **HTTP monitor** on the NetScaler; however, it is recommended as a best practice to create a new monitor whenever you need a custom parameter.

The following are the steps to associate the HTTP monitor to a service:

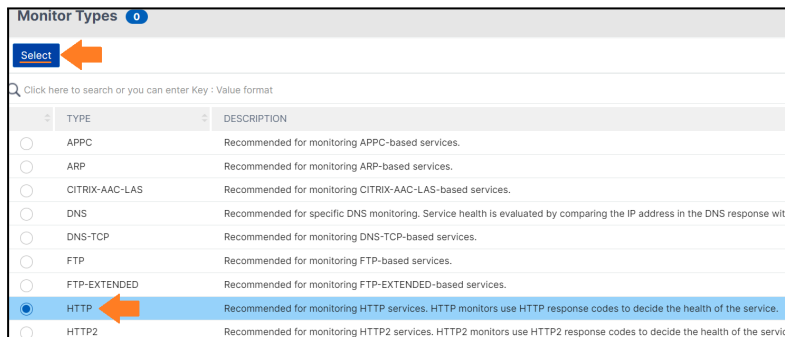
1. Navigate to **Traffic Management > Load Balancing > Monitors**.
2. Select the built-in monitor HTTP and click Add.



3. Enter the name **"monitor\_http\_lab"** and then click **"Click to select"**.



4. Click the **"HTTP"** radio button and then click **Select**.



5. Under Interval, adjust the Interval from 5 to 10 seconds. This means that the SNIP will probe the target server every 10 seconds. The **Time-out** value can remain unchanged, which

implies that if the NetScaler SNIP does not receive a positive response [200 response] within 2 seconds, the service will be considered as **DOWN**.

Basic Parameters

Interval: 10 Second

Response Time-out: 2 Second

Response Codes: 200

Custom Header:

HTTP Request: HEAD /

Secure

Advanced Parameters

Create Use

Your monitor is created and ready to be bound to your service/services.

Monitors 29

Add Edit Delete Select Action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	CONFIGURED STATE	TYPE
<input checked="" type="checkbox"/>	monitor_http_Jab	ENABLED	HTTP

6. Navigate to **Traffic Management > Services**, select the service “**srcv\_http\_blue**” and click **Edit**.

Services 2 Auto Detected Services 0 Internal Services 8

Add Edit Delete Rename Statistics Select Action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE
<input checked="" type="checkbox"/>	srcv_http_01	UP
<input type="checkbox"/>	srcv_http_02	UP

Total 2

7. Click **1 Service to Load Balancing Monitor Binding**.

Monitors

1 Service to Load Balancing Monitor Binding

8. Click **Add Binding**.

Service Load Balancing Monitor Binding

Add Binding Edit Binding Unbind Edit Monitor Refresh

<input type="checkbox"/>	MONITOR NAME	CONFIGURED STATE	CURRENT STATE
<input type="checkbox"/>	tcp-default	ENABLED	UP

9. Click **Click to select** to bind the monitor created before.

**Load Balancing Monitor Binding**

Select Monitor\*

Binding Details

Weight

State

10. Scroll down the page, navigate to page number 2, select your monitor “**monitor\_http\_lab**” and click **Select**.

**Monitors** 29

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	CONFIGURED STATE	TYPE
<input type="checkbox"/>	stasecure	● ENABLED	CITRIX-STA-SERVICE
<input type="checkbox"/>	sta	● ENABLED	CITRIX-STA-SERVICE
<input type="checkbox"/>	VPN_INT_MON-0	● ENABLED	TCP
<input checked="" type="checkbox"/>	monitor_http_lab	● ENABLED	HTTP

11. Click **Bind**.

**Load Balancing Monitor Binding**

Select Monitor\*

ⓘ

Binding Details

Weight

State

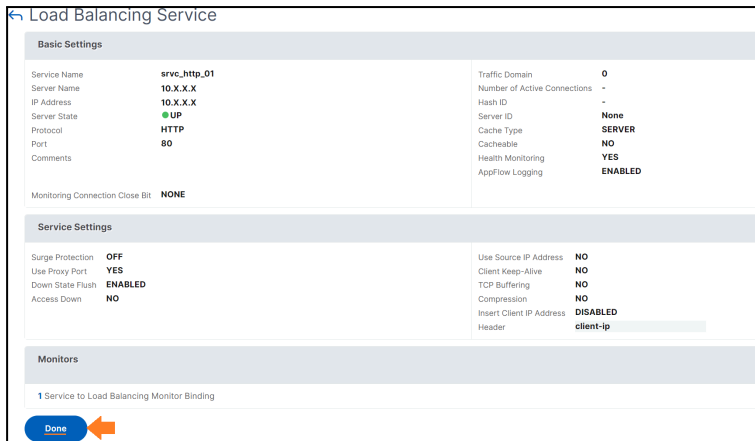
The monitor has been successfully bound to the server, and the server's response is now “**200 OK**” as expected. If you wish, you can bind the same monitor to your other Web Servers.

12. Click **Close**.

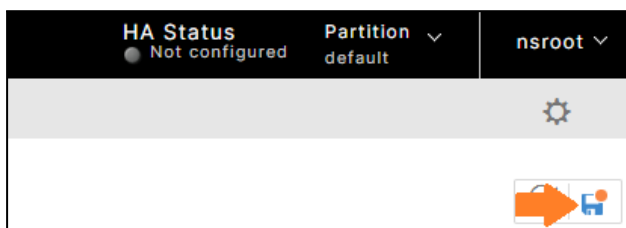
**Service Load Balancing Monitor Binding**

<input type="checkbox"/>	MONITOR NAME	CONFIGURED STATE	CURRENT STATE	LAST RESPONSE
<input type="checkbox"/>	monitor_http_lab	ENABLED	● UP	Success - HTTP response code 200 received.

13. Click **Done**.



14. Save the configuration.



## Curl Tool and nstcpdump.sh

**Note:** Putty will be used for the below exercise. If you do not have putty installed, please [download](#) it and install it on your Jump Box VM. Once you open the Putty, insert your NetScaler IP (NSIP) and click Open.

1. To verify the response header that the NetScaler receives from CLI, you have the option to employ the "curl" tool. In the NetScaler **SHELL**, enter the following command, targeting one of your **Web Servers**.

command: shell

command: curl -I http://Your-Web-Server-IP (e.g., http://10.10.1.50)

Since the NetScaler receives a response header of "**200 OK**", the HTTP 01 service is marked as **UP**.

```
> shell
root@netscaler01# curl -I http://Your-Web-Server-IP
HTTP/1.1 200 OK
Date: Thu, 04 Jan 2024 13:24:43 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
Last-Modified: Wed, 03 Jan 2024 14:00:41 GMT
ETag: "4515-60e0b0a60005e"
Accept-Ranges: bytes
Content-Length: 17685
Content-Type: text/html; charset=UTF-8
```

2. Using the nstcpdump.sh script tool, you can observe the communication between the NetScaler SNIP and the Server. It provides a clear view of the NetScaler SNIP's probing of the Back-end-Server using the **HTTP HEAD** method and the Server responding with a "**200 OK**." Additionally, you can observe the SNIP performing these probes every 10 seconds, as configured in the "interval" setting before.

command: nstcpdump.sh -X host Web-Server-IP and port 80 | egrep 'HEAD|200 OK'

```

root@netscaler01# nstcpdump.sh -X host Web-Server-IP and port 80 | egrep 'HEAD|200 OK'
reading from file -, link-type EN10MB (Ethernet), snapshot length 65535
13:19:56.792265 IP SNIP.6026816 > Web Server IP.80: Flags [P.], seq 1:62, ack 1,
win 31, length 61: HTTP: HEAD / HTTP/1.1
0x0020:  5018 001f 9f41 0000 4845 4144 202f 2048  P...A..HEAD./.H
13:19:56.793460 IPWeb Server IP.80 > SNIP .60268:      Flags [P.], seq 1:277, ack 62
, win 229, length 276: HTTP: HTTP/1.1 200 OK
13:20:06.793858 IP SNIP.2761446 >Web Server IP.80: Flags [P.], seq 1:62, ack 1,
win 31, length 61: HTTP: HEAD / HTTP/1.1
0x0020:  5018 001f 9f41 0000 4845 4144 202f 2048  P...A..HEAD./.H
13:20:06.795152 IPWeb Server IP.80 > SNIP.27614:      Flags [P.], seq 1:277, ack 62
, win 229, length 276: HTTP: HTTP/1.1 200 OK

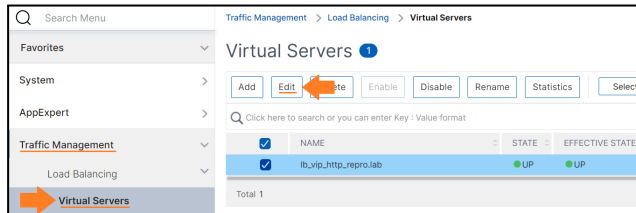
```

**Note:** The nstcpdump.sh script is used for troubleshooting low-level issues only.

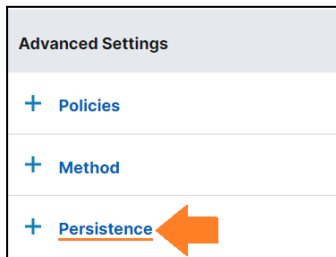
## Configuring Persistence and LB method

Persistence ensures that user sessions are consistently directed to the **same server**, critical for maintaining session continuity. The LB method (Load Balancing Method) determines how incoming requests are distributed among backend servers and includes options like Round Robin, Least Connections, and Least Response Time.

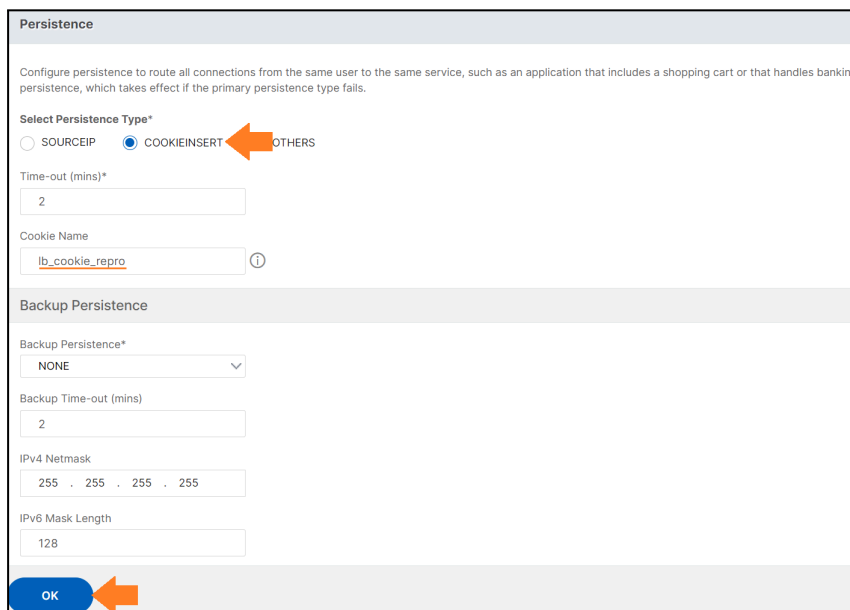
1. Click **Edit**.



2. Click **Persistence** under **Advanced Settings**.



3. Set COOKIEINSERT, enter the name "my\_cookie\_repro.lab" and click OK.



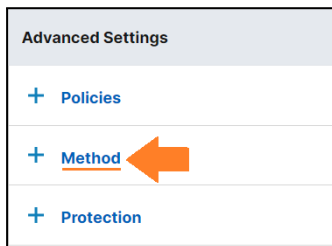


---

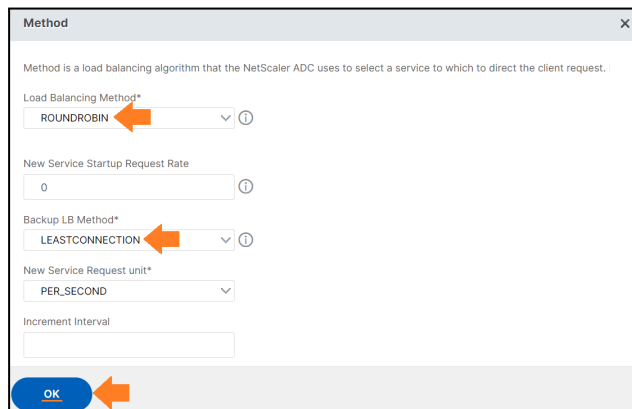
**Notes:**

1. Be aware that the default time-out value is set to **2 minutes**. In practical terms, this means that if the LB VIP does not receive any new requests from the same client or browser **within this 2-minute period**, the LB may select another server and set a new cookie. It is important to note that specifying the cookie name is **optional**, and certain persistence types may be specific to particular Virtual Servers as stated in the [official documentation](#).
  2. Take note that while configuring COOKIEINSERT persistence, you have the option to set the expiry time value to **0**, indicating **no expiration**. In this case, the session cookie will only expire when the user closes the browser session. Additionally, it's possible to define a backup persistence method, which will come into play if, for any reason, the cookie insertion process fails.
- 

4. Select **Method** under **Advanced Settings**.



5. Select **ROUNDROBIN** and **LEASTCONNECTION** as Backup LB and click **OK**.

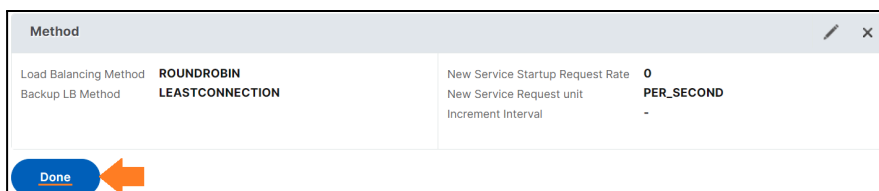


---

**Note:** Please, keep in mind that the **ROUNDROBIN** method is "**static**," implying that it distributes traffic evenly to services in a 1:1 fashion, irrespective of their current load. The default method is **LEASTCONNECTION**.

---

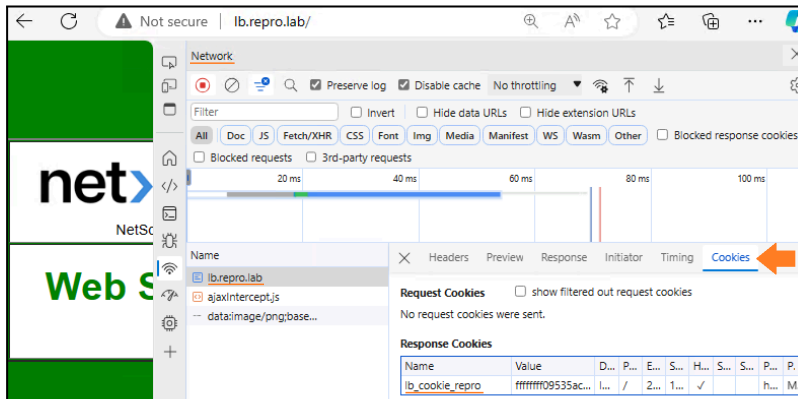
6. Click **Done**.



## Testing Persistence

1. Open your web browser, access the developer tools (**press F12**), enter your **HTTP LB VIP** address or **FQDN** (<http://lb.repro.lab>), and then click the **REFRESH** button. You should

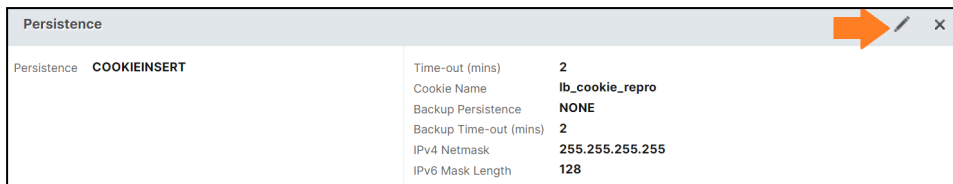
observe that the server color remains consistent, confirming that the cookie is set according to the configured parameters.



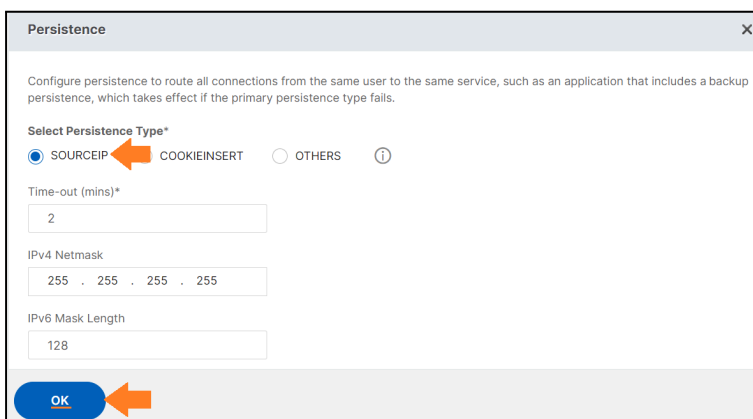
Notes:

1. Take note that you can view the date and time when the cookie is set to expire. If you consistently refresh the page, you will observe that the expiration time gets updated as well, consistently expiring 2 minutes after the last interaction from the browser.
2. It is important to understand that COOKIEINSERT persistence is managed by the browser and not controlled by the NetScaler once it is set. In contrast, NetScaler has the ability to control the SOURCE IP persistence type, as demonstrated in the following exercise.

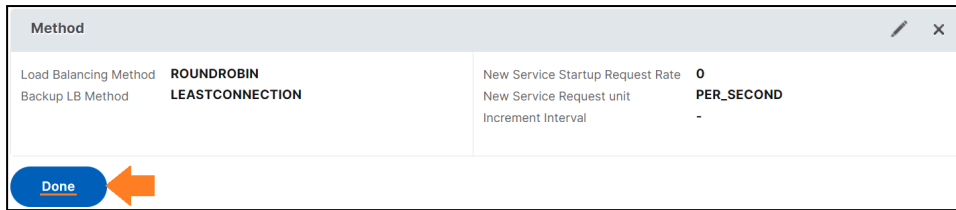
2. Return to the NetScaler GUI and **Edit** the same **LB HTTP VIP** again.
3. Scroll down until the persistence section and click to **edit**.



4. Select **SOURCEIP** this time and click **OK**. The default **time-out** value is also 2 minutes.



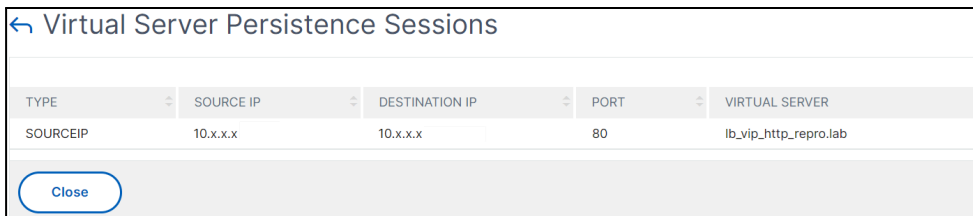
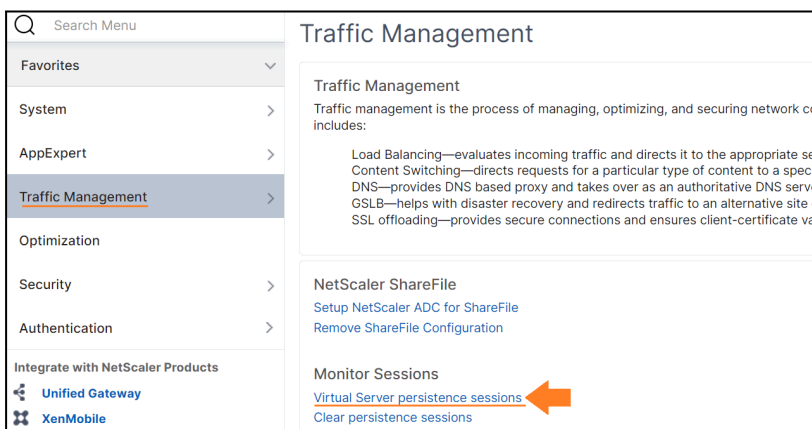
5. Click **Done**.



6. Close and reopen your browser, access the developer tools again (**F12**), enter your **HTTP LB VIP** address or **FQDN** (<http://lb.repro.lab>), and **REFRESH** the page once more.

This time, you will not find an HTTP Header related to a cookie in the headers. As previously mentioned, it is the NetScaler that manages the **SOURCE IP** persistence in a dedicated table.

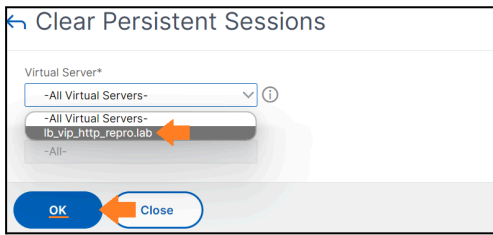
7. To check the SOURCE IP persistence table, navigate to **Traffic Management > Virtual Server persistence sessions** on your NetScaler.



#### Notes:

1. Take note that in the table, you will encounter the client's Source IP. Ideally, this should display the actual CLIENT IP of the user. This is expected to be the external, public IP for users accessing from external networks, or the genuine internal IP from their client machines for internal users.
2. If there is a firewall or router situated between the client and the NetScaler, and this intermediary is not set up to perform Network Address Translation (NAT) to the NetScaler using the actual CLIENT IP of the user, you will observe only an internal IP in the Source field (typically the Firewall/Router IP). This situation can disrupt the Load Balancing (LB) method since the Source IP of the client will consistently appear as the same Firewall/Router IP.
3. Be aware that by repeatedly refreshing the HTTP LB VIP page, you will observe that the TIME OUT value resets, extending for another 120 seconds (2 minutes). When the timer reaches 0, another service will be chosen if the same user reconnects. As an alternative, you can clear the persistence directly from the NetScaler GUI to observe this behavior. Another service will be selected when you connect again to the HTTP LB VIP.

8. Select your **HTTP LB VIP** and click **OK**.

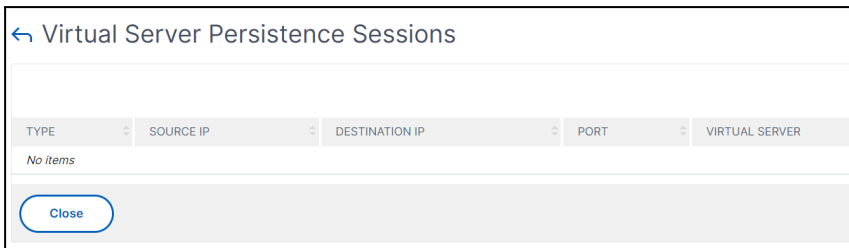


---

**Note:** This will ensure you will clear the persistence only for the LB VIP you are working on.

---

If you return to the Persistence Sessions page, you will see the session was cleared.



If you refresh the browser (<http://lb.repro.lab>) again, another persistence session will be created.

# Creating a Root-CA and SSL Certificate on the NetScaler

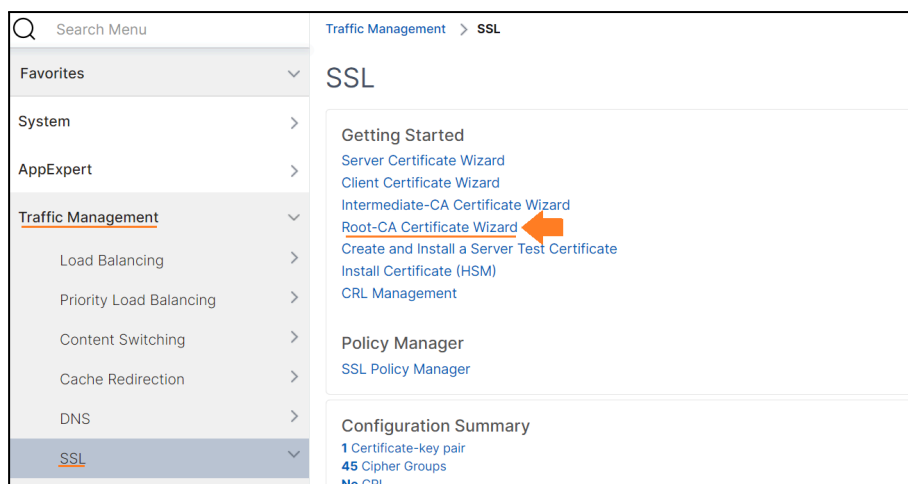
## Notes:

1. For this task, a valid SSL certificate is required. If you already have one, you can utilize it. In that case, please skip this exercise and proceed to the "How to configure an SSL offload Virtual Server" activity.
2. We will generate a Root Certificate (with NetScaler acting as an internal CA Server) and a Server certificate that will be assigned by NetScaler.

**Important Note:** CSG recommends that you use certificates obtained from authorized CAs, such as Verisign, for all your SSL transactions. Use certificates generated on the NetScaler appliance for testing purposes only, not in any live deployment.

The following are the steps to create a Root-CA and SLL certificate on the NetScaler:

1. On the NetScaler, navigate to **Traffic Management > SSL**.
2. Click **Root-CA Certificate Wizard**.



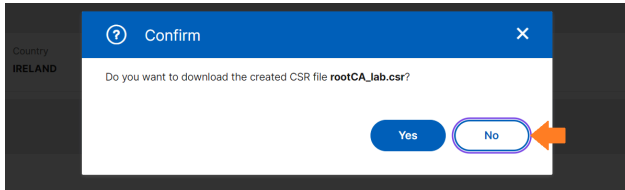
3. Enter **rootCA\_lab.key** in the Key **Filename** inputfield.
4. Keep the other settings as default, and click **Create**.

5. Enter **rootCA\_lab.csr** in the **Request File Name** and skip to the **Distinguished Name Fields** section.

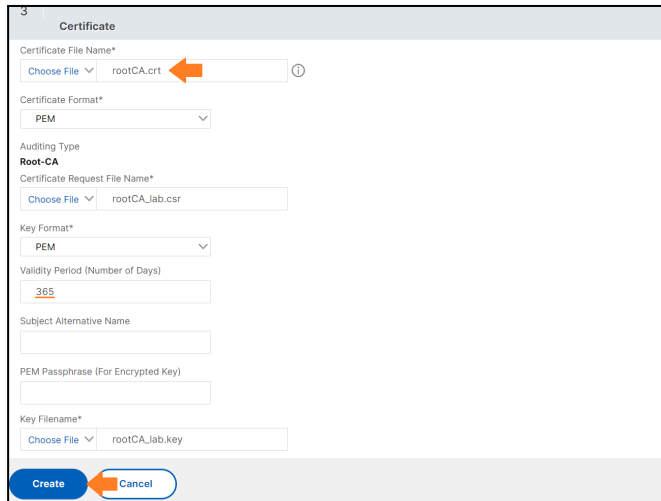
6. Complete the mandatory fields with your region details.
7. Enter **RootCA LAB** in the **Common Name** input field.
8. Click **Create**.



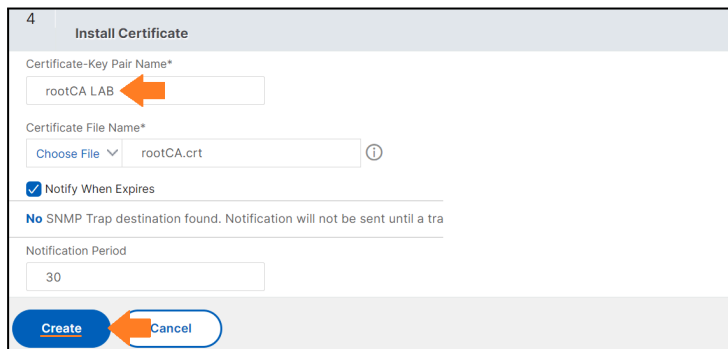
9. Click **NO**.



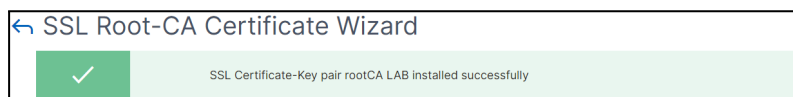
10. Enter **rootCA\_lab.crt** in the **Certificate File Name** input field, and then click **Create**.  
You can increase the certificate validity period by changing 365 (1 year).



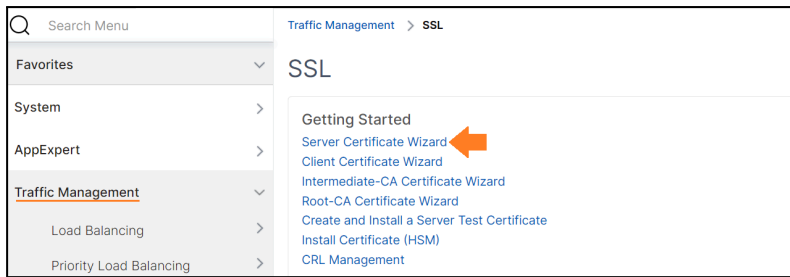
11. Enter **rootCA LAB** in the **Certificate-Key Pair Name** input field, and then click **Create**.



12. You will see the message "SSL Certificate-Key pair rootCA LAB installed successfully" within a green box. Click **Done**.

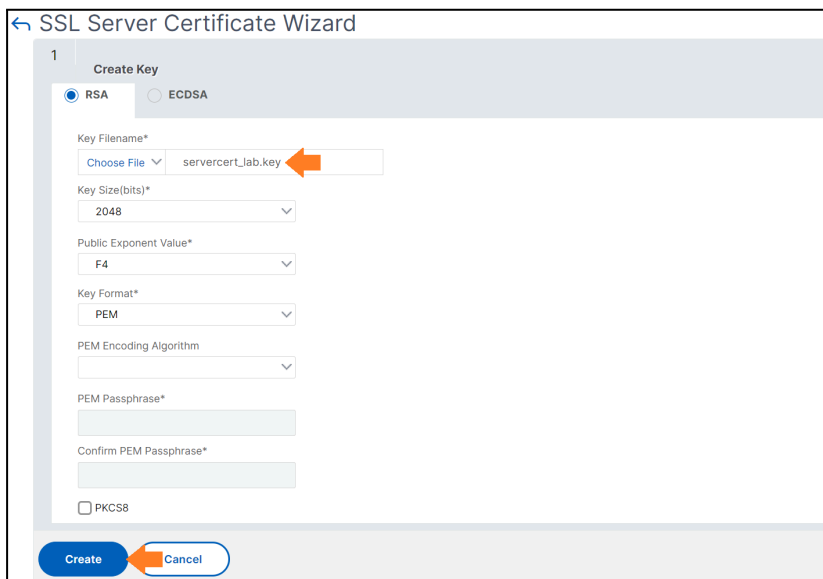


13. Click **Server Certificate Wizard** to create the Server certificate.



14. Enter **servercert\_lab.key** in the **Key Filename** input field.

15. Keep the other settings as default and click **Create**.



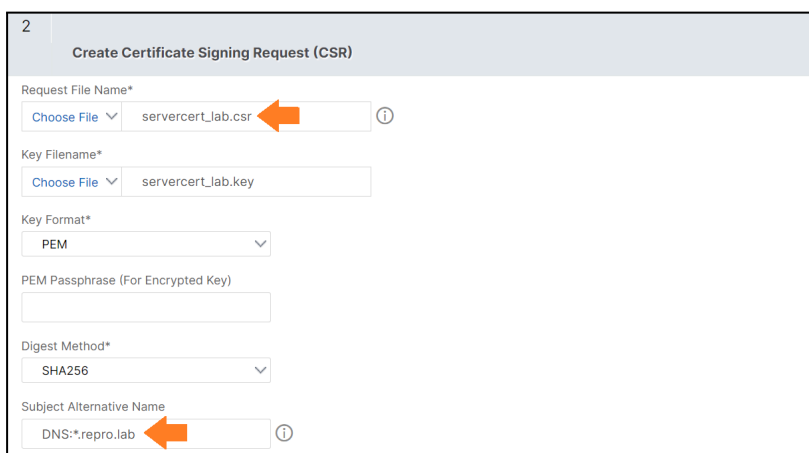

---

**Note:** **RSA KEY** will be used during this training. **ECDSA KEY** is also an option (ECDSA cipher suites use elliptical curve cryptography (ECC) with DHE key algorithm). **ECC CURVES** must be bound to the SSL Vservers.

---

16. Enter **servercert\_lab.csr** in the **Request File Name** input field.

17. Enter **DNS:\*.repro.lab** in the **Subject Alternative Name** input field.




---

**Note:** SAN ensures that the certificate is valid for all specified names, providing flexibility and convenience for securing various components within a network or server.

---

18. Complete the mandatory fields with your region details.

19. Enter **\*.repro.lab** in the **Common Name** input field. Click **Create**.

---

**Note:** This SSL certificate (Wildcard) will be valid for any host entry associated with **“.repro.lab”**.

---

Distinguished Name Fields

Country\*  
IRELAND

State or Province\*  
Dublin

Organization Name\*  
Repro LAB

City

Email Address

Organization Unit

Common Name\*  
\*.repro.lab

Attribute Fields

Challenge Password

Company Name

Create Cancel

20. Click **No**.

Confirm

Do you want to download the created CSR file servercert\_lab.csr?

Yes No

---

**Note:** Should you wish to assign this CSR within a Public CA, you can click YES to download it.


---

21. Enter **servercert\_lab.crt** in the **Certificate File Name** input field.

You can increase the certificate validity period by changing 365 (1 year).

22. Enter **DNS:\*.repro.lab** in the **Subject Alternative Name** input field.

3 **Certificate**

Certificate File Name\*  
 


Certificate Format\*

Auditing Type  
**Server**



Certificate Request File Name\*


Key Format\*

Validity Period (Number of Days)

Subject Alternative Name  
 

23. Click **Choose File** under the **CA Certificate File Name** section, and select click **Appliance** from the drop-down list.

CA Certificate File Name\*  
   Please choose file

**Appliance** 

CA Certificate File Format\*


CA Key File Name\*

CA Key File Format\*

PEM Passphrase (For Encrypted CA Key)

CA Serial File Number\*


24. Select the Root CA certificate created before (**rootCA.crt**) and click **Open**.

**File Browser** 

Current Directory: /nsconfig/ssl/

	File Name	Type	Created	Modified
<input type="radio"/>	ns-sftrust.sig	File	Wed Dec 20 10:11:07 2023	Wed Dec 20 10:11:07 2023
<input type="radio"/>	ns-server.cert.23-12-20-10:47:49	File	Wed Dec 20 10:11:07 2023	Wed Dec 20 10:11:07 2023
<input type="radio"/>	ns-server.key.23-12-20-10:47:49	File	Wed Dec 20 10:11:06 2023	Wed Dec 20 10:11:06 2023
<input type="radio"/>	ns-server.req.23-12-20-10:47:49	File	Wed Dec 20 10:11:06 2023	Wed Dec 20 10:11:06 2023
<input type="radio"/>	rootCA_lab.csr	File	Fri Jan 5 10:02:58 2024	Fri Jan 5 10:02:58 2024
<input checked="" type="radio"/>	rootCA.crt	File	Fri Jan 5 10:06:13 2024	Fri Jan 5 10:06:13 2024
<input type="radio"/>	servercert_lab.key	File	Fri Jan 5 10:36:53 2024	Fri Jan 5 10:36:53 2024
<input type="radio"/>	servercert_lab.csr	File	Fri Jan 5 10:50:27 2024	Fri Jan 5 10:50:27 2024

Total 25      25 Per Page      Page 1 of 1

**Open**  **Cancel**

25. Click **Choose File** under the **CA Key File Name** section, and select click **Appliance** from the drop-down list.

CA Certificate File Name\*  
Choose File ▾ rootCA.crt ⓘ

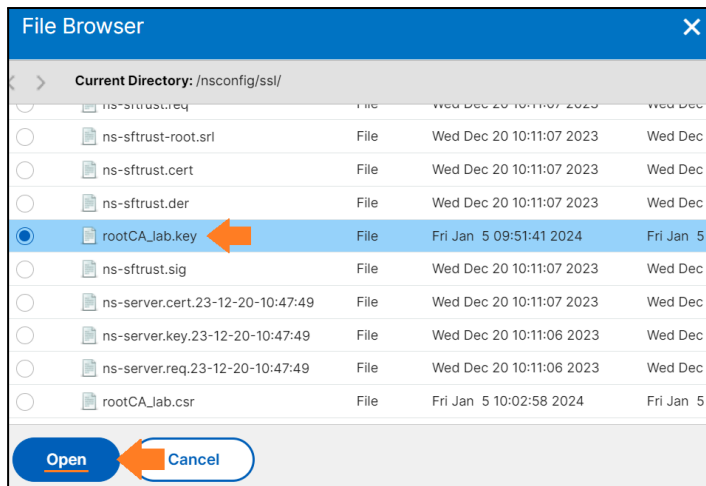
CA Certificate File format\*  
PEM ▾

CA Key File Name\*  
Choose File ▾ ⓘ Please choose file  
Appliance ←

PEM Passphrase (For Encrypted CA Key)  
[Empty field]

CA Serial File Number\*  
Choose File ▾ [Empty field]

26. Select the Root CA Key File created before (**rootCA\_lab.key**) and click **Open**.



27. Enter **servercert\_lab.txt** in the **CA Serial File Number** input field and click **Create**.

CA Certificate File Name\*  
Choose File ▾ rootCA.crt ⓘ

CA Certificate File format\*  
PEM ▾

CA Key File Name\*  
Choose File ▾ rootCA\_lab.key ⓘ

CA Key File Format\*  
PEM ▾

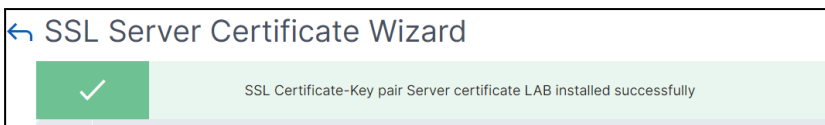
PEM Passphrase (For Encrypted CA Key)  
[Empty field] ⓘ

CA Serial File Number\*  
Choose File ▾ servercert\_lab.txt ← ⓘ

Create ← Cancel

28. Enter the name **Server certificate LAB** and click **Create**.

29. You will notice a message “SSL Certificate-Key pair Server certificate LAB installed successfully” in a green box. Click **Done**.



30. To see the SSL certificate installed, navigate to **SSL > Certificates > Server Certificates**.

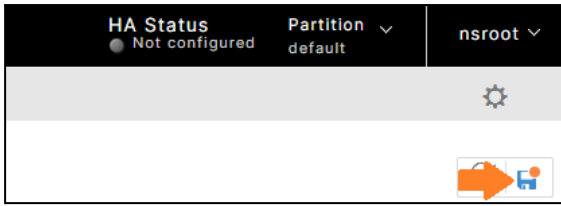
NAME	CERTIFICATE TYPE	COMMON NAME	ISSUER NAME
ns-server-certificate	CLINT_CERT, SRVR_CERT	default BANZVD	default BANZVD
Server certificate LAB	CLINT_CERT, SRVR_CERT	*repro.lab	RootCA LAB

**Notes:**

1. By default, all the SSL keys, CSR, and Certificates are located in the /nsconfig/ssl directory.
2. Client machines usually contain the ROOT CA certificate in their local certificate store, but not one or more Intermediate CA certificates. The NetScaler must send one or more intermediate CA certificates to the clients, but the appliance must not send the ROOT CA certificate to the client. Check out the official documentation.
3. The Public Key Infrastructure (PKI) trust relationship model requires ROOT CA certificates to be installed on clients through an out-of-band method. The client ignores a ROOT CA certificate sent by the appliance.
4. The ROOT CA was linked as an example of what must be done in case you have an INTERMEDIATE certificate. The INTERMEDIATE certificate is the correct certificate that must be linked and not the ROOT CA (The ROOT CA certificate must be present on the CLIENT side).

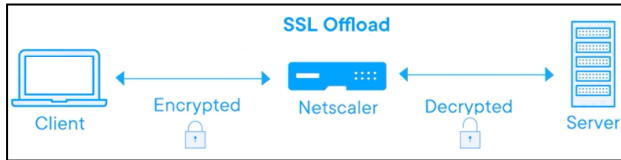
31. Save the configuration.





# Configuring an SSL Offloading LB VIP

SSL offloading on the NetScaler refers to the process of relieving the backend servers of the task of decrypting and encrypting SSL/TLS traffic. In this setup, the NetScaler appliance takes on the responsibility of handling SSL/TLS encryption and decryption, thereby offloading this intensive task from the backend servers. The virtual server intercepts SSL traffic, decrypts it, and then forwards it to a service or services bound to the virtual server. The image below illustrates the setup.



## Notes:

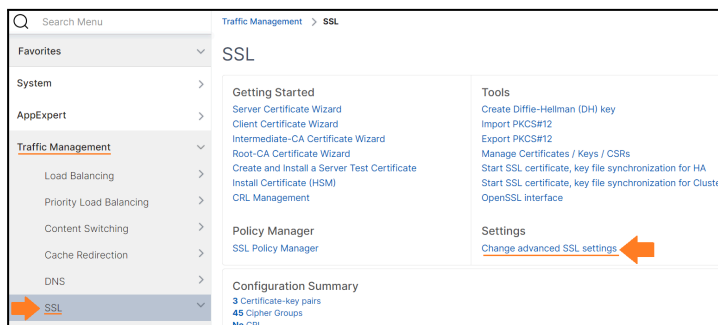
Enable the SSL feature under **System > Settings > Basic Features > SSL Offload** before proceeding.

CSG recommends using the enhanced profiles instead of legacy profiles. For information about the enhanced profile infrastructure, see [SSL profile infrastructure](#).

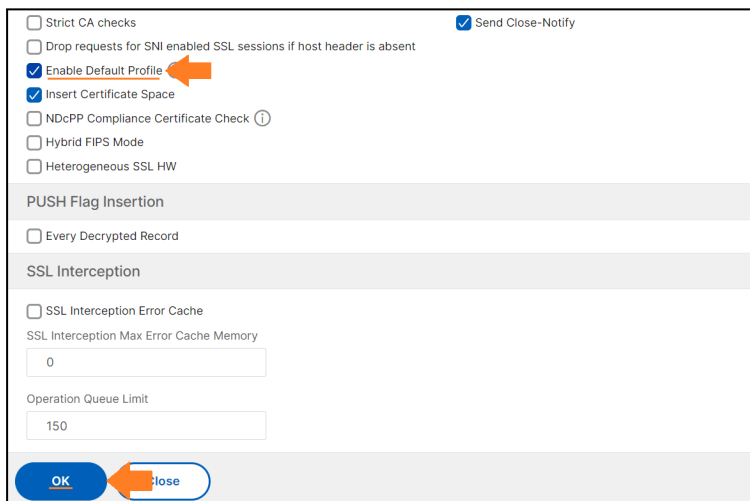
## Enabling Enhanced/Default SSL Profile

Follow these steps to enable enhanced/default SSL profile:

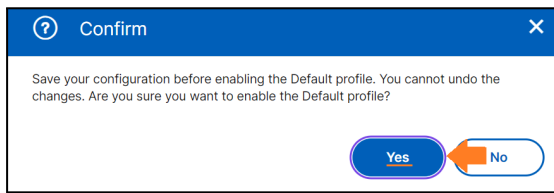
1. Navigate to **Traffic Management > SSL**, and under **Settings**, click **Change advanced SSL settings**.



2. Scroll down the page and enable **“Enable Default Profile”**. Click **OK**.

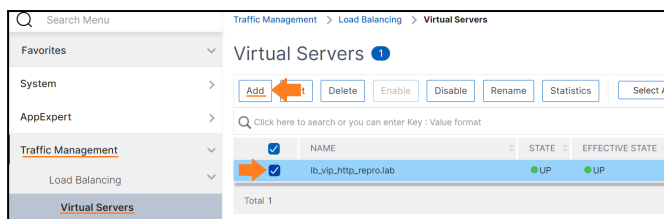


- Click **Yes** to confirm.



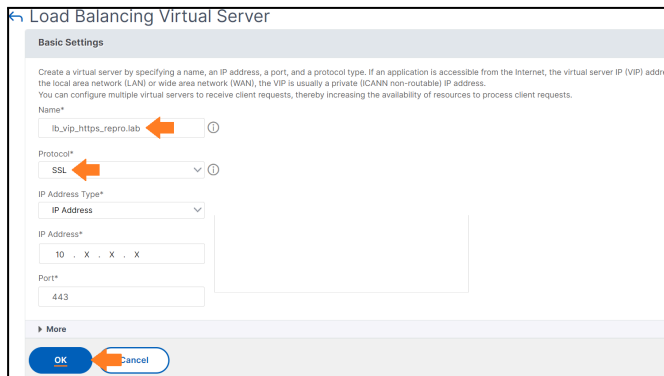
**Note:** When you enable the **default profile**, the inbuilt default SSL profile is automatically bound to all the **front-end SSL entities**, and the **ns\_default\_ssl\_profile\_backend** is bound to all the **back-end SSL entities**. The profile comes with some **default settings** and when you enable the default profile, your **custom settings are lost**. Manually fixing a large configuration can be tedious, time-consuming, and error-prone. For more information, check out the [official documentation](#).

- On the **NetScaler ADC01**, navigate to **Traffic Management > Load Balancing > Virtual Servers**, select the existing **HTTP Virtual Server** you already have, and click **Add**.

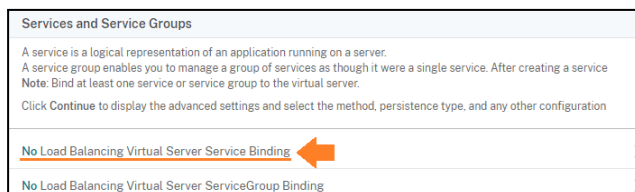


**Note:** The IP address assigned to the HTTP VIP will also be used for the HTTPS VIP. Besides conserving an IP address, using the same IP address will simplify the HTTP to HTTPS redirection, which will be covered later.

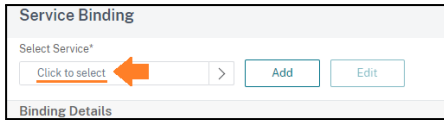
- Enter the name **lb\_vip\_https\_repro.lab**, change the protocol to **SSL**, keep your **IP address**, and ensure the port of VIP is **443**. Click **OK**.



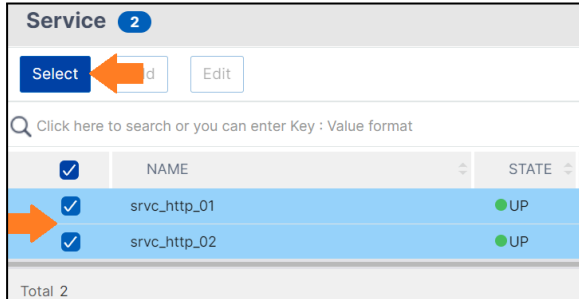
- Under **Services and Service Groups**, click **No Load Balancing Virtual Server Service Binding** and bind your Web servers port 80 you have configured before.



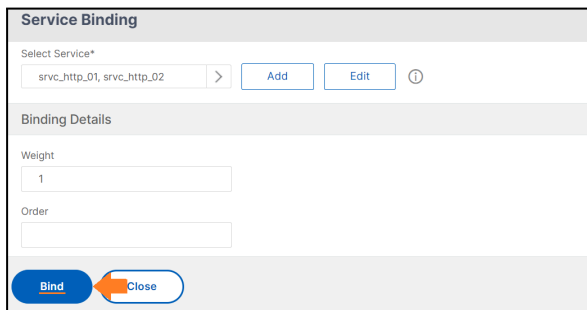
- Select **Click to Select**.



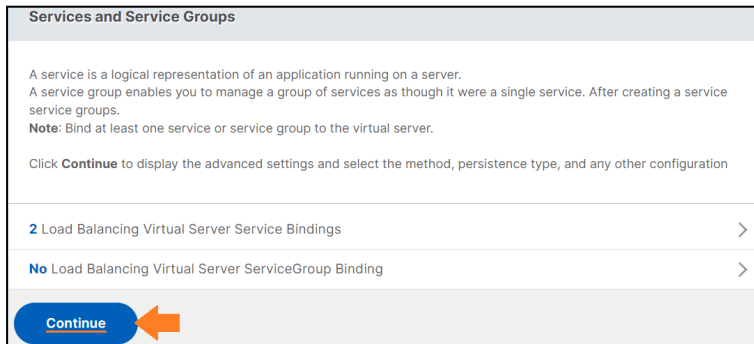
8. Select all your services and click **Select**.



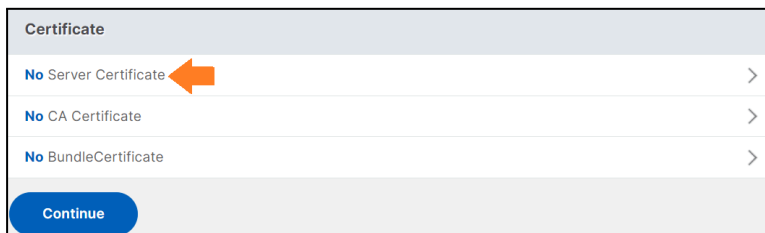
9. Click **Bind** to bind all the services to your SSL Load balance VIP.



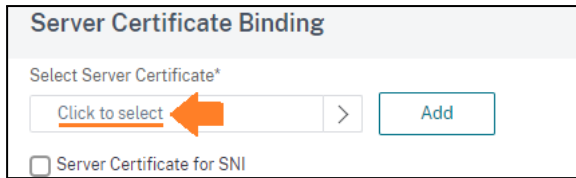
10. Click **Continue**.



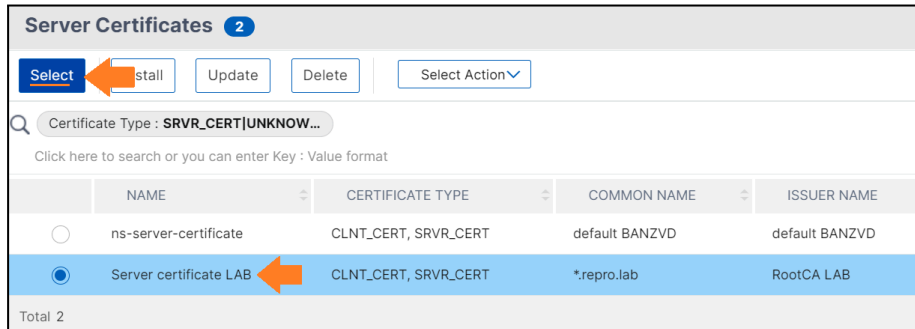
11. Under **Certificate**, click **No Server Certificate** to select the Certificate created before.



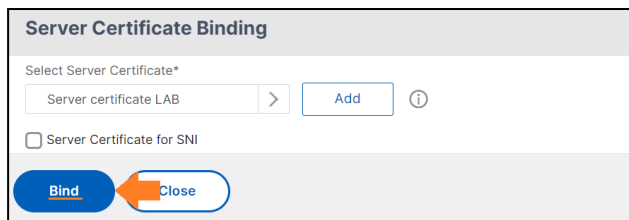
12. Click **Click to Select**.



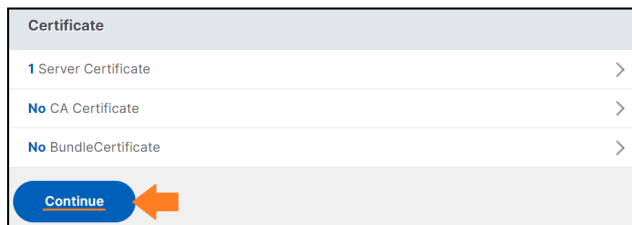
13. Select the Server Certificate **Server Certificate LAB** and click **Select**.



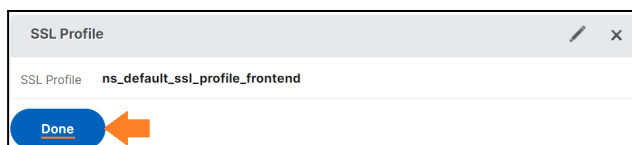
14. Click **Bind**.



15. Click **Continue**.



16. Click **Done**.



17. The SSL VIP is now configured with the default SSL parameters. HTTP and HTTPS VIPs should appear as below.

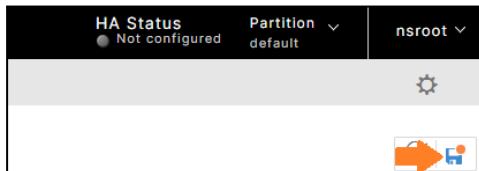
Traffic Management > Load Balancing > Virtual Servers

### Virtual Servers 2

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE	IP ADDRESS	PORT	PROTOCOL
<input type="checkbox"/>	lb_vip_http_repro.lab	UP	UP	10.x.x.x	80	HTTP
<input type="checkbox"/>	lb_vip_https_repro.lab	UP	UP	10.x.x.x	443	SSL

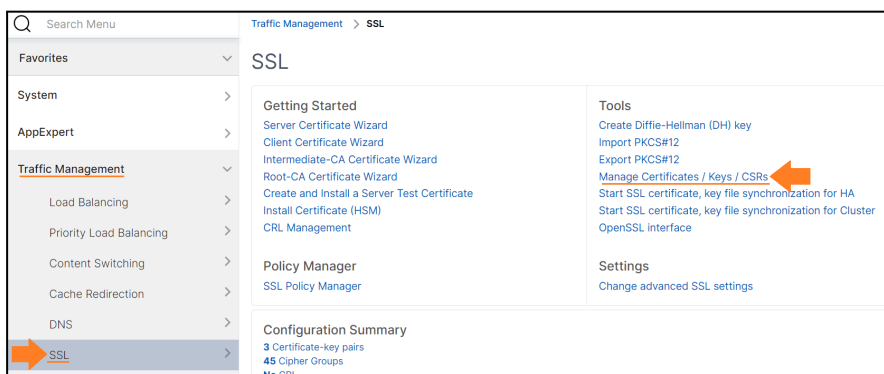
18. Save the config.



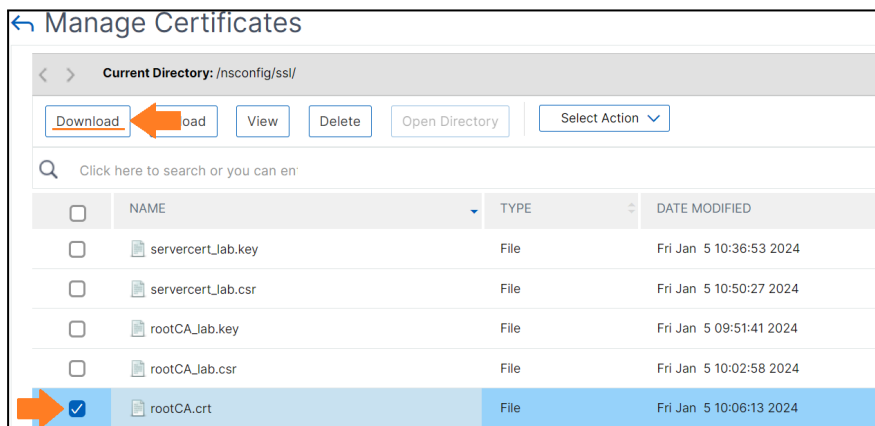
## Installing the Root CA certificate on Windows Client (Jump box)

**Note:** A root certificate authority (CA) installed on a machine is essential for ensuring the trust, security, and authenticity of digital interactions. In our specific scenario, we will install the **root CA** certificate from the **NetScaler Internal CA** to validate the SSL Server certificate presented by the SSL LB VIP. The first step involves downloading the CA certificate from the NetScaler and installing it on the Jump Box VM.

1. On the NetScaler, navigate to **Traffic Management > SSL** and click **Manage Certificates/Keys/CSRs**.



2. Locate the **rootCA.crt** created before and click **Download**.

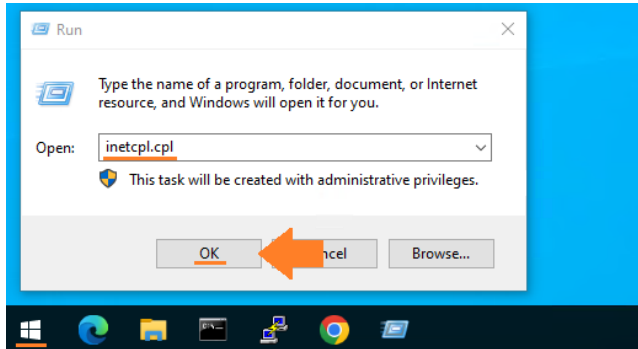


3. The certificate is ready to be installed on the Jump box VM.

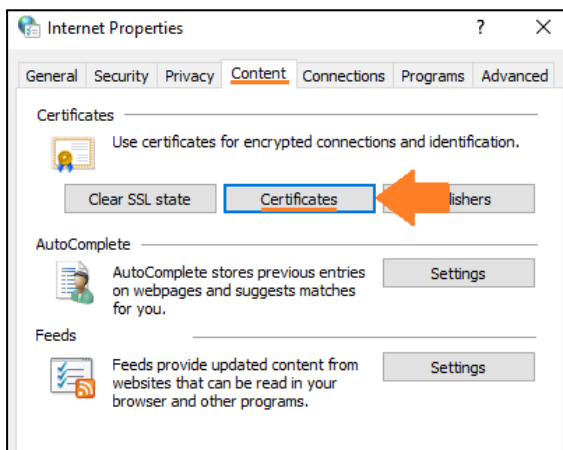




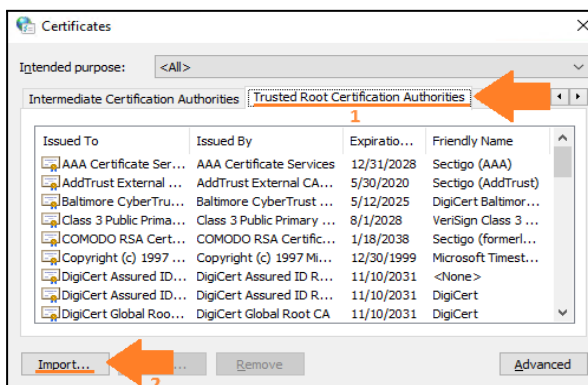
4. On your client VM, navigate to **Start > Run >** and enter **inetcp.cpl**.



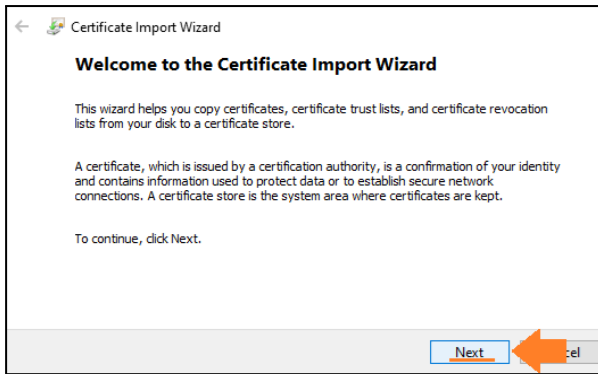
5. Click **Content** and then **Certificates**.



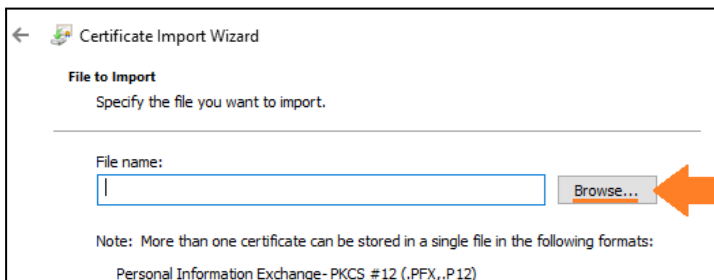
6. Select the **Trusted Root Certification Authorities** tab and then click **Import**.



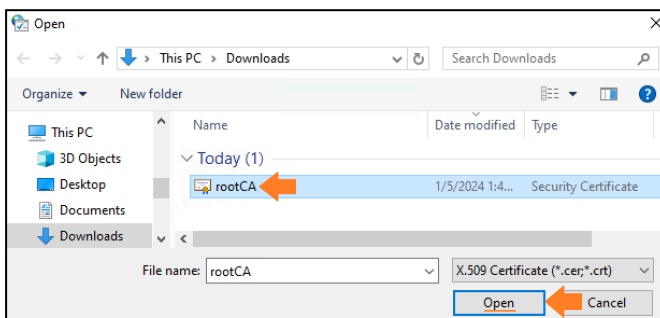
7. Click **Next**.



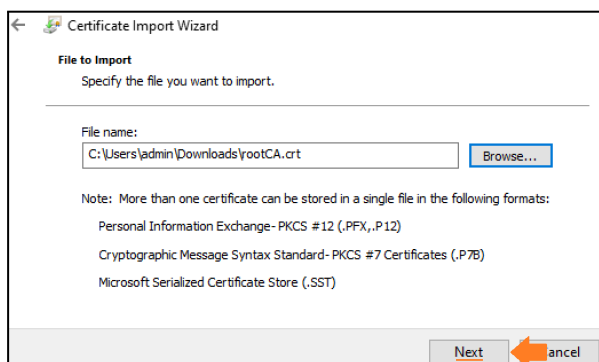
8. Click **Browse**.



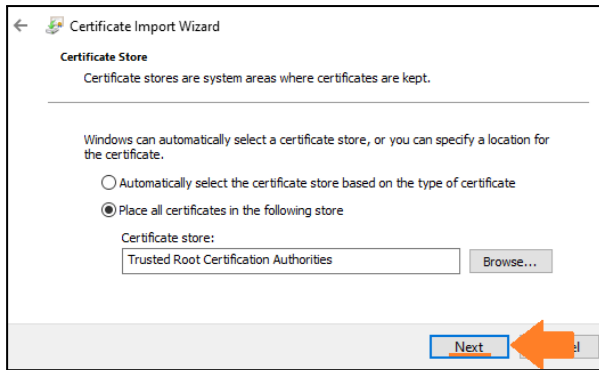
9. Select the **Root CA certificate** you have downloaded before from the NetScaler.



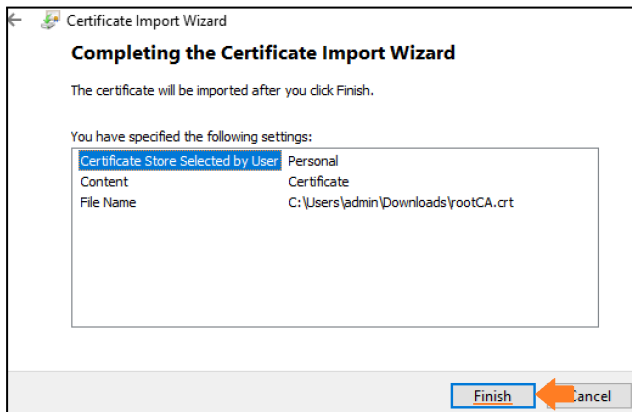
10. Click **Next**.



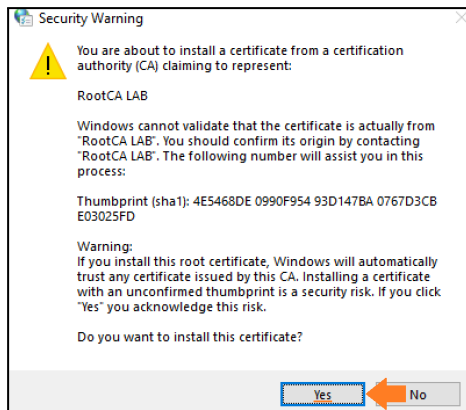
11. Click **Next**.



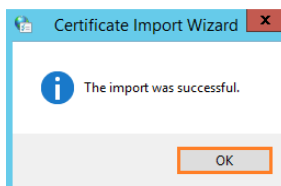
12. Click **Finish**.



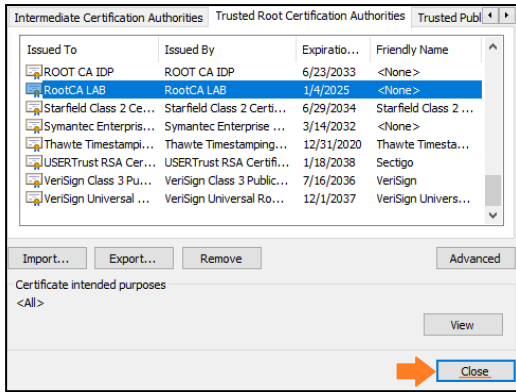
13. Click **Yes** to trust any certificate issued by your **ROOT CA certificate**.



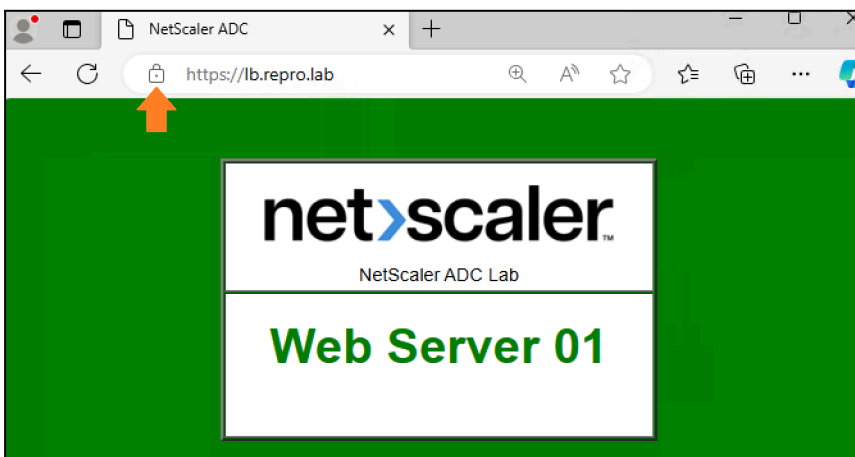
14. Click **OK**.



15. The **Root CA certificate** is now listed and installed. Click **Close**.



16. From your **Jump box VM**, open your browser and **type** the hostname <https://lb.repro.lab>. You should be able to see your page with **no** SSL issues as below.



Notes:

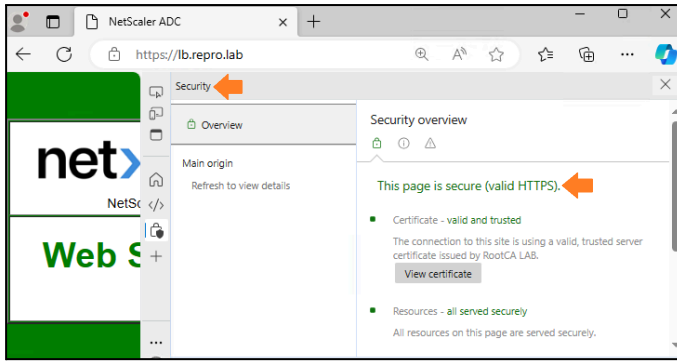
1. If you type `https://YOUR-VIP-Address`, you will show a certificate warning due to a Common Name issue.
2. Since you added an internal entry in the Windows hosts file for the HTTP LB VIP lab, and the IP address for both the HTTP and HTTPS VIPs are identical, the FQDN "lb.repro.lab" functions interchangeably for both.

## Enabling TLS 1.3

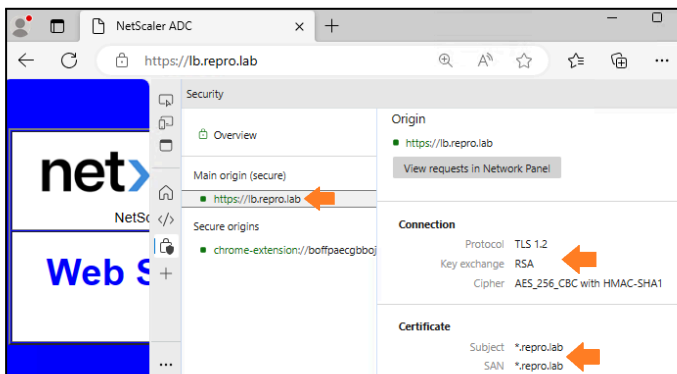
**Note:** TLS 1.3 is disabled by default on an SSL profile. For more about TLS 1.3, check the following doc [Enable TLS 1.3](#).

Follow these steps to enable TLS 1.3:

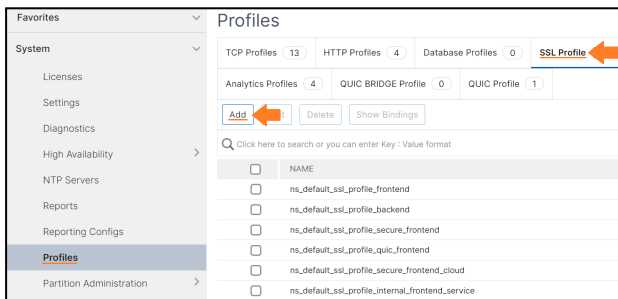
1. Using the **Development tools**, you can check what is the **TLS/cipher version** in place. On your browser, navigate to **Settings > More tools > Developer tools** and select the **Security** tab to review SSL information, including TLS version, ciphers, and protocols. In our case, **TLS 1.2** and **AES\_256\_CBC**.



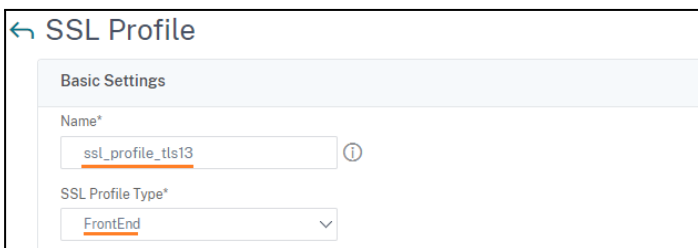
- Refresh the page once more, and on the left side, click your domain to view more information.



- To create a custom SSL profile, navigate to **System > Profiles > SSL Profile** and click **Add**.



- Enter the name **ssl\_profile\_tls13** and ensure **FrontEnd** is selected.



- Scroll down the page, under the **Protocol** section, disable **TLS1/TLS11** and enable **TLS 1.3**. Click **OK** and **Done**.

Protocol

- SSLv3
- TLSv1 ⓘ
- TLSv11 ⓘ
- TLSv12 ←
- TLSv13 ⓘ
- Zero RTT Early Data

ECC Curve ×

5 ECC Curves >

**Done** ←

6. Your profile is ready for binding (next step). Once bound, you can utilize **Show bindings** to identify its associations.

Profiles

TCP Profiles 13   HTTP Profiles 4   Database Profiles 0   **SSL Profile 7**   SSL Log Profile 0

Analytics Profiles 4   QUIC BRIDGE Profile 0   QUIC Profile 1

[Add](#)   [Edit](#)   [Delete](#)   [Show Bindings](#)

🔍 Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME
<input checked="" type="checkbox"/>	ssl_profile_tls13

7. Navigate to Traffic Management > Virtual Servers and Edit your SSL LB Virtual Server.

Favorites

System >

AppExpert >

Traffic Management

Load Balancing >

**Virtual Servers** ←

Virtual Servers 2

[Add](#)   **[Edit](#)** ←   [Delete](#)   [Enable](#)   [Disable](#)   [Rename](#)   [Statistics](#)   [Select All](#)

🔍 Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE
<input type="checkbox"/>	lb_vip_http_repro.lab	UP	UP
<input checked="" type="checkbox"/>	lb_vip_https_repro.lab	UP	UP

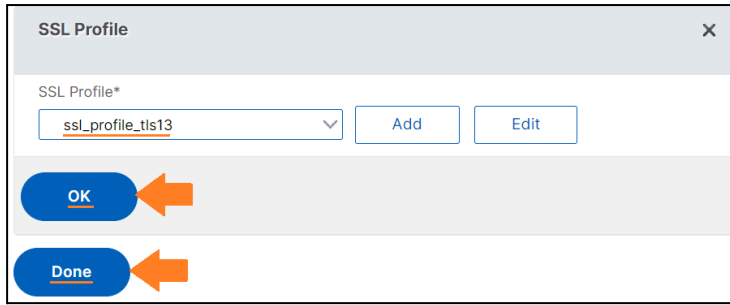
Total 2

8. Under "SSL Profile", click to Edit.

SSL Profile ✎ ←

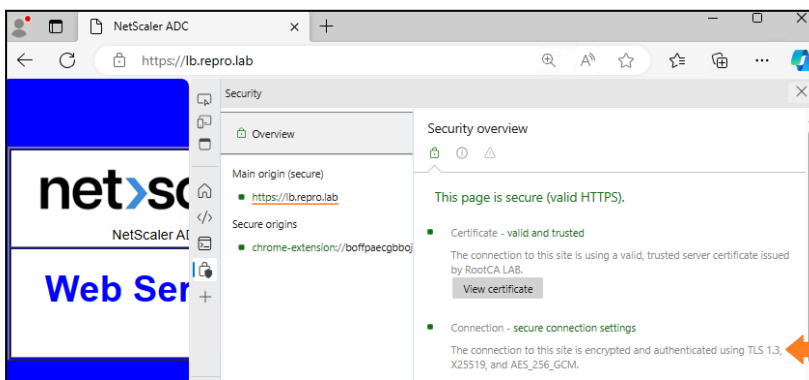
SSL Profile **ns\_default\_ssl\_profile\_frontend**

9. Select the profile created "ssl\_profile\_tls13", click **OK** and **Done**.



**Note:** This SSL profile can be applied across multiple VIPs to ensure they will share the same SSL parameters.

10. If you **re-do** the test and check the **Security** tab again, you will see **TLS 1.3** in place along with **AES\_256\_GCM**.

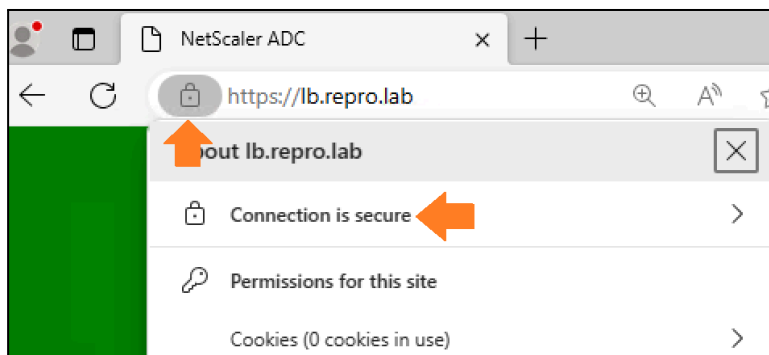


**Note:** The DEFAULT SSL CIPHER group already includes TLS 1.3 ciphers, eliminating the need for manual activation.

11. Save the configuration.

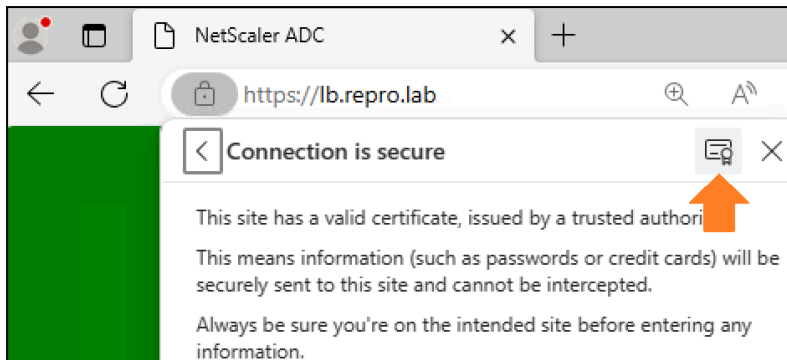
## Troubleshooting Common SSL Client Issues

1. Click the secure padlock and then click **Connection is secure**.

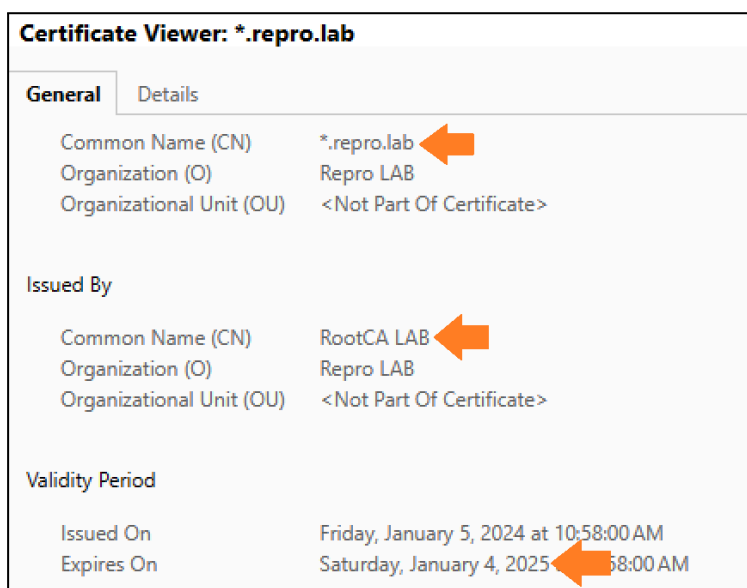


2. Click the certification icon.

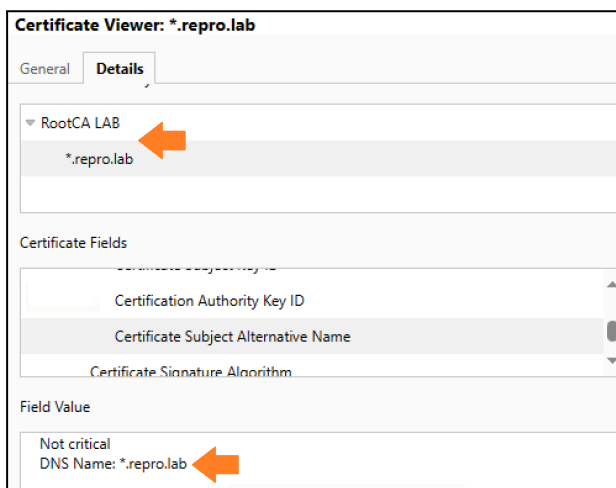




3. You can check some important information that might cause SSL Warnings/Errors if not correct.  
You can check the certificate's validity, issuer name, common name (subject), type of signature algorithm, key size, and SAN (Subject Alternative Name).



4. Under the **Details/Certificate Hierarchy** (Certification path in old browsers) tab, you can confirm the certificate chain.
5. Under the **Certificate Fields**, confirm other information.



- By capturing a full NetScaler trace, you can observe the SSL conversation between the client and the VIP, including the SSL handshake. Subsequently, the HTTP SNIP conversation with the back-end server becomes visible. After the SSL handshake, the client sends the HTTP GET, and the SNIP forwards the request to the server.

Source	Destination	Protocol	SrcPort	DestPort	Info
Client-PC	lb.repro.lab	TCP	52441	443	52441 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1
lb.repro.lab	Client-PC	TCP	443	52441	443 → 52441 [SYN, ACK] Seq=0 Ack=1 Win=8190 L
Client-PC	lb.repro.lab	TCP	52441	443	52441 → 443 [ACK] Seq=1 Ack=1 Win=12590848 Le
Client-PC	lb.repro.lab	TLSv1.2	52441	443	Client Hello
lb.repro.lab	Client-PC	TLSv1.2	443	52441	Server Hello
lb.repro.lab	Client-PC	TCP	443	52441	443 → 52441 [PSH, ACK] Seq=102 Ack=518 Win=13
lb.repro.lab	Client-PC	TLSv1.2	443	52441	Certificate, Server Hello Done
Client-PC	lb.repro.lab	TCP	52441	443	52441 → 443 [ACK] Seq=518 Ack=1562 Win=125908
Client-PC	lb.repro.lab	TLSv1.2	52441	443	Client Key Exchange, Change Cipher Spec, Fini
lb.repro.lab	Client-PC	TCP	443	52441	443 → 52441 [ACK] Seq=2154 Ack=860 Win=129792
lb.repro.lab	Client-PC	TLSv1.2	443	52441	Change Cipher Spec, Finished
Client-PC	lb.repro.lab	HTTP	52441	443	GET / HTTP/1.1
SNIP	Back-end Server	TCP	54369	80	54369 → 80 [SYN] Seq=0 Win=8190 Len=0 MSS=146
Back-end Server	SNIP	TCP	80	54369	80 → 54369 [SYN, ACK] Seq=0 Ack=1 Win=29200 L
SNIP	Back-end Server	HTTP	54369	80	GET / HTTP/1.1
Back-end Server	SNIP	TCP	80	54369	80 → 54369 [ACK] Seq=14601 Ack=744 Win=30720
Back-end Server	SNIP	TCP	80	54369	80 → 54369 [ACK] Seq=16061 Ack=744 Win=30720
Back-end Server	SNIP	HTTP	80	54369	HTTP/1.1 200 OK (text/html)
SNIP	Back-end Server	TCP	54369	80	54369 → 80 [ACK] Seq=744 Ack=17521 Win=138752

- You can see the **Client Hello** and **Server Hello** and TLS and Cipher selected.

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 512

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 508

Version: TLS 1.2 (0x0303)

> Random: e3ca9b62c3ee845ec96c7bbf8ee19a85927e839f5330a157b7ca887d8e514

Session ID Length: 32

Session ID: 99c18f22cd87c400963eee22e63c58125ccea7f5dcfd6acb64f0f4e41e35354d

Cipher Suites Length: 32

▼ Cipher Suites (16 suites)

Cipher Suite: Reserved (GREASE) (0xaeaa)

Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)

Cipher Suite: TLS\_AES\_256\_GCM\_SHA384 (0x1302)

Cipher Suite: TLS\_CHACHA20\_POLY1305\_SHA256 (0x1303)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 59

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 55

Version: TLS 1.2 (0x0303)

> Random: 62ab2149d03a8f389b6c8d10be0021ee51ed9a3568831e2f9aac9b32bbe5ff

Session ID Length: 0

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)

Compression Method: null (0)

Extensions Length: 15

> Extension: application\_layer\_protocol\_negotiation (len=11)

[JA35: 7599681580be1df90c786a4b8c44bf39]

## Using OpenSSL tool to match SSL Certificate and SSL Key

To check if an **SSL certificate** and **private key** match using OpenSSL, you can use the following commands:

command: `cd /nsconfig/ssl`

command: `openssl x509 -noout -modulus -in certificate.cert | openssl sha256`

command: `openssl rsa -noout -modulus -in private-key.key | openssl sha256`

Note: Replace certificate.cert with your SSL certificate file and key-file.key with your private key file.

```
root@ADC03# cd /nsconfig/ssl
root@ADC03# openssl x509 -noout -modulus -in certificate-name.cert | openssl sha256
(stdin)= 3848ee913e634f4d5171c86e274b655877f8e983753400b790f8847b1c8a0d77
root@ADC03#
root@ADC03# openssl rsa -noout -modulus -in key-file.key | openssl sha256
(stdin)= 3848ee913e634f4d5171c86e274b655877f8e983753400b790f8847b1c8a0d77
root@ADC03#
```

If the output (stdin) of both commands is the same, then the **certificate** and **private key match**. The modulus is a mathematical property of the key, and if it matches between the certificate and the private key, it indicates a match. If there is a mismatch, you will see different outputs.

To view the content of an **SSL certificate** or **SSL key file** using OpenSSL, you can use the following commands:

command: `cd /nsconfig/openssl`

command: openssl x509 -noout -text -in certificate-name.cer

command: openssl rsa -noout -text -in key-file.key

```
root@ADC03# openssl x509 -noout -text -in certificate-name.cer
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      1f:00:00:00:05:c0:d1:d6:3e:8d:04:9b:da:00:00:00:00:05
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=lab, DC=repro, CN=ROOT CA AD NEW LABSTAGE
    Validity
      Not Before: May 22 09:40:46 2023 GMT
```

```
root@ADC03# openssl rsa -noout -text -in key-file.key
Private-Key: (2048 bit)
modulus:
  00:ea:c2:69:36:0d:bc:9d:d5:96:d3:36:22:e1:17:
  8c:1f:0e:de:83:2a:f9:e8:3a:c3:ca:c2:4c:85:56:
  da:50:93:ae:a3:2e:0d:e6:c6:11:bc:1d:72:4b:24:
  63:a6:b5:05:3c:ee:de:ab:22:9f:01:e3:4e:32:42:
  fb:0f:b5:2f:cd:67:8c:24:71:22:ef:6d:25:f6:af:
  e1:15:eb:d4:fe:4f:10:9d:2f:bd:65:a8:e6:15:1f:
```

# Configuring Rewrite and Responder Policies

## Notes:

1. Classic policy expressions are deprecated from NetScaler 12.0 build 56.20 onwards. Customers are recommended to use Advanced policies instead.
2. Enable the Rewrite feature under **System > Settings > Basic Features > Rewrite** before proceeding. Alternatively, you can enable it at the time you start the configuration.

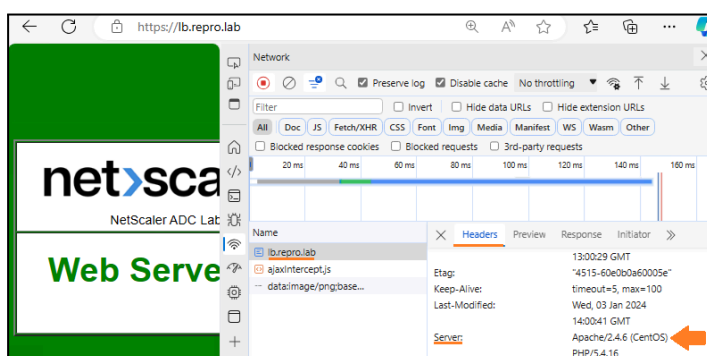
## Rewrite – Removing an HTTP Header

In this exercise, you will learn how to remove header data from the back-end server using the rewrite feature.

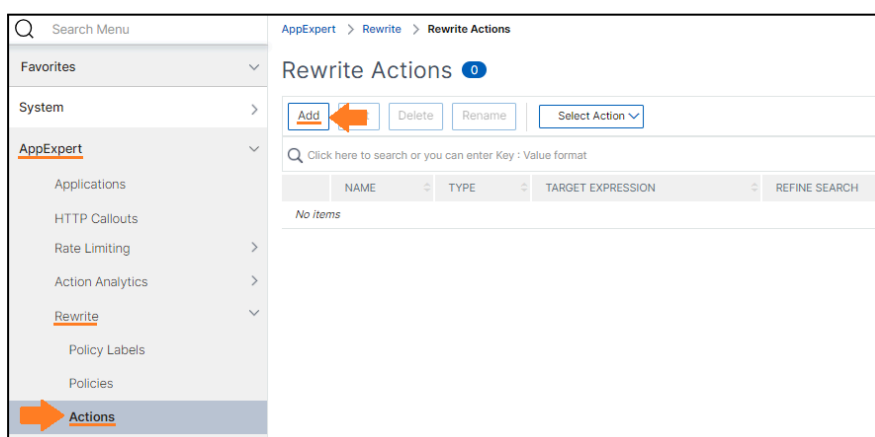
**Note:** If you do not see the header “Server” in your Web Server, you can remove other headers as testing only, such as “Last-Modified:” or “X-Powered-By:”.

The following are the steps to remove header data from the back-end server using the rewrite feature:

1. On the same page “<https://lb.repro.lab>”, open the developer tools and observe the headers. In the below example, the **Server Apache version** and **Linux dist** are visible. This is not recommended as an attacker can explore possible vulnerabilities in the versions exposed.



2. On the NetScaler, navigate to **AppExpert > Rewrite > Action**. Click **Add**.



3. Enter **action\_remove\_server\_header** in the **Name** input field.
4. Enter **DELETE\_HTTP\_HEADER** in the **Type** input field.

5. Enter **Server** in the **Header Name** input field.
6. Click **Create**.

← Create Rewrite Action

Name\*

Type\*

Use this action type to delete HTTP headers.

Header Name\*

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

**Create** Close

7. Navigate to **Rewrite > Policies** and click **Add**.

Favorites

System

AppExpert

- Applications
- HTTP Callouts
- Expressions
- Rate Limiting
- Action Analytics
- Rewrite**
  - Policy Labels
  - Policies**
  - Actions

Rewrite Policies 0

**Add** Delete Show Bindings Policy Manager Statistics Rename

Q Click here to search or you can enter Key : Value format

NAME	EXPRESSION
No Items	

8. Enter **policy\_remove\_server\_header** in the Name input field.
9. Select **action\_remove\_server\_header** from the **Action** drop-down list.
10. Enter **HTTP.RES.IS\_VALID** in the **Expression** field.
11. Click **Create**.

← Create Rewrite Policy

Name\*

Action\*

Configure Assignments

Configure Rewrite Actions

Log Action  
 **Add** **Edit**

Undefined-Result Action\*

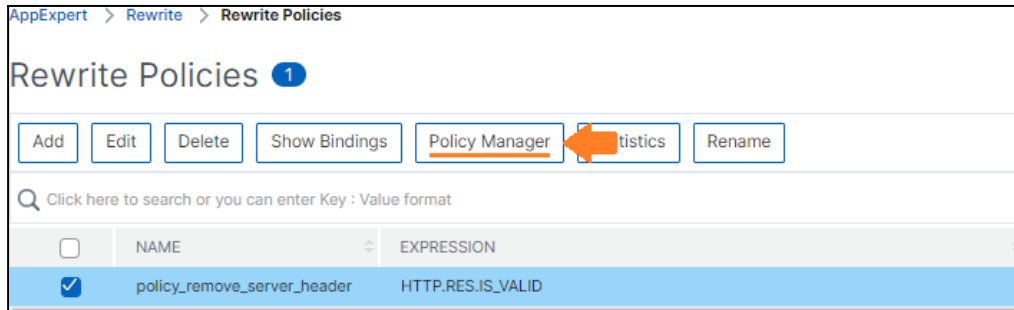
Expression\*

Comments

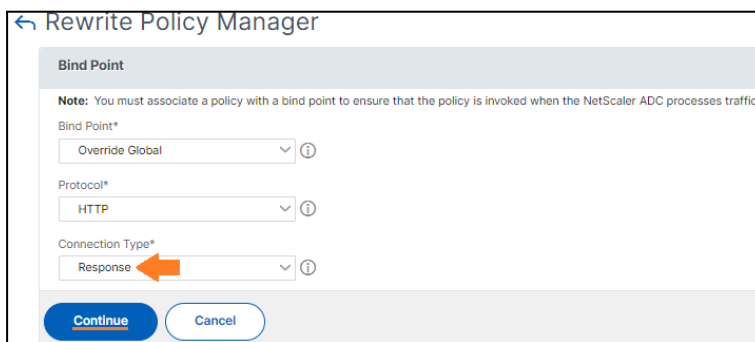
**Create** Close

**Note:** HTTP.RES.IS\_VALID returns TRUE if the HTTP request is properly formed.

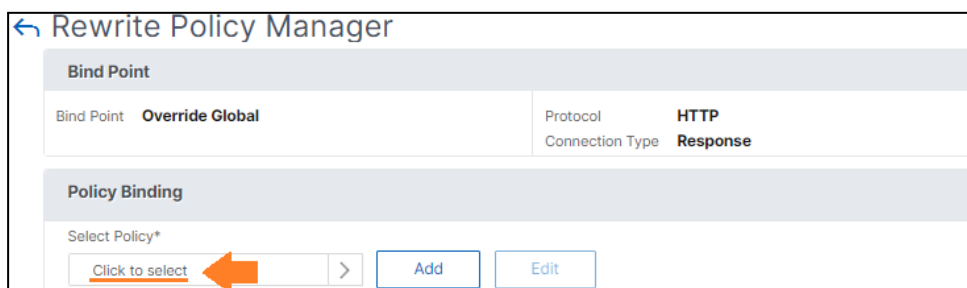
12. While still in the Rewrite Policies pane, click **Policy Manager** at the top of the screen. This policy will be bound **GLOBALLY** and not at a Virtual Server for practice purposes only. **GLOBALLY** means that ALL the HTTP responses received from the back-end servers will be evaluated.



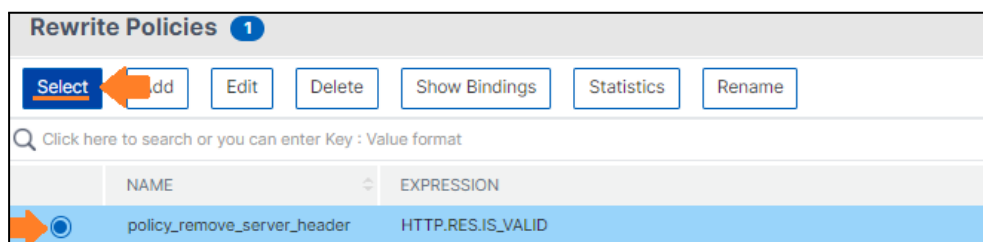
13. Select **Override Global** from the **Bind Point** drop-down list item.
14. Select **HTTP** from the Protocol drop-down list item.
15. Select **Response** from the **Connection Type** drop-down list.
16. Click **Continue**.



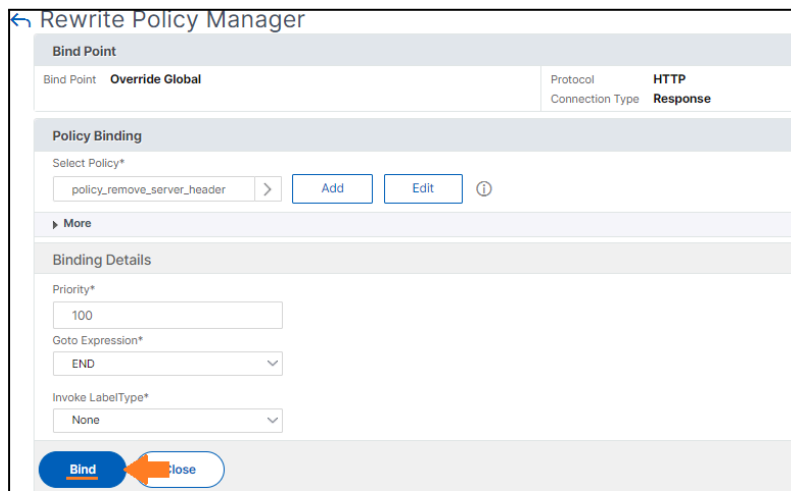
17. Click **Click to select** under the Policy Binding.



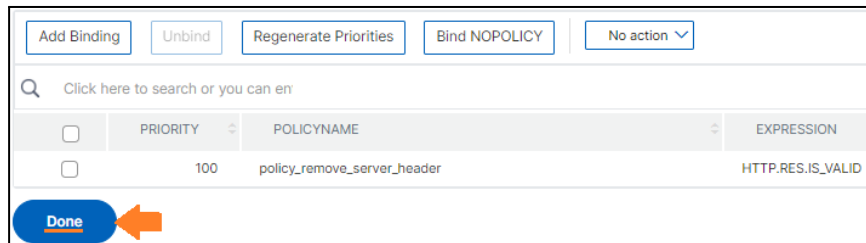
18. Select **policy\_remove\_server\_header** and then click **Select**.



Click **Bind**.

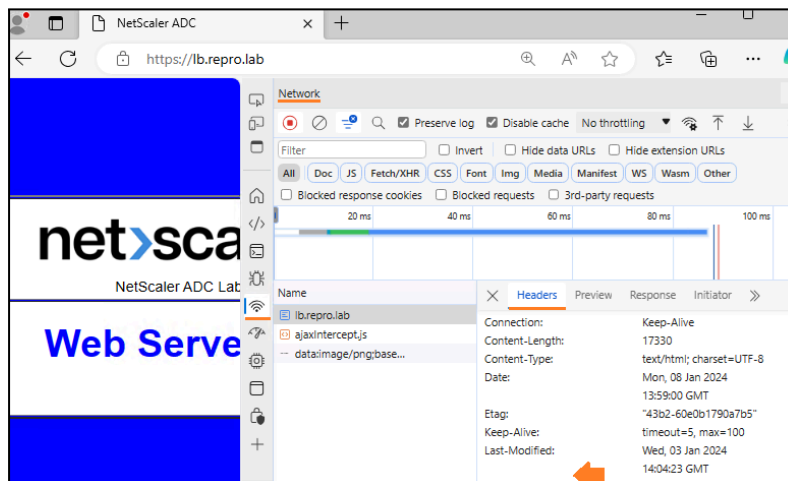


19. Click **Done**.



## Testing

From your **Jump Box VM**, open a new incognito browse page, access your VIP <https://lb.repro.lab> and check the headers once again. The header "**Server**" should not appear as it was removed by the Rewrite policy.



You can confirm the **hits** under the Responder policy page.



Rewrite Policies 1						
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Show Bindings"/> <input type="button" value="Policy Manager"/> <input type="button" value="Statistics"/>						
<input type="text" value="Click here to search or you can enter Key : Value format"/>						
<input type="checkbox"/>	NAME	EXPRESSION	ACTION	LOG ACTION	UNDEFINED-RESULT ACTION	HITS
<input type="checkbox"/>	policy_remove_server_header	HTTP.RES.IS_VALID	action_remove_server_header		-Global undefined-result action-	5

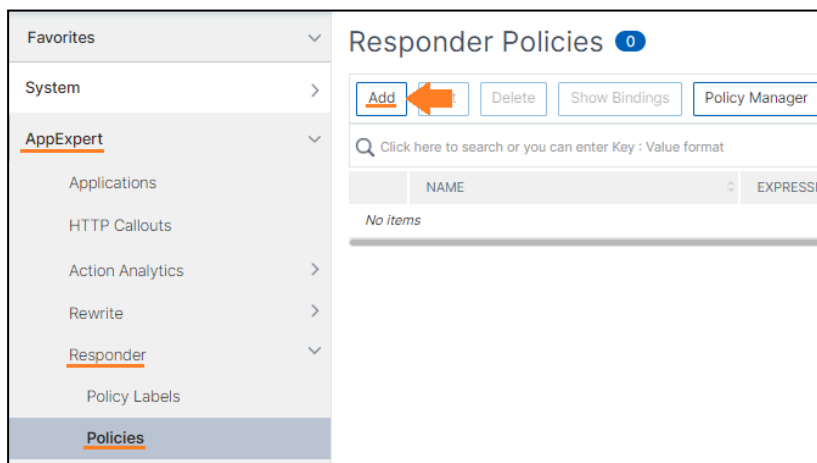
## Responder Policy to Redirect from HTTP to HTTPS

Redirecting incoming **HTTP** traffic to **HTTPS** on the NetScaler can be achieved through various methods, with the Responder policy being one of the most used. When HTTP traffic matches (evaluates) the defined Responder Policy expression, it will automatically redirect to the configured HTTPS URL.

Typically, the Responder policy is associated with the **HTTP LB VIP** (or can be applied globally). When the **HTTP LB VIP** receives a request, such as **http://lb.repro.lab/site**, the policy is evaluated, and it triggers the Responder action. This action commonly preserves the Hostname and URL path while simply switching the protocol from HTTP to HTTPS, such as **https://lb.repro.lab/site**.

The following are the steps to configure the responder on your NetScaler:

1. Navigate to **AppExpert > Responder > Policies** and click **Add**.



2. Enter the name **policy\_redirect\_to\_https** and under **Action** click **Add**.

3. Give it the name **action\_redirect\_to\_https**, change the **Type** to **Redirect**, change the **Response Status code** to 302 and paste the below expression under **Expression**.  
**"https://" + HTTP.REQ.HOSTNAME.HTTP\_URL\_SAFE + HTTP.REQ.URL.PATH\_AND\_QUERY.HTTP\_URL\_SAFE**
4. Click **Create**.

---

**Note:** The expression provided above indicates that solely the protocol will be modified to "https", while the hostname and URL will remain unchanged.

---

**Create Responder Action**

Name\*

Type\*

In string expressions, string constants and expressions can be concatenated with "+" operator.

Expression\*

Response Status Code

Reason Phrase

Comments

[Create](#) [Close](#)

5. If you get the below prompt, click Yes to enable the RESPONDER feature.

**Confirm**

Feature 'RESPONDER' is disabled.  
 Do you wish to enable it?

[Yes](#) [No](#)

6. Type the following expression under **"Expression"**: !CLIENT.SSL.IS\_SSL and click **Create**.

**Create Responder Policy**

Name\*

Action\*  
 [Add](#) [Edit](#)

Log Action  
 [Add](#) [Edit](#)

AppFlow Action  
 [Add](#) [Edit](#)

Undefined-Result Action\*

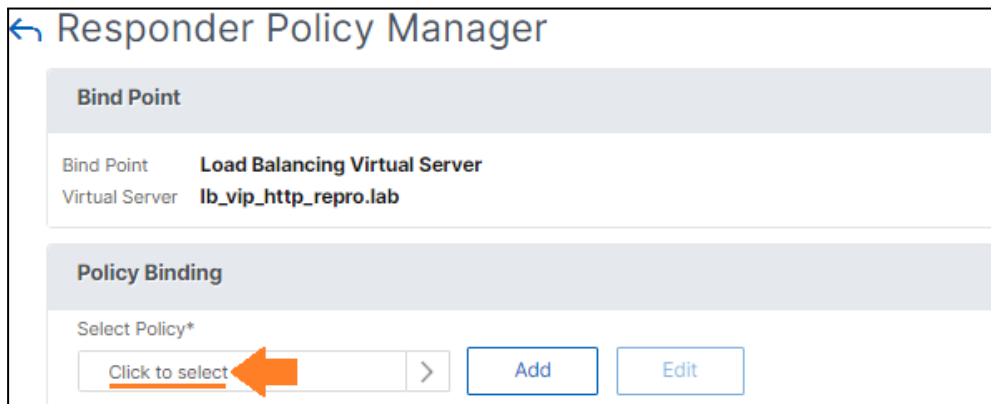
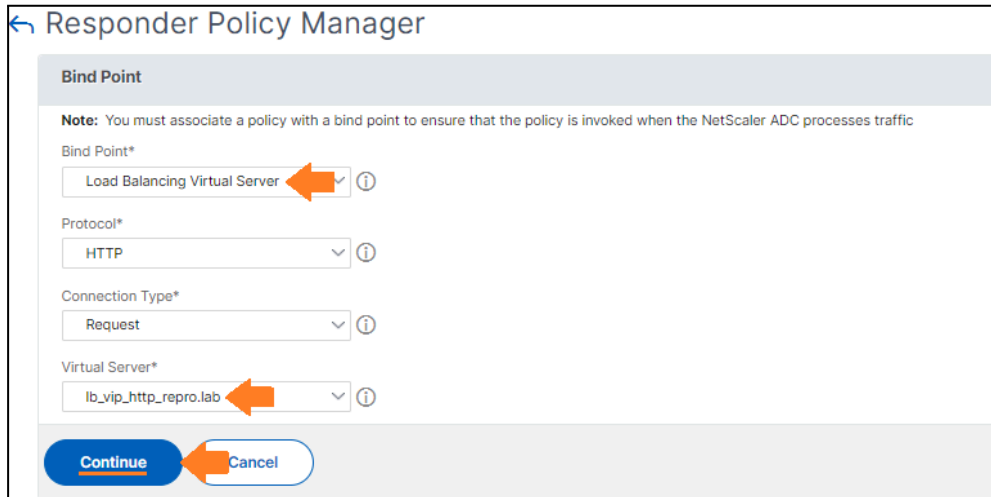
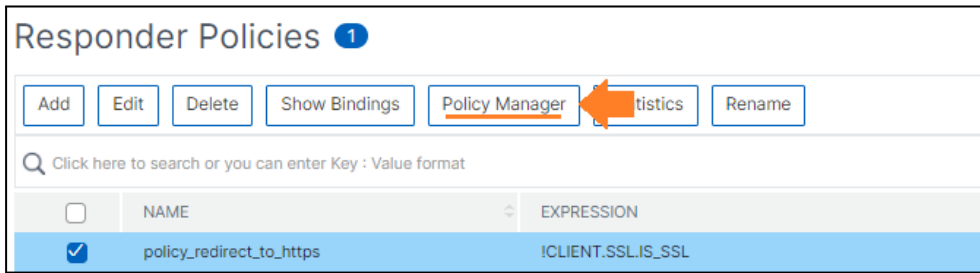
Expression\*

Comments

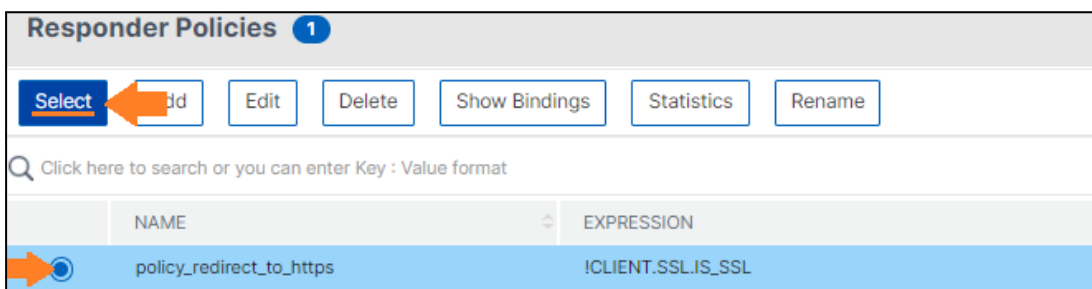
[Create](#) [Close](#)

**Note:** This Expression means that if the request received is not SSL, then the action will be triggered. The "!" symbol in front of an expression is a logical negation or "NOT" operator.

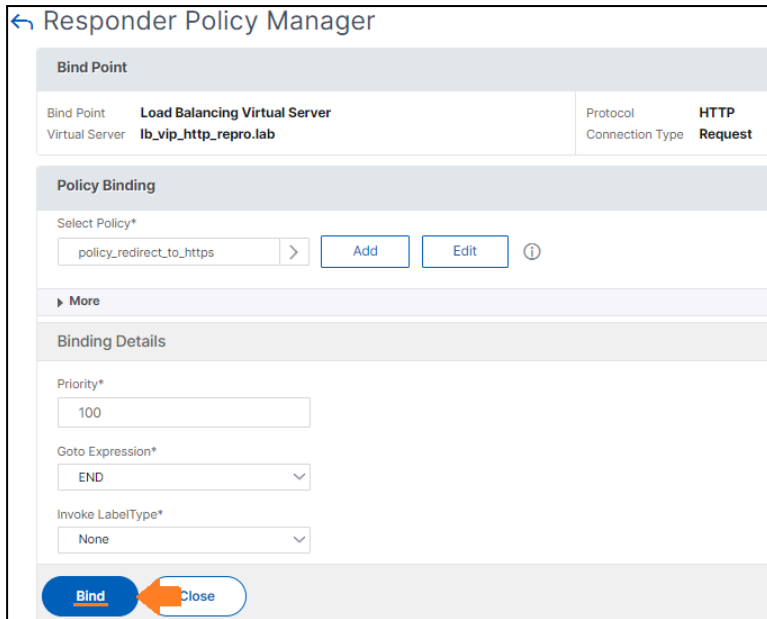
7. The responder policy is ready to be bound to the **HTTP LB VIP** on port **80**. Click **“Policy Manager”**.



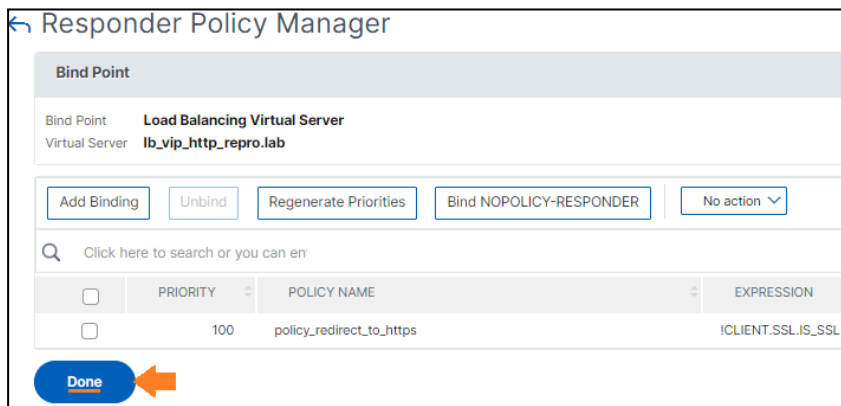
8. Select the Responder policy **policy\_redirect\_to\_https** and click **Select**.



Click **Bind**.

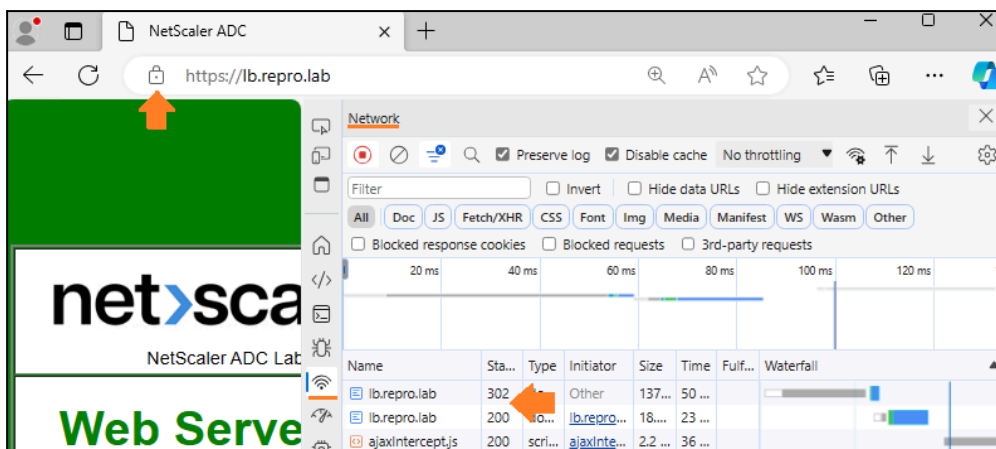


9. Scroll down and click **Done**.

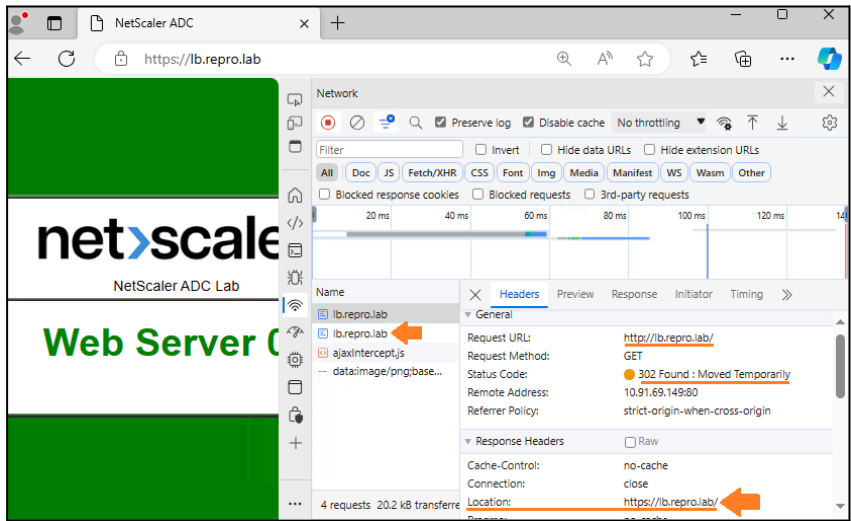


10. From your **Jump Box VM**, access the developer tools of the browser, and select the **Network** tab.

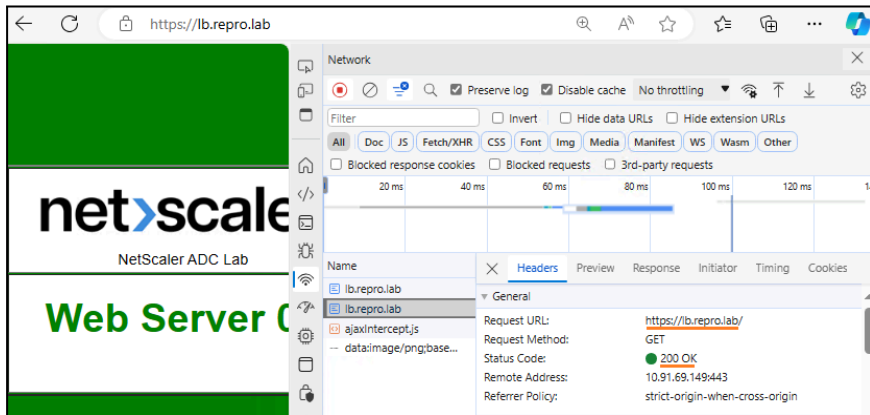
11. Type the **HTTP hostname** that resolves to your **HTTP LB VIP**, in this case, **http://lb.repro.lab**. The URL will be redirected automatically to <https://lb.repro.lab>.



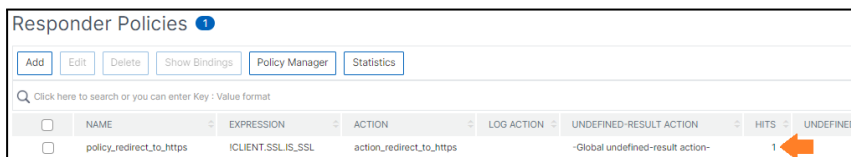
12. Under the **Network** tab, you can see the first response as **302 Moved Temporarily** and the **new location**, in this case, [HTTPS://lb.repro.lab](https://lb.repro.lab) (200 OK).



13. In the second HTTP message, you can see the HTTP response **200** and the content fetched.



14. Navigate to **AppExpert > Responder > Responder policies** to confirm the number of hits received.



### Policy hits via NetScaler shell

command: shell

command: nsconmsg -d current -g pcp\_hits

**Note:** Run the command and then access the HTTP VIP. The below is a “real-time” output. You will see two policy hists, one rewrite (remove server header), and one responder (http to https redirect).

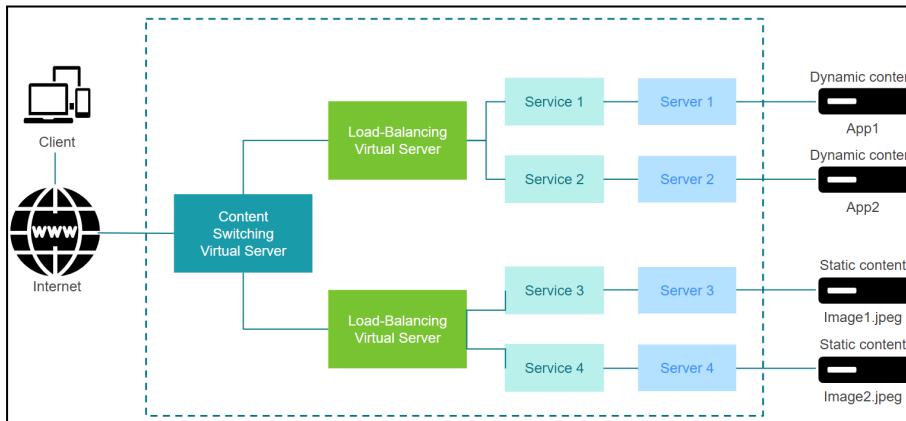
```
> shell
root@netscaler01# nsconmsg -d current -g pcp_hits
Displaying performance information
NetScaler V20 Performance Data
NetScaler NS14.1: Build 12.30.nc, Date: Nov 22 2023, 10:23:35 (64-bit)

reltime: milliseconds between two records Mon Jan 8 14:24:14 2024
  Index  rtime totalcount-val  delta rate/sec  symbol-name&device-no
    0    21034         8         1         0  pcp_hits rewrite(policy_remove_server_header)
    1         0         3         1         0  pcp_hits responder(policy_redirect_to_https)
```

15. Save the configuration.

# Configuring an HTTP Content Switching VIP

NetScaler content switching is a feature that allows you to efficiently distribute incoming network traffic to the most appropriate destination based on various criteria. When a client initiates a request to the NetScaler, the content switching feature evaluates the request against the criteria established within a content switching policy. These criteria can include factors such as the URL, host header, source IP address, HTTP method, and more. When a request matches a content switching policy, the specified action is executed, and the request is directed to a specific virtual server, in most cases, a “non-addressable” LB Virtual Server. A Non-Addressable VIP is a virtual server that does not have its own dedicated IP address and is used to route traffic without IP address binding.



## Configuring Non-Addressable Virtual Servers by CLI

For practice purposes, the following instructions will guide you in adding the non-addressable virtual servers required for Content Switching, along with their associated services. You have the option to add entities to the Netscaler using either the GUI or CLI based on your preference.

For this lab, the same HTTP Web servers added for the LB VIP will be used.

1. Add the Non-Addressable Virtual Servers + bind the Services created before (HTTP/HTTPS exercise) by the below CLI commands.

```
add lb vserver cs_vip_01 HTTP -IPPattern 0.0.0.0 -IPMask * 0
bind lb vserver cs_vip_01 svc_http_01
add lb vserver cs_vip_02 HTTP -IPPattern 0.0.0.0 -IPMask * 0
bind lb vserver cs_vip_02 svc_http_02
```

```
> add lb vserver cs_vip_01 HTTP -IPPattern 0.0.0.0 -IPMask * 0
Done
> bind lb vserver cs_vip_01 svc_http_01
Done
> add lb vserver cs_vip_02 HTTP -IPPattern 0.0.0.0 -IPMask * 0
Done
> bind lb vserver cs_vip_02 svc_http_02
Done
```

### Notes:

You might see the warning “[Secure deployment guide: Http profile bound to your server, to keep it secure enable Drop invalid HTTP requests in your http profile. This is due to the “Drop invalid HTTP request” parameter being disabled in the default HTTP profile. You can disregard this for now.

You can use the command “**rm**” to remove an entity (e.g., **rm lb vserver vip\_name**).

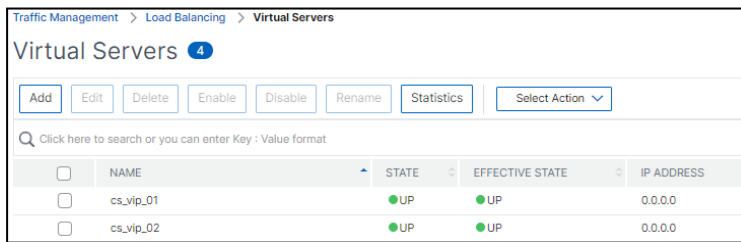


- You can verify that the non-addressable virtual servers have been successfully added and are displayed as UP.

command: show lb vserver -summary

```
> show lb vserver -summary
-----
      Name      State  Effec State  IP Addr      Port  Prot  Method
-----
1  lb_...lab  UP    UP           10.X.X.X      80    HTTP  RO...IN
2  lb_...lab  UP    UP           10.X.X.X      443   SSL   LE...ON
3  cs_vip_01  UP    UP           0.0.0.0       0     HTTP  LE...ON
4  cs_vip_02  UP    UP           0.0.0.0       0     HTTP  LE...ON
Done
```

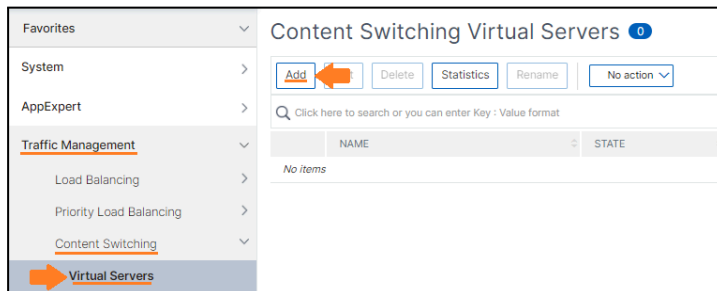
Alternatively, you can verify the same via GUI. (Traffic Management > Load Balancing > Virtual Servers)



## Configuring the Content Switching VIP and Policies

The following are the steps to configure the Content Switch VIP and Policies:

- Navigate to **Traffic Management > Content Switching > Virtual Servers** and click **Add**.



- Enter the name "**cs\_vip\_http.repro.lab**", confirm the **HTTP** protocol is selected, and **enter a new IP Address** (must be free in the network). Click **OK** to create the CS VIP.

Content Switching Virtual Server

**Basic Settings**

Name\* cs\_vip\_http.repro.lab ⓘ

Protocol\* HTTP ⓘ

Target Type\* NONE ▾

Persistence Type ▾

Persist Mask 255 . 255 . 255 . 255

IPv6 Persist Mask Length 128

Timeout 2

IP Address Type\* IP Address ▾

IP Address\* 10 . X . X . X ←

Port\* 80

More

OK Cancel

3. Click **No Content Switching Policy Bound**.

Content Switching Virtual Server

**Basic Settings**

Name	cs_vip_http.repro.lab	Listen Priority	-
Protocol	HTTP	Listen Policy Expression	NONE
Target Type	NONE	Range	1
State	● UP	IPset	-
IP Address	10.X.X.X	Traffic Domain	0
Port	80	RHI State	PASSIVE
Persistence Type	NONE	AppFlow Logging	ENABLED
Persist Mask	255.255.255.255	DTLS	false
IPv6 Persist Mask Length	128	Probe Protocol	-
Persistence Timeout	2	Probe Success Response Code	-
Backup Persistence Timeout	2	Probe Port	-
		Comments	-

**Content Switching Policy Binding**

[No Content Switching Policy Bound](#) ←

No Default Virtual Server Bound

4. Click **Add** to add the first cs policy.

**Policy Binding**

Select Policy\*

Click to select > **Add** ← Edit

5. Enter **cs\_policy\_01**, in the **Name** input field, and then click **Add** to add an Action.

6. Enter **action\_lb\_01** in the **Name** input field.
7. Click **Click to select** under **Target Load Balancing Virtual Server**.

8. Select the Non-Addressable Virtual Server "**cs\_vip\_01**" created by CLI and click **Select**.

	NAME	STATE	EFFECTIVE STATE
<input type="radio"/>	lb_vip_http_repro.lab	● UP	● UP
<input type="radio"/>	lb_vip_https_repro.lab	● UP	● UP
<input checked="" type="radio"/>	cs_vip_01	● UP	● UP

9. Click **Create**.

10. Under the expression, add the following one and click **Create**.  
**HTTP.REQ.HOSTNAME.EQ("blue.repro.lab")**

**Create Content Switching Policy**

Name\*

Action

Log Action

Expression\* [Expression Editor](#)

**NOTE:** In this example, the FQDN “blue.repro.lab” will be used and redirect the requests to the cs VIP 01 created before. Feel free to use any other FQDN.

11. Click **Bind**.

Target Load Balancing Virtual Server

>

12. Click “**1 Content Switching Policy**” to add the second cs policy.

**Content Switching Policy Binding**

1 Content Switching Policy >

No Default Virtual Server Bound >

13. Click **Add Binding**.

**Content Switching Virtual Server Content Switching Policy Binding**

<input type="checkbox"/>	PRIORITY	POLICY NAME	EXPRESSION	ACTION
<input type="checkbox"/>	100	cs_policy_01	HTTP.REQ.HOSTNAME.EQ("blue.repro.lab")	action_lb_01

14. Click **Add**.

**Policy Binding**

Select Policy\*  
 >

15. Under name, type **cs\_policy\_02**, and click **Add** under **Action**.

**Create Content Switching Policy**

Name\*  
 ⓘ

Action  
 Add Edit

16. Enter **action\_lb\_02** in the **Name** input field.
17. Click **Click to Select** under **Target Load Balancing Virtual Server**.

**Create Content Switching Action**

Name\*  
 ⓘ

Choose Virtual Server or Expression\*  
 ▾

Target Load Balancing Virtual Server\*  
 > Add Edit

18. Select the Non-Addressable Virtual Server "**cs\_vip\_green**" created via CLI and click **Select**.

**Virtual Servers** 4

Select Add Edit Delete Enable Disable Rename Statistics Select Act

Click here to search or you can enter Key : Value format

	NAME	STATE	EFFECTIVE STATE	IP ADDRESS
<input type="radio"/>	cs_vip_01	UP	UP	0.0.0.0
<input checked="" type="radio"/>	cs_vip_02	UP	UP	0.0.0.0

19. Click **Create**.

**Create Content Switching Action**

Name\*  
 ⓘ

Choose Virtual Server or Expression\*  
 ▾

Target Load Balancing Virtual Server\*  
 > Add Edit ⓘ

Comment

Create Close

20. Under expression, add the following one and click **Create**.  
**HTTP.REQ.HOSTNAME.EQ("green.repro.lab")**

**Create Content Switching Policy**

Name\*

Action

Log Action

Expression\* [Expression Editor](#)

**Note:** In this example, the FQDN “green.repro.lab” will be used and redirect the requests to the cs VIP 01 created before. Feel free to use any other FQDN.

21. Click **Bind**.

Target Load Balancing Virtual Server

22. Both policies have been bound. Click **Close**.

**Content Switching Virtual Server Content Switching Policy Binding**

<input type="checkbox"/>	PRIORITY	POLICY NAME	EXPRESSION	ACTION
<input type="checkbox"/>	100	cs_policy_01	HTTP.REQ.HOSTNAME.EQ("blue.repro.lab")	action_lb_01
<input type="checkbox"/>	110	cs_policy_02	HTTP.REQ.HOSTNAME.EQ("green.repro.lab")	action_lb_02

23. Click **No Default Virtual Server Bound** under **Content Switching Policy Binding**.

**Content Switching Virtual Server**

**Basic Settings**

Name	cs_vip_http.repro.lab	Listen Priority	-
Protocol	HTTP	Listen Policy Expression	NONE
Target Type	NONE	Range	1
State	UP	IPset	-
IP Address	10.X.X.X	Traffic Domain	0
Port	80	RHI State	PASSIVE
Persistence Type	NONE	AppFlow Logging	ENABLED
Persist Mask	255.255.255.255	DTLS	false
IPv6 Persist Mask Length	128	Probe Protocol	-
Persistence Timeout	2	Probe Success Response Code	-
Backup Persistence Timeout	2	Probe Port	-
		Comments	-

**Content Switching Policy Binding**

2 Content Switching Policies >

[No Default Virtual Server Bound](#) <

24. Select any of your Web Server and click **Add**.

The screenshot shows a dialog box titled "Configure Content Switching Virtual Server to Load Balancing Virtual Server Binding". It features a dropdown menu for "Default Load Balancing Virtual Server Name" with "cs\_vip\_01" selected. Below the dropdown are "Add" and "Edit" buttons. At the bottom, there are "Bind" and "Close" buttons, with an orange arrow pointing to the "Close" button.

**NOTE:** Requests on the **CS HTTP LB VIP** that do not satisfy the criteria outlined in the **CS Policies** (expression) will be directed to the designated default "Web server" of your choice.

25. Both policies + a default policy have been bound to the CS VIP. Click **OK**.

The screenshot shows a dialog box titled "Content Switching Policy Binding". It contains two rows: "2 Content Switching Policies" and "Default Load Balancing Virtual Server", each with a right-pointing chevron. At the bottom, there is an "OK" button with an orange arrow pointing to it.

26. Click to **Edit**.

The screenshot shows a "Traffic Settings" dialog box with a list of configuration options. The options are arranged in two columns. The right column includes "ICMP Virtual Server Response" (PASSIVE), "Cacheable" (NO), "Down State Flush" (ENABLED), "Case Sensitive", "State Update" (DISABLED), and "Precedence". An orange arrow points to the "State Update" option.

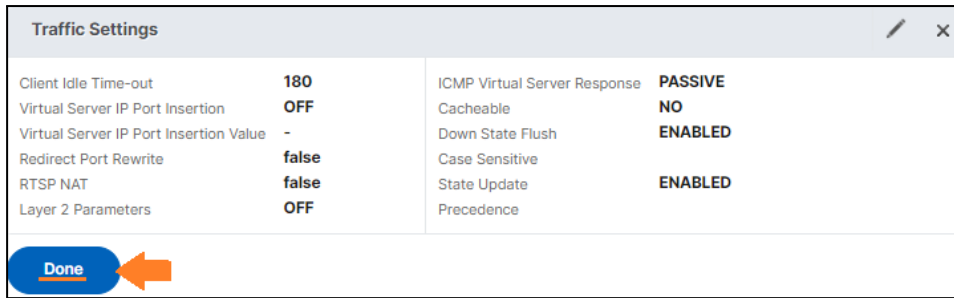
27. Enable **State Update** and click **OK**.

This screenshot is similar to the previous one but shows the "State Update" option checked. Below the checkboxes is a "Precedence\*" dropdown menu with "RULE" selected. At the bottom, there is an "OK" button with an orange arrow pointing to it.

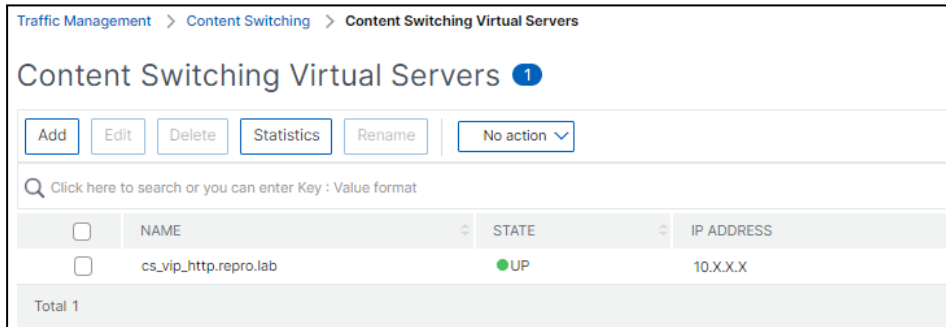
**NOTE:** The Content Switching operates independently of an LB Vserver to maintain an "UP" status. Even when no LB Vserver is bound to the CS Vserver, it will naturally be in a "UP" state. However, if you want the CS Vserver to adjust its state based on the target LB Virtual Servers bound to it, you can utilize the "state update" option. Now, if you disable all your "Non-Addressable Virtual Servers", the CS VIP will show as DOWN.

28. Click **Done**.

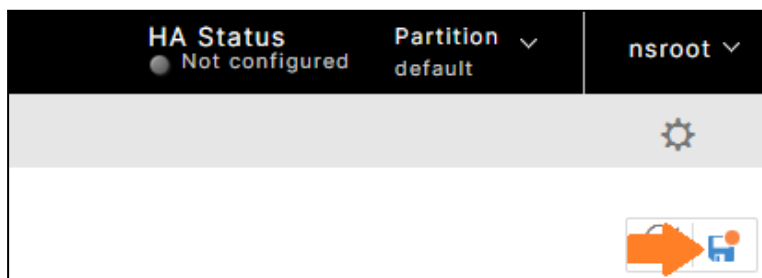




29. The CS VIP has been created.

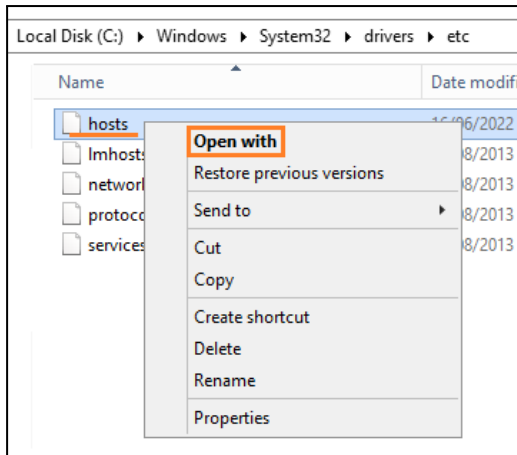


30. Save the configuration.

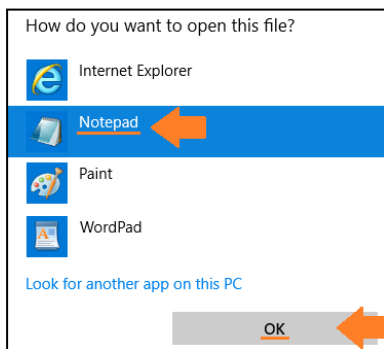


**NOTE:** For the upcoming task, create the Content Switching hosts entry following the same process as the Load Balance VIP. If you have a DNS server, include the entries as detailed below.

31. From your **Jump Box Windows Client**, either navigate to **Windows Explorer > Local Disk (C:) > Windows > System32 > Drivers > etc.** or from **Run**, execute the below path.  
c:\Windows\System32\drivers\etc
32. Click over **“hosts”** again and select **Open with**.



33. Select **Notepad**.



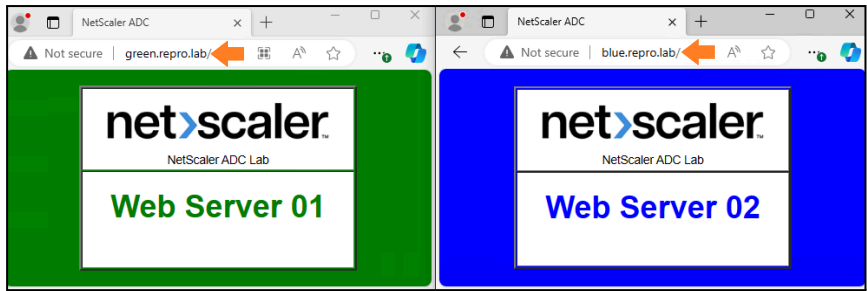
34. Add your **Content Switching LB Virtual Server IP** followed by the hostnames **green.repro.lab** **blue.repro.lab** **cs.repro.lab**. Replace **10.X.X.Y** with your actual **Content Switching LB VIP** (e.g., 10.50.1.10 green.repro.lab blue.repro.lab cs.repro.lab).

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
10.X.X.X lb.repro.lab
10.X.X.Y blue.repro.lab green.repro.lab cs.repro.lab
```

**NOTE:** The two first FQDNs (blue.repro.lab and green.repro.lab) must match the two CS policies (expressions) you created before. "cs.repro.lab" is the only one that does not need to match.

## Testing and Checking the Policy Hits

1. From your **Windows 10 Client**, type the hostnames that we created for the cs policies, such as: **blue.repro.lab** and **green.repro.lab**. You will see the content based on their respective colors.



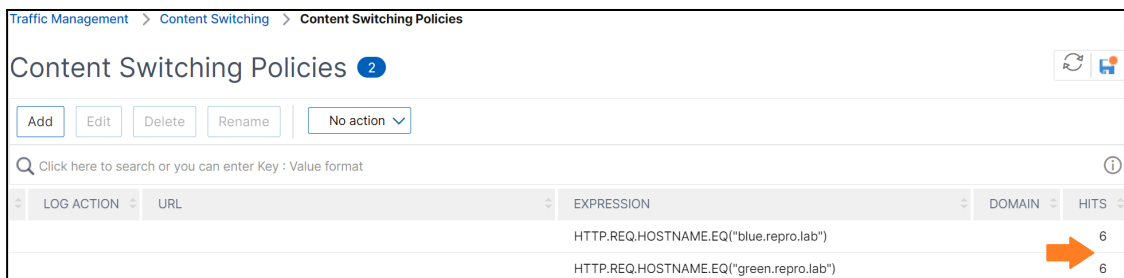
- For the CLI, type `nsconmsg -d current -g pcp_hits` to verify the policy hits. Now, try to reach either **blue.repro.lab** or **green.repro.lab** again and you will see the below output:

```
> shell
root@netscaler01#
root@netscaler01# nsconmsg -d current -g pcp_hits
Displaying performance information
NetScaler V20 Performance Data
NetScaler NS14.1: Build 12.30.nc, Date: Nov 22 2023, 10:23:35 (64-bit)

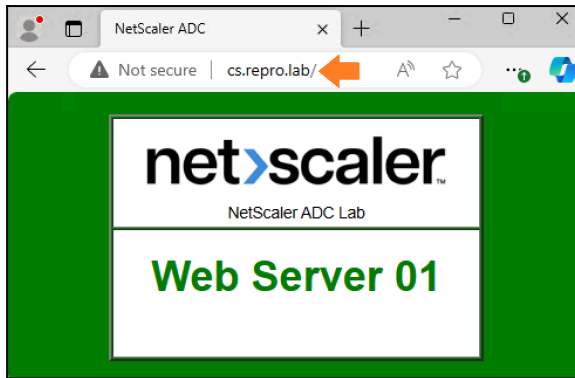
reltime: milliseconds between two records Tue Jan 9 10:30:11 2024
  Index  rtime totalcount-val  delta  rate/sec  symbol-name&device-no
  0      7011         19          1          0  pcp_hits rewrite(policy_remove_server_header)
  1       0           5          1          0  pcp_hits cspolicy(cs_policy_01)
  2    14022         21          1          0  pcp_hits rewrite(policy_remove_server_header)
  4       0           6          1          0  pcp_hits cspolicy(cs_policy_02)
```

The Content Switch will deliver the content based on hostnames (domain) when you test them:

- If you hit the CS VIP hostname blue.repro.lab:**  
Result: cs policy "01" will deliver the content from **LB VIP HTTP 01**
  - If you hit the CS VIP hostname green.repro.lab:**  
Result: cs policy "02" will deliver the content from **LB VIP HTTP 02**
- For GUI, navigate to **Traffic Management > Content Switching > Policies**. Next to each of the policies you can see the total of hits received as well.

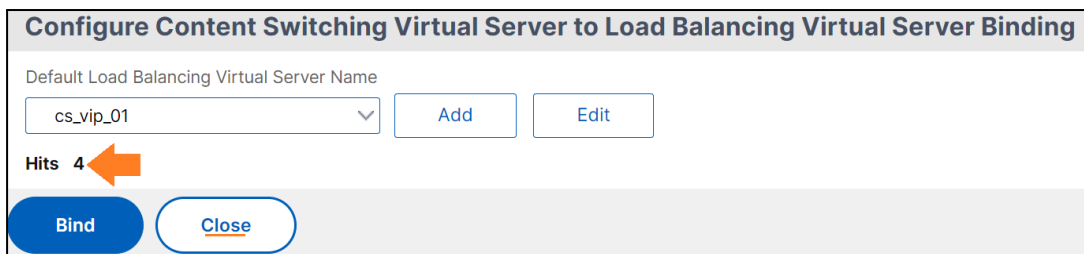


- Type now the hostnames that we did not create the cs policies, "cs.repo.lab". The content served by the **Default CS LB VIP** will display content in **green**.



- If you hit the CS VIP IP address (http//CS VIP) on the browser or cs.repro.lab:  
Result: default VIP binding will deliver the content ( )
5. If you return to your **Content Switching VIP > Default Load Balancing Virtual Server**, you will be able to see the number of hits the Default CS VIP received.

**NOTE:** You will need to click on the drop-down menu and select any other VIP to "hits" appear. Click **Close**.

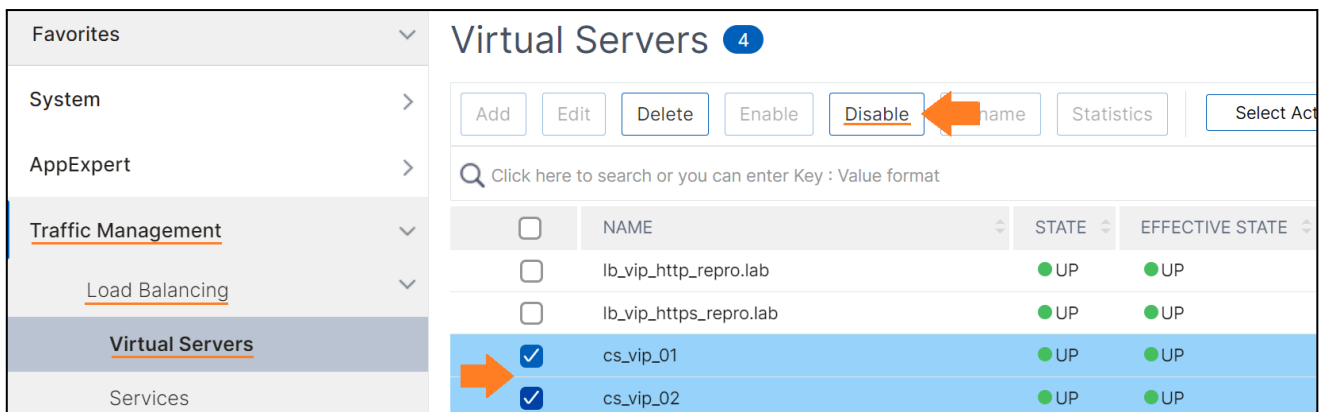


## Content Switching Backup Virtual Server

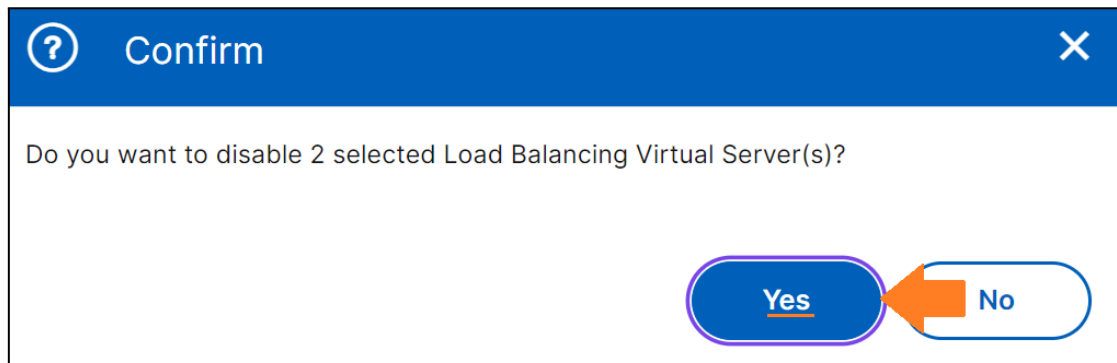
Content switching may encounter issues when the CS LB VIP experiences a failure, becomes unavailable due to high traffic loads, or faces other challenges. To mitigate the risk of failure, you have the option to set up a backup Virtual Server and/or enable Spillover.

In case the CS LB VIP is marked as DOWN or DISABLED, the NetScaler can redirect incoming requests to a specific location (URL), backup CS LB VIP, or to a standard LB VIP. Additionally, the spillover feature can be enabled to direct new connections to a backup CS LB VIP/URL when the number of connections to the primary CS LB VIP surpasses the defined threshold value. **Backup Virtual Server/Redirect URL** will be covered in this section only.

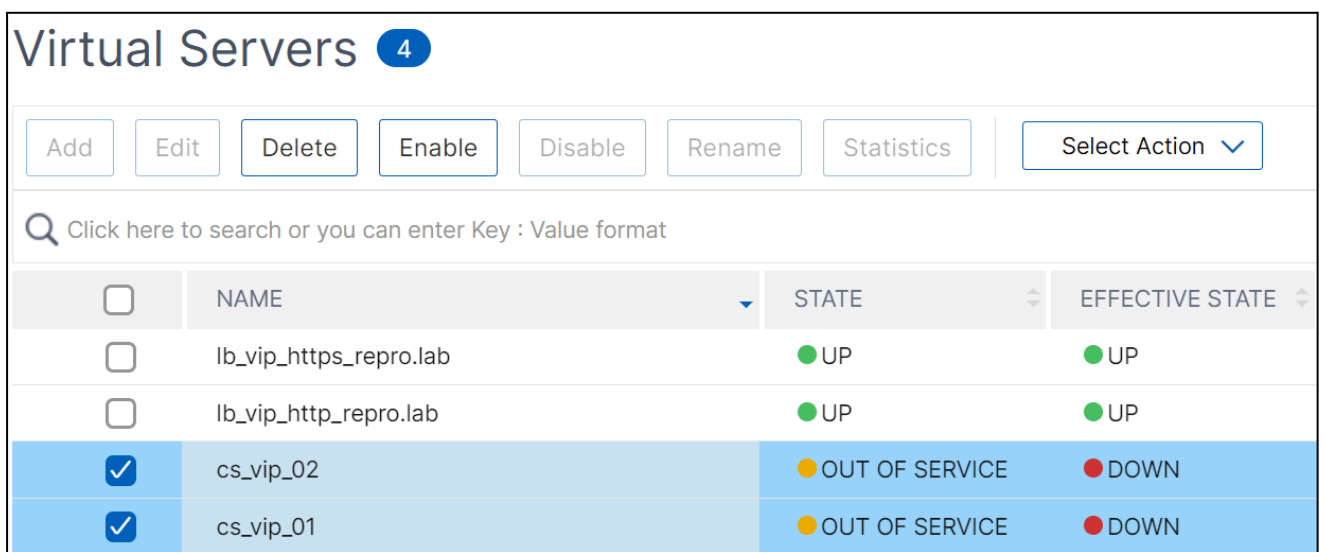
1. On your NetScaler, navigate to **Traffic Management > Load Balancing > Virtual Servers** and **disable** all your **cs\_vips** (cs\_vip\_01 and cs\_vip\_02).



2. Click **Yes** to confirm.



3. Confirm the two cs\_vips are showing as **DOWN**.



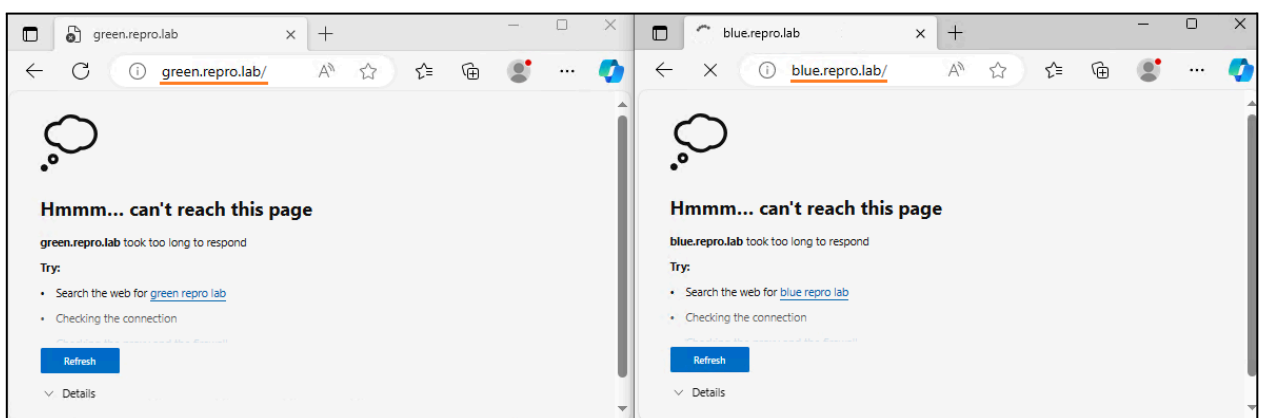
Virtual Servers 4

Add Edit Delete Enable Disable Rename Statistics Select Action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE
<input type="checkbox"/>	lb_vip_https_repro.lab	● UP	● UP
<input type="checkbox"/>	lb_vip_http_repro.lab	● UP	● UP
<input checked="" type="checkbox"/>	cs_vip_02	● OUT OF SERVICE	● DOWN
<input checked="" type="checkbox"/>	cs_vip_01	● OUT OF SERVICE	● DOWN

4. From your Jump Box VM, try to hit the cs hostnames created before, **green.repro.lab** and **blue.repro.lab**. You will observe an error page indicating the inability to reach the services.



5. Navigate to **Traffic Management > Content Switching > Virtual Servers**. Your CS LB VIP is expected to display a **"DOWN"** state, as we enabled the **"State Update"** option during the CS VIP configuration. If, for any reason, your CS LB VIP is still indicated as **"UP"**, ensure that the **"State Update"** option under **"Traffic Settings"** within the CS VIP is set to **"ENABLED"**.

**Content Switching Virtual Servers** 2

Add Edit Delete Statistics Rename No action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE
<input type="checkbox"/>	cs_vip_http.repro.lab	DOWN

Total 2

6. Select the CS VIP and click **Edit**.

**Content Switching Virtual Servers** 2

Add Edit Delete Statistics Rename Select Action

Click here to search or you can enter Key : Value format

<input checked="" type="checkbox"/>	NAME	STATE
<input checked="" type="checkbox"/>	cs_vip_http.repro.lab	DOWN

Total 2

7. On the right side of the page under “**Advanced Settings**”, select **Protection**.

**Advanced Settings**

- + Policies
- + **Protection**
- + Profiles
- + Push

8. Under “**Redirect URL**”, type any external website such as “https://netscaler.com” and click **OK**.

**Protection**

Redirect URL  
 ⓘ

Backup Virtual Server

Disable Primary When Down

**Spillover**

Spillover Method\*

Spillover Threshold

Spillover Backup Action

Spillover Persistence Timeout (mins)

Spillover Persistence

**OK**

**NOTE:** You also have the option to select any internal LB Virtual Server already created under “Backup Virtual Server”.

9. Click **Done**

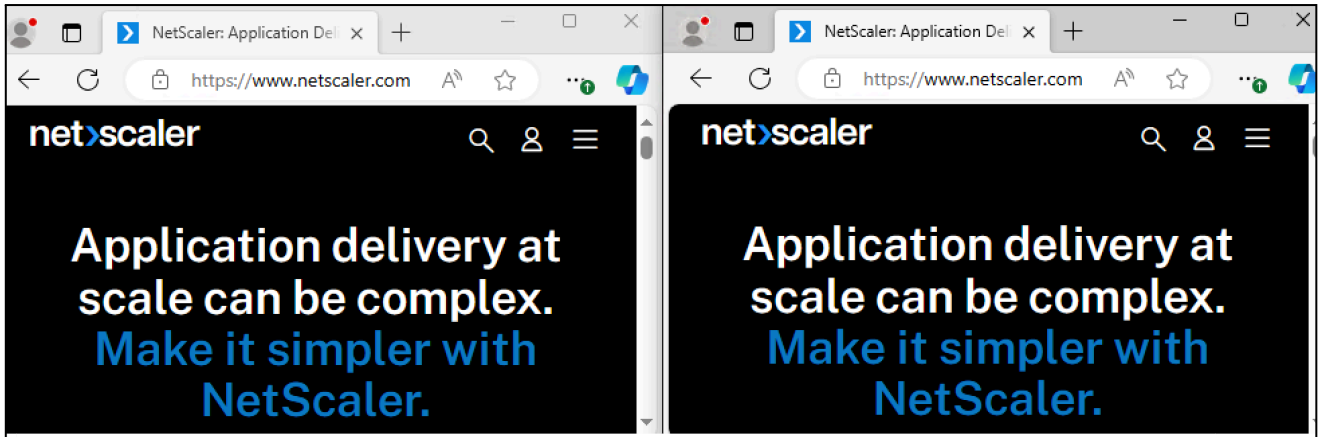
**Protection** ✎ ✕

Redirect URL	<b>https://netScaler.com</b>	Spillover Method	<b>NONE</b>
Backup Virtual Server	-	Spillover Threshold	-
Disable Primary When Down	<b>DISABLED</b>	Spillover Backup Action	-
Spillover Persistence Timeout (mins)	<b>2</b>		
Spillover Persistence	<b>false</b>		

**Done**

10. Go back to your **Jump box VM** and **REFRESH** the page. You will notice a redirect to “https://netScaler.com”.



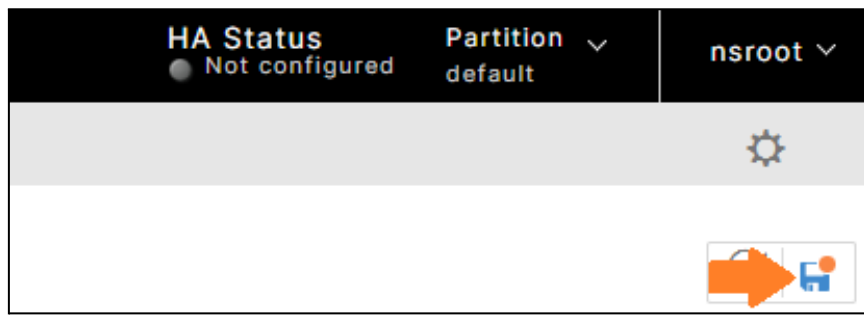


---

**NOTE:** Please **re-enable** your CS VIP HTTP Virtual Servers.

---

11. Save the configuration.



## Second NetScaler 14.1 (HA) Install

**NOTE:** If you have already downloaded the NetScaler firmware and configured the initial NetScaler IP (NSIP), subnet mask and gateway, please skip the steps 1 - 3.

1. Set up NetScaler VPX 02 following the identical process used for installing VPX 01. Ensure that you use the same software version.

Download the NetScaler firmware:

<https://www.citrix.com/downloads/citrix-adc/>

For steps on how to deploy the NetScaler on the supported platforms, please refer to the official documentation:

<https://docs.netScaler.com/en-us/citrix-adc/current-release/deploying-vpx>

2. After selecting the NetScaler platform and installing the firmware, proceed to configure the **management IP (NSIP)**, **Netmask**, and your designated **Gateway** using the **NetScaler Console**.

```
-----[DSA 1024]-----+
+==*+*==. . |
0.+ .0.+* . |
* *000.0 |
. X0+00. . . |
S 0E=. . . |
. *.0 |
. .0 |
*0 |
.0 |
-----[SHA256]-----+
kern.sched.idlespinthresh: 157 -> 32
Start daemons: syslogd Dec 19 13:34:40 <kern.info> ns syslogd: kernel boot file
is /flash/ns-14.1-4.42
Dec 19 13:34:40 <kern.notice> ns kernel: lo0: link state changed to UP
inetd cron httpd monit sshd /etc/ssh_config line 19: Deprecated option UsePrivilegeSeparation
!There is no ns.conf in the /nsconfig!
Start Netscaler software
tput: no terminal type specified and no TERM environmental variable.
Enter Citrix ADC's IPv4 address []: |
```

3. Enter the **new IP**, **netmask** and **your own gateway**. **Save** and **quit** if everything is correct by pressing the number **4**.

```
-----
Citrix ADC Virtual Appliance Initial Network Address Configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.

After the network changes are saved, you may either login as nsroot and
use the Citrix ADC command line interface, or use a web browser to
http://10.91.69.145 to complete or change the Citrix ADC configuration.
-----

  1. Citrix ADC's IPv4 address [ 10.X.X.X ]
  2. Netmask [255.X.X.X]
  3. Gateway IPv4 address [ 10.X.X.X ]
  4. Save and quit
Select item (1-4) [4]: 4
```

The NetScaler will boot, and the login prompt will appear.

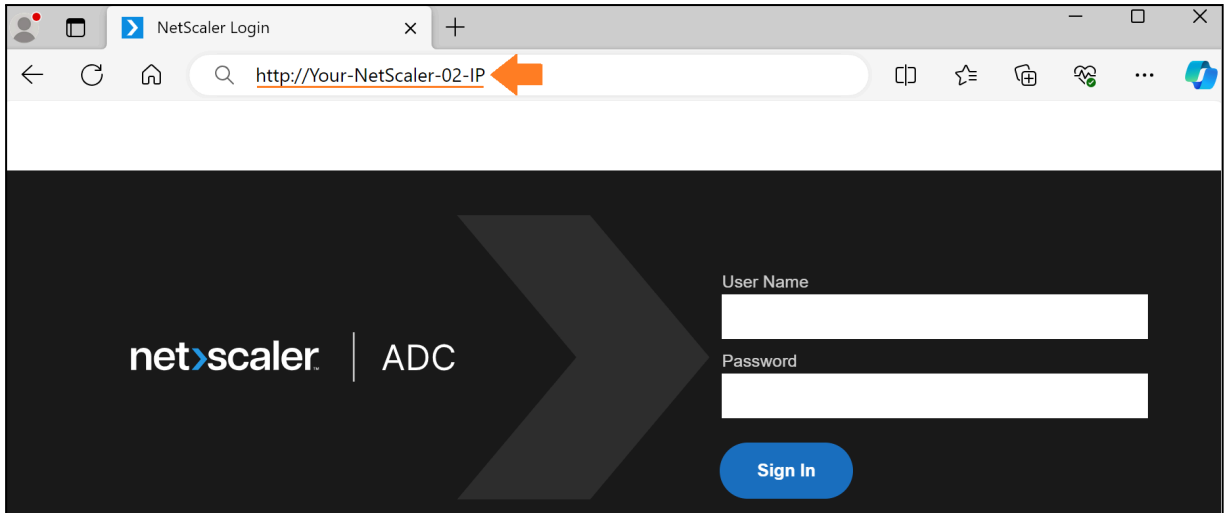
```
NetScaler initialization is still in progress; please wait
20 to 30 seconds before attempting to log in.
Jan 13 14:58:12 <local0.alert> 10.110.73.136 01/13/2023:14:57:47 GMT 0-PPE-0 :
default EVENT STATECHANGE 27 0 : Device "self node 10.110.73.136" - State UP
#####
#
#      WARNING: Access to this system is for authorized users only.      #
#      Disconnect IMMEDIATELY if you are not an authorized user!      #
#
#####
login:
```

- 4. Enter "nsroot" as the username and "nsroot" as the password. You will be prompted to change your nsroot password. Set a new password (The same password you set on the NetScaler 01). Save the configuration using the command "save config".

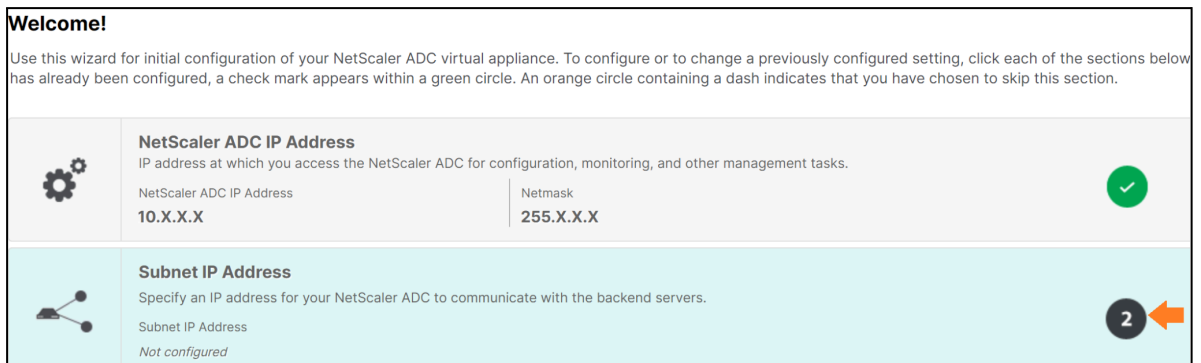
```
login: nsroot
Password:
Dec 20 10:15:25 <auth.notice> ns login: ROOT LOGIN (nsroot) ON ttyv0

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
> save config
Done
```

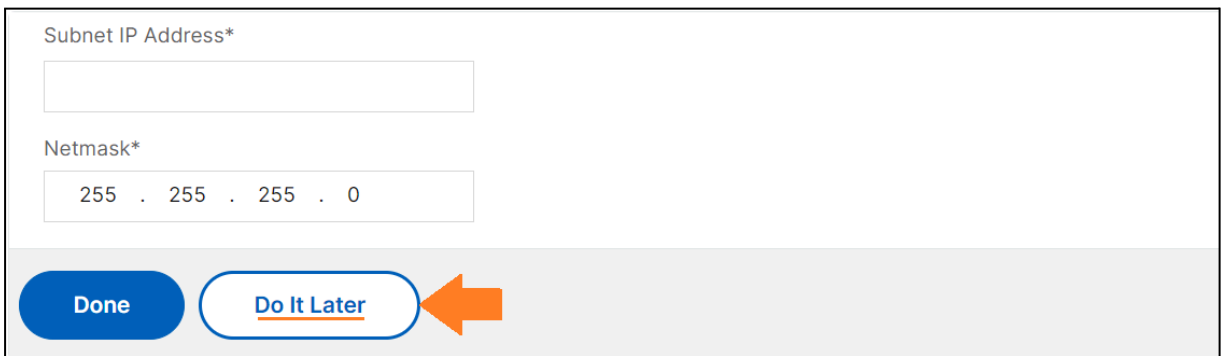
- 5. Open your browser, type http(s)://YOUR-NETSCALER-02-IP and hit the Enter key. Type "nsroot" for username and your new password. Click Log on.



6. Click over option **number 2**.



7. Click **Do It Later**.









**NOTE:** Please be aware that you should **NOT** configure ANY SNIP (Subnet IP) for the second NetScaler **ADC02**. The SNIP from the first NetScaler will be automatically "synced" to the second NetScaler ADC02 once the High Availability (HA) setup is established.

8. Click over option **number 3**.

**Welcome!**

Use this wizard for initial configuration of your NetScaler ADC virtual appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<p><b>NetScaler ADC IP Address</b></p> <p>IP address at which you access the NetScaler ADC for configuration, monitoring, and other management tasks.</p> <p>NetScaler ADC IP Address: 10.X.X.X      Netmask: 255.X.X.X</p>	
	<p><b>Subnet IP Address</b></p> <p>Specify an IP address for your NetScaler ADC to communicate with the backend servers.</p> <p>Subnet IP Address: Not configured</p>	
	<p><b>Host Name, DNS IP Address, Time Zone, NTP Server, NetScaler ADM Service Connect</b></p> <p>Specify a host name to identify your NetScaler ADC, an IP address for a DNS server to resolve domain names, the time zone in which your NetScaler ADC is located, an IP address/fully qualified domain name of the NTP server which is required for NetScaler ADC clock synchronization and NetScaler ADM Service Connect settings to discover your NetScaler ADC instances effortlessly on NetScaler ADM service.</p> <p>Host Name: Not configured      DNS IP Address: Not configured      Time Zone: CoordinatedUniversalTime      NTP Server: Not configured      NetScaler ADM Service Connect: ENABLED</p>	

9. Enter the hostname **“netscaler02.repro.lab”**, and set your **local time zone**. If you already have an internal DNS/NTP server in your network, feel free to enter the IP(s). Click **Done**.

Host Name

DNS IP Address

+

Time Zone\*

NTP Server

+

**NetScaler ADM Service Connect**

This feature helps you discover your NetScaler ADC instances effortlessly on NetScaler ADM service and get insights and curated machine learning. NetScaler ADC instance automatically send system, usage and telemetry data to NetScaler ADM service.

Click [here](#) to learn more about this feature.

You can also configure this feature anytime using the NetScaler ADC command line interface, API or GUI Settings. Use of this feature is subject to the NetScaler End User Service Agreement [here](#).

Enable NetScaler ADM Service Connect

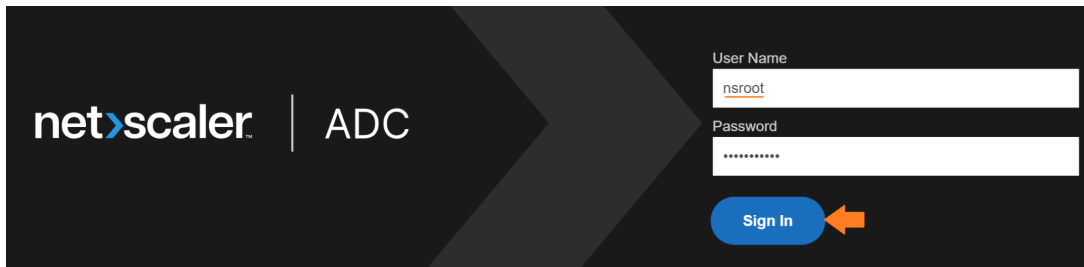
10. When prompted to save and reboot the NetScaler, click **YES**. The NetScaler GUI will be available again in about a minute.

**Confirm**

The configuration must be saved and the system rebooted for these settings to take effect.

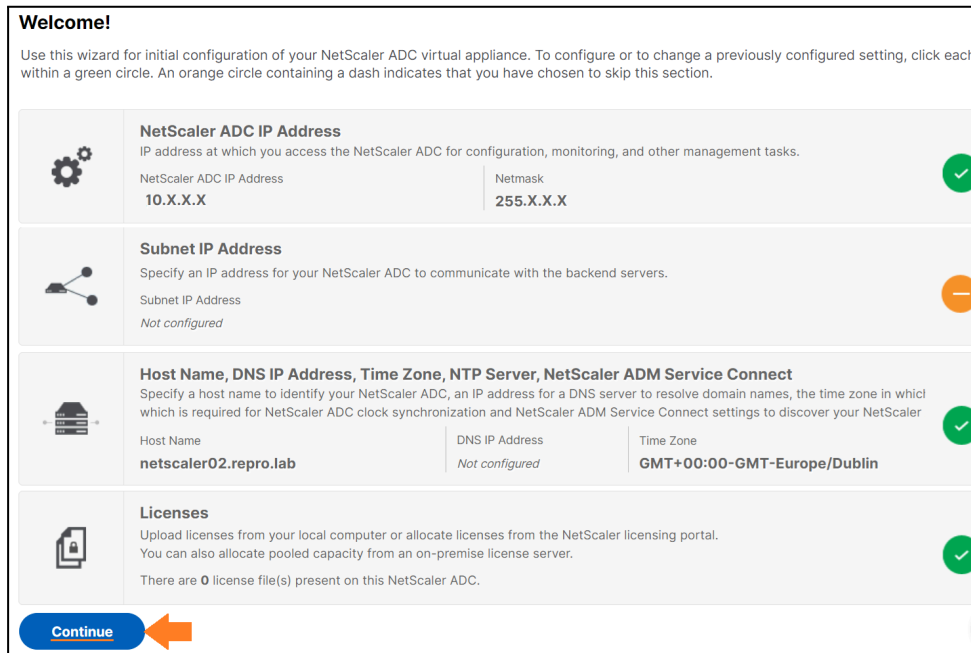
Save the configuration and reboot now ?

11. Log on again to your NetScaler with **nsroot** username and your **new password**.



The image shows the NetScaler ADC login interface. On the left is the 'net>scaler | ADC' logo. On the right, there are two input fields: 'User Name' with 'nsroot' entered and 'Password' with a masked password '\*\*\*\*\*'. Below these fields is a blue 'Sign In' button with an orange arrow pointing to it from the right.

12. Click **Continue**. The Initial configuration is **done**.



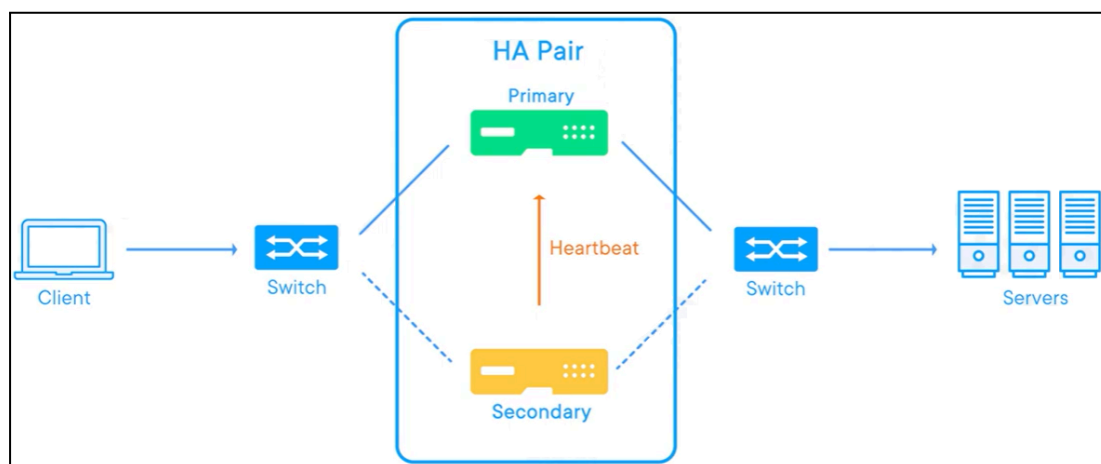
The image shows the 'Welcome!' configuration wizard for NetScaler ADC. It contains the following sections:

- NetScaler ADC IP Address**: IP address at which you access the NetScaler ADC for configuration, monitoring, and other management tasks. Fields: NetScaler ADC IP Address (10.X.X.X), Netmask (255.X.X.X). Status: Green checkmark.
- Subnet IP Address**: Specify an IP address for your NetScaler ADC to communicate with the backend servers. Field: Subnet IP Address (Not configured). Status: Orange circle with a dash.
- Host Name, DNS IP Address, Time Zone, NTP Server, NetScaler ADM Service Connect**: Specify a host name to identify your NetScaler ADC, an IP address for a DNS server to resolve domain names, the time zone in which which is required for NetScaler ADC clock synchronization and NetScaler ADM Service Connect settings to discover your NetScaler. Fields: Host Name (netscaler02.repro.lab), DNS IP Address (Not configured), Time Zone (GMT+00:00-GMT-Europe/Dublin). Status: Green checkmark.
- Licenses**: Upload licenses from your local computer or allocate licenses from the NetScaler licensing portal. You can also allocate pooled capacity from an on-premise license server. There are 0 license file(s) present on this NetScaler ADC. Status: Green checkmark.

At the bottom left, there is a blue 'Continue' button with an orange arrow pointing to it from the right.

## NetScaler High Availability (HA) Configuration

High availability synchronization is the method used to maintain identical configurations between the NetScaler nodes. This synchronization happens through a process called "nssync" over the **TCP** port **3008** or **3010**. Any command issued on the primary node propagates automatically to the secondary. Command propagation also uses the **TCP** port **3008** or **3010**. The two nodes in a high availability configuration send and receive heartbeat messages to and from each other on all interfaces that are enabled. The dead interval is the time interval after which the peer node is marked DOWN if heartbeat packets are not received. By default, the hello interval is set to 200 milliseconds, and the dead interval is set to 3 seconds. The heartbeat messages use **UDP** port **3003**.



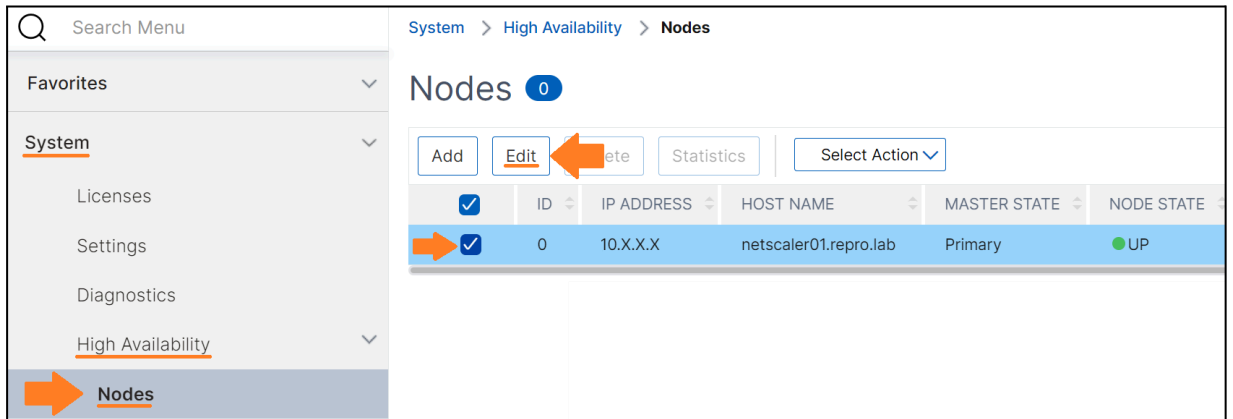
### Points to Note:

- In an HA configuration, the primary and secondary NetScaler must be of the same model. Also, NetScaler VPXs deployed on different models are not supported in an HA pair.
- In an HA setup, both nodes must run the same version of NetScaler.
- Entries in the **ns.conf** on both the primary and the secondary must match, with the following exceptions:
  - The primary and the secondary nodes must each be configured with their own unique NSIPs.
  - If you create a configuration file on either node by using a method that does not go directly through the GUI or the CLI (for example, importing SSL certificates, or changing to startup scripts), you must copy the configuration file to the other node or create an identical file on that node.
- Initially, all NetScaler appliances are configured with the same RPC node password. RPC nodes are internal system entities used for system-to-system communication of configuration and session information. RPC nodes maintain this information, which includes the IP addresses of the other systems, and the passwords they require for authentication.
- In a high availability, all configuration files are synchronized automatically from the primary node to the secondary node at an interval of one minute (**TCP 22**). Synchronizing configuration files can be performed manually by using the command line interface or the GUI at either the primary or the secondary node.

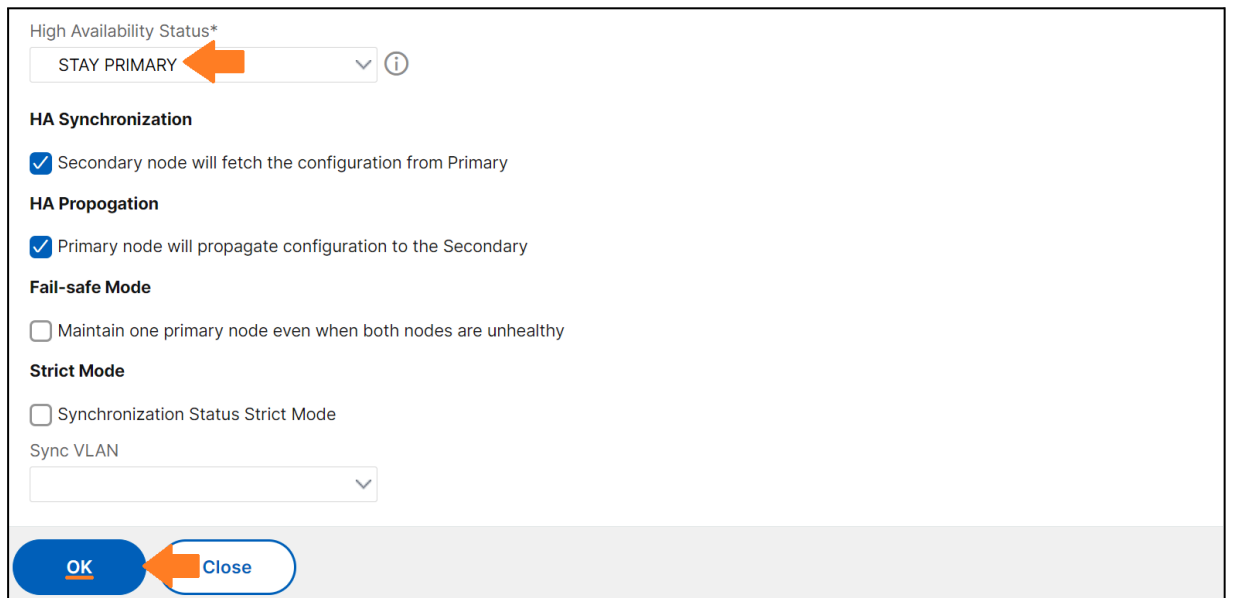
For more about Synchronization and Propagation, check this [CTX article](#)



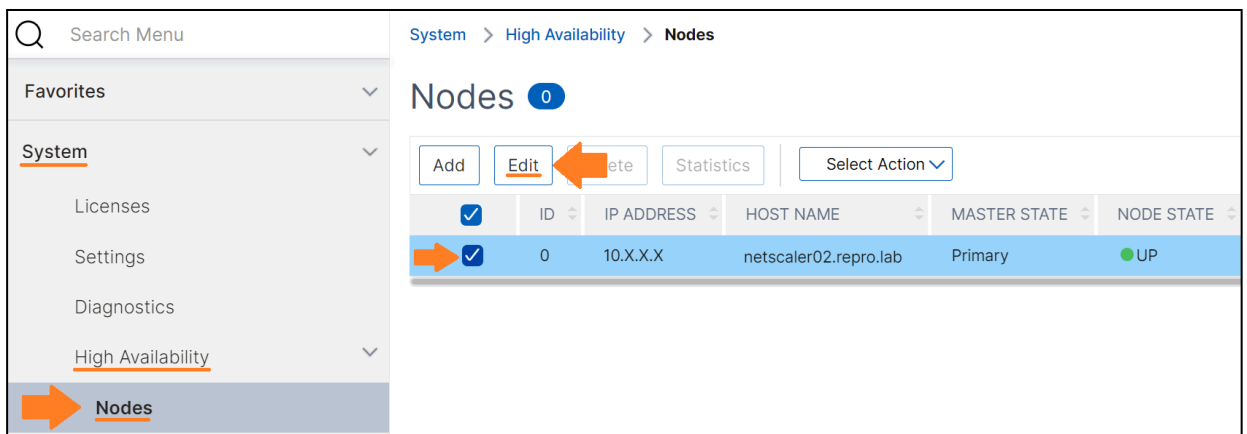
1. To start the HA setup, on the NetScaler **ADC01** navigate to **System > High Availability > Nodes**, select the **netScaler01.repro.lab**, and then click **Edit**.



2. Select **STAY PRIMARY** from the **High Availability Status** drop-down and click **OK**. This action will guarantee that NetScaler ADC01 is elected as the Primary when the HA configuration is established, and its existing configuration will be retained.



3. On the NetScaler **ADC02**, navigate to **System > High Availability > Nodes**, select the **NetScaler02.repro.lab** and then click **Edit**.



- Select **STAY SECONDARY (Remain in Listen mode)** from the “High Availability Status” drop-down and click **OK**. This will ensure the **NetScaler ADC02** will remain Secondary when the HA configuration is done.

High Availability Status\*

STAY SECONDARY (Remain in Listen mode) ▼

**HA Synchronization**

Secondary node will fetch the configuration from Primary

**HA Propagation**

Primary node will propagate configuration to the Secondary

**Fail-safe Mode**

Maintain one primary node even when both nodes are unhealthy

**Strict Mode**

Synchronization Status Strict Mode

Sync VLAN

▼

OK Close

- Take notes of the NetScaler **ADC02 NSIP**, the IP that shows under **IP Address**.

Nodes 0

Add Edit Delete Statistics No action ▼

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE
<input type="checkbox"/>	0	10.X.X.X	netscaler02.repro.lab	Primary	STAYSECONDARY

- Return to the NetScaler **ADC01** and click Add under High Availability > Nodes.

Nodes 0

Add Edit Delete Statistics No action ▼

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE
<input type="checkbox"/>	0	10.91.69.145	netscaler01.repro.lab	Primary	STAYPRIMARY

- Enter the **NSIP** of the NetScaler **ADC02** (The same IP address you copied before), under “**Remote System Login Credential**”, type the NetScaler **ADC02 credentials**, and enable “**Secure Access**”. Click **Create**.

## ← Create HA Node

Remote Node IP Address\*

10 . X . X . X

Configure remote system to participate High Availability setup

Turn Off HA Monitor interface/channels that are down

Turn on INC(Independent Network Configuration) mode on self node

---

Remote System Login Credential

User Name

nsroot

Password


\*\*\*\*\*

Secure Access ⓘ

**Create** **Cancel**

**NOTE:** When you enable the **Secure** option, the NetScaler encrypts all the RPC communication sent from one ADC node to another. This secure communication uses the **TCP** port number **3008**.

- Click on the **refresh** icon located in the upper-right corner of the GUI to view the current status of the HA Pair. You will either observe "**UNKNOWN**" or "**IN PROGRESS**" as the status.

Nodes 0 

Add Edit Delete Statistics Select Action

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE	SYNCHRONIZATION
<input type="checkbox"/>	0	10.X.X.X	netScaler01.repro.lab	Primary	STAYPRIMARY	DISABLED	ENABLED	-NA-
<input type="checkbox"/>	1	10.X.X.X		Secondary	STAYSECONDARY	DISABLED	<u>IN PROGRESS</u>	-NA-

- After clicking on the **refresh** button, you will see that the HA Pair has been created and that both nodes are showing as Up. The node Synchronization process will show as **SUCCESS** after a few seconds.

Nodes 0

Add Edit Delete Statistics Select Action

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE
<input type="checkbox"/>	0	10.X.X.X	netScaler01.repro.lab	Primary	STAYPRIMARY	DISABLED	ENABLED
<input type="checkbox"/>	1	10.X.X.X		Secondary	STAYSECONDARY	DISABLED	<u>SUCCESS</u>

- Select the **ADC01** node and click **Edit** to change the state of the availability.

Nodes 0

Add Edit Delete Statistics Select Action

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE
<input checked="" type="checkbox"/>	0	10.X.X.X	netScaler01.repro.lab	Primary	STAYPRIMARY
<input type="checkbox"/>	1	10.X.X.X		Secondary	STAYSECONDARY

11. Select from the “High Availability Status” drop-down “Enabled (Actively Participate in HA)” and click **OK**.

High Availability Status\*

ENABLED (Actively Participate in HA)

**HA Synchronization**

Secondary node will fetch the configuration from Primary

**HA Propagation**

Primary node will propagate configuration to the Secondary

**Fail-safe Mode**

Maintain one primary node even when both nodes are unhealthy

**Strict Mode**

Synchronization Status Strict Mode

Sync VLAN

OK Close

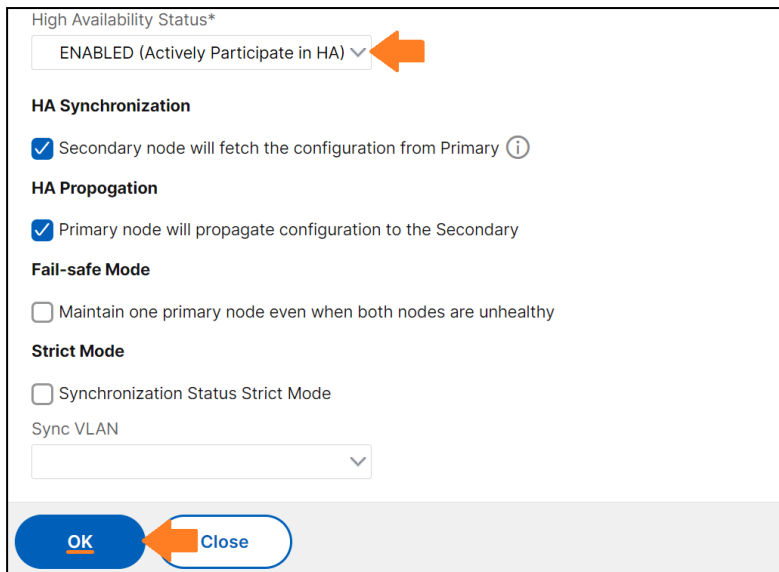
12. Return to the NetScaler **ADC02** high availability page (**System > High Availability > Nodes**) and refresh the page, you should be able to see both nodes. Select the **ADC02** and click **Edit**.

Nodes 0

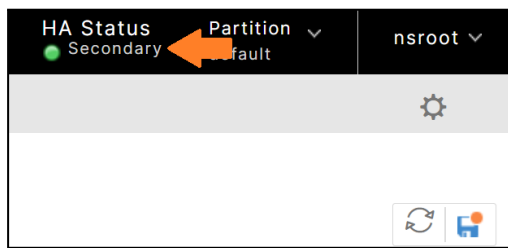
Add Edit Delete Statistics Select Action

<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE
<input checked="" type="checkbox"/>	0	10.X.X.X	netScaler02.repro.lab	Secondary	STAYSECONDARY
<input type="checkbox"/>	1	10.X.X.X		Primary	STAYPRIMARY

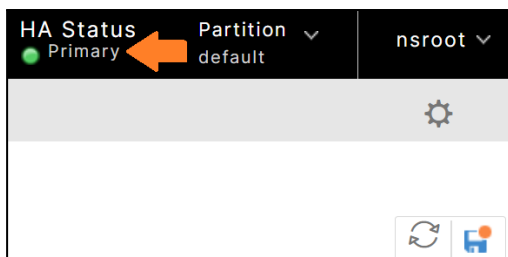
13. Click the **High Availability Status** drop-down button and select **Enabled (Actively Participate in HA)** list item and then click **OK**.



14. In the upper-right corner of the GUI, you will be able to see the current state of the HA Pair, **Secondary**.



15. Return to the NetScaler **ADC01** and **save** the configuration.



**Quick Reminder:** NetScaler HA relies on the following ports for Heartbeats, propagation, and synchronization:

**Heartbeats:** UDP 3003

**RPC SECURE ENABLED:** HA Synchronization: TCP 3008

**RPC SECURE ENABLED:** HA Propagation: TCP 3008

**RPC SECURE DISABLED:** HA Synchronization: TCP 3010

**RPC SECURE DISABLED:** HA Propagation: TCP 3010

**File Synchronization (rsync):** TCP 22

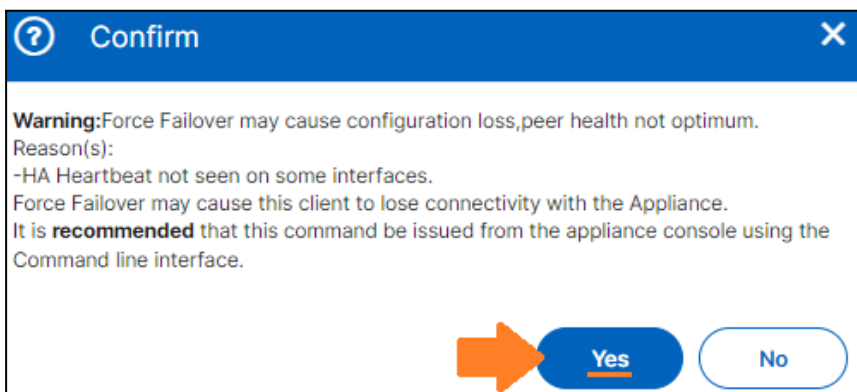
Nodes <span>0</span>							
	Add	Edit	Delete	Statistics	Select Action		
<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE
<input type="checkbox"/>	0	10.X.X.X	netScaler01.repro.lab	Primary	● UP	DISABLED	ENABLED
<input type="checkbox"/>	1	10.X.X.X		Secondary	● UP	DISABLED	SUCCESS

## Triggering a Manual Failover

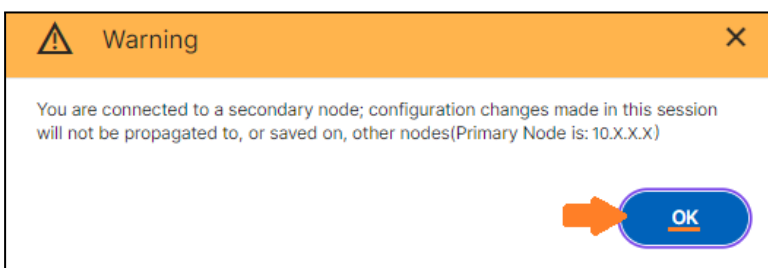
16. At present, NetScaler **ADC01** is responsible for managing all incoming requests due to its status as the **PRIMARY** node. To intentionally initiate a failover and enable NetScaler **ADC02** to assume the **PRIMARY** role and take over the active connections, click **"Select Action"** and **"Force Failover"**.

Nodes <span>0</span>							
	Add	Edit	Delete	Statistics	Select Action		
<input type="checkbox"/>	ID	IP ADDRESS	HOST NAME	MASTER STATE	NODE STATE	INC	SYNCHRONIZATION STATE
<input type="checkbox"/>	0	10.X.X.X	netScaler01.repro.lab	Primary	● UP	DISABLED	ENABLED
<input type="checkbox"/>	1	10.X.X.X		Secondary	● UP	DISABLED	SUCCESS

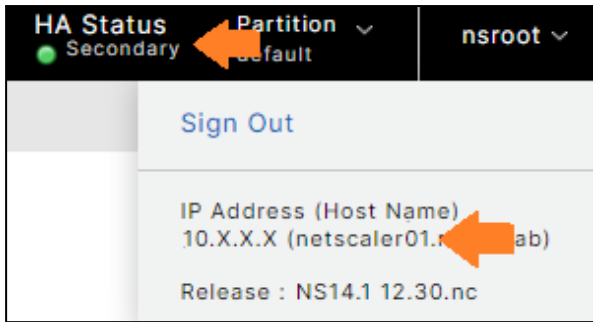
17. When the Force Failover warning box appears, click **Yes** and **OK**.



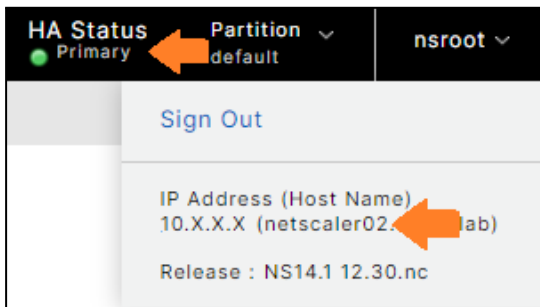
18. If you Refresh the browser, you will see the below warning coming from the NetScaler ADC01. Press **OK**.



19. Top-right corner, click over **"nsroot"** to show the NetScaler version, NSIP + hostname.



20. Open the NetScaler **ADC02**, and confirm its status, it should now show as **PRIMARY**.



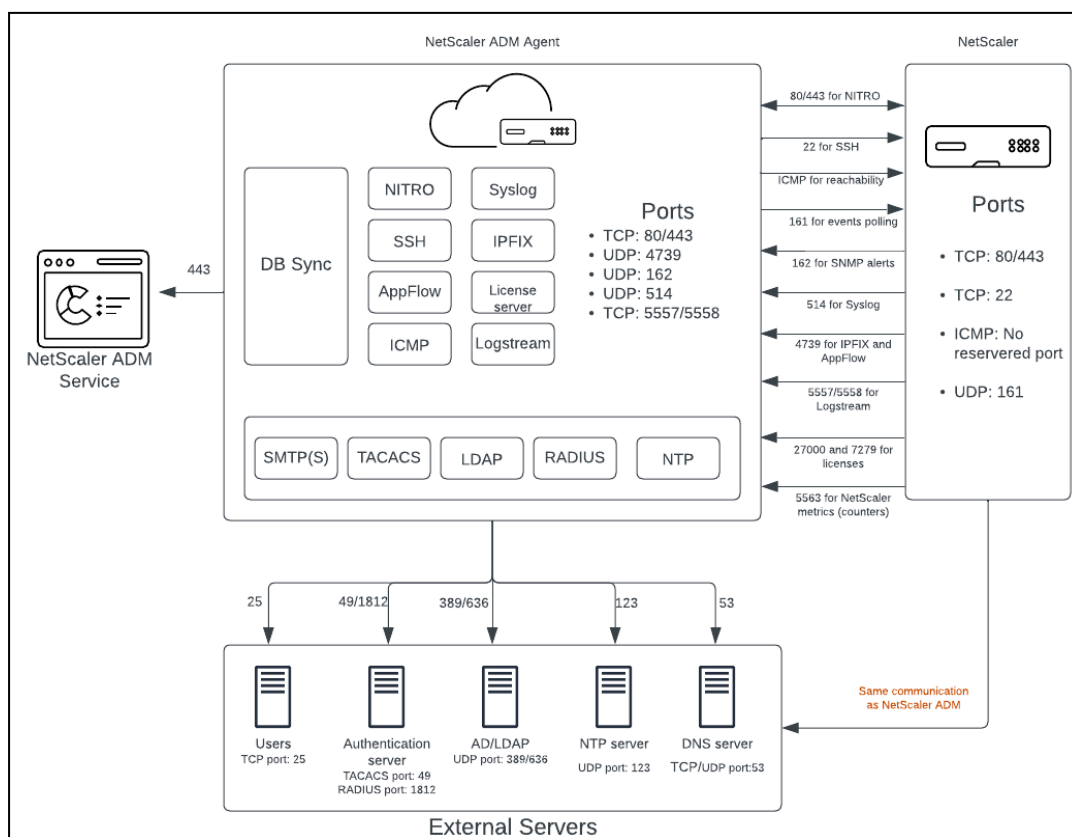


# NetScaler Console Service and NetScaler Agent Setup

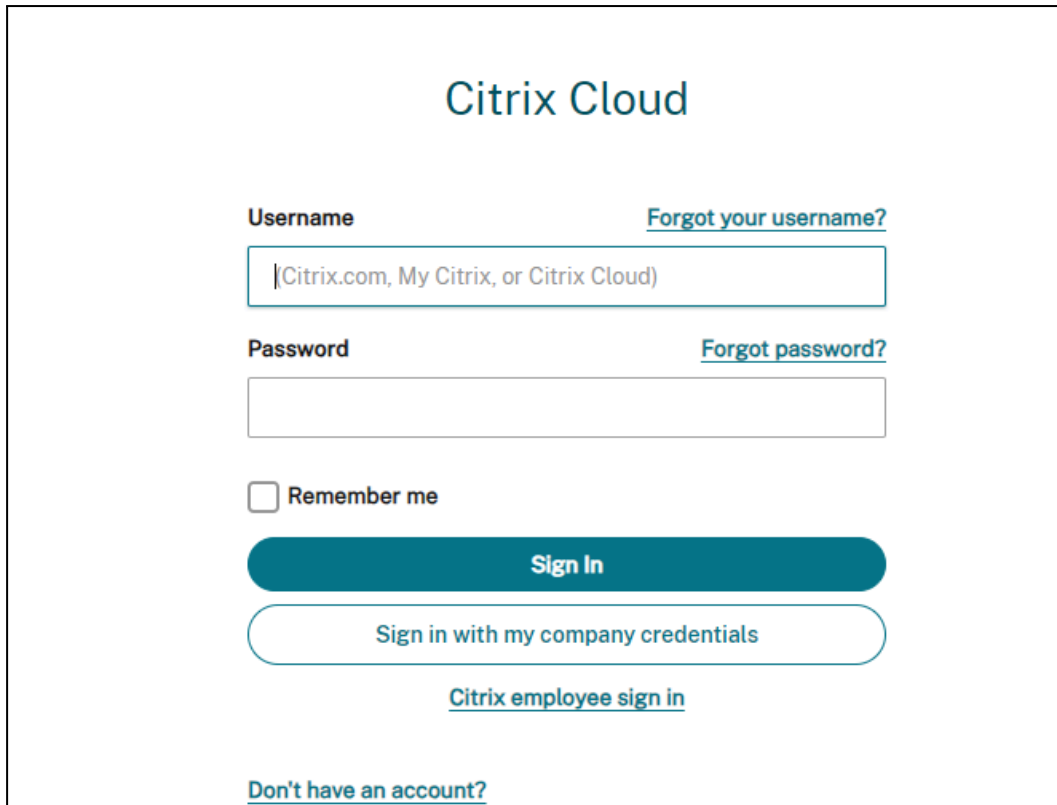
## Notes:

1. To complete this exercise you must have Pooled Licenses (Bandwidth and Instance licenses).
2. This guide will cover NetScaler Agent installation on-prem (Hypervisor). If you will install it on any other platform, please refer to the [Official documentation](#).
3. This lab intends to cover NetScaler Console pooled capacity only, not other NetScaler Console functionalities. The NetScaler agent will be installed locally in the network and connected to the NetScaler Console. NetScaler ADM on-prem is also an option, but this guide will not cover it.

Below you can see the NetScaler Console Service/Agent diagram and firewall ports.

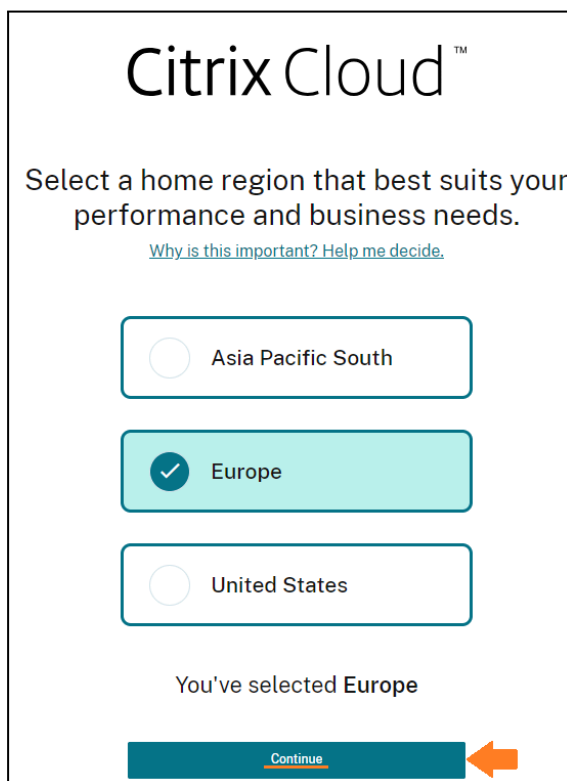


1. Navigate to <https://cloud.citrix.com/>.
2. If you already have created your account, just sign in. Otherwise, click "don't have an account?" and create your account by following the instructions displayed on the screen.




The image shows the Citrix Cloud login page. At the top, the text "Citrix Cloud" is centered. Below it, there are two input fields: "Username" and "Password". The "Username" field has a placeholder text "(Citrix.com, My Citrix, or Citrix Cloud)". To the right of the "Username" field is a link "Forgot your username?". To the right of the "Password" field is a link "Forgot password?". Below the "Password" field is a checkbox labeled "Remember me". There are three buttons: a dark teal "Sign In" button, a light teal "Sign in with my company credentials" button, and a link "Citrix employee sign in" below it. At the bottom, there is a link "Don't have an account?".

3. Select your **region**, accept the **terms of service**, and click **Continue**.



The image shows the Citrix Cloud region selection page. At the top, the text "Citrix Cloud™" is centered. Below it, the text "Select a home region that best suits your performance and business needs." is centered. Below this text is a link "Why is this important? Help me decide.". There are three radio button options: "Asia Pacific South", "Europe", and "United States". The "Europe" option is selected, indicated by a checkmark in a teal circle. Below the options, the text "You've selected Europe" is centered. At the bottom, there is a dark teal "Continue" button with an orange arrow pointing to it from the right.

4. **Acknowledge** your choice and click **Continue**.




**You've chosen Europe as your home region.**


This is where all of your account data will live and connector communications will be routed. Please note that once the home region is set this cannot be changed. For more details please [click here](#).

If you're happy this region suits your business and performance needs, please check the box and continue.

I acknowledge that my home region is set to Europe.

[Change](#) [Continue](#) 


5. Accept again the **terms of service** and click **Continue**.

 We've updated our [Terms of Service](#). Please take a moment to read through the changes.

I have read, understand, and agree to the Terms of Service

[Continue](#)

6. If you see the below, select Networking and Security. Click **Continue**.



**Welcome, let's get you set up for success!**

---

**What will you manage in Citrix Cloud?**  
(Select all that apply)

- Virtualization
- Networking
- Security
- Help Desk
- Files
- Other

[Continue](#)

7. Select **Maybe later**.

**Priority #1: Set up Authentication**

To start building and delivering secure digital workspaces to your end users, the first step is setting up an [authentication method](#).

[Set up authentication method](#)

[Take a quick tour](#)    [Maybe later](#) ←

8. Select **manage** for **Application delivery management**.

**NOTE:** If this is the first time you are launching the Citrix Cloud portal, you will see no services under “My services” but will see a list of **available services**.

9. Select your **region/country**, **accept** the note information this choice cannot be changed and click **Done**.

**NOTE:** Citrix assigns an **Express account** to manage the ADM resources, this is a **free** and **limited** version.

### Choose a region

Select a region that best suits your performance and business needs.

North America

EMEA

Asia Pacific






South America

I understand that I cannot change the region after set up.

10. Select your role. You can select the first 3 options and click **Continue**.

### Welcome to ADM Express Account

Select roles and use cases that apply to you

<input checked="" type="checkbox"/>		<b>Network Admin</b>	<ul style="list-style-type: none"> <li>Monitor ADC Infrastructure</li> <li>Automate ADC Configuration</li> <li>Manage SSL Certificates</li> </ul>
<input checked="" type="checkbox"/>		<b>App Admin</b>	<ul style="list-style-type: none"> <li>Remediate app health anomalies</li> <li>Assess app usage trend &amp; deviation</li> <li>Simplified app maintenance management</li> </ul>
<input checked="" type="checkbox"/>		<b>Gateway Admin</b>	<ul style="list-style-type: none"> <li>Track work from home usage</li> <li>Debug user access issues</li> <li>Troubleshoot user latency issues</li> </ul>
<input checked="" type="checkbox"/>		<b>Security Admin</b>	<ul style="list-style-type: none"> <li>Assess security configuration posture</li> <li>Identify WAF, Bot &amp; API security violations</li> <li>Remediate identified ML based violations</li> </ul>
<input type="checkbox"/>		<b>SRE</b>	<ul style="list-style-type: none"> <li>Cross microservice interaction visibility</li> <li>Identify bottlenecks through distributed tracing</li> <li>Troubleshoot golden signal deviations</li> </ul>

11. The ADM service will take a few minutes to get started.

Let's get you started with your Citrix ADM service.

Initialization : 1 of 4 complete

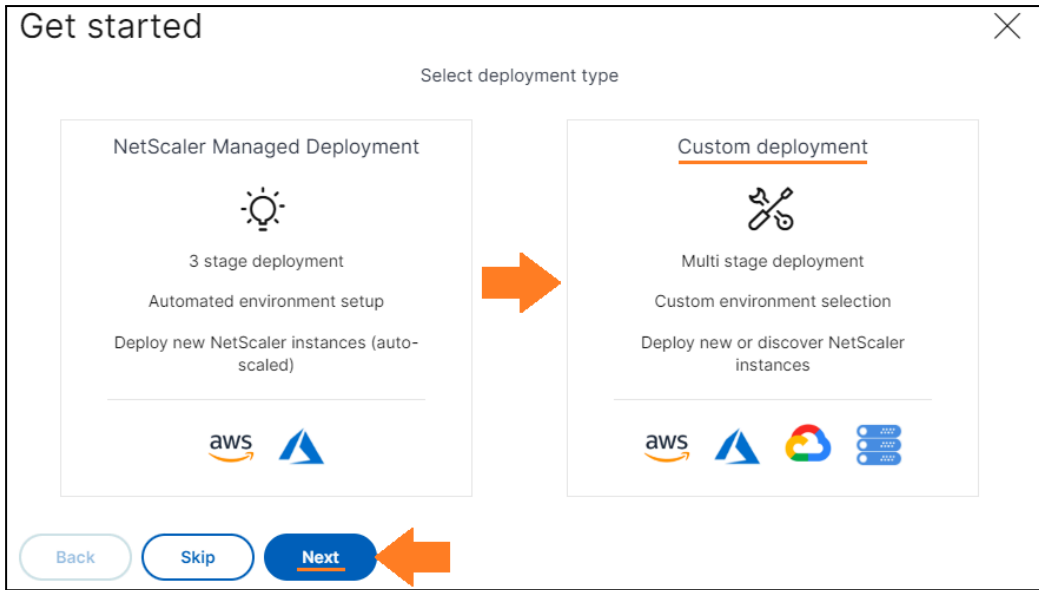
- ✓ Validating account information
- Creating an account
- Creating RBAC policies
- Adding a license

Watch this video on [Infrastructure Analytics](#) for a complete view of ADC health status while we create your tenant.

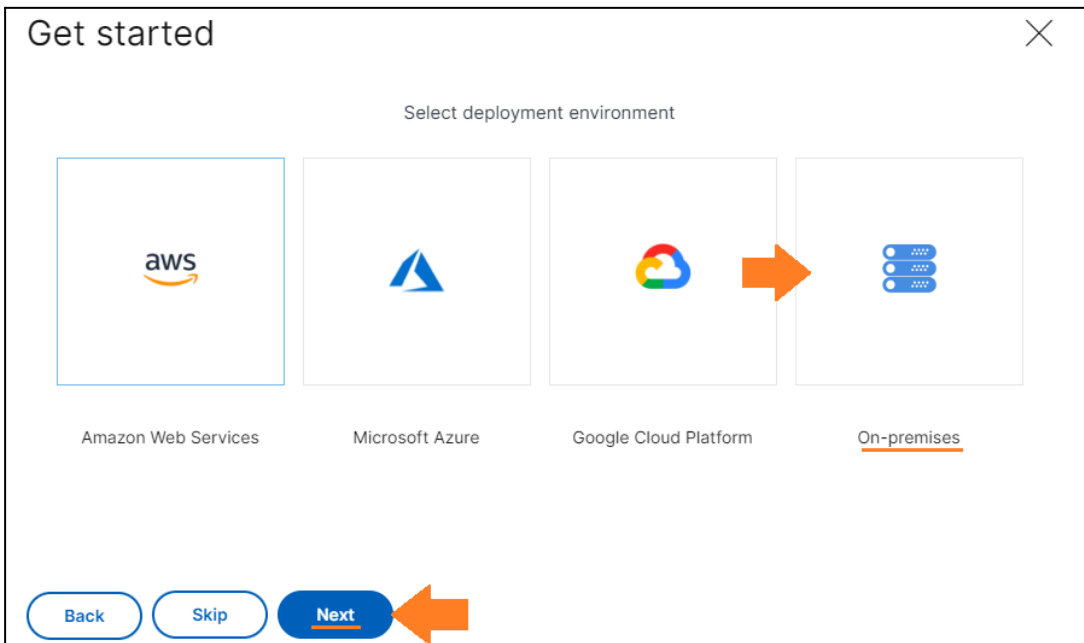
12. Click **Get Started**.

**NOTE:** If you have previously configured the NetScaler console, you will not see the screen above. In such a scenario, to set up the Agent, please navigate to **“Infrastructure > Instances > Agents”** and then select the option **“Set up Agent”**.

13. Select **Custom deployment** and click **Next**.

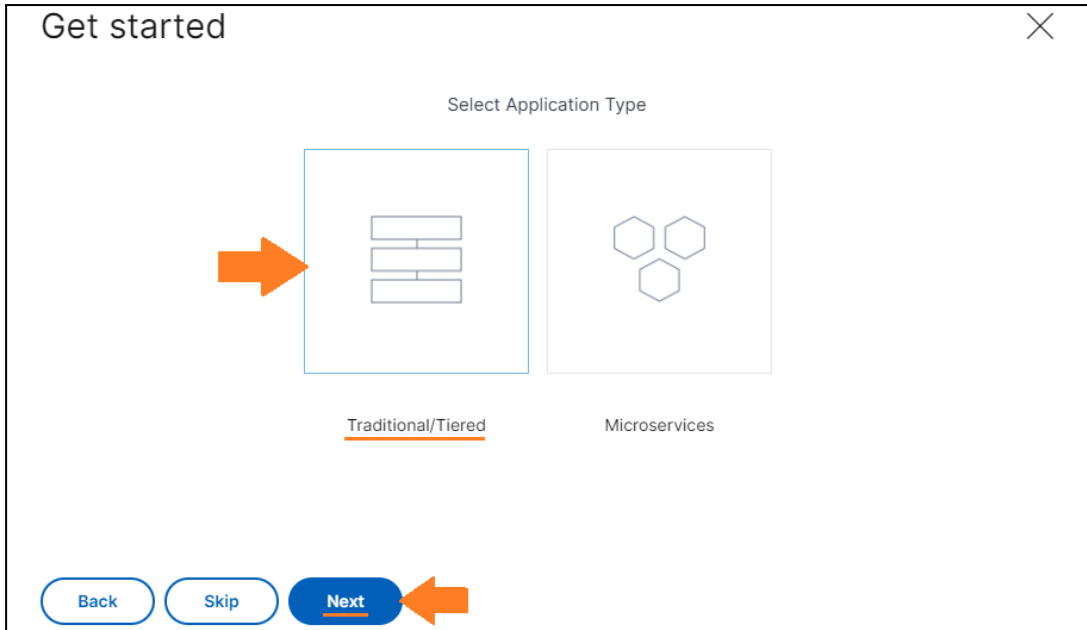


14. Select **On-premises** and click **Next**.

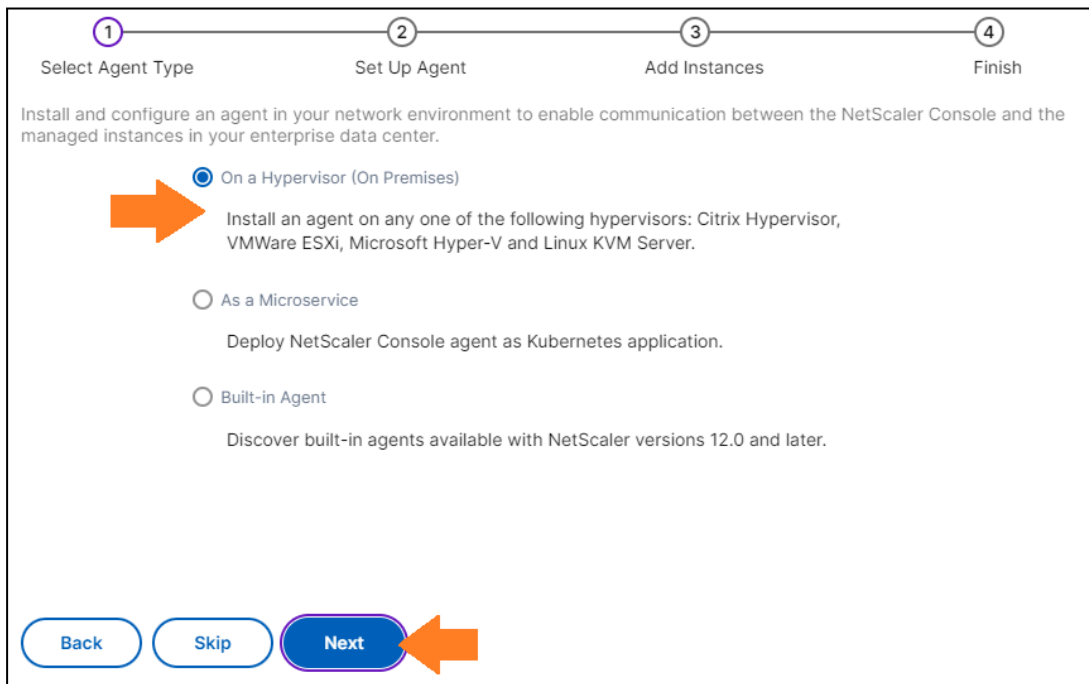


15. Select **Traditional/Tiered** and click **Next**.

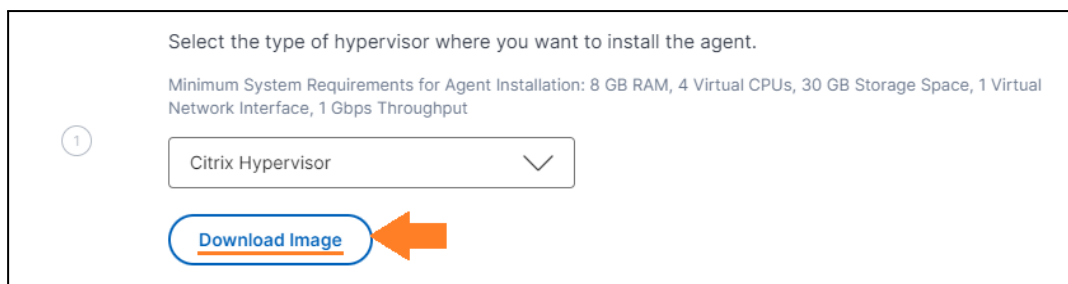
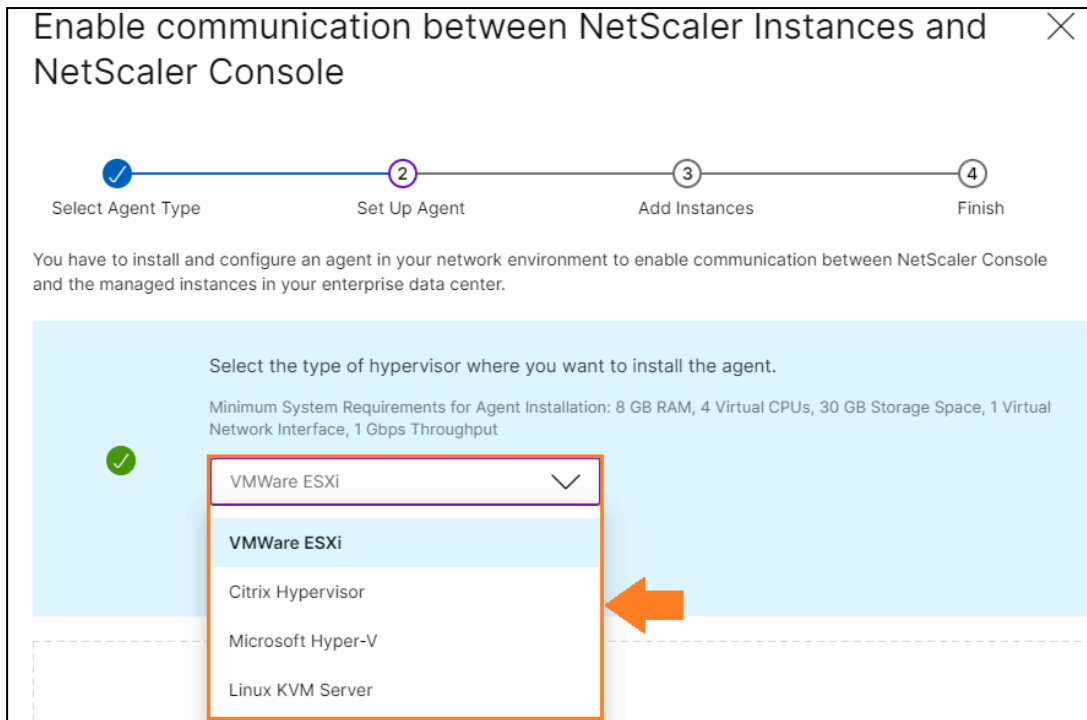




16. Select **On a Hypervisor (On Premises)** and click **Next**.



17. Select the type of hypervisor you want to install your agent and click **Download Image**.



18. The image will be downloaded to your computer. Once done, please install the image on your hypervisor. If you wish, you can check the [official documentation](#).
19. Boot your NetScaler agent.
20. The **networkconfig** script will be invoked automatically. Set your network.

```

NetScaler Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----
 1. NetScaler Agent Host Name []:
 2. NetScaler Agent IPv4 address []:
 3. Netmask []:
 4. Gateway IPv4 address []:
 5. DNS IPv4 Address []:
 6. Second NIC IPv4 address []:
 7. Second NIC Netmask []:
 8. Second NIC Network address []:
 9. Second NIC Gateway IPv4 address []:
10. Cancel and quit.
11. Save and quit.

Select a menu item from 1 to 11 [11]:

```

21. Select **1** and type the hostname **adm-agent.repro.lab**.

```
Select a menu item from 1 to 7 [7]: 1 ←  
Enter Citrix ADM Host Name : adm-agent.repro.lab
```

22. Select **2** and type your **ADM agent IP** (21<sup>st</sup> IP). It must be a new Free IP.

```
Select a menu item from 1 to 11 [11]: 2 ←  
Enter Citrix ADM Agent IPv4 address : 10.X.X.X
```

23. Select **3** and type your **subnet mask**.

```
Select a menu item from 1 to 11 [11]: 3 ←  
Enter Netmask : 255.X.X.X
```

24. Select **4** and type your **gateway**.

```
Select a menu item from 1 to 11 [11]: 4 ←  
Enter Gateway IPv4 address : 10.X.X.X
```

25. Select **5** and type your DNS server IP. If you do not have one, you can use any public DNS (such as 8.8.8.8).

```
Select a menu item from 1 to 11 [11]: 5 ←  
Enter DNS IPv4 Address : 8.8.8.8
```

26. Confirm everything is set and type **11** to **save and quit**.

```
7. Second NIC Netmask []:  
8. Second NIC Network address []:  
9. Second NIC Gateway IPv4 address []:  
10. Cancel and quit.  
11. Save and quit.  
  
Select a menu item from 1 to 11 [11]: 11 ←
```

---

**NOTE:** The Second NIC is optional and will not be configured.

---

```

Select a menu item from 1 to 11 [11]: 11
1/1: 2 link states coalesced
Jan 17 12:35:43 <kern.notice> ns kernel: 1/1: link state changed to UP

Save: Network configuration is completed successfully.
Registering masd with monit
Registering counterd with monit
Registering admsysinfo with monit
Reinitializing monit daemon
[Tue Jan 17 12:35:43 UTC 2023] Adding new crontab entry for MetricsCollector
[Tue Jan 17 12:35:43 UTC 2023] Adding new crontab entry for Daily Maintenance script
[Tue Jan 17 12:35:43 UTC 2023] Adding new crontab entry for Weekly Maintenance script
this is agent deployment, not starting nsaaad.
$Detecting NS UPX distribution version: OK
$Starting xe daemon: OK

login:

```

27. Log on to the **NetScaler agent** with the **nsrecover** username and **nsroot** password.

```

login: nsrecover
Password:
bash-3.2#

```

---

**NOTE: NSRECOVER** user account can be used by the administrator to recover **ADM/NetScaler** appliances.

---

28. Confirm you can **ping** the endpoint URL **adm.cloud.com**. For more about endpoint URLs, check the [official documentation](#).


```

bash-3.2# ping adm.cloud.com
PING adm.cloud.com (54.146.76.49): 56 data bytes

```

29. Run the script **deployment\_type.py** to start registering the local NetScaler agent to the NetScaler Console on Cloud.  
If you use a Proxy to connect to the Internet, please type “y” and set up it, otherwise, type “n”.

```

bash-3.2# deployment_type.py
-----
NetScaler Agent Registration with NetScaler Console. This menu allows
rl and obtain an instance ID for your device.
-----
Are you using proxy? y/n n 
Enter Service URL:

```


30. Return to the NetScaler Console portal and copy the SERVICE URL.

**Set Up Agent**

Install the agent on your hypervisor. Click [here](#) for instructions. Copy and enter the **service URL** and the **activation code** while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.

**Note:** One activation code can be used for only one agent. Also, you can install and register only one agent at a time using this wizard.

2 > Click [here](#) to know all the URLs the agent tries to connect during the agent installation which may be granted access

SERVICE URL  Copy 

**NOTE:** If you do not see the Service URL/Activation code, it might be due to **insufficient user's admin rights.**

- Return to the NetScaler Agent bash and past the SERVICE URL. Press **Enter**. If all is good with the communication with the NetScaler console, you will receive a prompt with the list of endpoint URLs. Just press enter to proceed.

```
bash-3.2# deployment_type.py
-----
NetScaler Agent Registration with NetScaler Console. This menu allows you to specify a cloud url and obtain an instance ID for your device.
-----
Are you using proxy? y/n n
Enter Service URL: juhu.agent.adm.cloud.com 
Working on agent diagnostic, please wait...
Endpoint connectivity checking done, all good
To view the list of all the endpoint URLs that must be allowed access, please enter 'yes' otherwise press any other key to continue:
Enter Activation Code :
```

- Return to the NetScaler Console portal and copy the **ACTIVATION CODE**.

SERVICE URL  Copy

ACTIVATION CODE  Copied  Generate new Activation Code

- Return to the NetScaler Agent bash and past the **ACTIVATION CODE**. Press **Enter**.

```
-----
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows specify a cloud url and obtain an instance ID for your device.
-----
Enter Service URL: carmel.agent.adm.cloud.com
Enter Activation Code : 800eb4a2-6821-42e6-a3c3-886d01275a78
-----
Agent registration successful.
-----
Restarting Agent Deamon. Please wait for a few minutes . . . . .
Stopping Agent
```

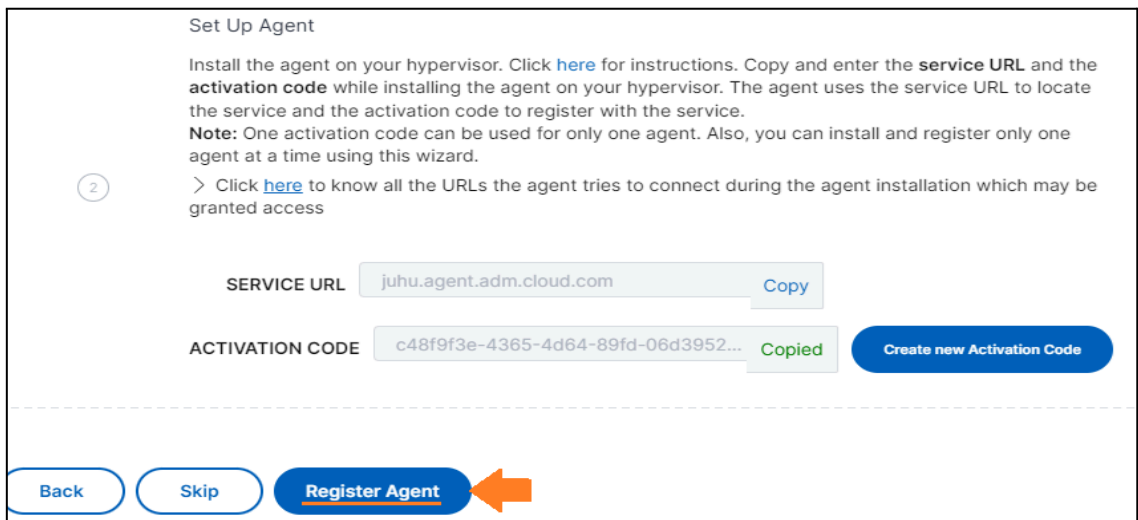
34. As the agent is configured with the default password, you will be prompted to change it. Please enter your own password and confirm it. Confirm you see the message saying, **Agent registration successful**.

```
Agent is configured with default password. Please change default password.
Password must be of minimum 6 characters length with at-least
one numeric, one upper case, one lower case, and one special character.
  Please Enter New Password :
  Please Re-enter New Password :
Updating Agent Password
-----
Agent registration successful.
-----
```

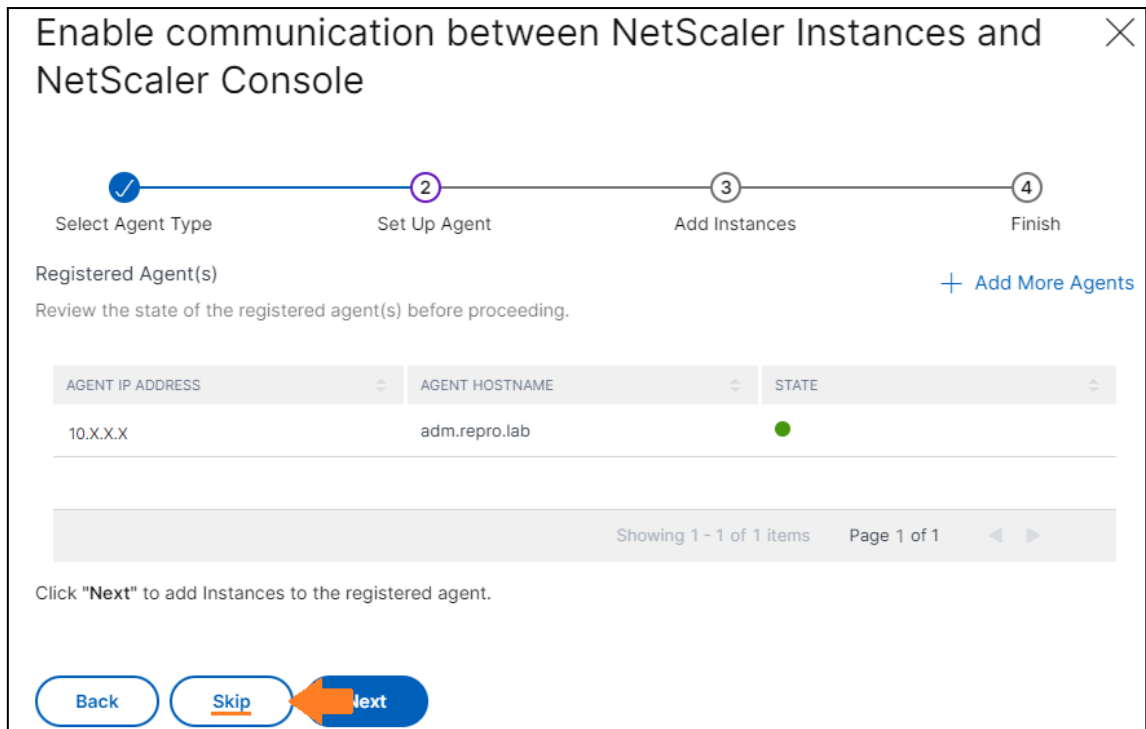
35. The ADM agent will stop/start some services. Just wait for a few seconds.

```
Restarting Agent Daemon. Please wait for a few minutes . . . . .
Stopping Agent
Reinitializing monit daemon
rm: /var/run/agent_upgrade.pid: No such file or directory
Reinitializing monit daemon
rm: /var/run/agent_monitor.pid: No such file or directory
Stopping nsulfd
Stopped nsulfd
Stopped Agent
Reinitializing monit daemon
Reinitializing monit daemon
Cloud Agent
Starting Agent
net.inet.tcp.fast_finwait2_recycle: 0 -> 1
kern.ipc.maxsockbuf: 262144 -> 16777216
Started nsulfd
Started Agent
bash-3.2#
```

36. Return to the **NetScaler Console portal** and click **“Register Agent”**. This process will take a few seconds.



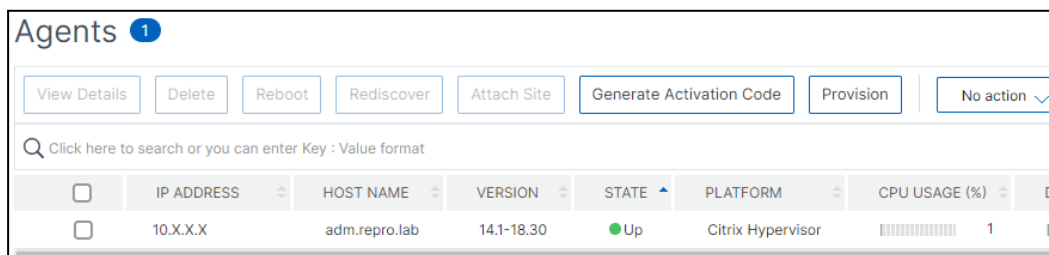
37. The **NetScaler agent** was recognized. Click **Skip** as we will not add any instances now.



38. On the top right, click on the **refresh** button to update the list of agents.



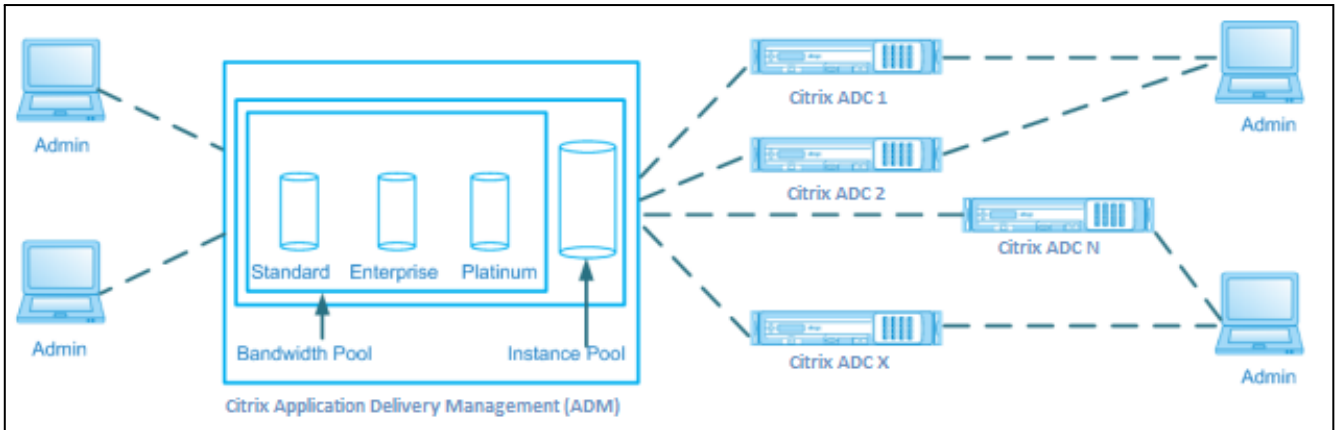
39. Your ADM agent is registered. Just for your knowledge, you can also change the ADM agent password through the **NetScaler Console** as shown below.



## Configure the ADM Service License Server (Pooled Capacity)

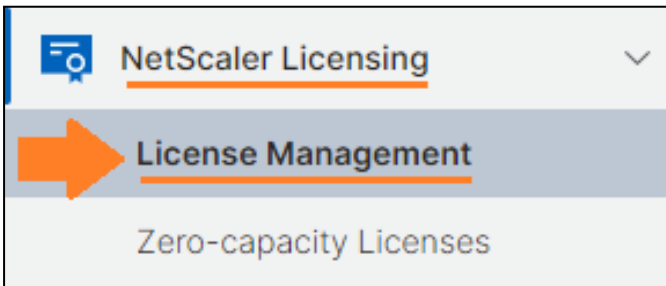
The pooled capacity allows you to share bandwidth or instance licenses across different NetScaler form factors as in the diagram below.



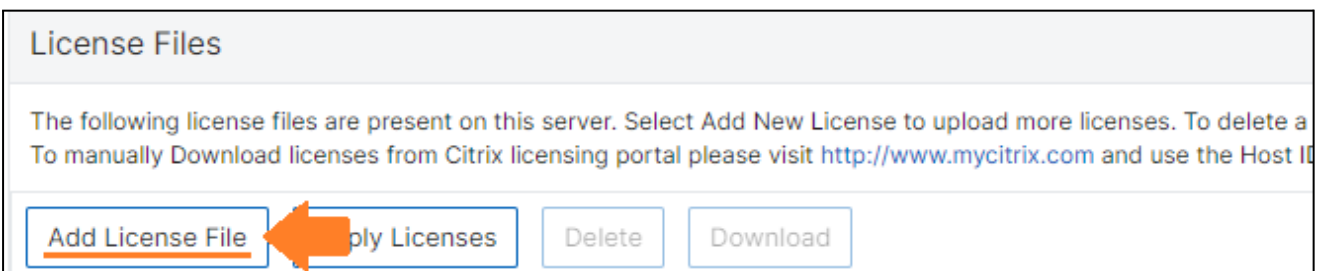


Notes:

1. To set up the ADM Service as a license server, we will need to upload the pooled capacity license files (bandwidth and instance pool) obtained from the Citrix License team. If you do not have the licenses, you can skip this exercise. However, you must have a valid license on the NetScaler for the upcoming exercises, such as GLSB and Gateway.
2. On the NetScaler console portal, navigate to “NetScaler Licensing > License Management”. On the right side of the page, you will find your unique HOST ID. This is the HOSTID that you need to provide to the Citrix License team to obtain your licenses.



You will upload **both licenses** to the **NetScaler console portal**. On the same page, you copied the **HOST ID**, you will find the **“Add license File”** button. Click on it to upload the licenses and click **“Apply licenses”**.



### License Files

You must upload the license files to this license server. If a license file is already present on your local computer.

Upload license files from a local computer  
 Use license access code



←

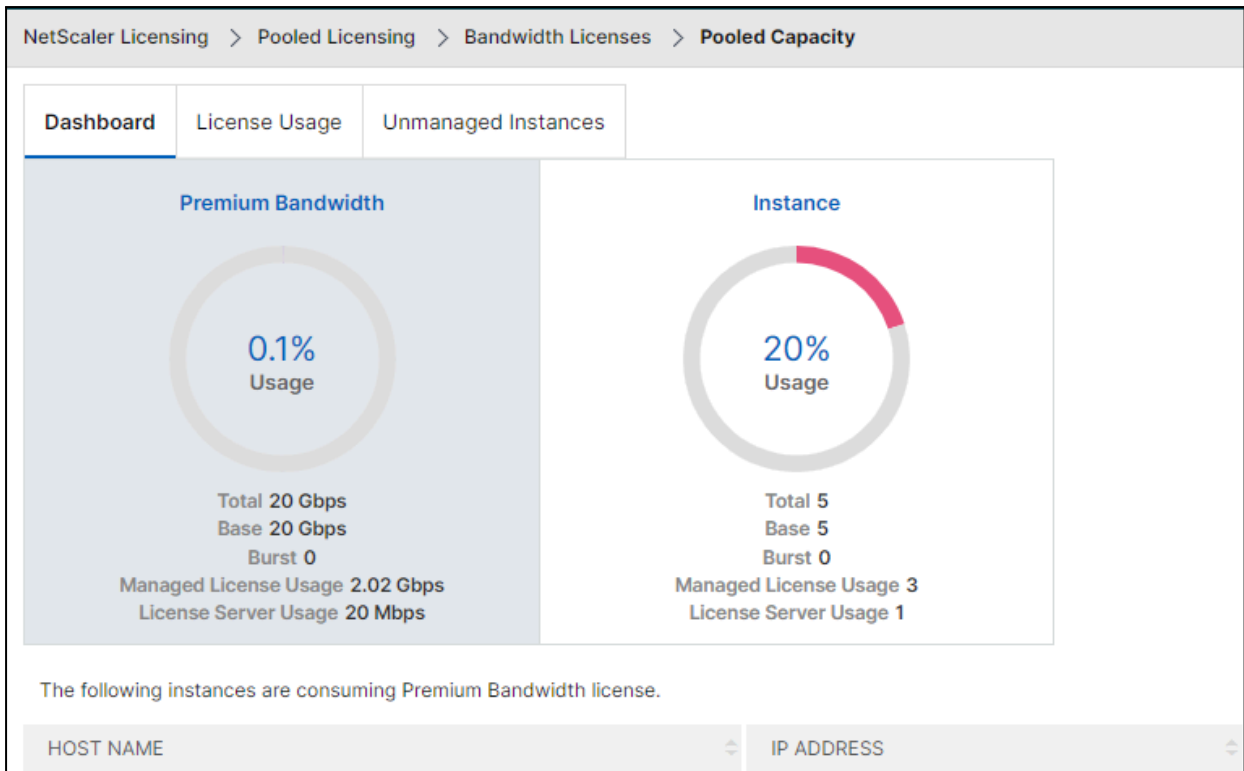
You should see both of your licenses applied as below. **20 Gbps** (this example) of bandwidth that can be consumed by up to **5 ADCs**.

License Expiry Information	
FEATURE	COUNT
Platinum Bandwidth	20,000
Instance	5
Total 2	

**NOTE:** If you do not see the licenses applied as above, **wait a few seconds, and refresh the page**

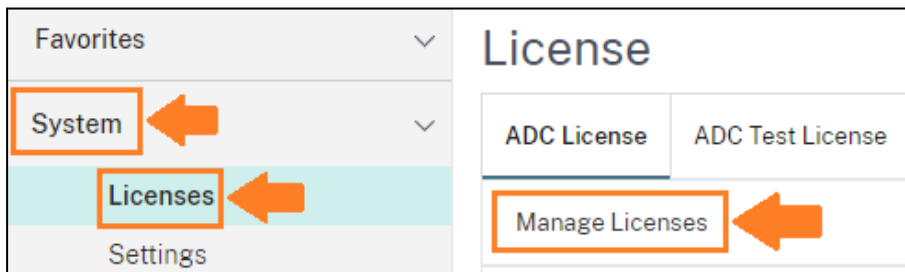
Navigate to **NetScaler Licensing > Pooled licensing > Pooled capacity** to view the license's dashboard. As soon as you start licensing your NetScalers, you will be able to manage the license through this dashboard.

-  **NetScaler Licensing** ▾
- License Management
- Zero-capacity Licenses
- Flexed Licensing ▾
- Dashboard
- Reporting
- Pooled Licensing** ▾
- Bandwidth Licenses ▾
-  **Pooled Capacity**

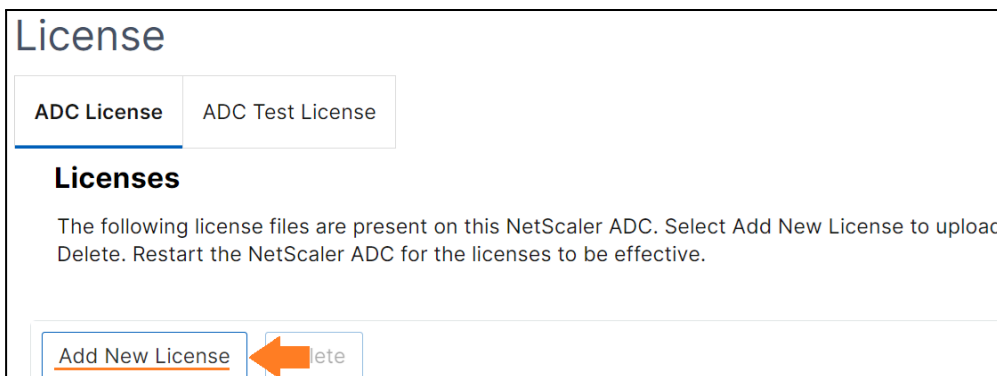


## Configure the Pooled License to the NetScaler

1. Log on to your NetScaler "ADC02" (As best practice, changes will start on the secondary ADC).
2. Navigate to **System > Licenses > Manage Licenses**.



3. Click **Add new license**.



4. Select **Use remote licensing**.

5. In the drop-down select "Pooled Licensing".
6. Enter the Server License IP: "Type YOUR ADM AGENT IP and port 27000"
7. Enter Username: "nsroot" and Password: "The Password you set in your ADM agent"
8. Click Continue.

Upload license files

Use License Access Code

Use remote licensing

Remote Licensing Mode

Pooled Licensing

Server Name/IP Address\*

Your-ADM-Agent-IP

License Port\*

27000

**NetScaler ADM access credentials to register**

Username\*

nsroot

Password\*

Your-ADM-Agent-Password

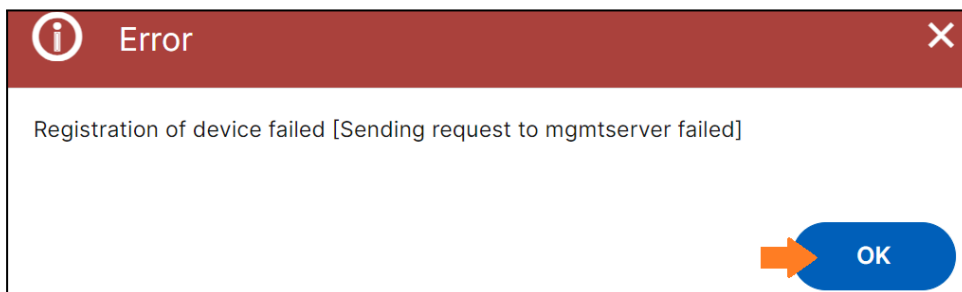
Validate Certificate

Device Profile Name

ns\_nsroot\_profile

Continue Back

**NOTE:** You might see the below error, please ignore it by clicking OK and wait.



9. Allocate **20 Mbps Bandwidth** and click **Get Licenses**. Feel free to allocate more bandwidth if you have more available bandwidth.

**NOTE:** As informed before, the ADM License server is showing its capabilities/available license. 5 Instances and 20 Gbps bandwidth.

**Allocate licenses** ✕

(License Server)

Platinum ▼

TYPE	TOTAL	AVAILABLE	ALLOCATE
Instance	500	440	1
Bandwidth	50 Gbps	41.99 Gbps	20 <span style="float: right;">←</span> Mbps

**Get Licenses** ← Cancel

**NOTE:** For both the primary and secondary instances, you need to allocate licenses of the same capacity.

10. Click **Reboot** and this will apply the license.

**License**

ADC License ADC Test License

⚠ Appliance should be rebooted for license to take effect

**Reboot** ←

**Confirm** ✕

Do you want to warm reboot now?

**Yes** ← No

11. Please perform the failover and update the license of the NetScaler “**ADC01**” by repeating the steps above (from 1 to 6).

## Third NetScaler 14.1 for GSLB Install CLI

**NOTE:** If you have already downloaded the NetScaler firmware and configured the initial NetScaler IP (NSIP), subnet mask, and gateway, please skip the steps 1 - 3.

1. Set up NetScaler **VPX 03** following the identical process used for installing VPX 01 and VPX 02. Ensure that you use the same software version.  
Download the NetScaler firmware:  
<https://www.citrix.com/downloads/citrix-adc/>  
For steps on how to deploy the NetScaler on the supported platforms, please refer to the official documentation:  
<https://docs.netScaler.com/en-us/citrix-adc/current-release/deploying-vpx>
2. After selecting the NetScaler platform and installing the firmware, proceed to configure the **management IP (NSIP), Netmask**, and your designated **Gateway** using the **NetScaler Console**.

```
+---[DSA 1024]---+
|
|  +=***. .
|  0.+ .0.+*.
|  * *000.0
|  . X0+00. .
|  S oE= . .
|  .*.0
|  ..0
|  *0
|  .0
+---[SHA256]---+
kern.sched.idlespinthresh: 157 -> 32
Start daemons: syslogd Dec 19 13:34:40 <kern.info> ns syslogd: kernel boot file
is /flash/ns-14.1-4.42
Dec 19 13:34:40 <kern.notice> ns kernel: lo0: link state changed to UP
inetd cron httpd monit sshd /etc/ssh_config line 19: Deprecated option UsePriv
legeSeparation
.
?There is no ns.conf in the /nsconfig!
Start Netscaler software
tput: no terminal type specified and no TERM environmental variable.
Enter Citrix ADC's IPv4 address []:
```

3. Enter the **new IP, netmask**, and **your own gateway**. **Save** and **quit** if everything is correct by pressing the number **4**.

```
-----
Citrix ADC Virtual Appliance Initial Network Address Configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([ ]).
Selecting the listed number allows the address to be changed.

After the network changes are saved, you may either login as nsroot and
use the Citrix ADC command line interface, or use a web browser to
http://10.91.69.145 to complete or change the Citrix ADC configuration.
-----
1. Citrix ADC's IPv4 address [ 10.X.X.X ]
2. Netmask [ 255.X.X.X ]
3. Gateway IPv4 address [ 10.X.X.X ]
4. Save and quit
Select item (1-4) [4]: 4
```

- 4. The NetScaler will boot, and the login prompt will appear.

```
NetScaler initialization is still in progress; please wait
20 to 30 seconds before attempting to log in.
Jan 13 14:58:12 <local0.alert> 10.110.73.136 01/13/2023:14:57:47 GMT 0-PPE-0 :
default EVENT STATECHANGE 27 0 : Device "self node 10.110.73.136" - State UP
#####
#
#          WARNING: Access to this system is for authorized users only.          #
#          Disconnect IMMEDIATELY if you are not an authorized user!          #
#
#####
login:
```

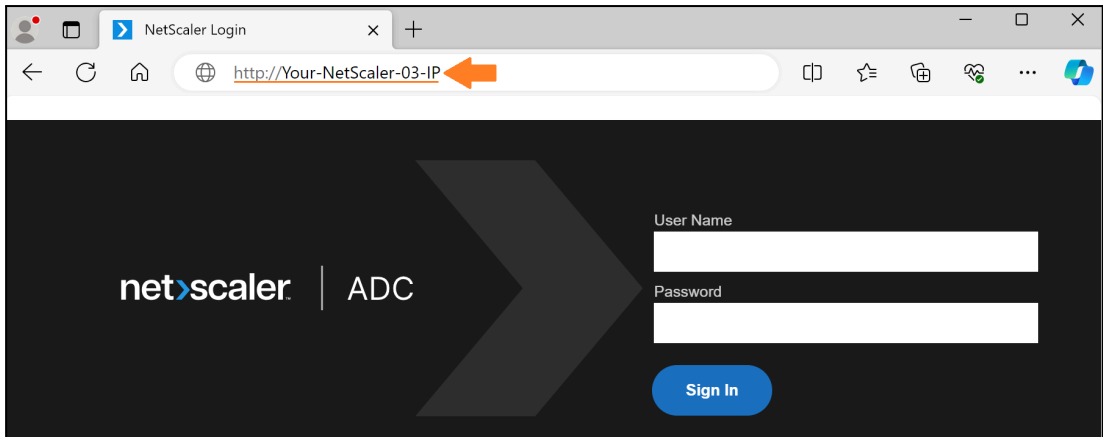
- 5. Enter **nsroot** as the username and "**nsroot**" as the password. You will be prompted to change your nsroot password. Set a new password (The same password you set on the NetScaler ADC01).
- 6. Save the configuration using the command **save config**.

```
login: nsroot
Password:
Dec 20 10:15:25 <auth.notice> ns login: ROOT LOGIN (nsroot) ON ttyv0

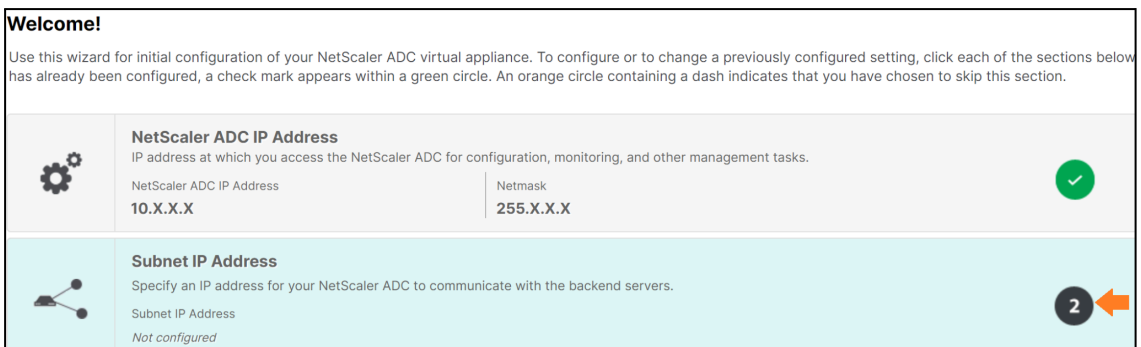
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
> save config
Done
```

- 7. Open your **browser**, type **http(s)://YOUR-NETSCALER-03-IP** and hit the **Enter key**. Type "**nsroot**" for username and your new password. Click **Log on**.

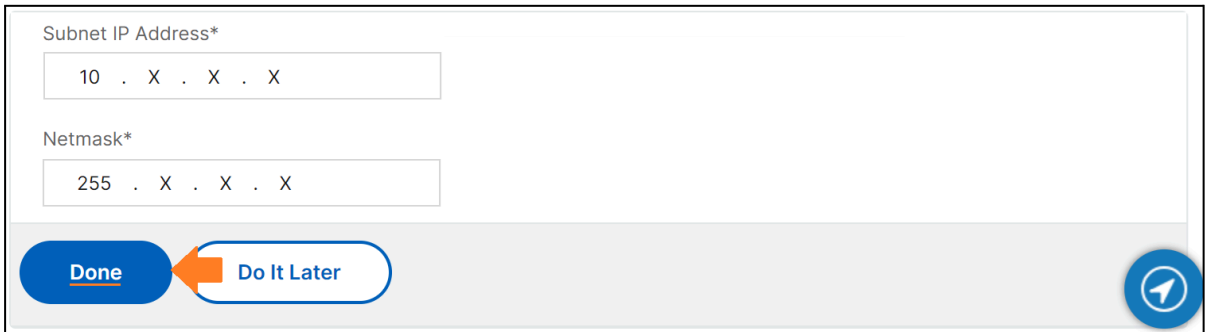




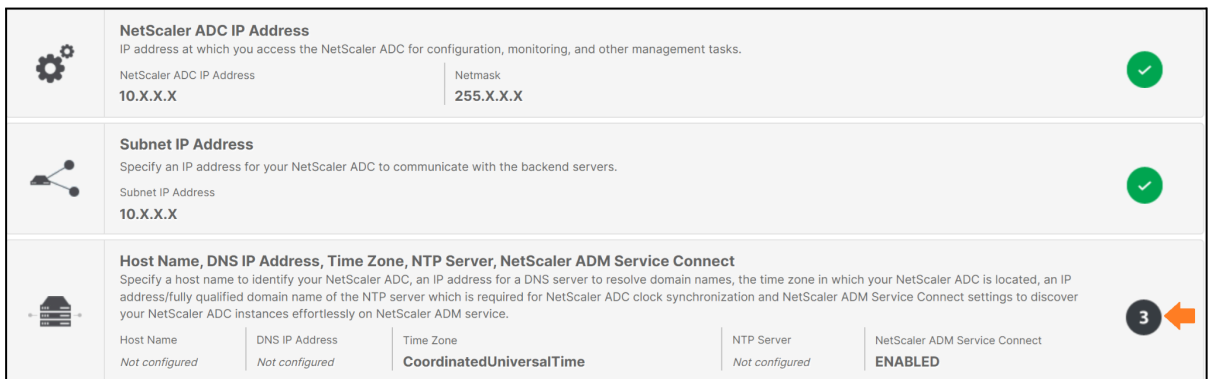
8. Click over option **number 2**.



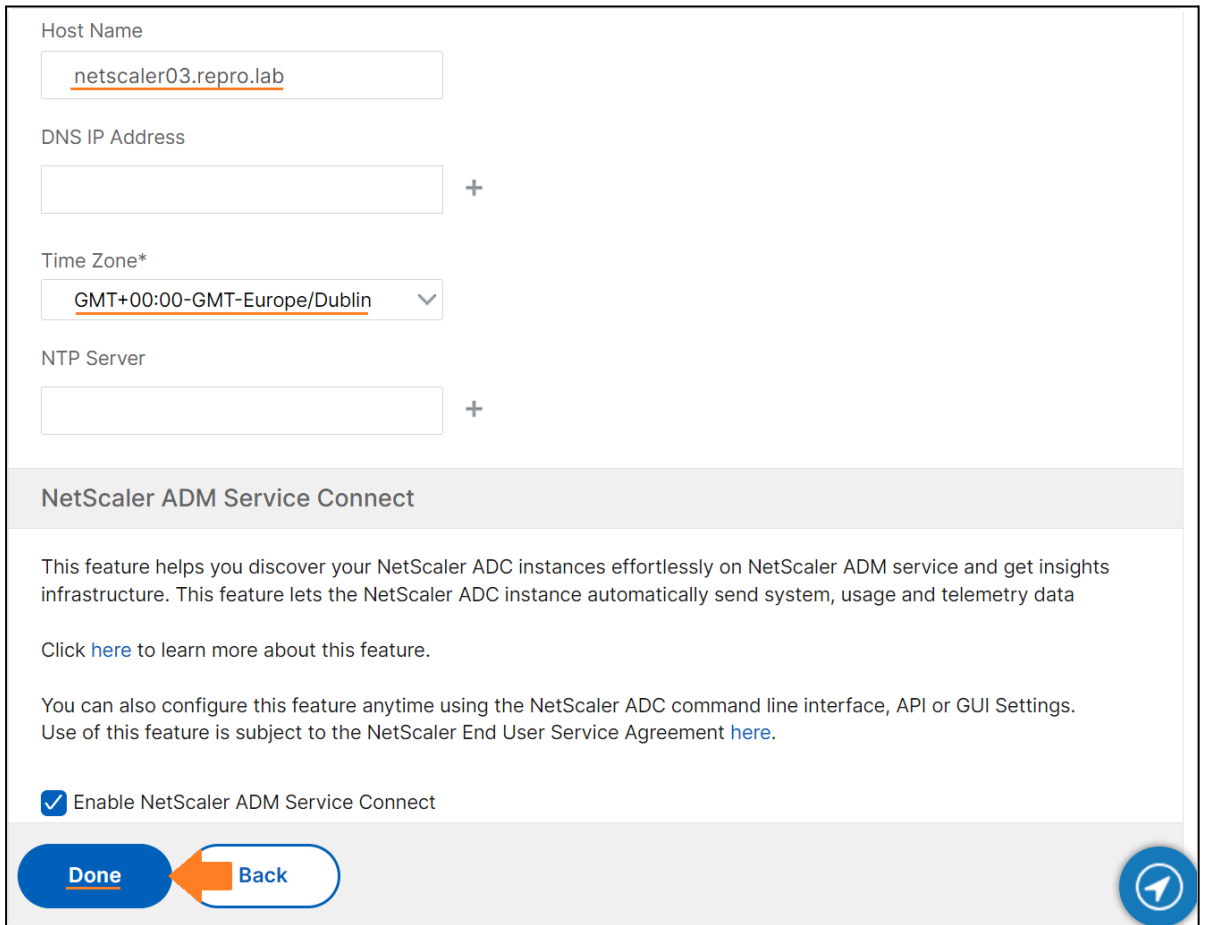
9. Enter your Subnet IP Address (SNIP) + Netmask. This IP must be free in the network. Click **Done**.



10. Click over option **number 3**.



11. Enter the hostname “**netScaler03.repro.lab**”, and set your **local time zone**. If you already have an internal DNS/NTP server in your network, feel free to enter the IP(s). Click **Done**.



Host Name

DNS IP Address  
 +

Time Zone\*  
 ▾

NTP Server  
 +

**NetScaler ADM Service Connect**

This feature helps you discover your NetScaler ADC instances effortlessly on NetScaler ADM service and get insights infrastructure. This feature lets the NetScaler ADC instance automatically send system, usage and telemetry data

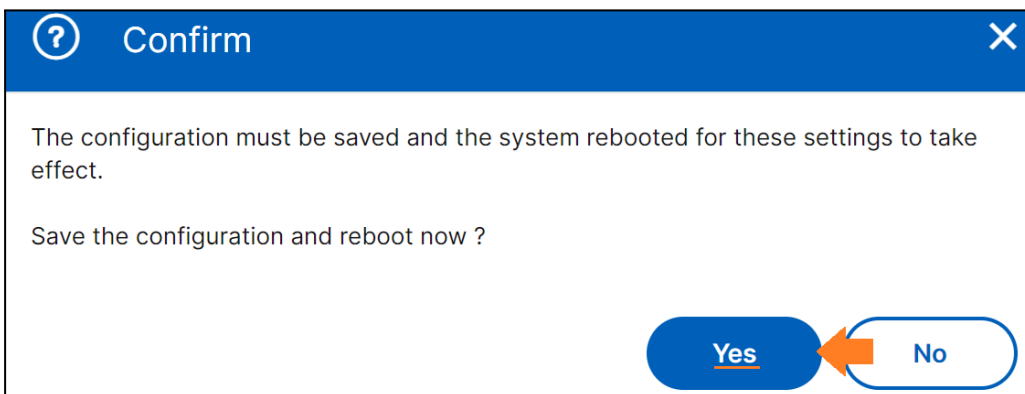
Click [here](#) to learn more about this feature.

You can also configure this feature anytime using the NetScaler ADC command line interface, API or GUI Settings. Use of this feature is subject to the NetScaler End User Service Agreement [here](#).

Enable NetScaler ADM Service Connect

**Done** ← **Back**

12. When prompted to save and reboot the NetScaler, click **YES**. The NetScaler GUI will be available again in about a minute.



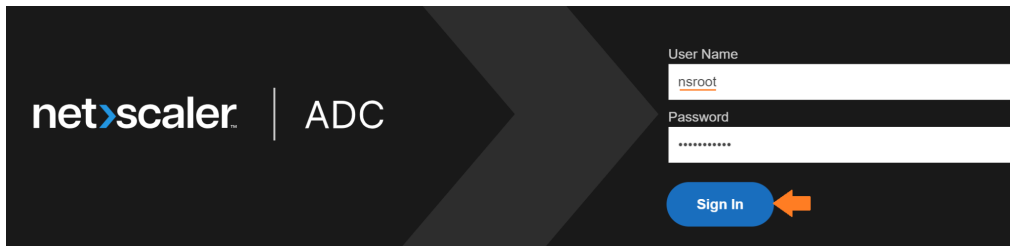
**Confirm**

The configuration must be saved and the system rebooted for these settings to take effect.

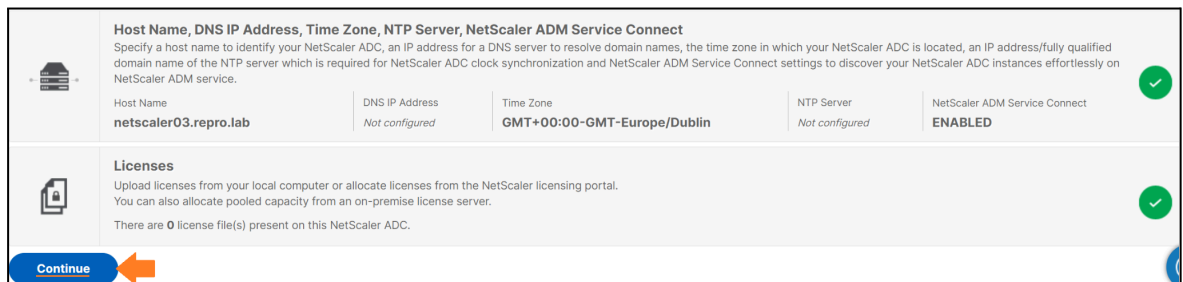
Save the configuration and reboot now ?

**Yes** ← **No**

13. Log on again to your NetScaler with your **nsroot** username and your **new password**.



14. Click **Continue**. The Initial configuration is **done**.



## Configuring an HTTP LB VIP

**NOTE:** Putty will be used for the below exercise. If you do not have putty installed, please [download](#) it and install it on your Jump Box VM. Once you open the Putty, insert your **NetScaler IP ADC 03** and click Open.

1. Enable the LoadBalancing feature, add your **Web Servers** using their respective IPs, add the **HTTP Services** and bind them with the **Servers**.

commands:

```
enable feature LoadBalancing
add server srv_http_01 10.X.X.X
add server srv_http_02 10.X.X.X
add service svc_http_01 srv_http_01 http 80
add service svc_http_02 srv_http_02 http 80
```

```
> enable feature LoadBalancing
Done
> add server srv_http_01 10.X.X.X
Done
> add server srv_http_02 10.X.X.X
Done
> add service svc_http_01 srv_http_01 http 80
Done
> add service svc_http_02 srv_http_02 http 80
Done
```

2. Add an **HTTP LB VIP** and utilize the same Web Server services created before. Please use a **new Free IP** for your VIP.

commands:

```
add lb vserver lb_vip_http_repro.lab HTTP 10.X.X.X 80
bind lb vserver lb_vip_http_repro.lab svc_http_01
bind lb vserver lb_vip_http_repro.lab svc_http_02
```

```

> add lb vserver lb_vip_http_repro.lab HTTP 10.X.X.X 80
Done
> bind lb vserver lb_vip_http_repro.lab srvc_http_01
Done
> bind lb vserver lb_vip_http_repro.lab srvc_http_02
Done

```

3. Increase the NetScaler session timeout to prevent the GUI session from timing out during further lab exercises. **Save** the configuration.

```

> set system user nsroot -timeout 7200
Done
> save config
Done

```

4. Confirm your HTTP Load Balancing shows as UP under Traffic Management> Load Balancing > Virtual Servers

---

Notes:

1. If the Virtual Server shows DOWN, please ensure you have configured your SNIP correctly (IP/netmask) and your LoadBalancing feature is enabled.
  2. There is no need to configure a fourth NetScaler. The **ADC03** will remain as **STANDALONE**.
- 

**\*\*CLI TIP\*\***

To explore additional functionalities of the CLI, aside from utilizing the "tab" key once for auto-completion or twice to reveal available options, consider creating the desired entity through the GUI and monitor the ns.log to capture the CLI command executed in the background. Below is a section of the ns.log, showing the command executed when creating an HTTP Load Balancer VIP and setting up a cookie persistence via the GUI.

```

<local0.info> 10.91.69.145 11/21/2023:10:48:15 GMT ADC03 0-PPE-0 : default GUI CMD_EXECUTED 4317 0 : User ns
ADM_User NONE - Remote ip 10.90.118.107 - Command "add lb vserver lb_vip_gui HTTP 1.2.3.4 80 -range 1 -timeout 2 -backu
eout 2 -lbMethod LEASTCONNECTION -rule none -Listenpolicy NONE -resRule none -persistMask 255.255.255.255 -v6pe
rsonality None -td 0 -macmodeRetainvlan DISABLED -dns64 DISABL" - Status "Success"

```

```

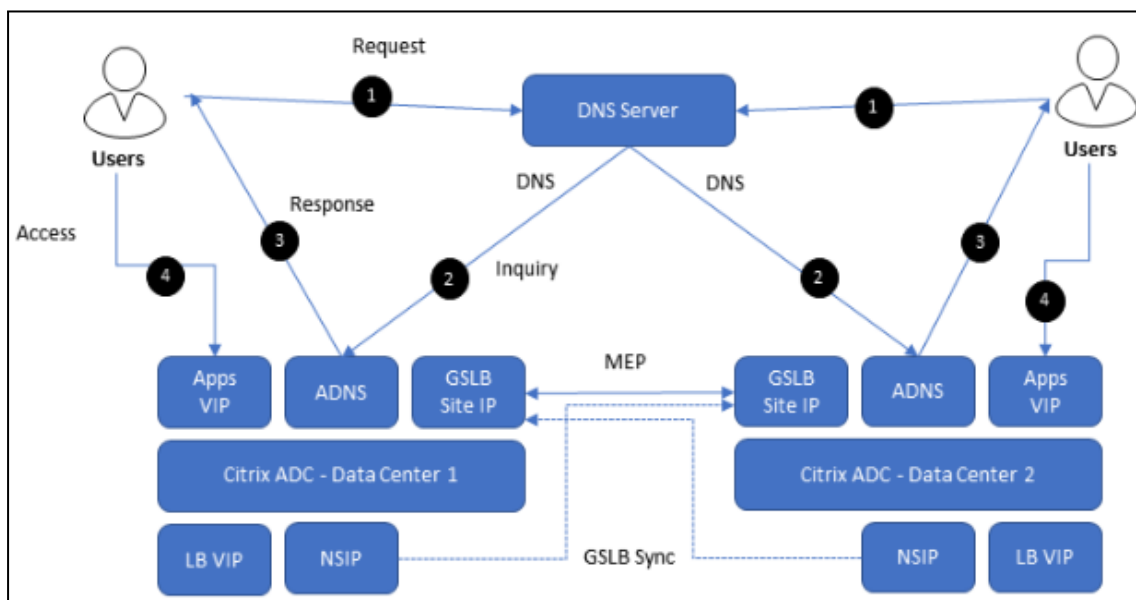
10:49:30 <local0.info> 10.91.69.145 11/21/2023:10:49:30 GMT ADC03 0-PPE-0 : default GUI CMD_EXECUTED 4397 0 : User ns
ADM_User NONE - Remote ip 10.90.118.107 - Command "set lb vserver lb_vip_gui -IPAddress 1.2.3.4 -IPPattern 0.0.0.0 -IPM
-persistenceType COOKIEINSERT -timeout 2 -persistenceBackup NONE -backupPersistenceTimeout 2 -lbMethod LEASTCONNECTION -
Name my_cookie_repro.lab -persistMask 255.255.255.255 -v6persistmasklen 128 -rtspNat OFF -m IP -dataOffset 0 -sessionles

```

# Configuring GSLB Active-Active

Global Server Load Balancing (GSLB) directs DNS requests to the best performing GSLB site in a distributed Internet environment. When you configure GSLB and enable MEP, the NetScaler systems use the DNS infrastructure to connect the client to the data center that best meets the criteria that you set.

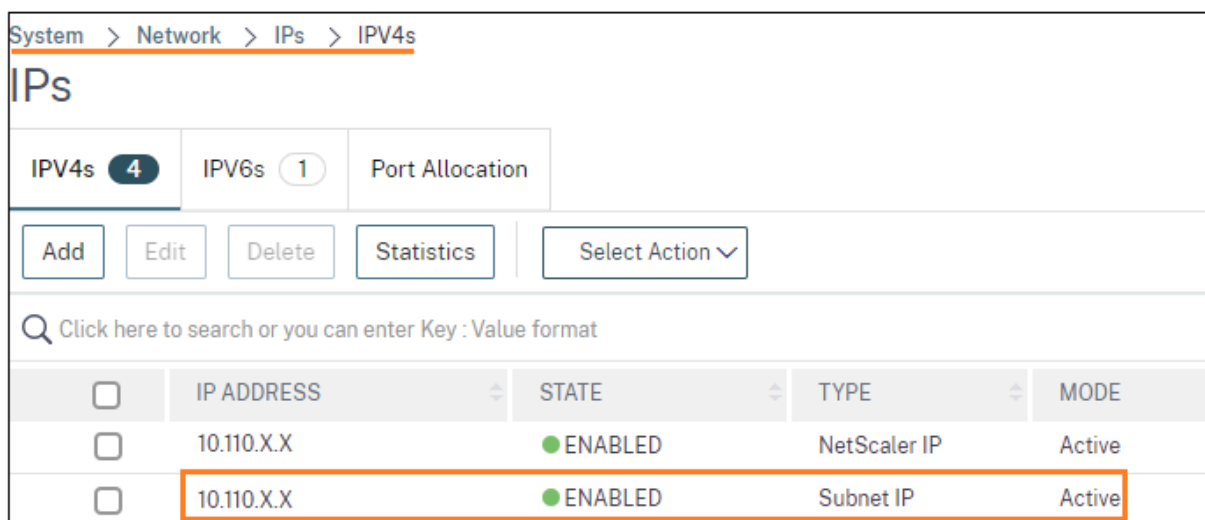
**NOTE: Active-Active** deployment type means, ADNS queries are addressed by any of the active sites based on the configured GSLB algorithm methods. The below illustration shows an example of **ACTIVE-ACTIVE**



**NOTE:** For this exercise, the NetScaler **ADC01** will be used as **SITE 01 AMERICA** and the NetScaler **ADC03** will be used as **SITE 02 EUROPE**.

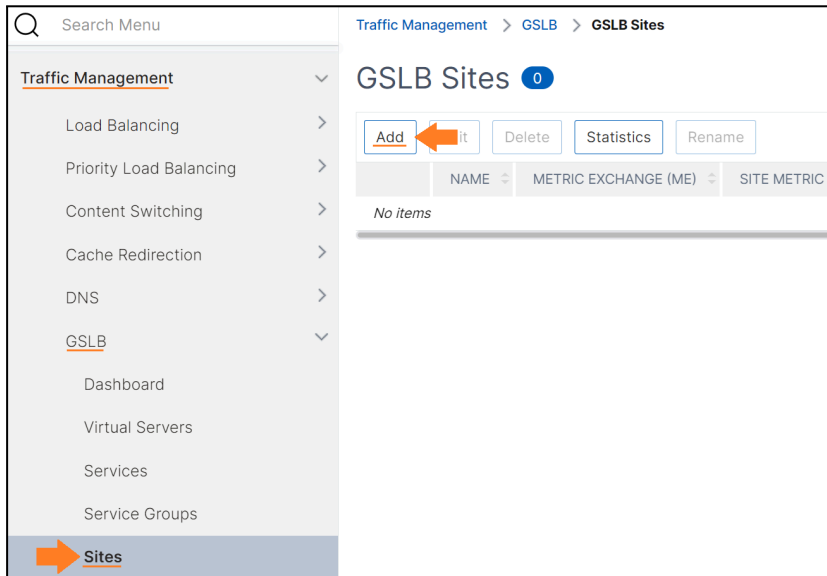
## Configuring GSLB SITE 01

1. Log on to the NetScaler ADC01 navigate System > Network > IPs and take notes of your SNIP.



**NOTE:** **ADC01 SNIP** will represent SITE 01 AMERICA and **ADC03 SNIP** will represent SITE 02 EUROPE.

2. Navigate to **Traffic Management > GSLB > Sites** and click **Add**. If you see a yellow circle next to GSLB, click over and enable the feature.



3. Enter the name **SITE01-AMERICA**, select **LOCAL** as the type, and insert your **ADC01 SNIP** as Site IP Address. Click **Create**.

← Create GSLB Site

Name\*

Type

Site IP Address\*

Public IP Address

Parent Site  Backup Parent Sites

Parent Site Name

Cluster IP

Public Cluster IP

NAPTR Replacement Suffix

Metric Exchange  
 Network Metric Exchange  
 Persistence Session Entry Exchange

**NOTE:** If you have not enabled the GSLB feature, you will see the below prompt. Just click **Yes**.

Confirm

Feature 'GSLB' is disabled.  
 Do you wish to enable it?

4. **Unselect** the **SITE01-AMERICA** and click **Add** to add the second site.

GSLB Sites 1

<input type="checkbox"/>	NAME	METRIC EXCHANGE (ME)	SITE METRIC MEP STATUS
<input type="checkbox"/>	SITE01-AMERICA	● ENABLED	

5. Enter the name **SITE02-EUROPE**, select **REMOTE** as the type, and insert your **ADC03 SNIP** as Site IP Address. Click **Create**.

**NOTE:** Get the ADC03 SNIP from ADC03 GUI > System > Network > IPs.



← Create GSLB Site

Name\*

Type

Site IP Address\*

Public IP Address

Parent Site  Backup Parent Sites

Parent Site Name

Cluster IP

Public Cluster IP

NAPTR Replacement Suffix

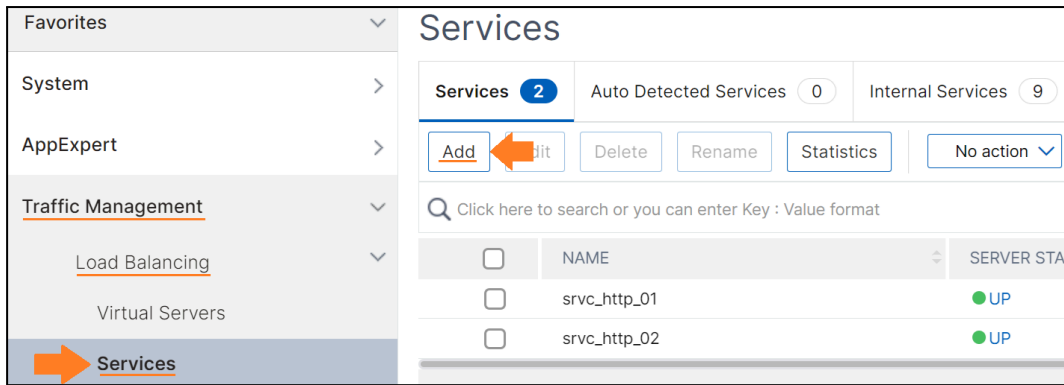
Metric Exchange  
 Network Metric Exchange  
 Persistence Session Entry Exchange

6. You should see both sites as below. Ensure the names match exactly as described. MEP is **DOWN** because the site entities on the **ADC03** are not yet configured.

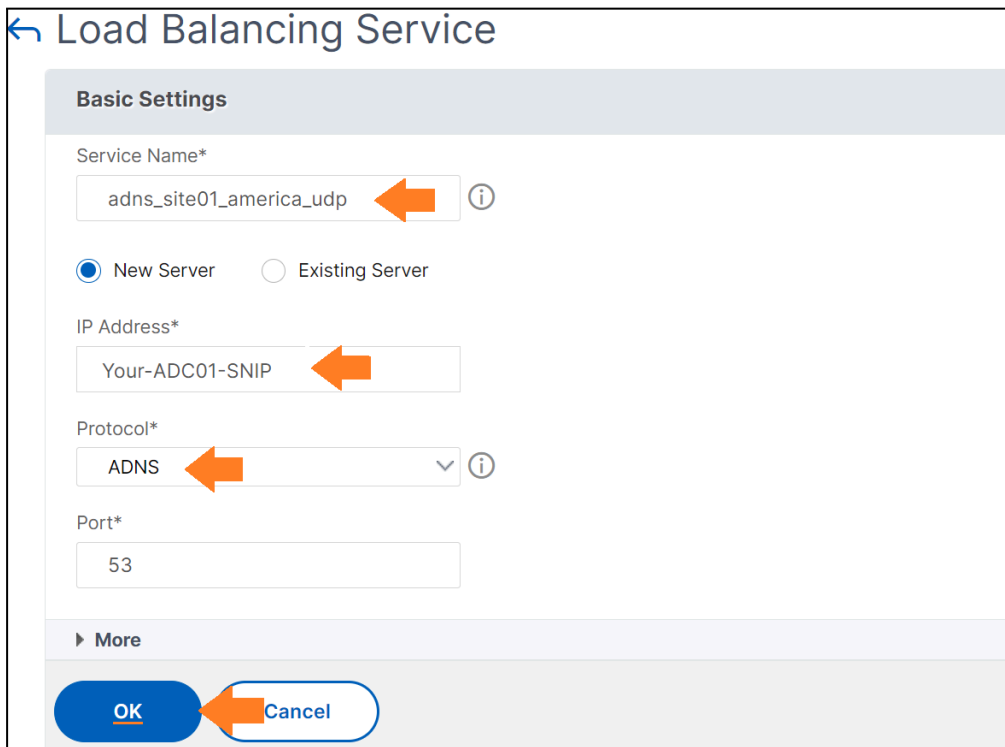
GSLB Sites 2

<input type="checkbox"/>	NAME	METRIC EXCHANGE (ME)	SITE METRIC MEP STATUS
<input type="checkbox"/>	SITE01-AMERICA	● ENABLED	
<input type="checkbox"/>	SITE-2-EUROPE	● ENABLED	● DOWN

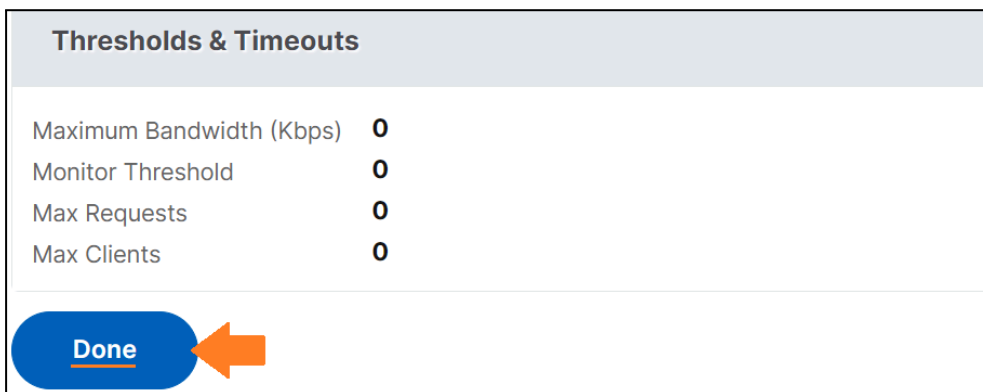
7. From the **NetScaler ADC01**, navigate to **Traffic Management > Load Balancing > Services** and click **Add**.



- Enter the name **adns\_site01\_america\_udp**, select **ADC01 SNIP** as the type, select **ADNS** as protocol and click **OK**.



- Ensure the server state shows UP. Click **Done**.



- Unselect the ADNS service created and click **Add** again.

## Services

Services **3**    Auto Detected Services **0**    Internal Services **9**

<input type="checkbox"/>	NAME	SERVER STATE
<input type="checkbox"/>	adns_site01_america_udp	<span style="color: green;">●</span> UP

- Enter the name `adns_site01_america_tcp`, type the ADC01 SNIP, select `ADNS_TCP` as protocol and click OK.

### Load Balancing Service

**Basic Settings**

Service Name\*

New Server     Existing Server

IP Address\*


Protocol\*

Port\*

- Ensure the server state shows **UP**. Click **Done**.

### Thresholds & Timeouts

Maximum Bandwidth (Kbps)	0
Monitor Threshold	0
Max Requests	0
Max Clients	0

**Done** 

## Services

Services **4**    Auto Detected Services **0**    Internal Services **9**

🔍 Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE
<input type="checkbox"/>	adns_site01_america_tcp	● UP
<input type="checkbox"/>	adns_site01_america_udp	● UP

**Notes:**

1. The ADNS service accepts incoming client requests for domains for which the NetScaler system is authoritative. ADNS will listen to DNS queries on port 53.
2. By default, some clients use the User Datagram Protocol (UDP) for DNS, which specifies a limit of 512 bytes for the payload length of UDP packets. To handle payloads that exceed 512 bytes in size, the client must use TCP, for this reason, ADNS TCP is created.

13. Navigate to **System > Network > Ips** and ensure your SNIP is shown as **SNIP |GSLB site IP | ADNS svc IP**.

**NOTE:** You can have one IP per service, but this is not required, thus, the SNIP is used for all the services.

System > Network > IPs > IPv4s

## IPs

IPV4s **5** | IPV6s **1** | Port Allocation

Add Edit Delete Statistics Select Action ▾

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	IP ADDRESS	STATE	TYPE
<input type="checkbox"/>	10.110.X.X	● ENABLED	NetScaler IP
<input type="checkbox"/>	10.110.X.X	● ENABLED	Subnet IP GSLB site IP ADNS svc IP

14. Select the SNIP and click **Edit**.

System > Network > IPs > IPv4s

## IPs

IPV4s **5** | IPV6s **1** | Port Allocation

Add Edit Statistics Select Action ▾

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	IP ADDRESS	STATE	TYPE
<input type="checkbox"/>	10.110.X.X	● ENABLED	NetScaler IP
<input checked="" type="checkbox"/>	10.110.X.X	● ENABLED	Subnet IP GSLB site IP ADNS svc IP

15. Scroll down the page, enable **“Management Access control...”** and enable **SSH**. This is required for GSLB SYNC between the Sites.

### Application Access Controls

Enable Management Access control to support the below listed applications. ⓘ

Telnet ⓘ       FTP ⓘ

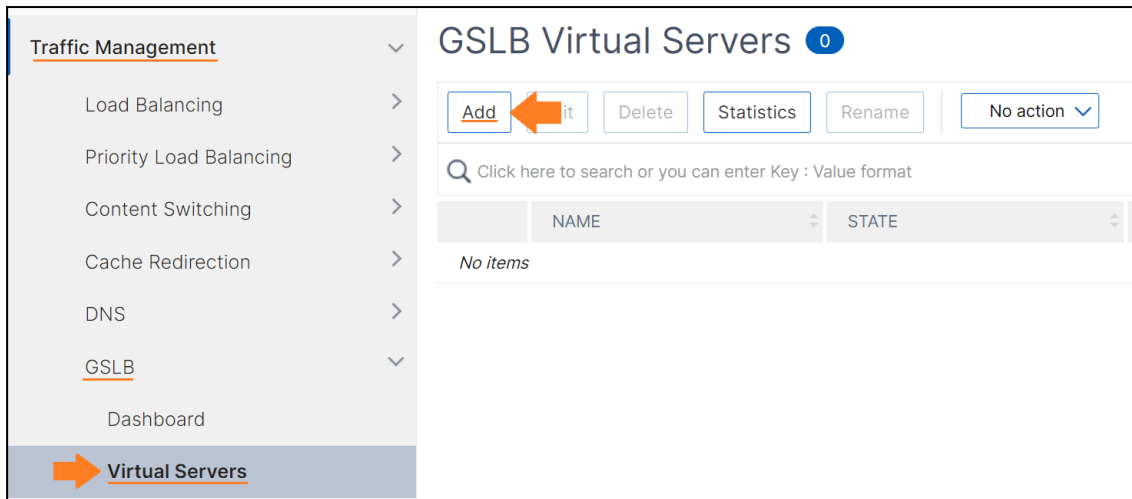
SSH ⓘ       SNMP ⓘ

GUI ⓘ       Secure Access Only

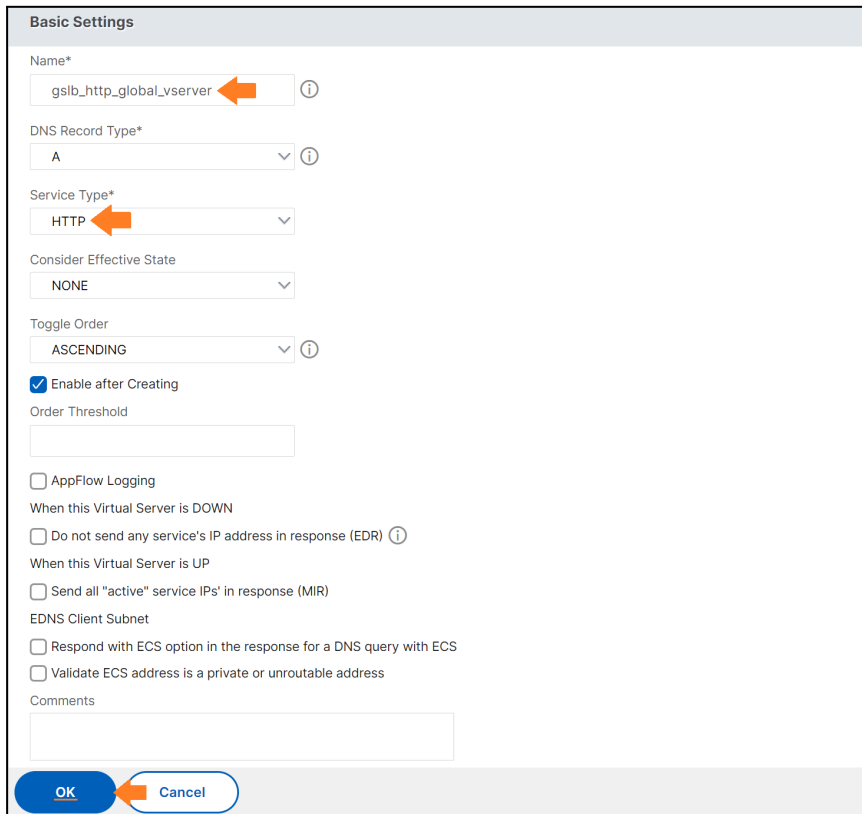
Allow access only to management applications

OK Close

16. Navigate to **Traffic Management > GSLB > GSLB Virtual Servers** and click **Add**.



17. Enter the name **gslb\_http\_global\_vserver**, keep the other settings, and click **OK**.



18. Click **No GSLB Virtual Server to GSLB Service Binding** to add your Service.

**NOTE:** In GSLB, “GSLB Service” means “Any NetScaler Virtual Server”, either LB VIP, CS VIP, or Gateway VIP.

### GSLB Virtual Server

**Basic Settings**

Name	gslb_http_global_vserver
DNS Record Type	A
Service Type	HTTP
Consider Effective State	NONE
State	● DOWN

**GSLB Services** | **GSLB Service Group Binding**

No GSLB Virtual Server to GSLB Service Binding

No GSLB Virtual Server to GSLB Service Group Binding

19. Click **Add**.

### GSLB Service Binding

Select Service\*

Click to select > **Add**

**Binding Details**

Weight

1

20. Enter the name **gslb\_http\_colors\_america**, select the **LOCAL** site **SITE01-AMERICA**, keep **HTTP** as a service, mark **“Virtual Server”**, select from the drop-down your **HTTP LB VIP**, click **OK** and **Done**.



**Basic Settings**

Service Name\*  
 ←

Site Name\*  
 ←

Site Type

Type\*

Service Type\*

Port\*

Existing Servers
  New Server
  Virtual Servers ←

Virtual Server\*  
 ←

Server IP\*

Public IP

Public Port

Enable after Creating  
 Enable Health Monitoring  
 AppFlow Logging

Comments

←

21. Click Bind.

**GSLB Service Binding**

Select Service\*  
 >

**Binding Details**

Weight

Dynamic Weight

Cumulative Weight

Order

←

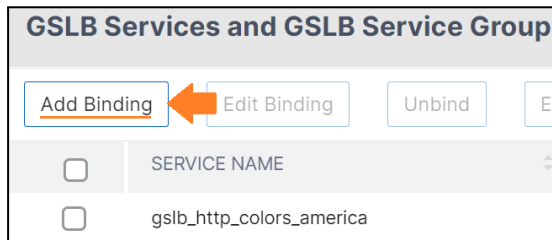
22. Click again **1 GSLB Virtual Server to GSLB Service Binding** to add the second LB VIP.

GSLB Services and GSLB Service Group Binding

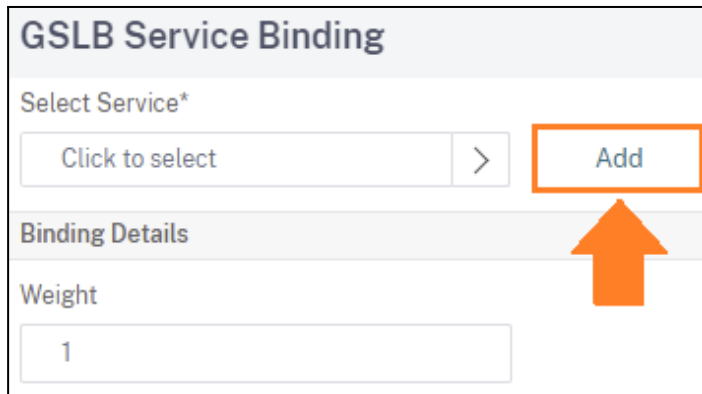
1 GSLB Virtual Server to GSLB Service Binding

No GSLB Virtual Server to GSLB Service Group Binding

23. Click **Add Binding**.






24. Click **Add**.



25. Enter the name **gslb\_http\_colors\_europe**, select the **REMOTE site SITE02-EUROPE**, keep **HTTP** as a service, mark **New Server**, and select ADC03 HTTP LB VIP address as the type, click **OK** and **Done**.

**Basic Settings**

Service Name\*  
 

Site Name\*  
   

Site Type

Type\*

Service Type\*

Port\*

Existing Servers  New Server

Server IP\*

Public IP


Public Port

Enable after Creating  
 Enable Health Monitoring  
 AppFlow Logging

Comments

26. Click **Bind**.

**GSLB Service Binding**

Select Service\*  
 

**Binding Details**

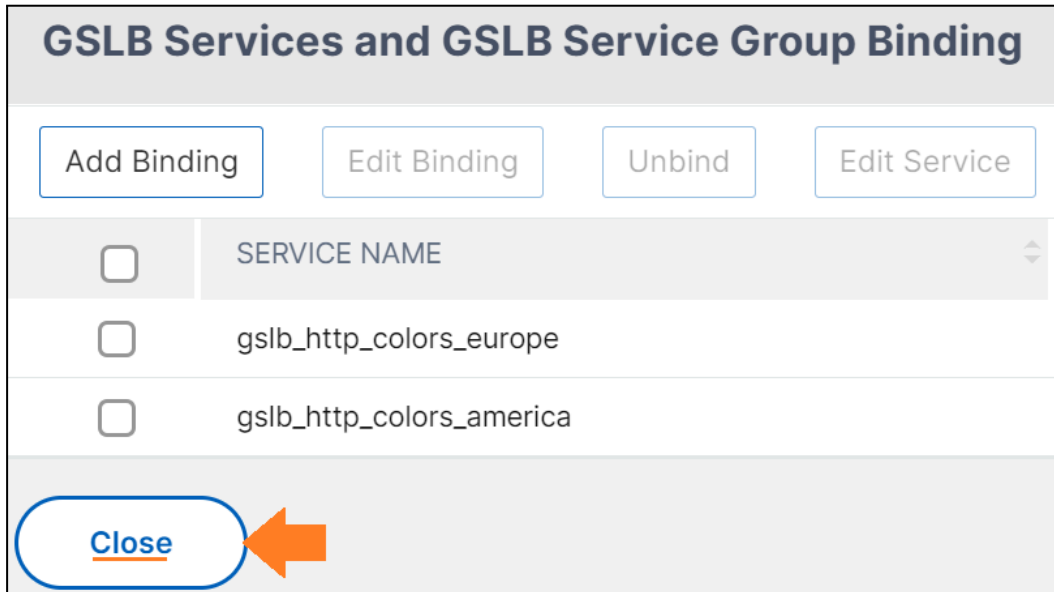
Weight

Dynamic Weight

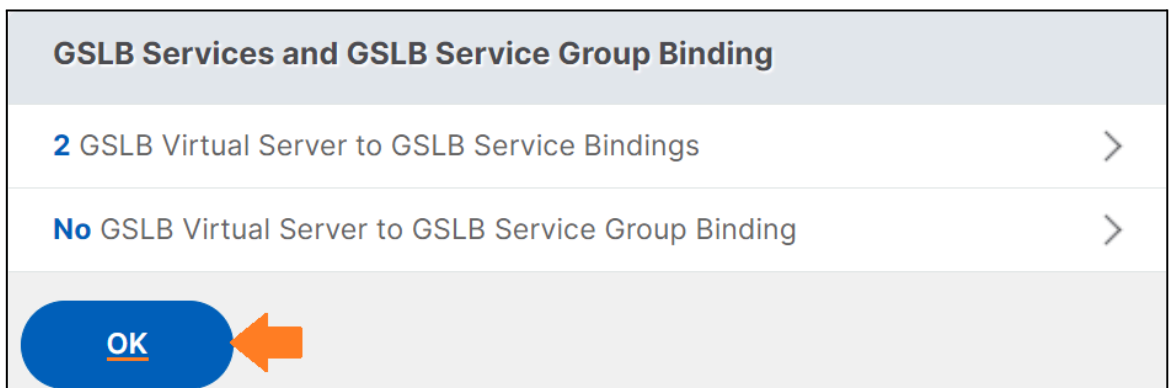
Cumulative Weight

Order

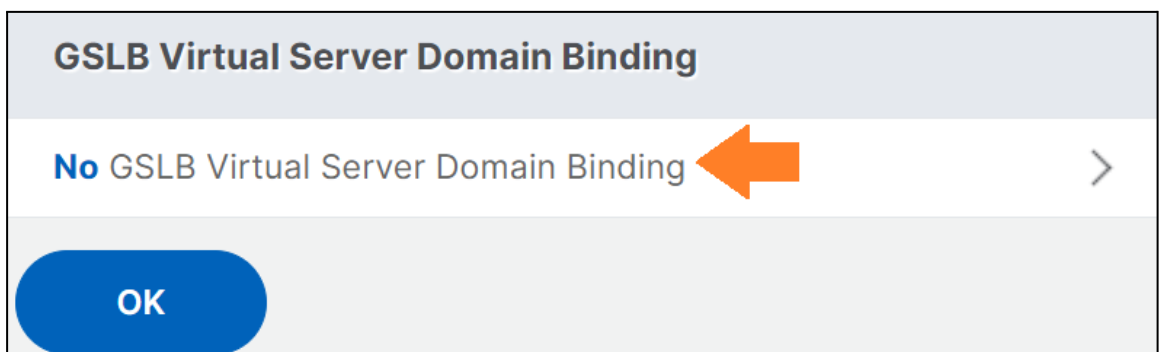
27. Both GSLB Services (HTTP LB VIPs) will show, and the remote service will show in the **DOWN** state as expected. Once **SITE 02** is configured, the service will come up due to MEP. Click **Close**.



28. Click **OK**.





29. Click **No GSLB Virtual Server Domain Binding**.



30. Add the domain FQDN "**gslb.repro.lab**". This GSLB Virtual server will reply to all DNS queries addressed to **gslb.repro.lab**. Click **Bind**.

**Domain Binding**

FQDN\*

gslb.repro.lab  

TTL (secs)

5

Backup IP


Cookie Domain

Cookie Time-out (mins)

0


Site Domain TTL (secs)


3600

**Bind**  **Close**

31. Click **OK**.

**GSLB Virtual Server Domain Binding**


1 GSLB Virtual Server Domain Binding 


**OK** 

**NOTE:** The GSLB Virtual Server is invoked by a DNS query/domain name configured rather than an IP address as any other Virtual server on the NetScaler.

32. The ADNSs created before are automatically bound to the GSLB Vserver. Click **OK**


**ADNS Service**

2 Services 

**OK** 

33. Keep the method **LEASTCONNECTION** but you can change it if you wish.

Method	
Choose Method	<b>LEASTCONNECTION</b>
Tolerance (ms)	<b>0</b>
IPv4 Netmask	<b>255.255.255.255</b>
Backup Method	<b>ROUNDROBIN</b>
IPv6 Mask Length	<b>128</b>
Dynamic Weight	<b>DISABLED</b>

**Done** 

34. GSLB Virtual Server is configured.



Traffic Management > GSLB > GSLB Virtual Servers

## GSLB Virtual Servers 1

[Add](#) [Edit](#) [Delete](#) [Statistics](#) [Rename](#)

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	PROTOCOL	% HEALTH
<input type="checkbox"/>	<a href="#">gslb_http_global_vserver</a>	<span style="color: green;">●</span> UP	HTTP	50.00% 1 UP/1 DOWN


 

35. 35. Save the configuration

## Configuring GSLB SITE 02

1. Log on to the **ADC03** and navigate to Traffic Management > GSLB > Sites and click Add.

Traffic Management

- Load Balancing
- Priority Load Balancing
- Content Switching
- Cache Redirection
- DNS
- GSLB**
  - Dashboard
  - Virtual Servers
  - Services
  - Service Groups
  - Sites** 

## GSLB Sites 0

[Add](#) [Edit](#) [Delete](#) [Statistics](#) [Rename](#)

	NAME	METRIC EXCHANGE (ME)	SITE METRIC MEP STATUS
<i>No items</i>			

2. Enter the name **SITE01-AMERICA**, select **REMOTE** as type, **ADC01 SNIP** as Site IP Address and Click **Create**.

← Create GSLB Site

Name\*  
 ⓘ

Type  
 ⓘ

Site IP Address\*

Public IP Address

Parent Site  Backup Parent Sites

Parent Site Name

Trigger Monitors\*

Cluster IP  
 ⓘ

Public Cluster IP

NAPTR Replacement Suffix

Metric Exchange  
 Network Metric Exchange  
 Persistence Session Entry Exchange

3. Unselect the **SITE01-AMERICA** and click **Add** to add the second site.

GSLB Sites 1

<input type="checkbox"/>	NAME	METRIC EXCHANGE (ME)
<input type="checkbox"/>	SITE01-AMERICA	<span style="color: green;">●</span> ENABLED

4. Enter the name **SITE02-EUROPE**, select **LOCAL** as the type, and insert your **ADC03 SNIP** as Site IP Address. Click **Create**.



← Create GSLB Site

Name\*  
 ⓘ

Type  
 ⓘ

Site IP Address\*

Public IP Address

Parent Site  Backup Parent Sites

NAPTR Replacement Suffix

Metric Exchange  
 Network Metric Exchange  
 Persistence Session Entry Exchange

5. You should see the **MEP** status as **ACTIVE** after you **REFRESH** the page. Save the configuration.

Traffic Management > GSLB > GSLB Sites

GSLB Sites 2

<input type="checkbox"/>	NAME	METRIC EXCHANGE (ME)	SITE METRIC MEP STATUS	TYPE
<input type="checkbox"/>	SITE01-AMERICA	● ENABLED	● ACTIVE	REMOTE
<input type="checkbox"/>	SITE02-EUROPE	● ENABLED		LOCAL

6. Navigate to **Traffic Management > Load Balancing > Services** and click **Add**.

Favorites

- System
- AppExpert
- Traffic Management**
  - Load Balancing
  - Virtual Servers
  - Services**

Services

Services 2 Auto Detected Services 0 Internal S

🔍 Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME
<input type="checkbox"/>	svc_http_01
<input type="checkbox"/>	svc_http_02

Total 2

7. Enter the name **adns\_site02\_europe\_udp**, type **ADC03 SNIP** in the IP Address, select **ADNS** as protocol, and click **OK**.

The screenshot shows the 'Basic Settings' dialog box. The 'Service Name\*' field contains 'adns\_site02\_europe\_udp'. The 'IP Address\*' field contains 'Your-ADC03-SNIP'. The 'Protocol\*' dropdown menu is set to 'ADNS'. The 'Port\*' field contains '53'. The 'New Server' radio button is selected. At the bottom, the 'OK' button is highlighted with an orange arrow pointing to it.

8. Ensure the server state shows **UP**. Click **Done**.

The screenshot shows the 'Service Settings' dialog box. The 'Use Proxy Port' is set to 'NO', 'Down State Flush' is 'ENABLED', and 'Access Down' is 'NO'. At the bottom, the 'Done' button is highlighted with an orange arrow pointing to it.

9. Unselect the ADNS service created and click **Add** again.

The screenshot shows the 'Services' list. At the top, there are three tabs: 'Services' (3), 'Auto Detected Services' (0), and 'Internal Services' (12). Below the tabs are buttons for 'Add', 'Delete', 'Rename', 'Statistics', and 'No action'. A search bar is present with the text 'Click here to search or you can enter Key : Value format'. Below the search bar is a table with two columns: 'NAME' and 'SERVER STATE'. The table contains one row with the name 'adns\_site02\_europe\_udp' and the state 'UP'.

	NAME	SERVER STATE
<input type="checkbox"/>	adns_site02_europe_udp	● UP

10. Enter the name **adns\_site02\_europe\_tcp**, enter ADC03 SNIP, select ADNS\_TCP, and click **OK**.

**Load Balancing Service**

**Basic Settings**

Service Name\*  
adns\_site02\_europe\_tcp

New Server  Existing Server

IP Address\*  
Your-ADC03-SNIP

Protocol\*  
ADNS\_TCP

Port\*  
53

▶ More

**OK** **Cancel**

11. Ensure the server state shows **UP**. Click **Done**.

**Service Settings**

Use Proxy Port **NO**  
Down State Flush **ENABLED**  
Access Down **NO**

**Done**

**Services**

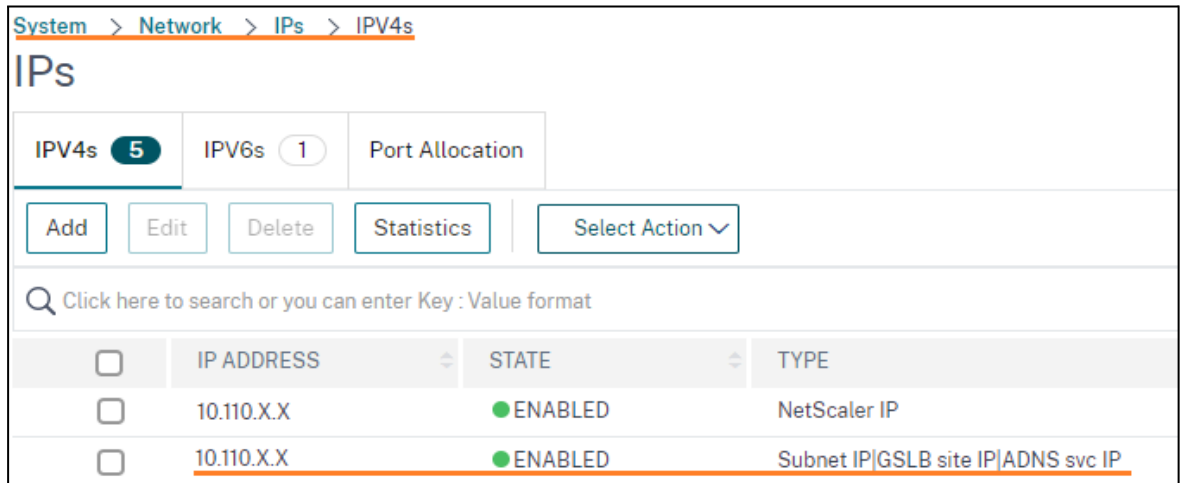
Services **4** Auto Detected Services **0** Internal Services **12**

Add Edit Delete Rename Statistics No action

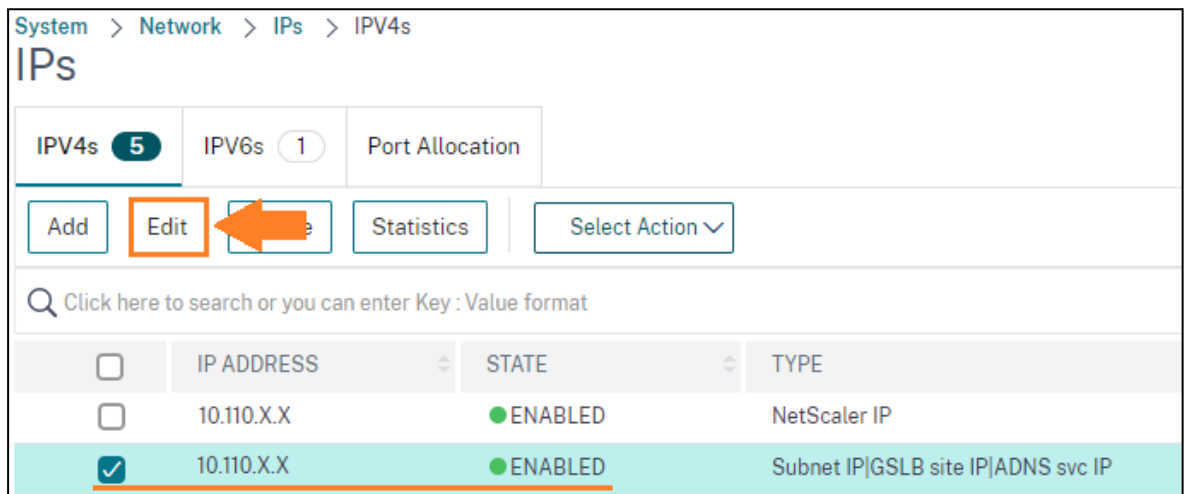
Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE
<input type="checkbox"/>	adns_site02_europe_tcp	● UP
<input type="checkbox"/>	adns_site02_europe_udp	● UP

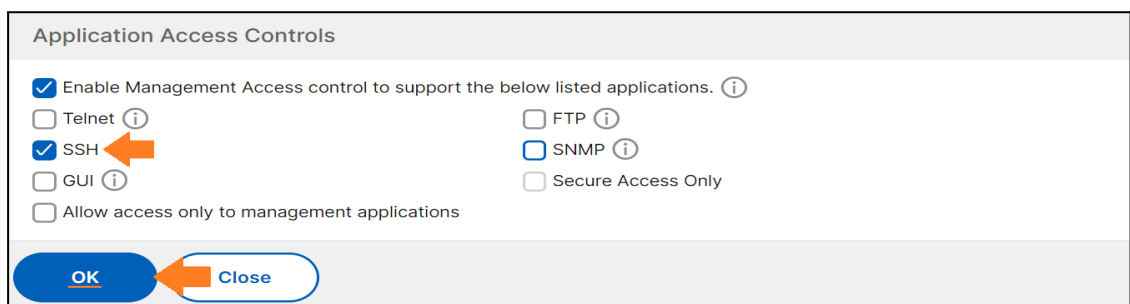
- Navigate to **System > Network > Ips** and ensure your SNIP is shown as SNIP |GSLB site IP |ADNS svc IP”.



- Select the **SNIP** and click **Edit**.



- Scroll down the page, enable **Management Access control...** and enable **SSH**. This is required for GSLB SYNC between the Sites.



- Save the configuration

## Manual Sync Between Site 01 and Site 02

**NOTE:** This process will push the GSLB Service and GSLB Vserver configuration to the **ADC03 – Site02**. For more information about Sync, check the [official documentation](#).

1. Log on to the NetScaler **ADC01** and confirm that **Site02 Europe** is **UP** and its GSLB Service is also **UP**. Navigate to **Traffic Management > GSLB > Sites**.

	NAME	METRIC EXCHANGE (ME)	SITE METRIC MEP STATUS
<input type="checkbox"/>	SITE01-AMERICA	● ENABLED	
<input type="checkbox"/>	SITE02-EUROPE	● ENABLED	● ACTIVE

2. Navigate to **GSLB > Services** and confirm both services are **UP**.

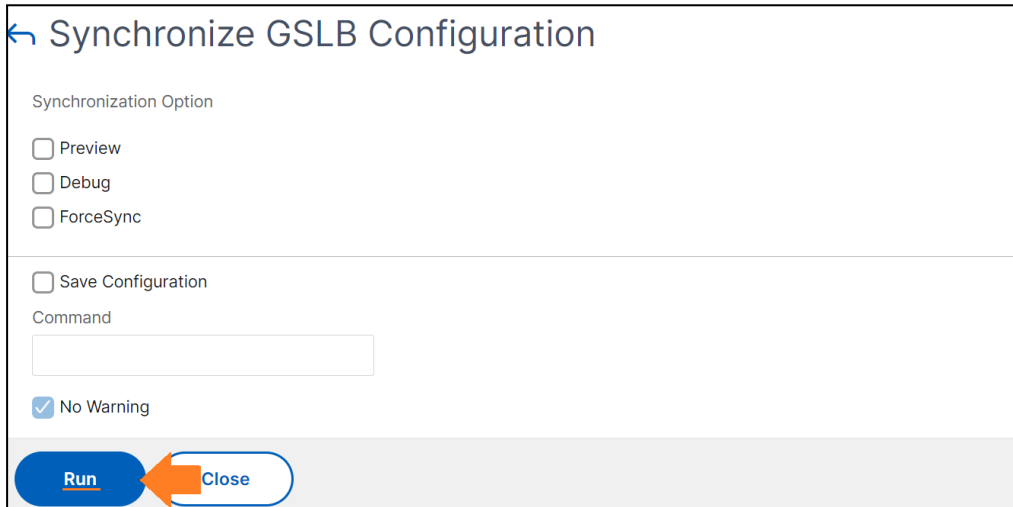
	NAME	STATE	EFFECTIVE STATE
<input type="checkbox"/>	gslb_http_colors_america	● UP	● UP
<input type="checkbox"/>	gslb_http_colors_europe	● UP	● UP

**NOTE:** In the example above, the local NetScaler learned the status of the Remote site via **MEP**. However, there is an option to bind a monitor to the remote service (known as an **Explicit monitor**). If one or more monitors are bound to a **GSLB service**, the health of this service is controlled by these monitors instead of MEP, thus, overriding the MEP. For more, please check the [CTX251348](https://www.citrix.com/help/netScaler/gslb/monitoring-gslb-services.html)

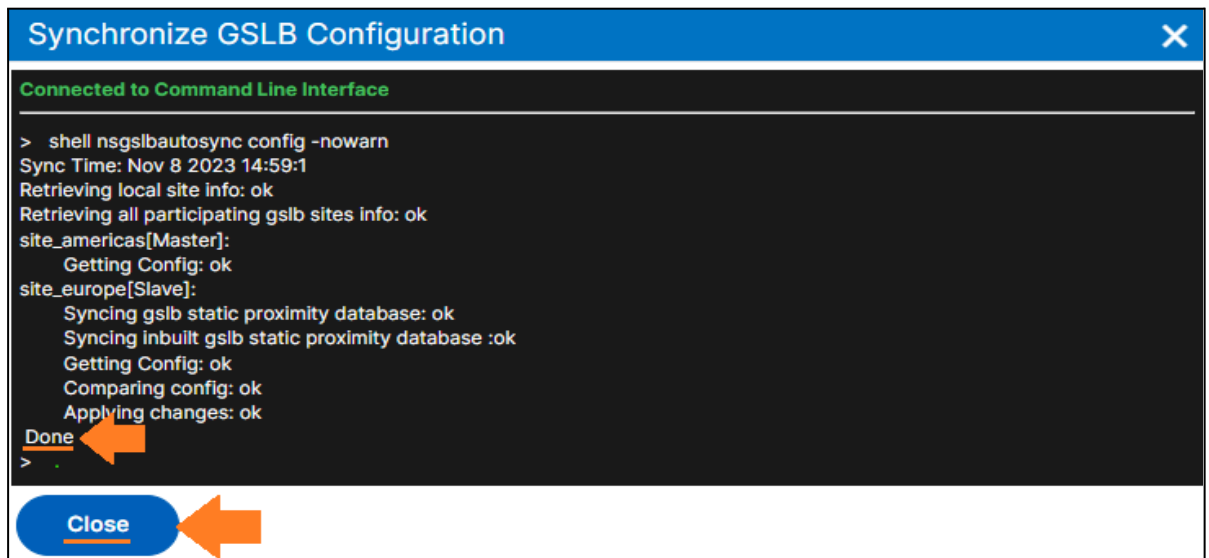
3. Navigate to **GSLB > Dashboard**. You will see the overall GSLB configuration/summary. Top right corner, click **Auto Synchronization GSLB**.

**NOTE:** Both nodes member of GSLB deployment must run the same software version for GSLB SYNC. The nodes can work in different versions (SYNC will not work only).

- Click **Run**. This will start the sync from **ADC01-Site 01** to **ADC03-Site 03**.



- Confirm you see **ok for** all the processes followed by **Done**. Click **Close** and **Close** again.

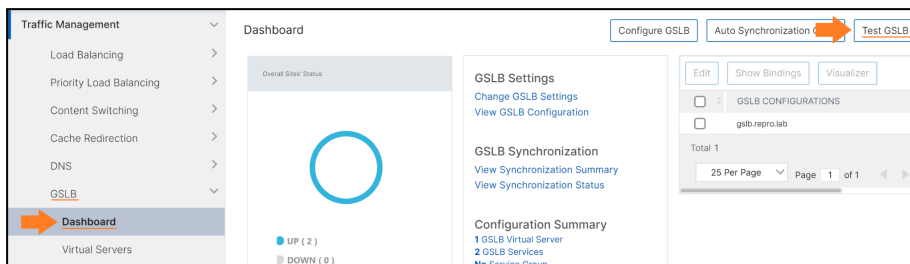


**NOTE:** If real-time synchronization is enabled, you do not have to click Auto Synchronize GSLB. To enable real-time synchronization, do the following: Navigate to **Traffic Management > GSLB > Dashboard**, click **Change GSLB Settings**, and select the **Automatic Config Sync** check box.

- Log on to the **ADC03 – Site 02** and confirm the GSLB Services and GSLB Vserver are visible.

## Testing the GSLB Deployment

- Navigate to **GSLB > Dashboard** and at the top right corner, click **Test GSLB**.



2. Select the domain created before under the GSLB Vserver **gslb.repro.lab**.
3. Select DNS Record Type **A** and click **Test**.

← Test GSLB

Domain Name\*  
gslb.repro.lab

ADNS Service  DNS Server

ADNS Service\*  
adns\_site01\_america\_udp Add

DNS Record Type  
A ⓘ

Test Close

**NOTE:** This will reproduce the DNS record type **A** the ADC GSLB will reply with whenever a DNS query (gslb.repro.lab) reaches its ADNS service.

4. You will see under **ANSWER SECTION** the IP Address of one of the HTTP Virtual Servers from either **SITE 01** or **SITE 02**. Click **Close**.

```
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id: 21693
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; gslb.repro.lab. IN A

;; ANSWER SECTION:
gslb.repro.lab. 5 IN A 10.91.50.50
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:

;; Query time: 0 msec
;; SERVER: 10.91.68.146
;; WHEN: Mon Jan 22 11:43:50 2024
;; MSG SIZE rcvd: 48
Done
>
```

Close

5. Re-do the test.



← Test GSLB

Domain Name\*  
 gslb.repro.lab

ADNS Service  DNS Server

ADNS Service\*  
 adns\_site01\_america\_udp Add

DNS Record Type  
 A ⓘ

Test Close

6. You will see under **ANSWER SECTION** the IP Address of the second HTTP Virtual Server. It proves the GSLB ACTIVE-ACTIVE is working fine. Click **Close**.

```

Test GSLB
-->HEADER<< opcode: QUERY, rcode: NOERROR, id: 4853
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; gslb.repro.lab. IN A

;; ANSWER SECTION:
gslb.repro.lab. 5 IN A 10.91.69.149
;; AUTHORITY SECTION:

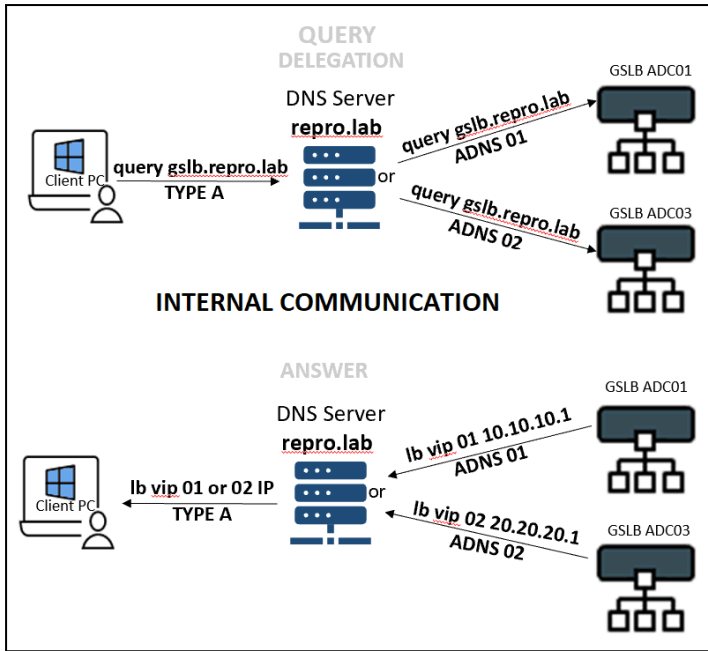
;; ADDITIONAL SECTION:

;; Query time: 0 msec
;; SERVER: 10.91.68.146
;; WHEN: Mon Jan 22 11:50:36 2024
;; MSG SIZE rcvd: 48
Done
>
  
```

Close

### Other Methods to Test:

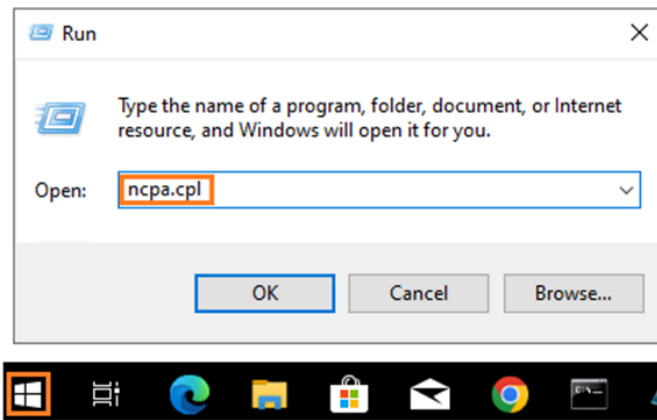
- Delegate a Subdomain to NetScaler
- o To enable a DNS server to respond to inquiries about any domain, it needs to establish connections to every zone within the namespace. These connections are formed through a process called delegation. Delegation involves the creation of a record in the parent zone (in this scenario, "**repro.lab**" on a **DNS Server**) that specifies a name server as the authority for the zone at the subsequent hierarchy level (in this instance, "**gslb.repro.lab**" on **NetScaler GSLB ADC01** and **ADC03**).



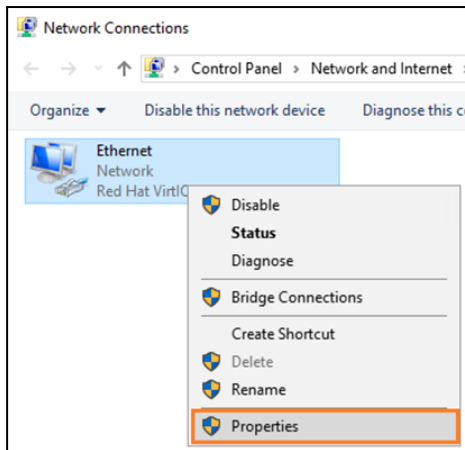
Article: [How to Delegate Zones](#)

By changing the DNS of a client machine (LDNS) to one of the NetScaler's ADNS IPs. We will cover this in the next steps.

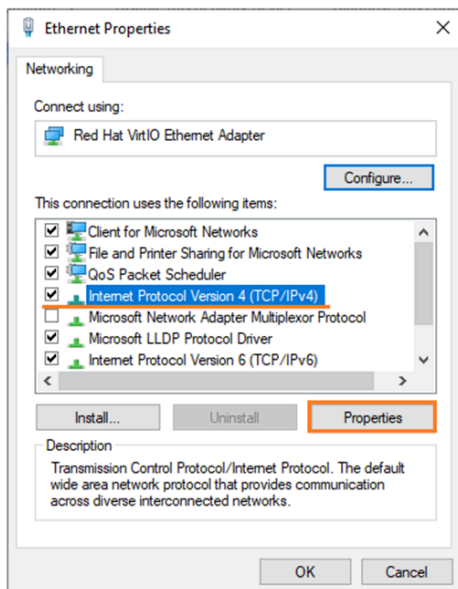
1. From a Windows JumpBox VM, click **on the start menu > type Run** and then type **ncpa.cpl**.



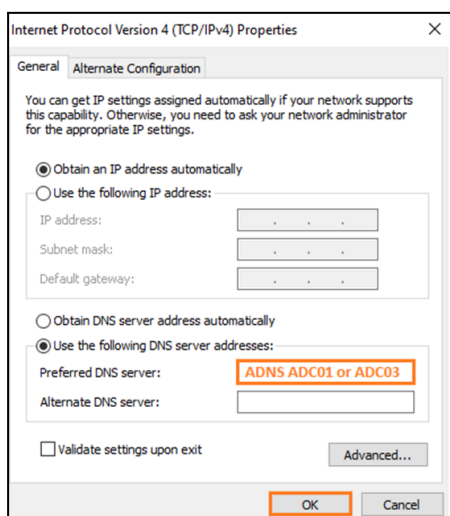
2. Right-click the **Ethernet** connection and choose **Properties**.



3. On the Ethernet Properties window, highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



4. Set either your ADC01 or ADC03 ADNS IP as Preferred DNS Server and click ok and close.



- Open the **cmd** (**Start > Run > cmd**), and ping **“gslb.repro.lab”** multiple times, you will notice the answers received will come with different IPs, from both sites.

```
C:\Users\admin>ping gslb.repro.lab

Pinging gslb.repro.lab [10.91.69.149] with 32 bytes of data:
Reply from 10.91.69.149: bytes=32 time<1ms TTL=254
Reply from 10.91.69.149: bytes=32 time<1ms TTL=254
Reply from 10.91.69.149: bytes=32 time<1ms TTL=254
Reply from 10.91.69.149: bytes=32 time<1ms TTL=254

Ping statistics for 10.91.69.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin>ping gslb.repro.lab

Pinging gslb.repro.lab [10.91.50.50] with 32 bytes of data:
Reply from 10.91.50.50: bytes=32 time<1ms TTL=254
Reply from 10.91.50.50: bytes=32 time<1ms TTL=254
Reply from 10.91.50.50: bytes=32 time<1ms TTL=254
Reply from 10.91.50.50: bytes=32 time<1ms TTL=254
```

- You can test with **nslookup** tool as well. Enter **nslookup gslb.repro.lab**.

```
C:\Users\admin>nslookup gslb.repro.lab
Server: UnKnown
Address: 10.X.X.X

Name:    gslb.repro.lab
Address: 10.91.50.50

C:\Users\admin>nslookup gslb.repro.lab
Server: UnKnown
Address: 10.91.68.200

Name:    gslb.repro.lab
Address: 10.91.69.149
```

Below you can double-check the IPs of the LB VIPs received above.

<input type="checkbox"/>	SERVICE NAME	IP ADDRESS	PORT	PROTOCOL	STATE	EFFECTIVE STATE
<input type="checkbox"/>	gslb_http_colors_europe	10.91.50.50	80	HTTP	● UP	● UP
<input type="checkbox"/>	gslb_http_colors_america	10.91.69.149	80	HTTP	● UP	● UP

- Open the browser and type **“gslb.repro.lab”**. The content of the LB VIP will appear.



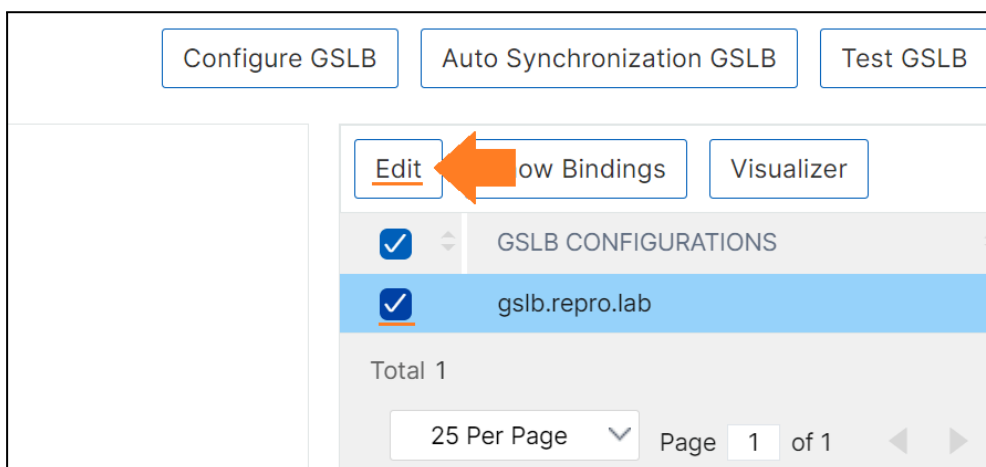
**Notes:**

1. If you open the ADC CLI of the ADNS you set on Windows and type "nstcpdump.sh port 53", you will see the ADC answers.
2. If either ADC01/LB VIP or ADC03/LBVIP goes down, the other site will continue working and serving applications and DNS responses to end-users.
3. Once you have your own DNS server (Windows Server), a sub-domain zone can be delegated to the ADC and it will remove the need to set the internal ADNS of the ADC in the Windows' interfaces.

## Changing Deployment Type to ACTIVE-PASSIVE

To change the deployment from **ACTIVE-ACTIVE** to **ACTIVE-PASSIVE**, follow the below steps. Usually, a passive site is called a disaster recovery site – DR).

1. You can double-check the deployment type by navigating to **Traffic Management > GSLB > Dashboard** and on the top right corner, select the domain created before **gslb.repro.lab** and click **Edit**.

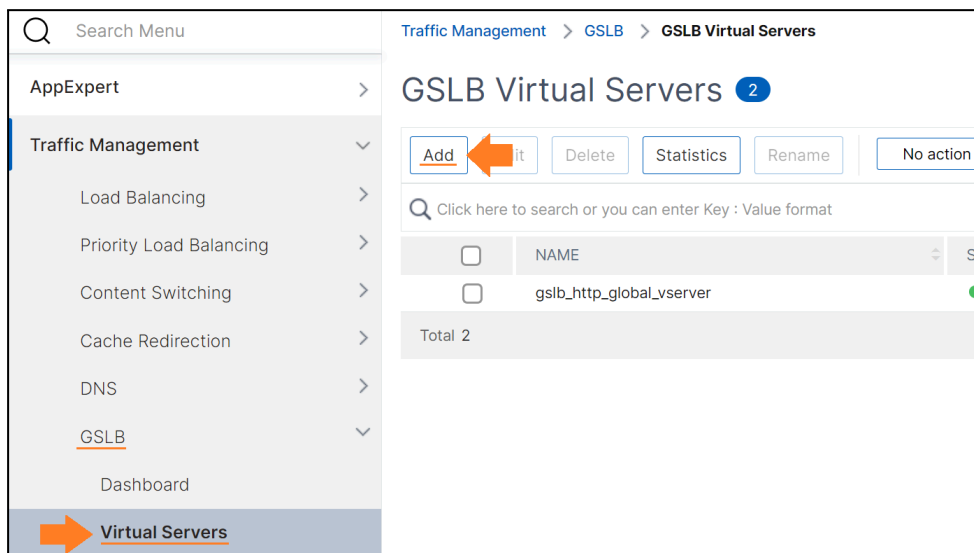


2. Top right corner, you will find the deployment type for that domain, in this case, **Active-Active**.




To change it, you need to create a new GSLB Virtual Server with the LB HTTP VIP that belongs to your Passive (DR) site. For context, **ADC01 – SITE 01 AMERICA** will be the **ACTIVE**, and **ADC03 – SITE 02 EUROPE PASSIVE**.

- On the ADC01 – SITE 01, navigate to **GSLB > Virtual Servers** and click **Add**.



- Give it the name **gslb\_passive\_DR\_site\_europe** and click **OK**.

**Basic Settings**

Name\*  
 

DNS Record Type\*

Service Type\*

Consider Effective State

Toggle Order

Enable after Creating

Order Threshold

AppFlow Logging

When this Virtual Server is DOWN  
 Do not send any service's IP address in response (EDR)

When this Virtual Server is UP  
 Send all "active" service IPs in response (MIR)

EDNS Client Subnet  
 Respond with ECS option in the response for a DNS query with ECS  
 Validate ECS address is a private or unroutable address


Comments

5. Click **No GSLB Virtual Server to GSLB Service Binding**.

**Basic Settings**

Name	<b>gslb_passive_DR_site_europe</b>	AppFlow Logging	<b>DISABLED</b>
DNS Record Type	<b>A</b>	EDR	<b>DISABLED</b>
Toggle Order	<b>ASCENDING</b>	MIR	<b>DISABLED</b>
Order Threshold	<b>0</b>	ECS	<b>DISABLED</b>
Service Type	<b>HTTP</b>	ECS Address Validation	<b>DISABLED</b>
Consider Effective State	<b>NONE</b>		
State	<b>● DOWN</b>		

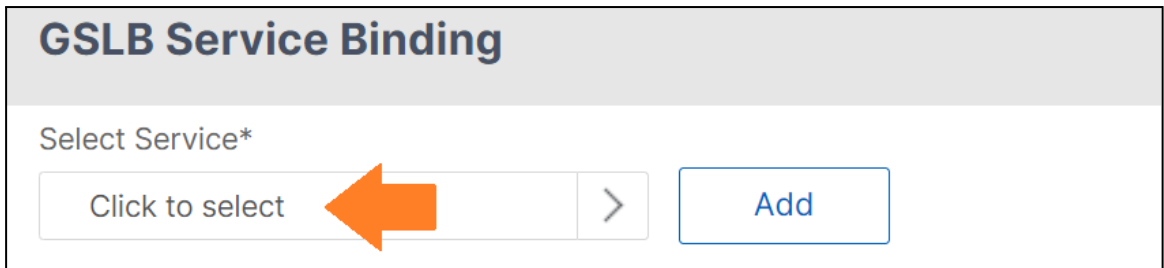
**GSLB Services and GSLB Service Group Binding**

**No** GSLB Virtual Server to GSLB Service Binding 

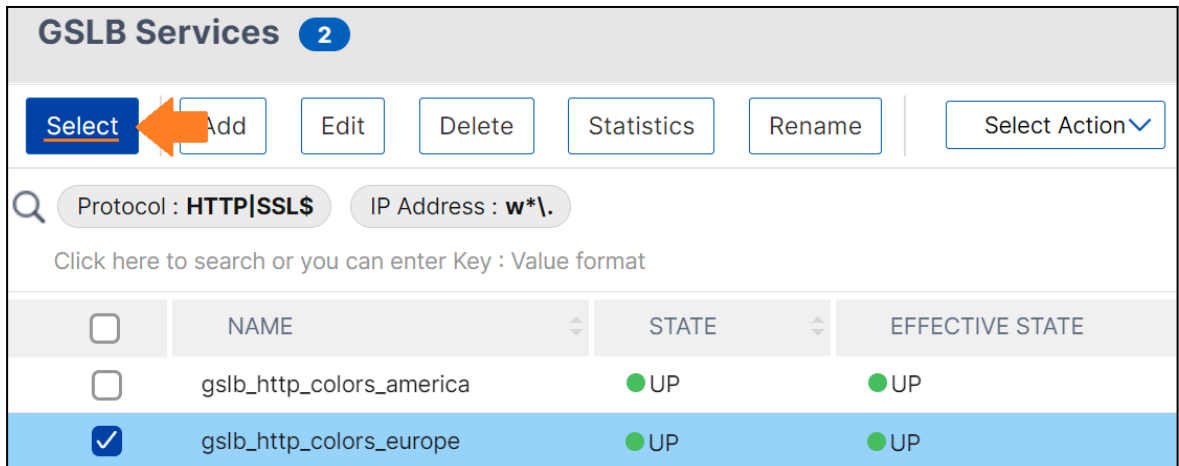
**No** GSLB Virtual Server to GSLB Service Group Binding

6. Click **Click to select**.

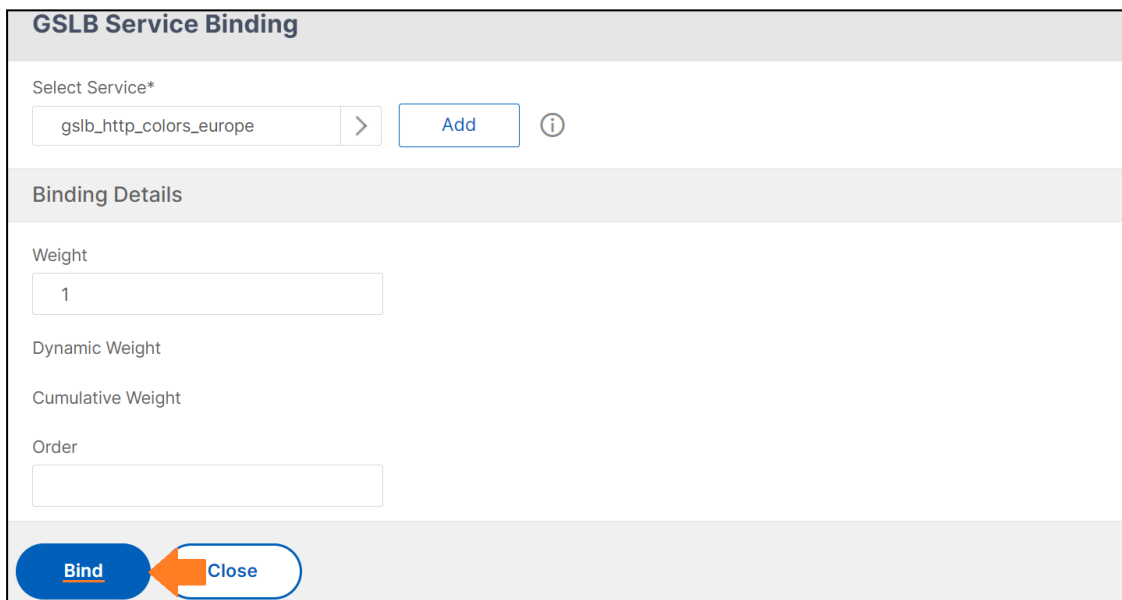




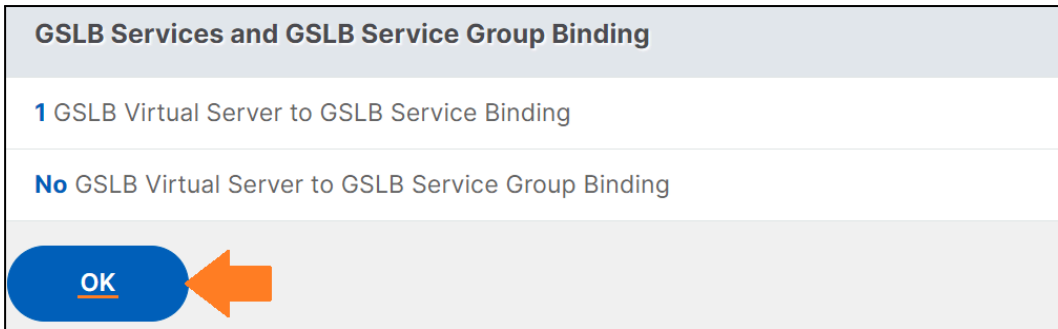
7. Select your **gslb\_http\_colors\_europe** and click Select. Site Europe (SITE 02) will act as Passive.



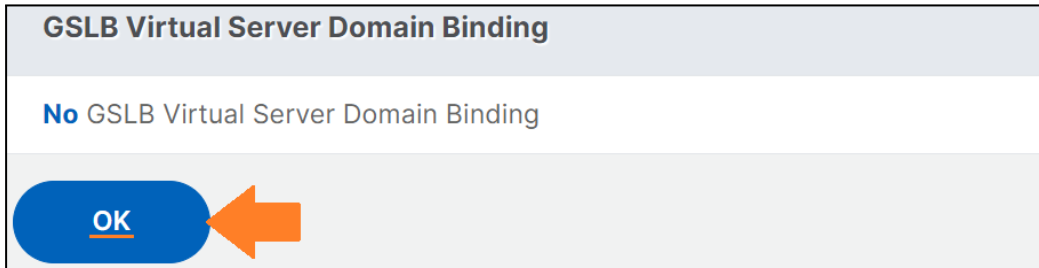
8. Click **Bind**.



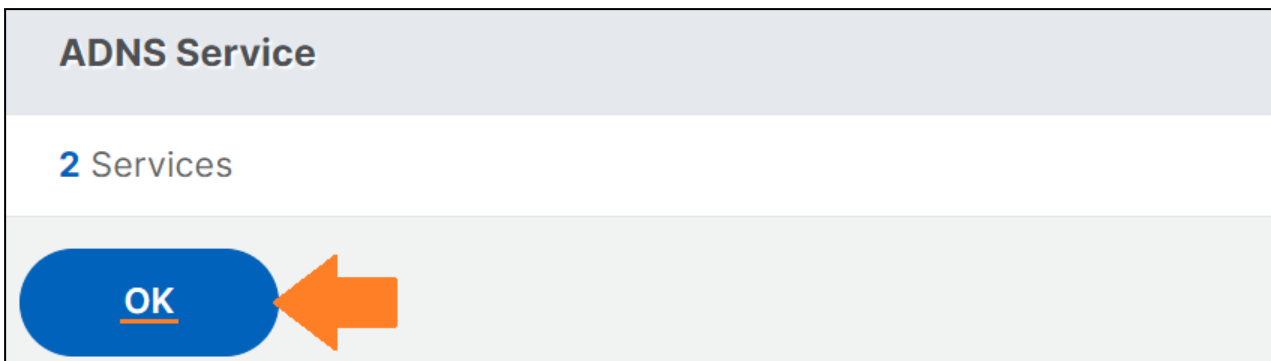
9. Click **OK**.



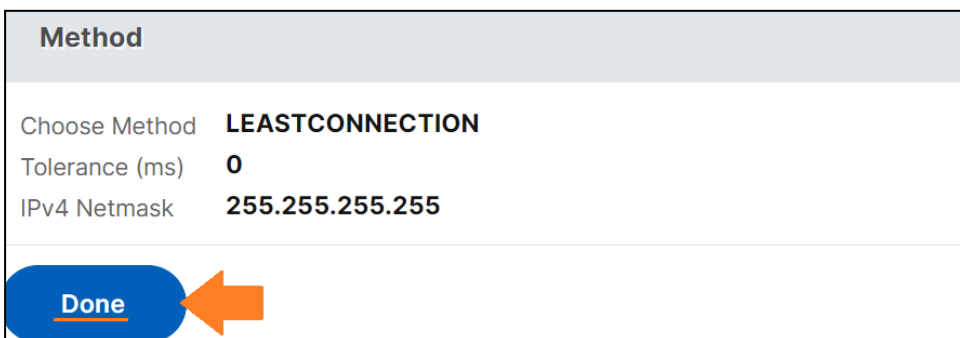
10. Click **OK**. There is no need for a domain when configuring the backup virtual server.



11. ADNSs are bound automatically. Click **OK**.



12. Click **Done**.



The `gslb_passive_DR_site_europe` is set.

### GSLB Virtual Servers

<input type="checkbox"/>	NAME	STATE	PROTOCOL
<input type="checkbox"/>	gslb_http_global_vserver	● UP	HTTP
<input type="checkbox"/>	gslb_passive_DR_site_europe	● UP	HTTP

13. Select the **gslb\_http\_global\_vserver** and click **Edit** to add the passive Vserver as a Backup Vserver.

### GSLB Virtual Servers 3

<input type="checkbox"/>	NAME	STATE
<input checked="" type="checkbox"/>	gslb_http_global_vserver	● UP

14. Click over **"2 GSLB Virtual Server..."** to **REMOVE** the LB VIP of the SITE 02 Europe.

#### Basic Settings

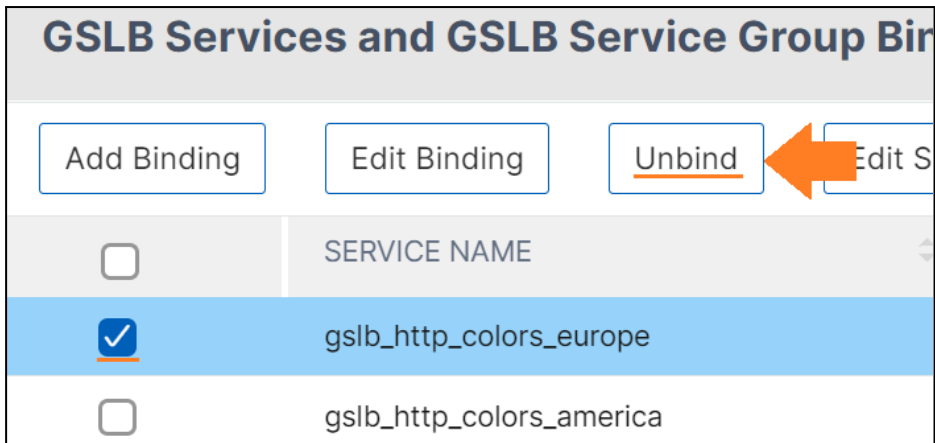
Name	<b>gslb_http_global_vserver</b>	AppFlow Logging	<b>DISABLED</b>
DNS Record Type	<b>A</b>	EDR	<b>DISABLED</b>
Toggle Order	<b>ASCENDING</b>	MIR	<b>DISABLED</b>
Order Threshold	<b>0</b>	ECS	<b>DISABLED</b>
Service Type	<b>HTTP</b>	ECS Address Validation	<b>DISABLED</b>
Consider Effective State	<b>NONE</b>		
State	● <b>UP</b>		

#### GSLB Services and GSLB Service Group Binding

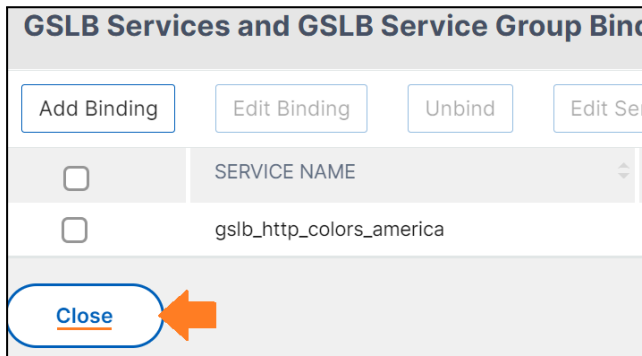
[2 GSLB Virtual Server to GSLB Service Bindings](#)

[No GSLB Virtual Server to GSLB Service Group Binding](#)

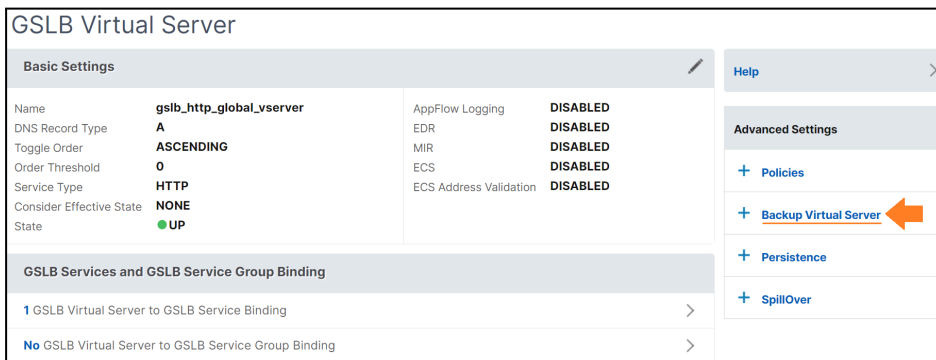
15. Select the "gslb\_http\_colors\_europe", click Unbind, and Yes.



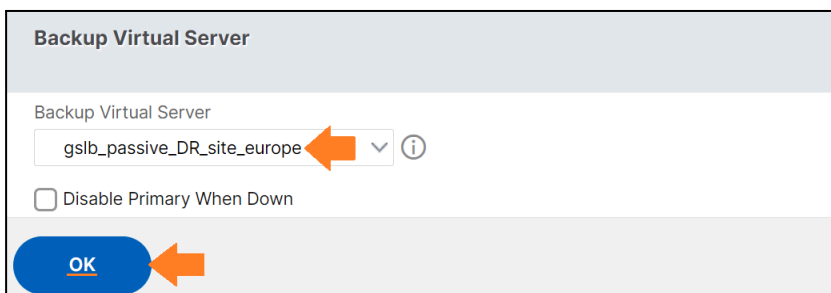
16. Ensure the **gslb\_http\_colors\_america** is the only one bound. This means that only this service will be provided to end-users when a type A query reaches either **SITE 01** or **SITE 02**. Click **Close**.

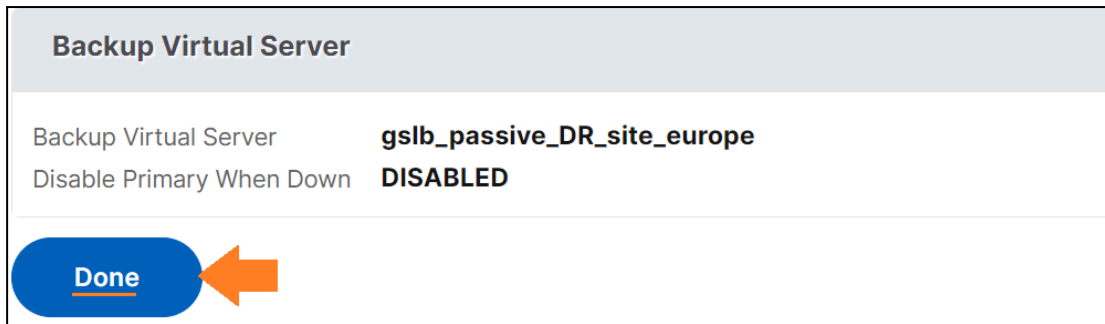


17. Right side, under **Advanced Settings** click **Backup Virtual Server**.

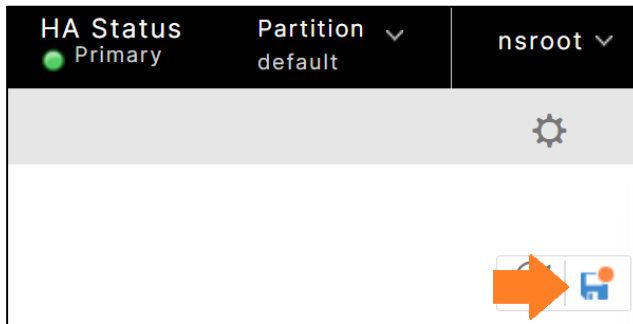


18. In server "**gslb\_passive\_DR\_site\_europe**", click **OK**, and **Done**.

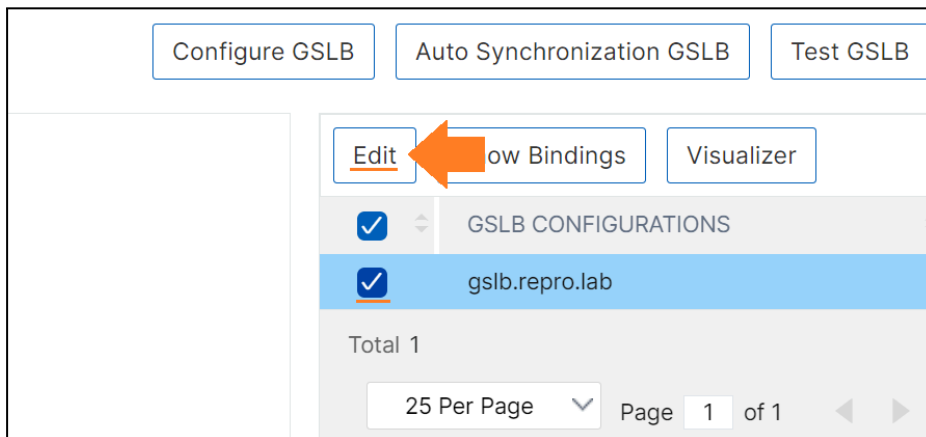




19. Save the configuration.



20. Check again the deployment type, navigate to **Traffic Management > GSLB > Dashboard**, and on the top right corner, select the domain created "**gslb.repro.lab**" and click **Edit**.



21. Top right corner, you will find the deployment type for that domain, now, showing **ACTIVE-PASSIVE**.

Steps		
1	<u>Deployment: Active-Passive</u>	✓
	↓	
2	GSLB Sites	✓
	↓	
3	GSLB Services	✓
	↓	
4	Backup GSLB Virtual Server	✓
	↓	
5	GSLB Virtual Server	✓

**NOTE:** The **ACTIVE-PASSIVE** is in place now. If the **ADC01** or **AMERICA HTTP VIP** fails, the traffic will be served from the **ADC03 – EUROPE HTTP VIP**.

22. SYNC the configuration to the **ADC03 – SITE 02**. Navigate to **GSLB > Dashboard**. You will see the overall GSLB configuration/summary. Top right corner, click **Auto Synchronization GSLB**.

The screenshot shows the 'GSLB Dashboard' interface. At the top right, there are three buttons: 'Configure GSLB', 'Auto Synchronization GSLB' (highlighted with an orange arrow), and 'Test GSLB'. Below these are sections for 'GSLB Settings' (with links for 'Change GSLB Settings' and 'View GSLB Configuration') and 'GSLB Synchronization' (with links for 'View Synchronization Summary' and 'View Synchronization Status'). On the right side, there are buttons for 'Edit', 'Show Bindings', and 'Visualizer'. Below these is a table of 'GSLB CONFIGURATIONS' with one entry: 'gslb.repro.lab'. At the bottom right, there is a pagination control showing 'Total 1', '25 Per Page', and 'Page 1 of 1'.

23. Click **Run**. This will start the sync from **ADC01-Site 01** to **ADC03-Site 03**.

The screenshot shows the 'Synchronize GSLB Configuration' dialog box. It has a title bar with a back arrow and the text 'Synchronize GSLB Configuration'. Below the title, there are several options: 'Synchronization Option' with checkboxes for 'Preview', 'Debug', and 'ForceSync'; 'Save Configuration' with a checkbox; and a 'Command' input field. At the bottom, there is a checkbox for 'No Warning' which is checked. At the very bottom, there are two buttons: 'Run' (highlighted with an orange arrow) and 'Close'.

24. Confirm you see **ok** for all the processes followed by **Done**. Click **Close** and **Close** again.

```
Synchronize GSLB Configuration
Connected to Command Line Interface
> shell nsgslbautosync config -nowarn
Sync Time: Nov 8 2023 14:59:1
Retrieving local site info: ok
Retrieving all participating gslb sites info: ok
site_americas[Master]:
  Getting Config: ok
site_europe[Slave]:
  Syncing gslb static proximity database: ok
  Syncing inbuilt gslb static proximity database :ok
  Getting Config: ok
  Comparing config: ok
  Applying changes: ok
Done
>
```

25. Follow the same steps shown before to test the GSLB deployment. You will notice that **LB HTTP VIP on ADC01 - SITE 01 AMERICA** will be the one provided to ALL the requests.

---

Notes:

1. In real scenarios assuming all the DNS delegations are properly configured for both ADNSs, regardless of the deployment type (ACTIVE-ACTIVE or ACTIVE-PASSIVE), BOTH sites receive DNS queries on port 53, then if ACTIVE-ACTIVE, both VIPs will be served or if ACTIVE-PASSIVE, only the VIP hosted on the ACTIVE site will be served.
  2. If the ADC01/HTTP LB VIP goes down, the BACKUP Virtual server will be triggered, and ADC03-SITE 02 EUROPE will answer the queries with its HTTP LB VIP instead. DISABLE the GSLB service `gslb_http_colors_america` and test it again, you will see the Backup Vserver as an answer.
-



# Citrix Virtual Apps and Desktops Install

**IMPORTANT:** We will explore the basics of **Virtual Apps and Desktop** installation and configuration, focusing on efficient resource utilization. If you are interested in setting up a more robust environment, please refer to the **Citrix Academy course** and its Lab Guide.

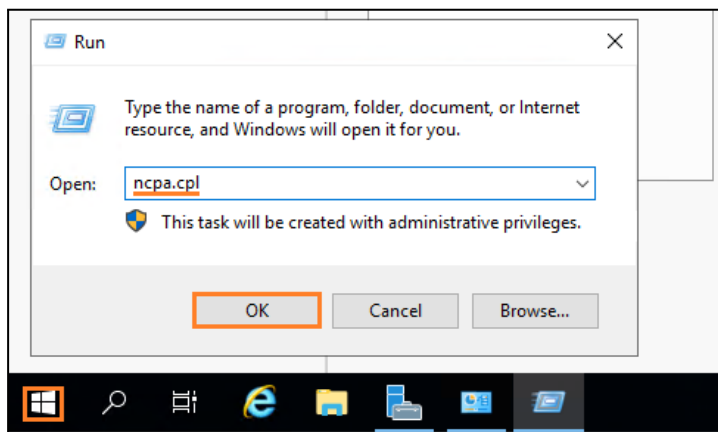
Make sure you have two Windows Server VMs and one Windows 10/11 ready to be configured.

- VM Windows Server 2019 for Citrix Delivery Controller (DDC) and StoreFront roles.
- VM Windows 10/11 VM for Citrix VDA role.
- VM Windows Server VM for Active Directory (AD) domain controller, DNS, and Certificate Authority roles.

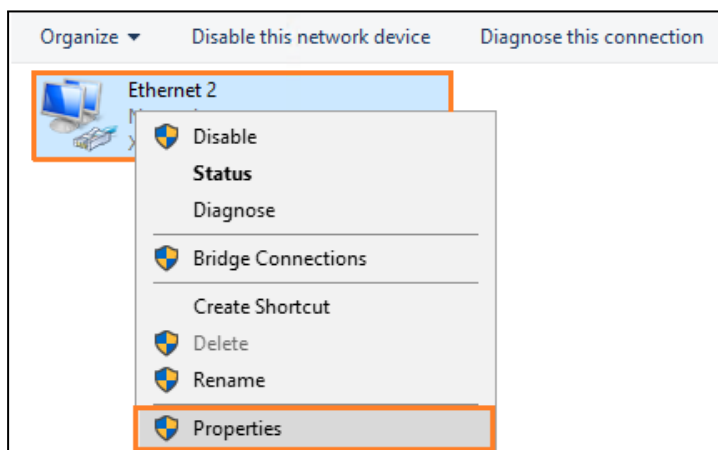
## Installing Active Directory Domain Services

### First VM: Windows Server 2019

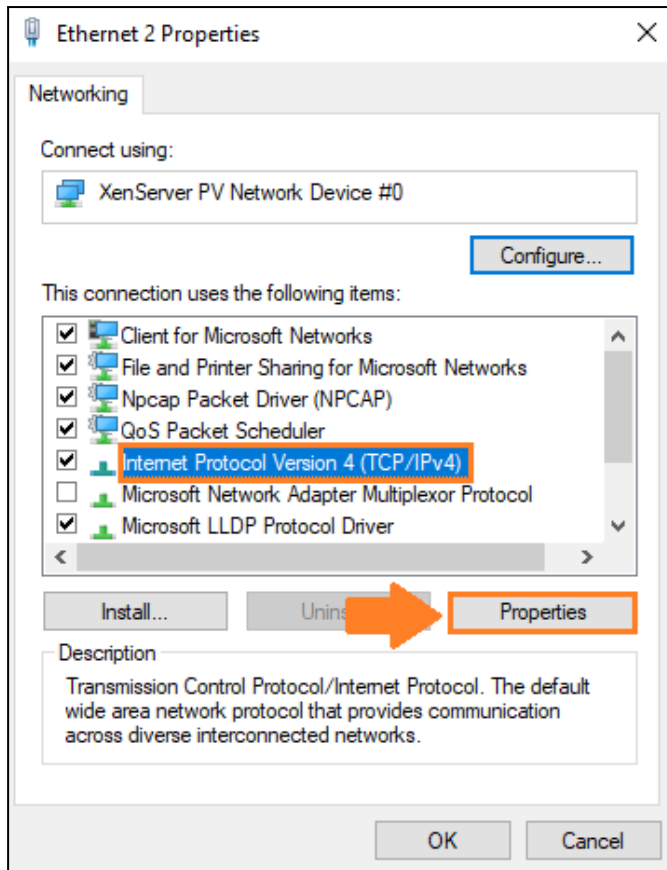
1. From the start menu, type/select **Run** and then type "**ncpa.cpl**". Click **OK**.



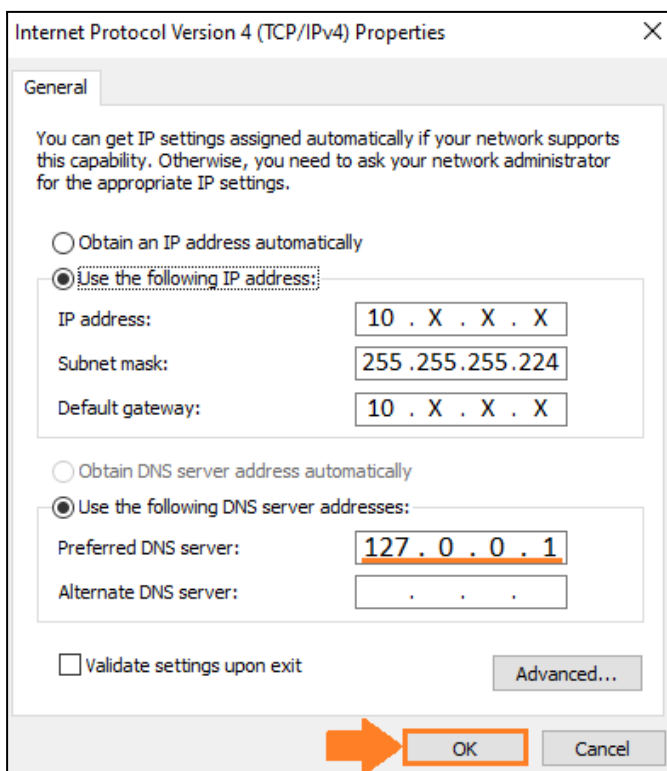
2. Right-click the **Ethernet** connection and choose **Properties**.



3. On the Ethernet Properties window, highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

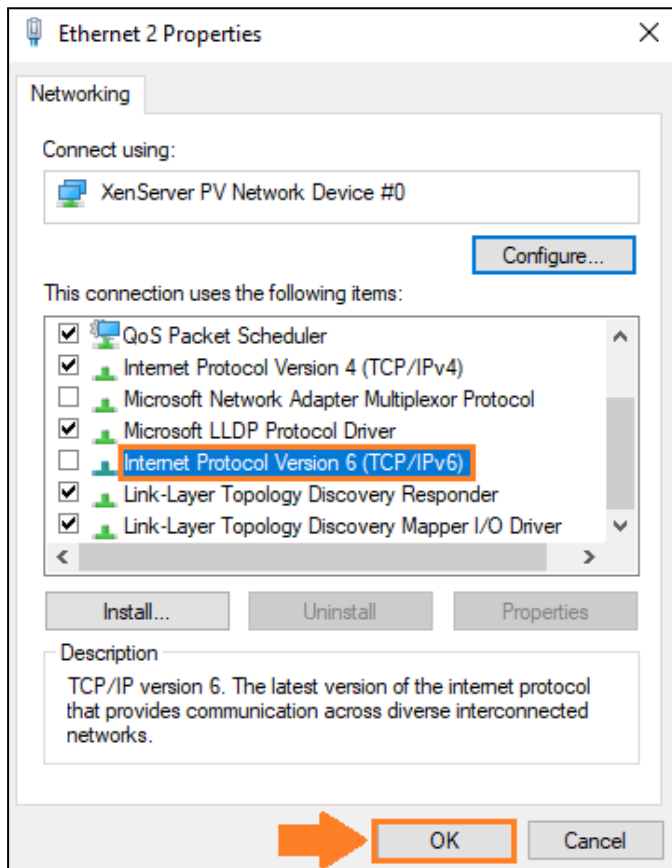


4. **Set your IP address, the subnet mask, and the default gateway** according to your network info. For DNS, set 127.0.0.1 and Click **OK**.

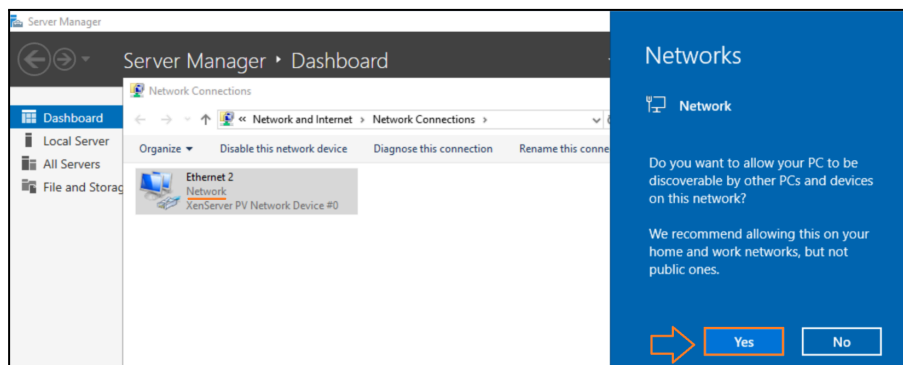


**NOTE:** As this server will act as a DNS server, we need to set 127.0.0.1 (localhost) as the DNS.

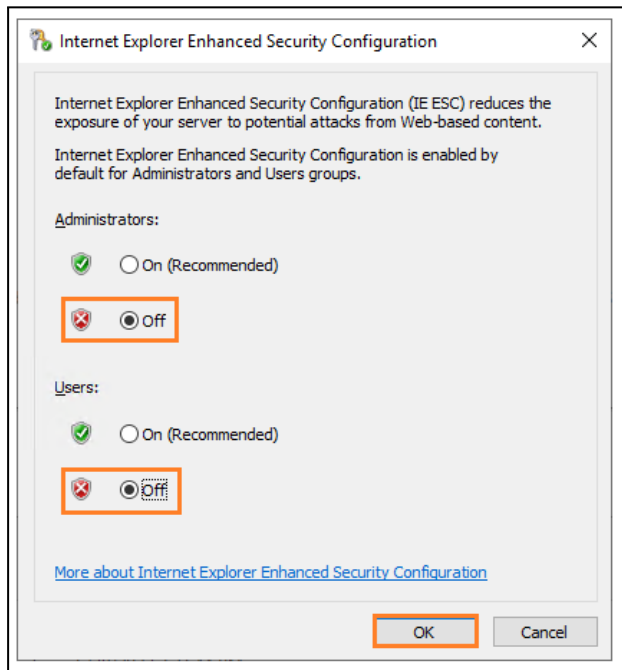
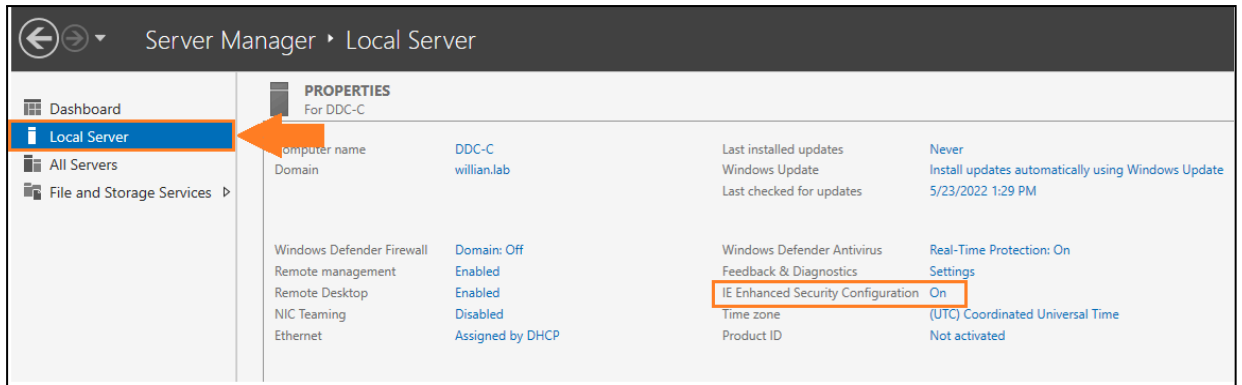
5. Uncheck **Internet Protocol Version 6** and Click **OK**.



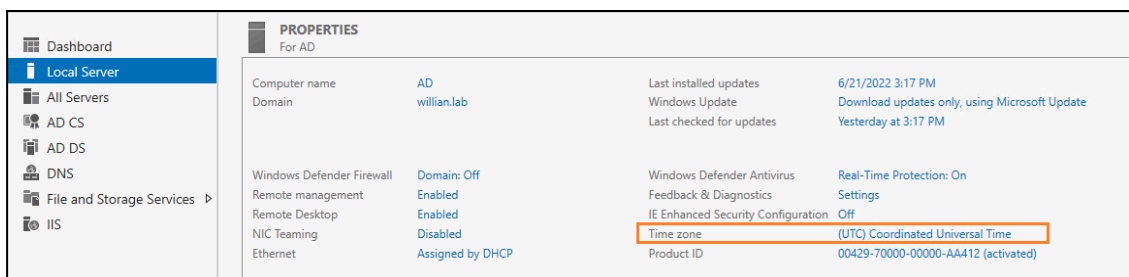
6. Select **Yes**. Your network is configured.



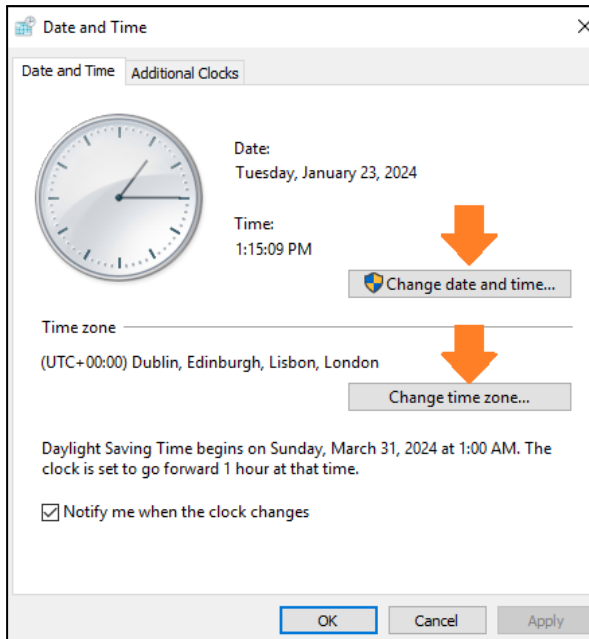
7. On the Server Manager page, click **Local Server** and set the **IE Enhanced Security Configuration** to **Off**.



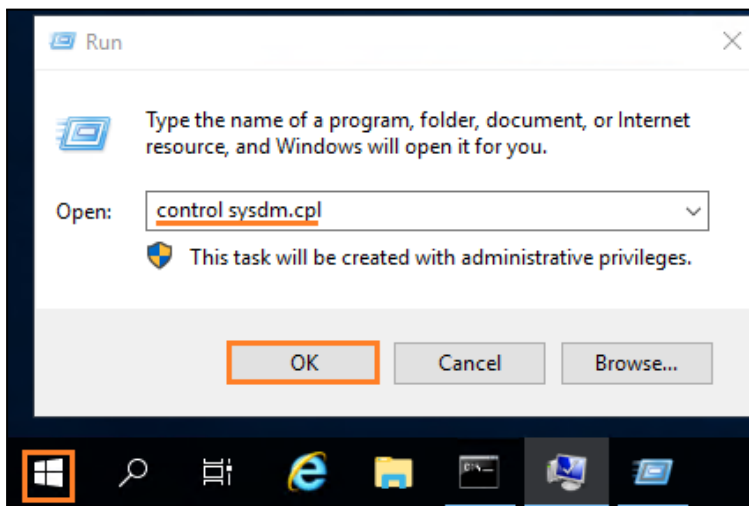
8. Click “(UTC) Coordinated Universal Time” and set your local time/time zone.



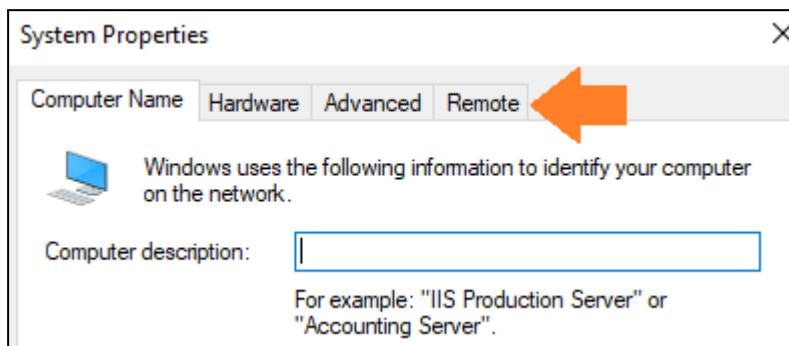
9. If the Time zone is incorrect, click the **Change time zone...** button and select the correct time zone. Once the correct time zone has been set, click the **Change date and time...** button to set the correct date and time if it is incorrect. Click **OK** once it is completed.



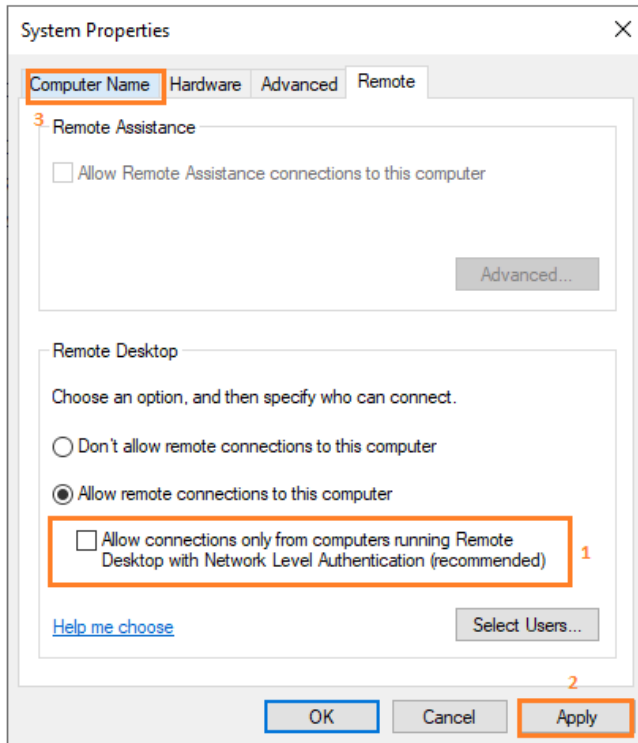
10. Navigate to **Start > Run** and enter **control sysdm.cpl**.



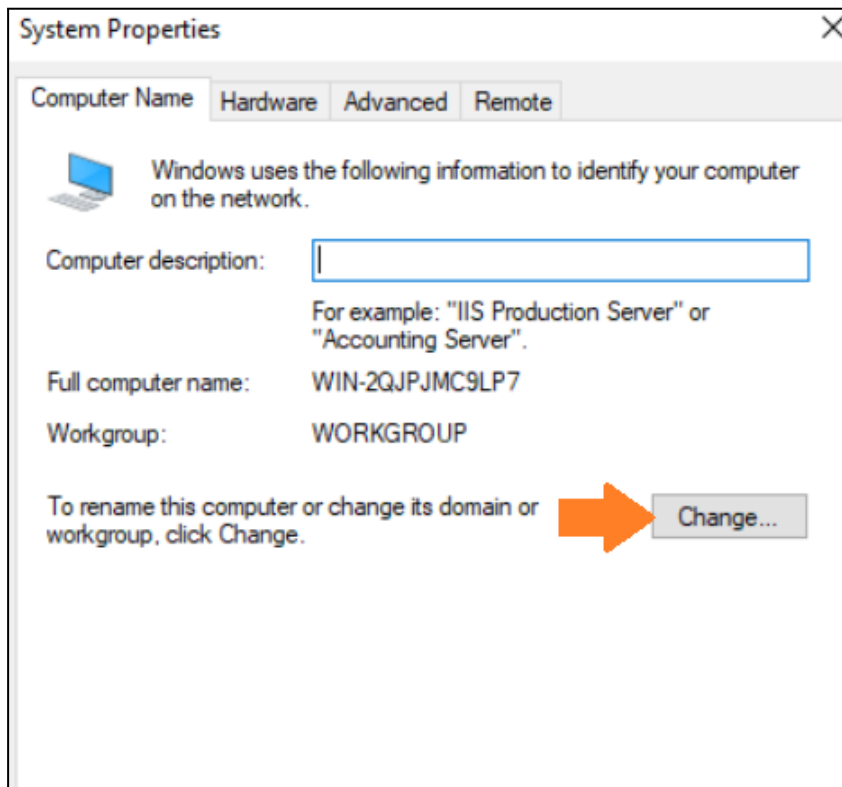
11. Click **Remote**.



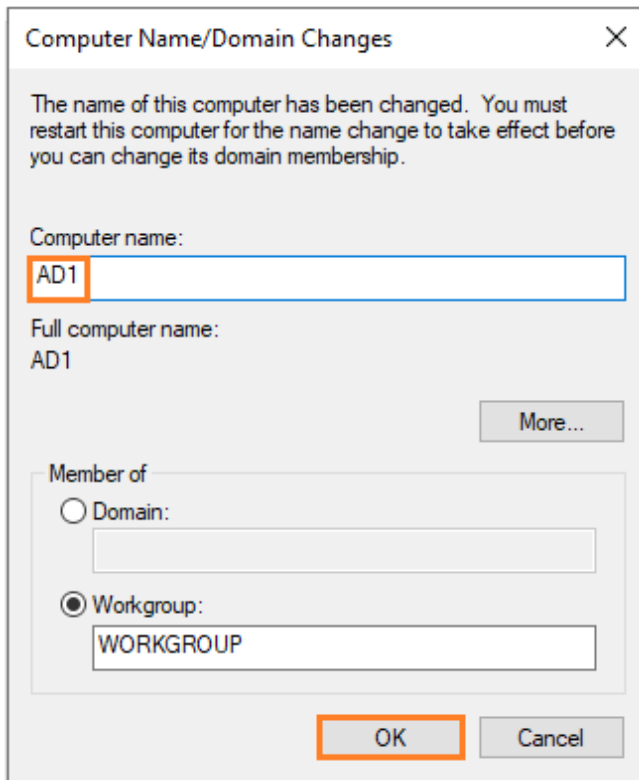
12. If **Allow connections only from computer Running Remote Desktop with NLA (recommended)** is checked, uncheck it, click **Apply**, and then click **Computer Name**.



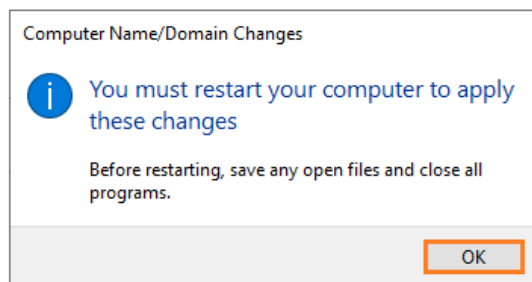
13. Click **Change**.



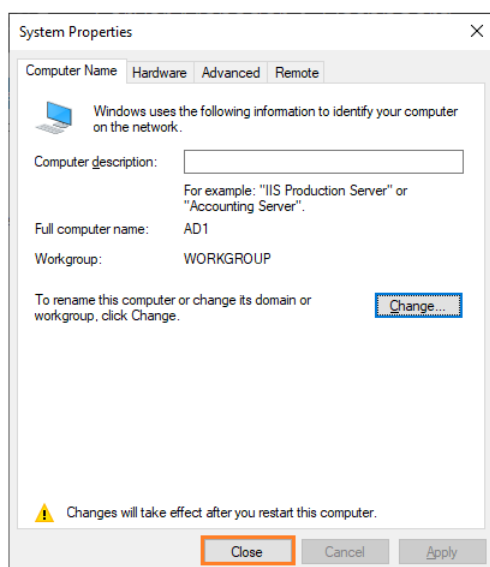
14. Change the Computer name to **AD1** and click **OK**. (You can create any other name if you wish).



15. Click **OK**.

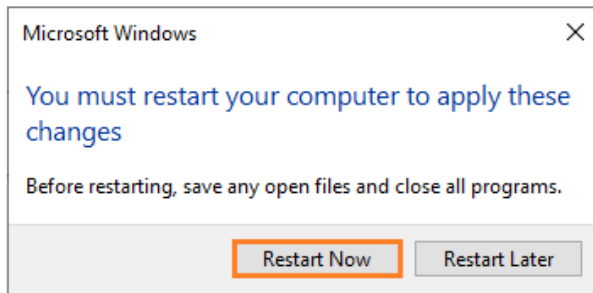


16. Click **Close**.

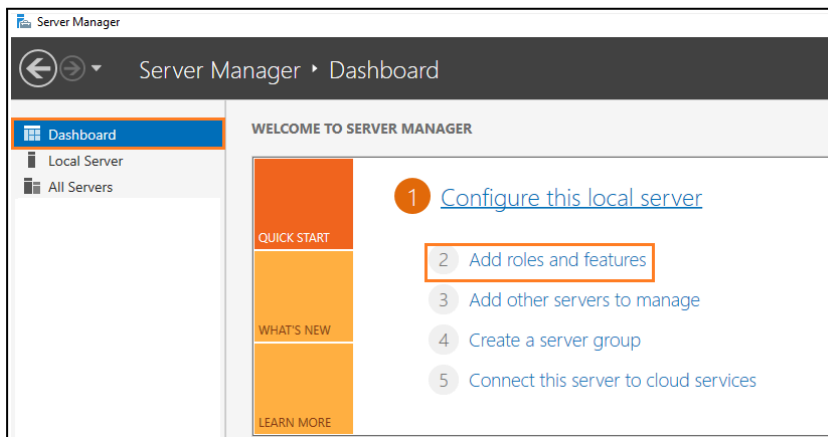




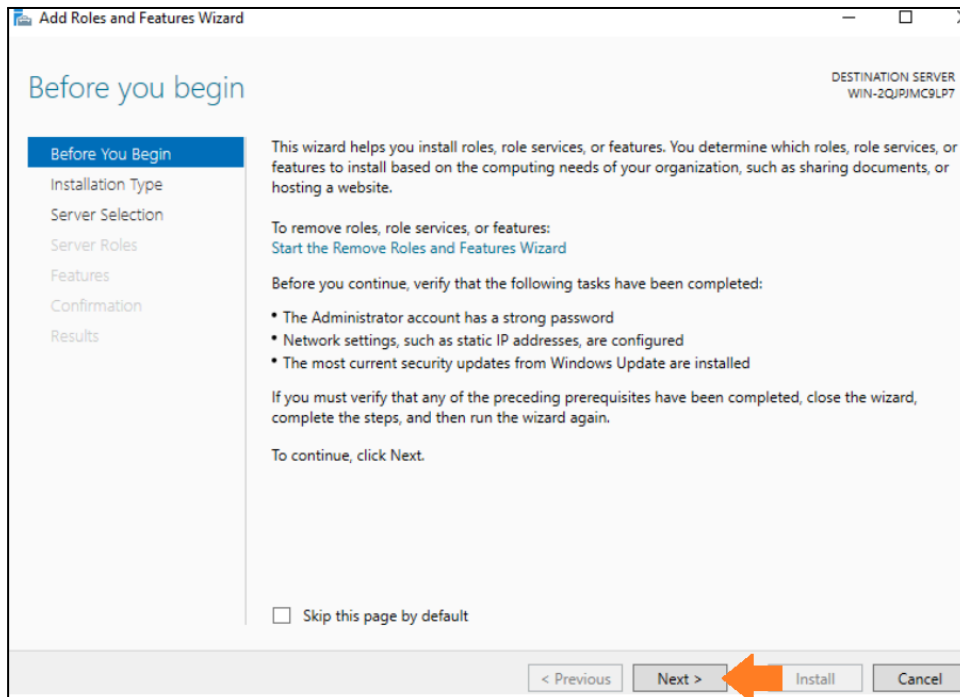
17. Click **Restart Now** and connect again to the Windows Server in a few minutes.



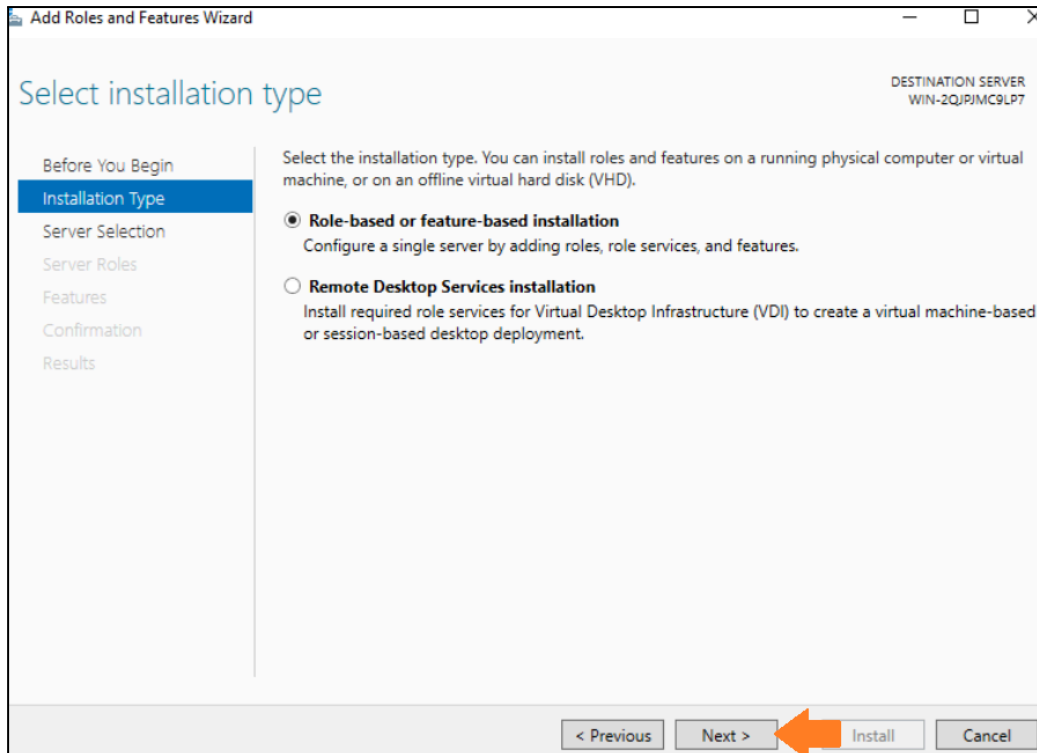
18. Open the **Server Manager** and click **Add roles and features**.



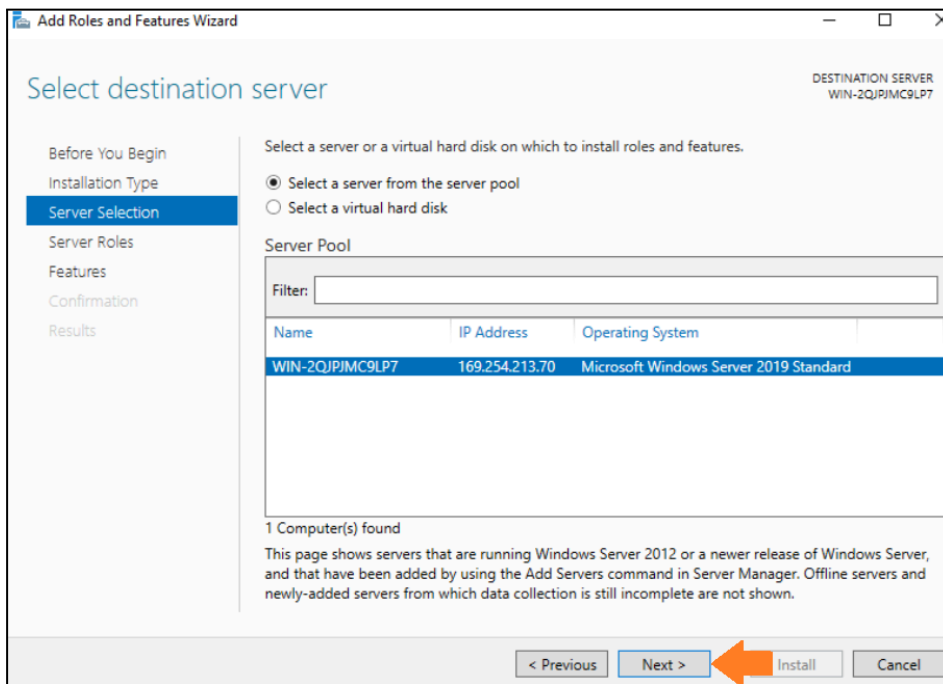
19. Read the information provided and click **Next**.



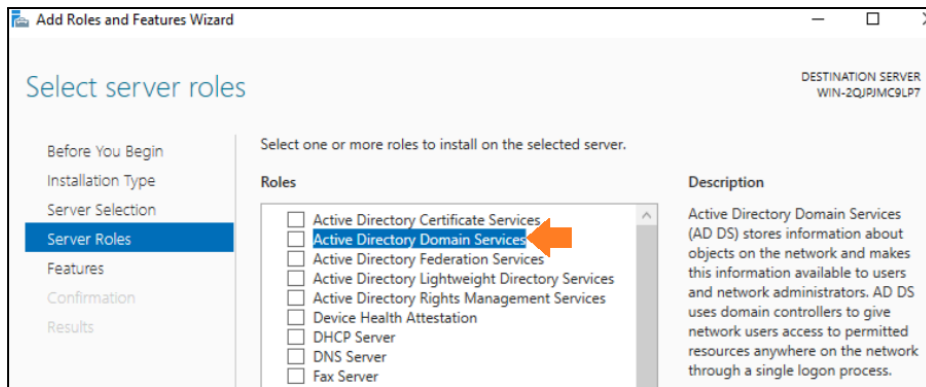
20. Keep **Role-Based or feature-based installation** ticked and click **Next**.



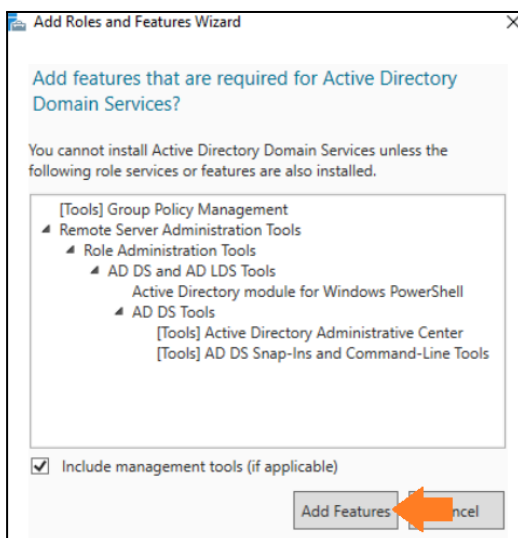
21. Keep **Select a server from the server pool** highlighted and click **Next**.



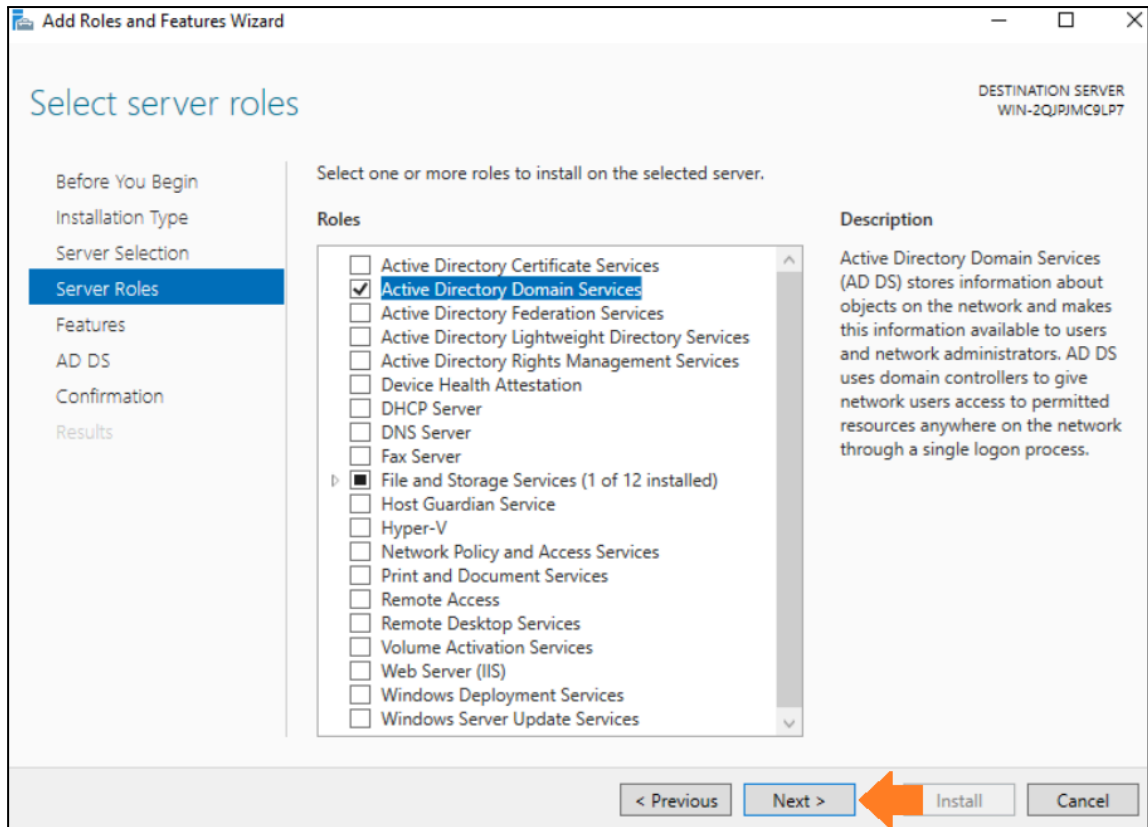
22. Tick the box next to **Active Directory Domain Services**.



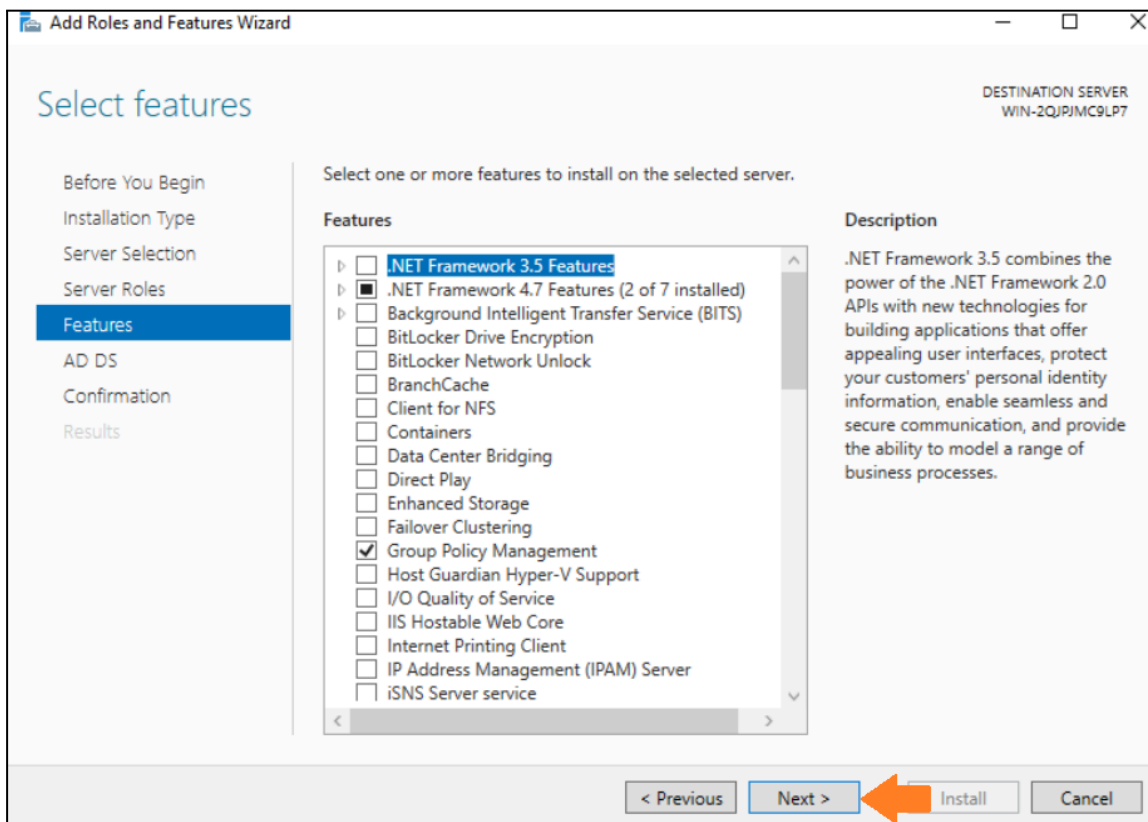
23. An additional dialog will open asking to add features required for Active Directory Domain Services. Confirm the box is ticked next to **Include management tools (if applicable)** and click the **Add Features** button.



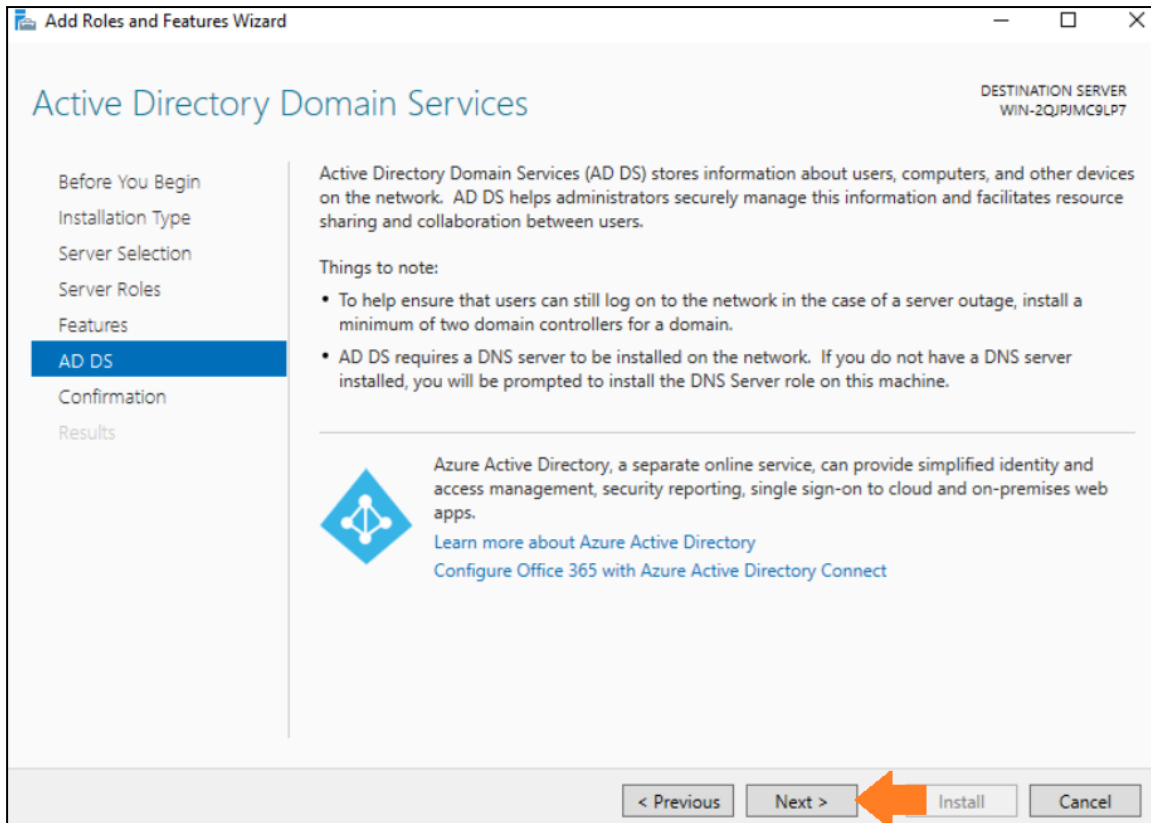
24. Active Directory Domain Services will now have a tick in the box next to it. Click **Next**.



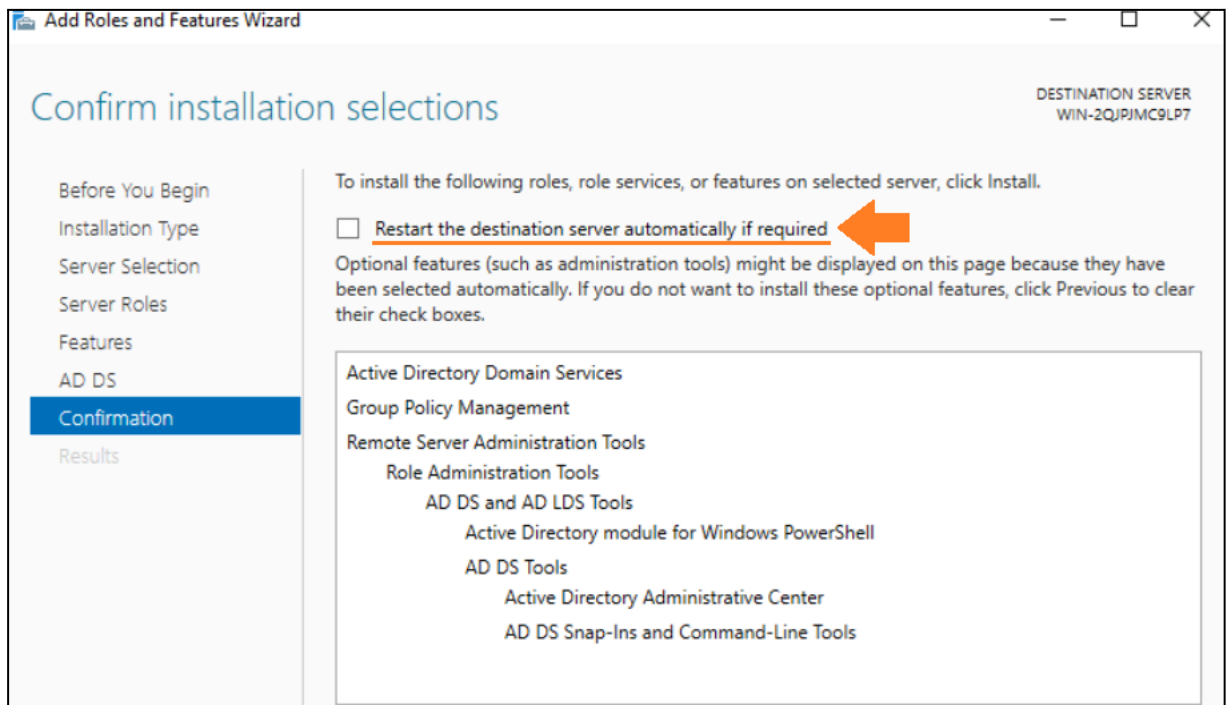
25. Click **Next** to continue.



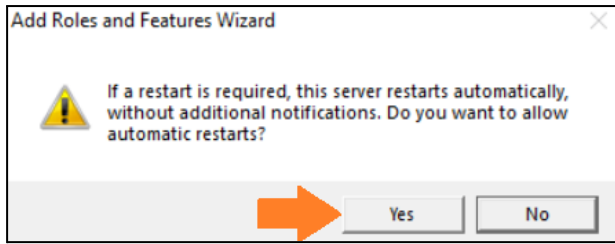
Click **Next** to continue.



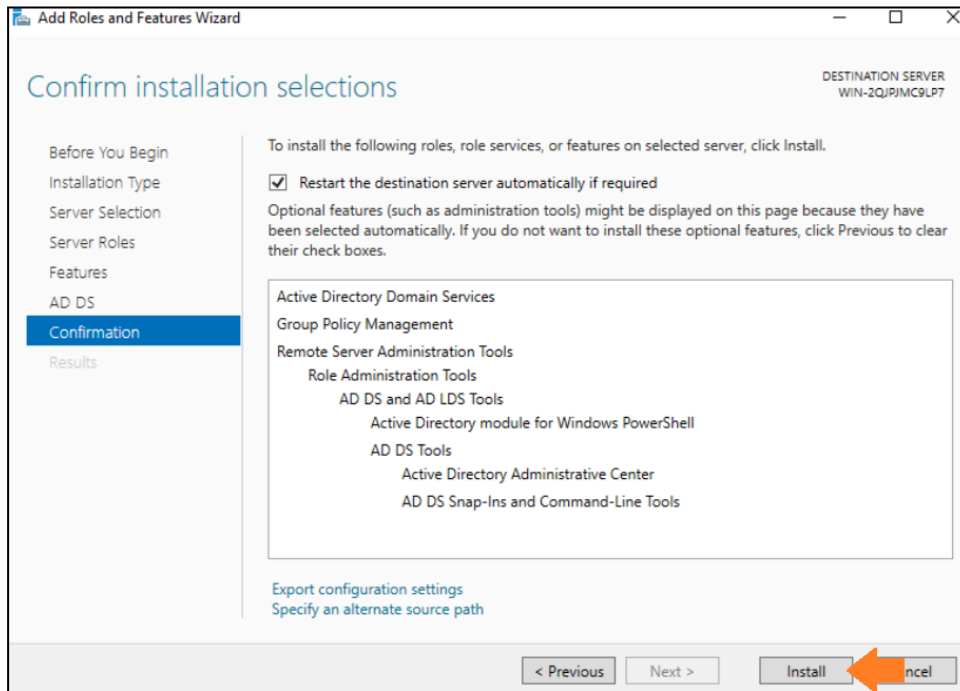
26. On the confirmation screen, tick the box next to **Restart the destination server automatically if required** then click **Yes** when asked to allow automatic restarts.



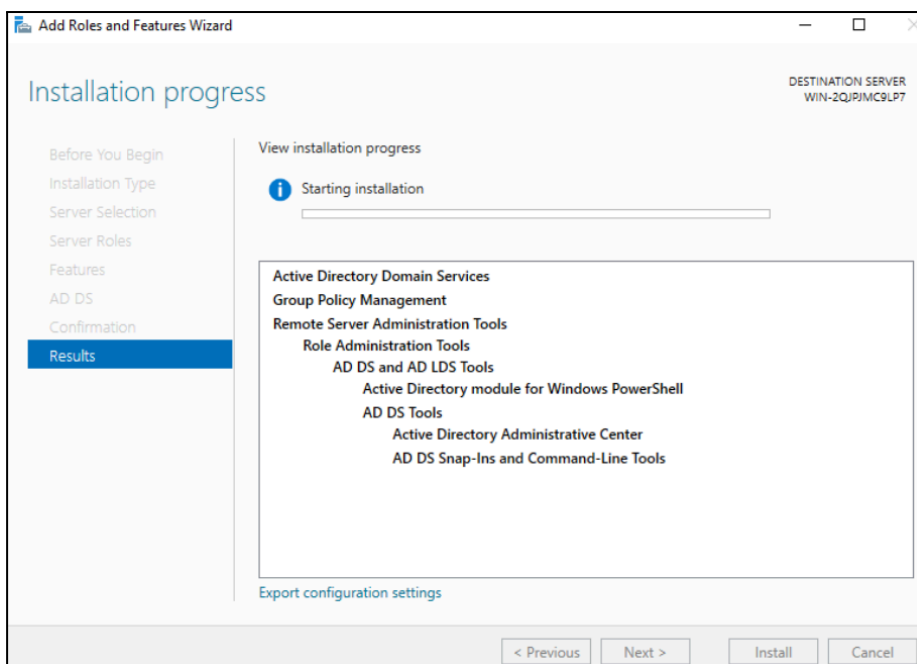
27. Click **Yes**.



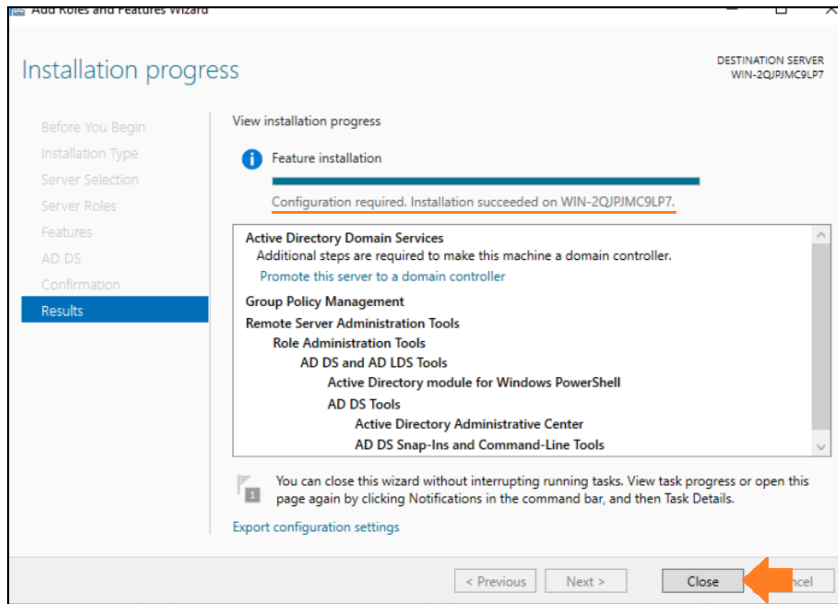
28. Click the **Install** button to begin the installation process.



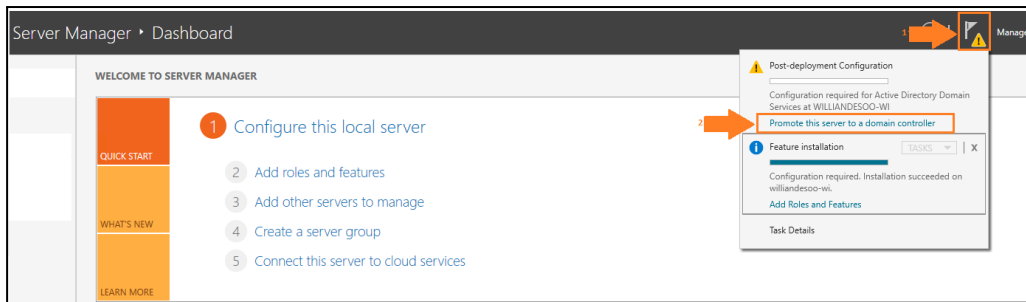
29. The installation process will take a few minutes and the server may restart.



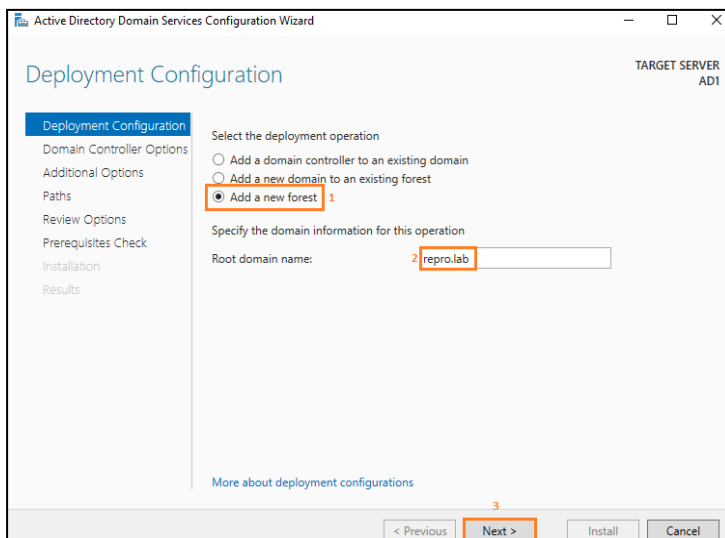
30. The installation succeeded. Click **Close** to start the configuration.



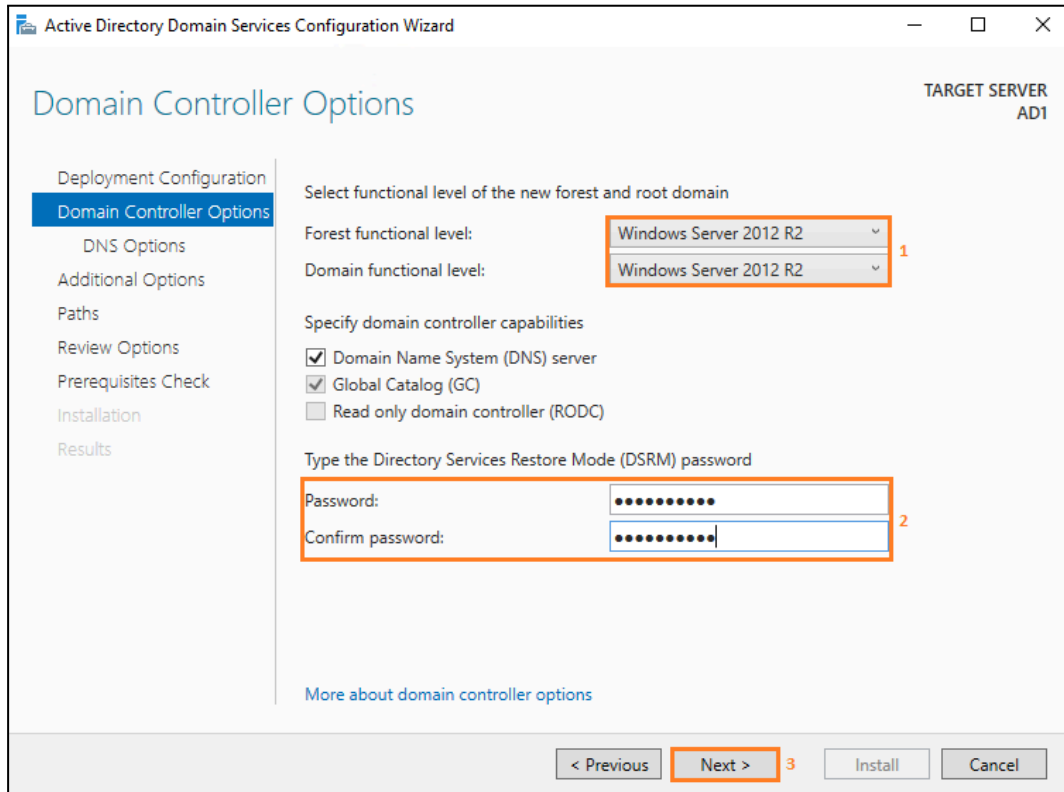
31. Click **Promote this server to a domain controller** to launch the Active Directory Domain Services Configuration Wizard.



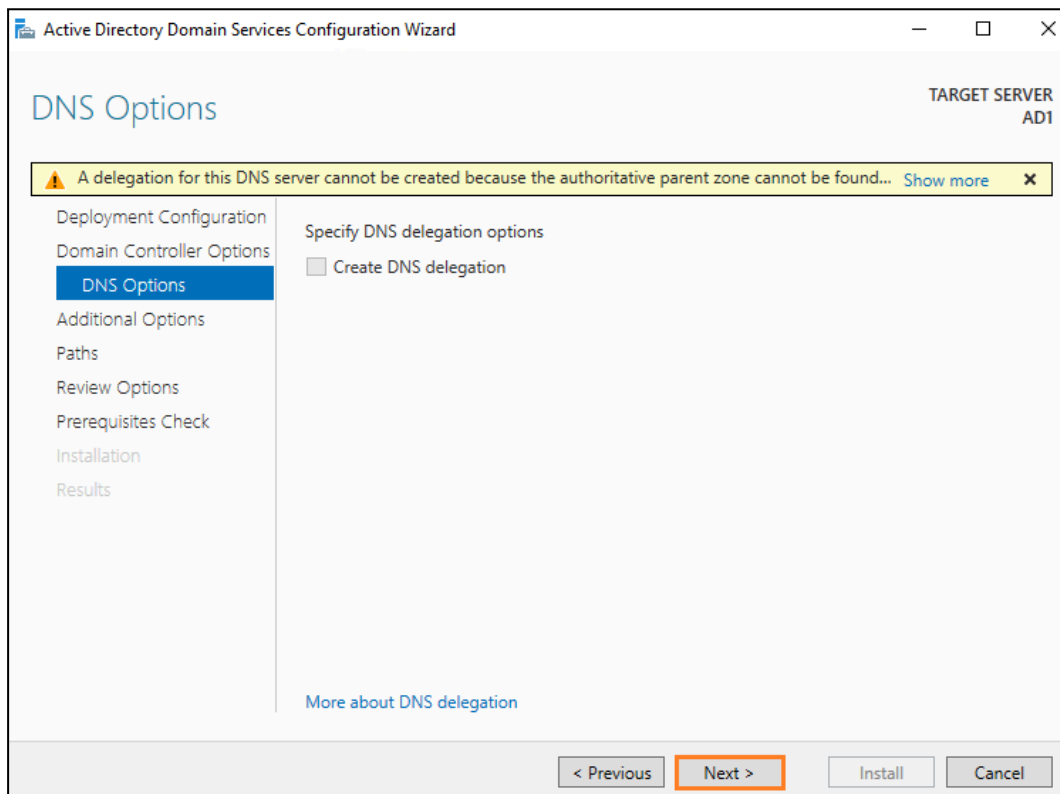
32. Select **Add a new forest** then enter **your unique forest name** (this guide will still refer to it as **repro.lab**) in the Root domain name field but feel free to create your own domain if you prefer and click **Next**.



33. Change both the Forest functional level and Domain functional level selections to Windows Server 2012 R2, type YOUR STRONG Password used for the user Administrator, confirm the password, and click Next.

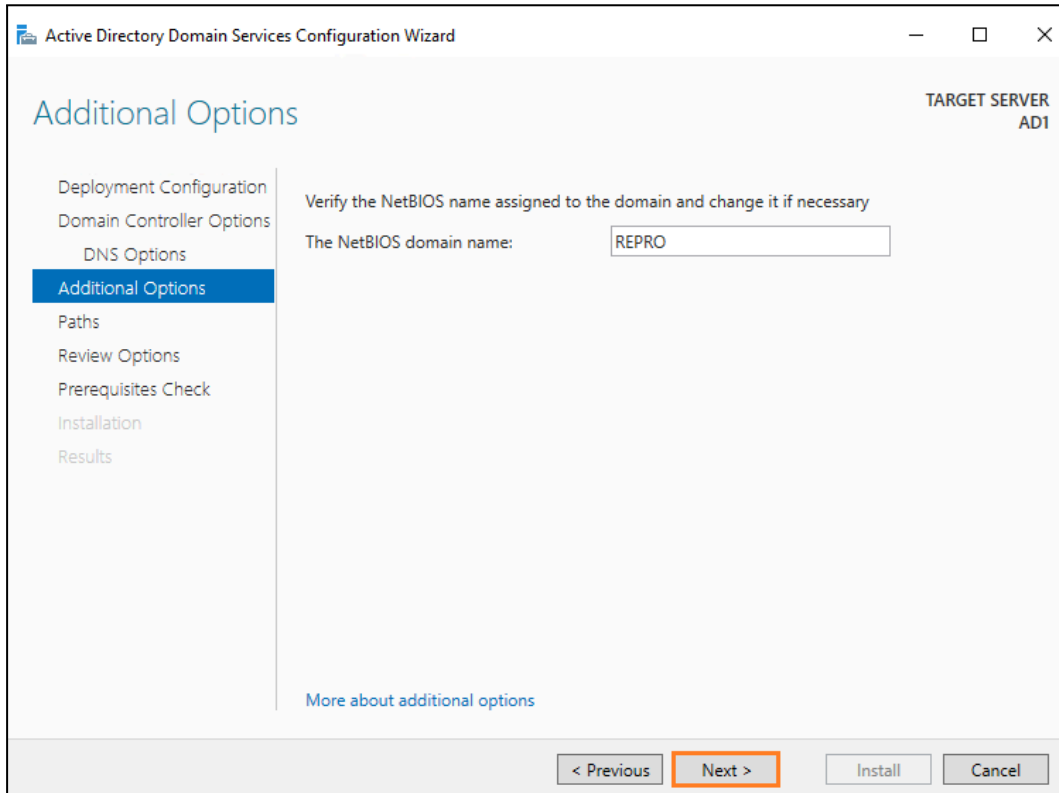


34. Click Next to continue.

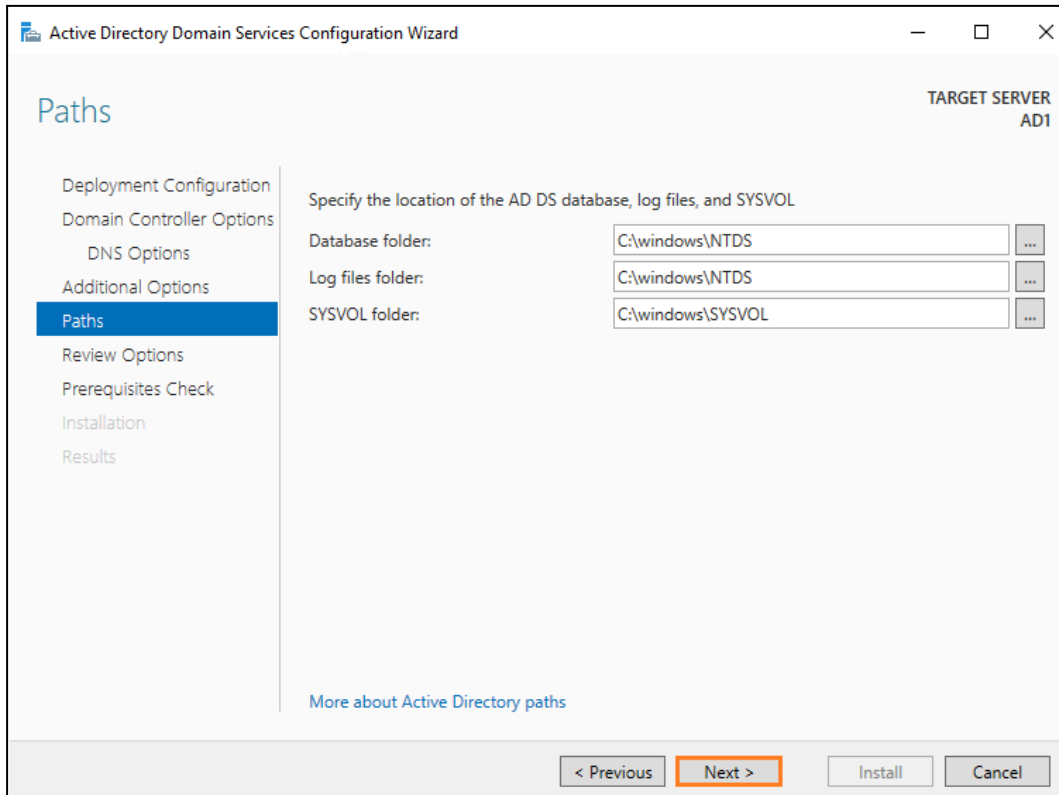




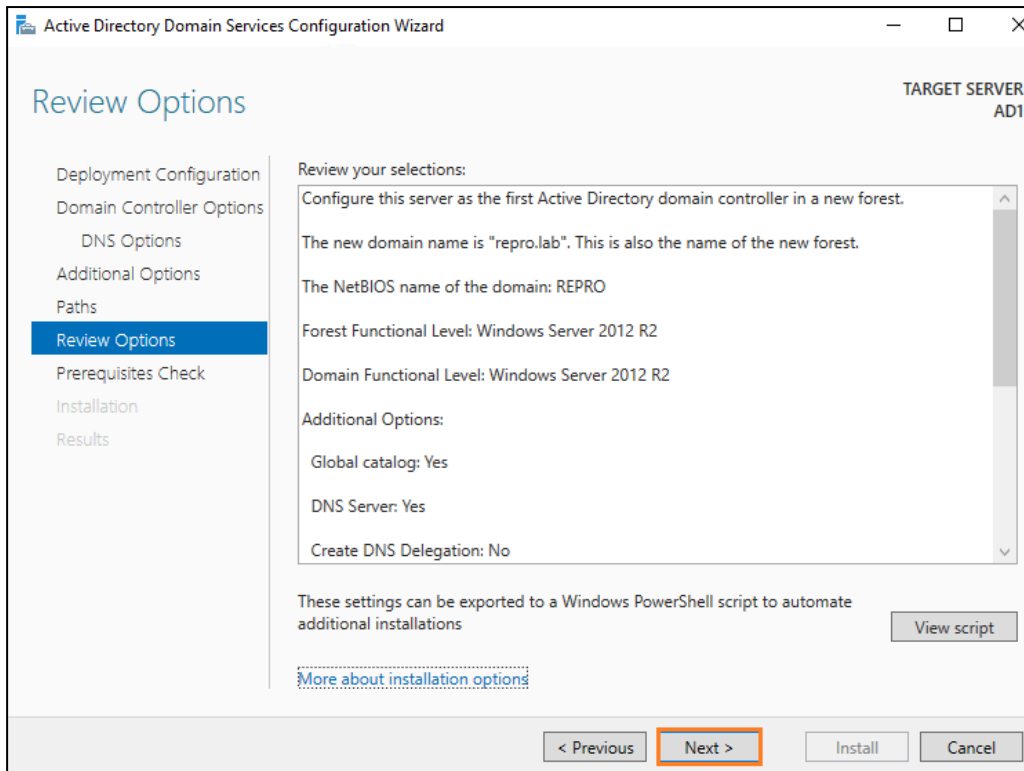
35. Confirm **your NETBIOS domain** is listed in the field and click **Next**.



36. Click **Next**.

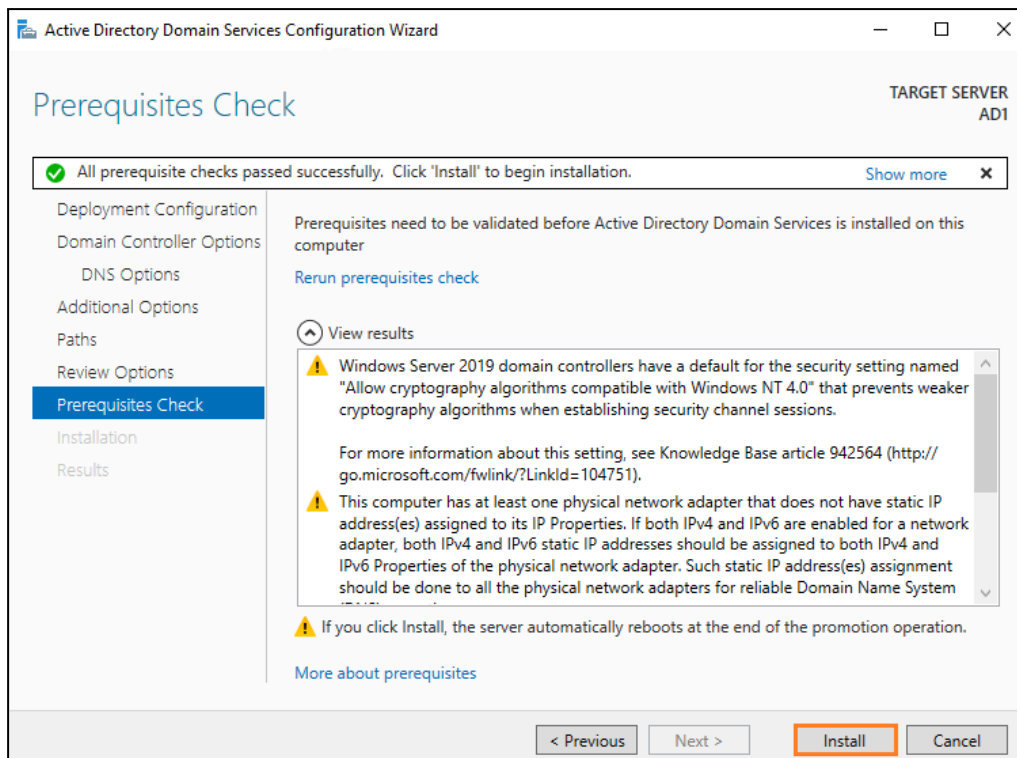


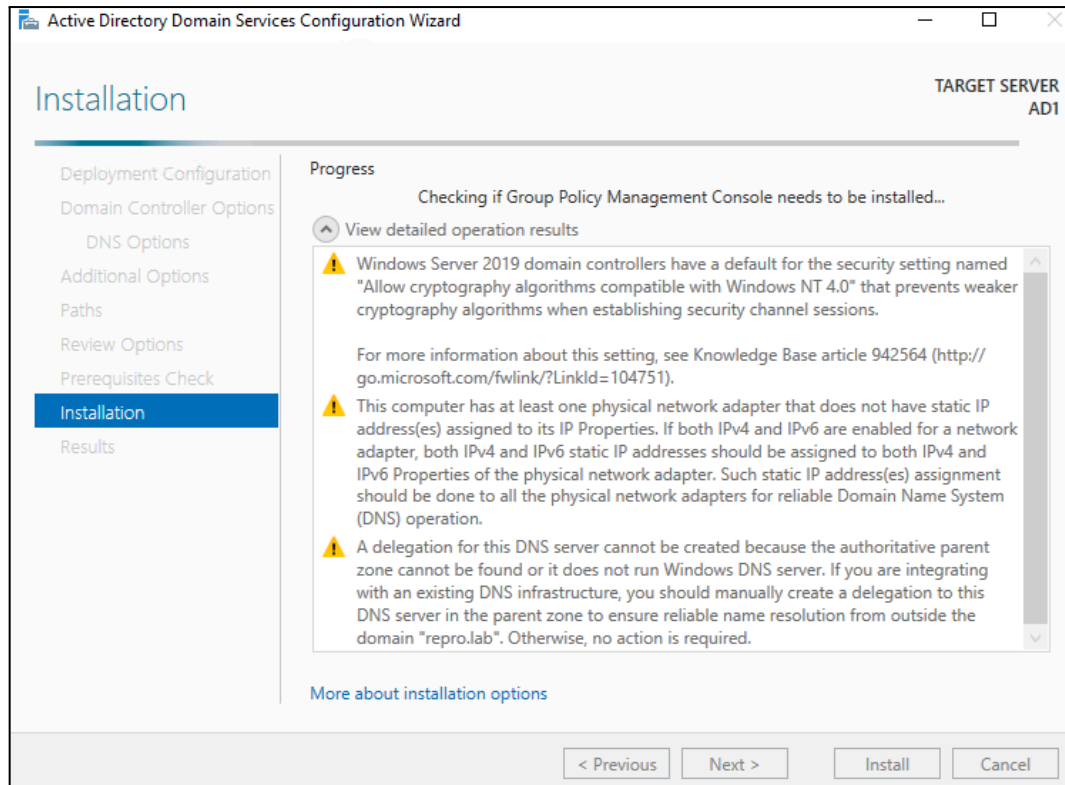
37. Review the configuration options and click **Next**.



38. Once completed, click **Install** to complete the Domain Controller promotion process.

**NOTE 1:** The server will restart when the promotion operation is complete.

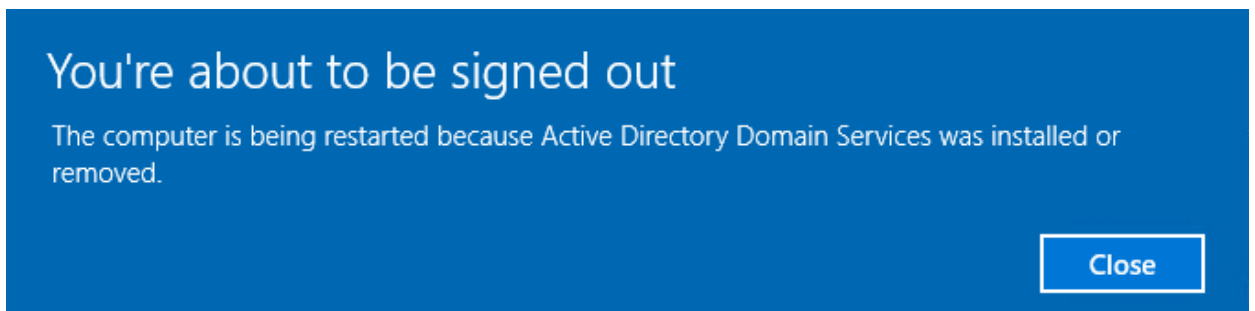




**AD1** is now configured as a **Domain Controller**

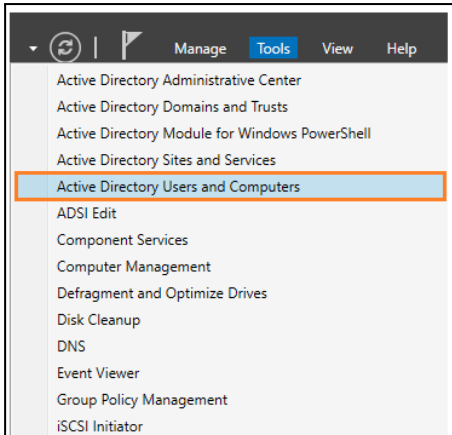
**NOTE:** Going forward, you must log on to your Windows Server AD with the following credentials/format: REPRO\Administrator as the username. If you created your own domain, use DOMAIN\Administrator as the username.

39. Either click close or wait until it reboots by itself.

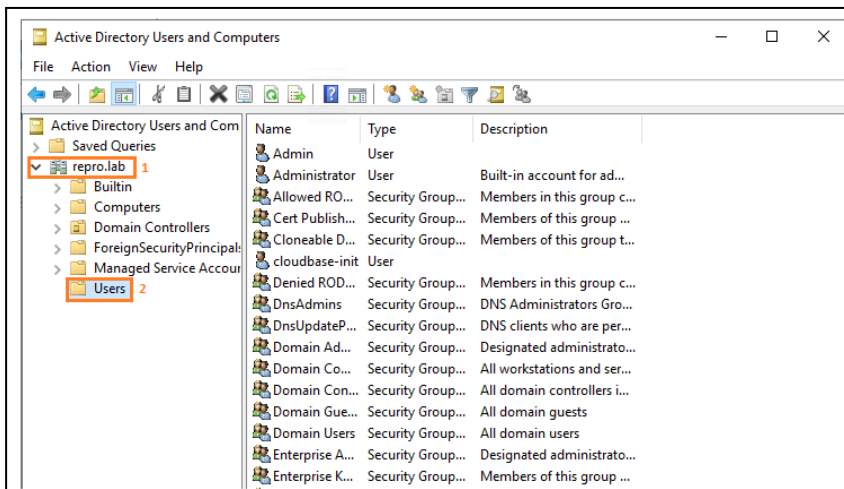


## Adding User Accounts and Configuring Group Membership

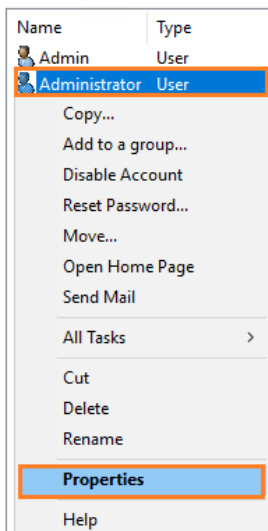
1. Log on again to the **Windows Server AD** using the new format "DOMAIN + Username", navigate to **Start > Server Manager**, click **Tools** in the upper-right, and select **Active Directory Users and Computers**.



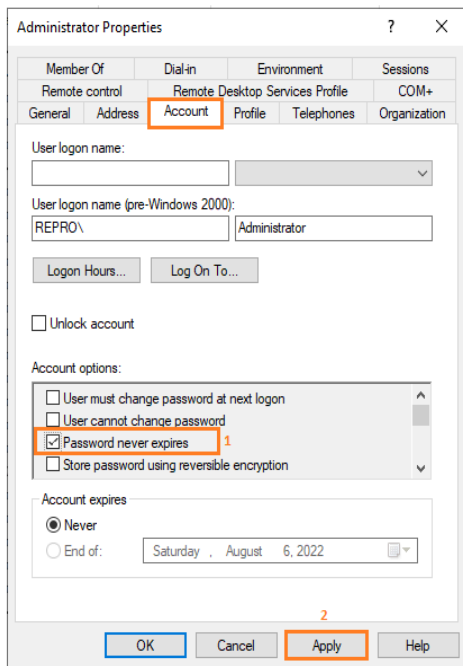
2. Expand **repro.lab** in the left menu and highlight the **Users** folder.



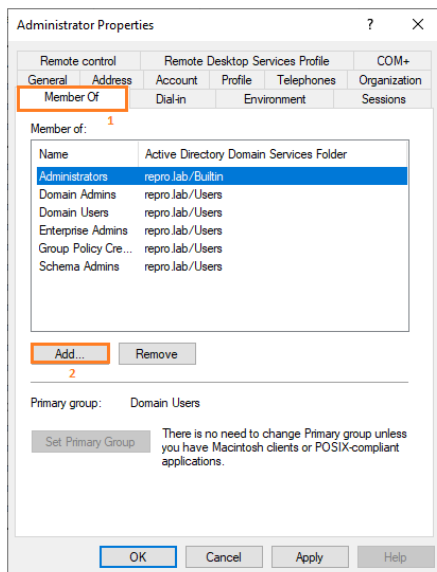
3. Right-click the **Administrator** account in the main field and choose **Properties**.



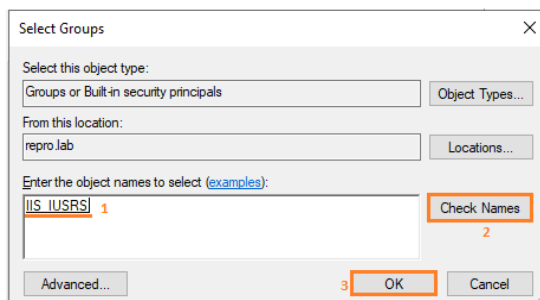
4. Select the **Account** tab, tick the box next to **Password never expires** and click **Apply**.



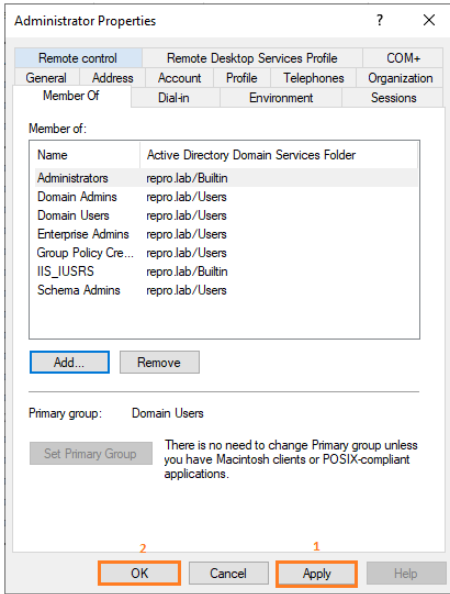
5. Select the **Member Of** tab and click **Add...**



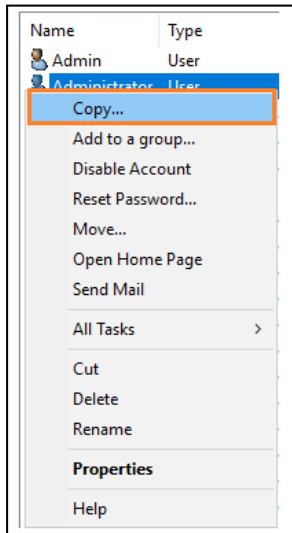
6. Enter **IIS\_IUSRS** and click **Check Names**. Click **OK** to confirm. Click **OK**.



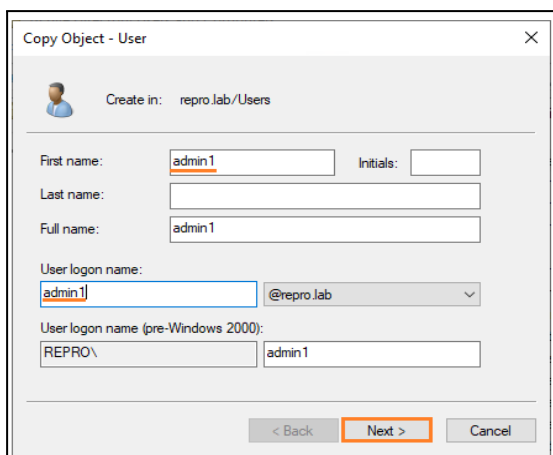
7. Click **Apply** and **OK**.



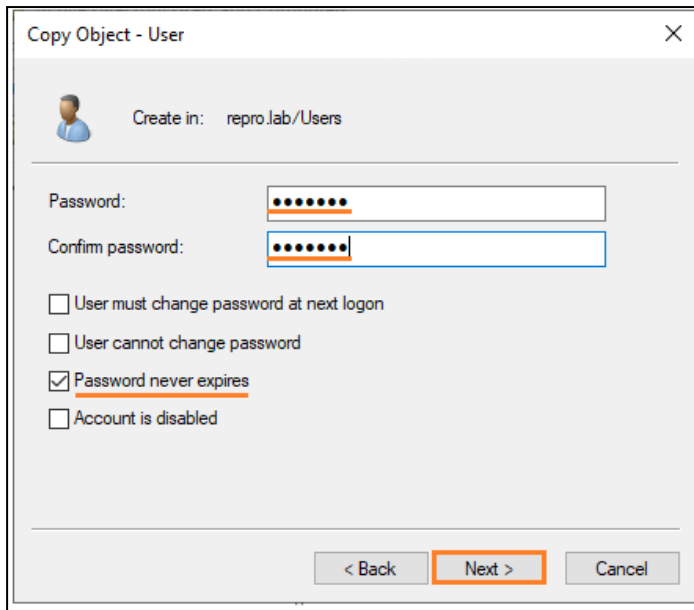
8. **Right-click** the **Administrator** account in the main field and choose **Copy...**



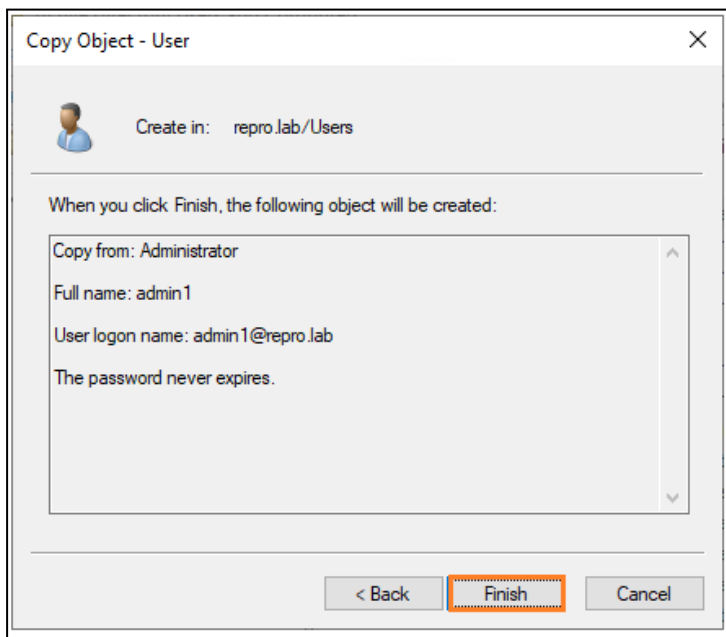
9. Enter **Admin1** in the First name field and **Admin1** in the User logon name field and click **Next**.



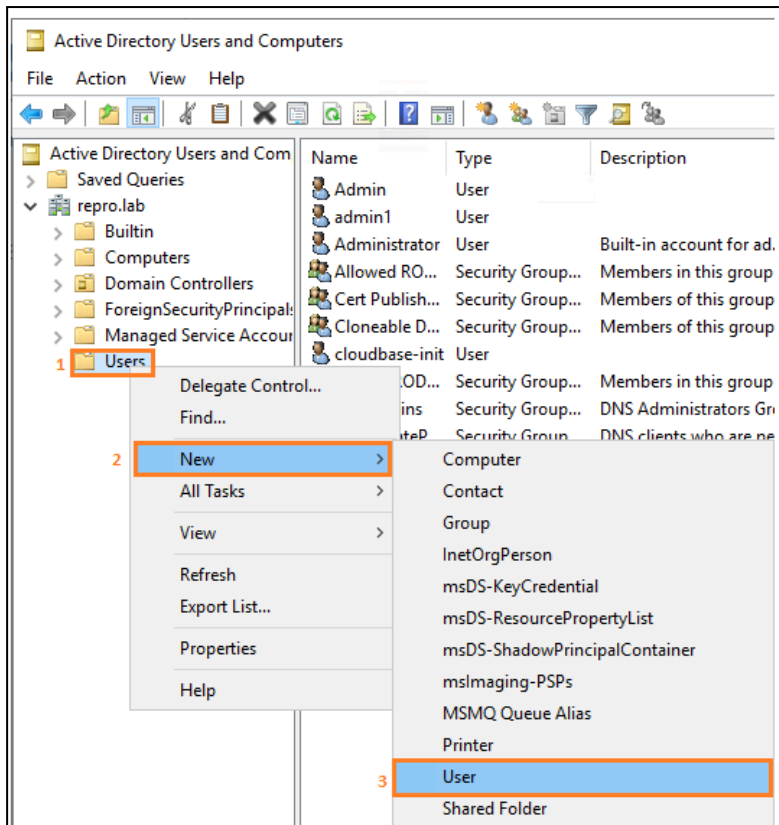
10. Enter **any strong password** in both the Password and Confirm password fields, tick **“Password never expires”** and click **Next**.



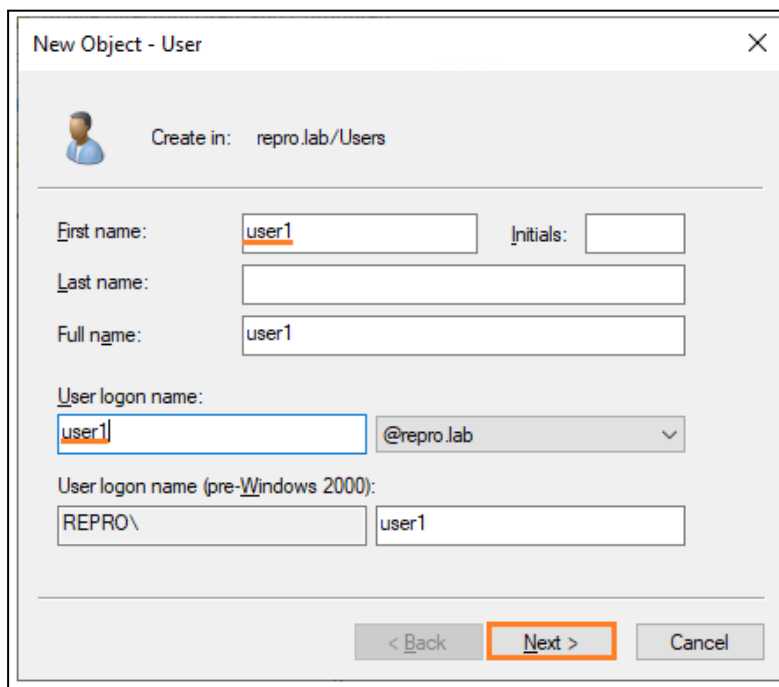
11. Click **Finish** to close the Copy Object.



12. **Right-click** the **Users** folder in the left field, select **New**, and then click **User**.

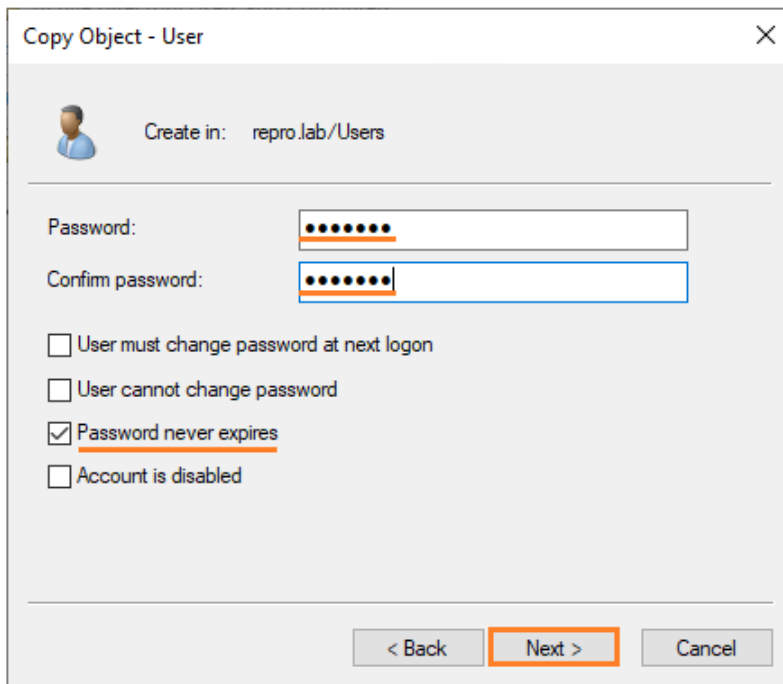


12. Enter **User1** in the First name field and **User1** in the User logon name field, and click **Next**.



13. Enter **any strong password** in both the Password and Confirm password fields, un-tick the box next to **User must change password at the next logon**, tick **“Password never expires”** and click **Next**.

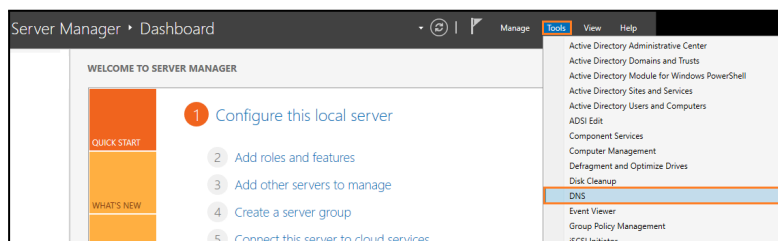




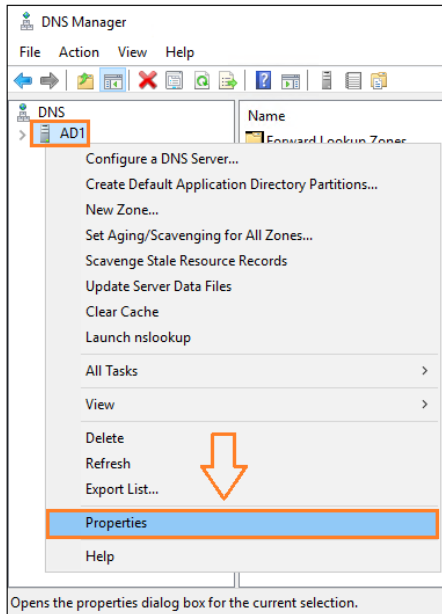
14. Click **Finish**.

## Configuring Active Directory DNS

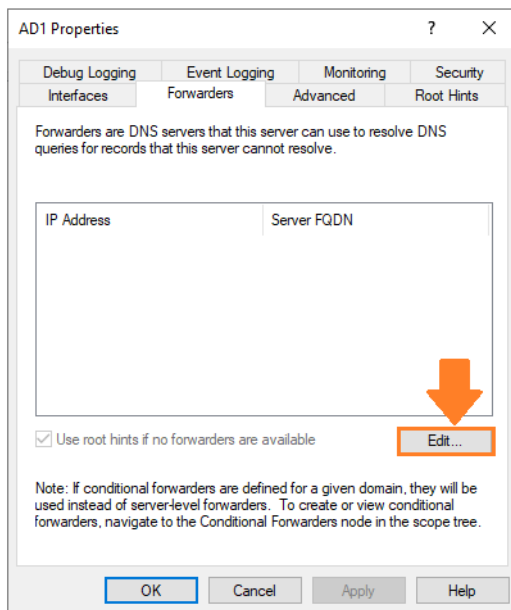
1. In **Server Manager**, click the **Tools** menu in the upper-right and select **DNS**.



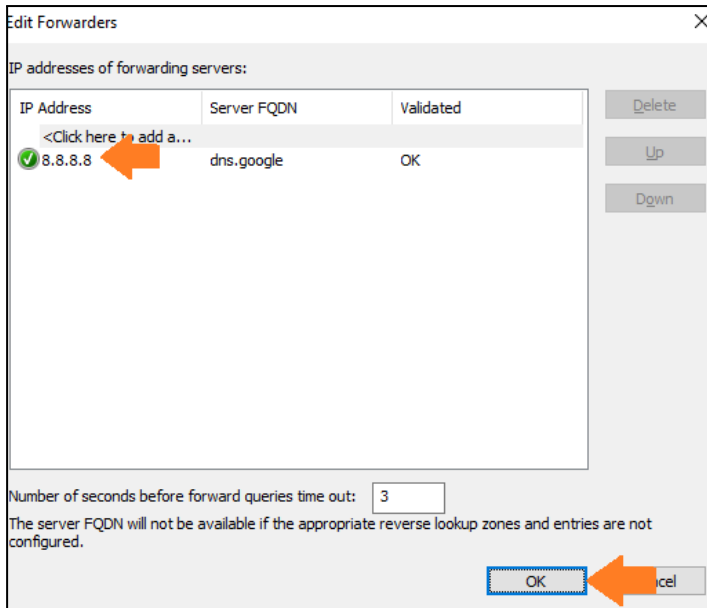
2. The DNS Manager console will launch. **Expand** the arrow located next to the server name, right-click **AD1** and choose **Properties**.



3. On the AD1 Properties screen click the Forwarders tab. Click the Edit... button to open the Edit Forwarders dialog.



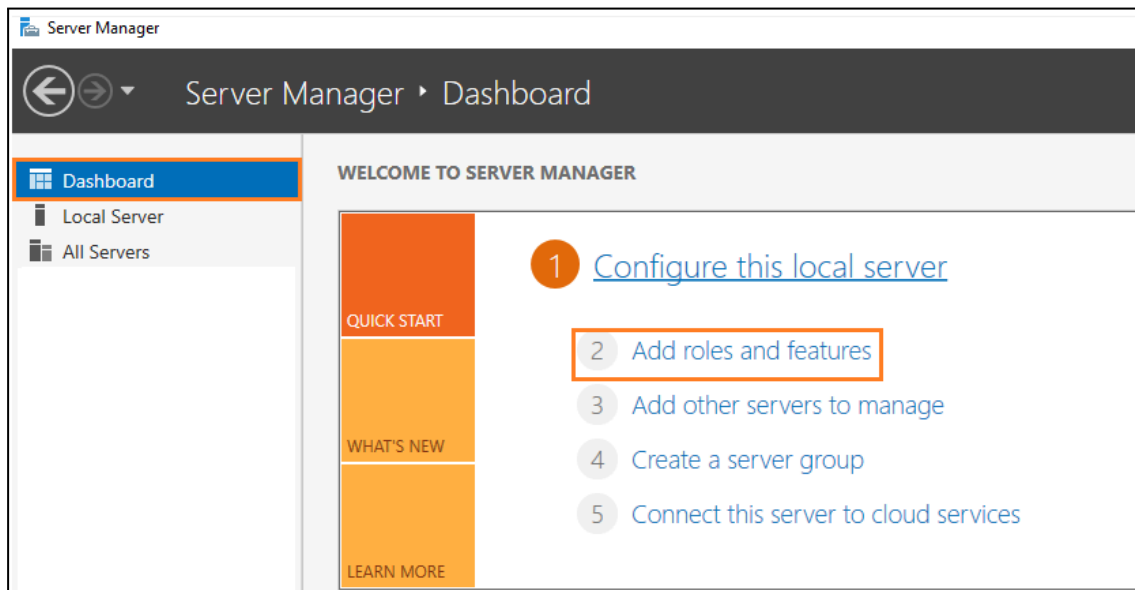
4. Please add any internal DNS server you have or add a Public DNS such as **8.8.8.8**. Click **OK** and **OK**.



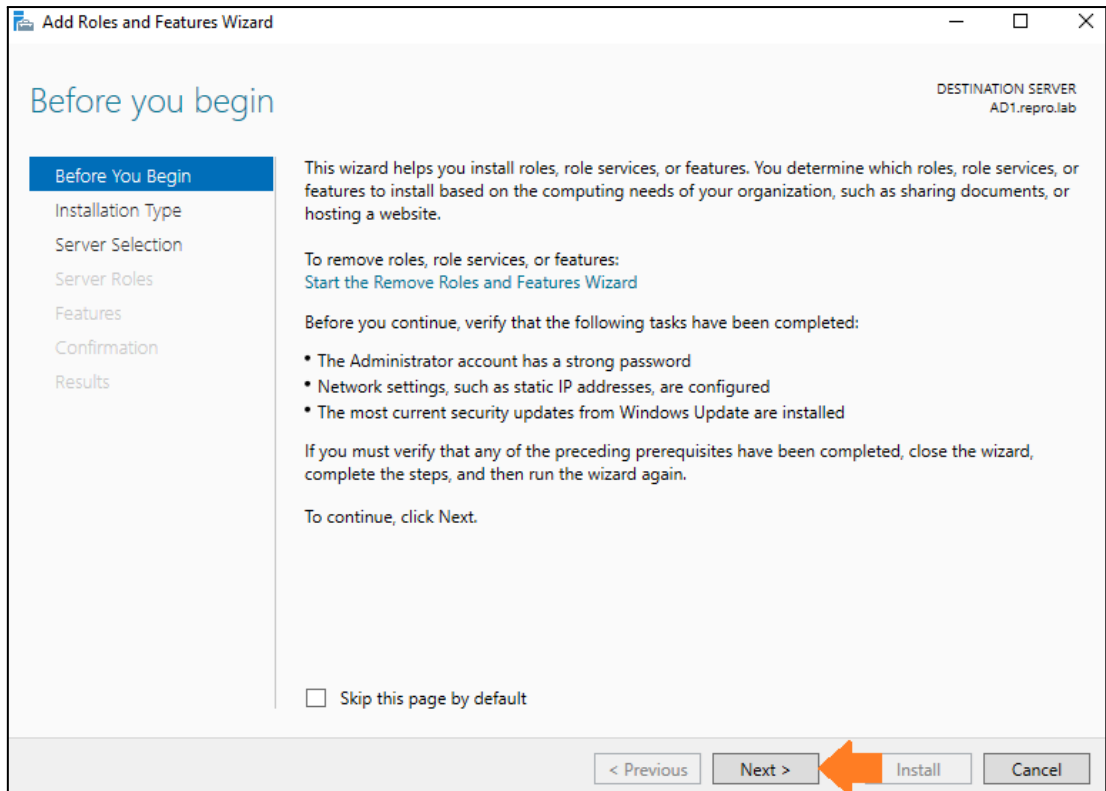
**NOTE:**

1. DNS forwarders will send requests for unresolved DNS names to these servers for resolution.
2. Active Directory Certificate Services (AD CS) will allow resources to request SSL certificates to provide HTTPS communication throughout the environment. SSL certificates are used with multiple Citrix products, including NetScaler Gateway and StoreFront.

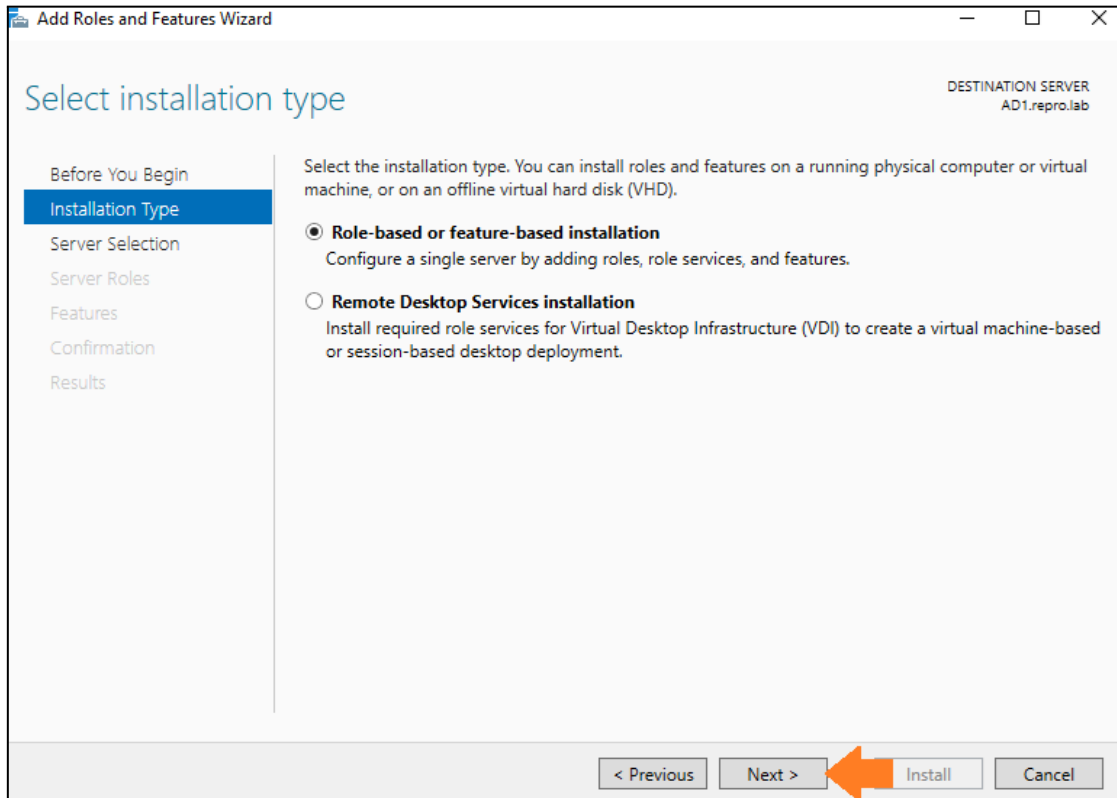
1. From the **Server Manager** console click the **Add roles and features** link in the main window.



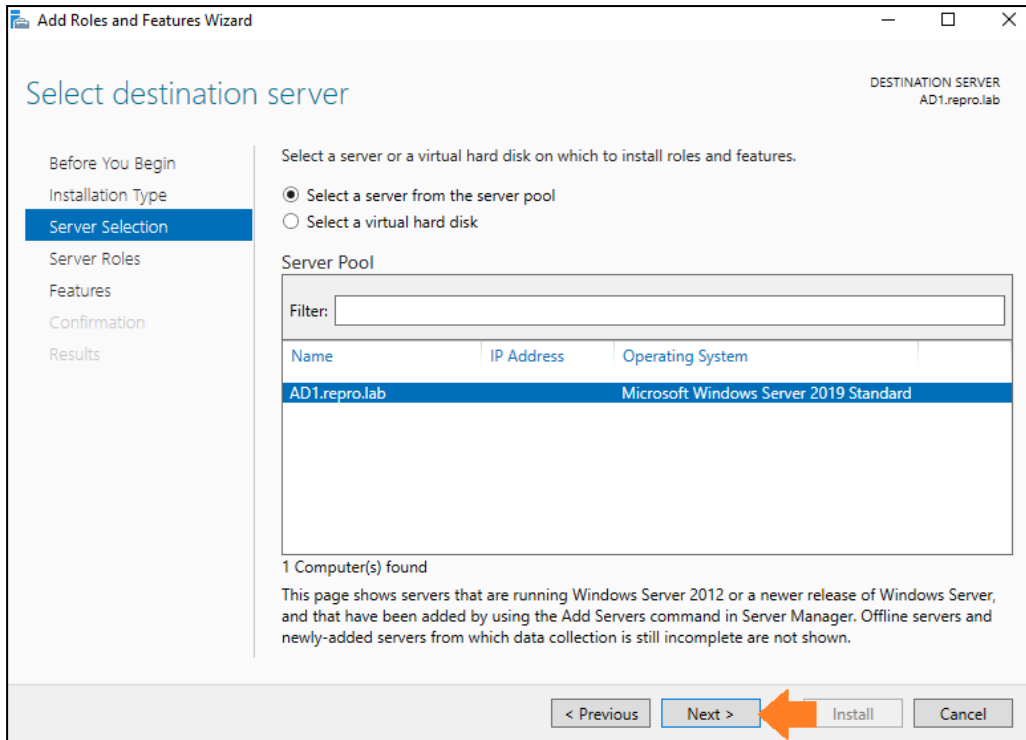
2. Read the information provided and click **Next**.



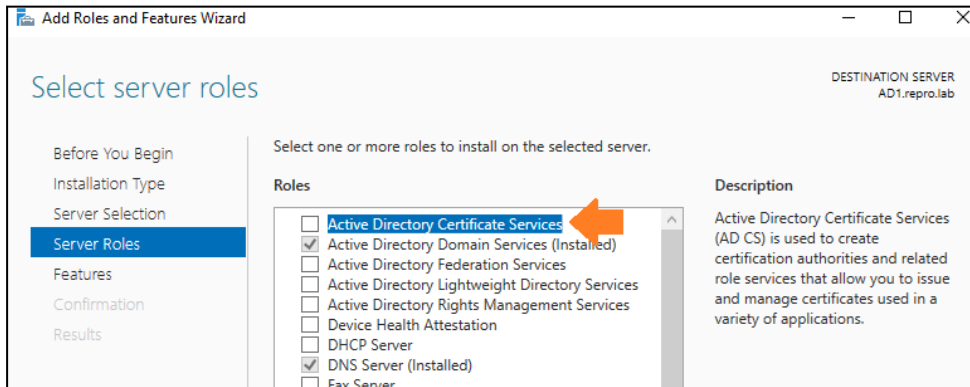
3. Keep **Role-Based or feature-based installation** selected and click **Next**.



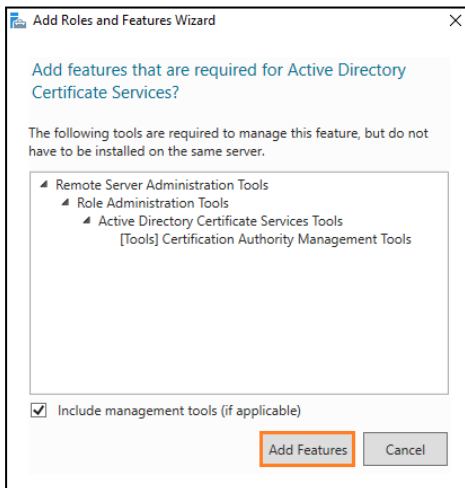
4. Keep **Select a server from the server pool** highlighted and click **Next**.



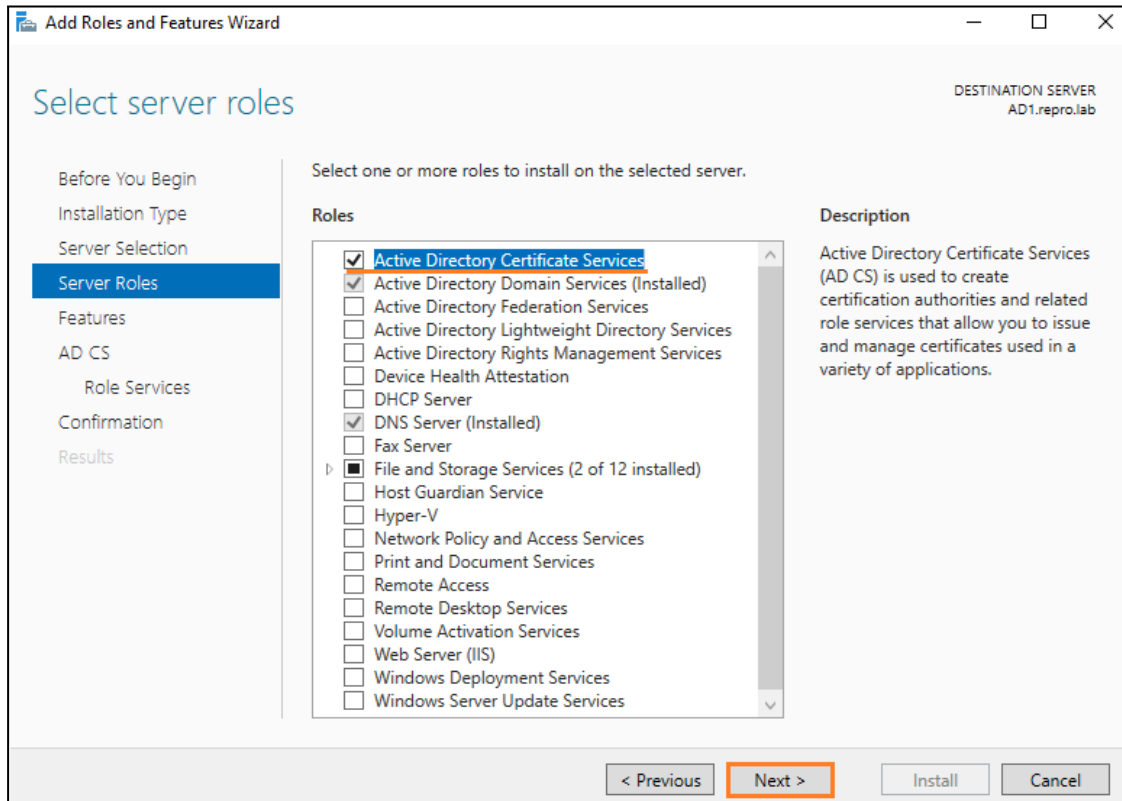
5. Tick the box next to **Active Directory Certificate Services**.



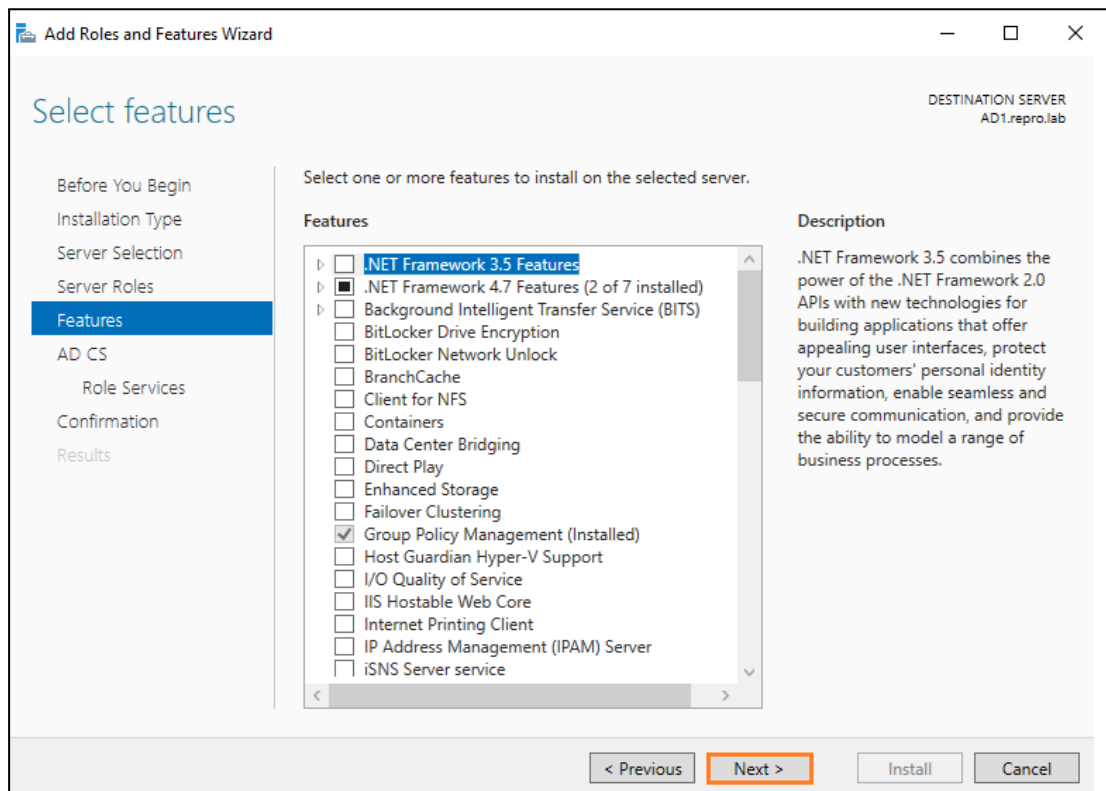
6. An additional dialog will open asking to add features required for Active Directory Domain Services. Confirm the box is ticked next to **Include management tools (if applicable)** and click the **Add Features** button.



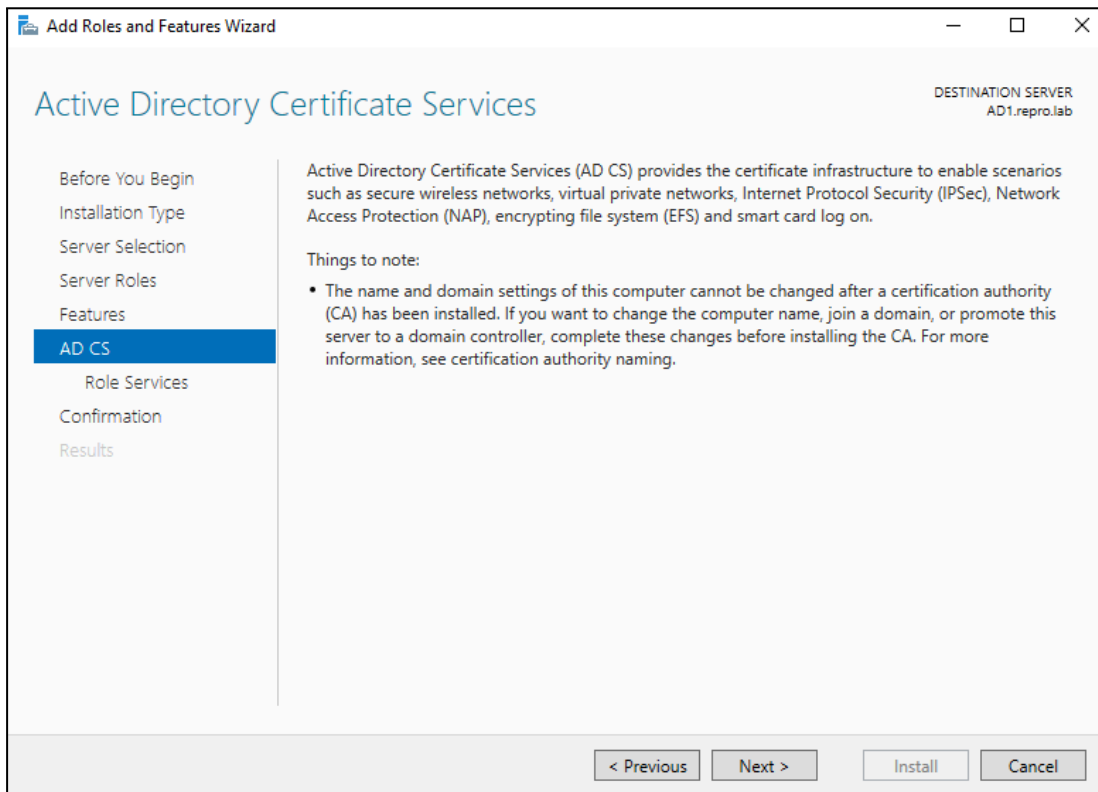
7. Active Directory Certificate Services will now have a tick in the box next to it. Click **Next** to continue.



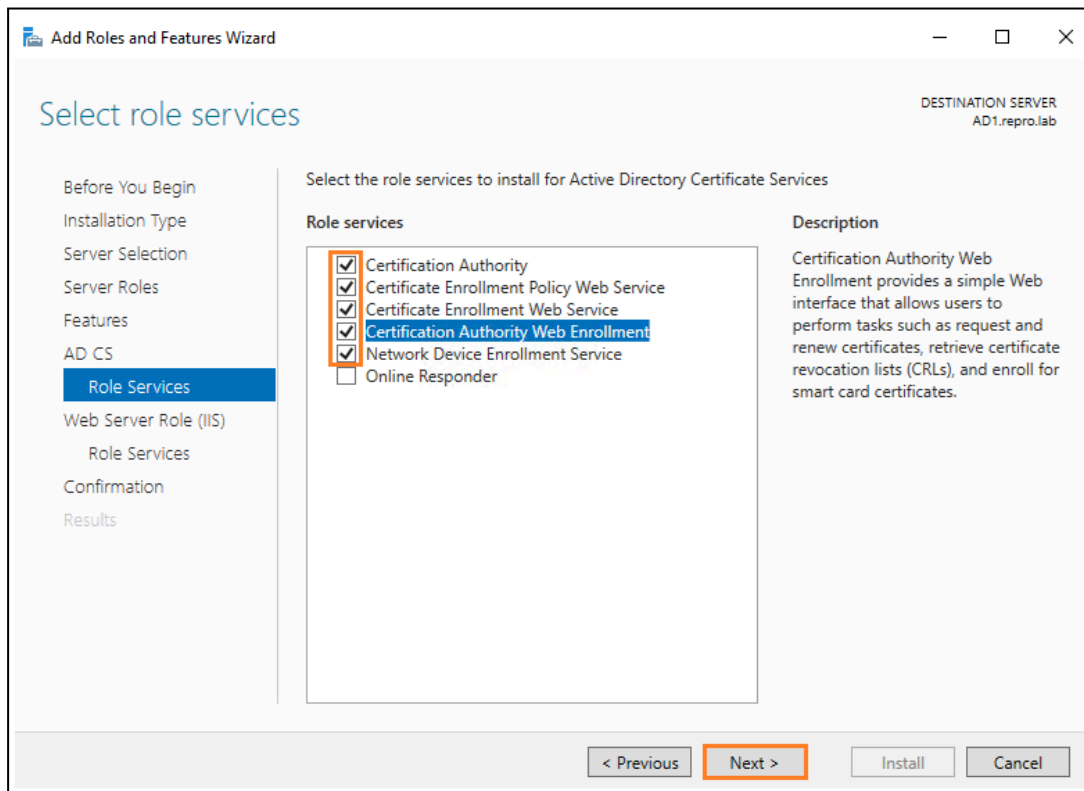
8. The next portion of the Wizard asks to select features. Since the previous step prompted to add the required features, no additional selections are necessary. Click **Next** to continue.

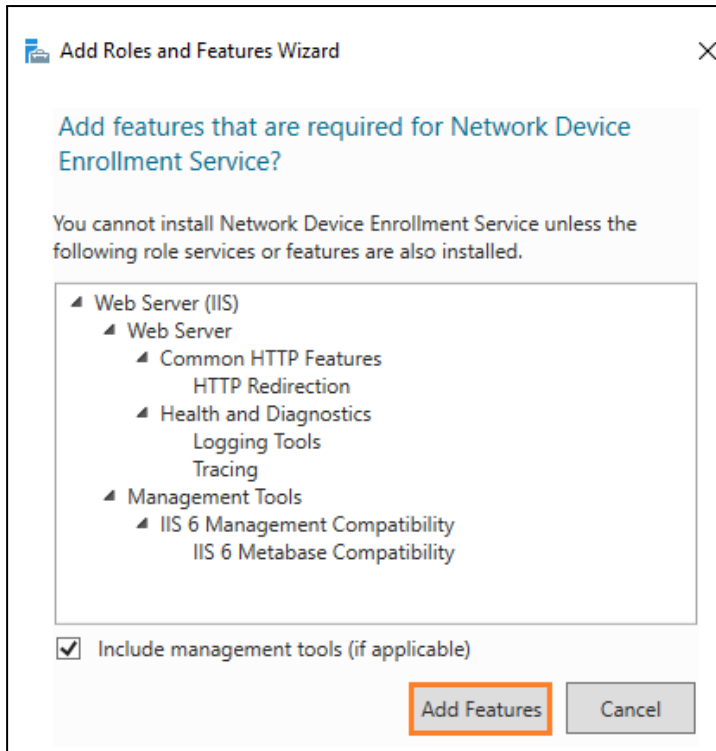


9. Review the description of Active Directory Certificate Services and click **Next**.

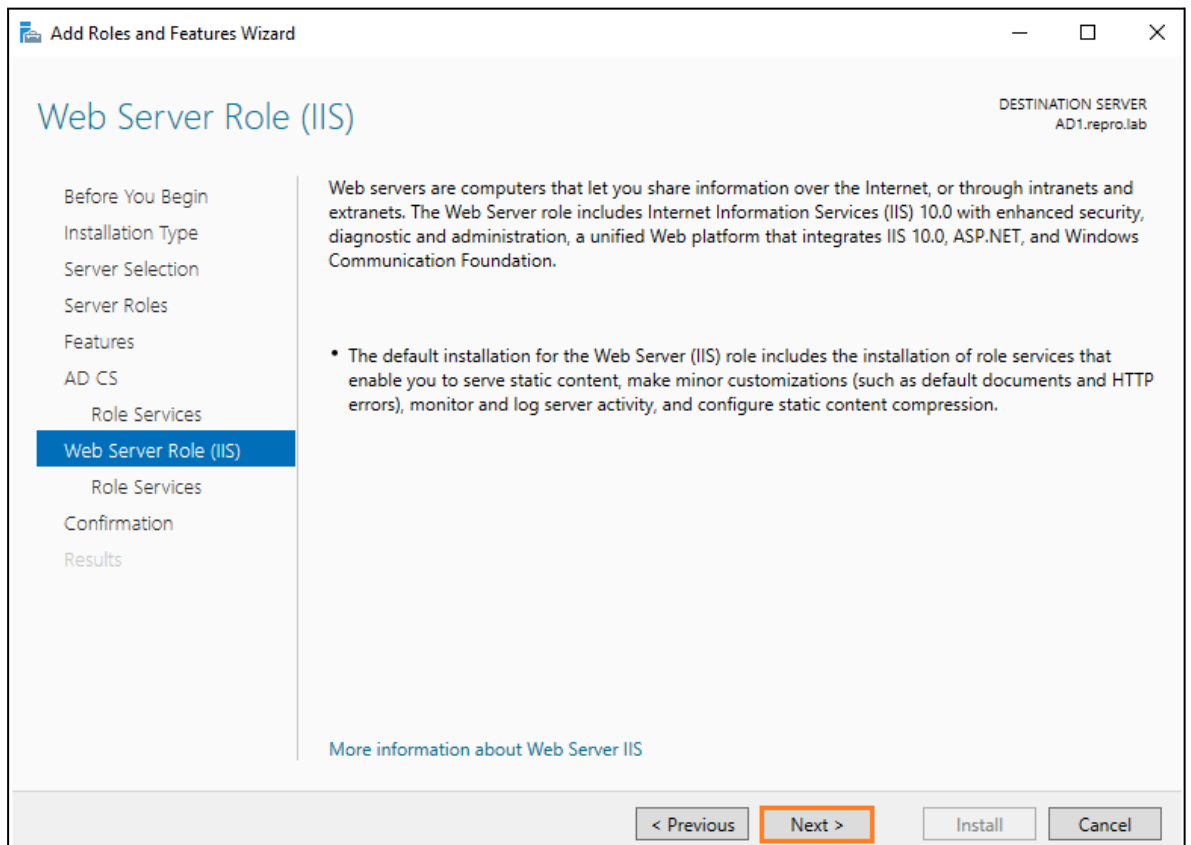


10. Tick the boxes next to **Certification Authority**, **Certificate Enrollment Policy Web Service**, **Certificate Enrollment Web Services**, **Certification Authority Web Enrollment**, and **Network Device Enrollment Service**. Some of these selections will open an additional Add Roles and Features window – click **Add Features** each time this window appears.



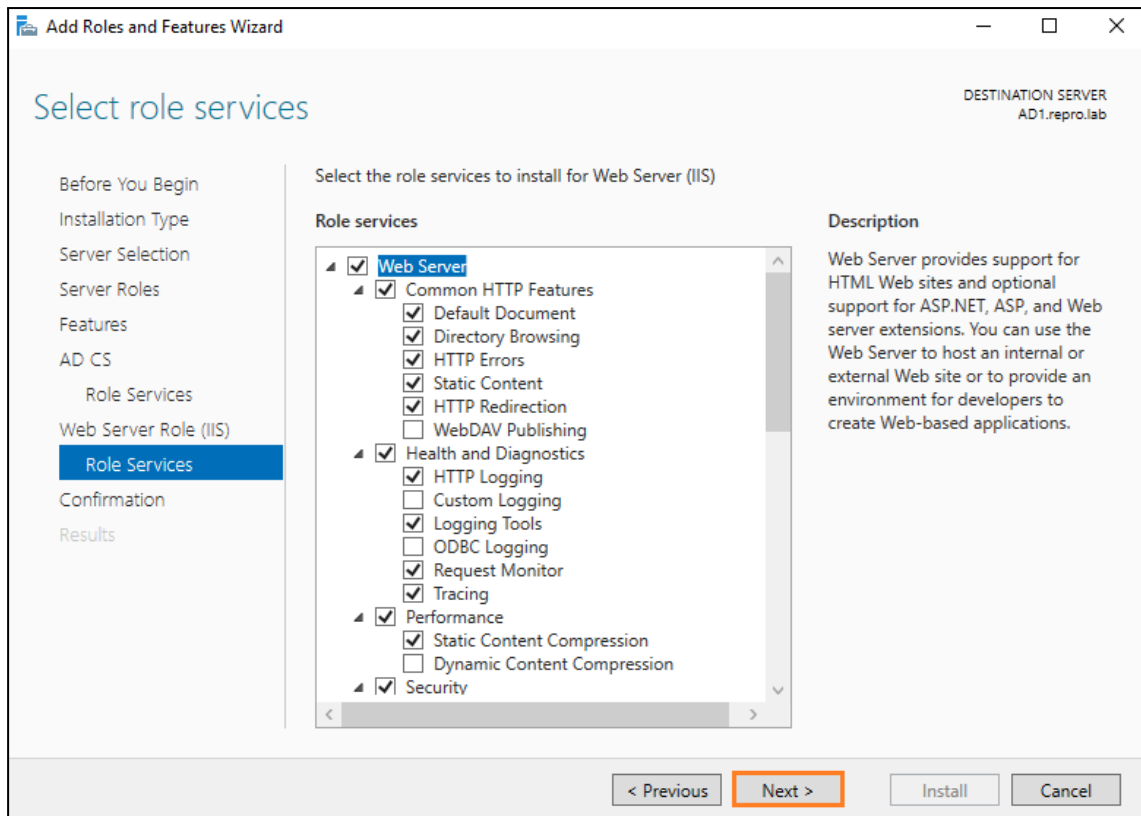


11. Review the information on the Web Server Role (IIS) screen and click **Next**.

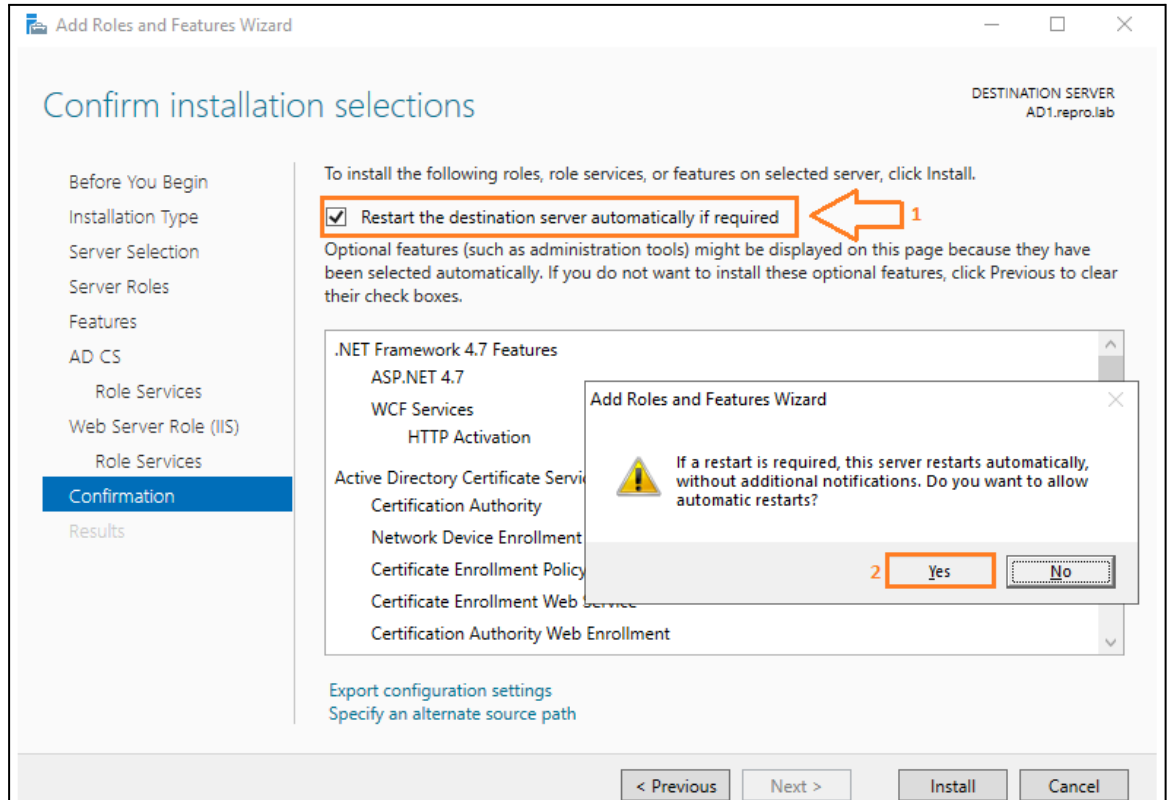


12. Leave the default selections on Select role services and click **Next**.

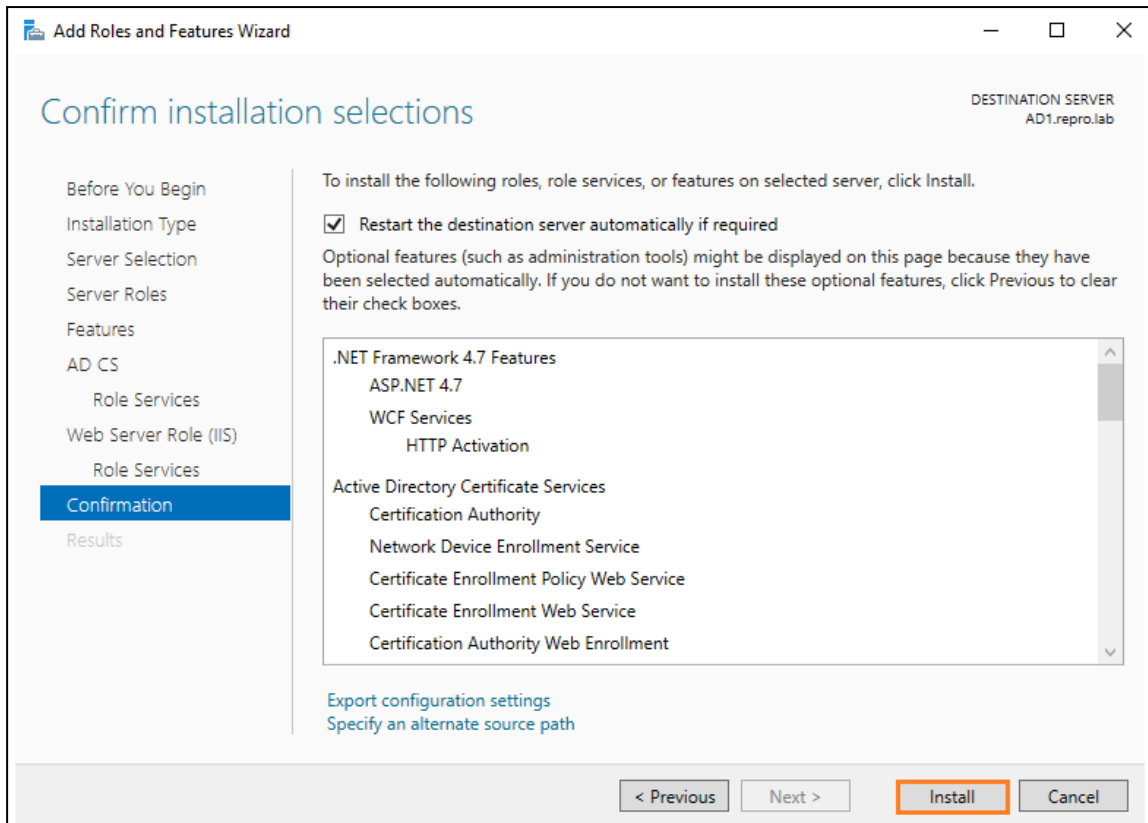




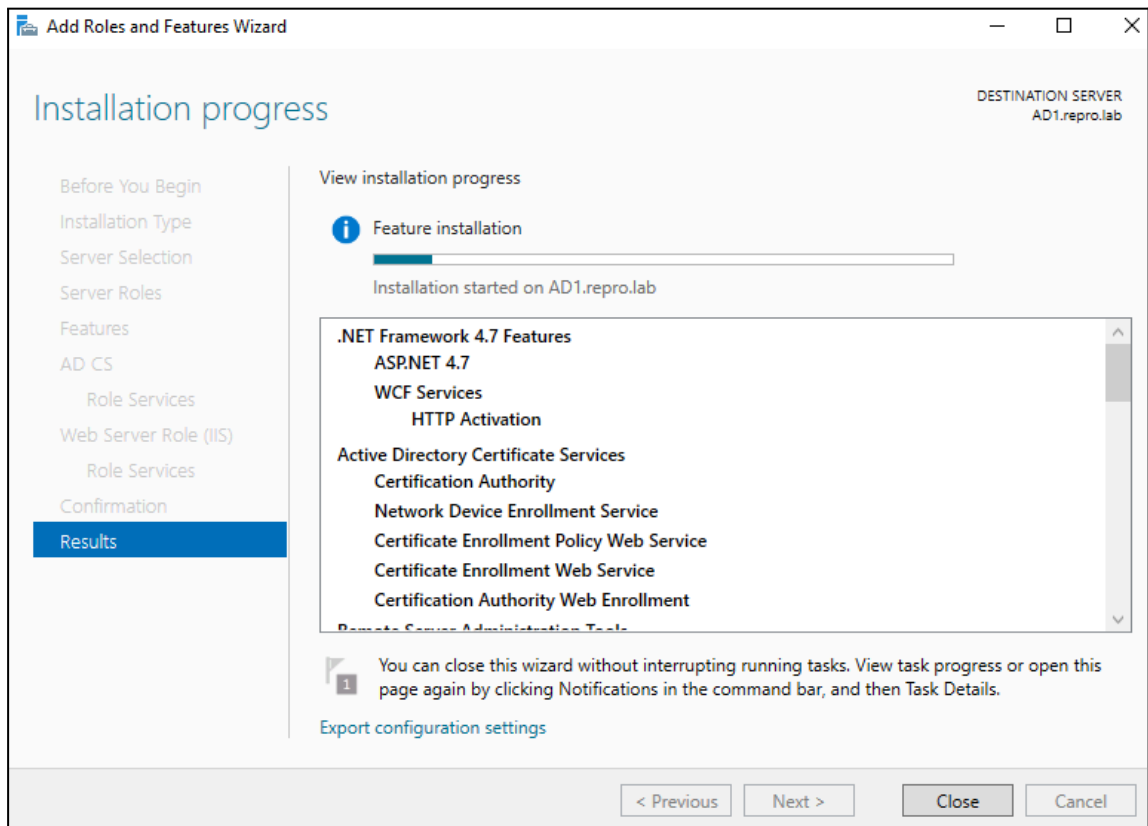
13. On the confirmation screen, tick the box next to **Restart the destination server automatically if required** then click **Yes** when asked to allow automatic restarts.



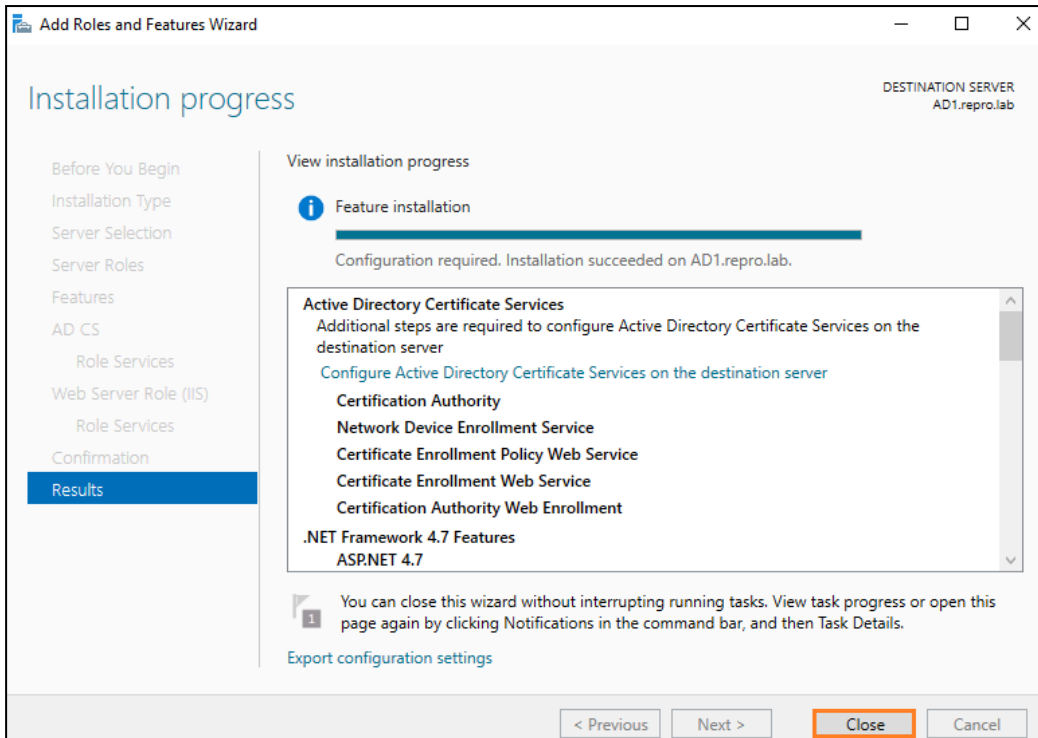
14. Click the **Install** button to begin the installation process.



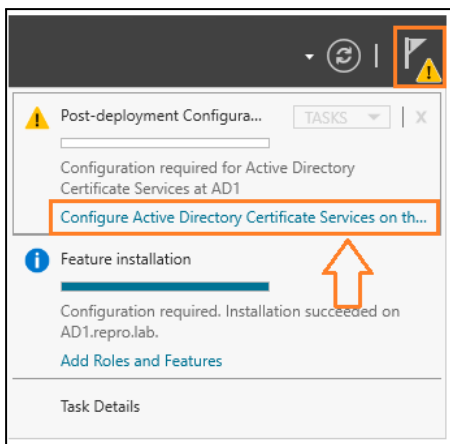
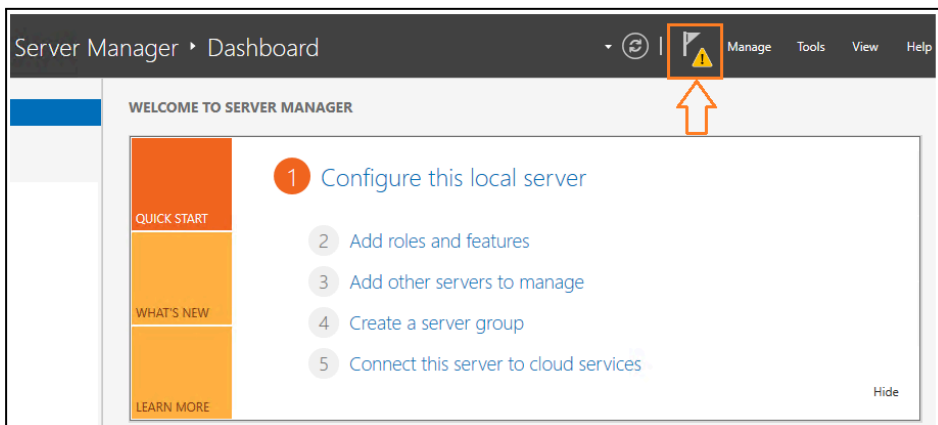
15. The installation process will take a few minutes and the server may restart



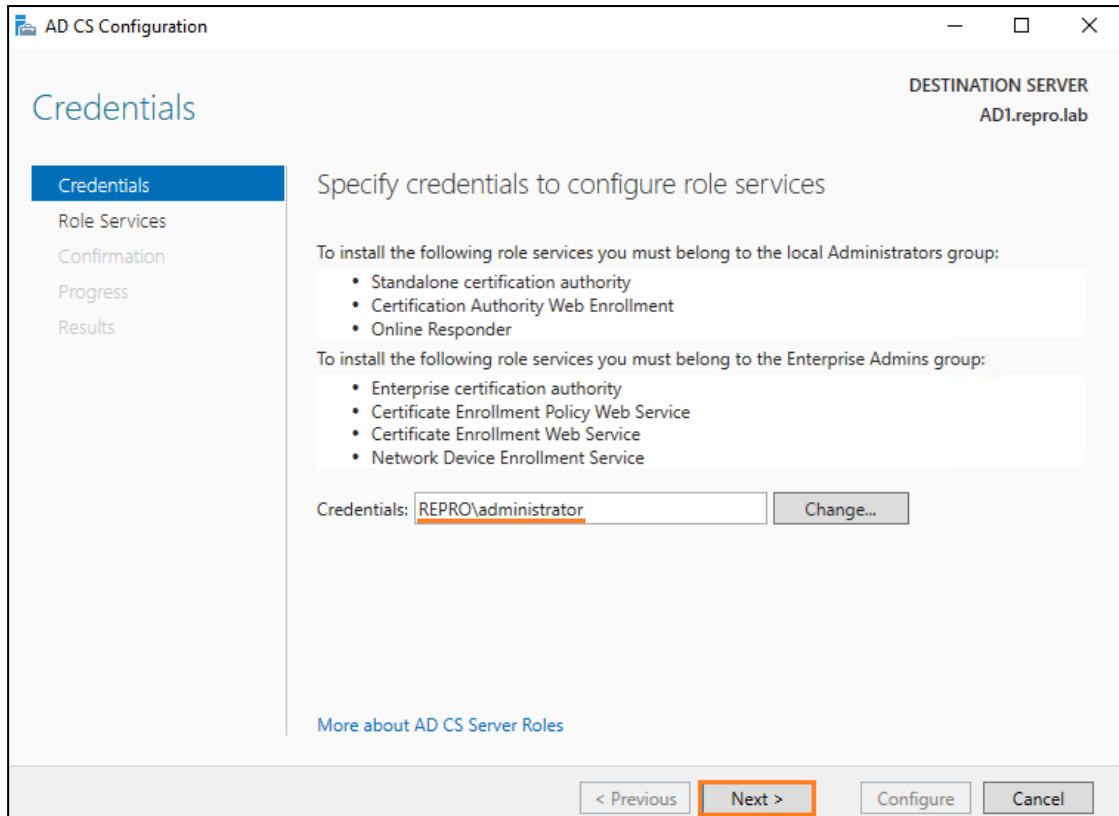
16. Once installation is complete, click **Configure Active Directory Certificate Services on the destination server** to launch the AD CS Configuration wizard.



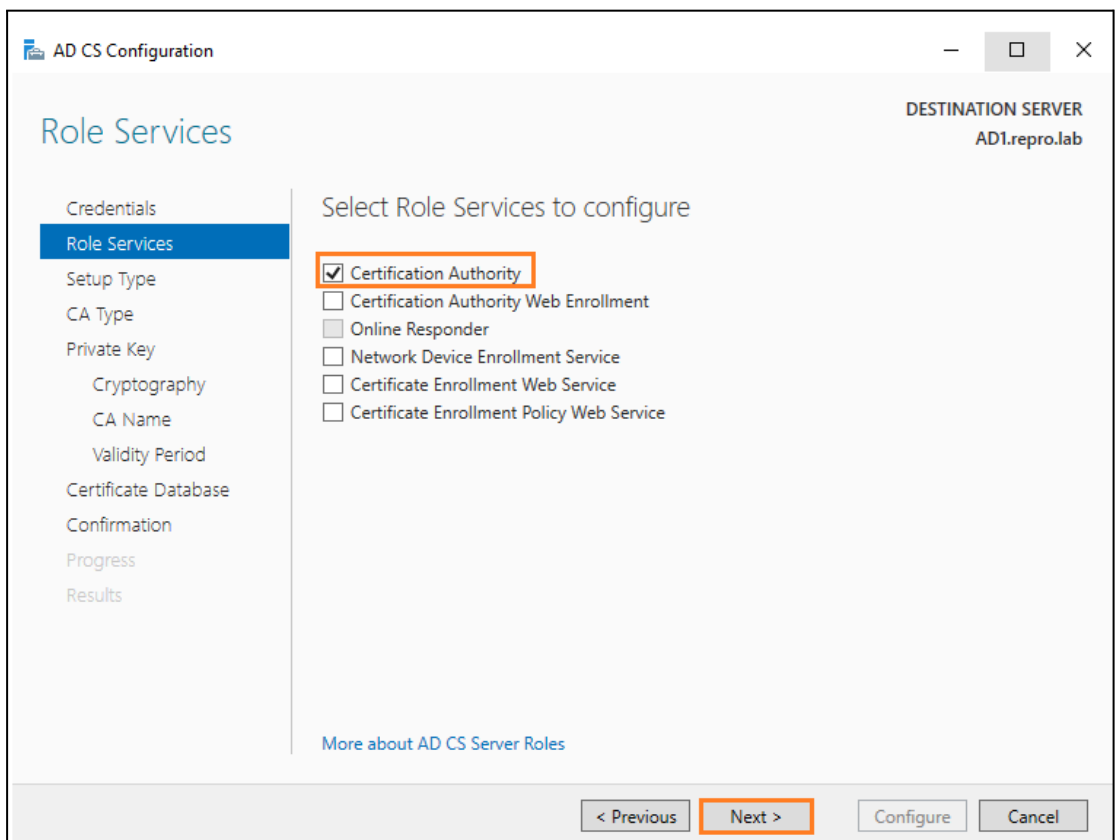
17. Go to the notifications icon on Server Manager and click on **Configure Active Directory Certificate Services**.



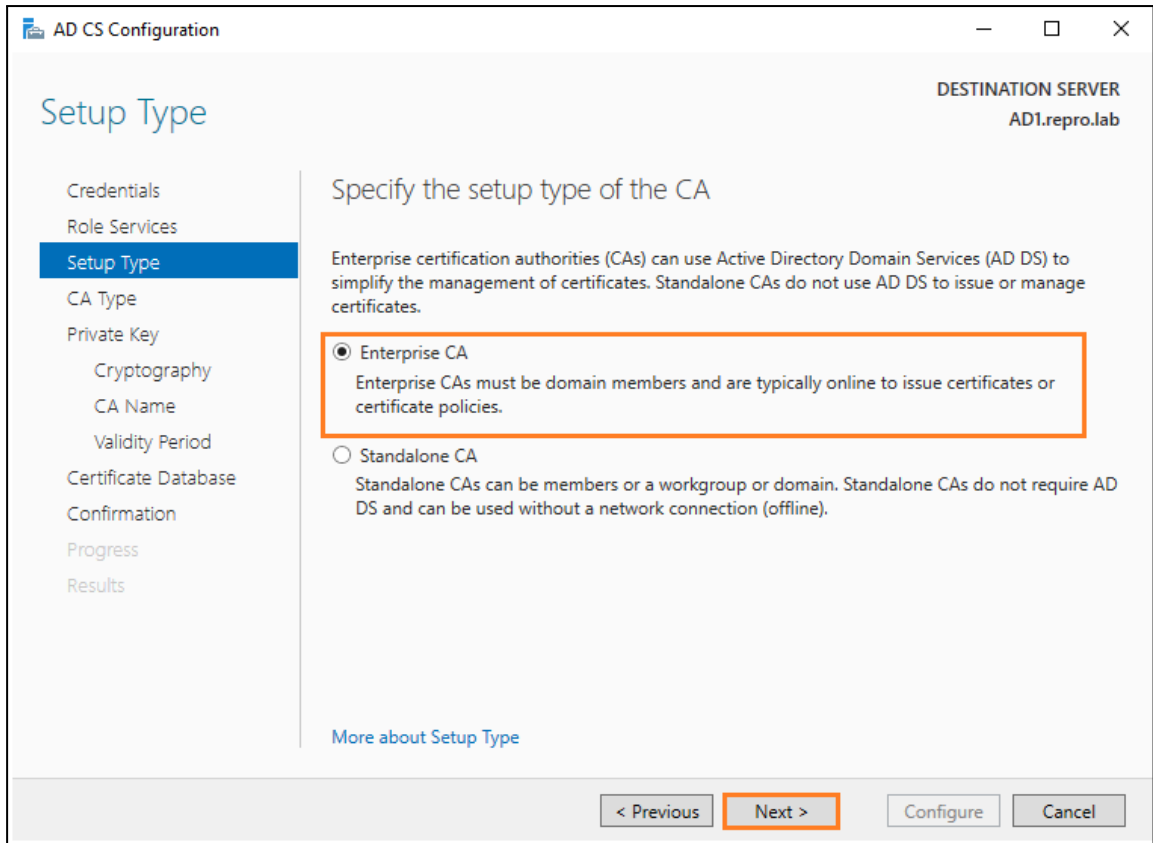
18. Confirm **REPRO\Administrator** (your domain\administrator) is listed in the **Credentials** field and click **Next**.



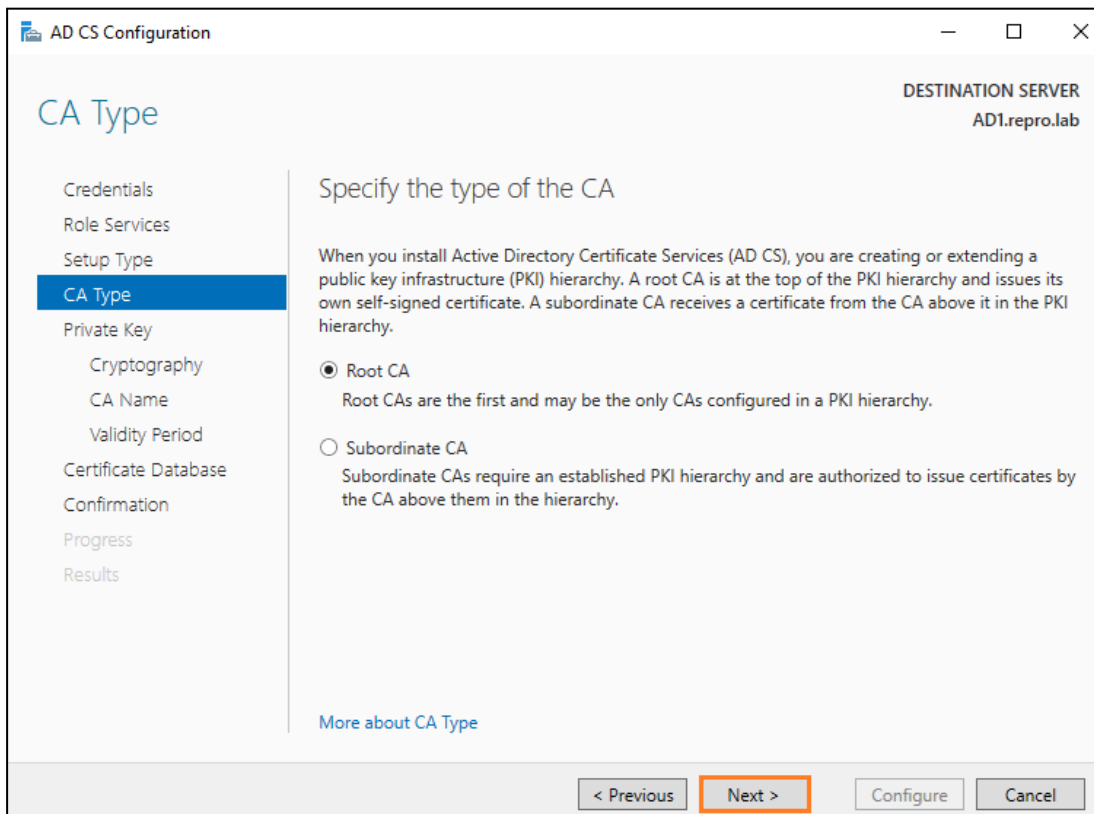
19. Tick the box next to the Certification **Authority** and click **Next**.



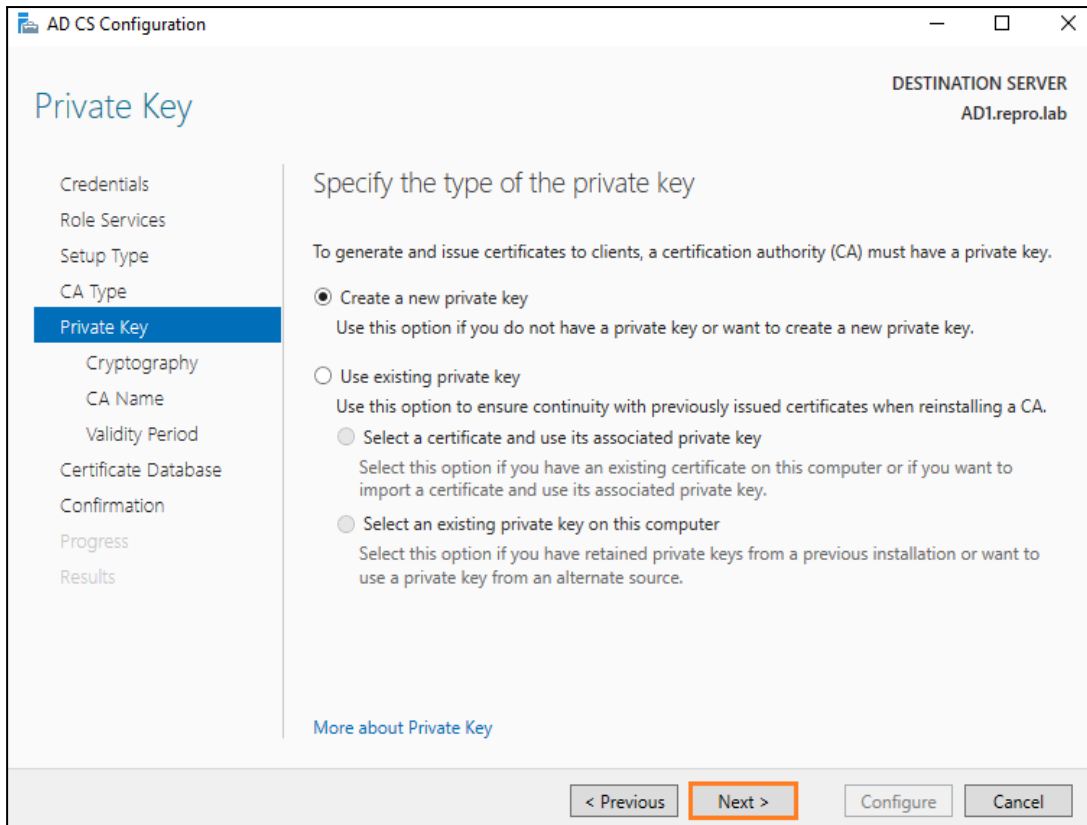
20. Confirm **Enterprise CA** is selected and click **Next**.



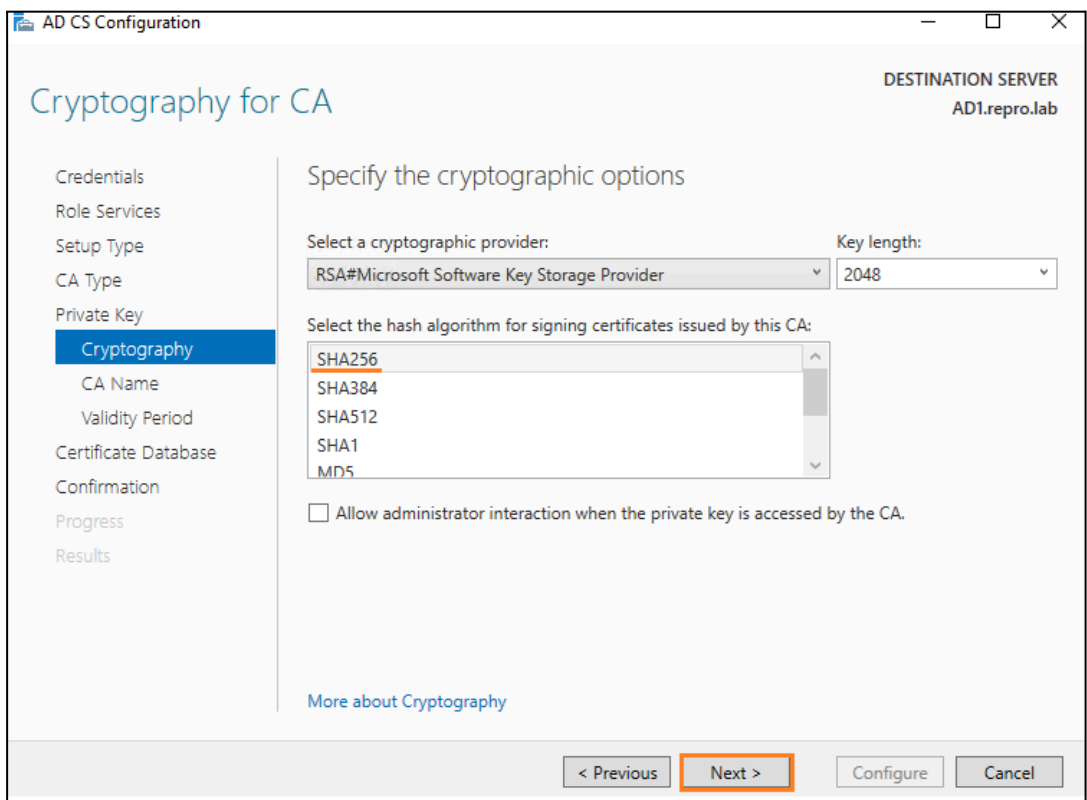
21. Confirm **Root CA** is selected and click **Next**.



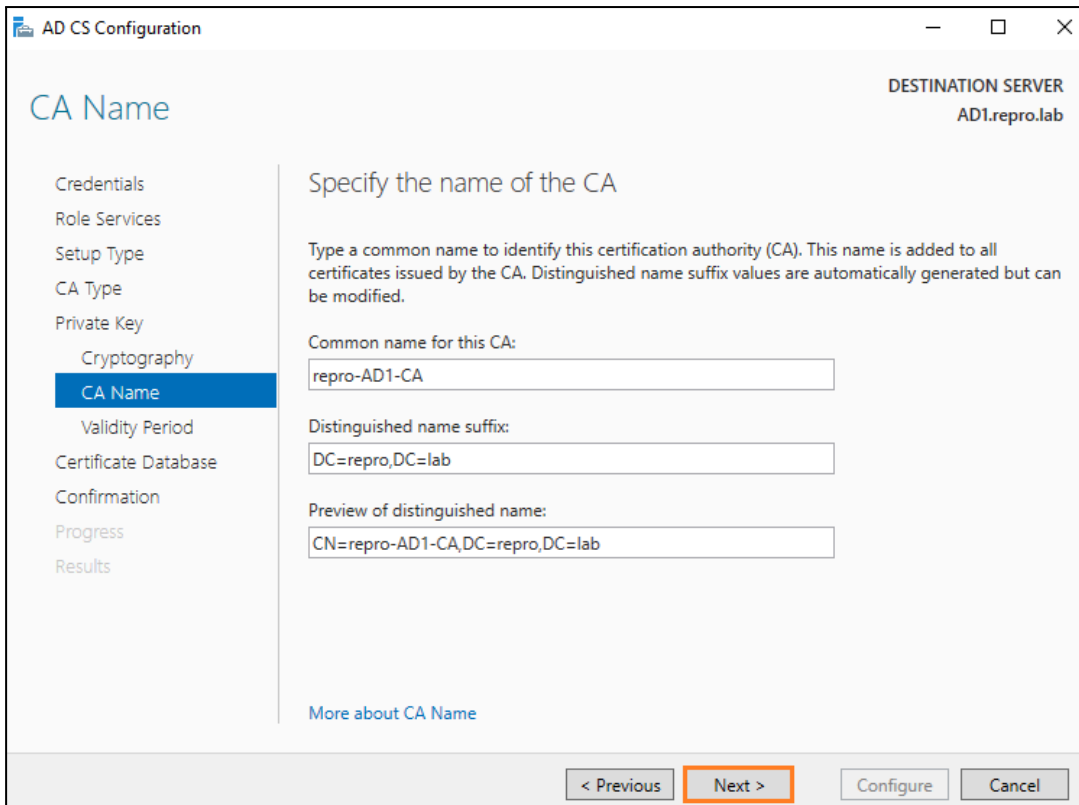
22. Confirm **Create a new private key** is selected and click **Next**.



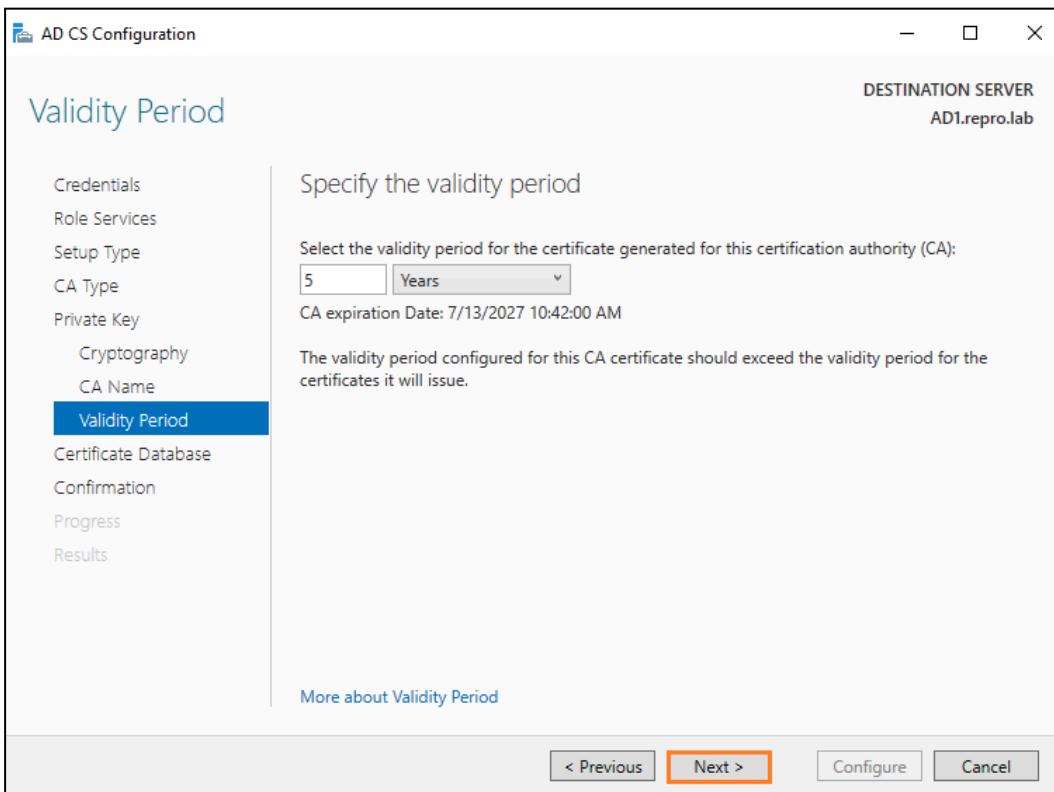
23. Choose SHA256 and click **Next**.



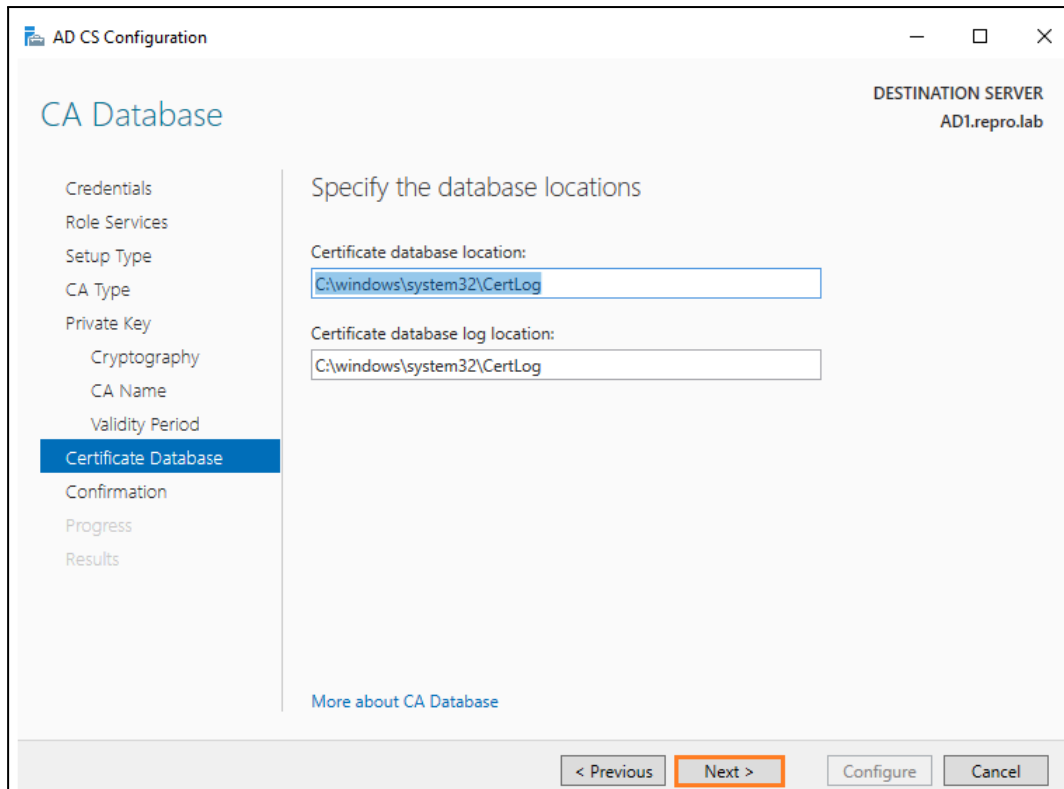
24. Leave the name of the CA at the default and click **Next**.



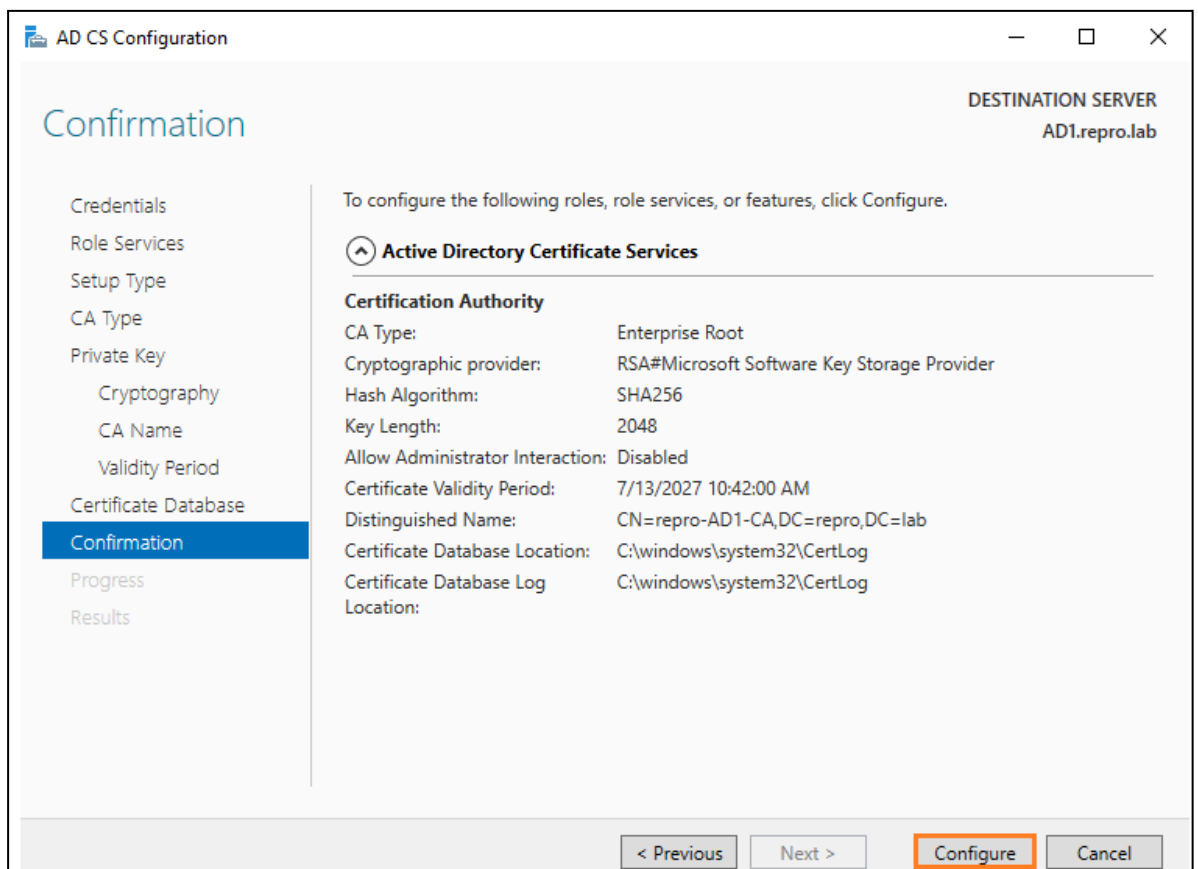
25. Leave the validity period at 5 Years and click **Next**.



26. Leave the database locations at their defaults and click **Next**.

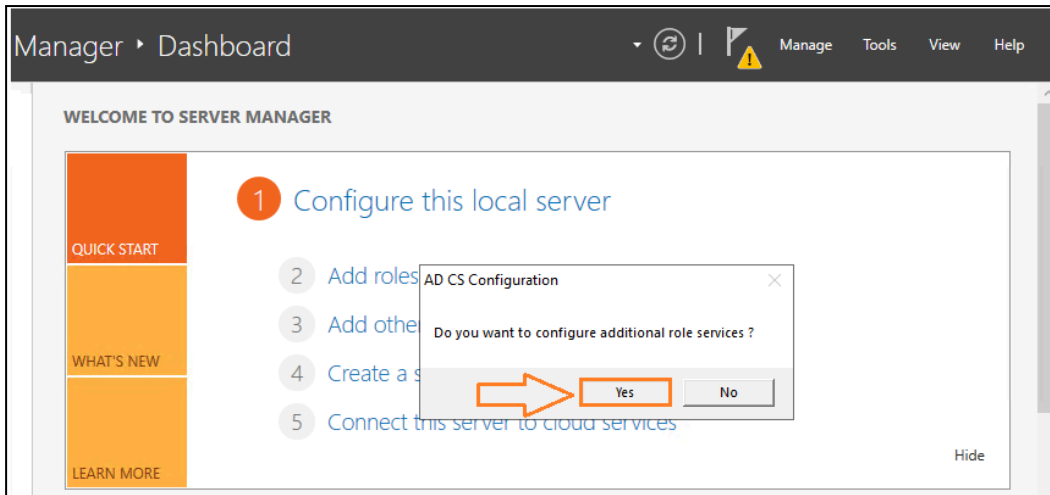


27. Review the configuration options and click **Configure**. Click **Close** once the configuration has succeeded.

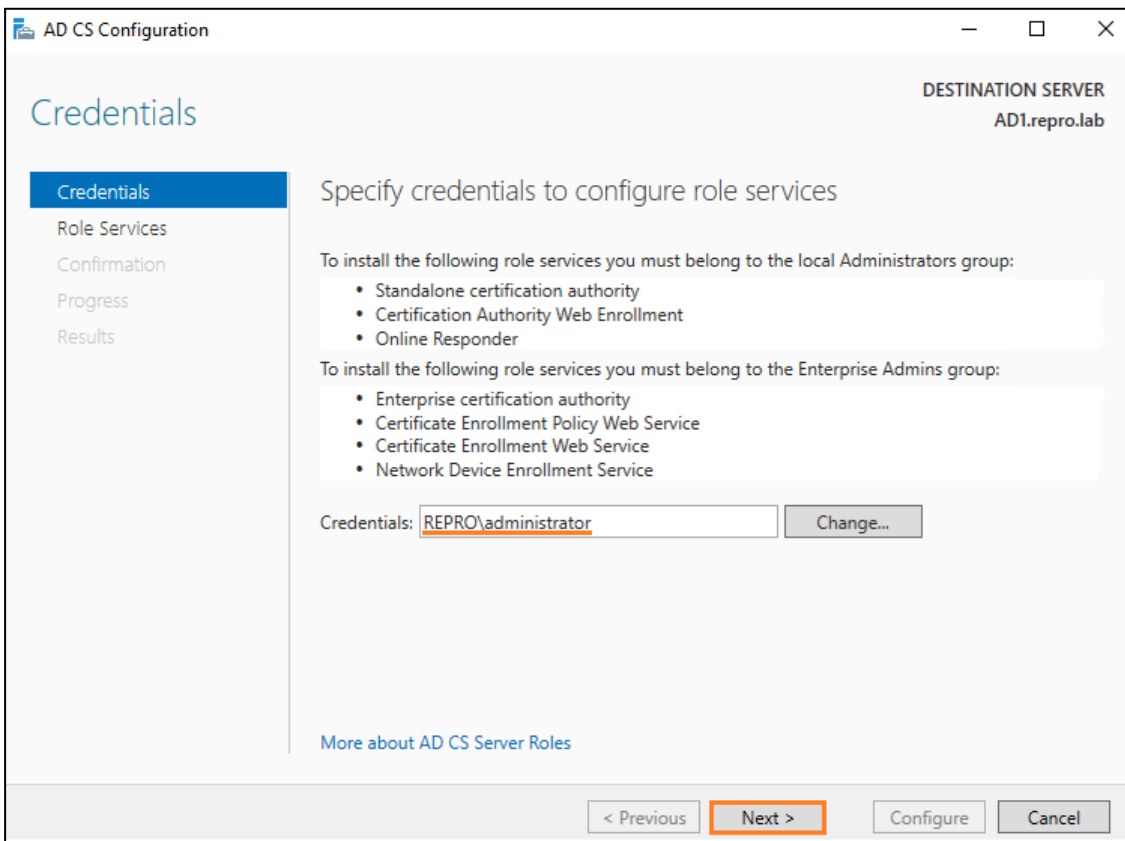


28. Click **Yes** when asked to configure additional role services.

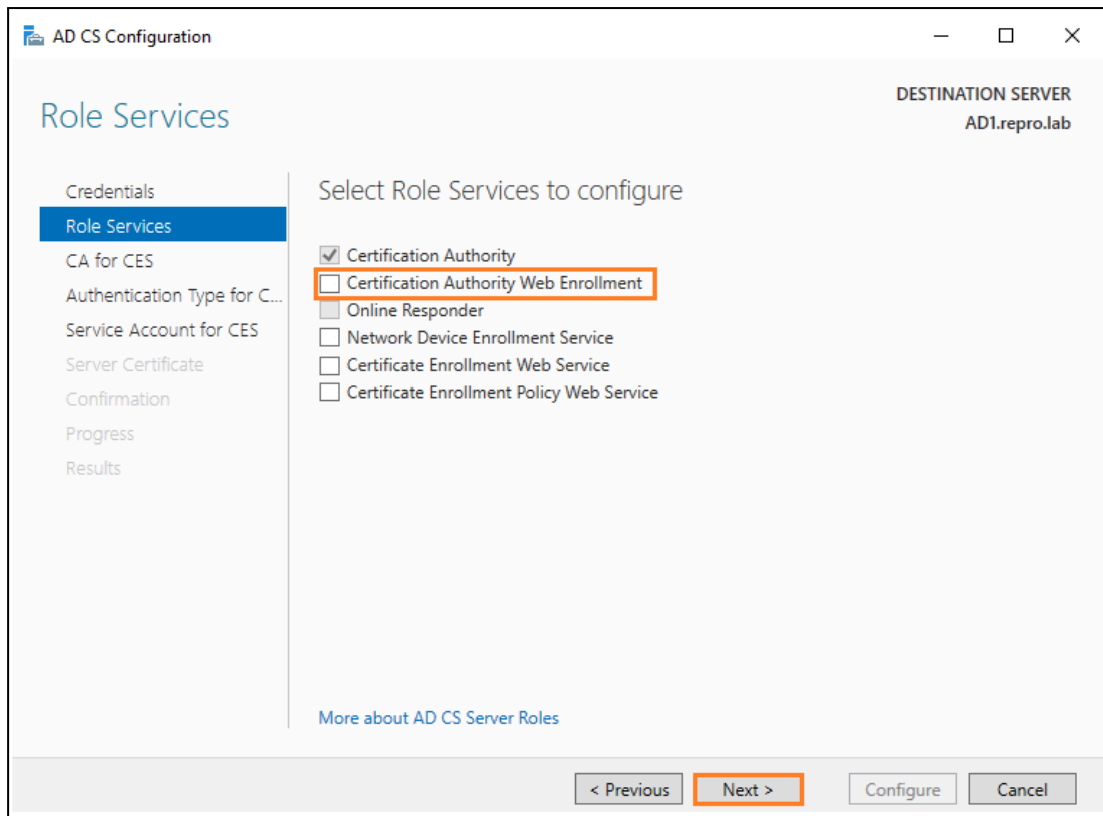




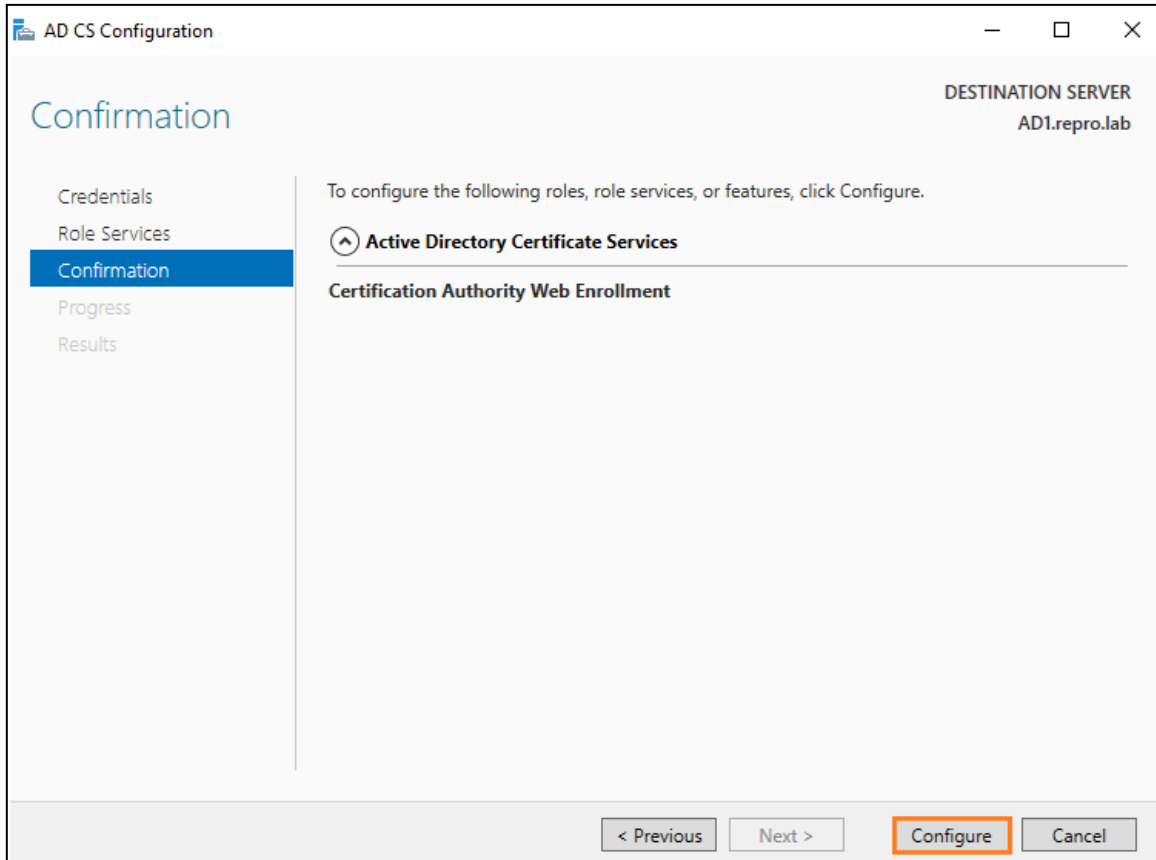
29. Confirm **REPRO\Administrator** or (**yourdomain\Administrator**) is listed in the Credentials field and click **Next**.



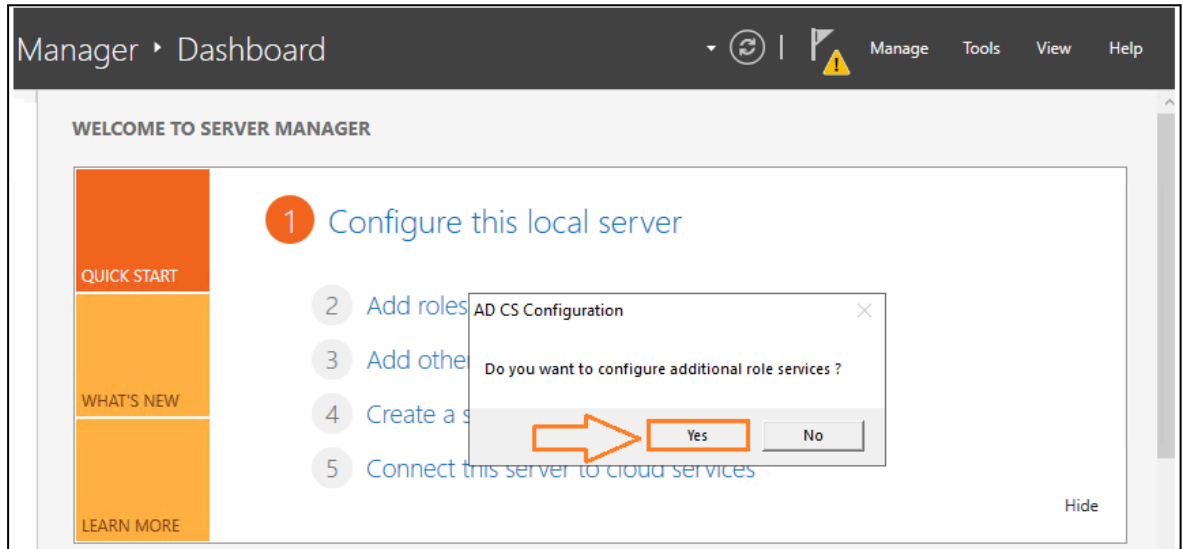
30. Tick the box next to **Certification Authority Web Enrollment** and click **Next**.



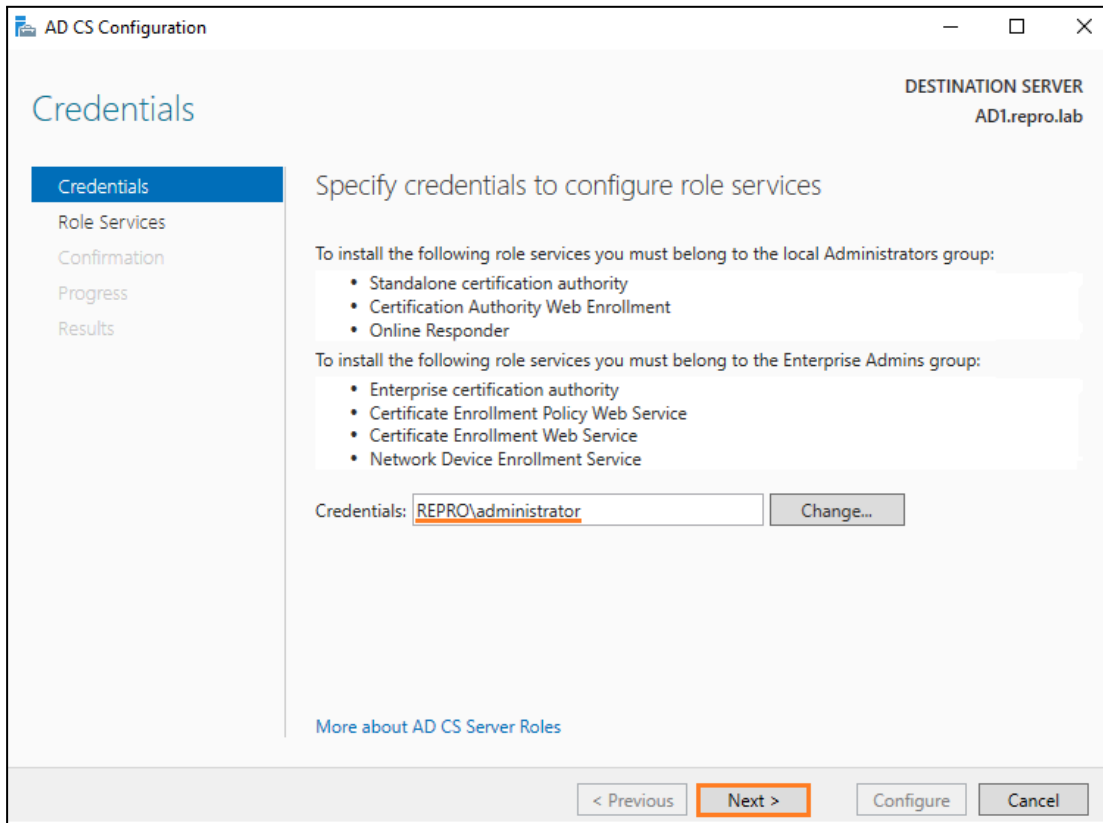
31. Click **Configure** on the Confirmation screen. Click **Close** once the configuration has succeeded.



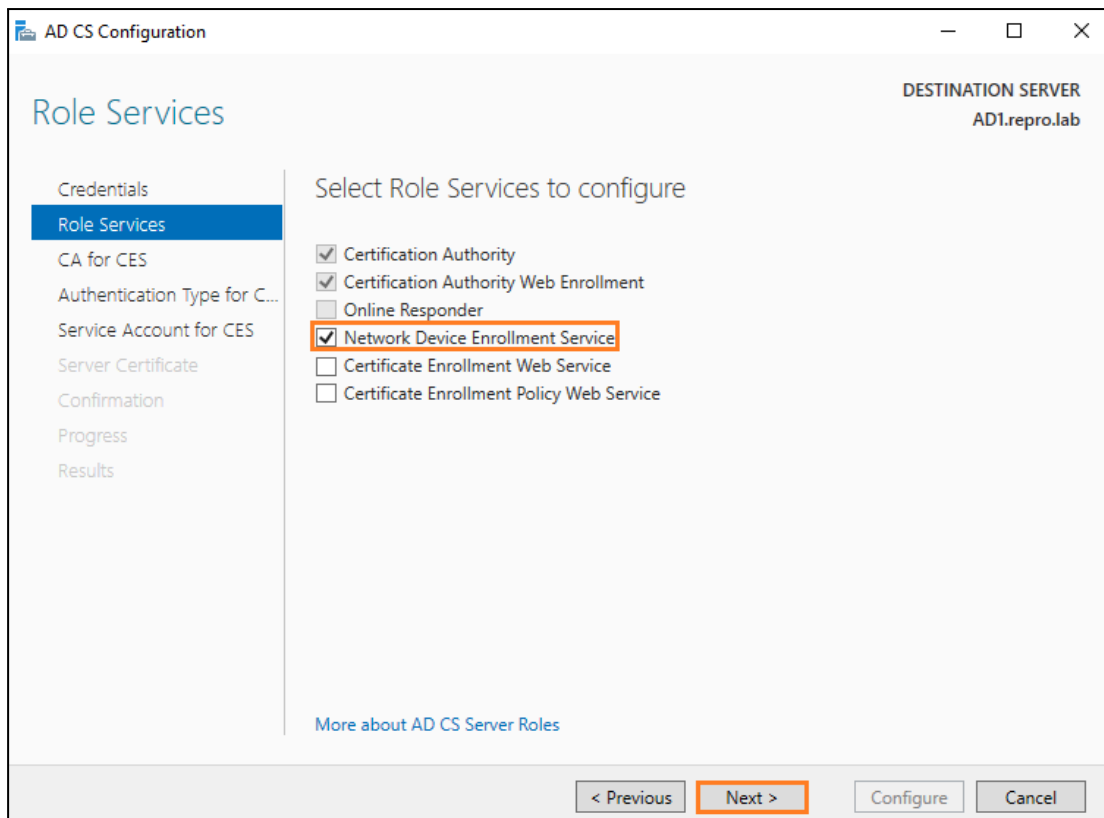
32. Click **Yes** when asked to configure additional role services.



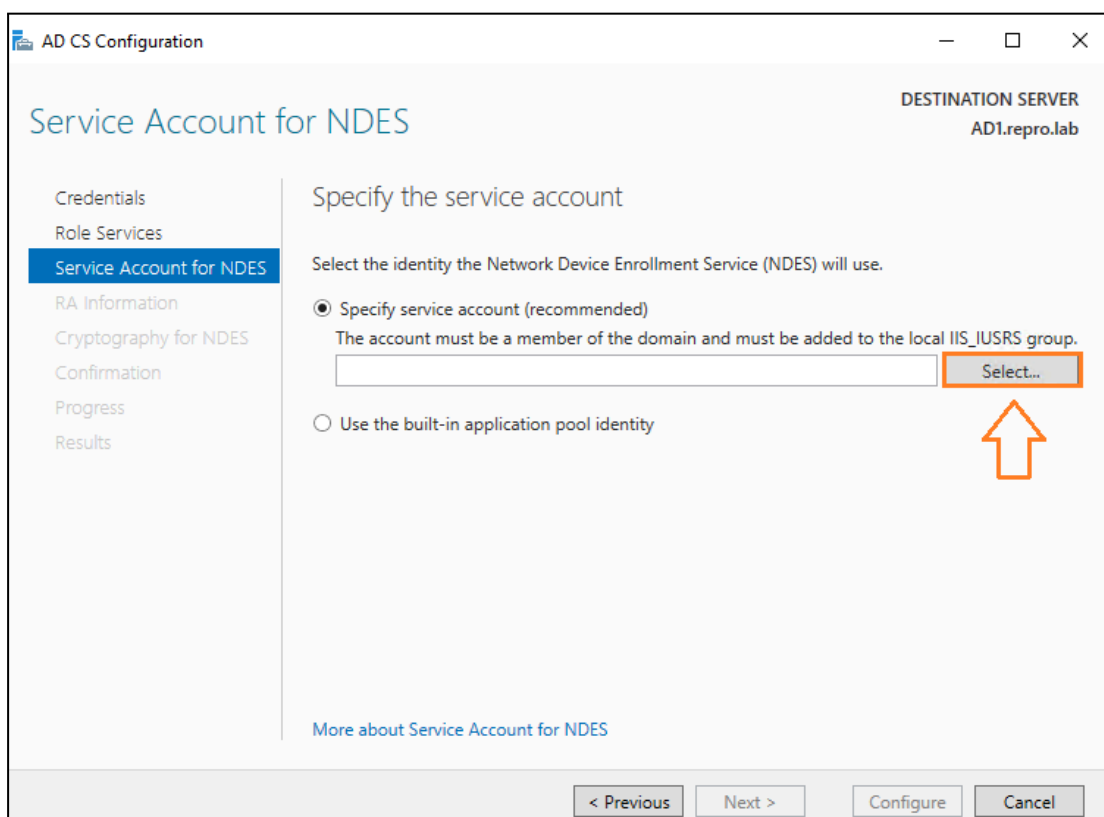
33. Confirm that **REPRO\Administrator** is listed in the Credentials field. Click **Next**.



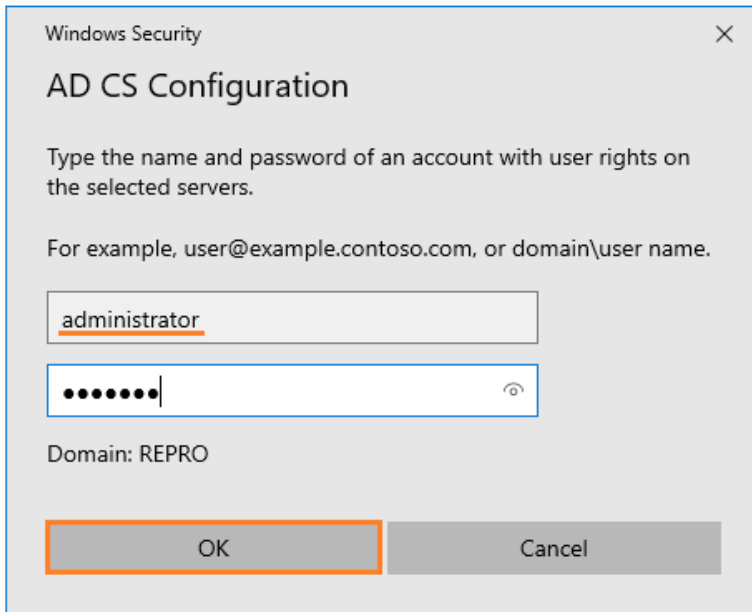
34. Tick the box next to **Network Device Enrollment Service** and click **Next**.



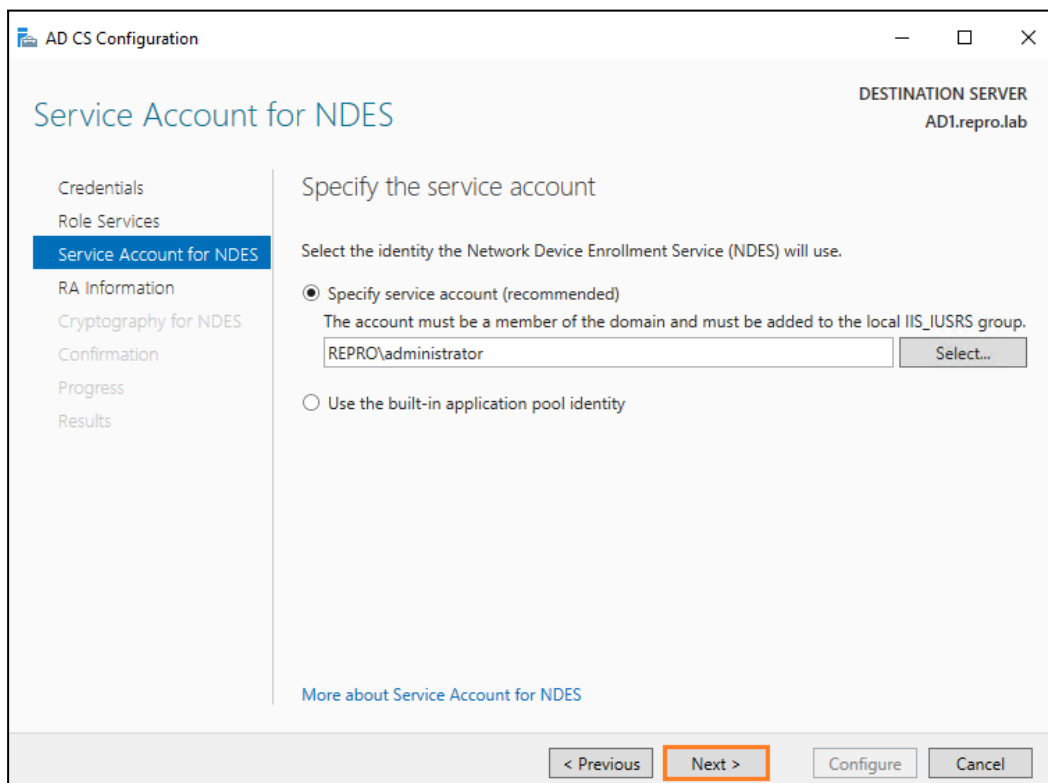
35. Click **Select...** when asked to Specify the service account.



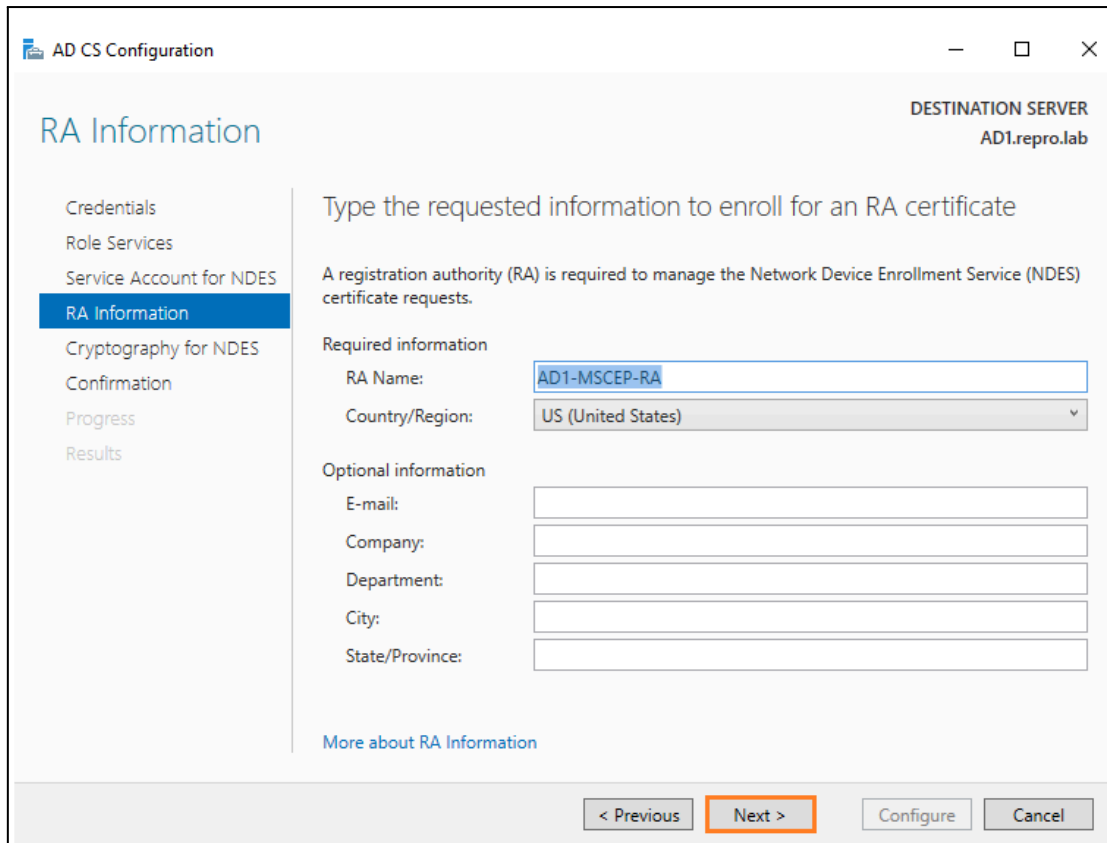
36. Enter **administrator** for the **Username** and **Your password** for the Password and click **OK**



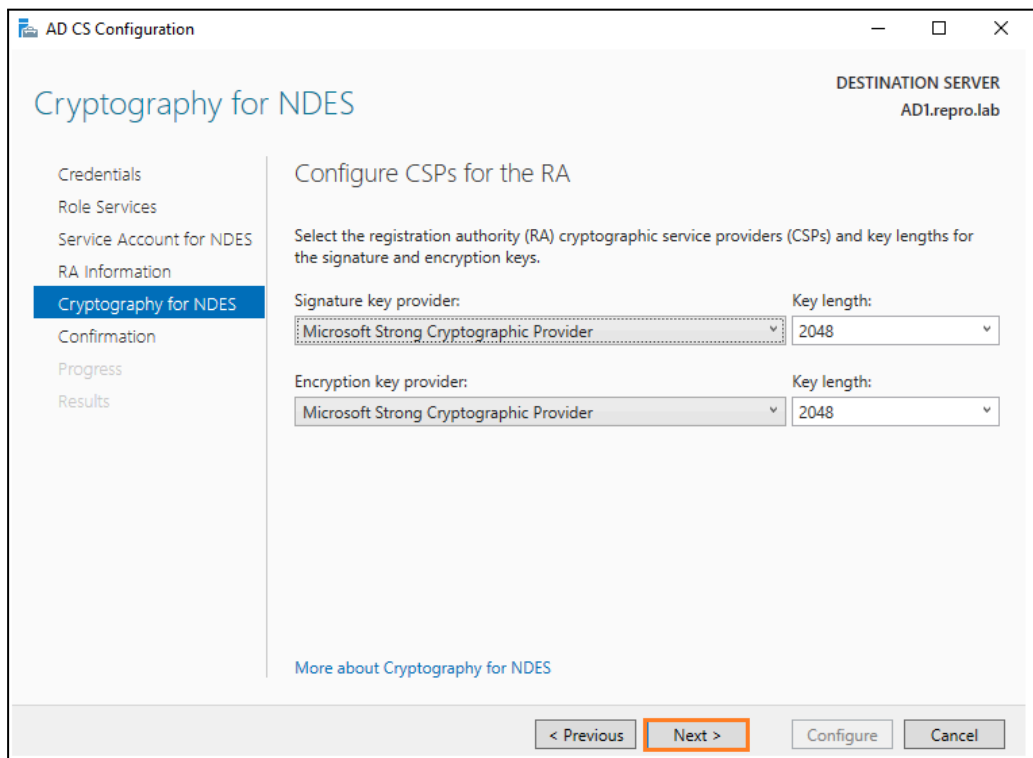
37. Confirm **REPRO\Administrator** is populated in the service account field and click **Next**.



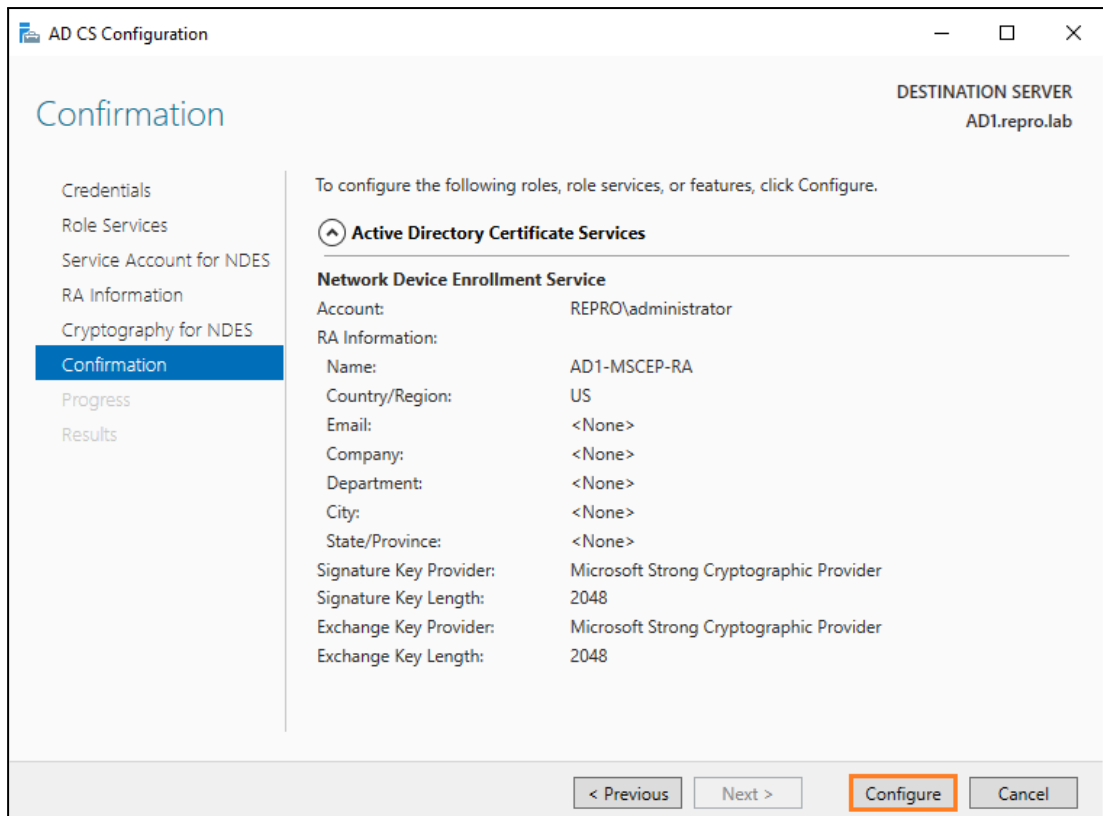
38. Leave the RA Information at the defaults and click **Next**.



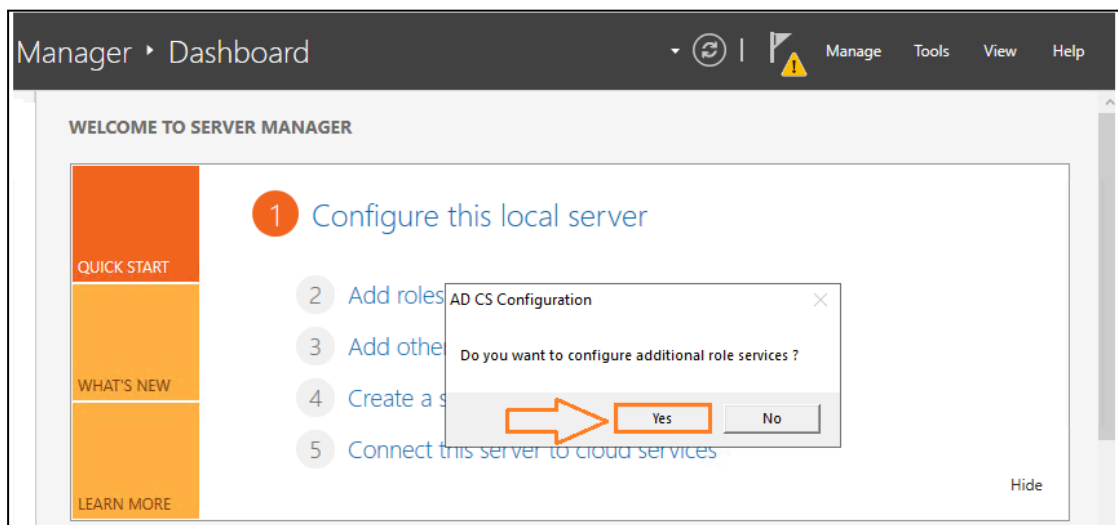
39. Leave the CSPs for the RA information at the defaults and click **Next**.



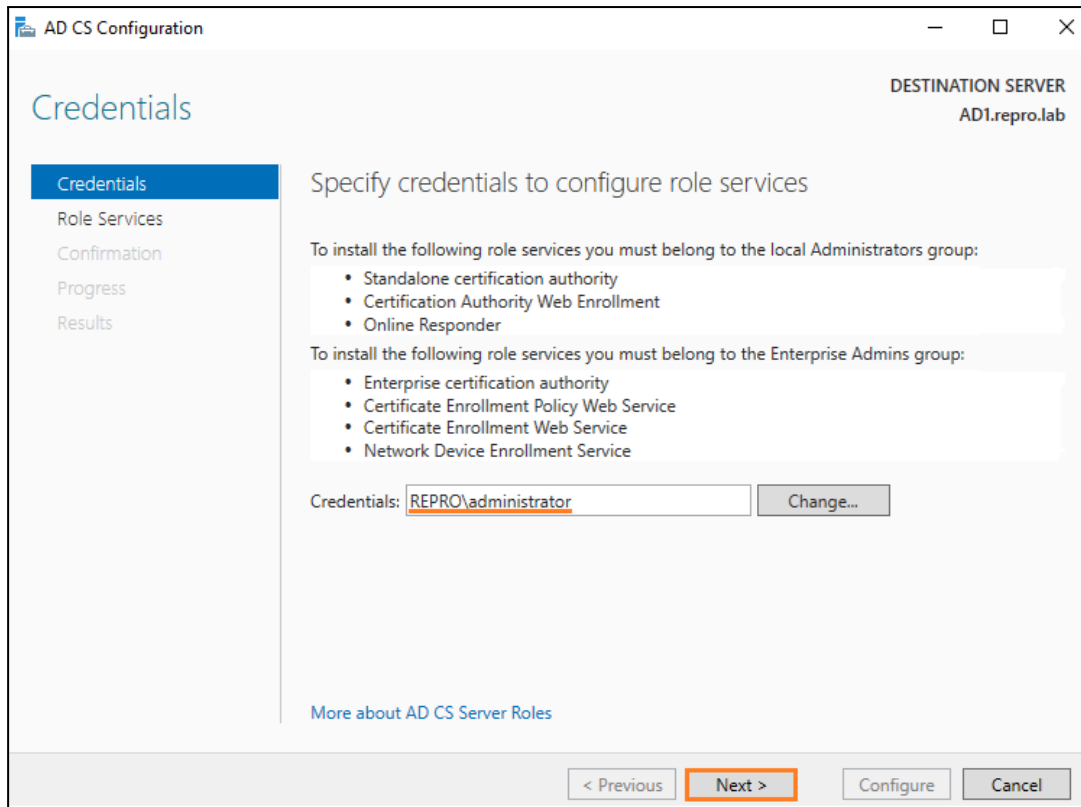
40. Review the configuration settings and click **Configure**. Click **Close** once the configuration has succeeded.



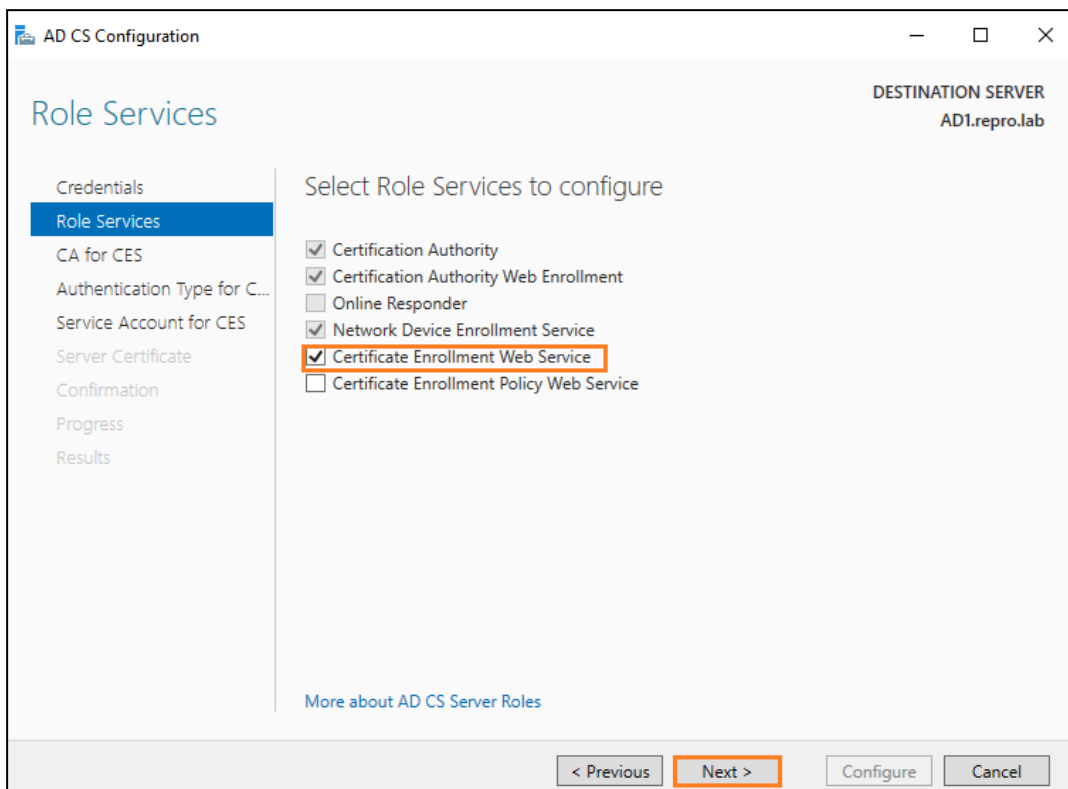
41. Click **Yes** when asked to configure additional role services.



42. Confirm **REPRO\Administrator** or (yourdomain\Administrator) is listed in the **Credentials** field and click **Next**.

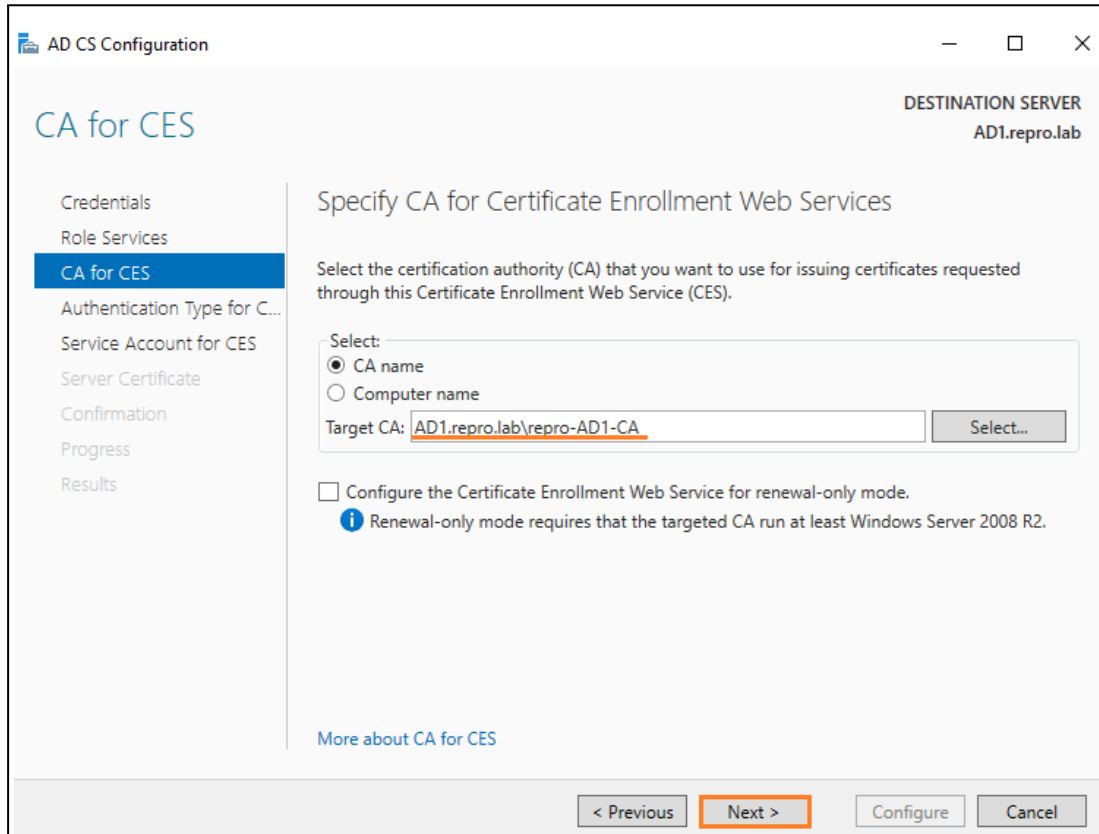


43. Tick the box next to **Certificate Enrollment Web Service** and click **Next**.

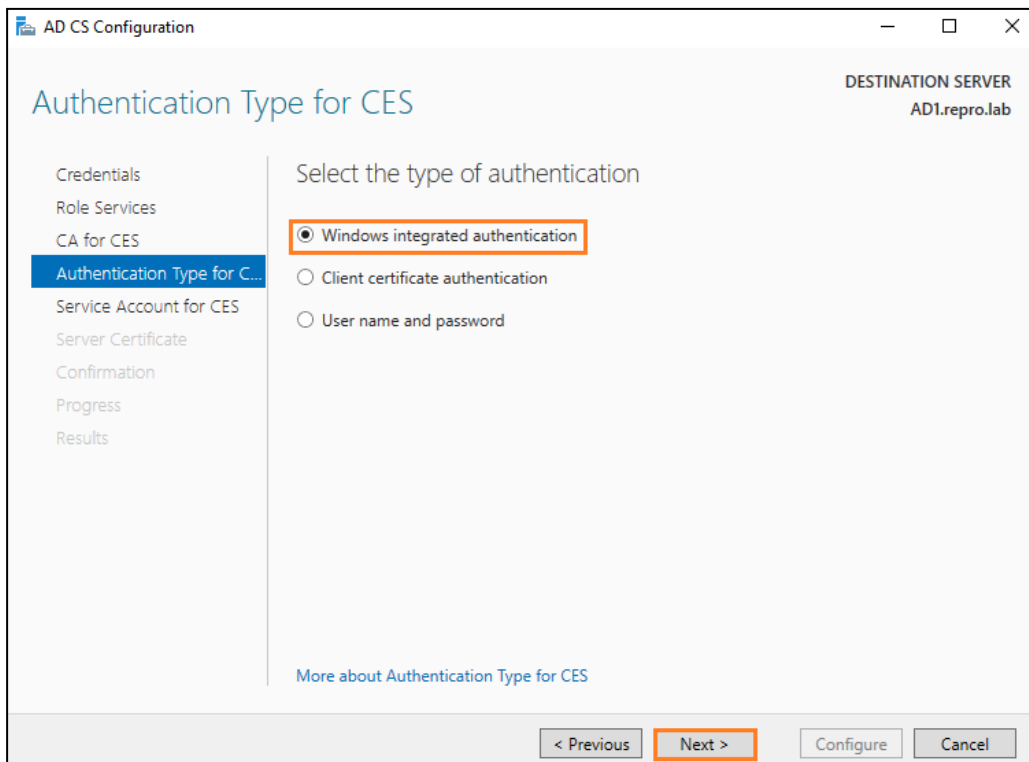




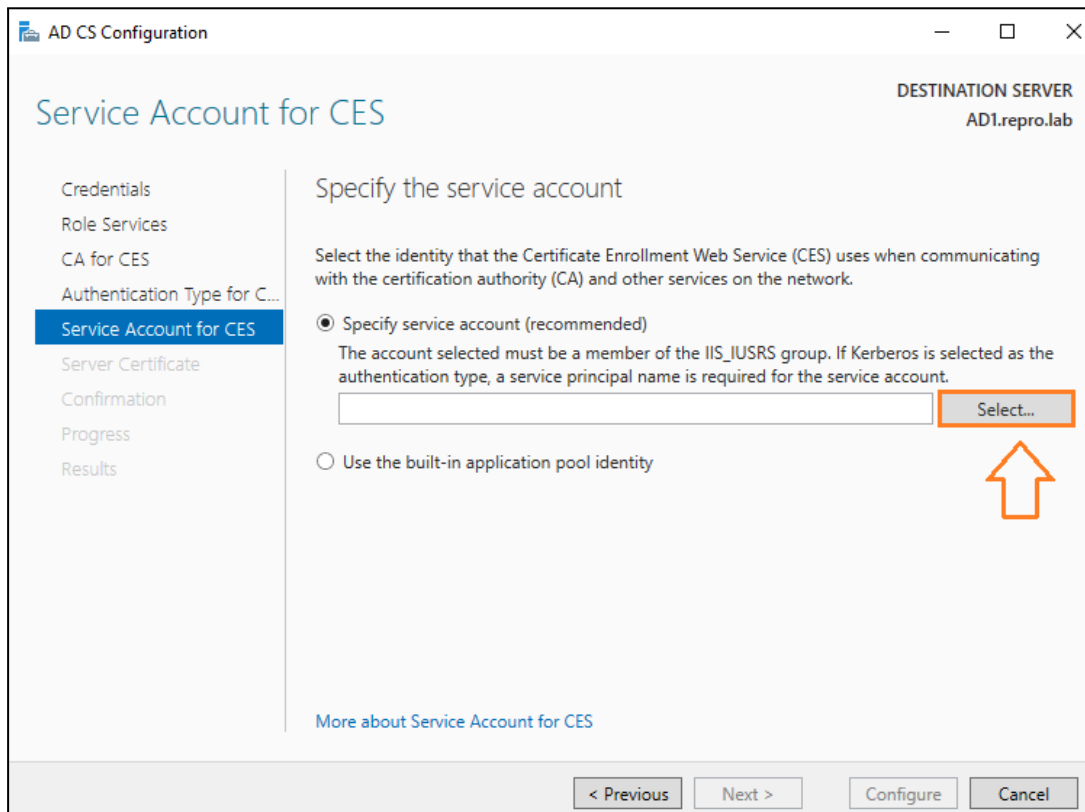
44. Confirm the **CA name** is selected and the Target CA field is filled. Click **Next**.



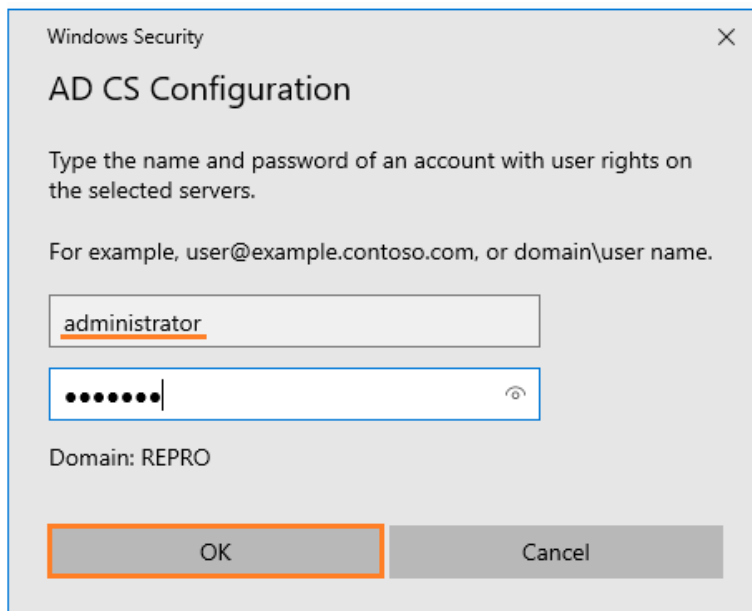
45. Confirm **Windows integrated authentication** is selected and click **Next**.



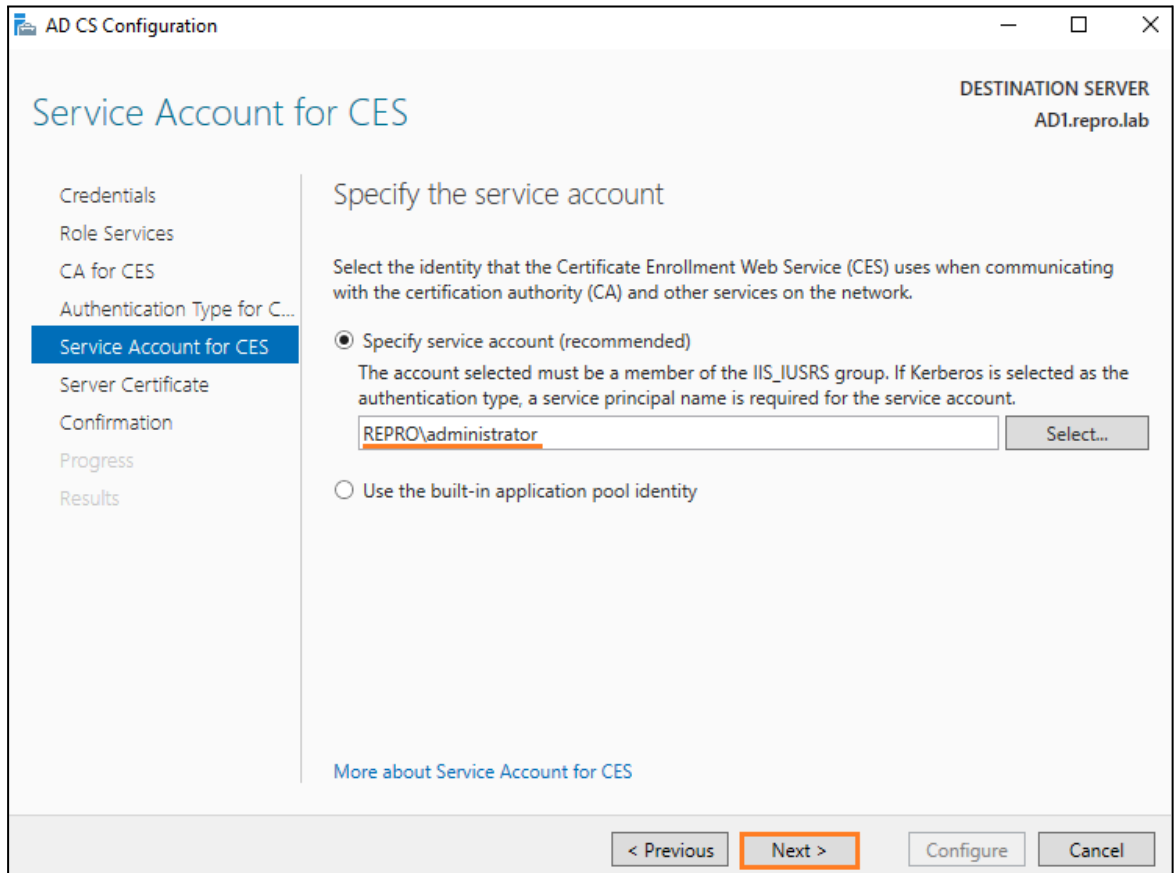
46. Click **Select...** when asked to Specify the service account.



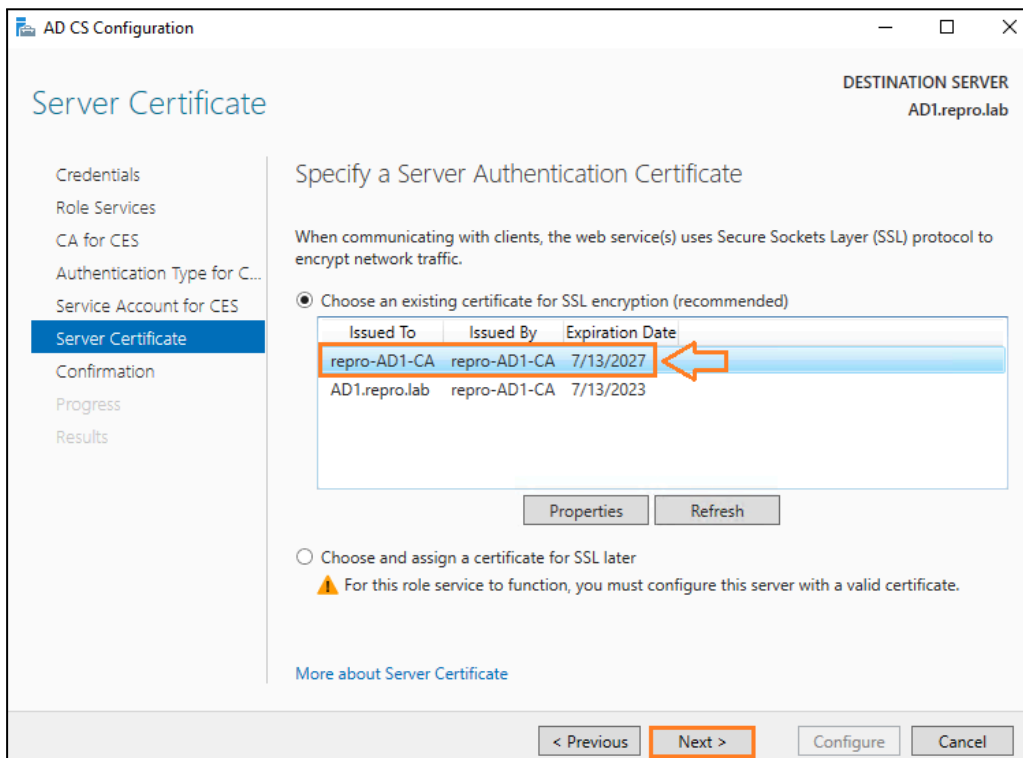
47. Enter **administrator** for the **Username** and **Your Password** for the Password and click **OK**.



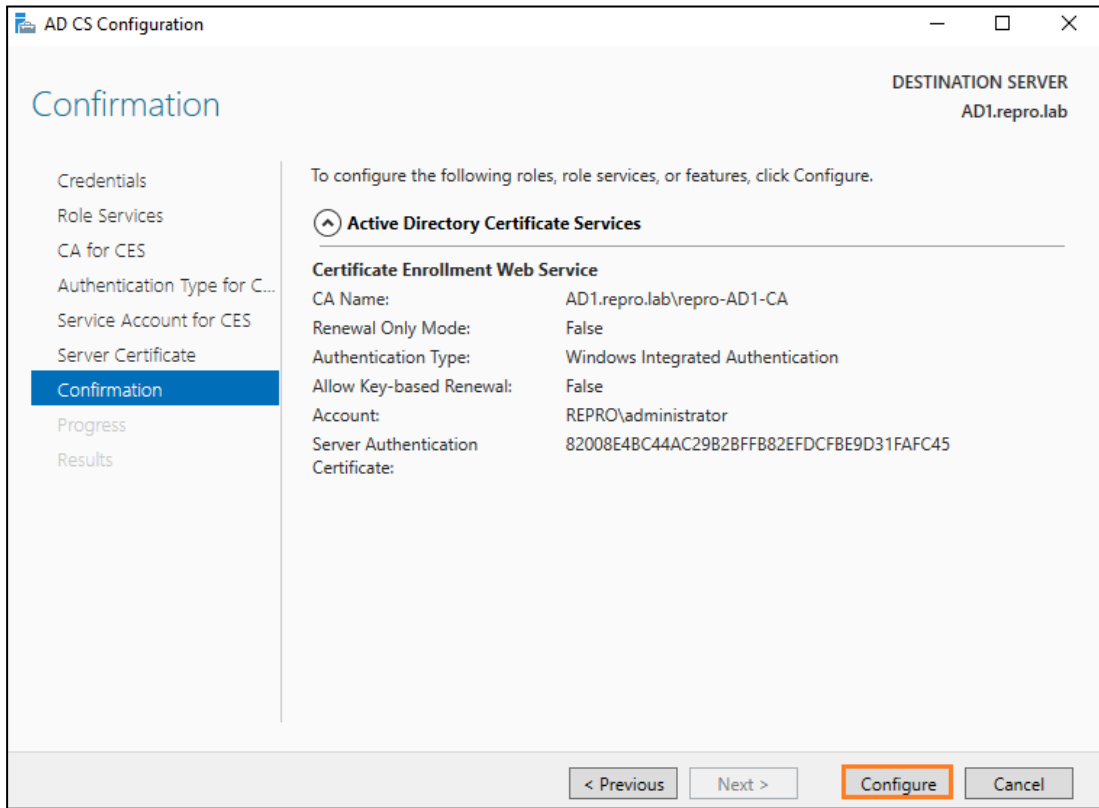
48. Confirm **REPRO\Administrator** or (**yourdomain\Administrator**) is populated in the service account field and click **Next**.



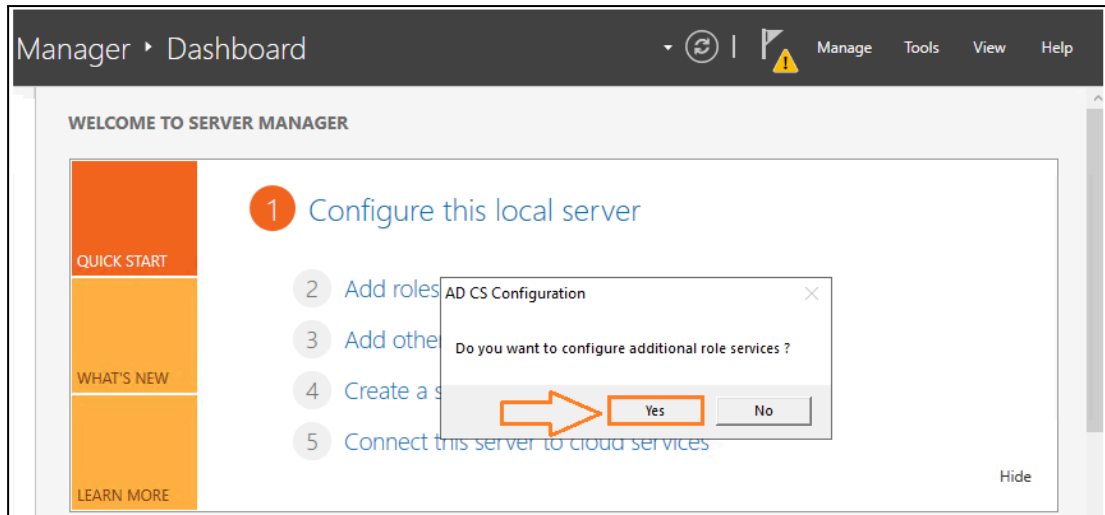
49. Confirm **Choose an existing certificate for SSL encryption (recommended)** is selected, highlight **repro-AD1-CA** in the field, and click **Next**.



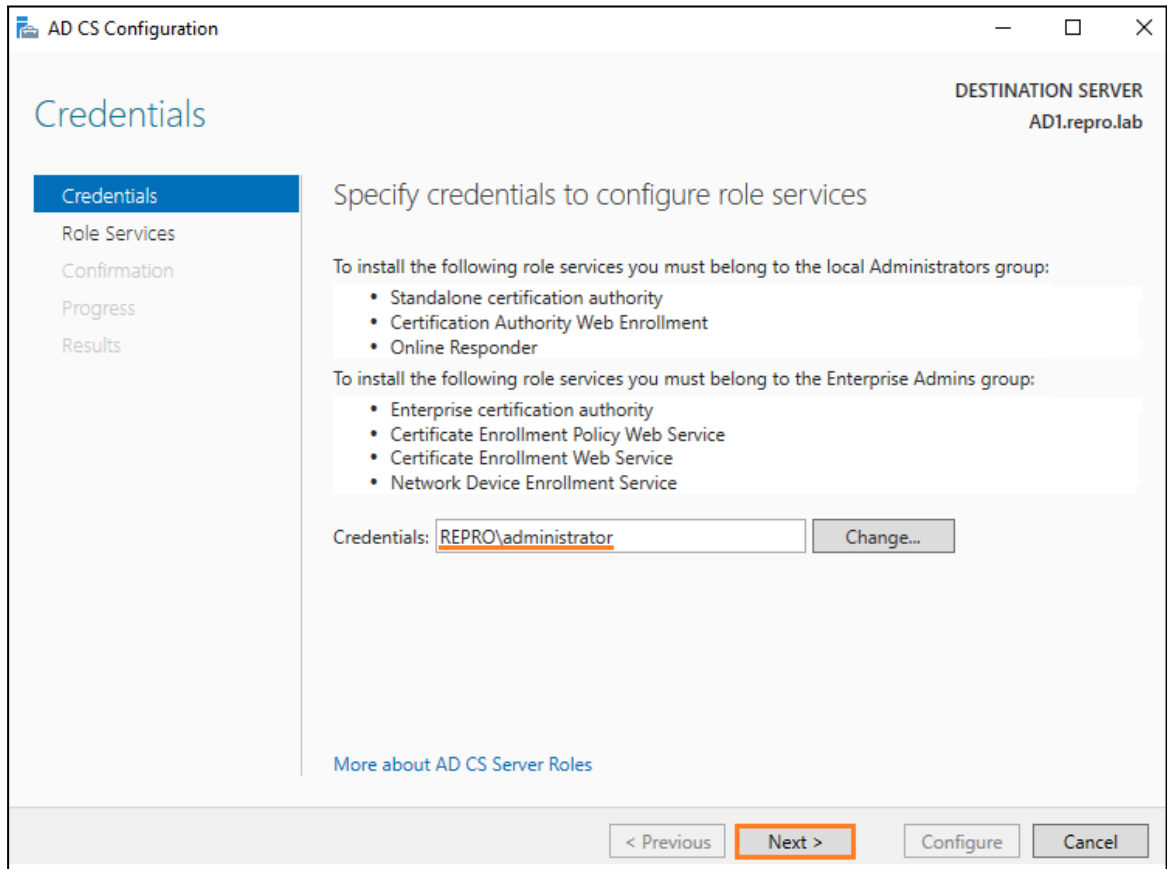
50. Review the configuration settings and click **Configure**. Click **Close** once the configuration has succeeded.



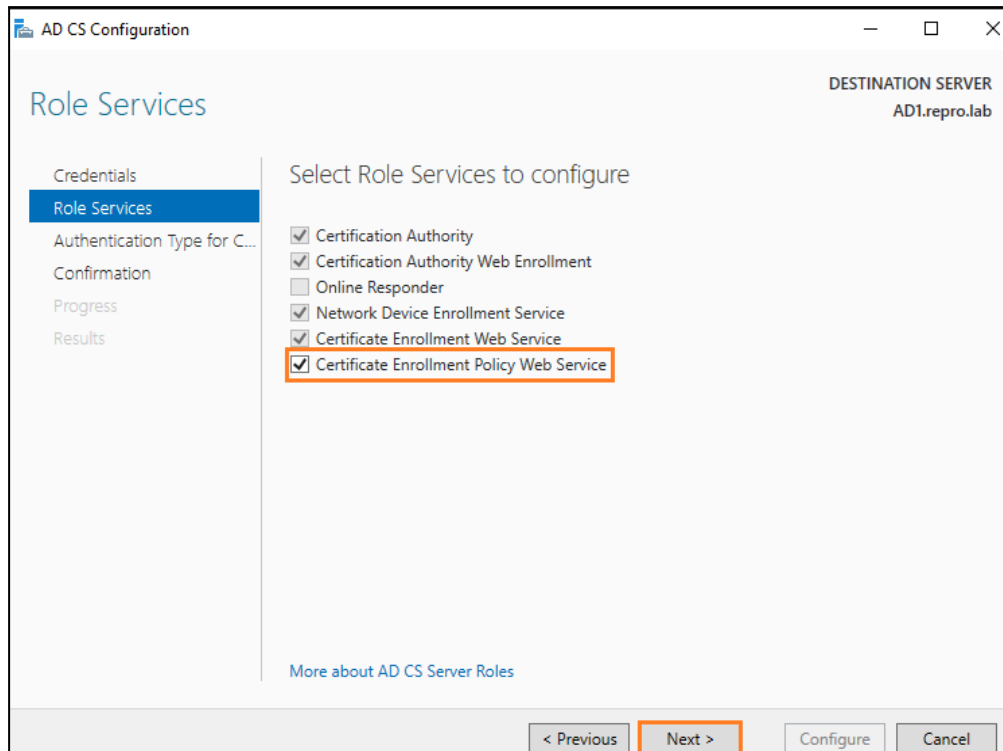
51. Click **Yes** when asked to configure additional role services.



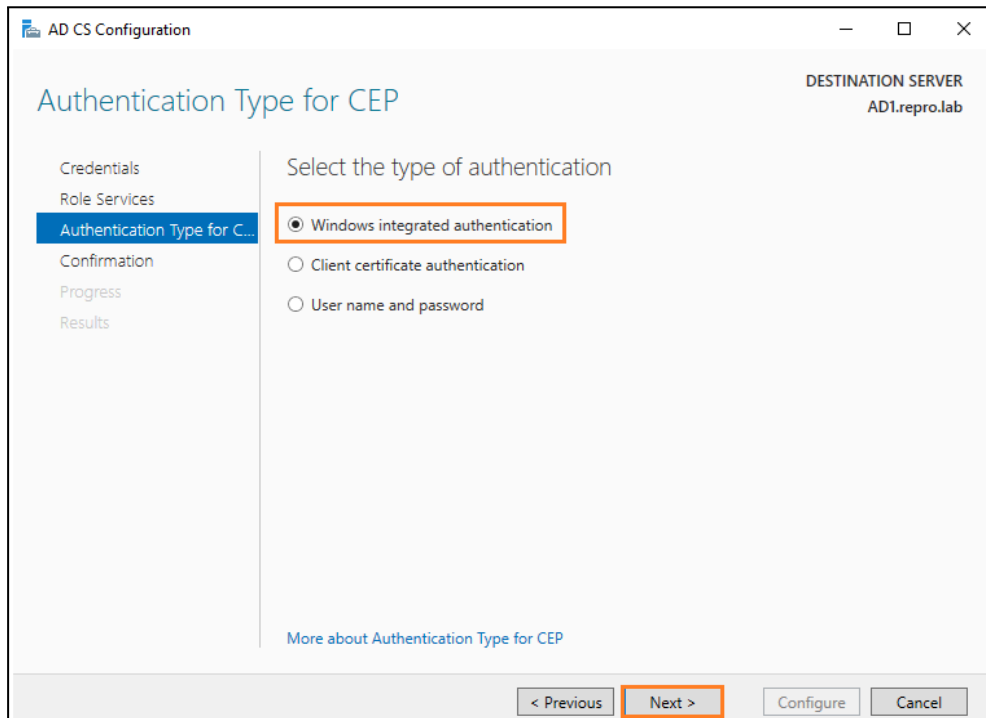
52. Confirm **REPRO\Administrator** or (yourdomain\Administrator) is listed in the **Credentials** field and click **Next**.



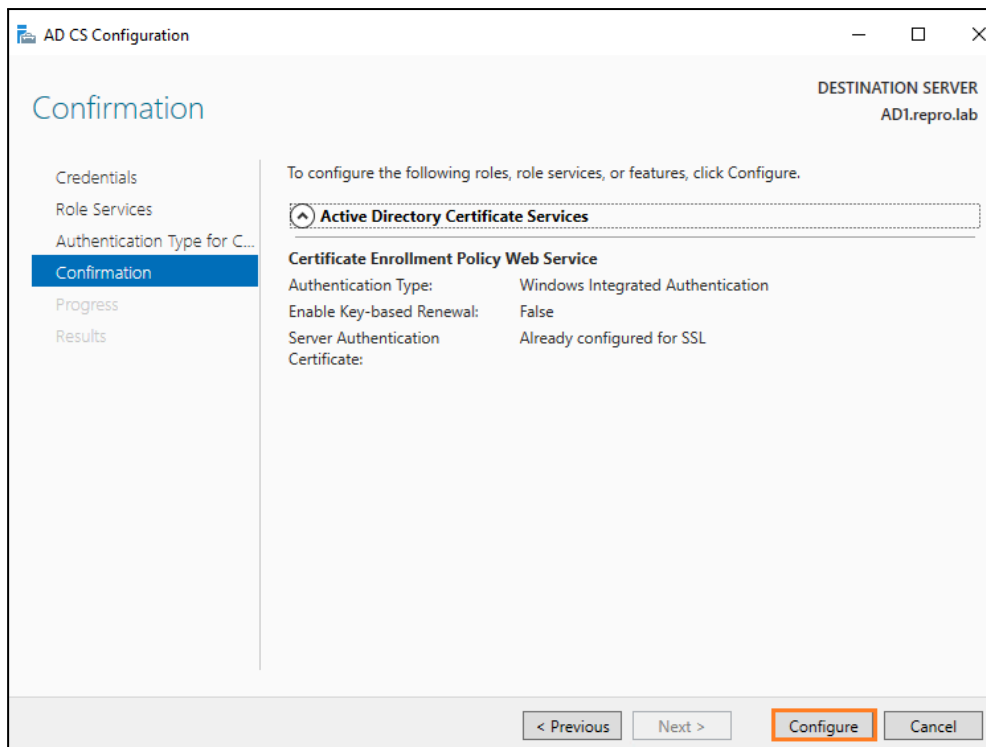
53. Tick the box next to **Certificate Enrollment Policy Web Service** and click **Next**.



54. Confirm **Windows integrated authentication** is selected and click **Next**.



55. Review the configuration settings and click **Configure**. Click **Close** once the configuration has succeeded. Click **Close** to close the Add Roles and Features Wizard.



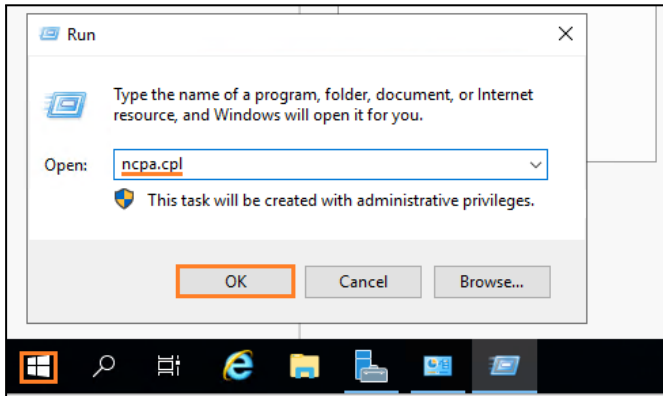
Active Directory Certificate Services is now installed, and the Root Certification Authority is available to complete SSL certificate requests.

## Configuring Delivery Controller, Storefront, and Studio

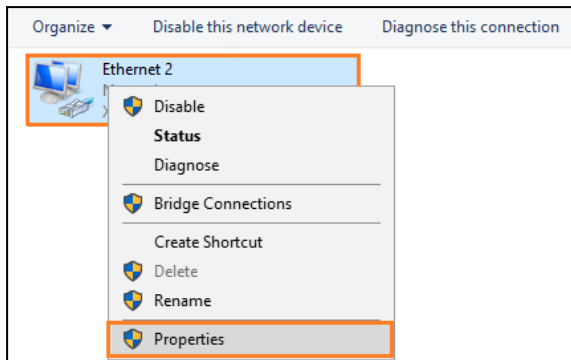
### Second VM: Windows Server 2019

**NOTE:** You will need to first join this VM to the Domain controller created in the previous steps.

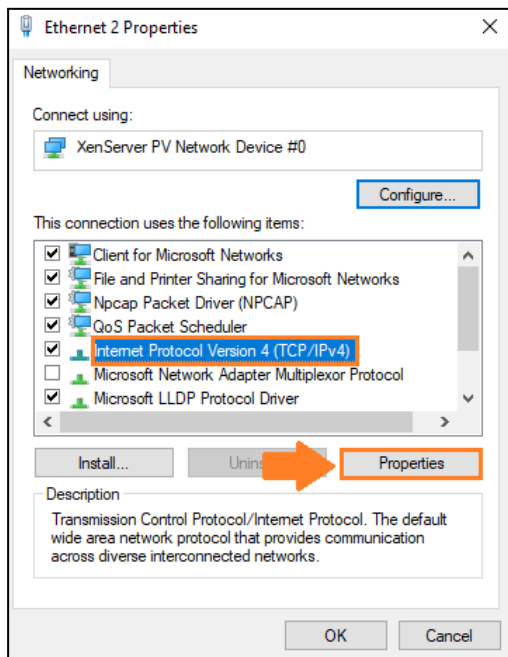
1. From the start menu, type/select **Run** and then type **ncpa.cpl**. Click **OK**.



2. Right-click the **Ethernet** connection and choose **Properties**.

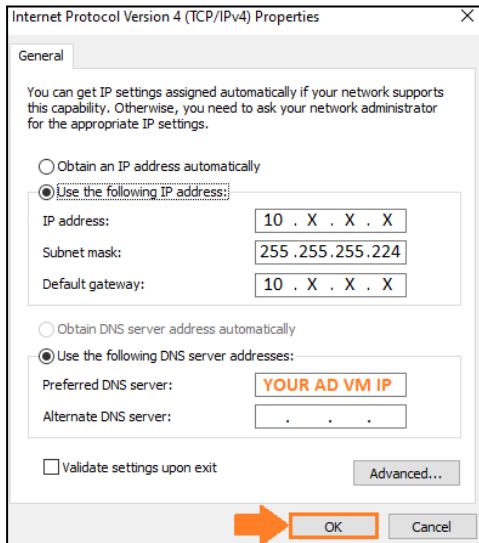


3. On the Ethernet Properties window, highlight **Internet Protocol Version 4 (TCP/IPv4)**. and click **Properties**.

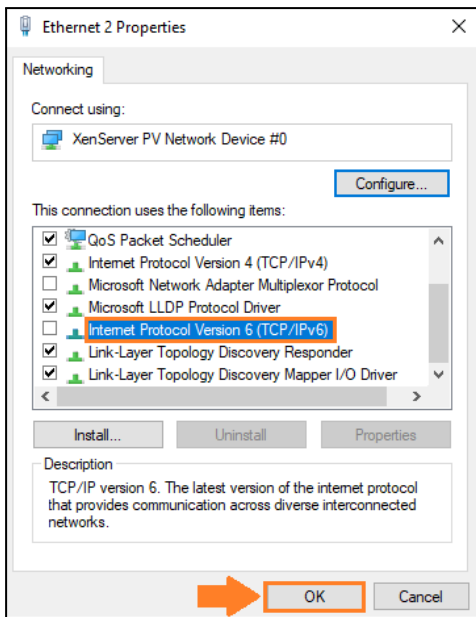


4. **Set your IP address**, along with **the subnet mask** and **default gateway** according to your network info.

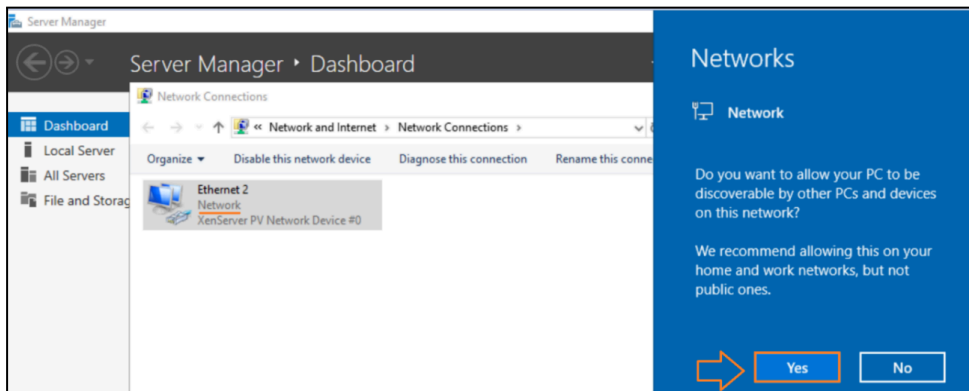
For **DNS**, please set your **WINDOWS SERVER AD IP**. Your Windows Server AD will act as DNS for all your VMs going forward.



5. Uncheck **Internet Protocol Version 6**, and Click **OK**.

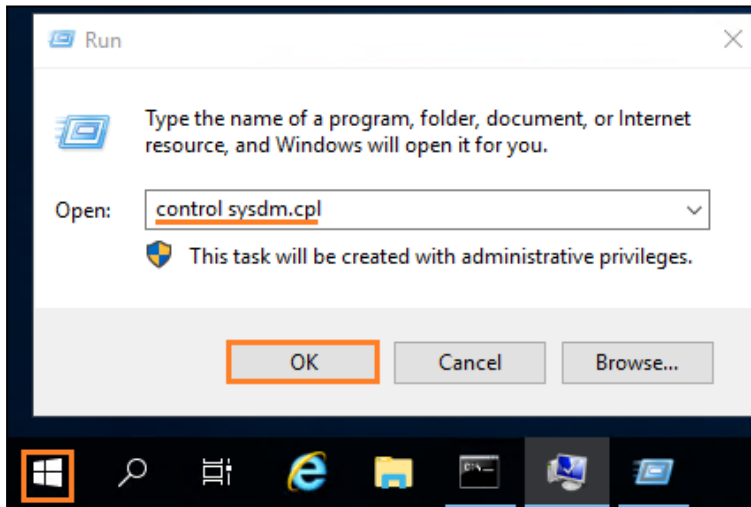


6. Select **Yes**. Your network is configured.

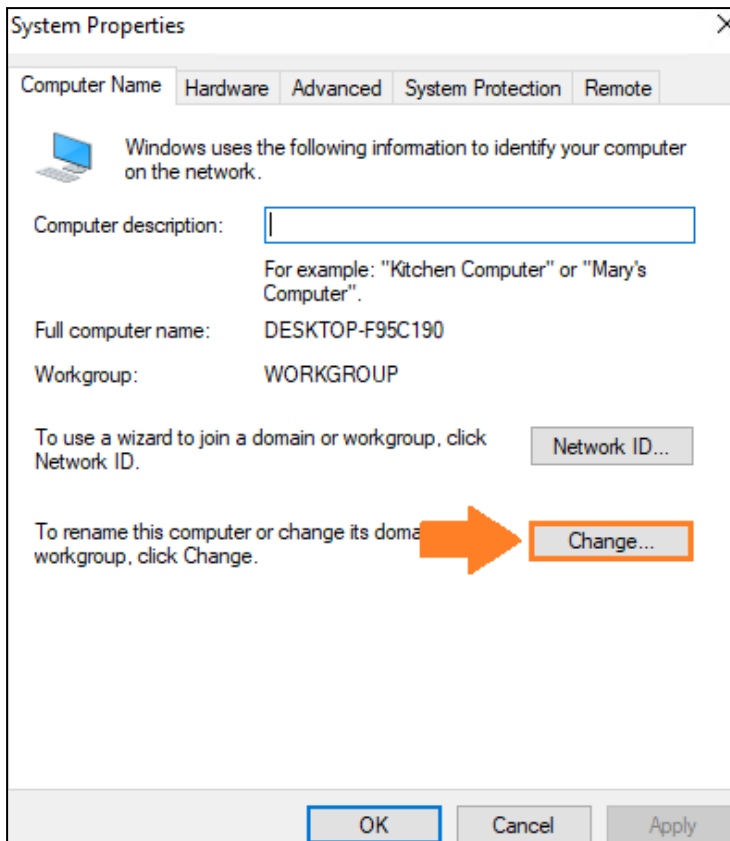




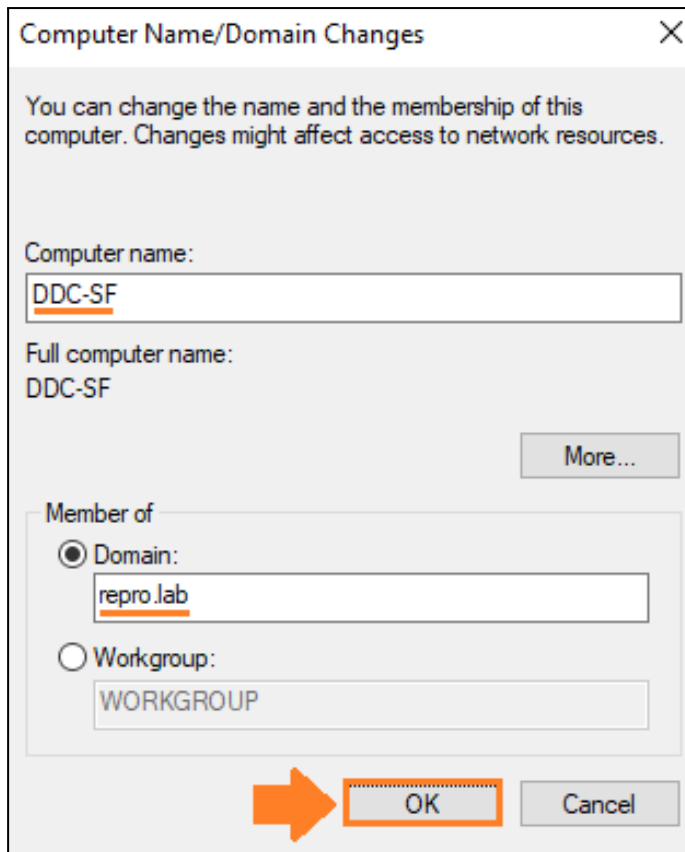
7. Confirm you can ping your local domain (repro.lab) from the DDC/SF VM.
8. Go **Run** and type **control sysdm.cpl**.



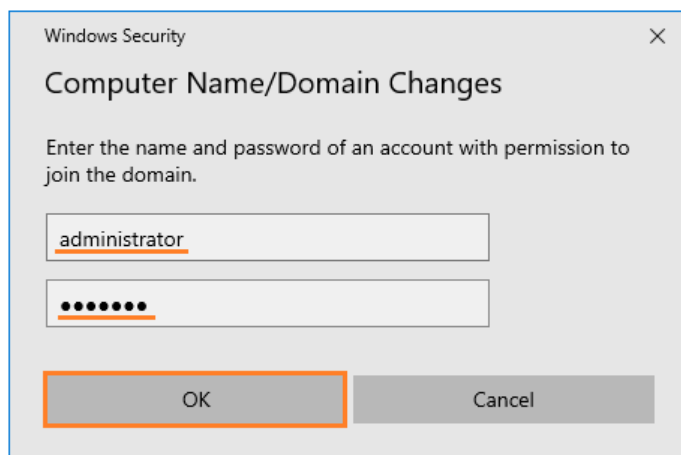
9. Click **Change**.



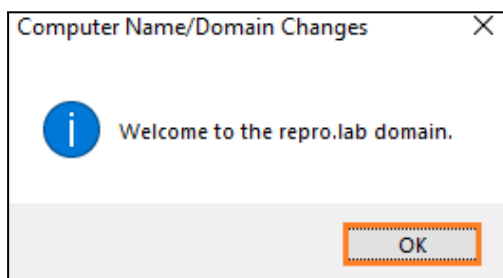
10. Change the VM name to **“DDC-SF”**, select **“domain”**, type your **domain name (repro.lab)**, and click **OK**.



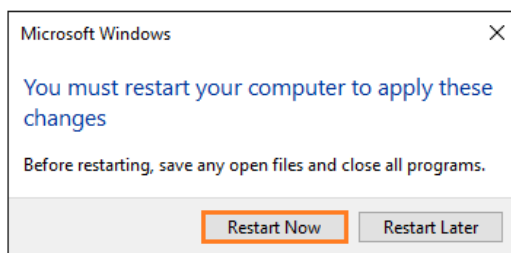
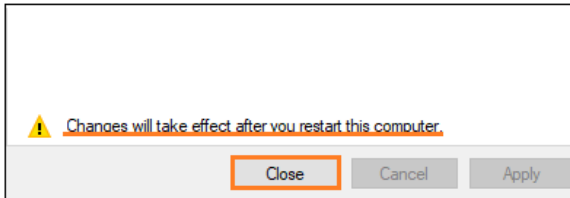
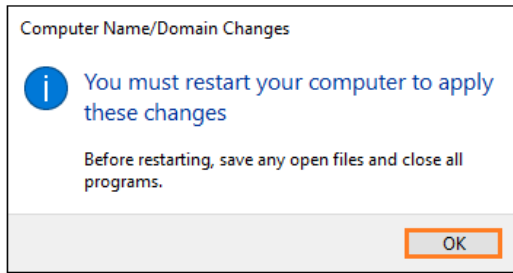
11. Enter your administrator credentials and click **OK**.



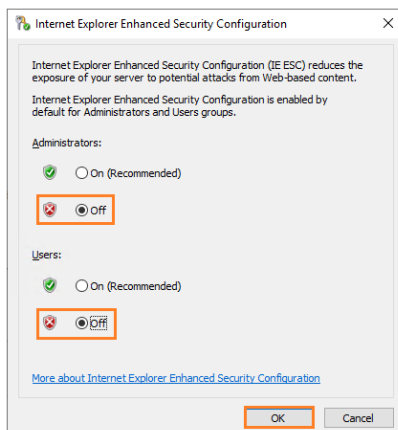
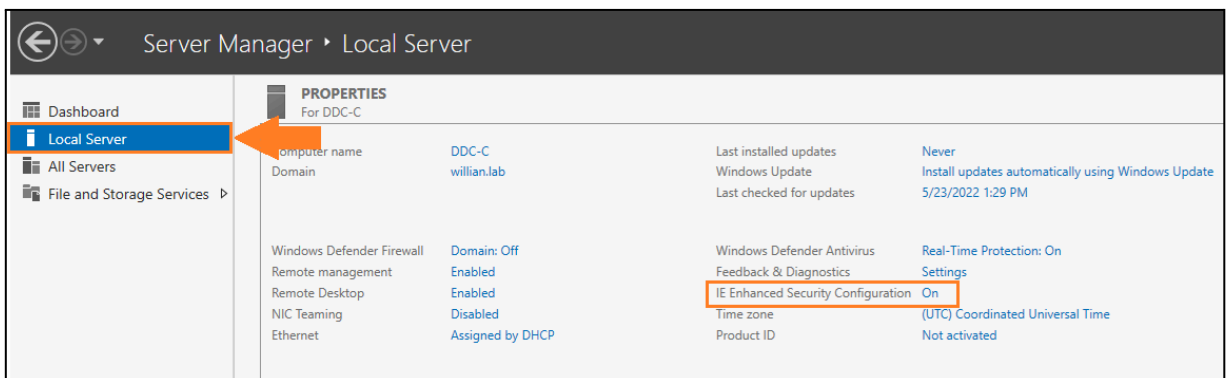
12. Click **OK**. The machine has joined the domain.



13. Click **OK**, **Close**, and **restart now** as requested.

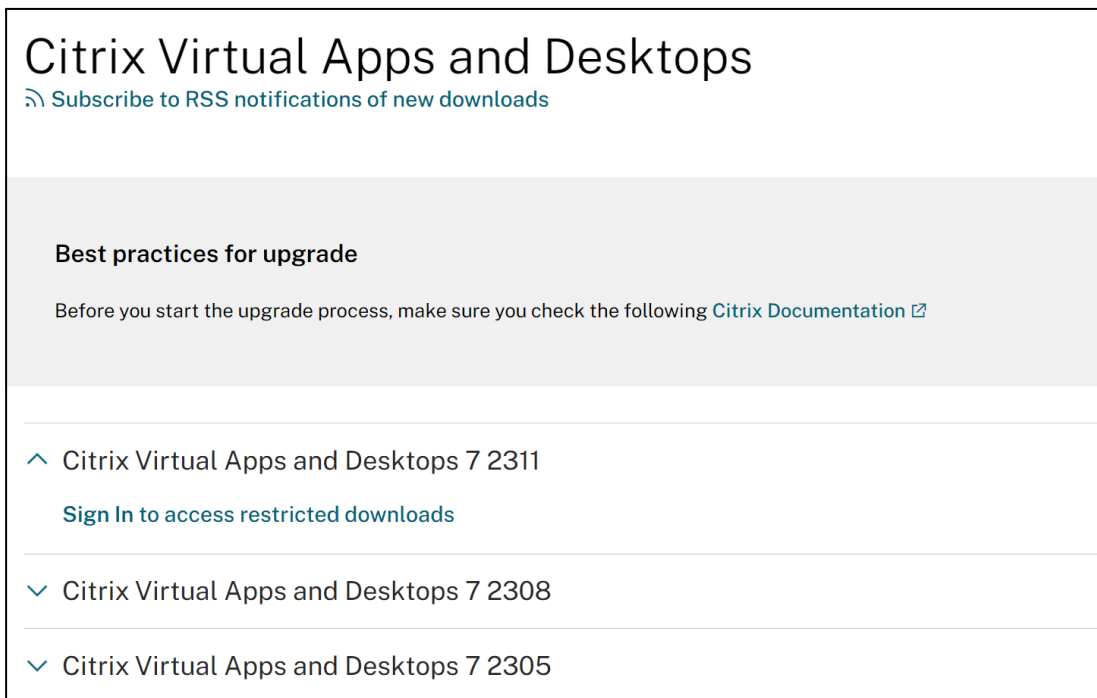


14. Connect again to your VM, click **Local Server**, and set the **IE Enhanced Security Configuration** to **Off**.



## Launching the CVAD installer

1. From your **DDC-SF VM**, open your browser and navigate to <https://www.citrix.com/downloads/> to download the CVAD installer iso.

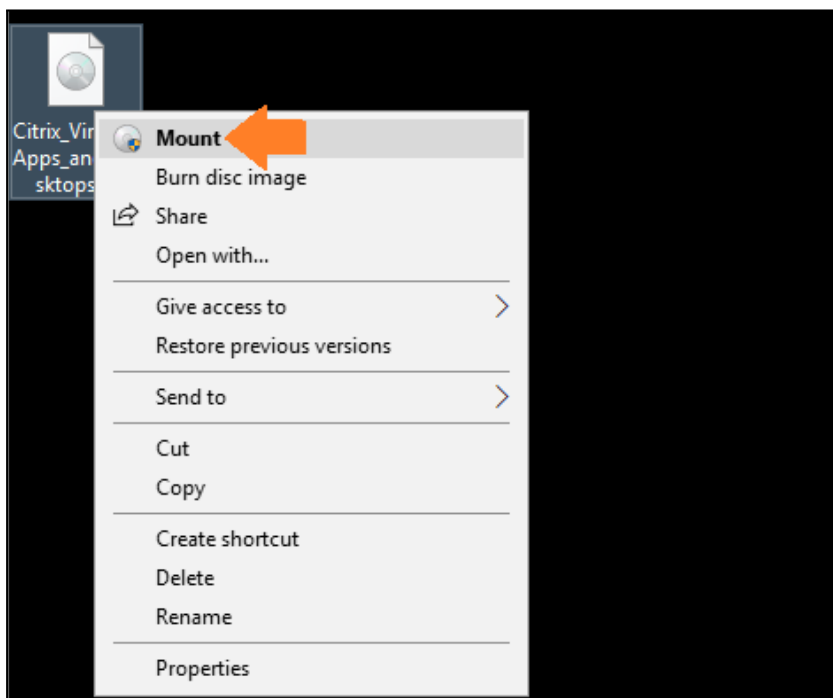


---

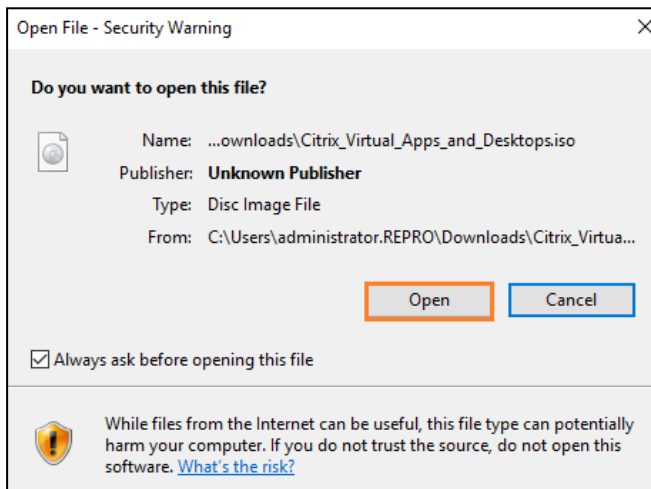
NOTE: We will cover the Citrix Virtual and Desktops 7 2003 version.

---

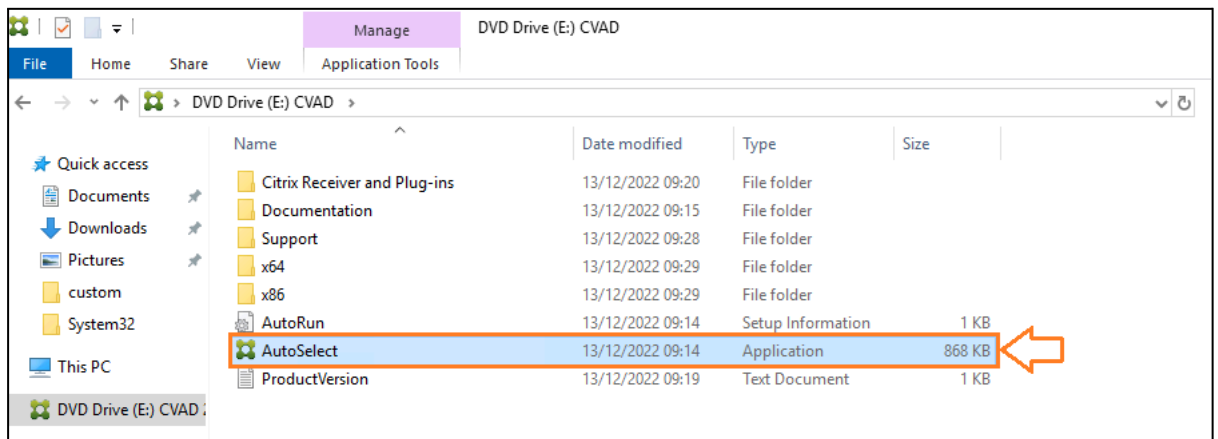
2. Once the image is downloaded, **right-click** and **mount** the image.



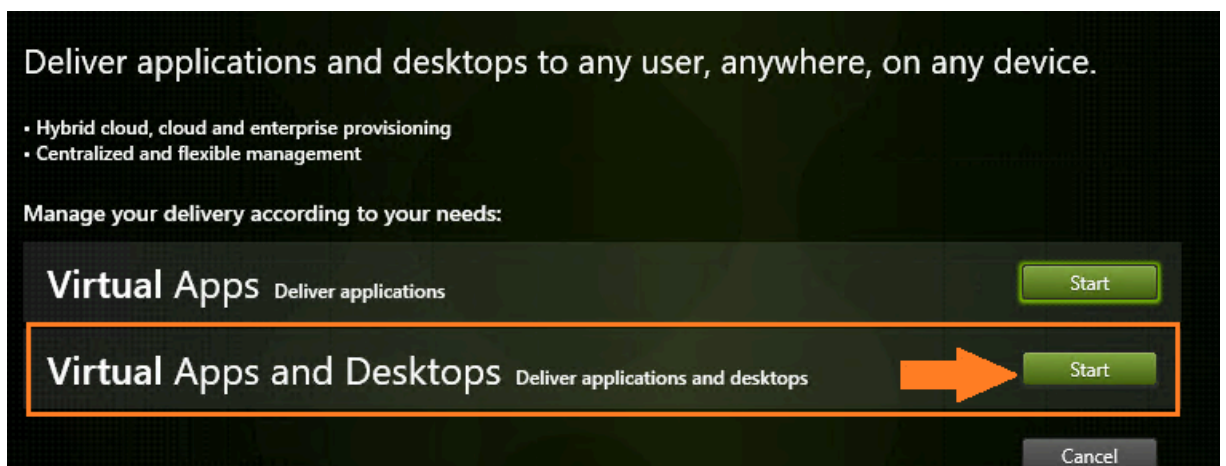
3. Click **Open**.



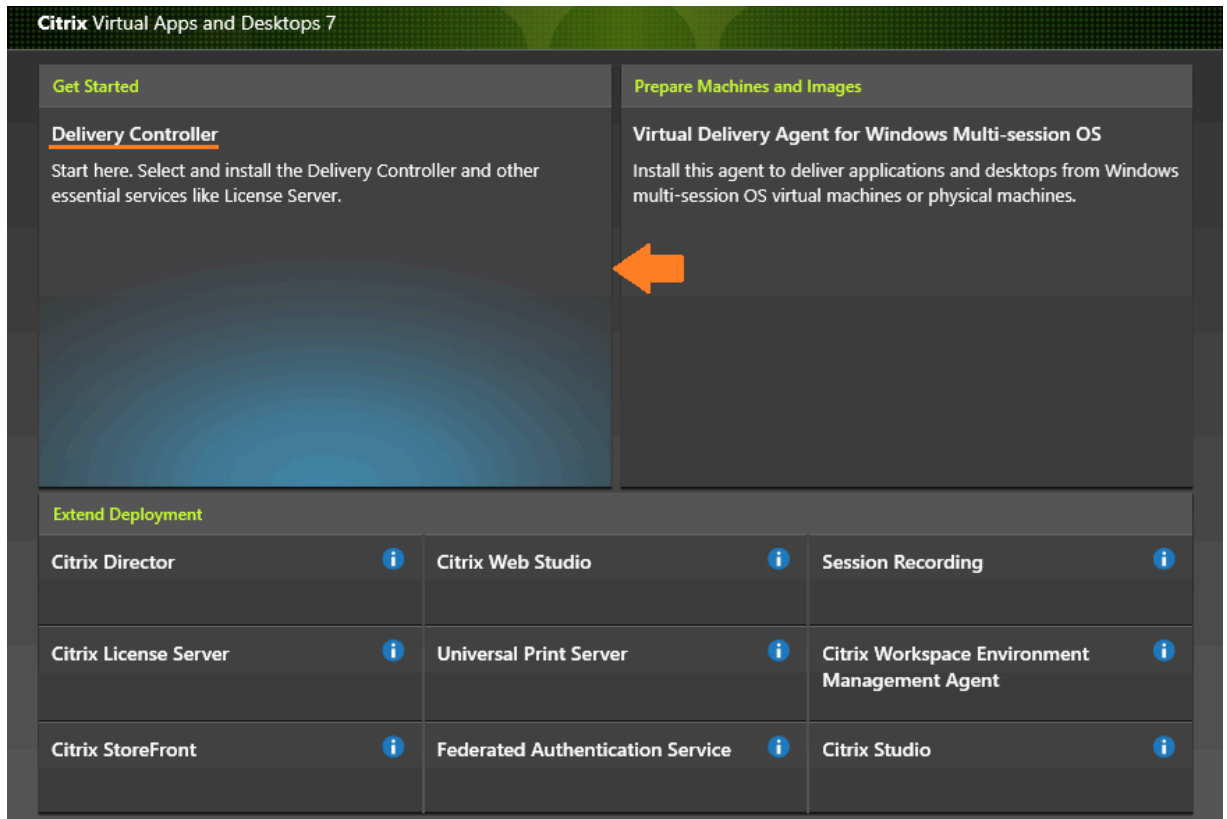
4. Click **AutoSelect**.



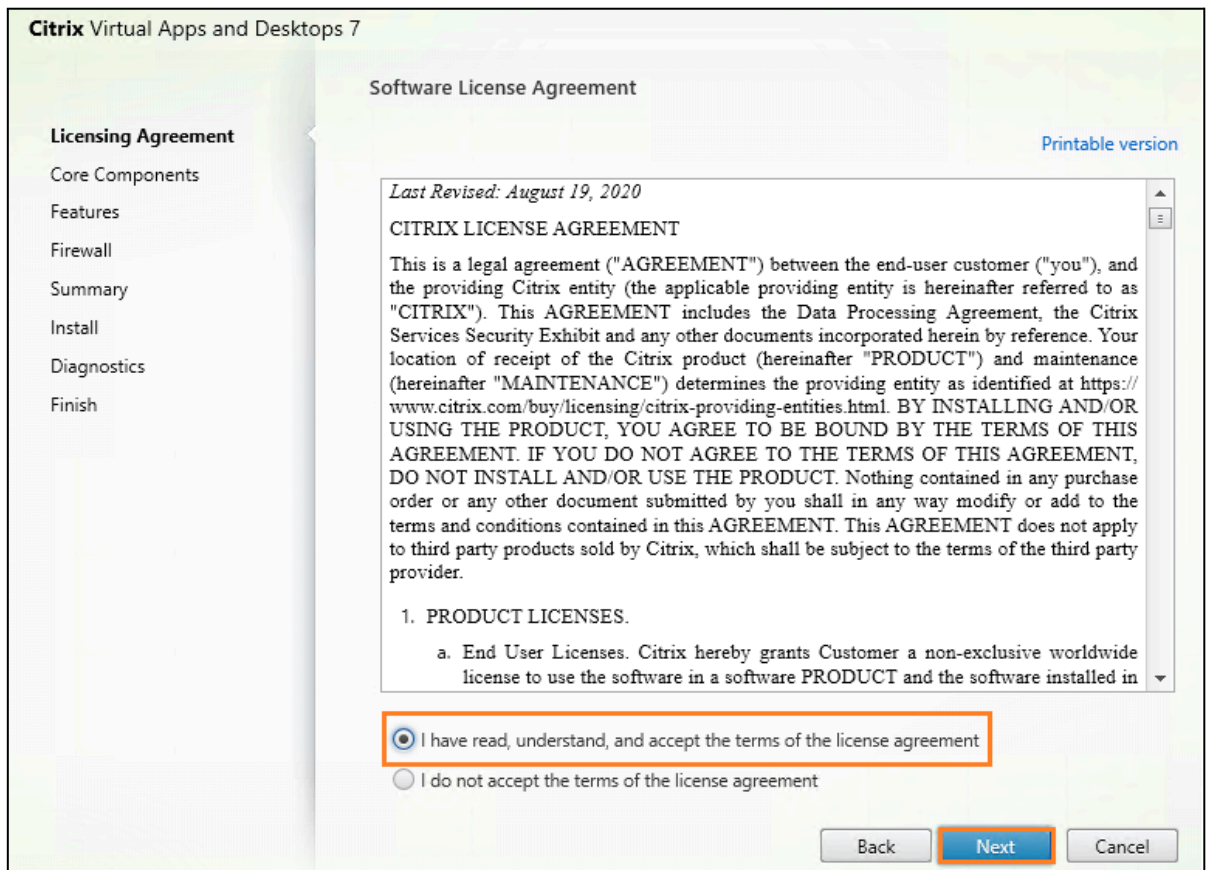
5. Click **Start** next to **Virtual Apps and Desktops**.



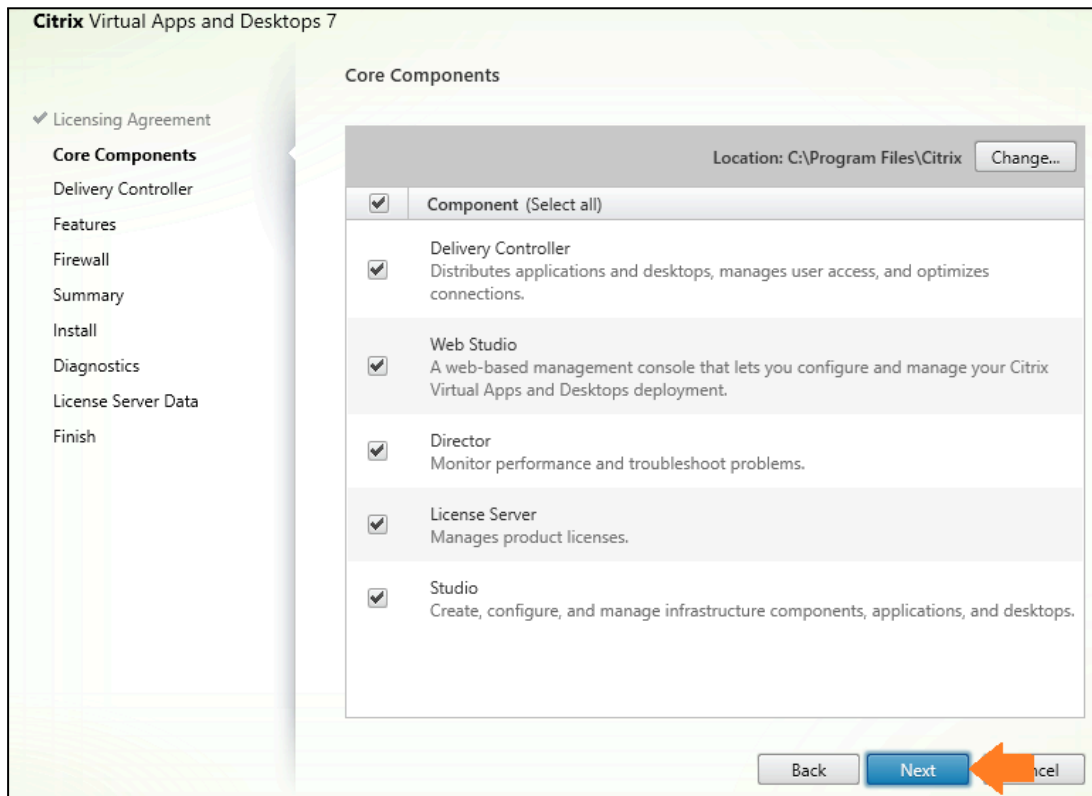
## 6. Select **Delivery Controller**.



## 7. Accept the License Agreement and Click **Next**.

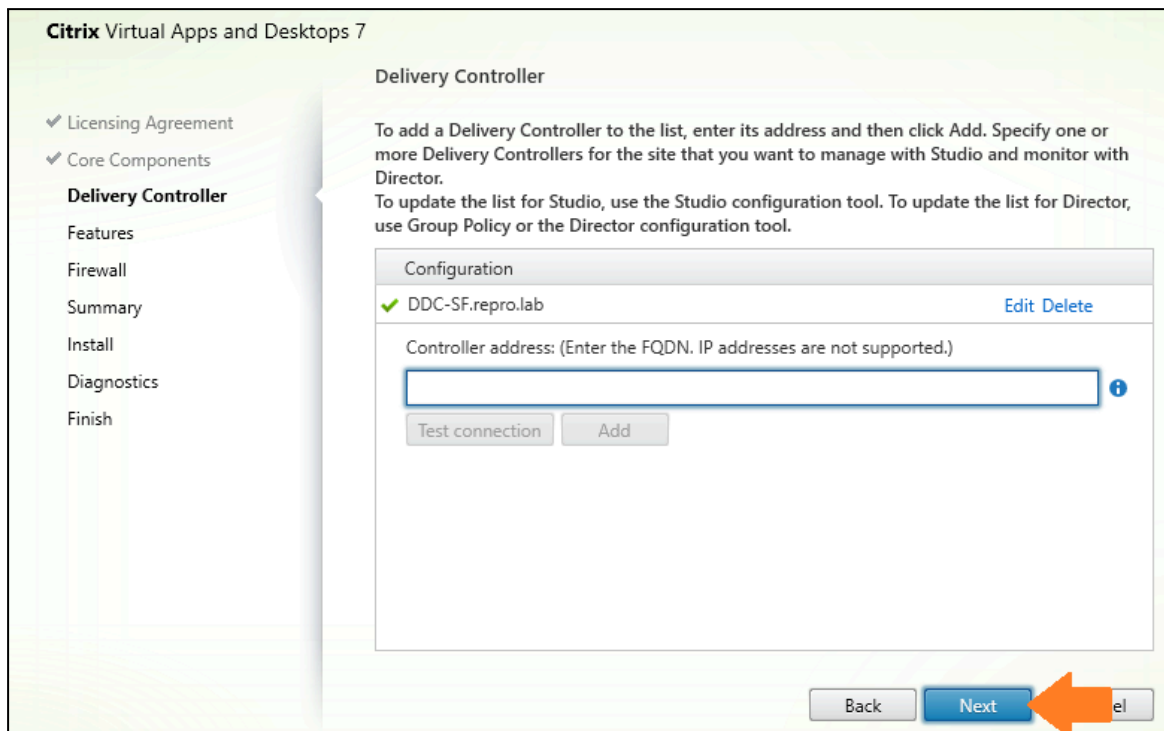


8. Under Core Components, **uncheck**, License Server and click **Next**.

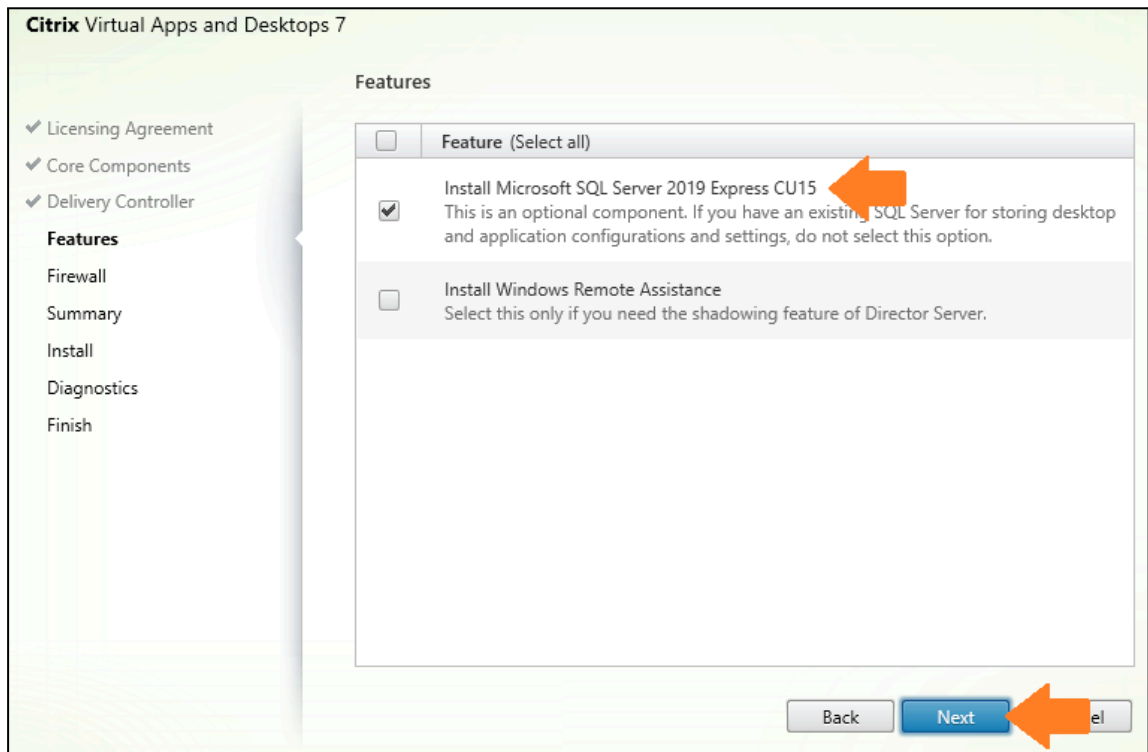


**NOTE:** You can use CVAD for 30 days without a license. Trial mode lets you use Citrix Virtual Apps and Desktops on-premises for 30 days, for 10 connections. For more information, see [Evaluation licenses](#).

9. Your **DDC-SF.repro.lab** will be populated automatically. Click **Next**.

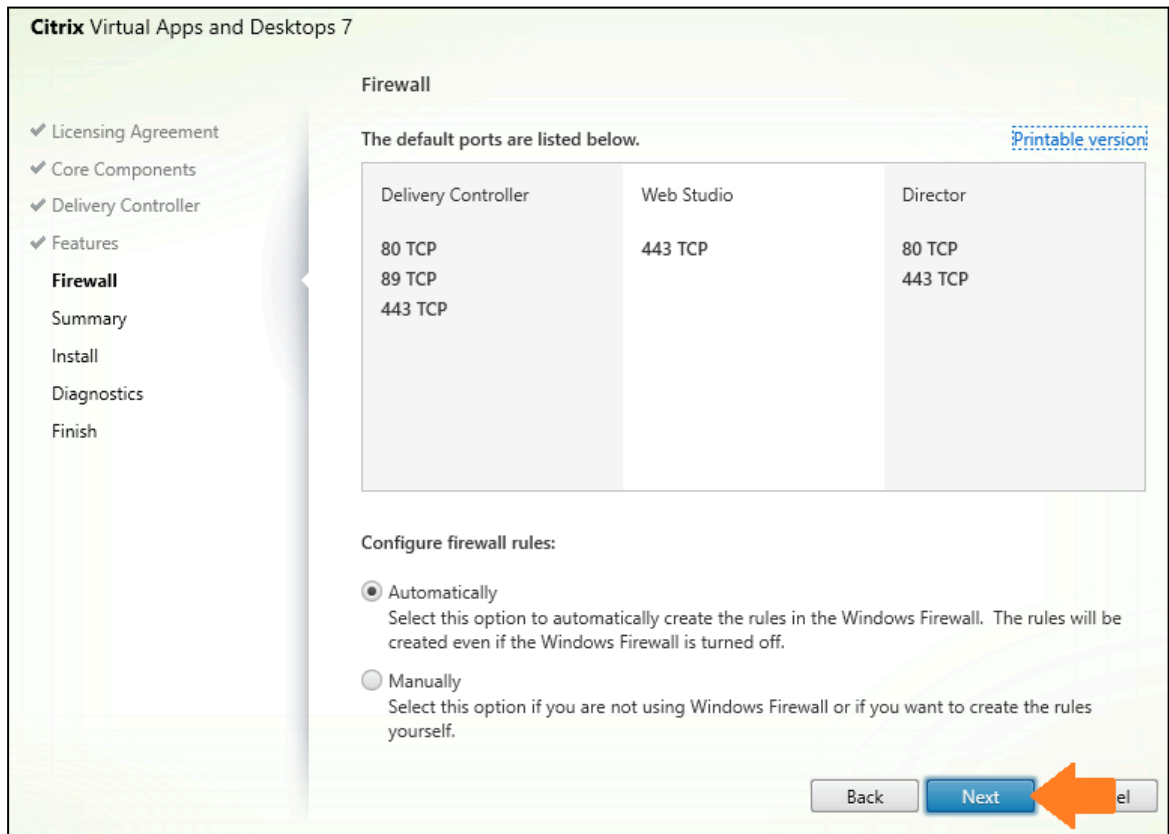


10. Install **Microsoft SQL Server 2019 Express** and click **Next**.



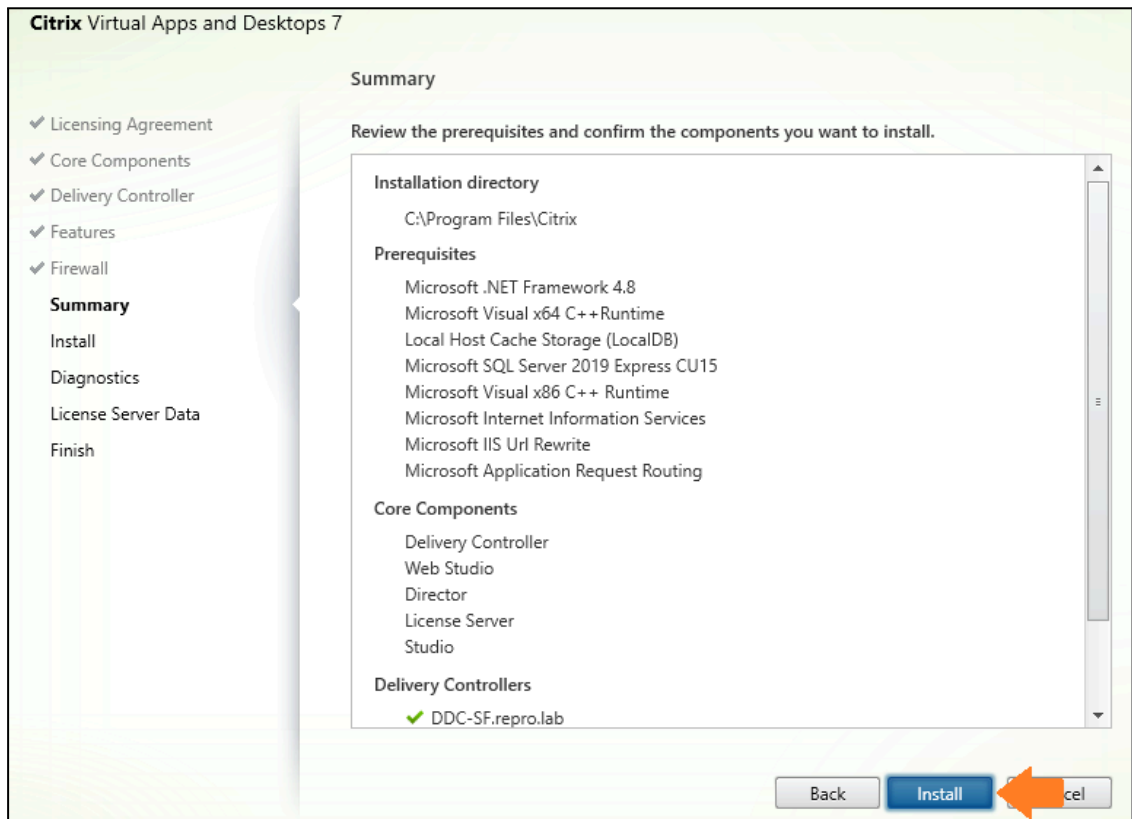
**NOTE:** As previously stated, we will address the essential prerequisites for CVAD. If you intend to use a SQL server, kindly refer to the Citrix Academy course/Lab Guide for detailed instructions.

11. Leave the Firewall settings at default and Click **Next**.

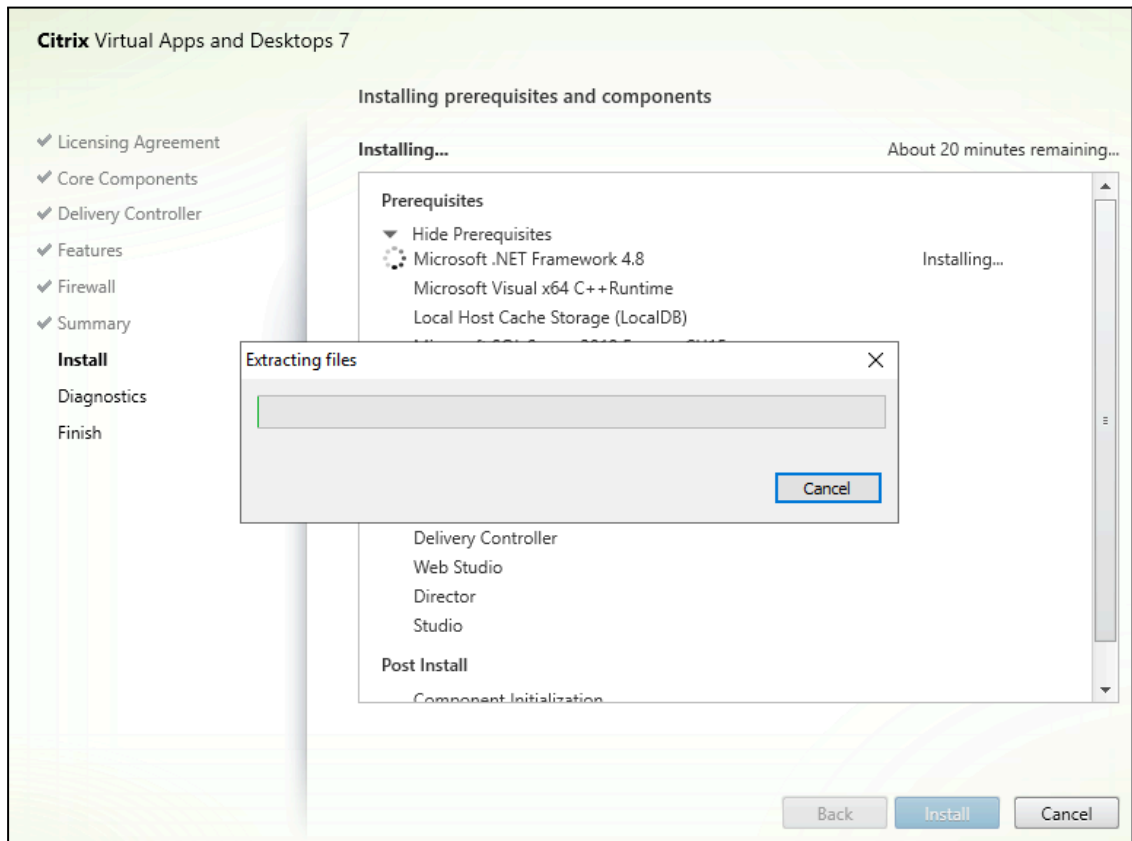




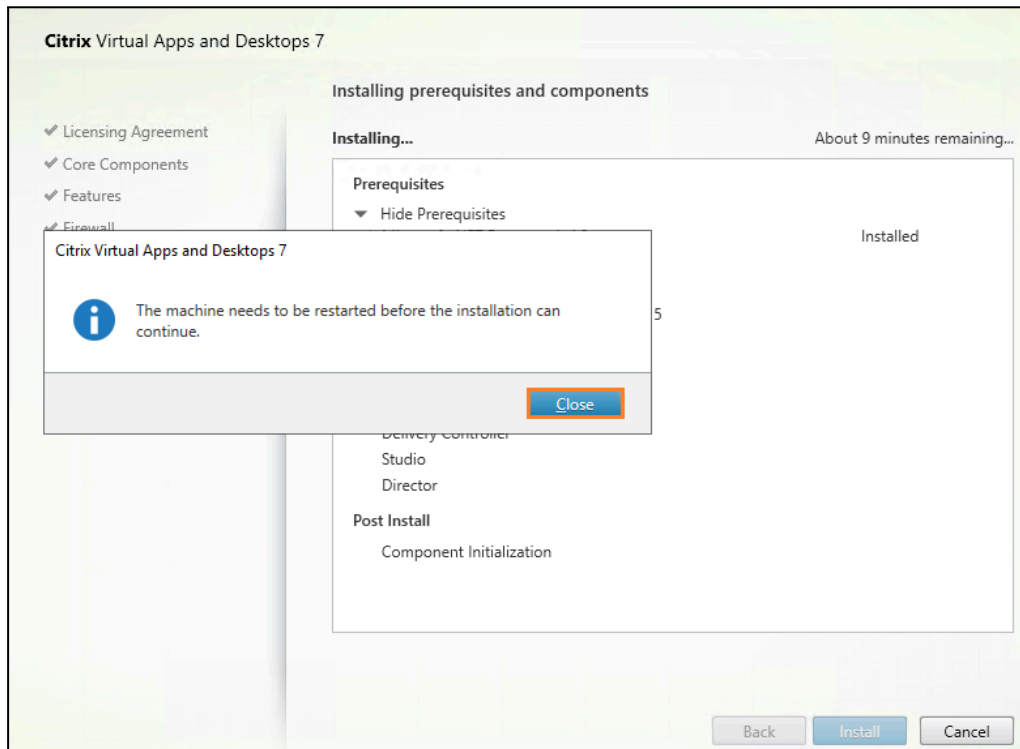
12. Click **Install**.



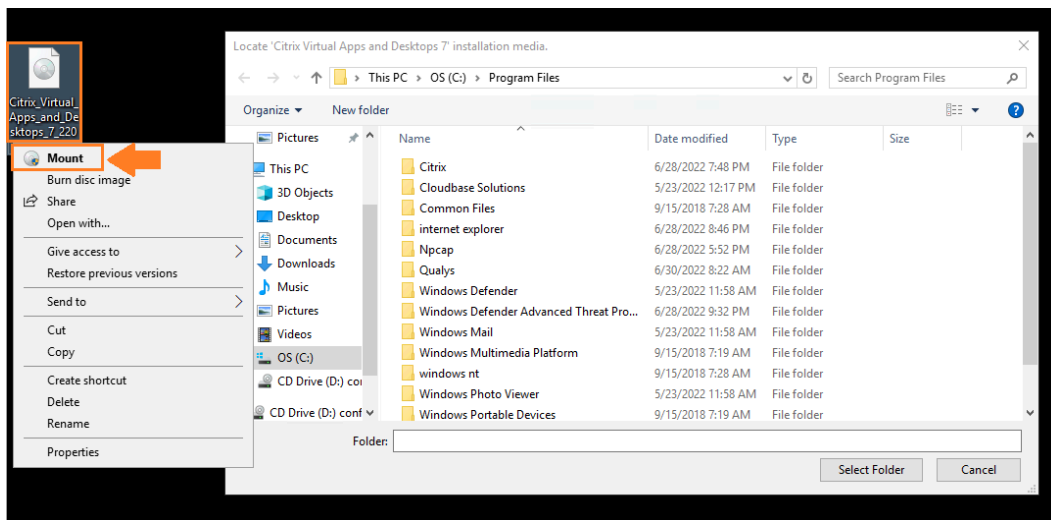
The installation process will take a few minutes.



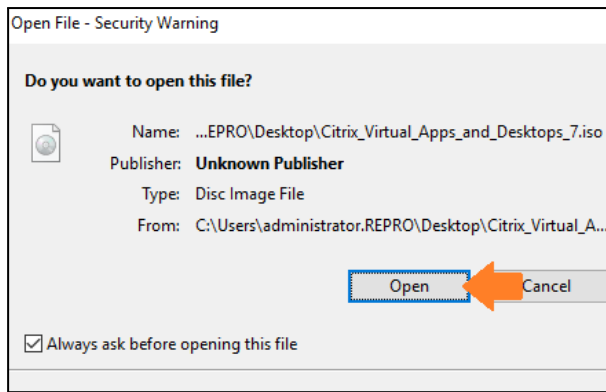
13. The installation requires 2 reboots. Please click **“close”** and **wait for the machine to restart**.



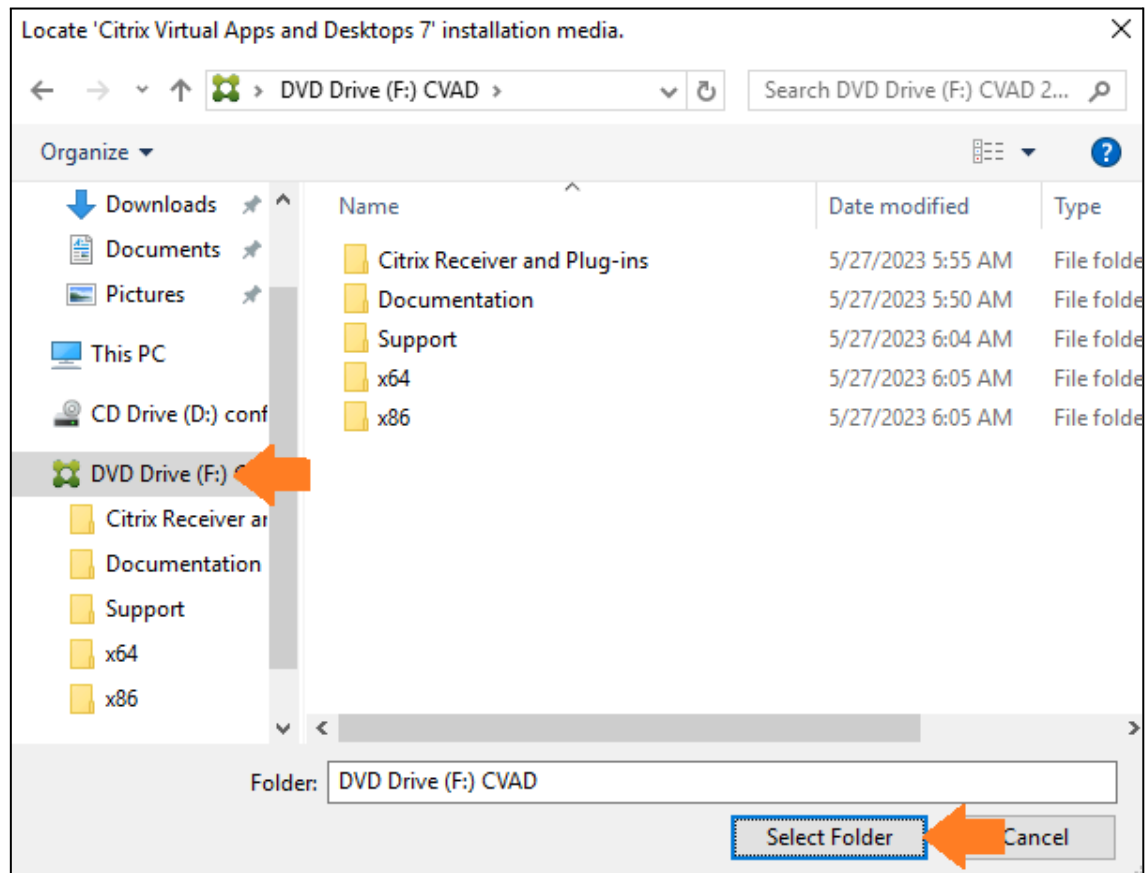
14. Mount the CVAD ISO again.



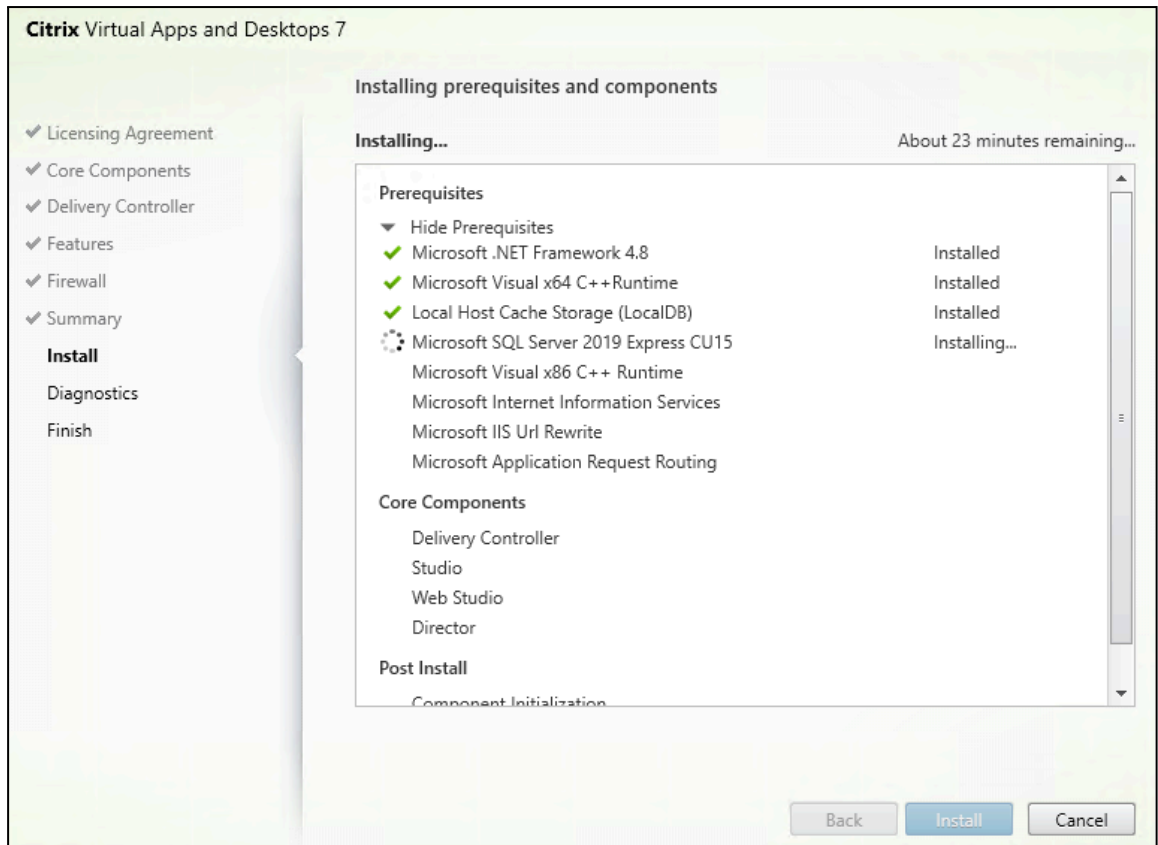
15. Click **Open**.



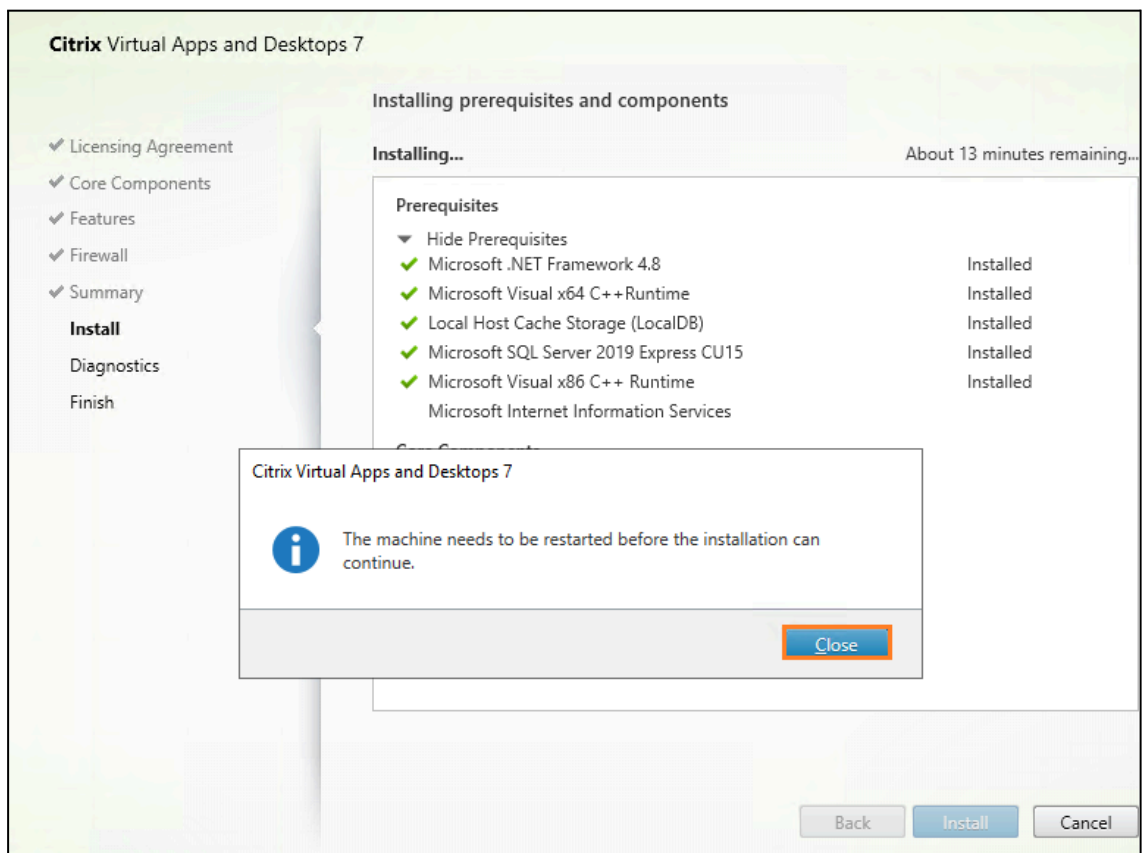
15. Click the CVAD **DVD Driver (E:)** and then click **Select Folder**.



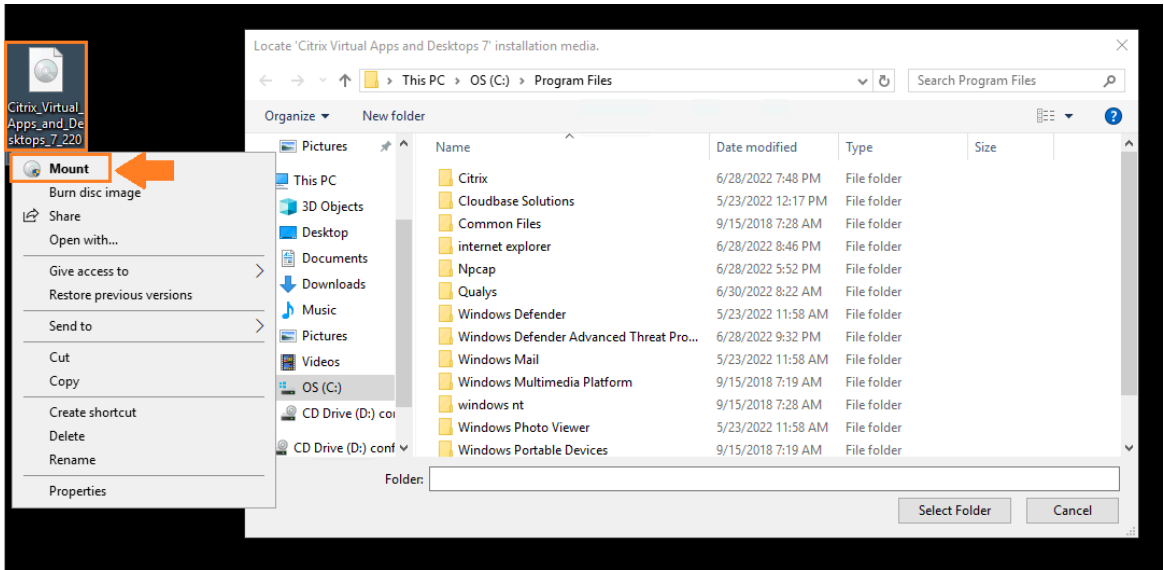
The installation will continue.



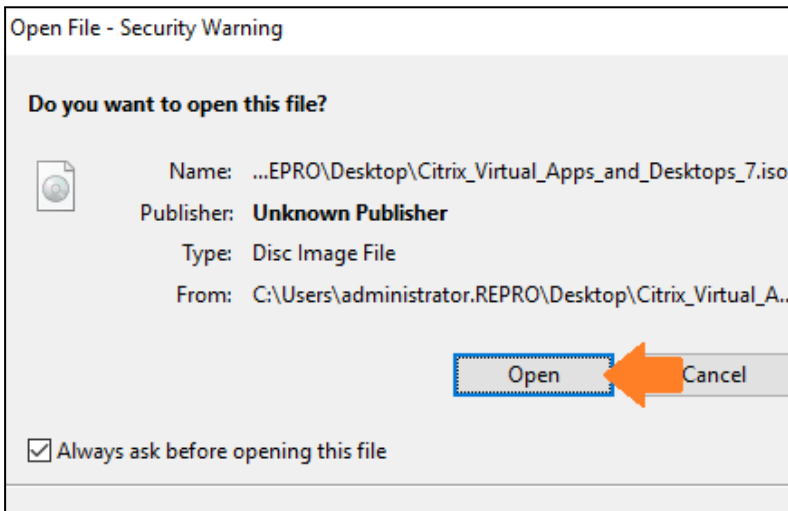
16. Click **Close** for the second reboot and wait for the machine to restart.



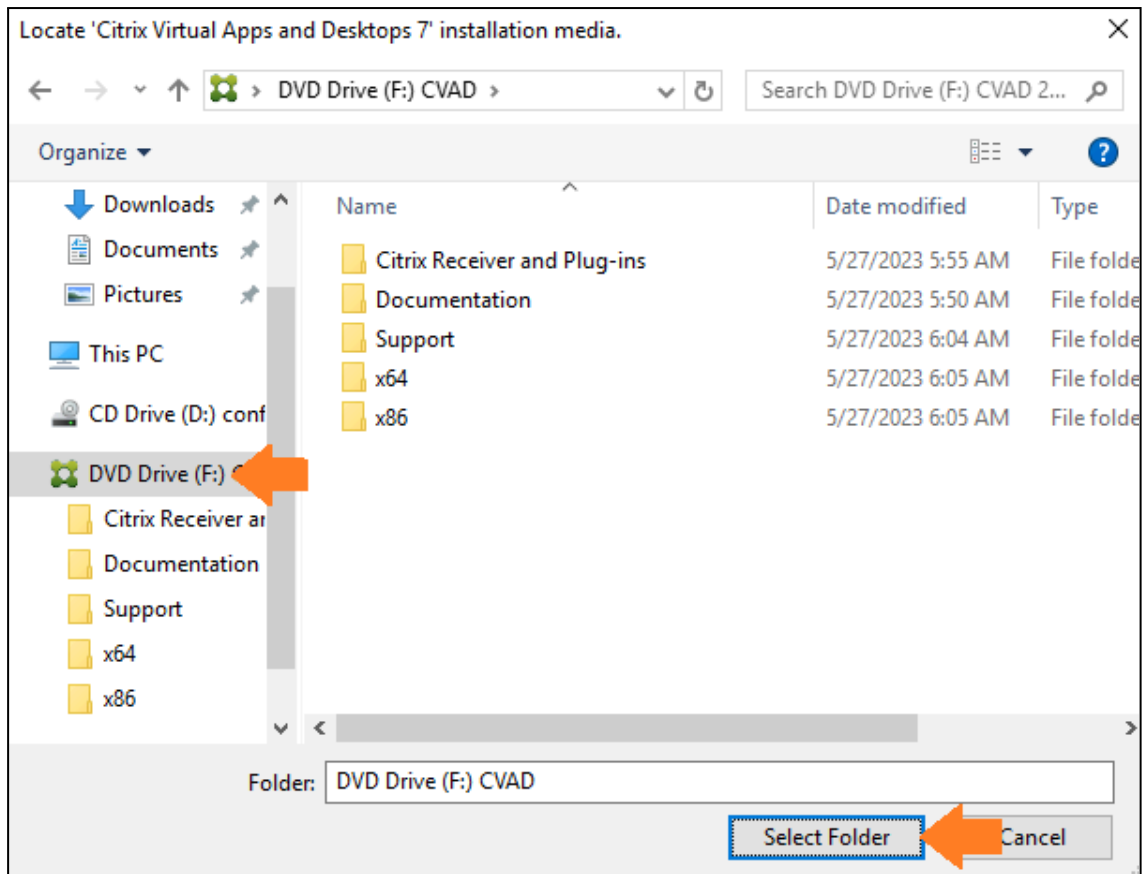
17. Mount the **CVAD ISO** again.



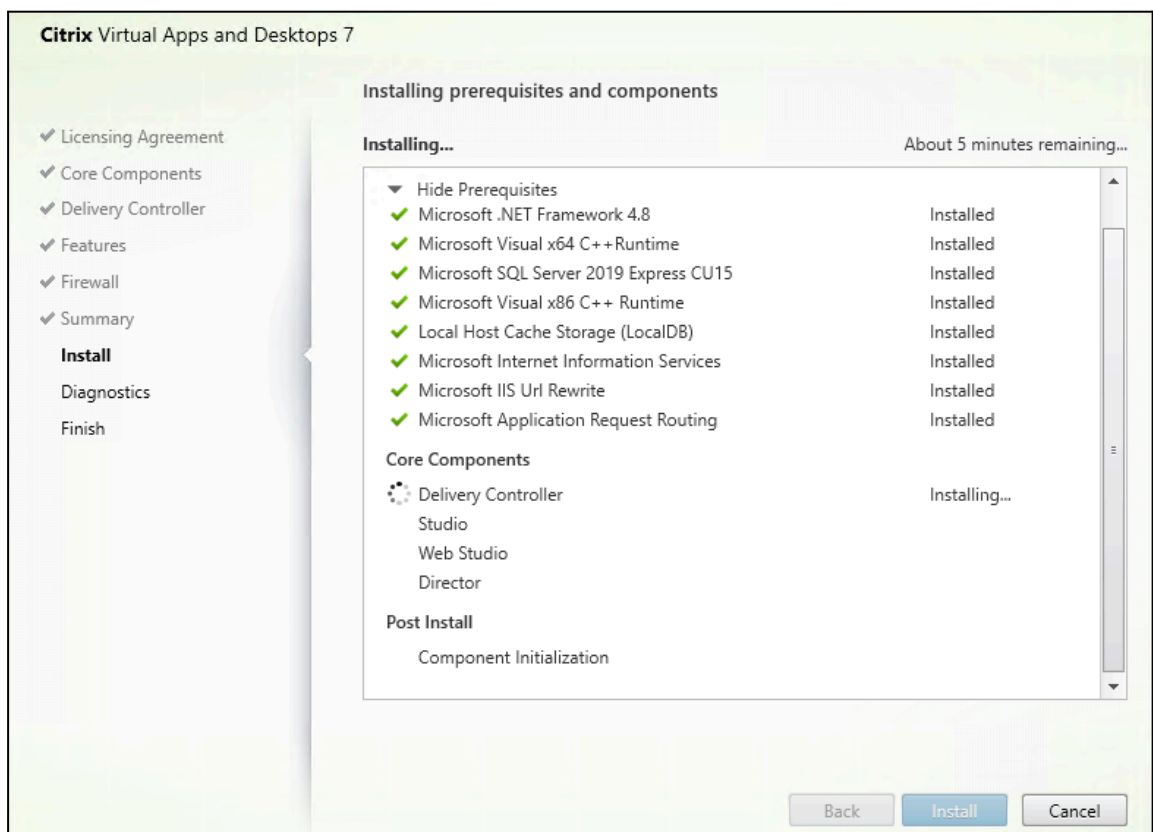
18. Click **Open**.



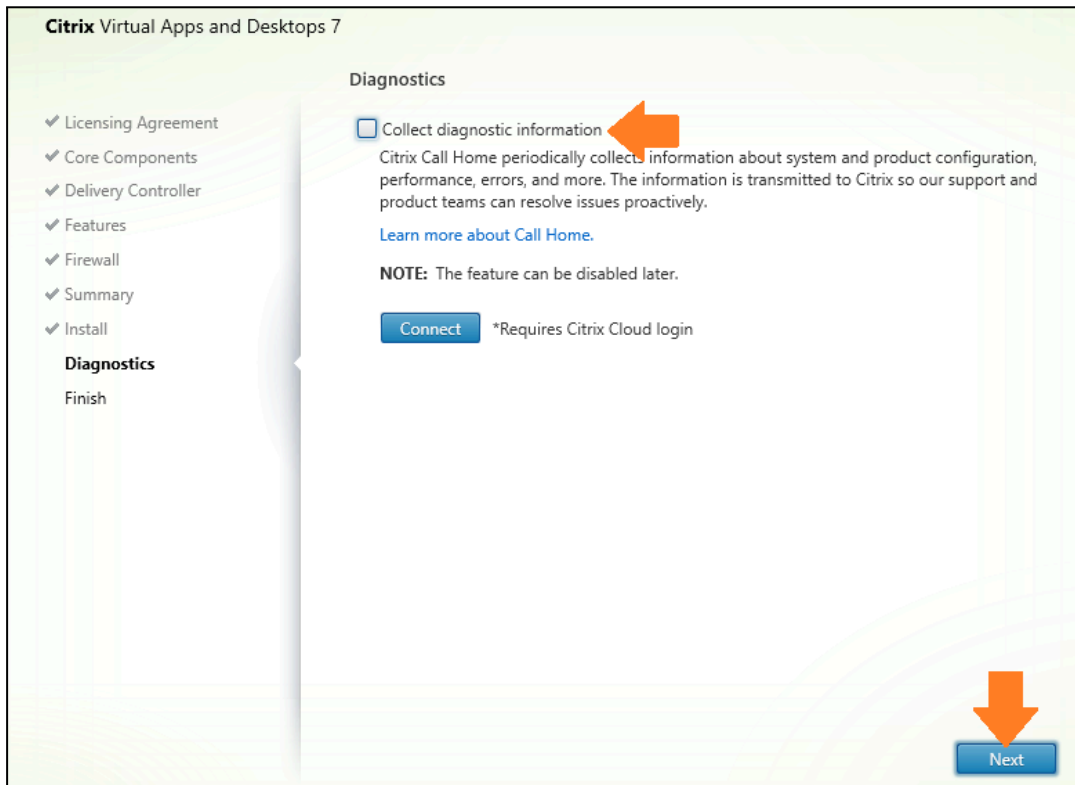
19. Click over the CVAD **DVD Driver (E:)** and **Select Folder**.



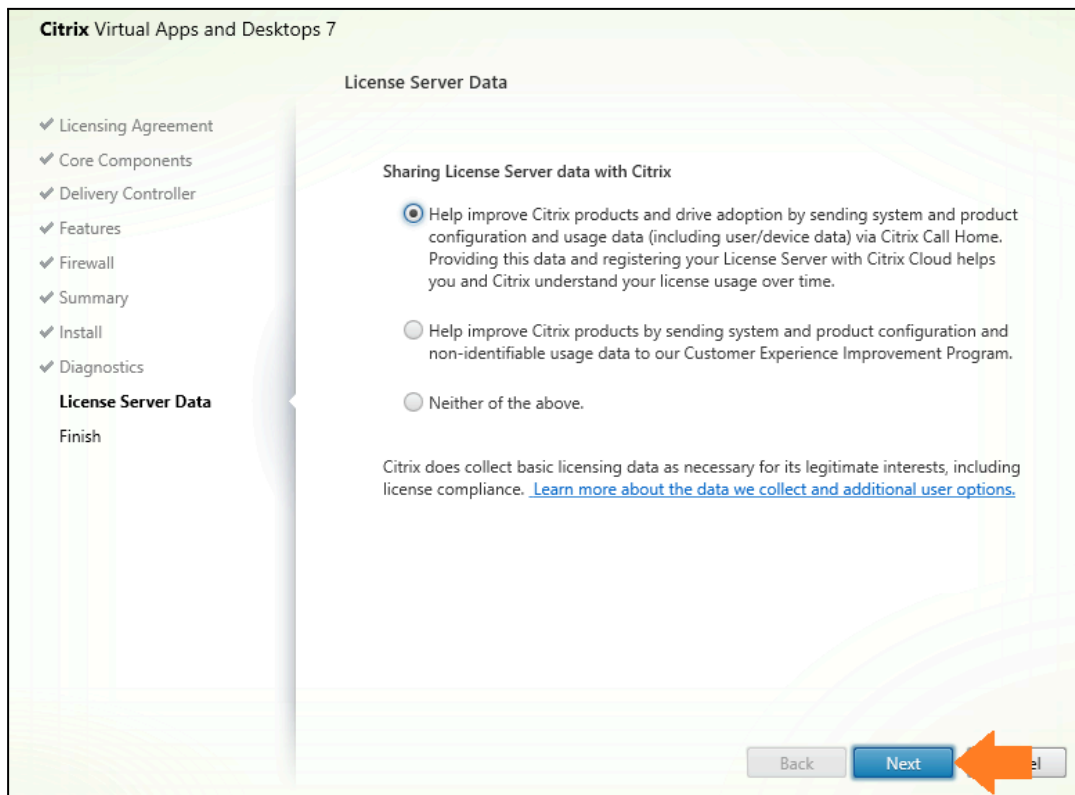
The installation will **continue**.



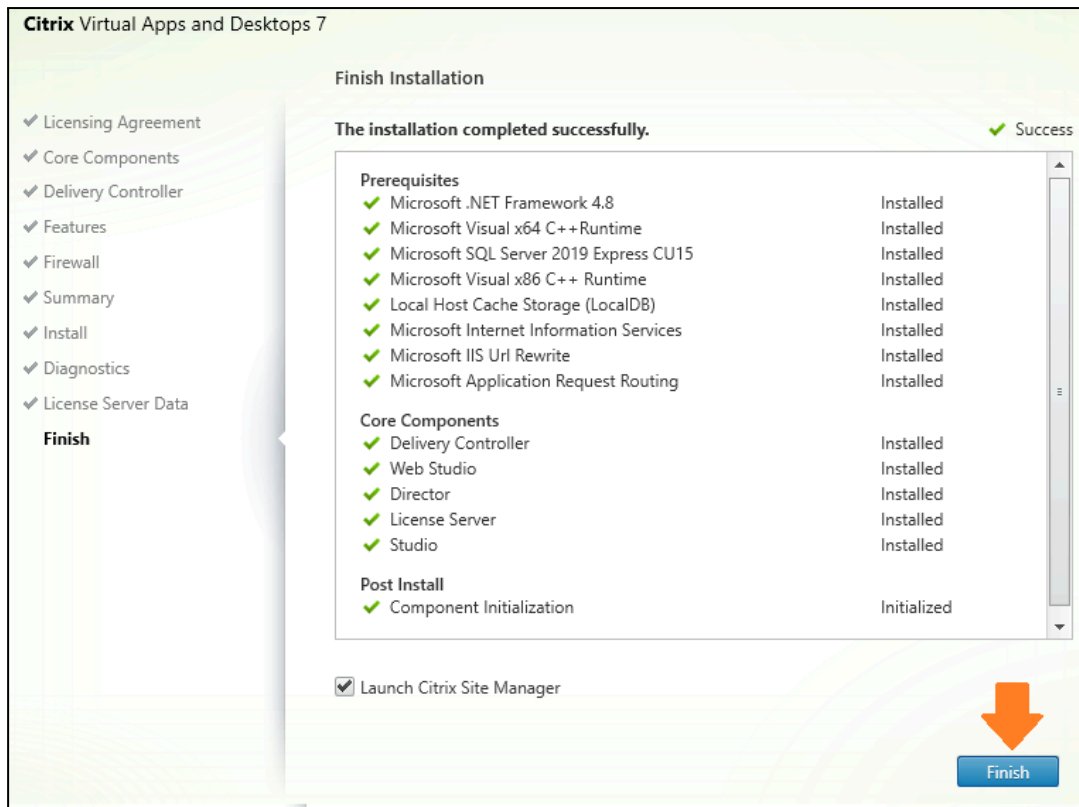
20. Uncheck **Collect diagnostic information** and **Next**.



21. Click **Next**.

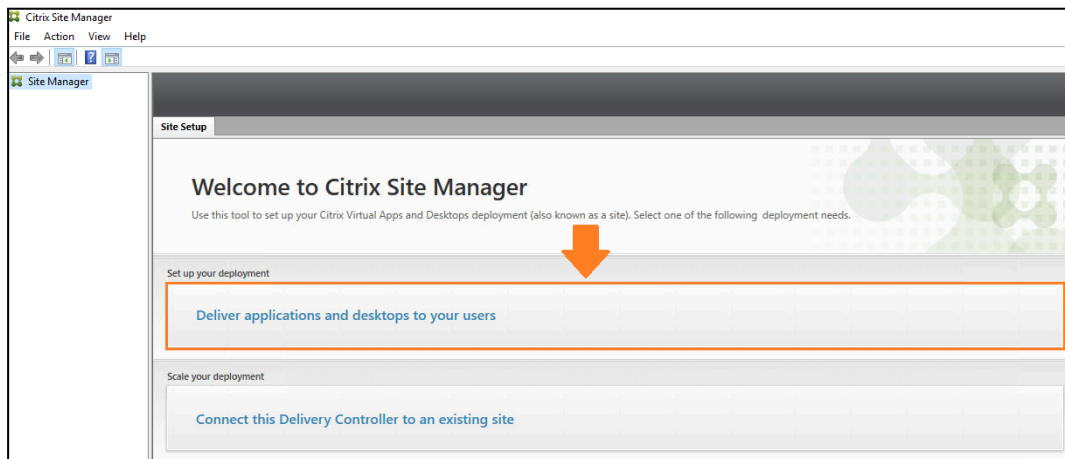


22. The installation is completed Click **Finish**. This will also Launch Studio to begin the Site configuration.



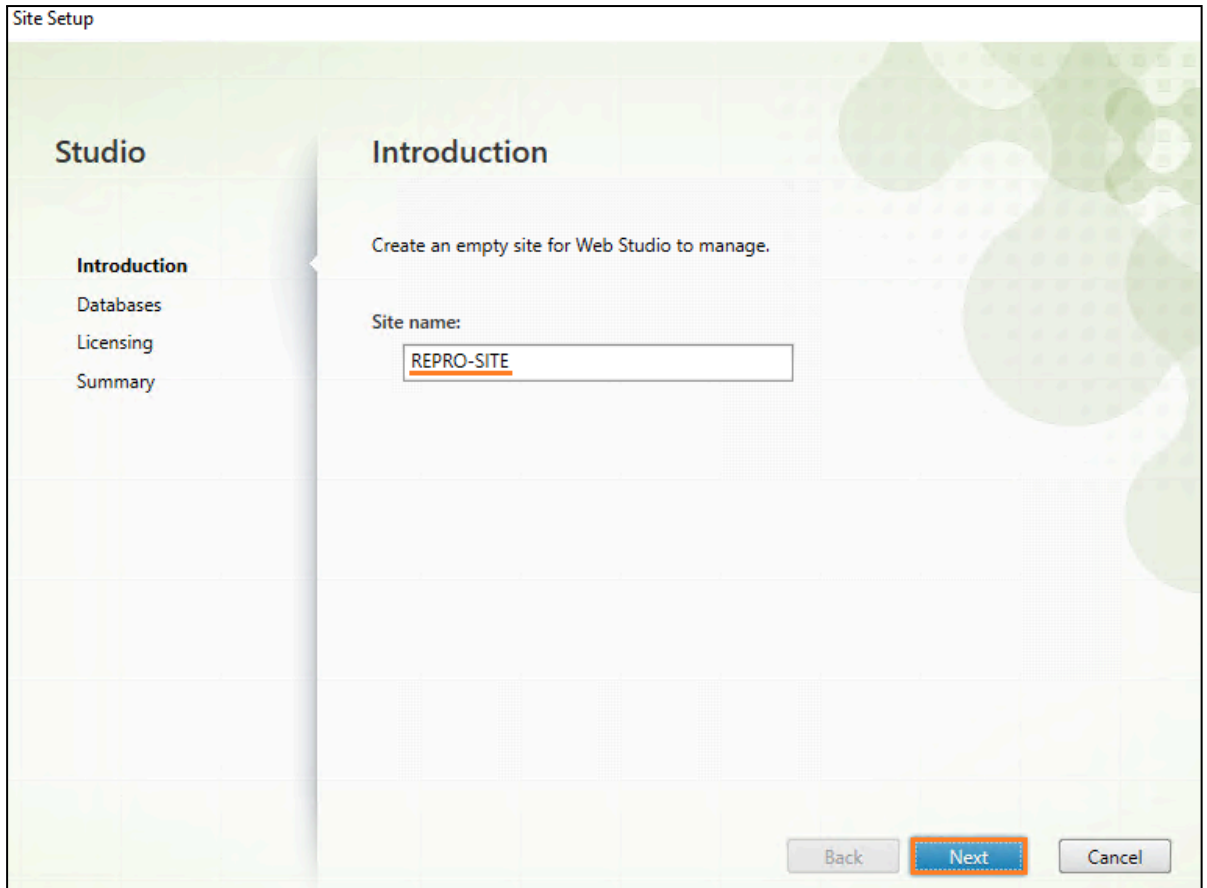
## Site Configuration

1. Your Citrix Site Manager will open. Select Deliver applications and desktops to your users.

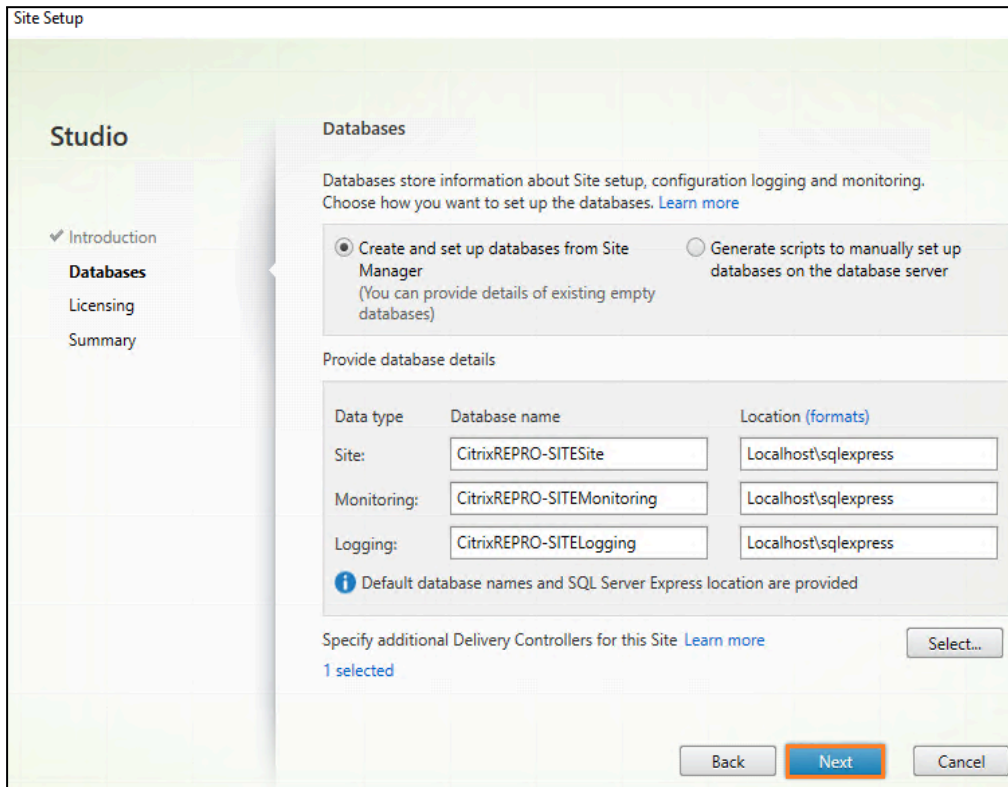


2. At the Introduction screen, set the site name to **"REPRO-SITE"** and click **Next**.



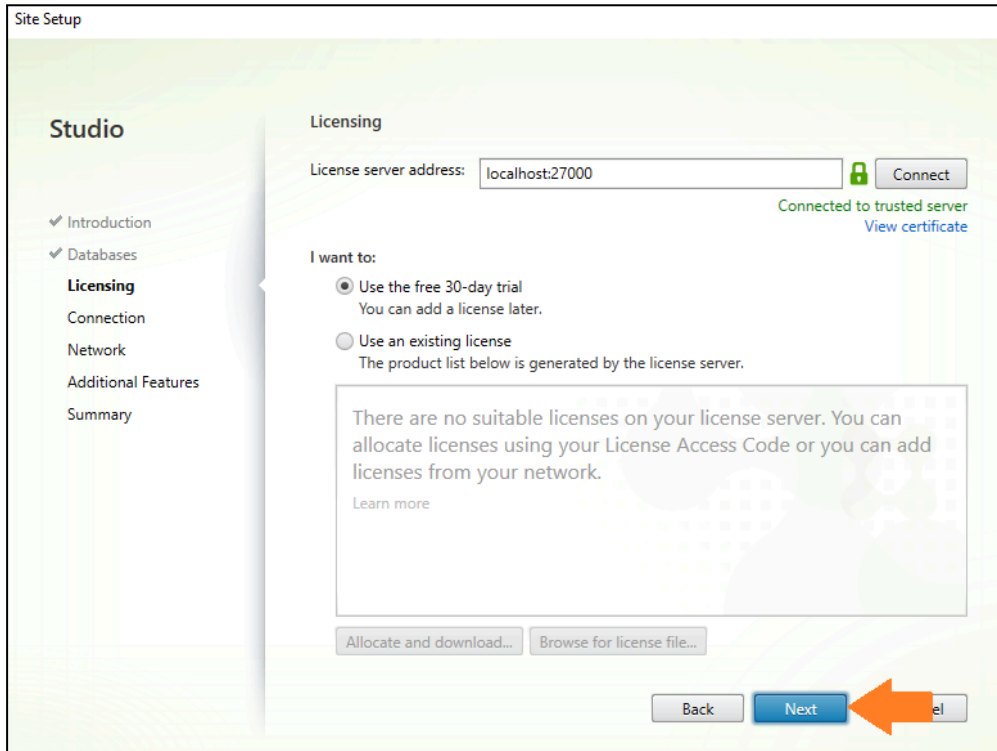


3. At the Databases screen, leave all defaults and click **Next**.



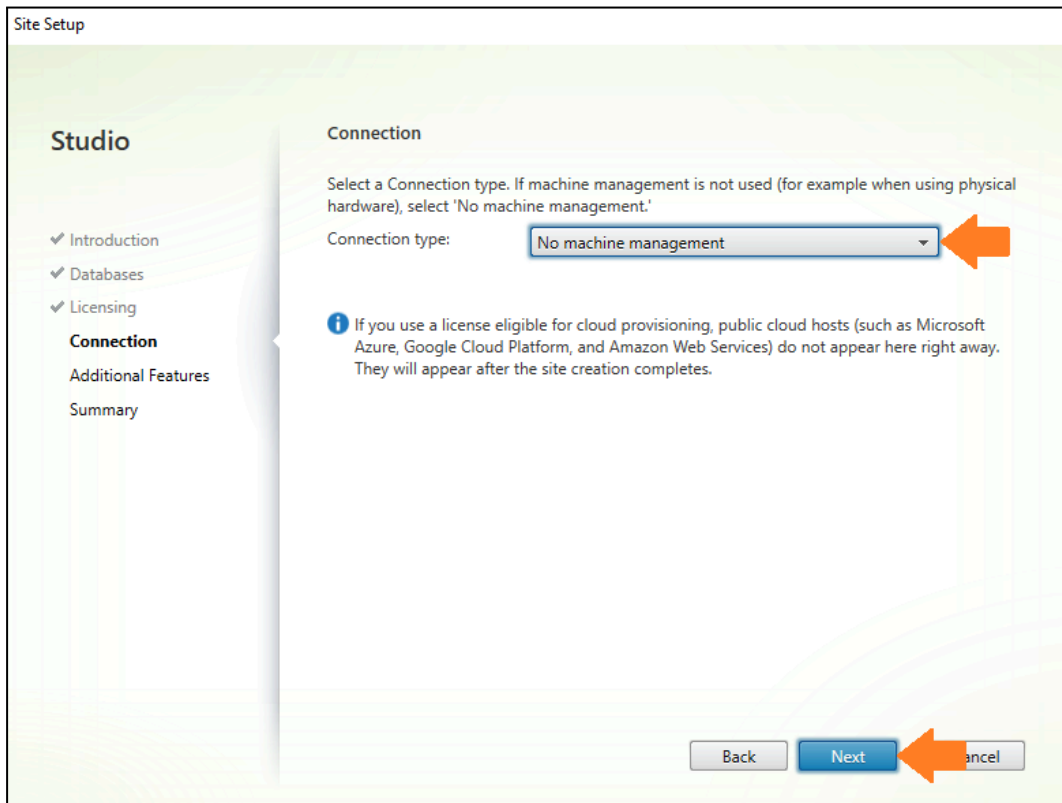
**NOTE:** If you are using your own database, set its location.

4. The localhost license server will be populated automatically. Click **Next**.

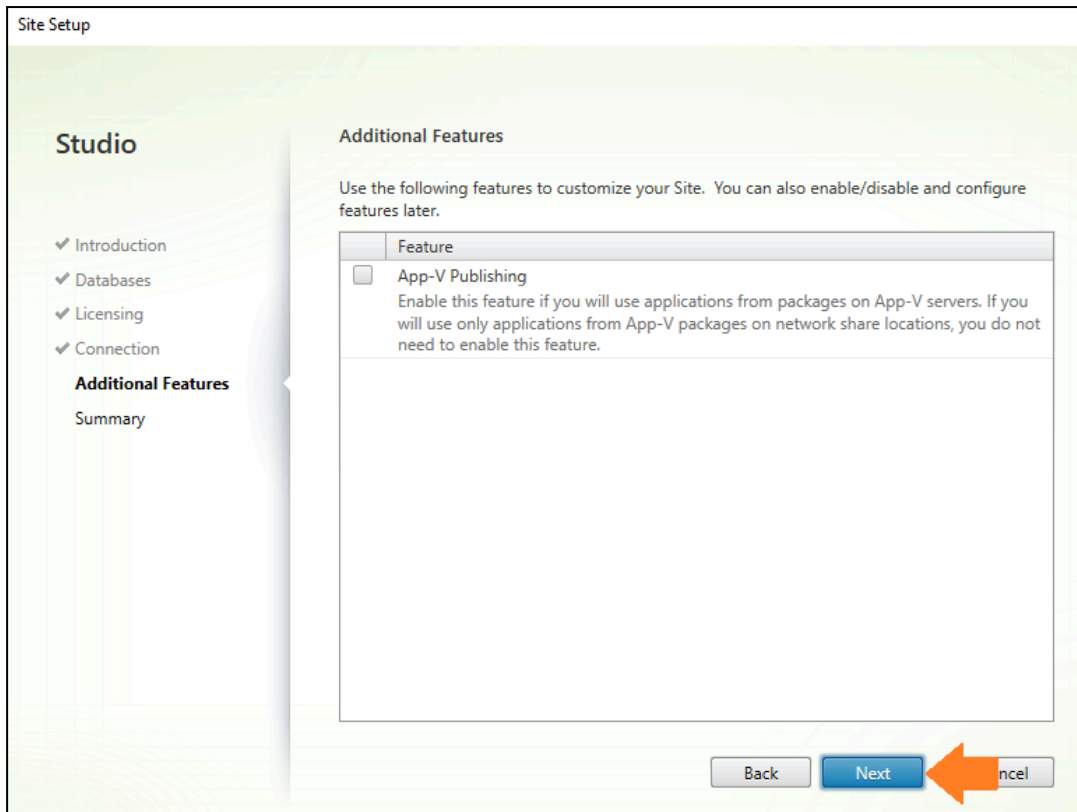


**NOTE:** As mentioned before, this trial will last for 30 days only

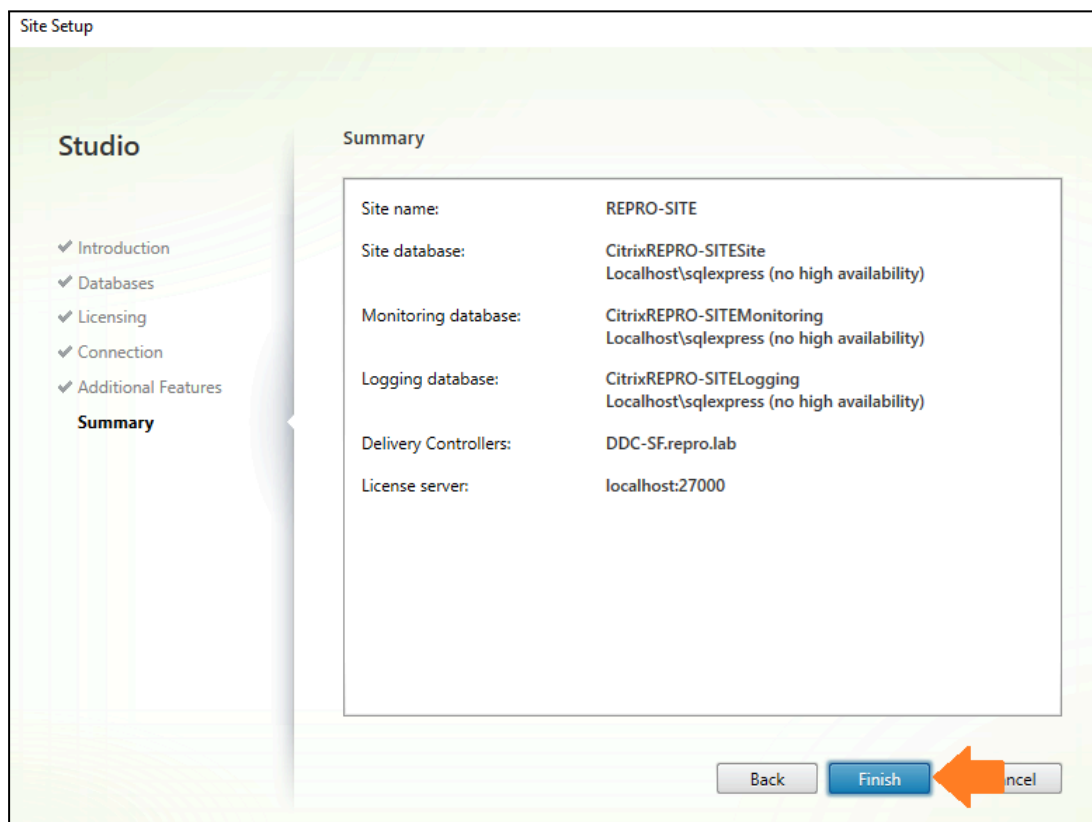
5. Select **No machine management** and click **Next**.



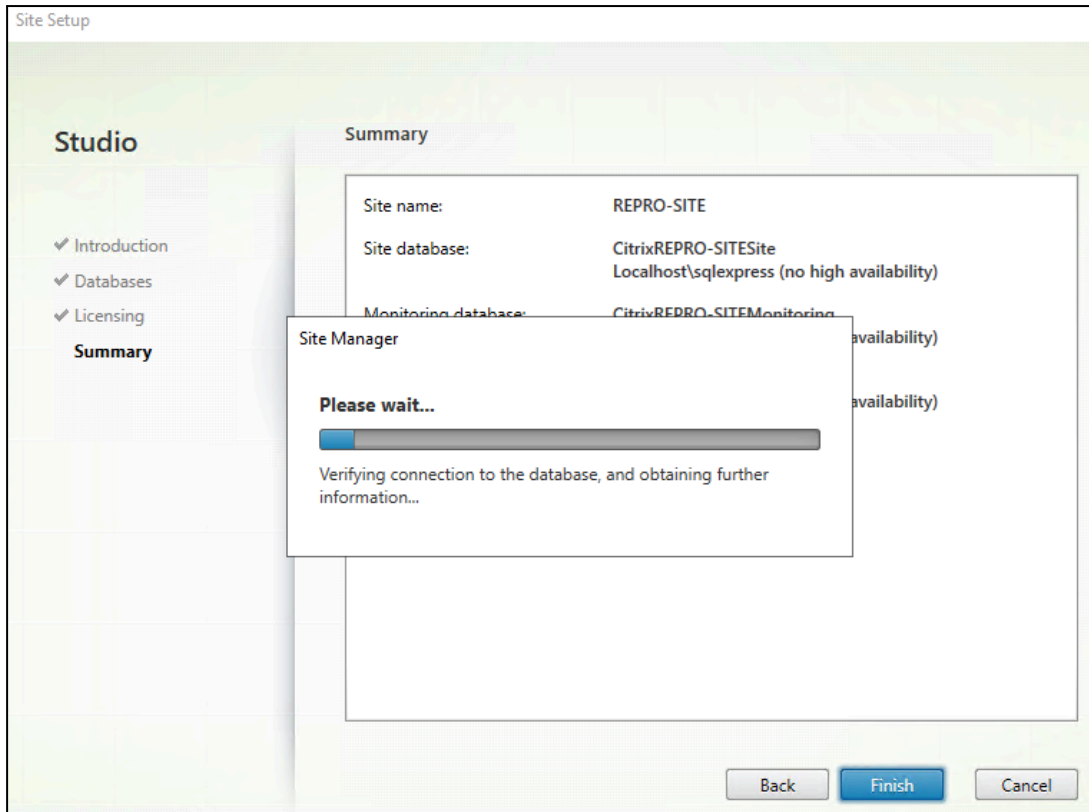
6. Click **Next**.



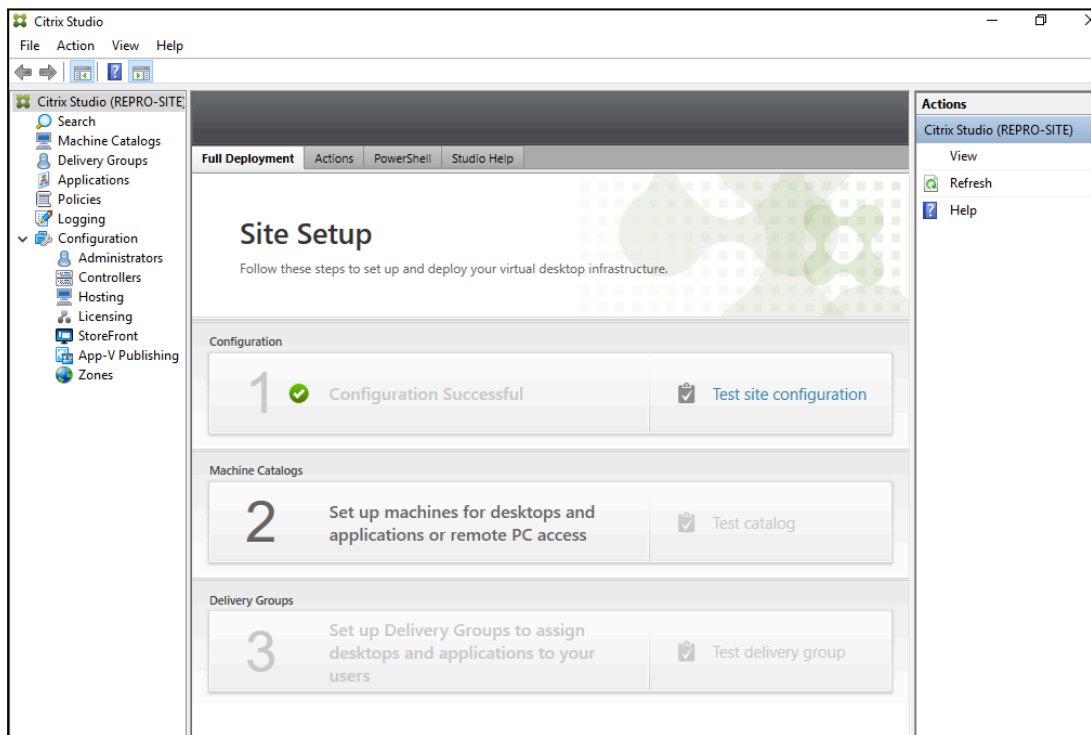
7. Click **Finish**.



8. Wait until everything is created.



9. The site configuration is **done**.

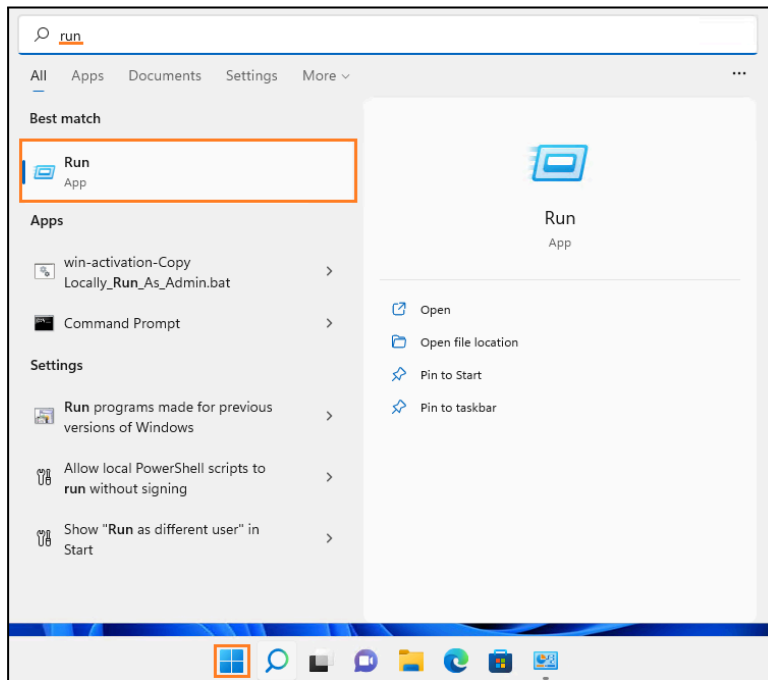


**NEXT STEPS:** Install the VDA VM (WINDOWS 10 or 11) before proceeding to the Machine catalog configuration.

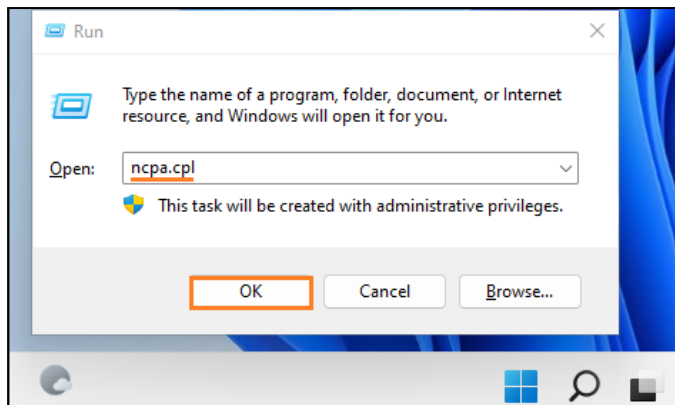
## Windows 11 Install for Virtual Delivery Agent (VDA)

### VM Windows 10 or Windows 11

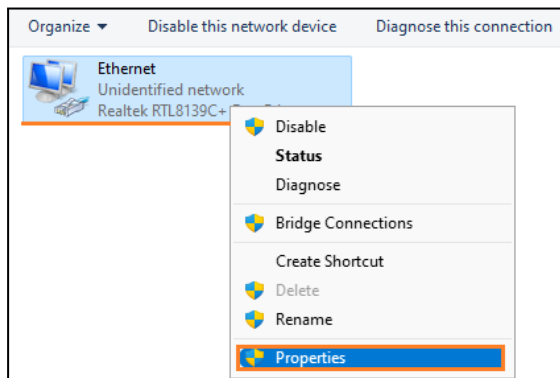
1. From your new VM, click **Start > Run** and then type “**ncpa.cpl**” to configure the network interface.



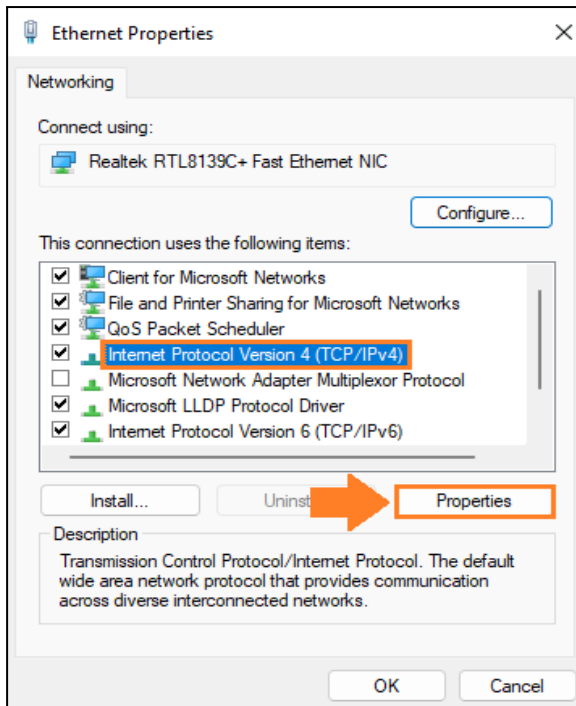
2. Type **ncpa.cpl** and click **OK**.



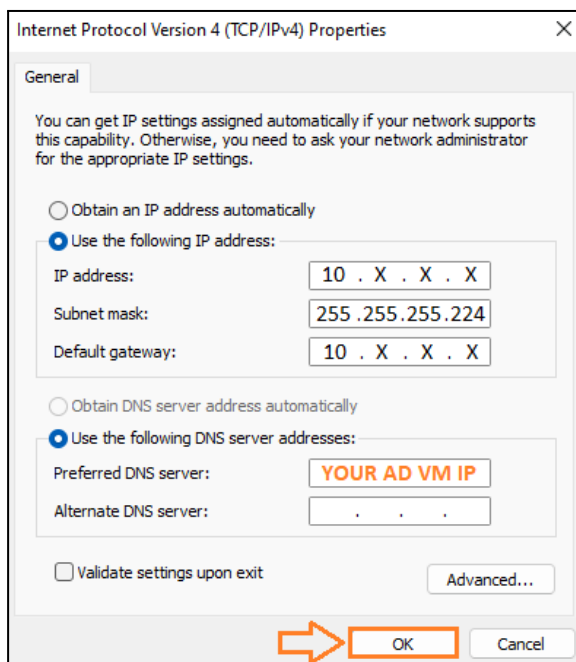
3. Right-click the **Ethernet** connection and choose **Properties**.



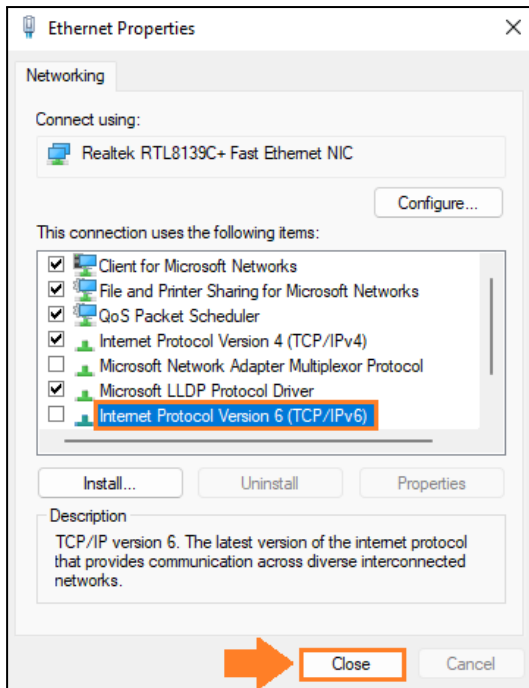
4. On the **Ethernet Properties** window, select **Internet Protocol Version 4 (TCP/IPv4)** in the list and click **Properties**.



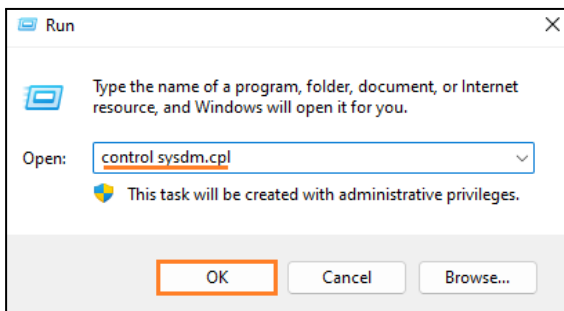
5. Set your **IP address**, along with the **Subnet Mask** and **Default Gateway** according to your network info.  
For **DNS**, please set your **WINDOWS SERVER AD IP**. Your Windows Server AD will act as DNS for all your VMs.



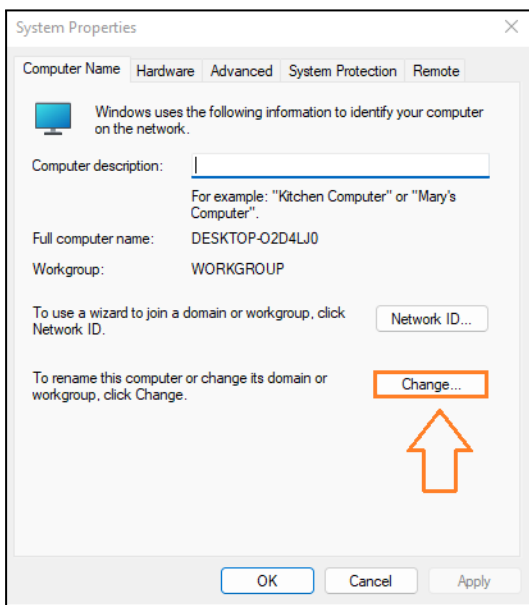
6. Click **Close**.



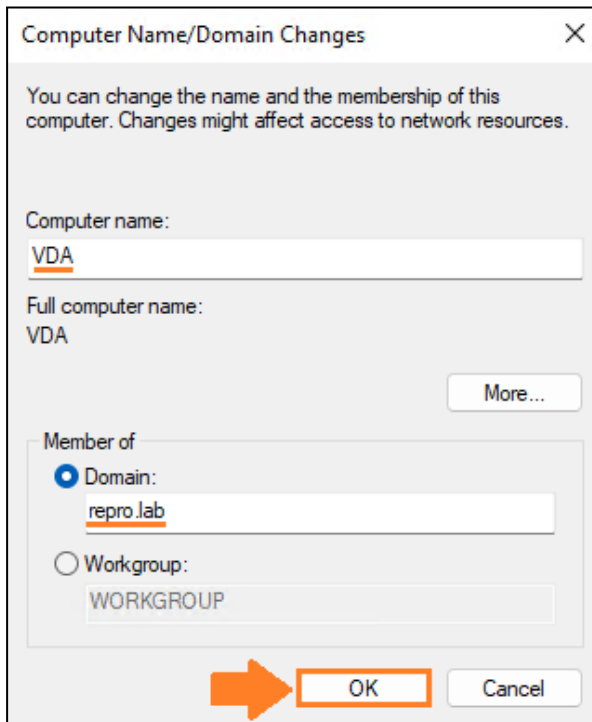
1. Confirm you can ping your **local domain** (repro.lab) from the Windows VDA VM.
2. Go **Start > Run** and type **“control sysdm.cpl”** to add your Windows 11 VDA to the domain



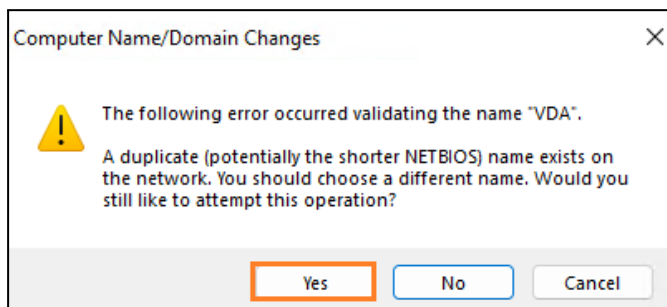
3. Click **Change**.



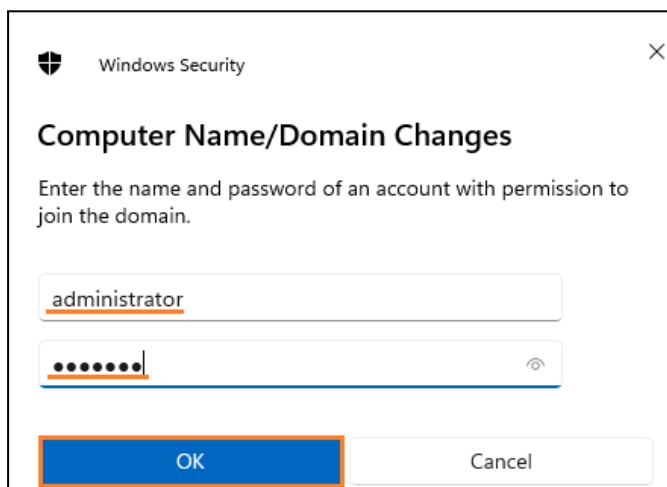
4. Change the VM name to **"VDA"**, select **"domain"**, type your **domain name (repro.lab)** and click **OK**.



5. If the below message appears, click **Yes**.

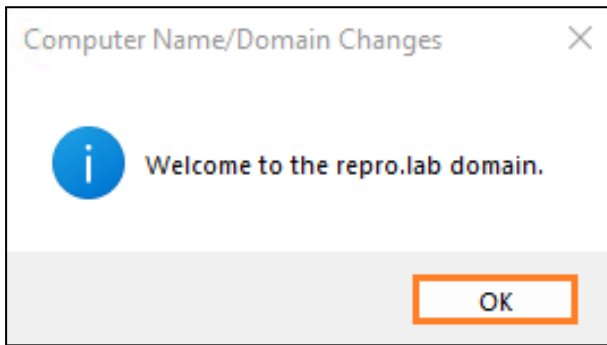


6. Enter your administrator credentials and click **OK**.

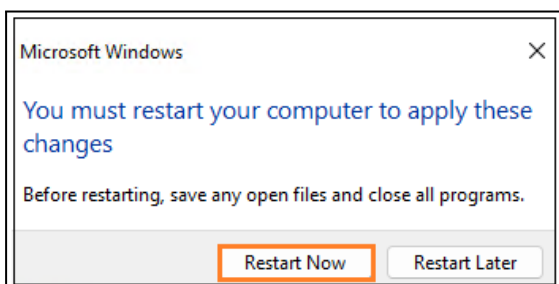
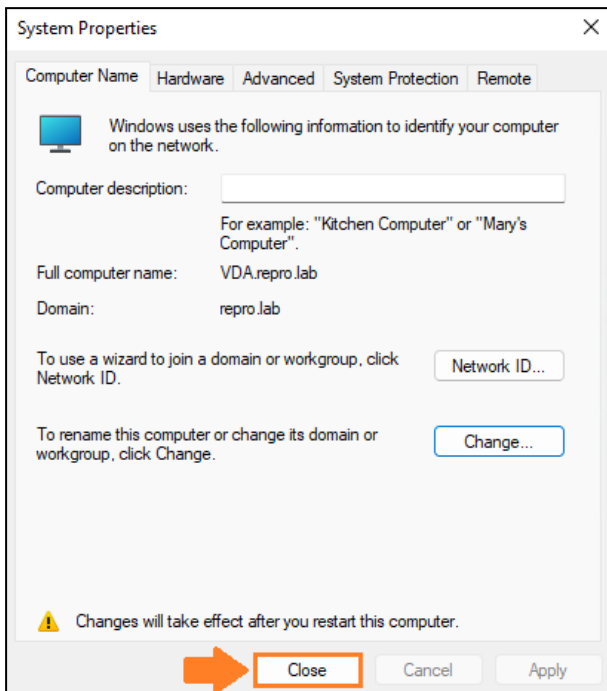
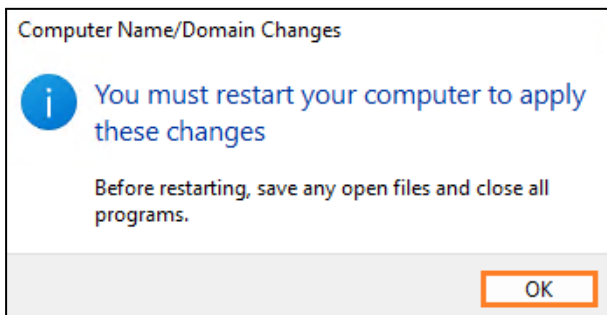




7. Click **OK**. The machine has joined the domain.

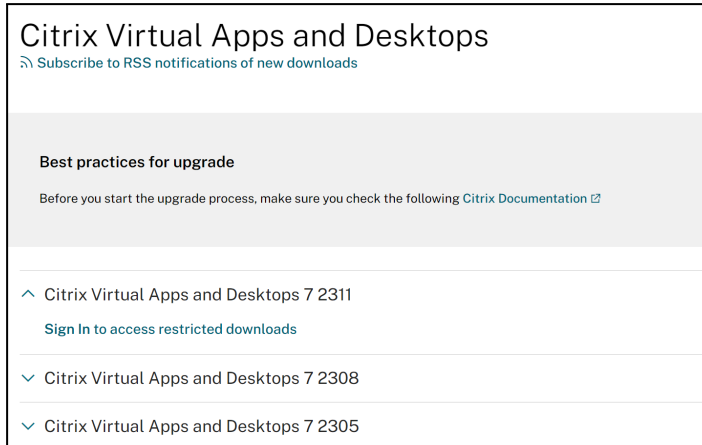


8. Click **OK**, **Close**, and **restart now** as requested.



## Launching the VDA installer

1. From your **Windows 10/11 VDA**, open your browser and navigate to <https://www.citrix.com/downloads/> to download the CVAD installer iso. Please download the same version you installed in the DDC.

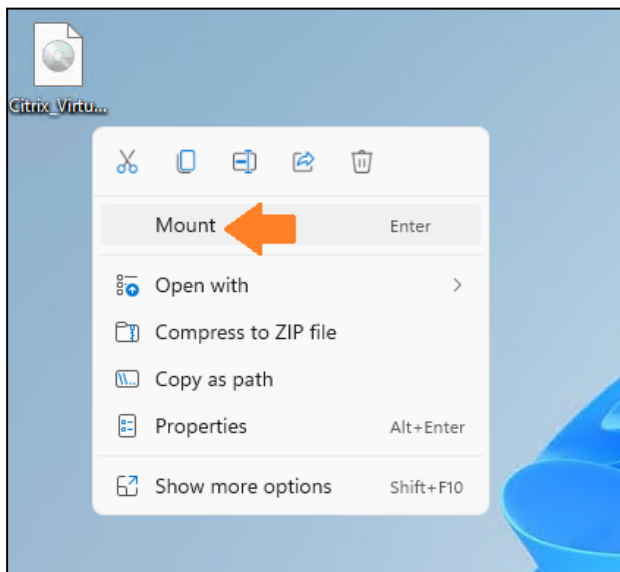


---

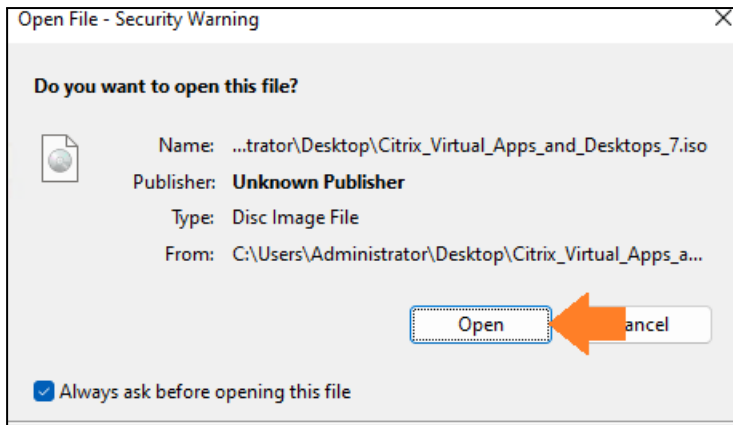
**NOTE:** We will cover the Citrix Virtual and Desktops 7 2003 version.

---

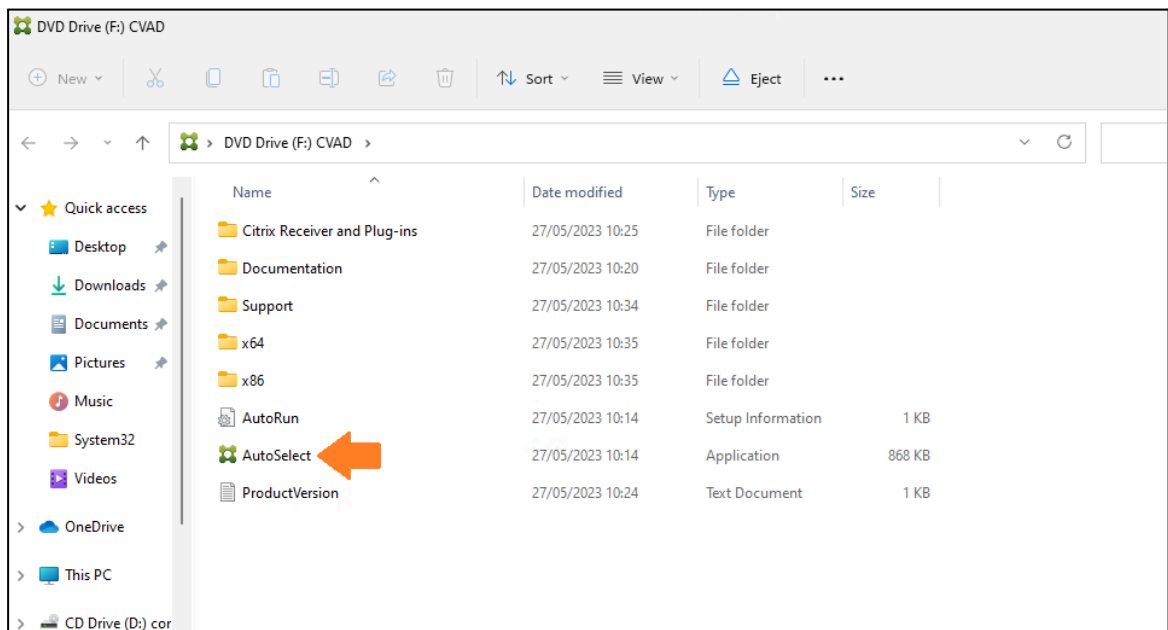
2. Once the image is downloaded, **right-click** and **mount** the image.



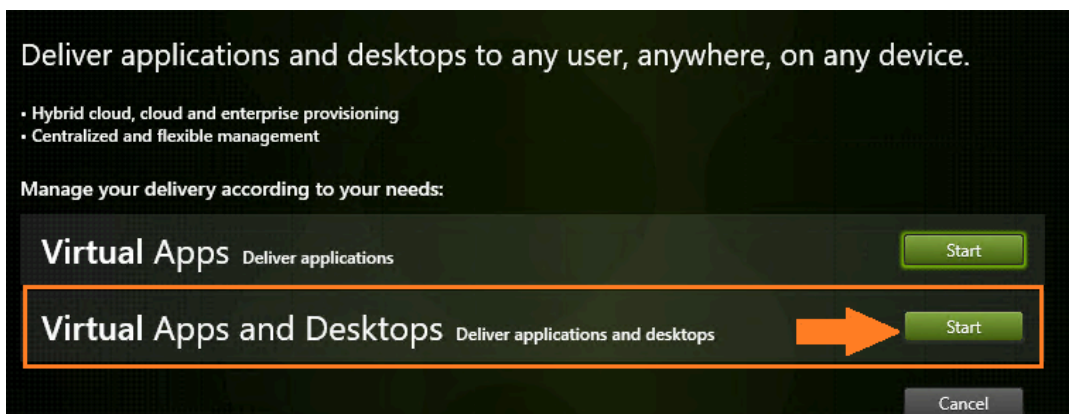
3. Click **Open**.



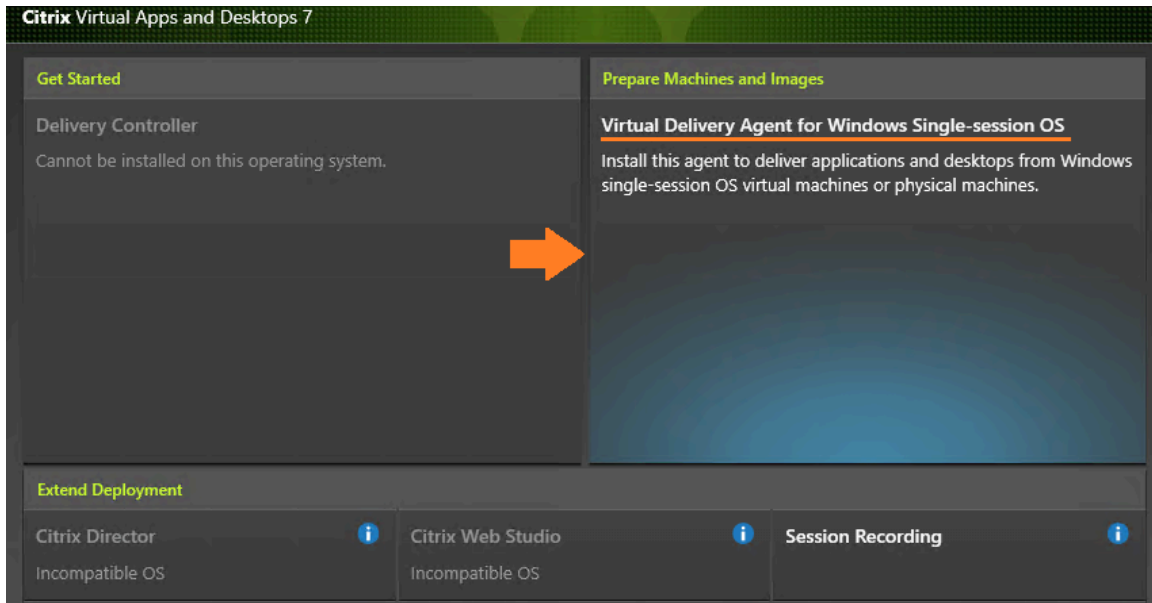
4. Click **AutoSelect**.



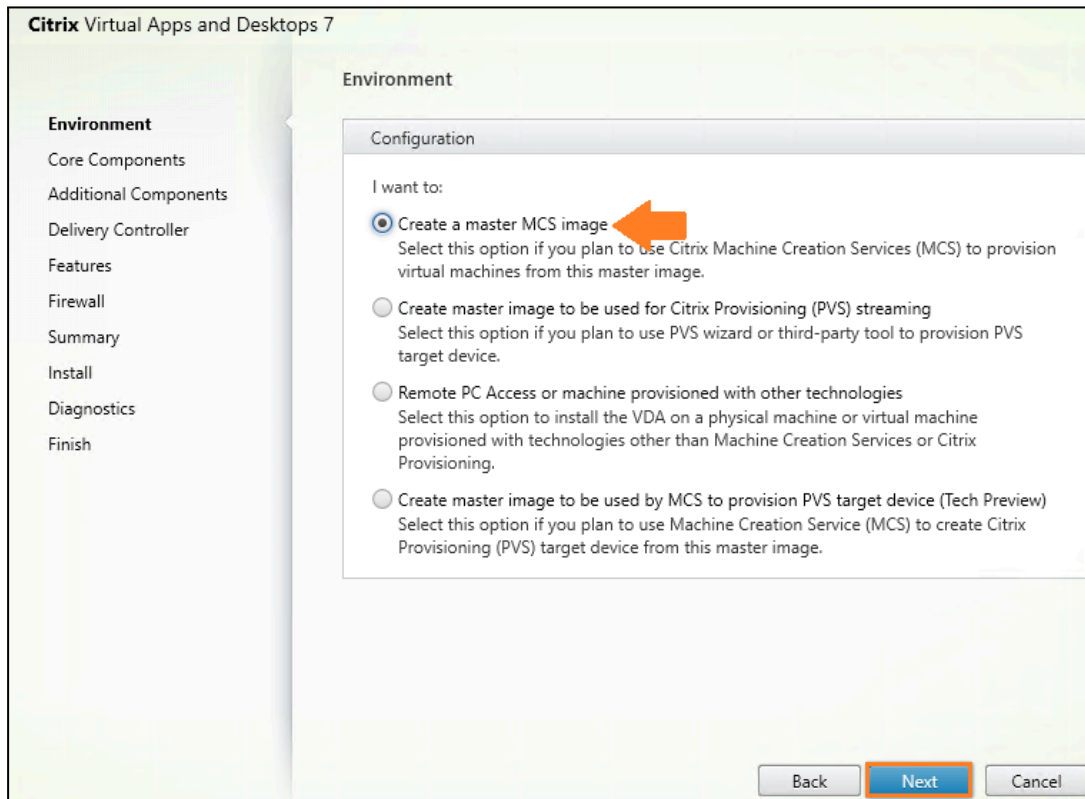
5. Click **Start** next to **Virtual Apps and Desktops**.



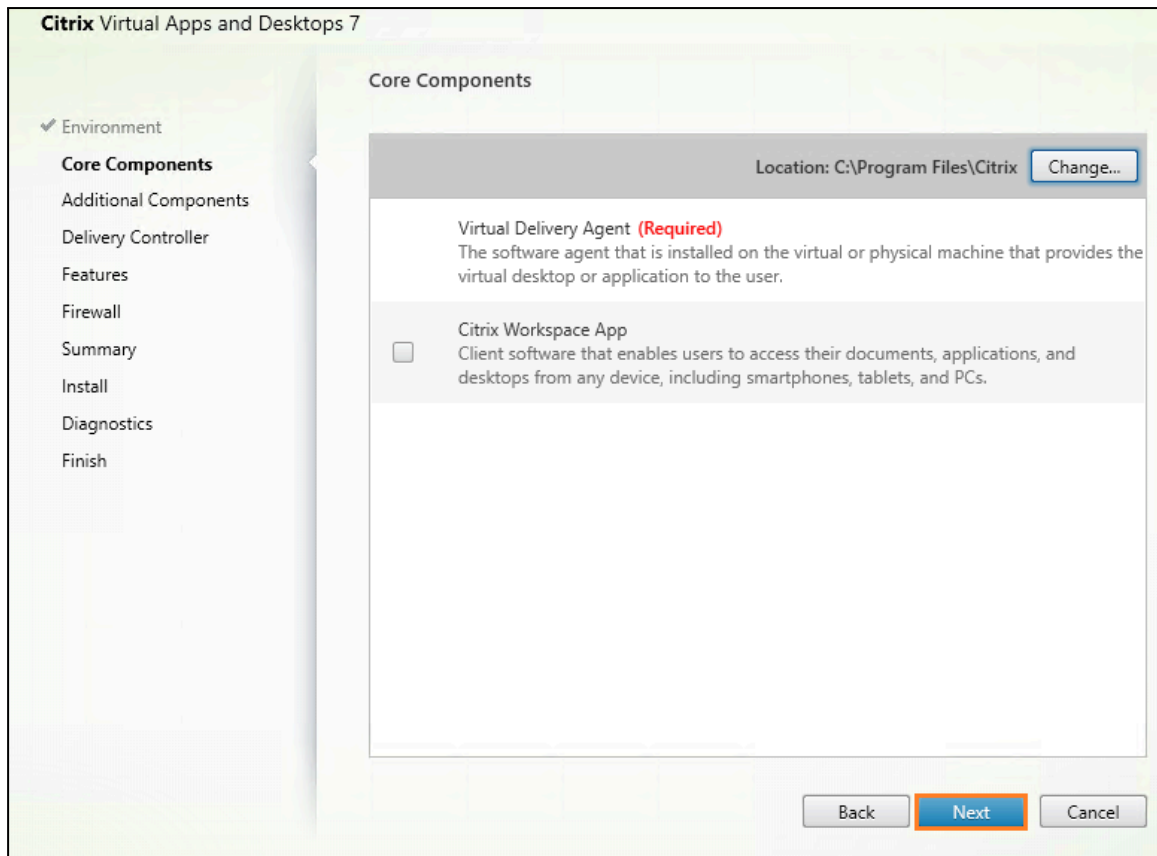
6. Select Virtual Delivery Agent for Windows Single-session OS.



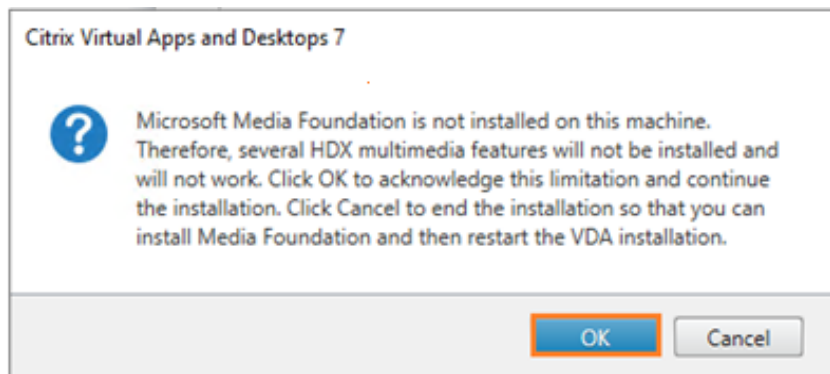
7. At the **Environment** screen, select **Create a master MCS image** and click **Next**.



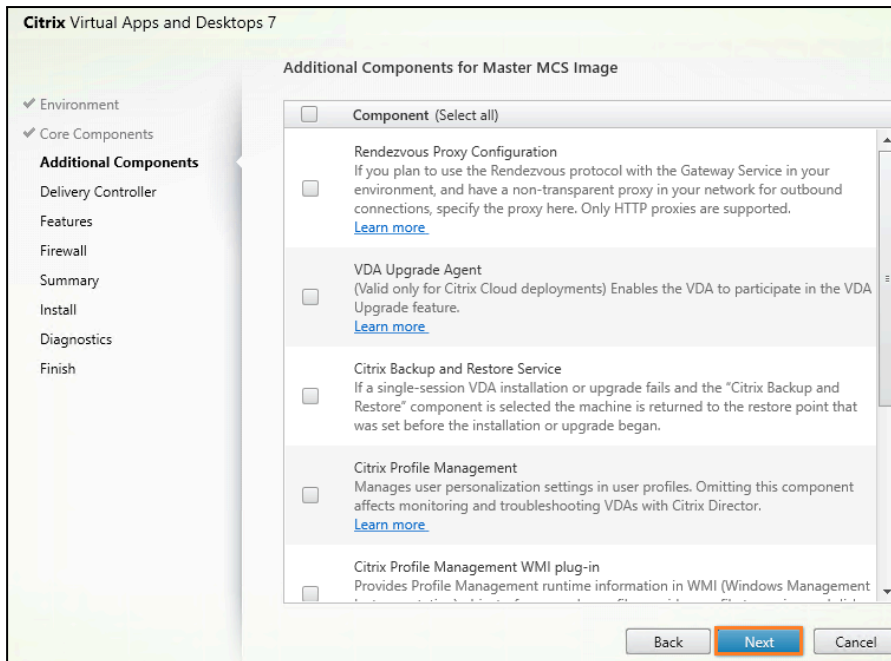
8. At the Core Components, click **Next**.



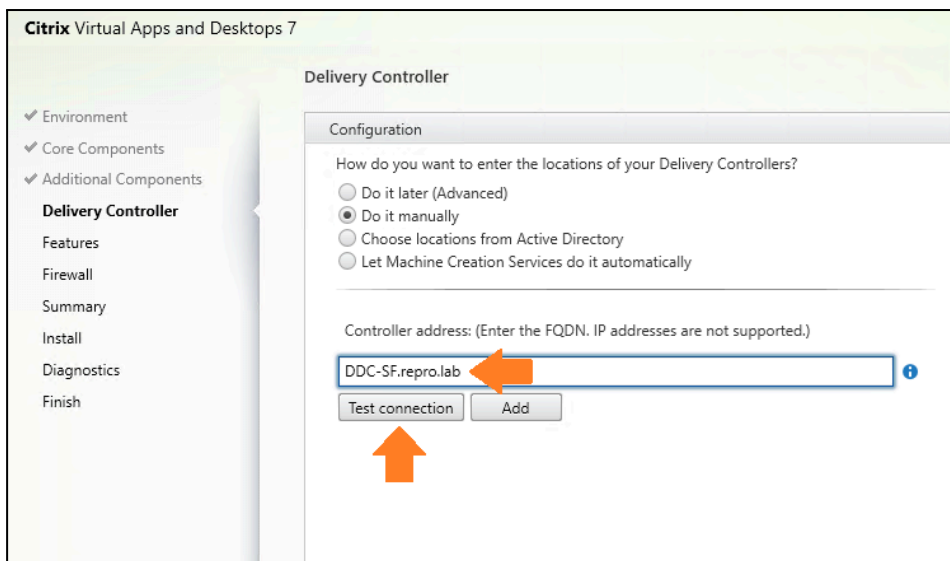
9. Click **Ok** (if you see this message).



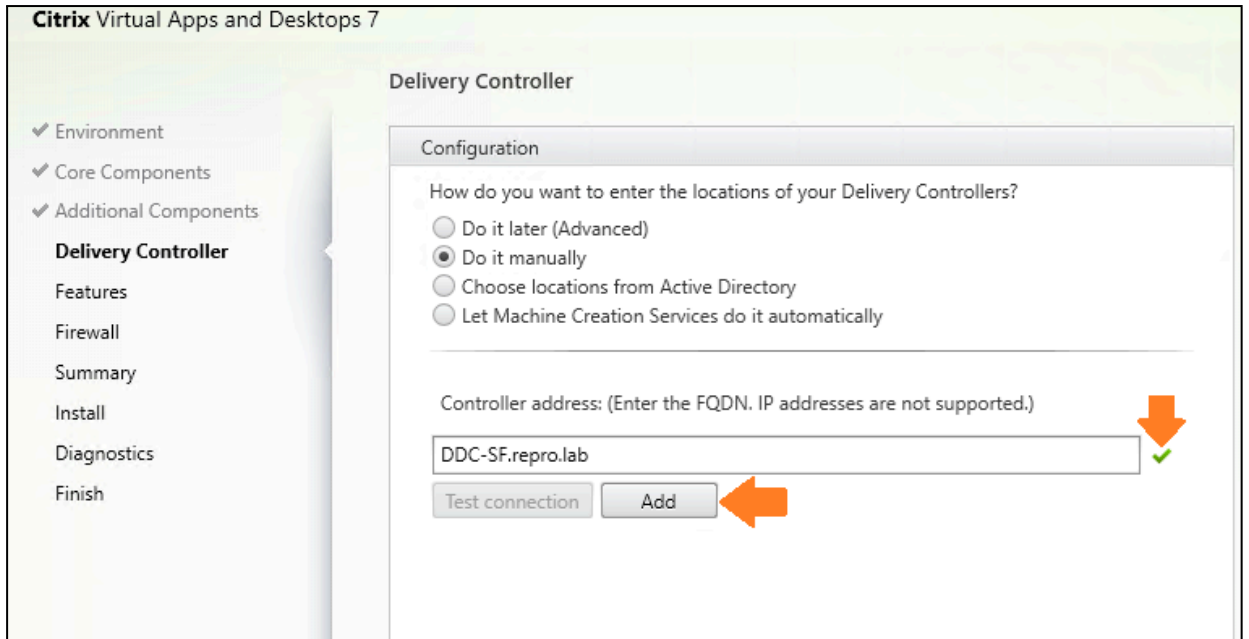
10. At the additional components, **UNSELECT** all the additional components and click **Next**.



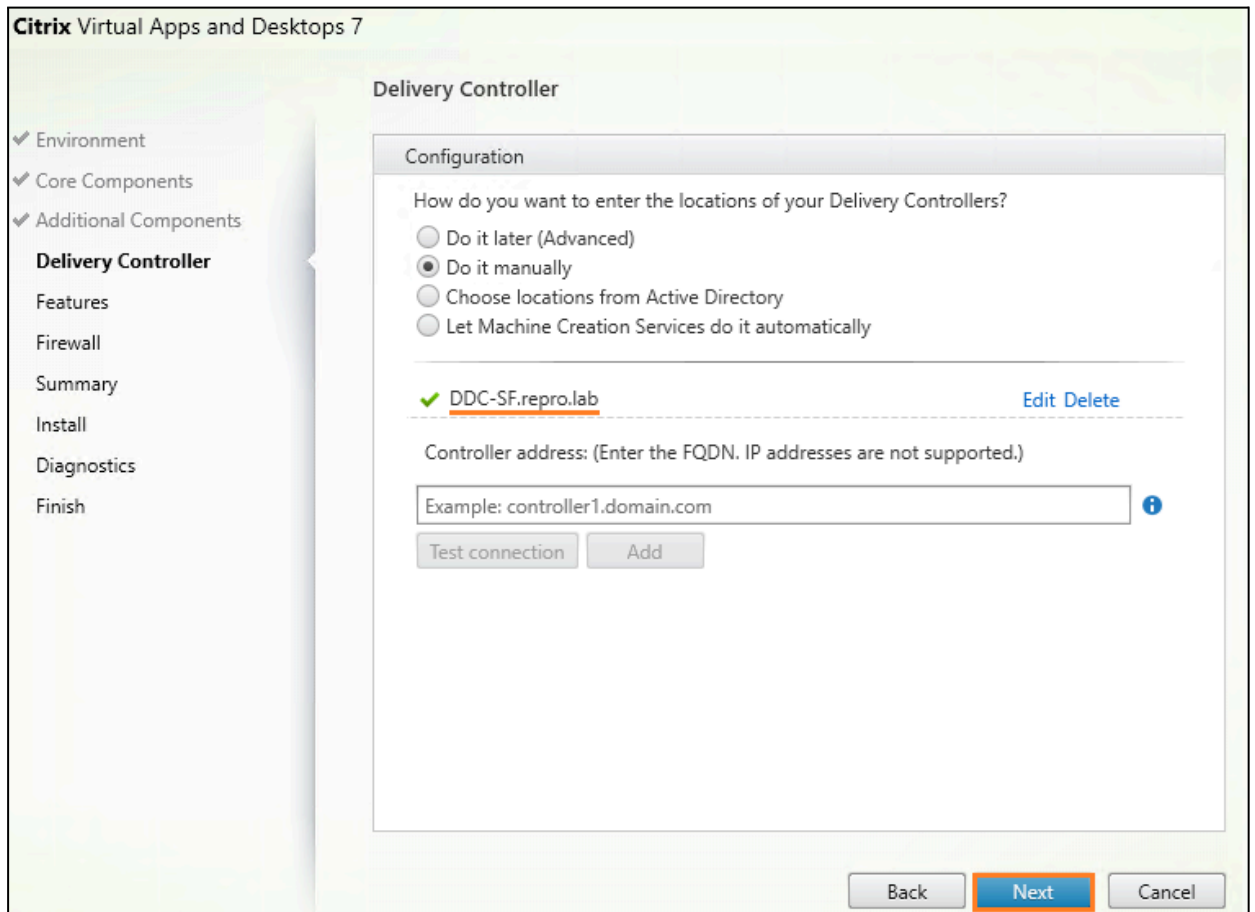
11. Add your DDC Hostname + domain (DDC-SF.repro.lab) and click **Test connection**.



12. Ensure you see the "green check" and then click **Add**.

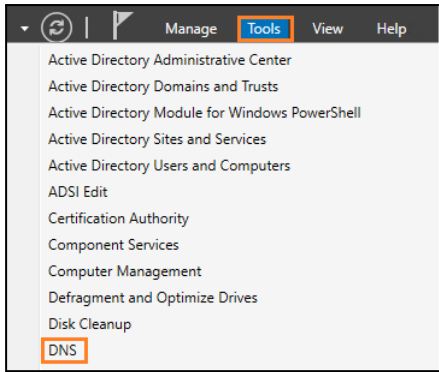


13. Click **Next**.

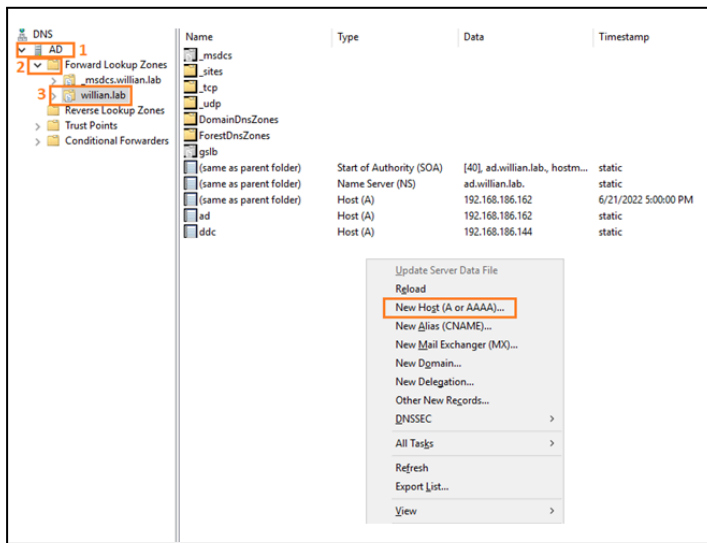


**NOTE:** Only follow the steps from 14 to 17 if you cannot resolve the domain name above.

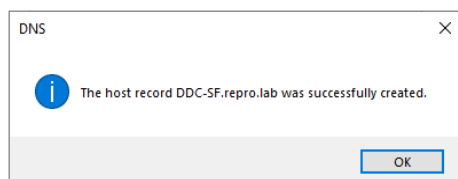
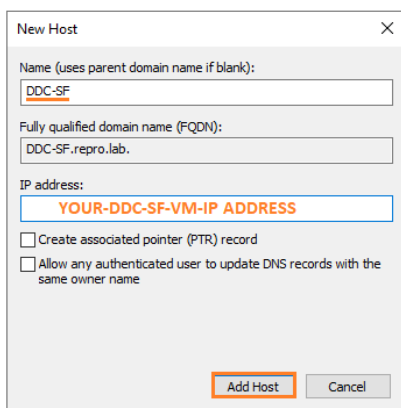
14. If you cannot resolve the name **DDC-SF.repro.lab**, add it to your DNS Server VM manually. Open your internal **Windows DNS server VM** and navigate to **Tools > DNS**.



15. Navigate to your domain. **AD > Forward Lookup Zones > Yourdomain.** On any white space, click with the right-button and select **New Host (A or AAAA)**...



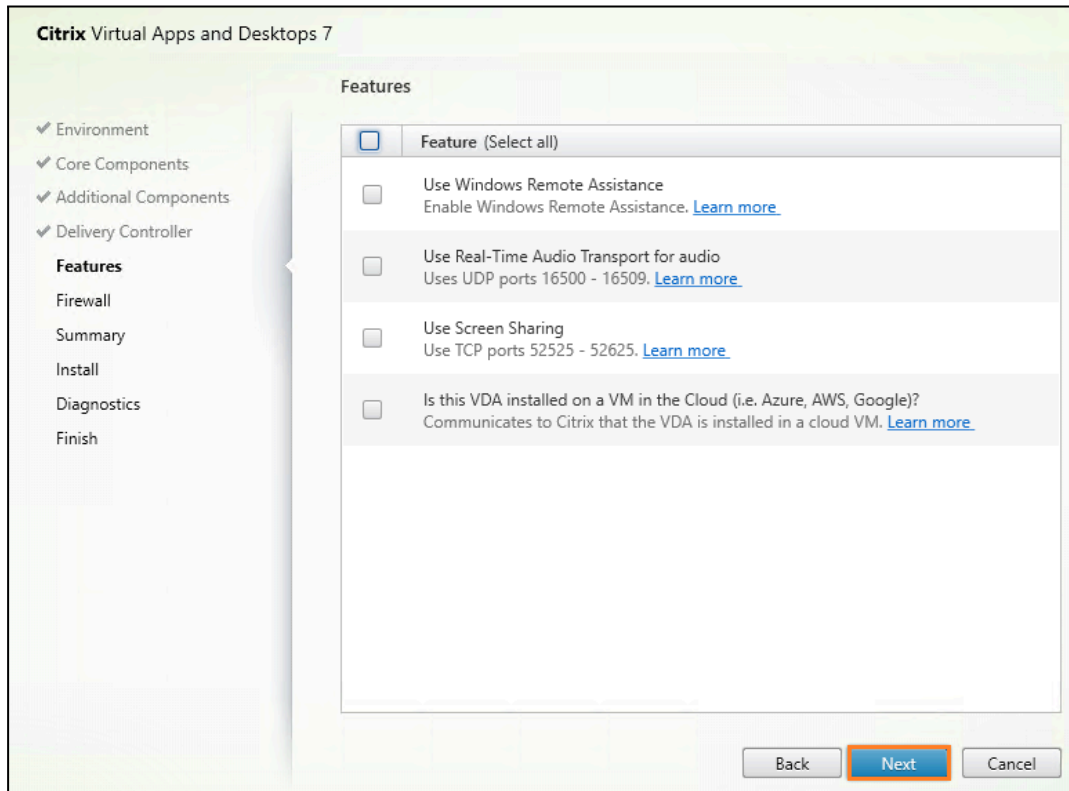
16. **Add** a host entry for your **DDC-SF**. You need to specify your **host + DDC-SF VM IP** (Access your DDC-SF VM, open the prompt command and type ipconfig. The IP you see for the VM is the IP you need to add below).



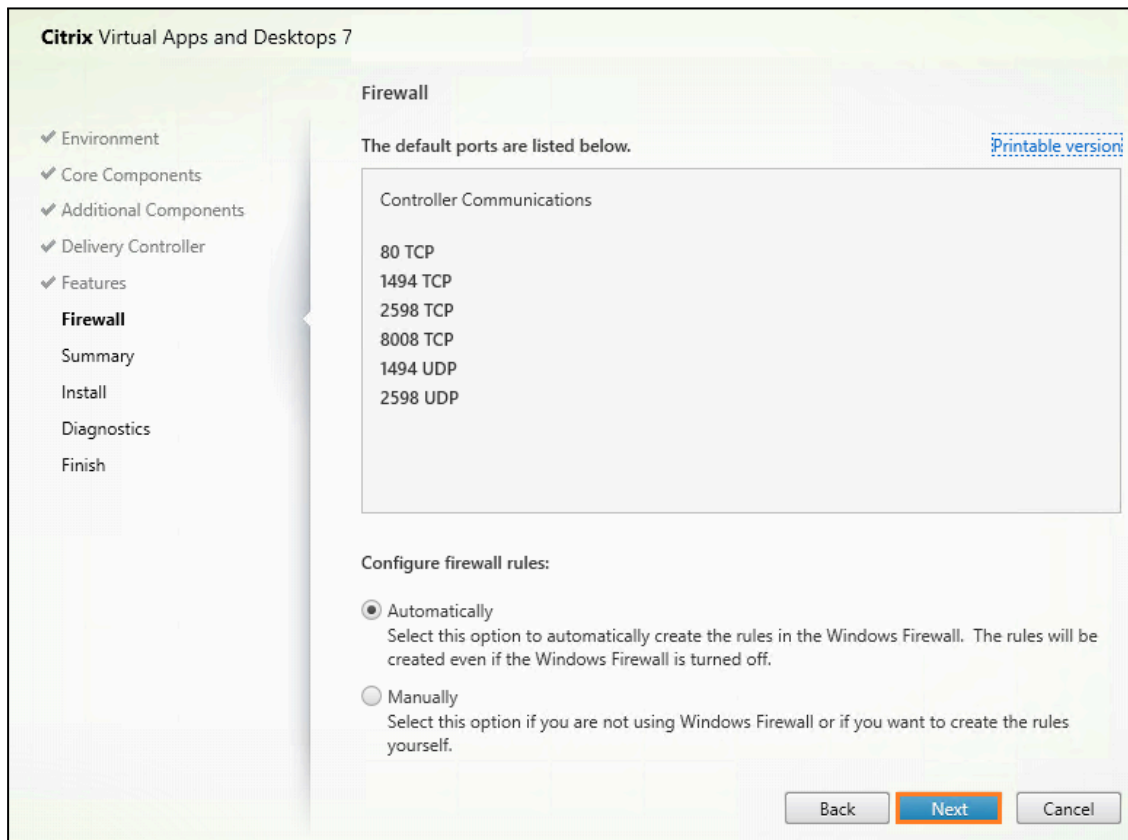


17. Try step 11 again and see if you can resolve the name this time (if it has failed before).

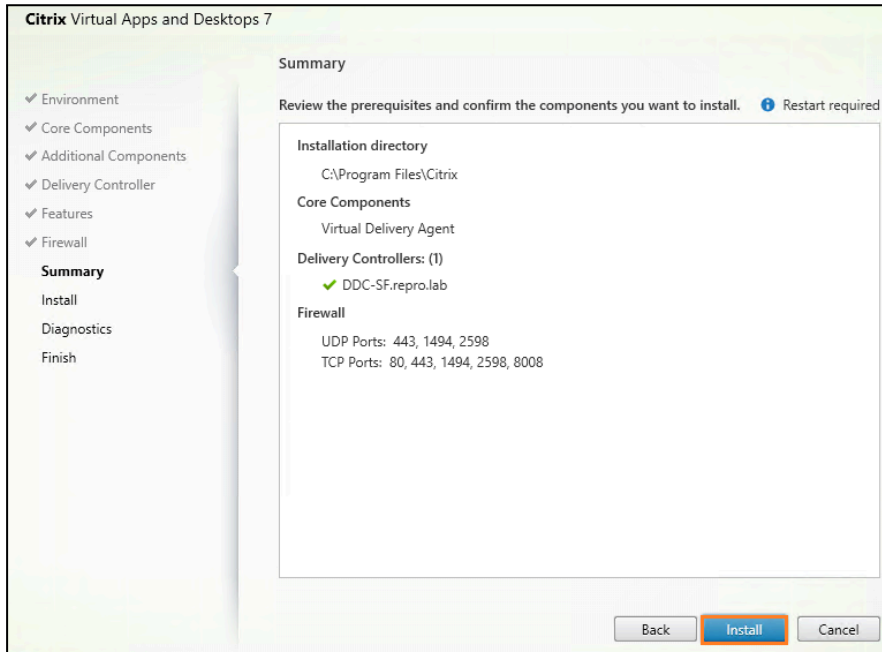
18. At the **Features** screen, click **Next**.



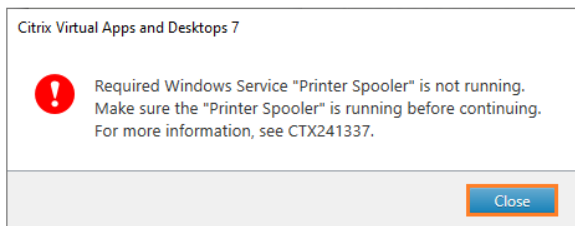
19. At the **Firewall** screen, click **Next**.



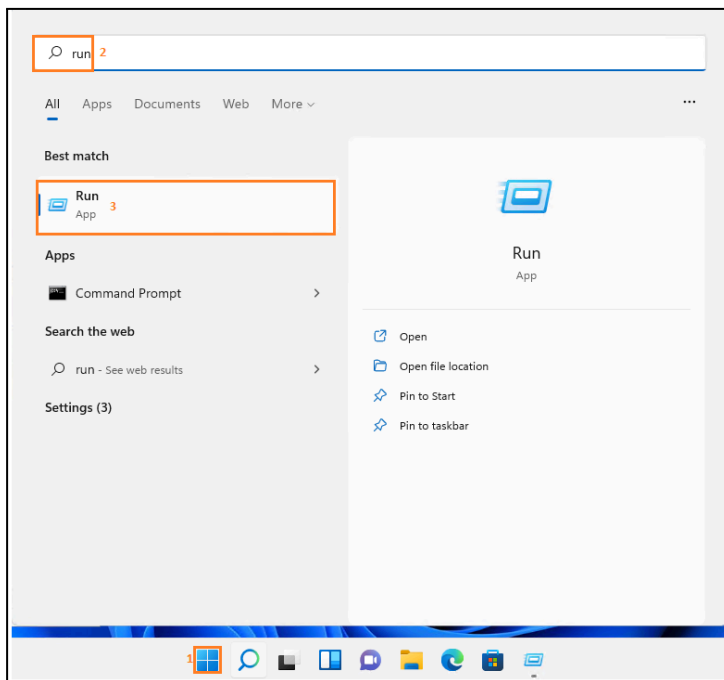
20. On the **Summary** screen, click **Install**.

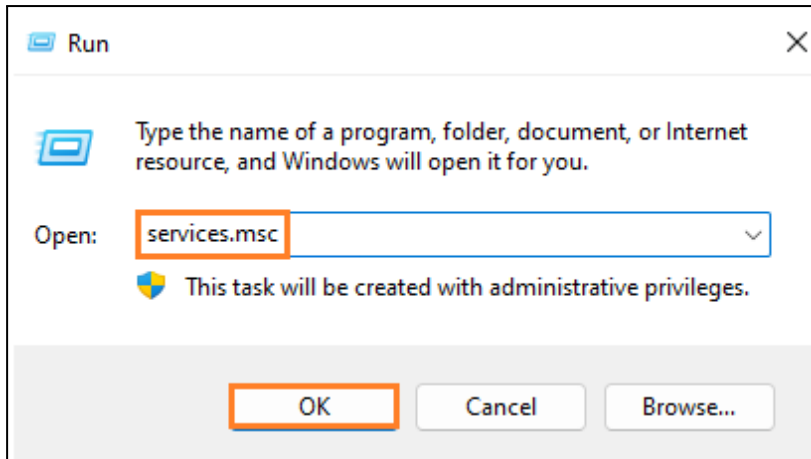


If you come across the below error, please start the Printer Spooler Service.

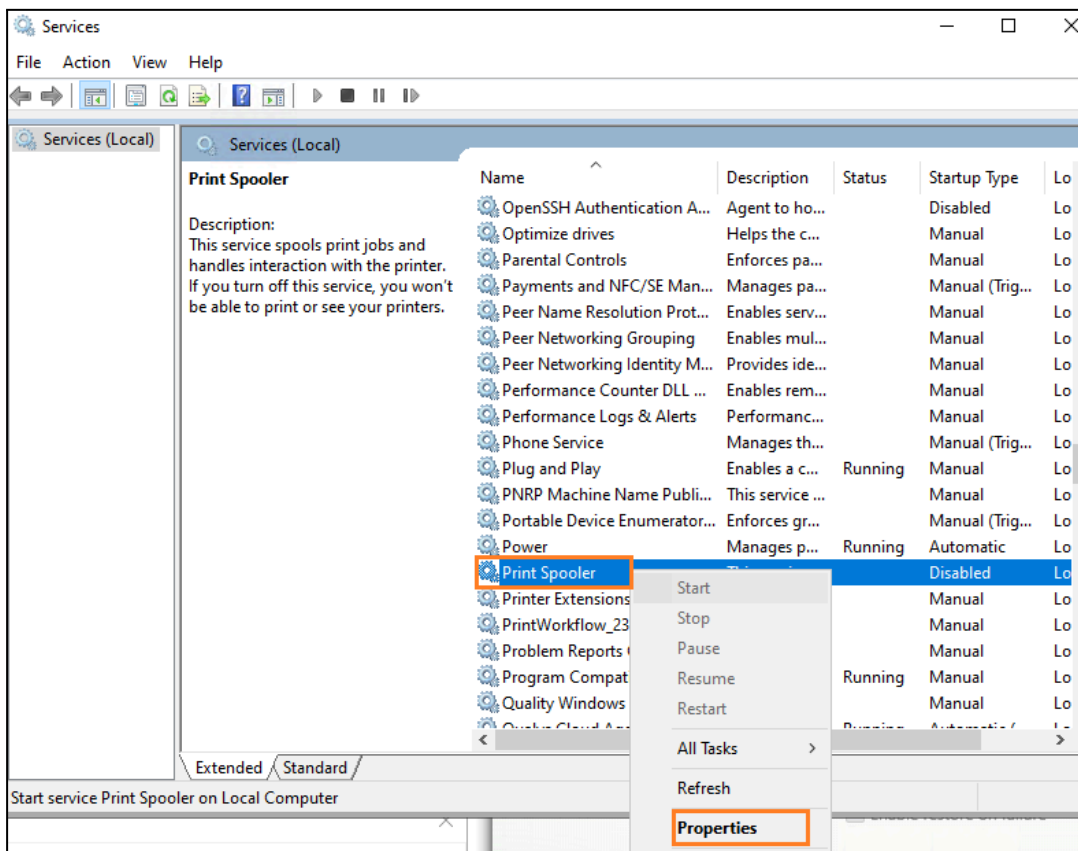


21. Navigate to **Run** and enter **services.msc**.

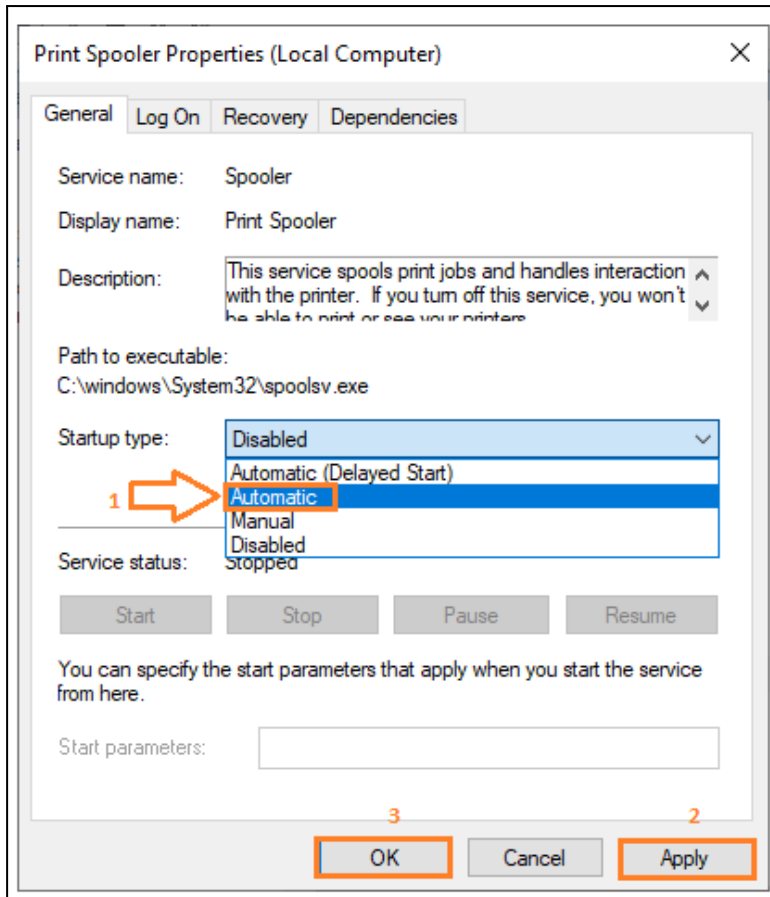




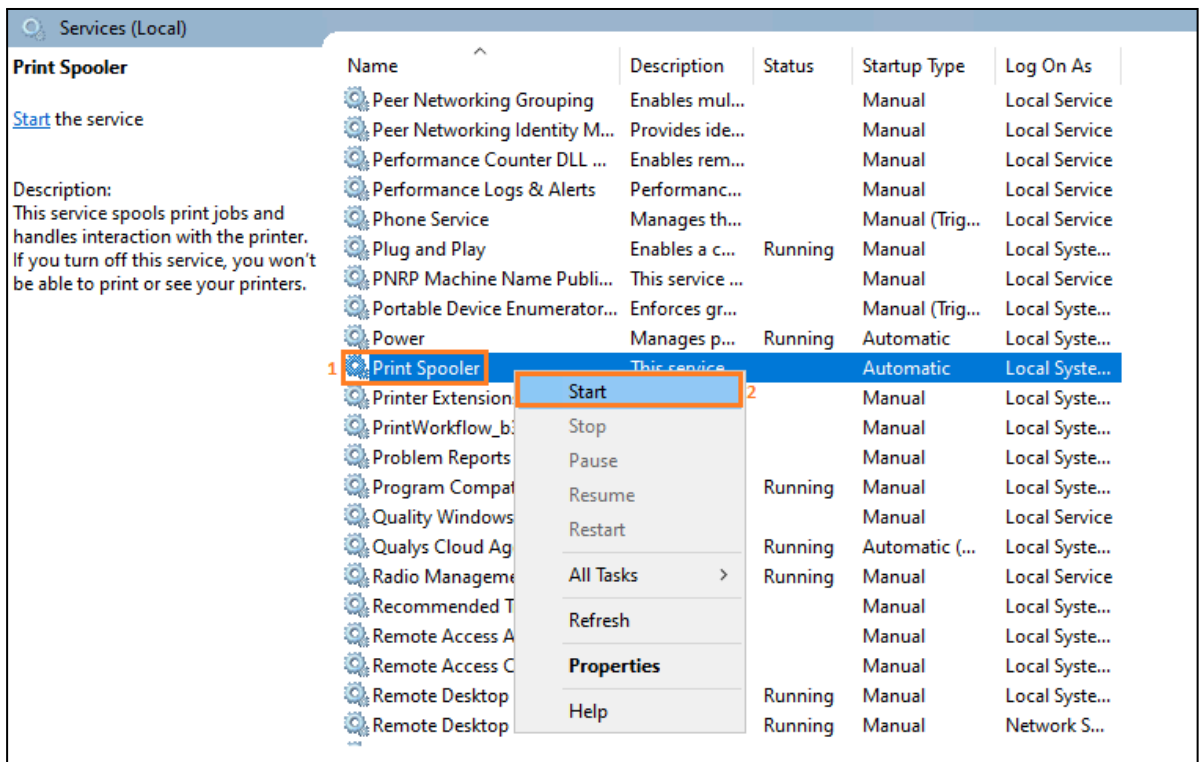
22. Right-click **Print Spooler** and click **Properties**.



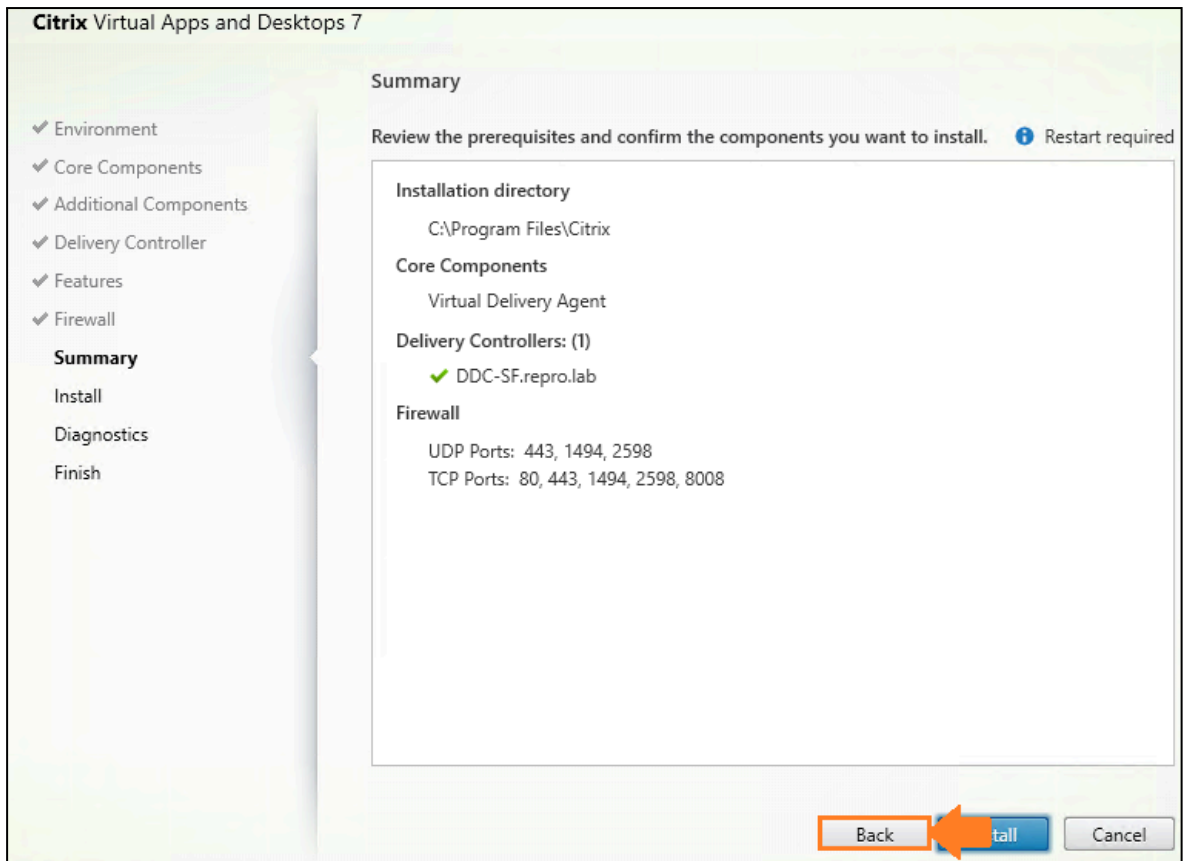
23. Click **Startup type** drop-down button, click **Automatic** list item to select it, click **Apply**, and then click **OK**.



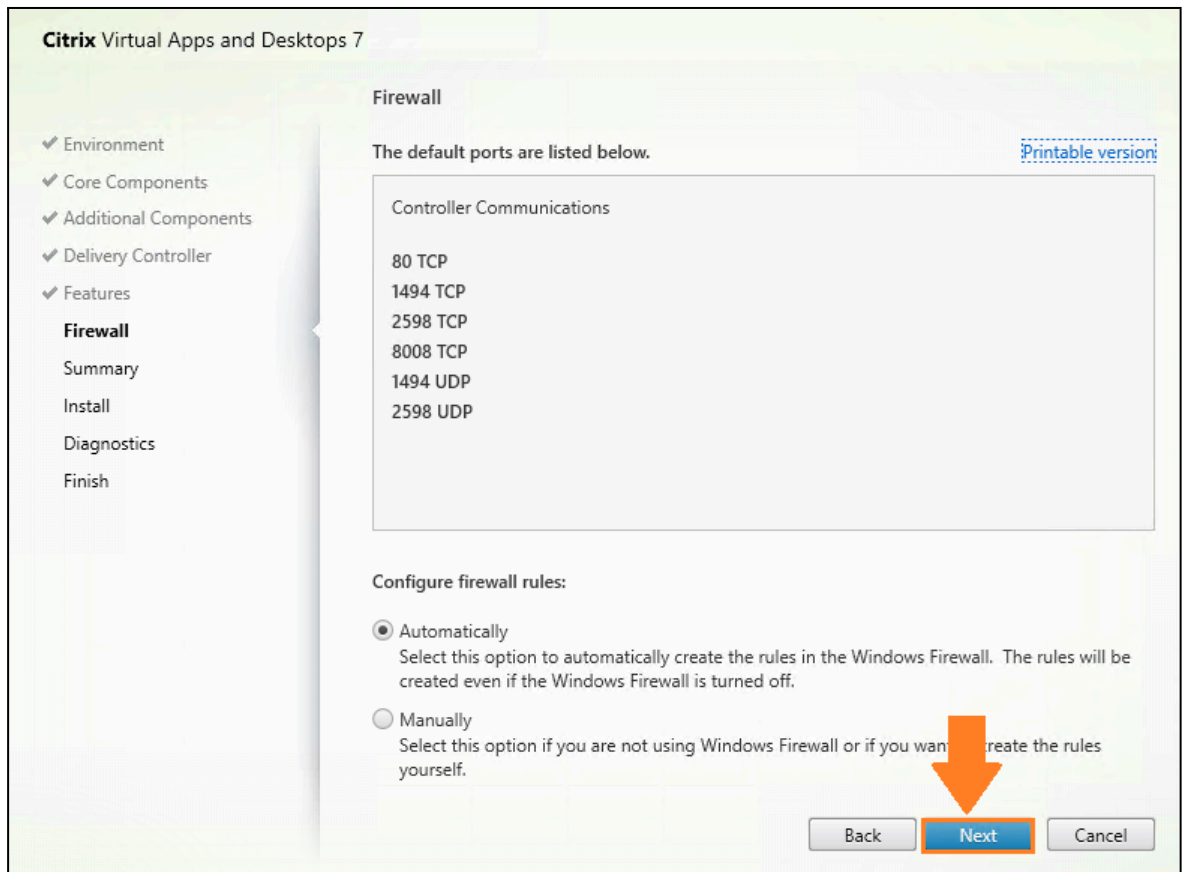
24. Right-Click **Print Spooler** and then click **Start**.



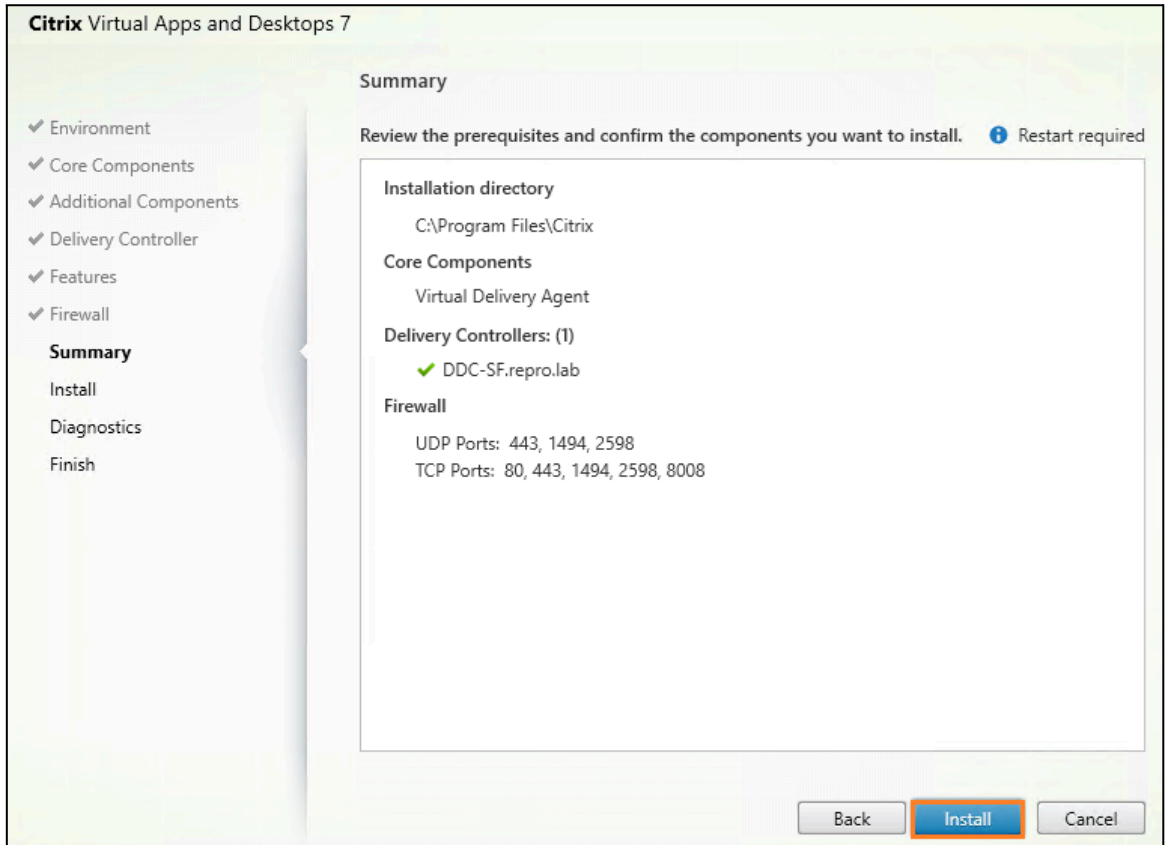
25. Return to the VDA installation, and then click **Back**.



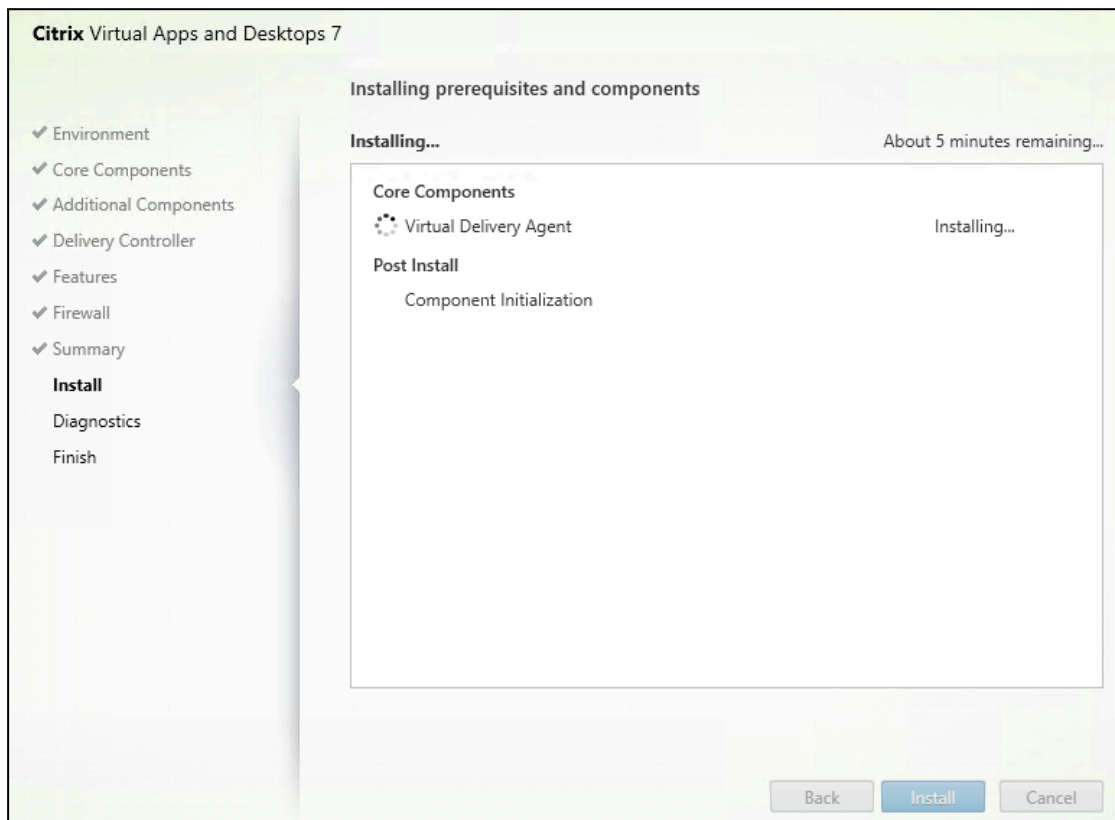
26. Click **Next**.



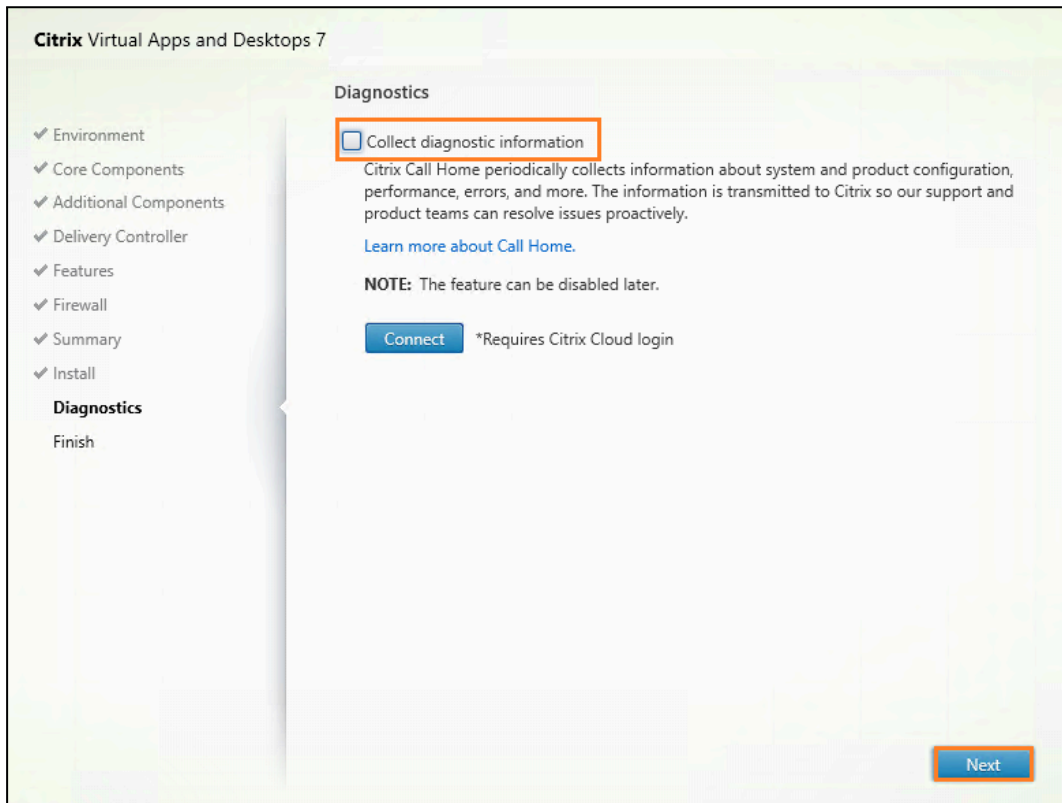
27. Click **Install**.



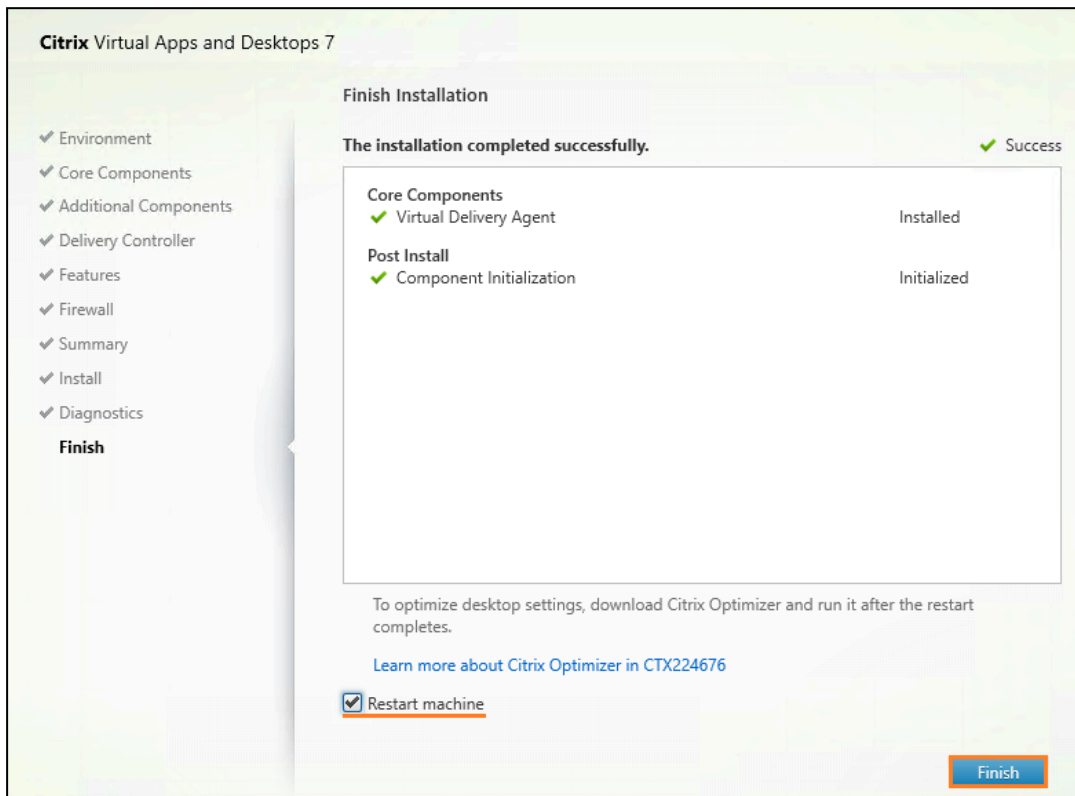
The installation will take a few minutes to complete.



28. Uncheck **Collect diagnostic information** and click **Next**.



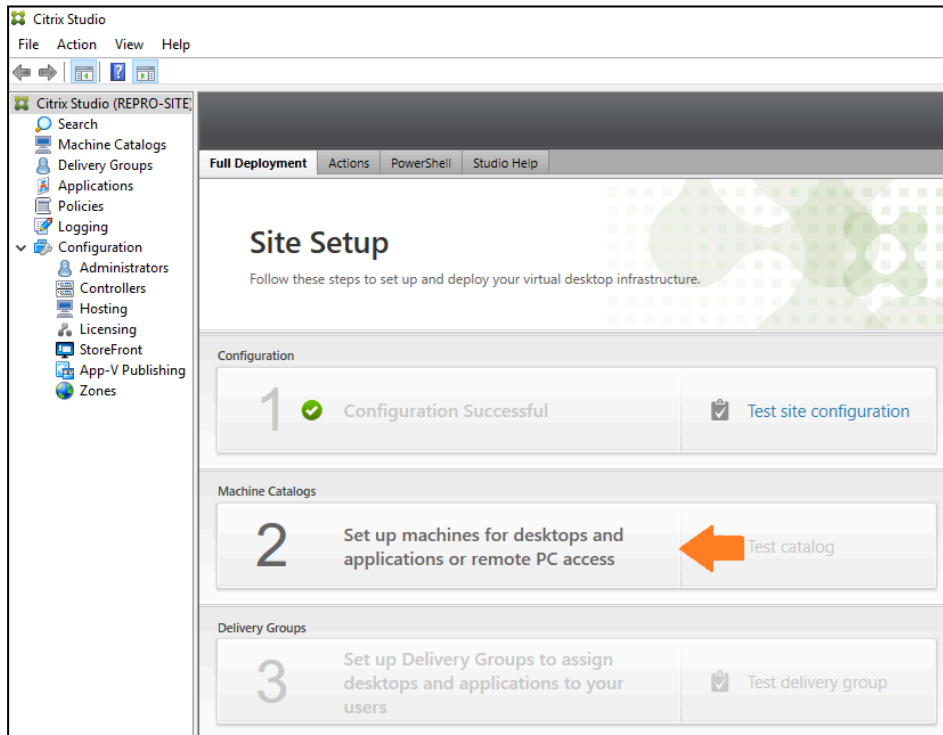
29. Click **Finish** and wait for the VDA VM to restart.



30. Return to the DDC-SF VM and complete the Machine catalog config.

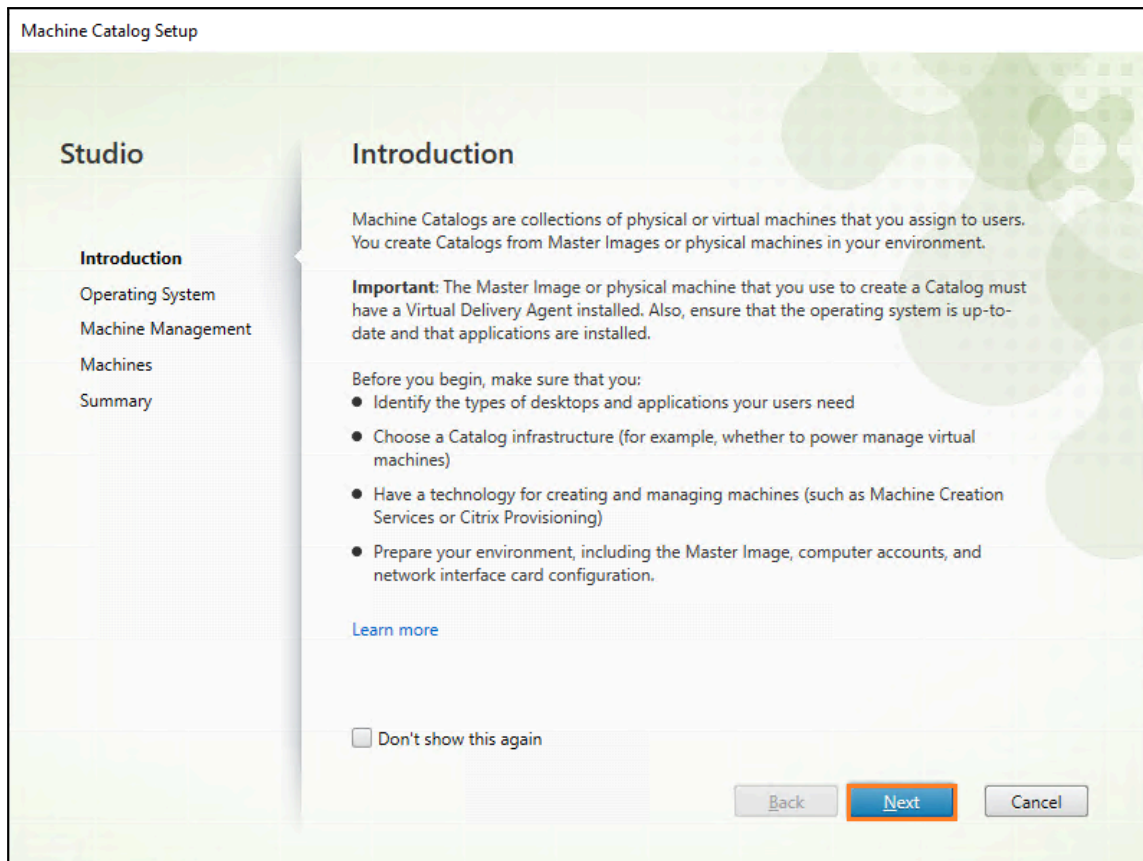
## Machine Catalog Configuration

1. Return to the DDC-SF VM, and open the Citrix Studio from the start menu should you closed it. Select “Set up machines for Desktop and Applications or Remote PC access” under “Machine Catalog”.

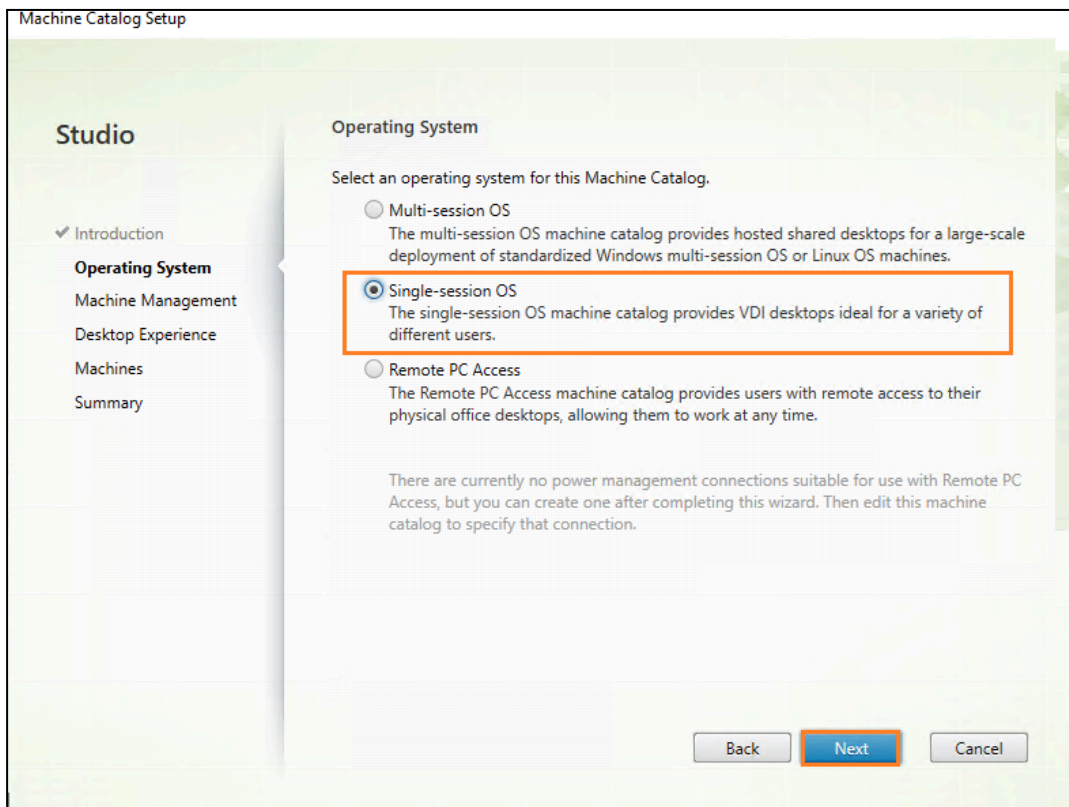


2. Click **Next**.

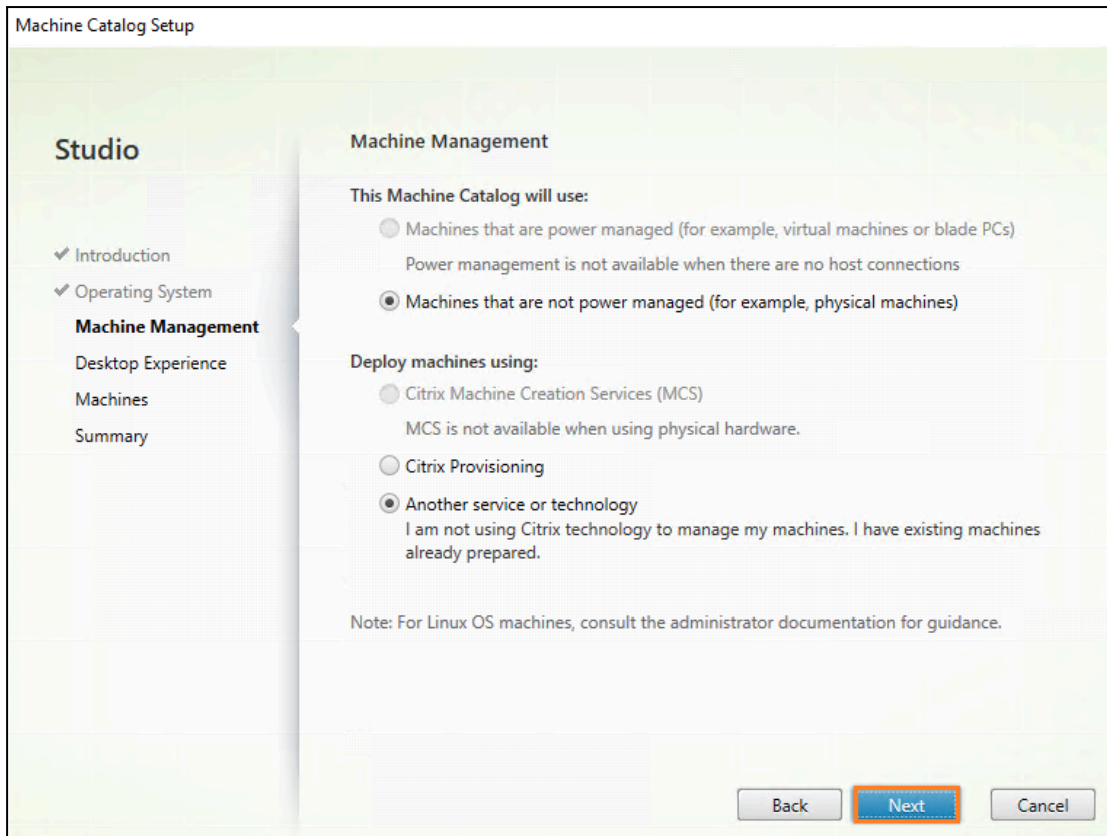




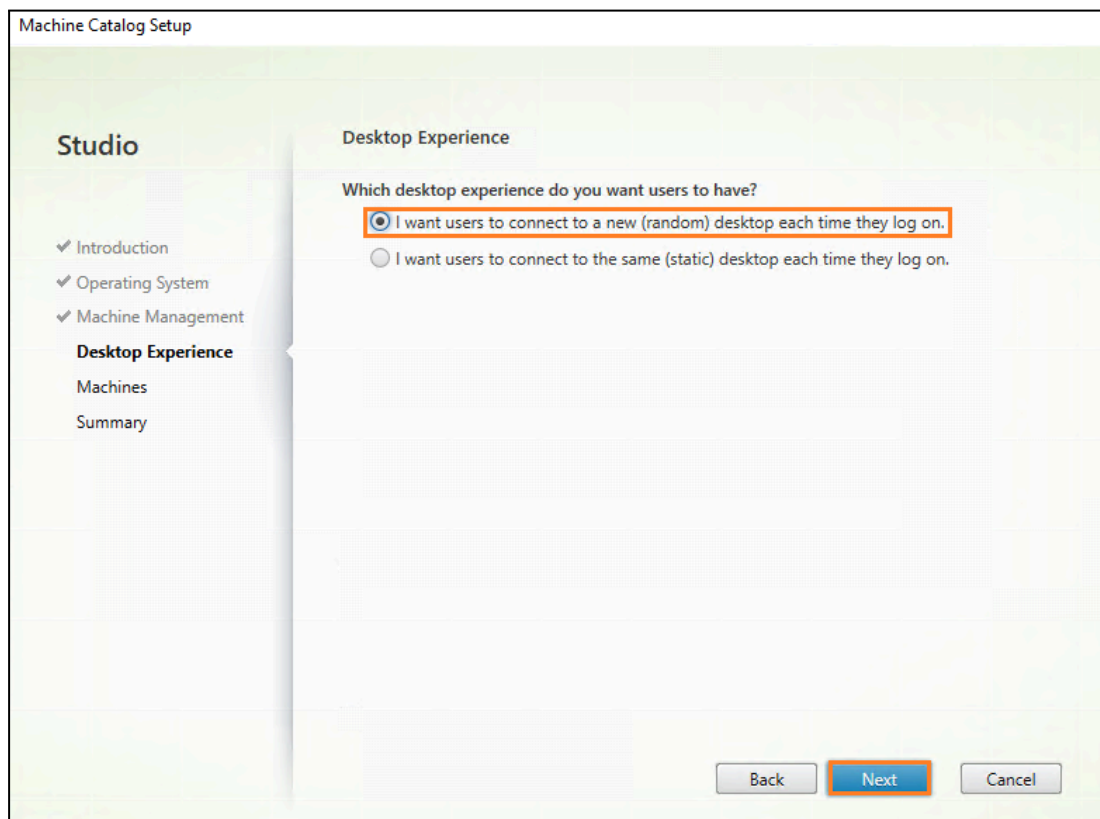
3. At the **Operating System** screen, select the **Single-session OS** type for your VDA and click **Next**.



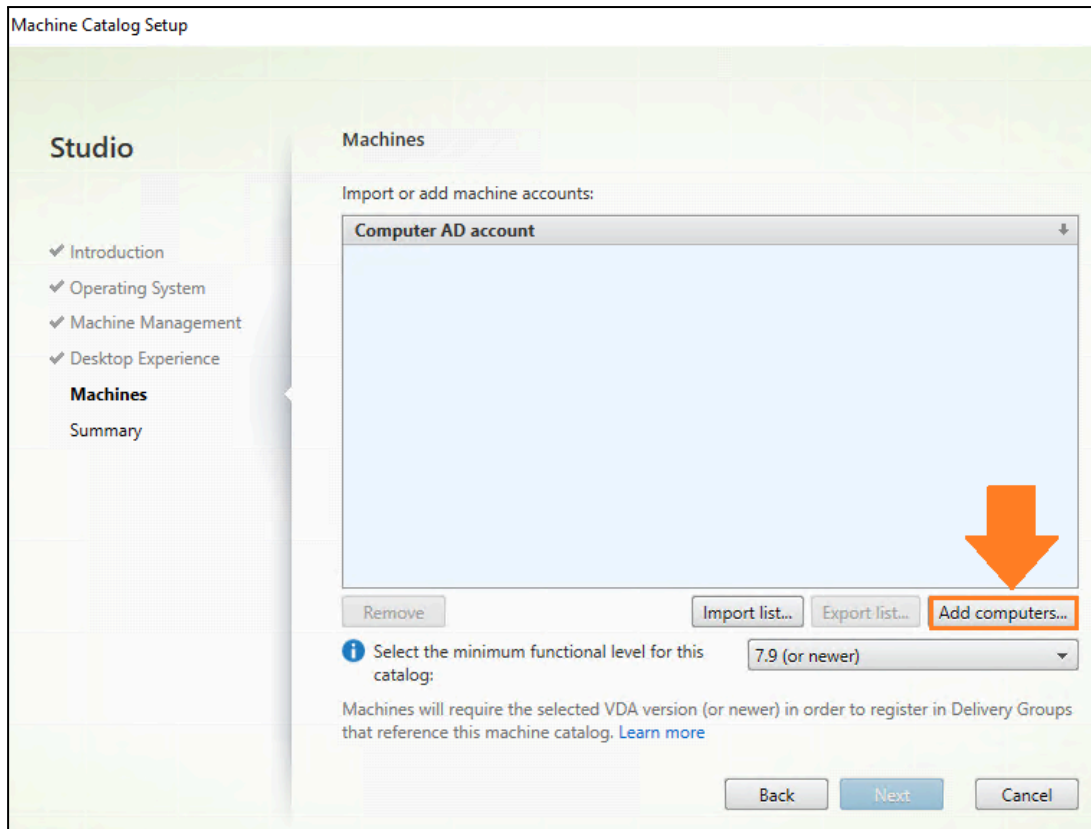
4. Click **Next**.



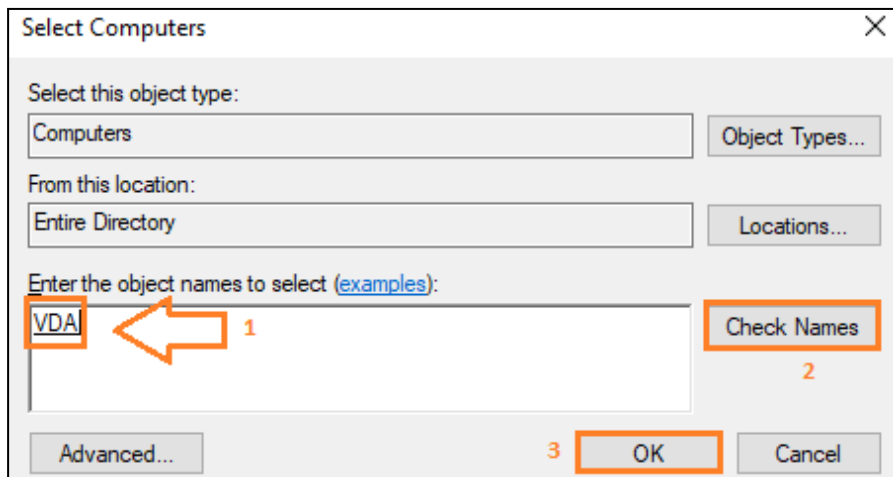
5. Select **I want users to connect to a new (random) desktop each time type log on**, and then click **Next**.



6. Click **Add Computers** to add your Windows 11 VDA.



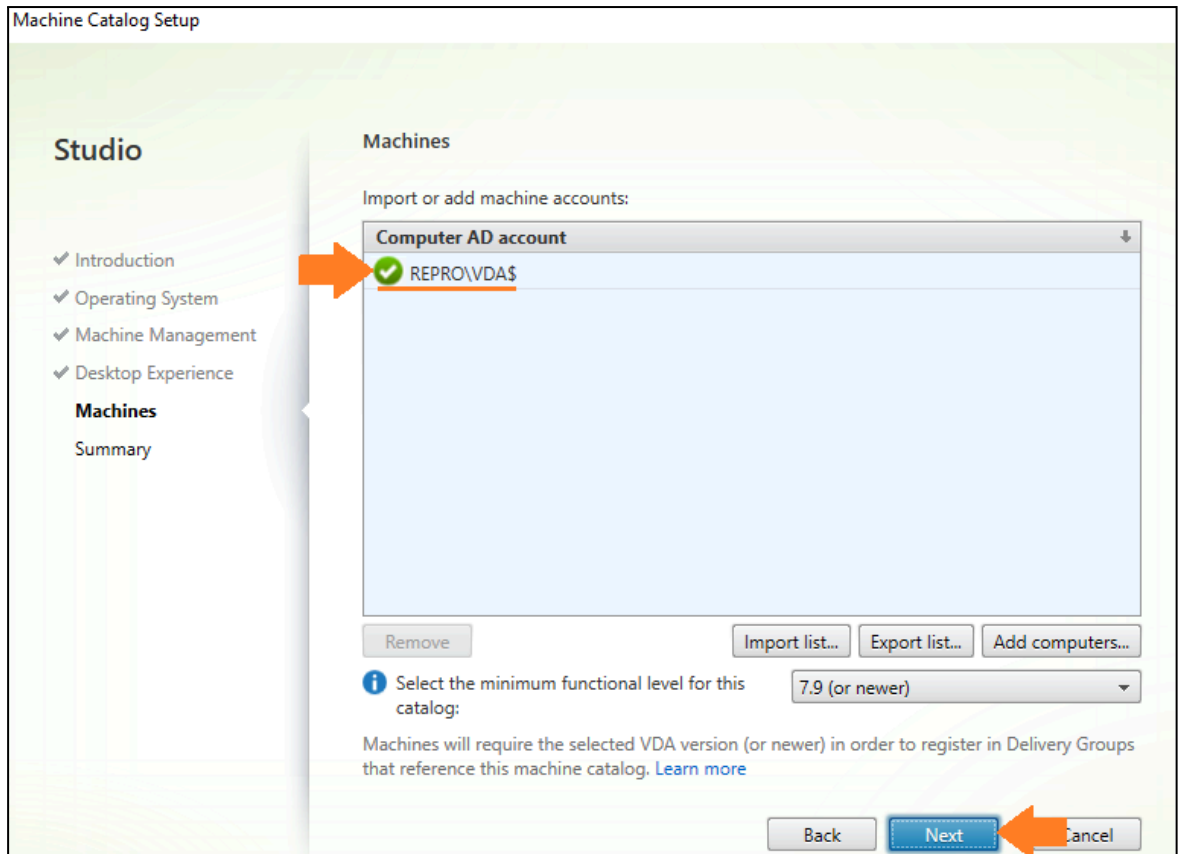
7. Enter the **hostname** of your **VDA** and click **Check Names**. Once your VDA name gets underlined, click **OK**.



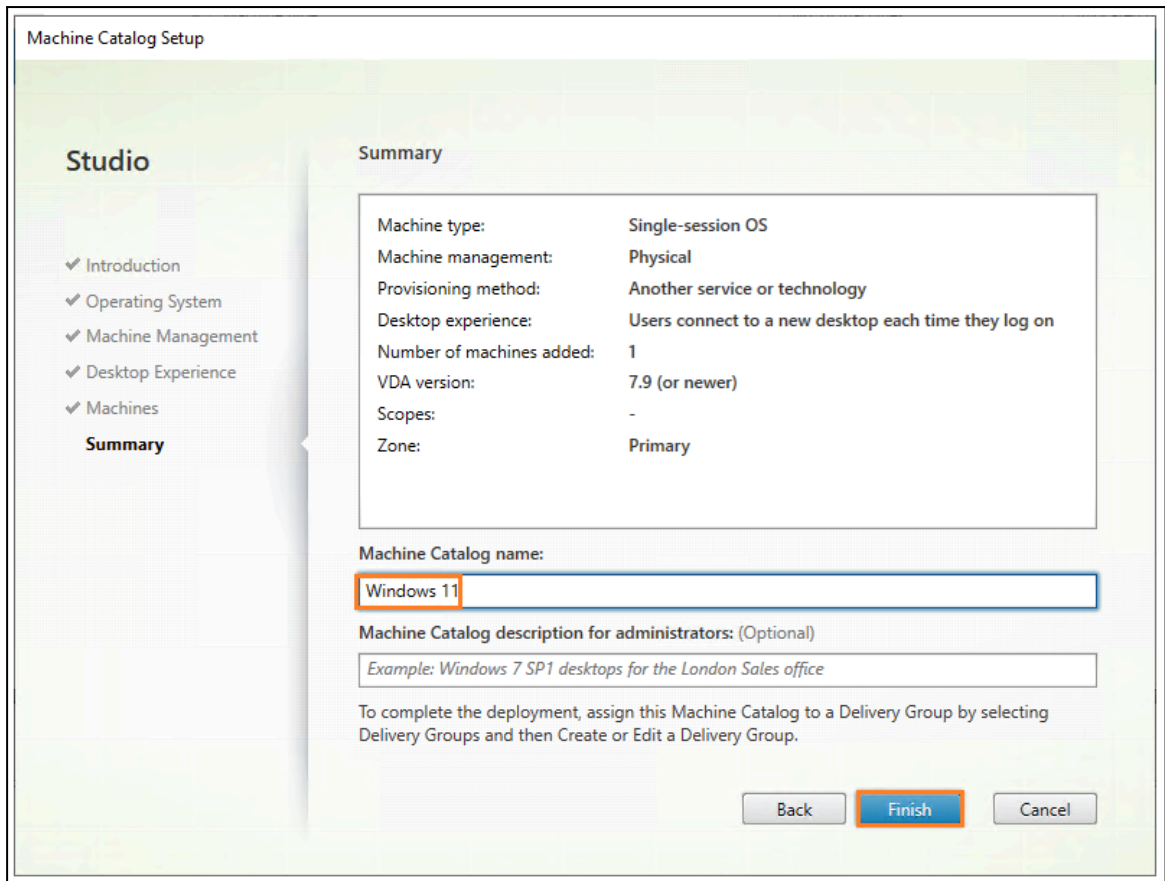
8. Make sure you see next to your **Domain\VDA\$** a **green check**, it indicates your VDA VM is ready. Click **Next**.

**NOTE:** If you do not see the **green check**, ensure you finished the VDA installation, and that you have entered the correct **DDC-SF hostname address** when you installed the VDA.

If everything on the VDA VM seems to be correct, click cancel on the above step, reboot the VDA VM, wait a few minutes, and try again to add the VDA to the Machine Catalog and confirm you see the "green check".

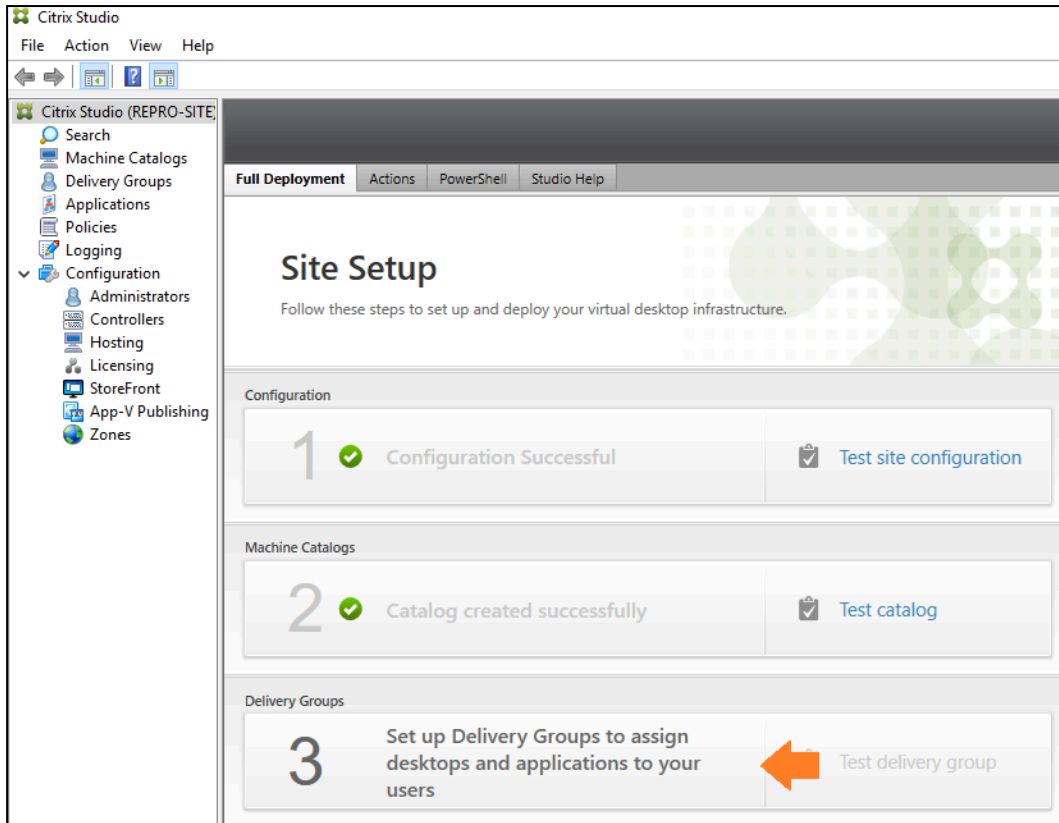


9. On the Summary screen, enter a name in the **Machine Catalog name** input field and click **Finish**.

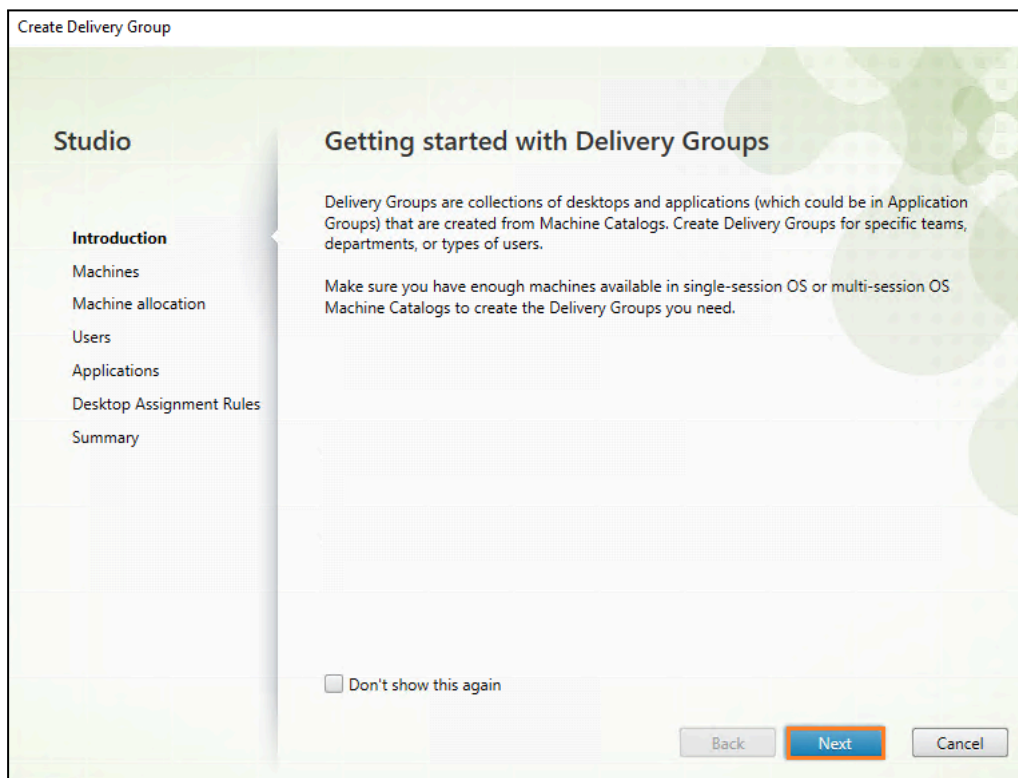


## Delivery Group Configuration

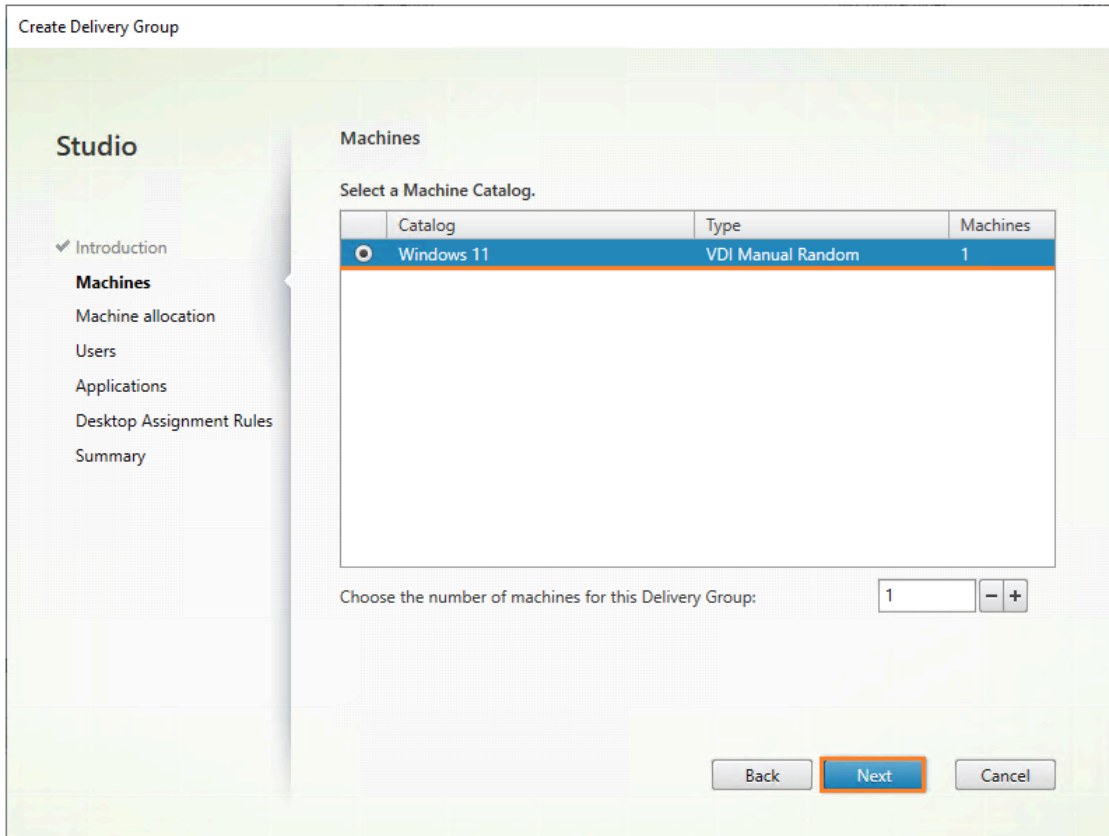
1. Click **Create a new Delivery Group**. If it shows in blank, click the **Refresh** button on the right side.



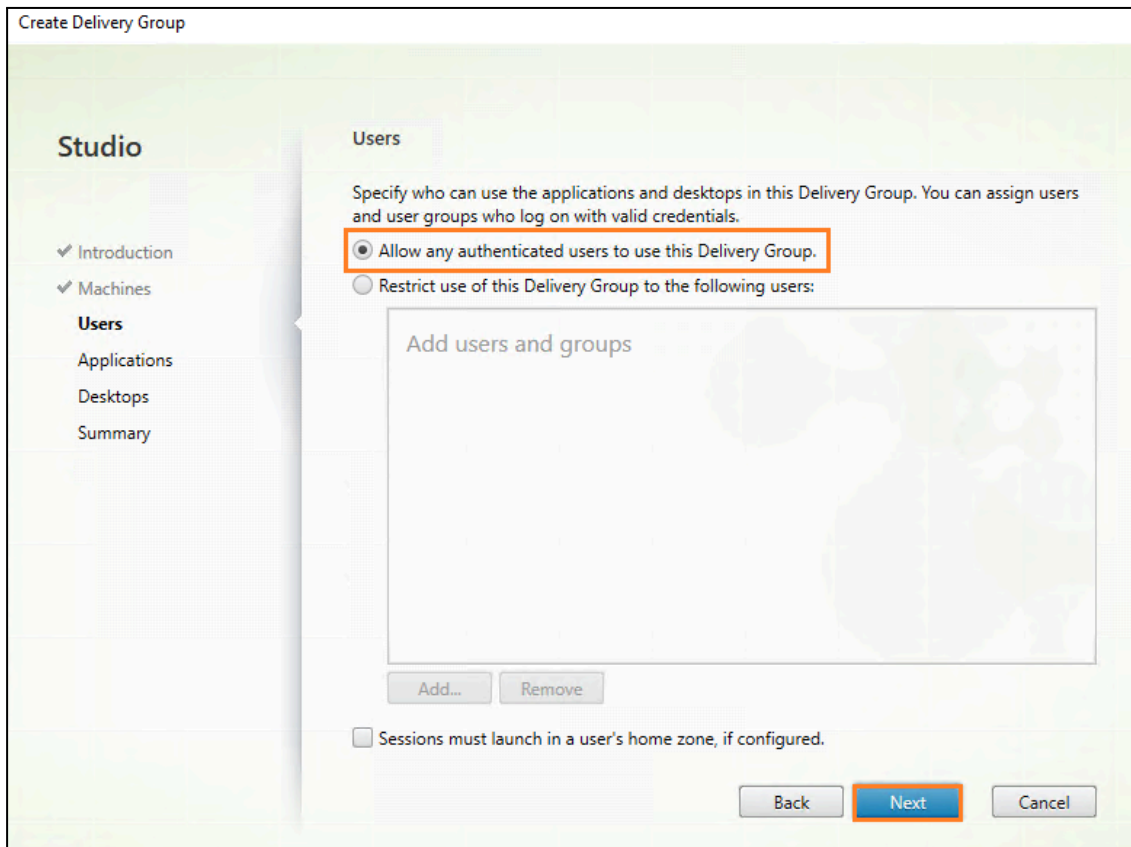
2. Click **Next** at the Getting Started screen.



3. Select your **Windows 11 VDA** as part of the Delivery Group and click **Next**.

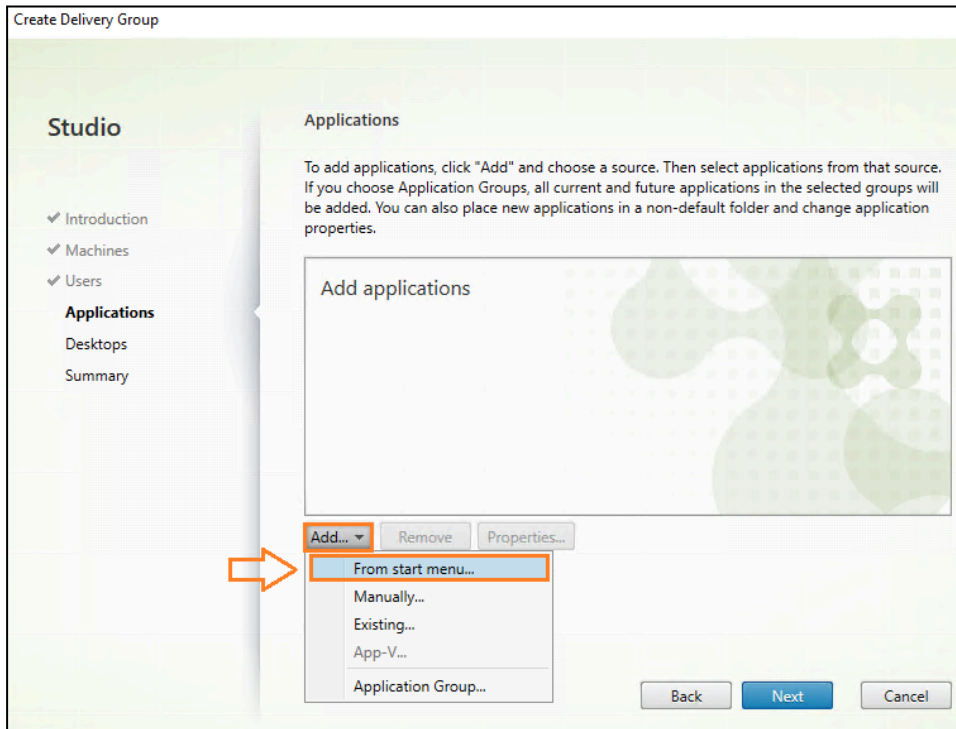


4. Click the **Allow any authenticated users to use this Delivery Group** radio button and then click **Next**.

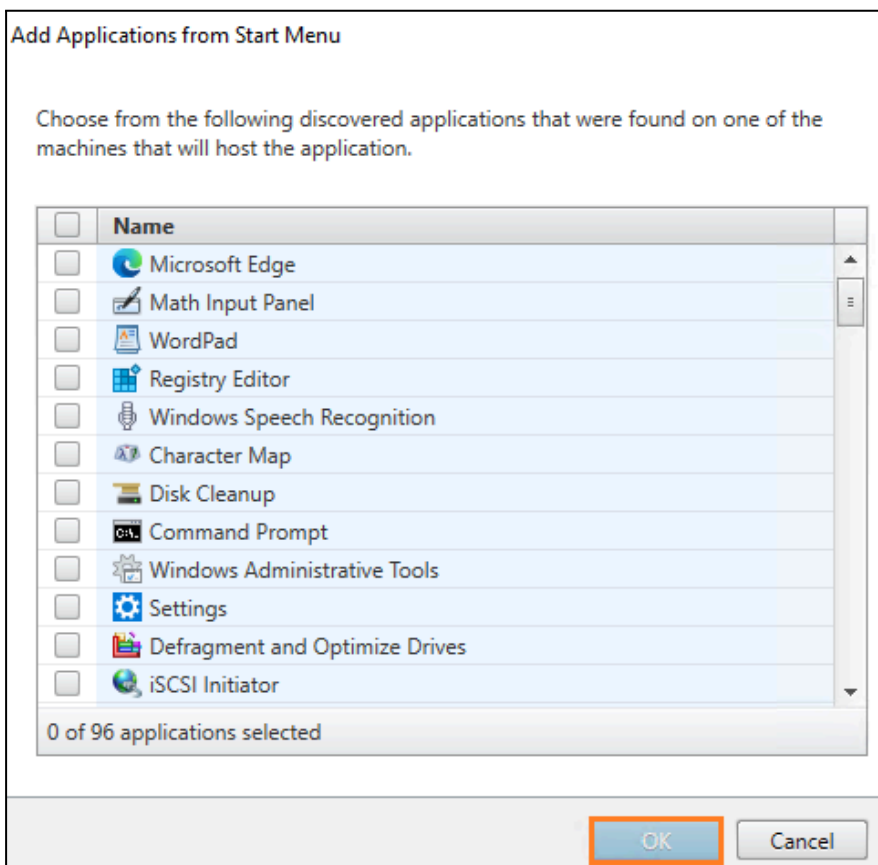




5. You can publish some applications from your **Windows 11 VDA** that can be used by the users. Click the **Add** drop-down button and then select the **From start menu** list item.

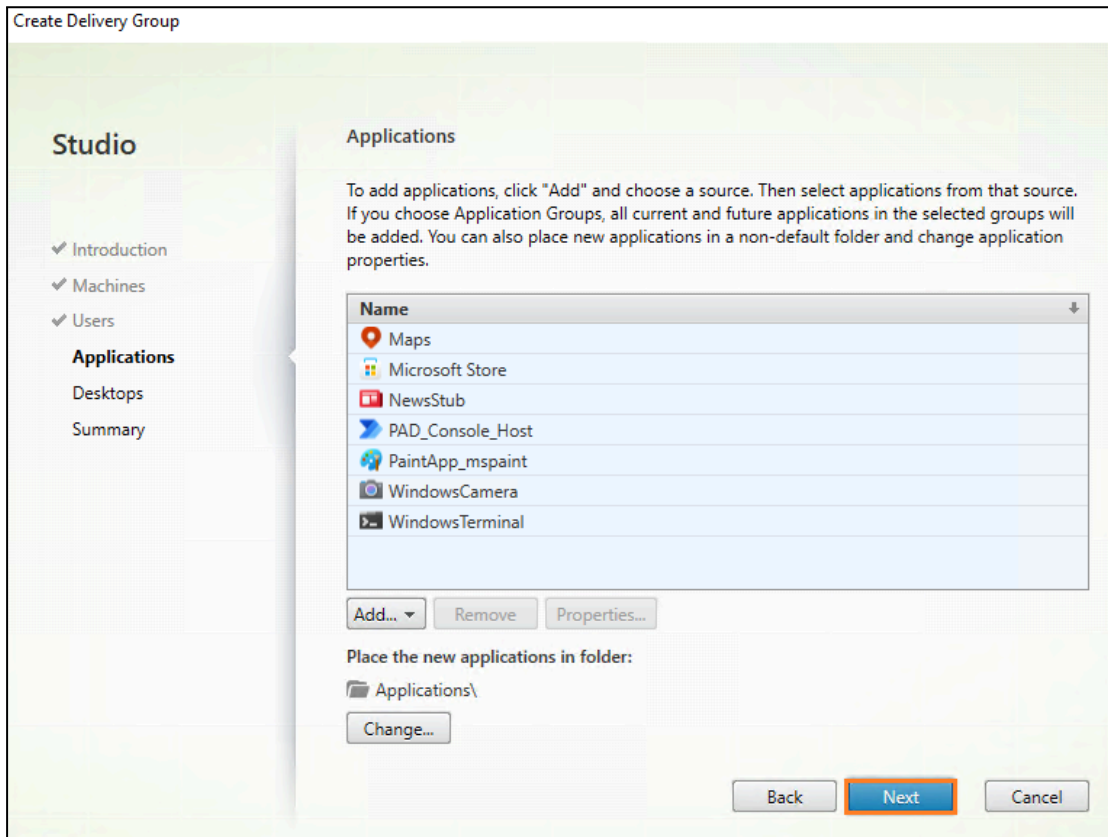


6. Select a couple of applications to publish and click **OK** (you can select anything).

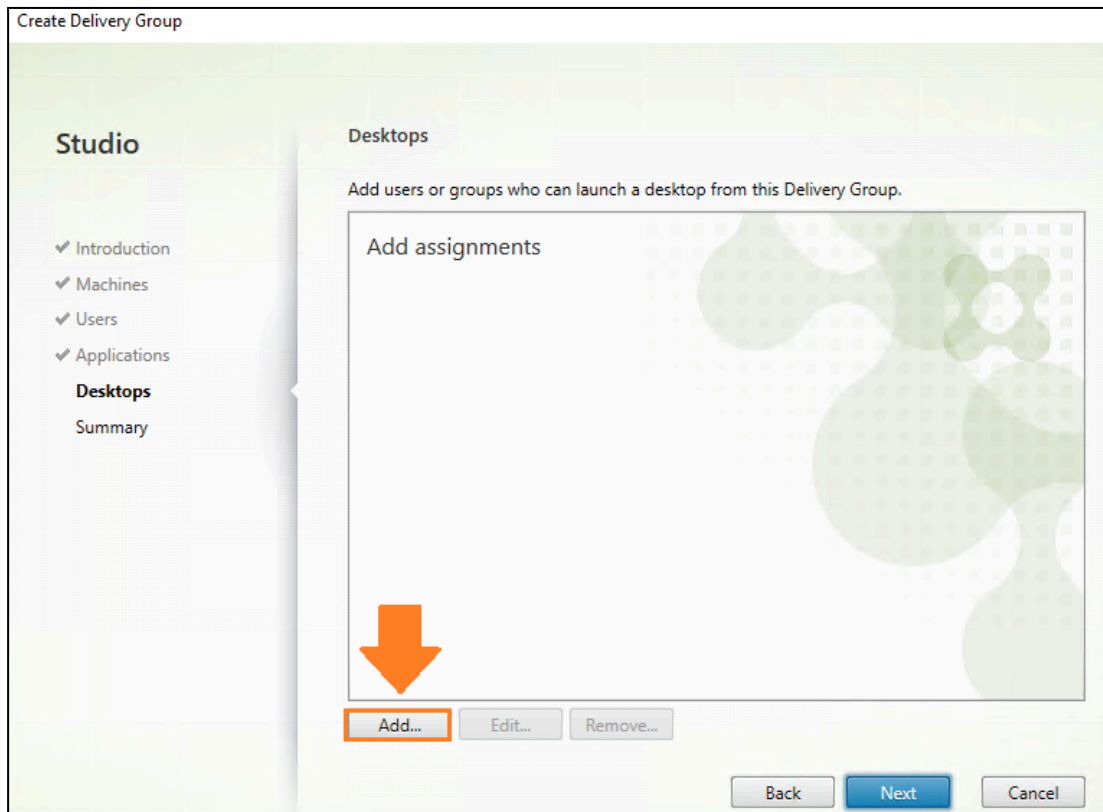




7. Click **Next**.



8. Add your **Windows 11 VDA** to the delivery group, and click **Add**.



9. Enter a **Display Name** for the VDA and click **OK**.

Add Desktop

Display name:

Description:

The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

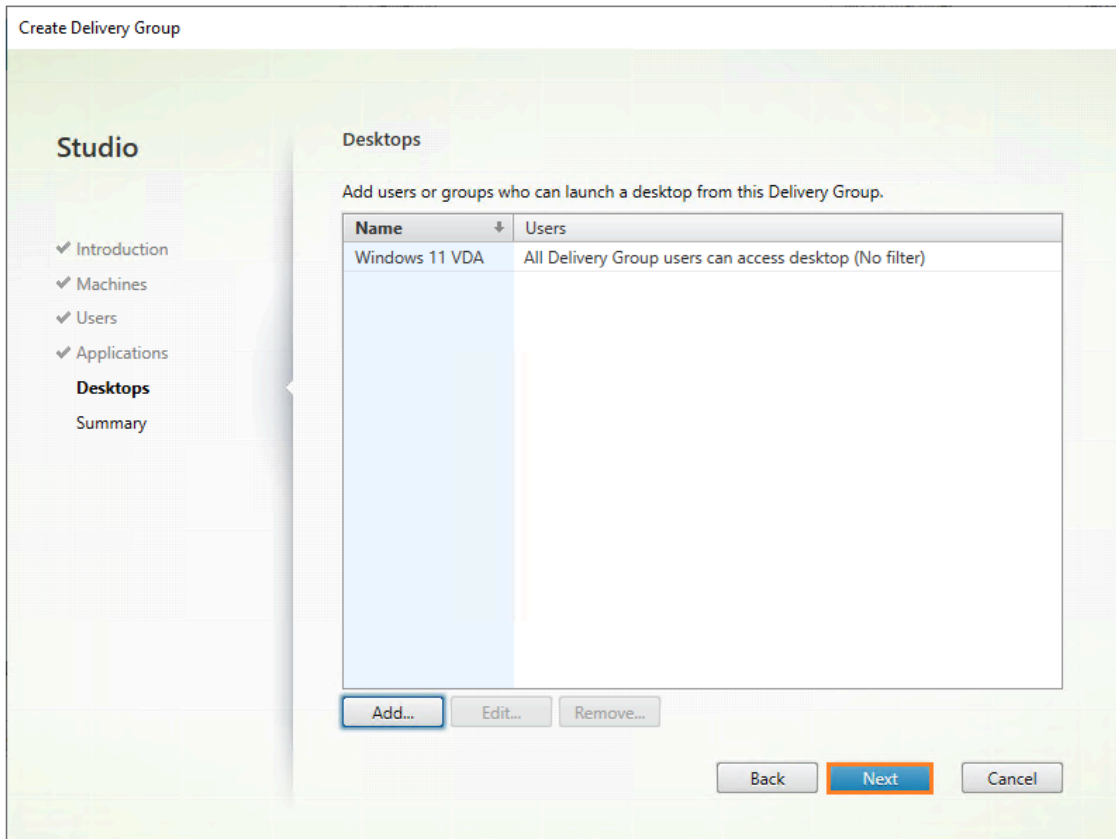
Allow everyone with access to this Delivery Group to use a desktop

Restrict desktop use to:

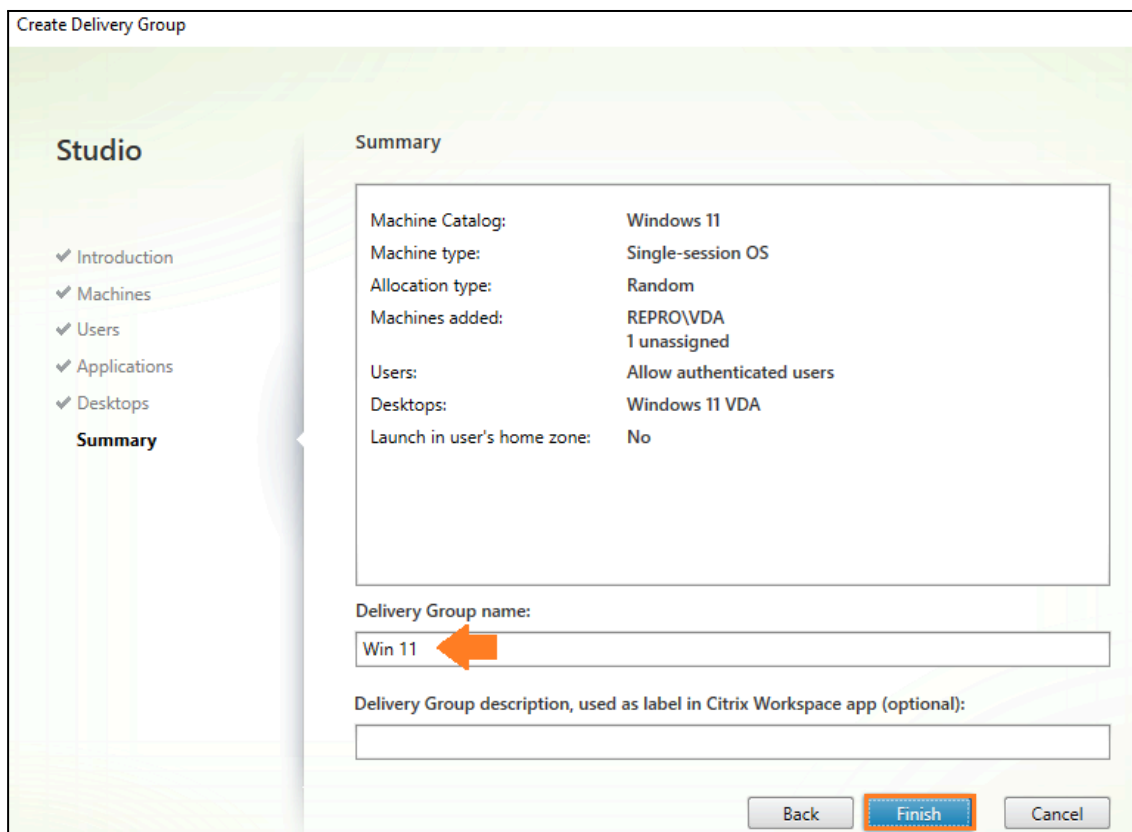
Add users and groups

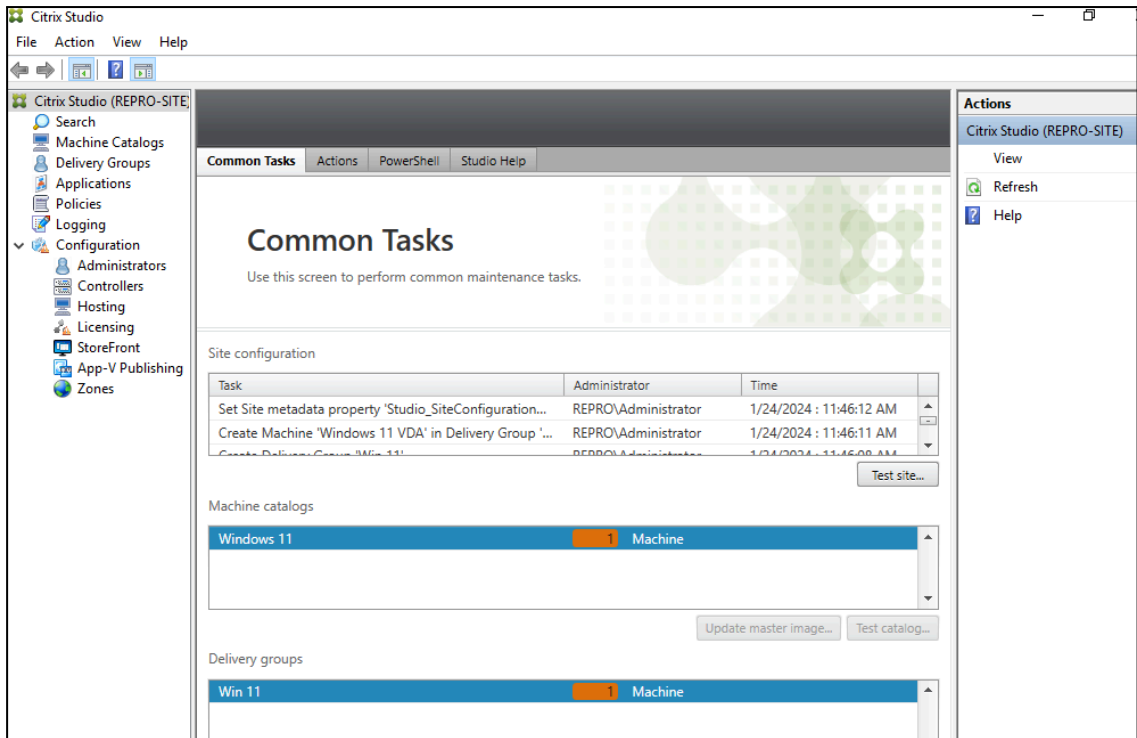
Enable desktop  
Clear this check box to disable delivery of this desktop.

10. Click **Next**.



11. On the **Summary screen**, enter a name in the **Delivery Group name** input field and click **Finish**.

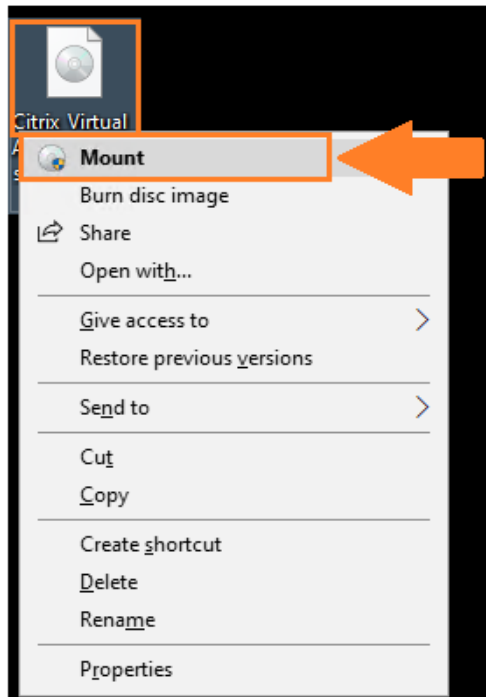




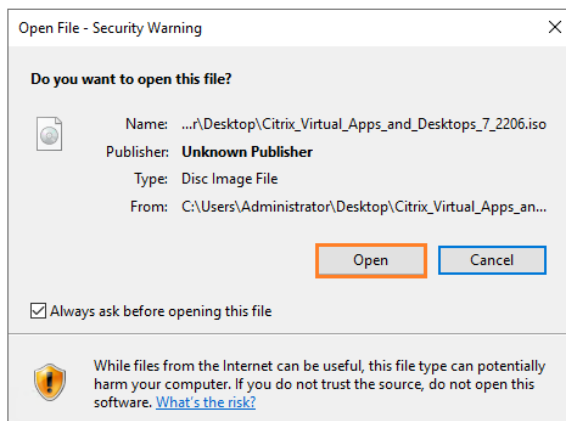
**NOTE:** As this version of Windows 11 is NOT multi-session, you cannot launch more than 1 Application/desktop at the same time.

# StoreFront installation and configuration

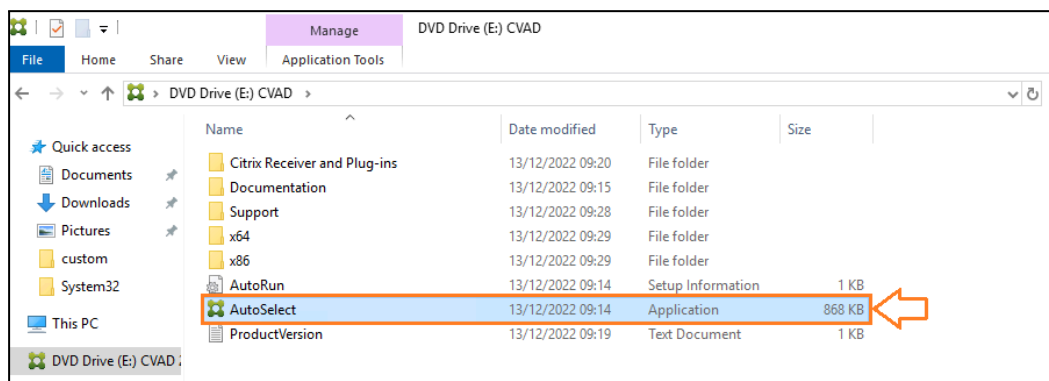
1. From your DDC-SF VM, mount again the Citrix Virtual Apps and Desktops iso.



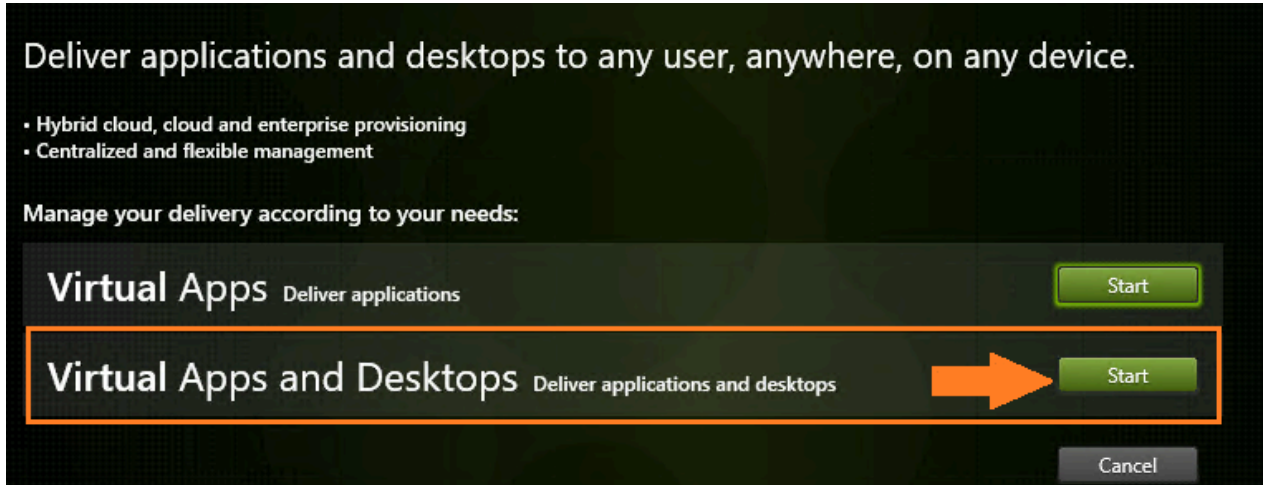
2. Click **Open**.



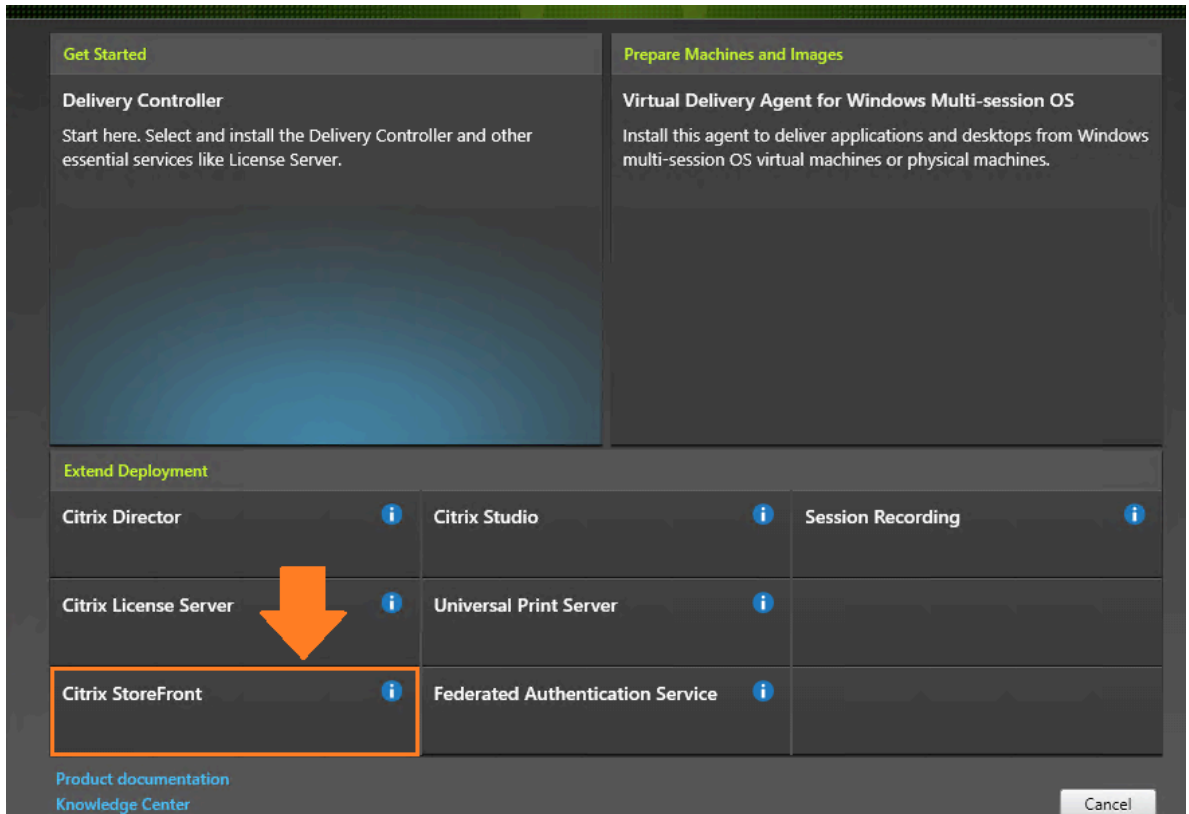
3. Click **AutoSelect**.



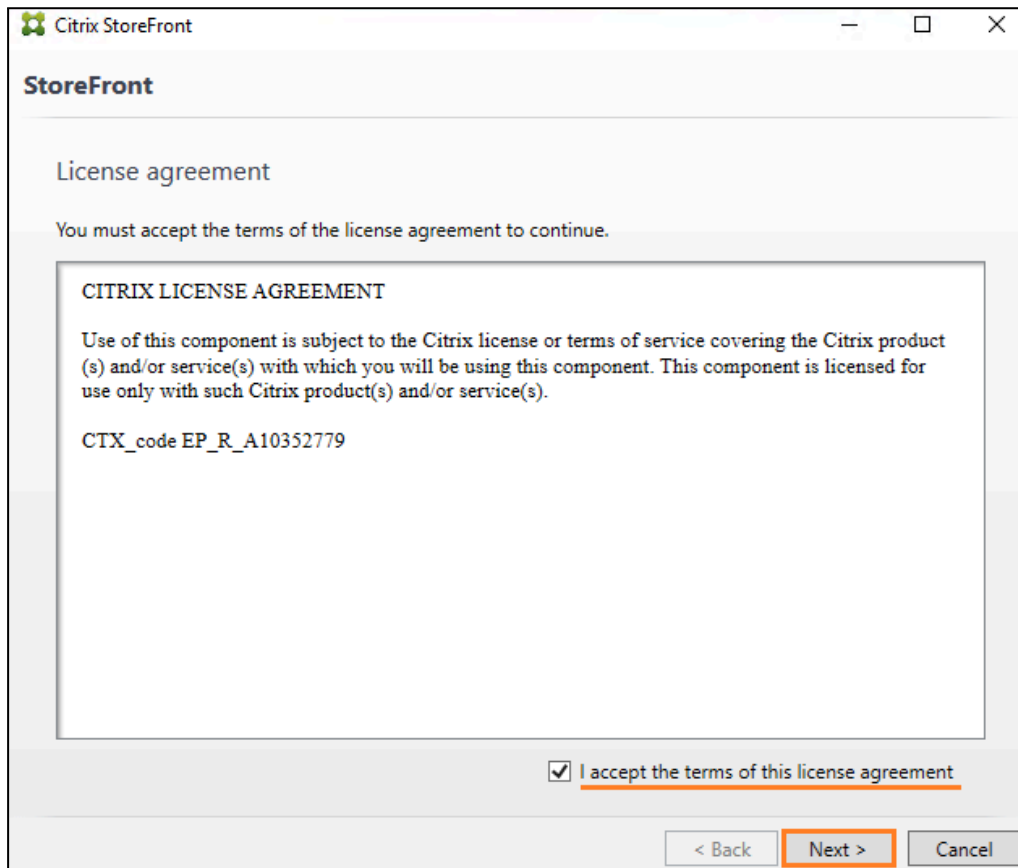
4. Click **Start** next to **Virtual Apps and Desktops**.



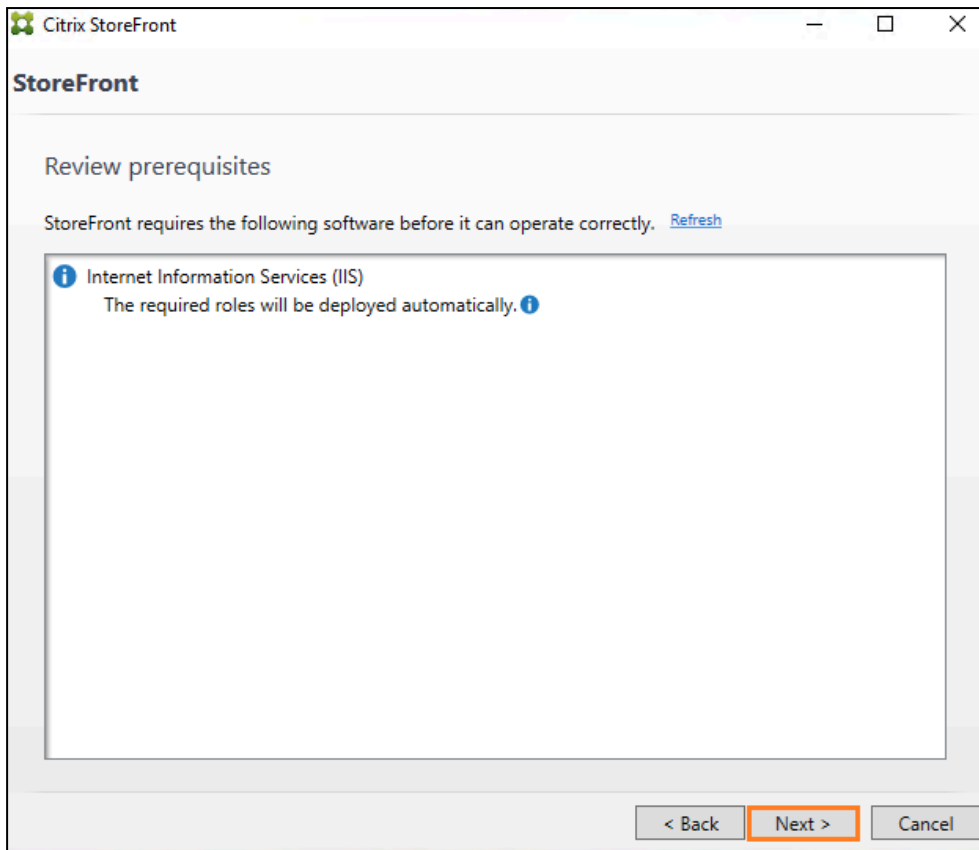
5. Click **Citrix StoreFront**.



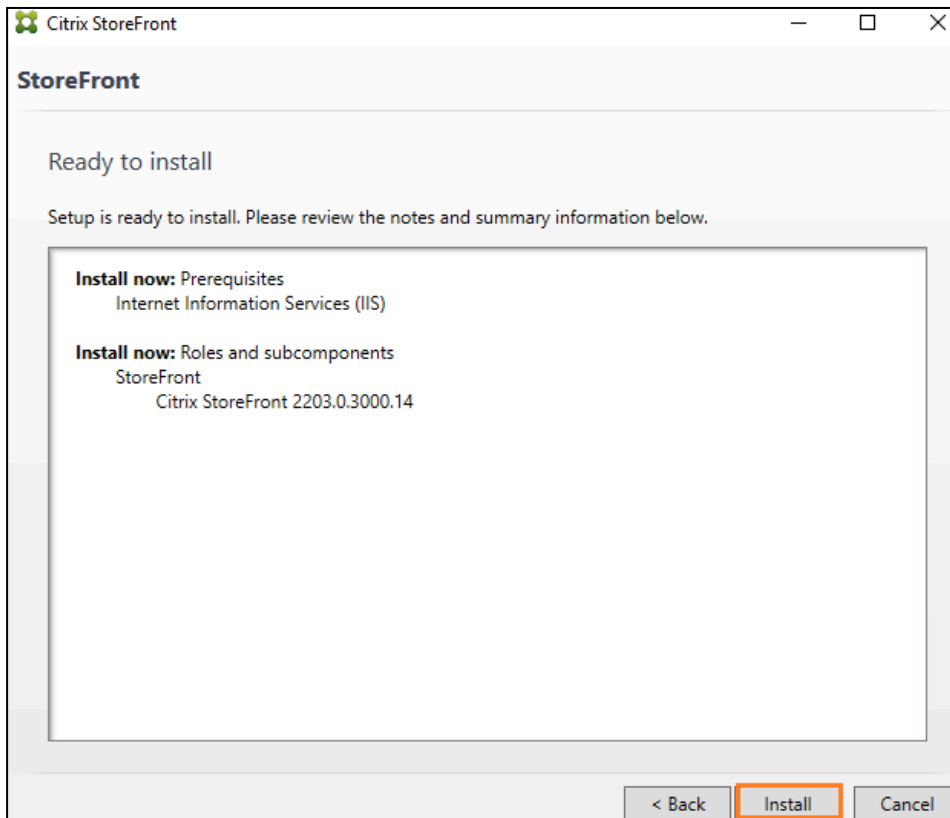
6. Accept the license agreement and click **Next**.



7. Click **Next**.

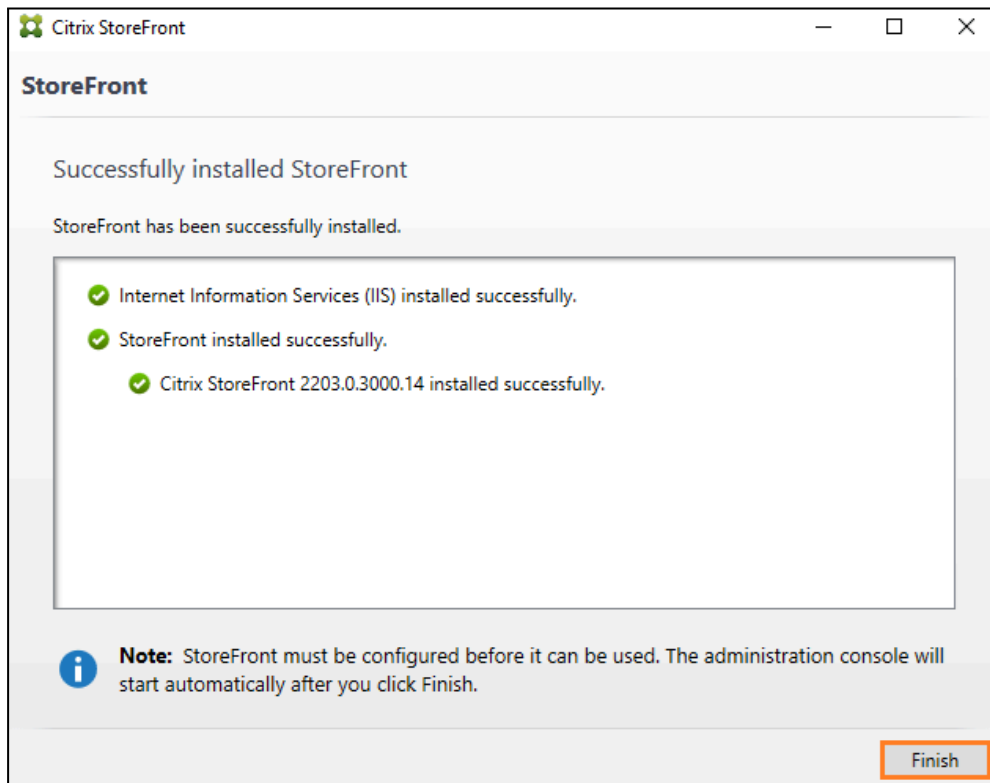


8. Click **Install**.

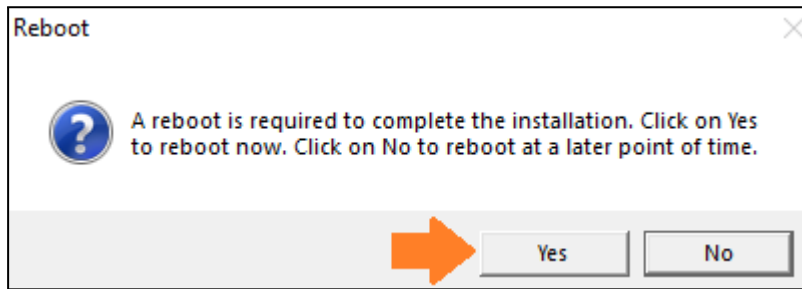




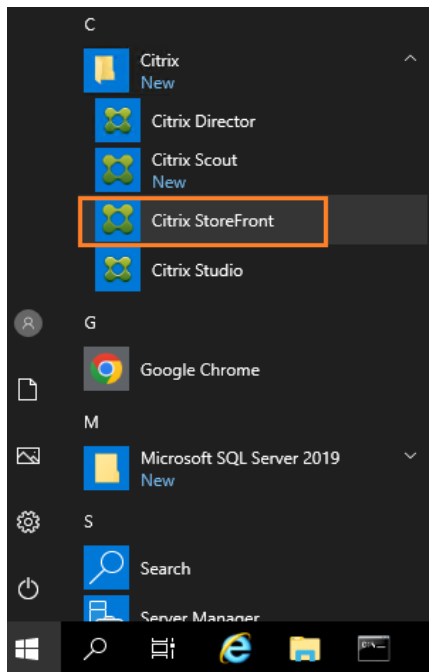
9. Once completed, click **Finish**. This will open the StoreFront Management Console to begin the configuration.



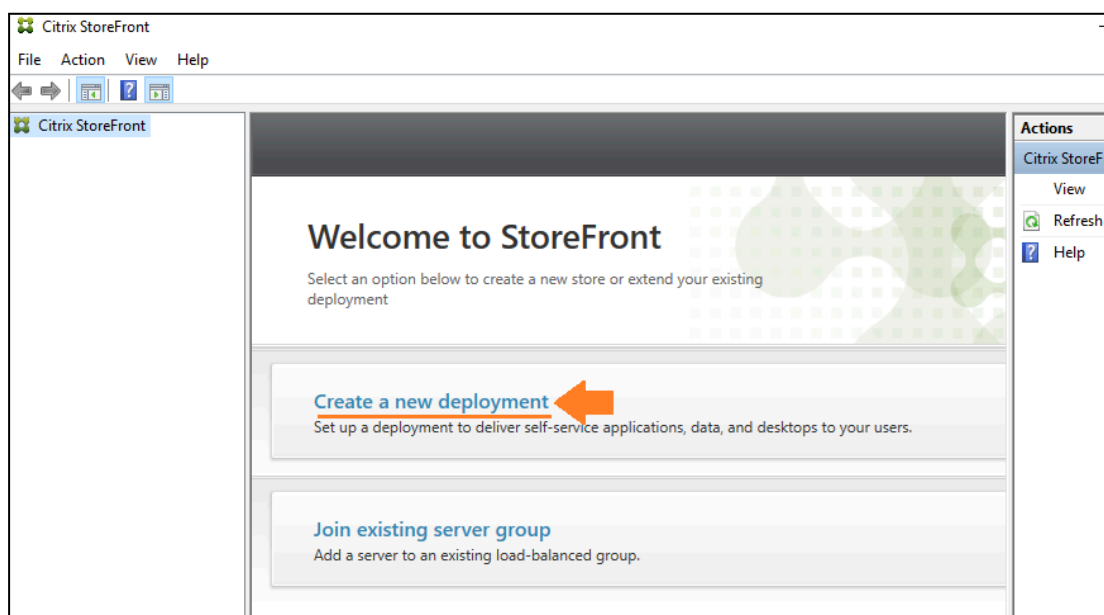
10. Click Yes to **Reboot**.



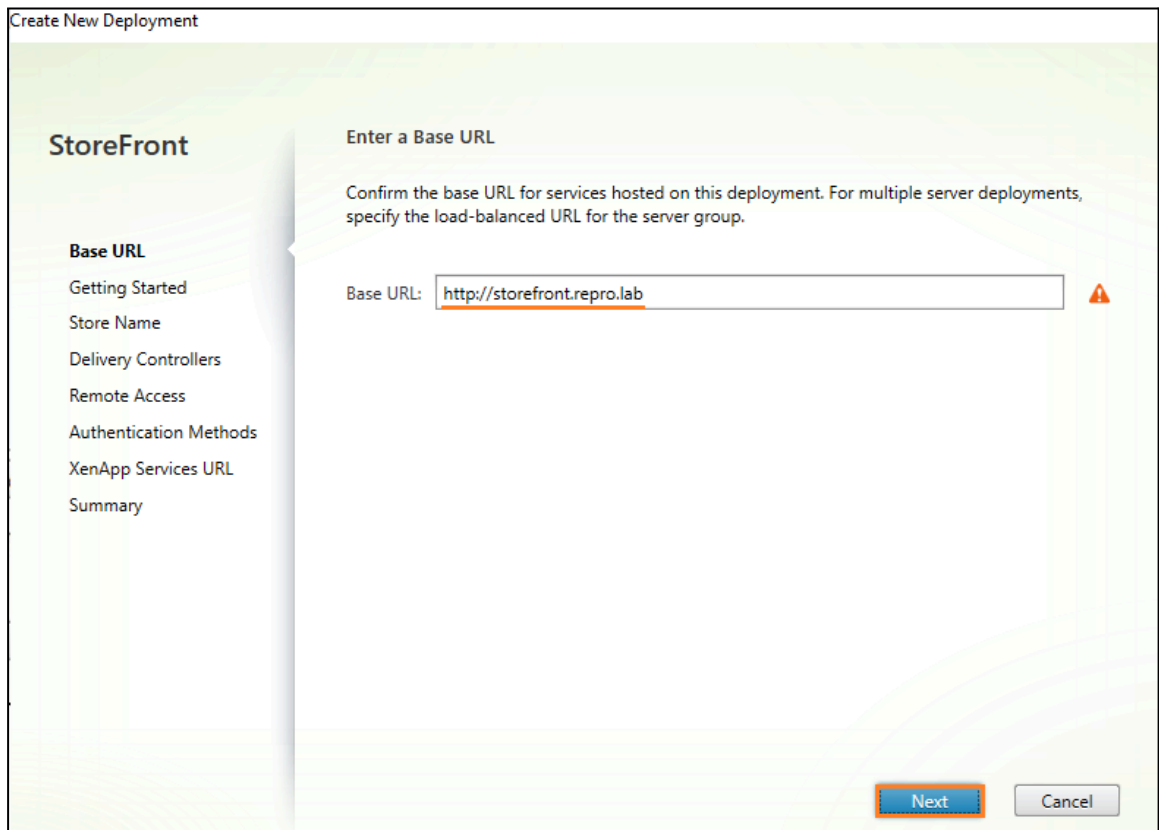
11. Connect again to the DDC-SF VM and open the StoreFront Management console.



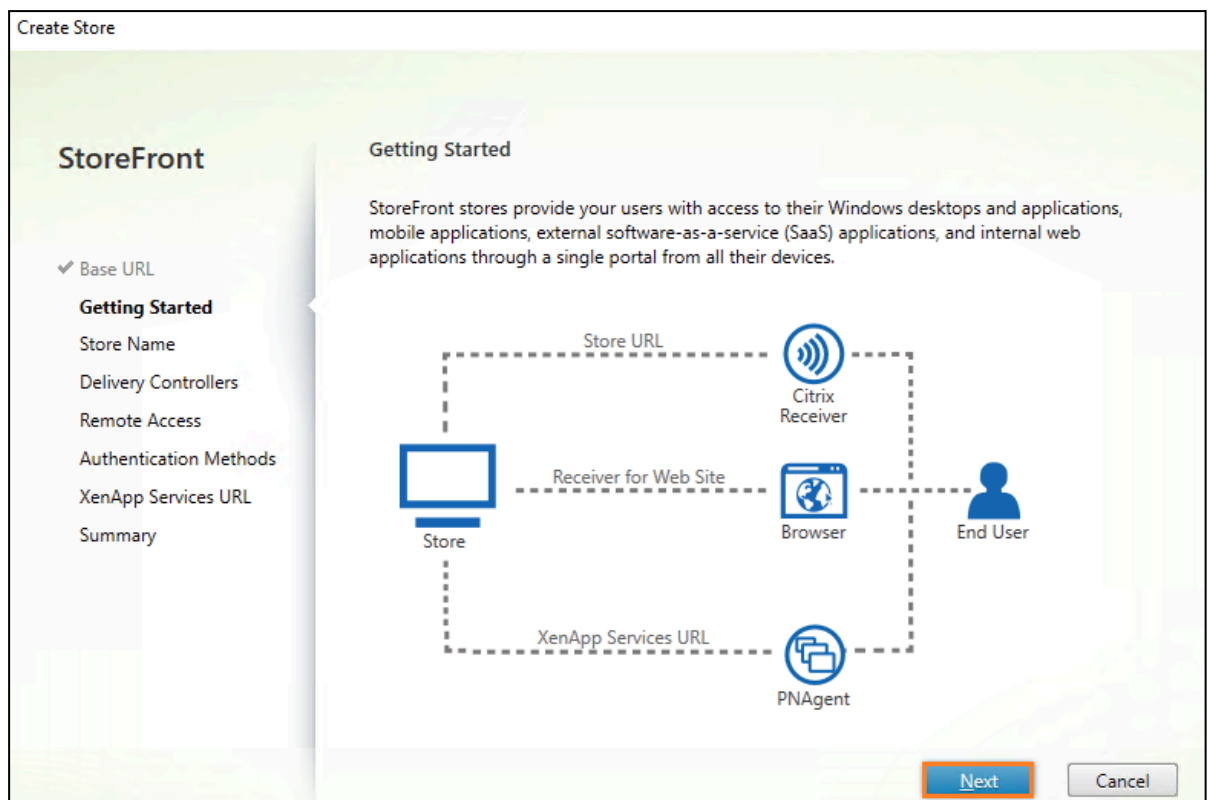
12. Select **Create a new deployment**.



13. Enter <http://storefront.repro.lab>. This will be the URL used to access the Storefront internally via Browser.



14. Click **Next**.



15. Enter a **Store Name** and click **Next**.

The screenshot shows the 'Create Store' wizard at the 'Store name and access' step. On the left, a 'StoreFront' sidebar lists navigation options: Base URL, Getting Started, Store Name (highlighted), Delivery Controllers, Remote Access, Authentication Methods, XenApp Services URL, and Summary. The main area is titled 'Store name and access' and contains the following text: 'Enter a name that helps users identify the store. The store name appears in Citrix Receiver/ Workspace app as part of the user's account.' Below this is an information icon and a message: 'Store name and access type cannot be changed, once the store is created.' A text input field for 'Store Name' contains the word 'Store'. There are two checkboxes: 'Allow only unauthenticated (anonymous) users to access this store' (unchecked) and 'Set this Receiver for Web site as IIS default' (unchecked). The 'Next' button is highlighted with a red box.

16. Click **Add** to configure the delivery controller.

The screenshot shows the 'Create Store' wizard at the 'Delivery Controllers' step. The 'StoreFront' sidebar on the left has 'Delivery Controllers' highlighted. The main area is titled 'Delivery Controllers' and contains the text: 'Specify the Citrix Virtual Apps and Desktops delivery controllers or XenApp servers for this store. Citrix recommends grouping delivery controllers based on deployments.' Below this is a table with three columns: 'Name', 'Type', and 'Servers'. The table is currently empty. At the bottom of the table area are three buttons: 'Add...' (highlighted with a red box), 'Edit...', and 'Remove'.

17. Enter **Controller** in the Display name input field.

18. Select the **Citrix Virtual Apps and Desktops** radio button, and click Add.

Add Delivery Controller

Display name:

Type:  Citrix Virtual Apps and Desktops  
 XenApp 6.5

Servers (load balanced):

19. Enter DDC hostname **DDC-SF.repro.lab** OR use your DDC VM IP and click **OK**.

---

**NOTE:** Make sure you can properly resolve the DDC Server name you enter in the below box. Ping the address and confirm it just in case.

---

Add Server

Server name:

20. Change the transport type to **HTTP**, port to **80**, and click **OK**.

**Edit Delivery Controller**

Display name:

Type:  Citrix Virtual Apps and Desktops  
 XenApp 6.5

Servers (load balanced):

Servers are load balanced

Transport type:

Port:

---

**Advanced Settings**  
 Configure delivery controller communication timeouts and other advanced settings using the 'Settings' dialog.

21. Click **Next**.

**Create Store**

**StoreFront**

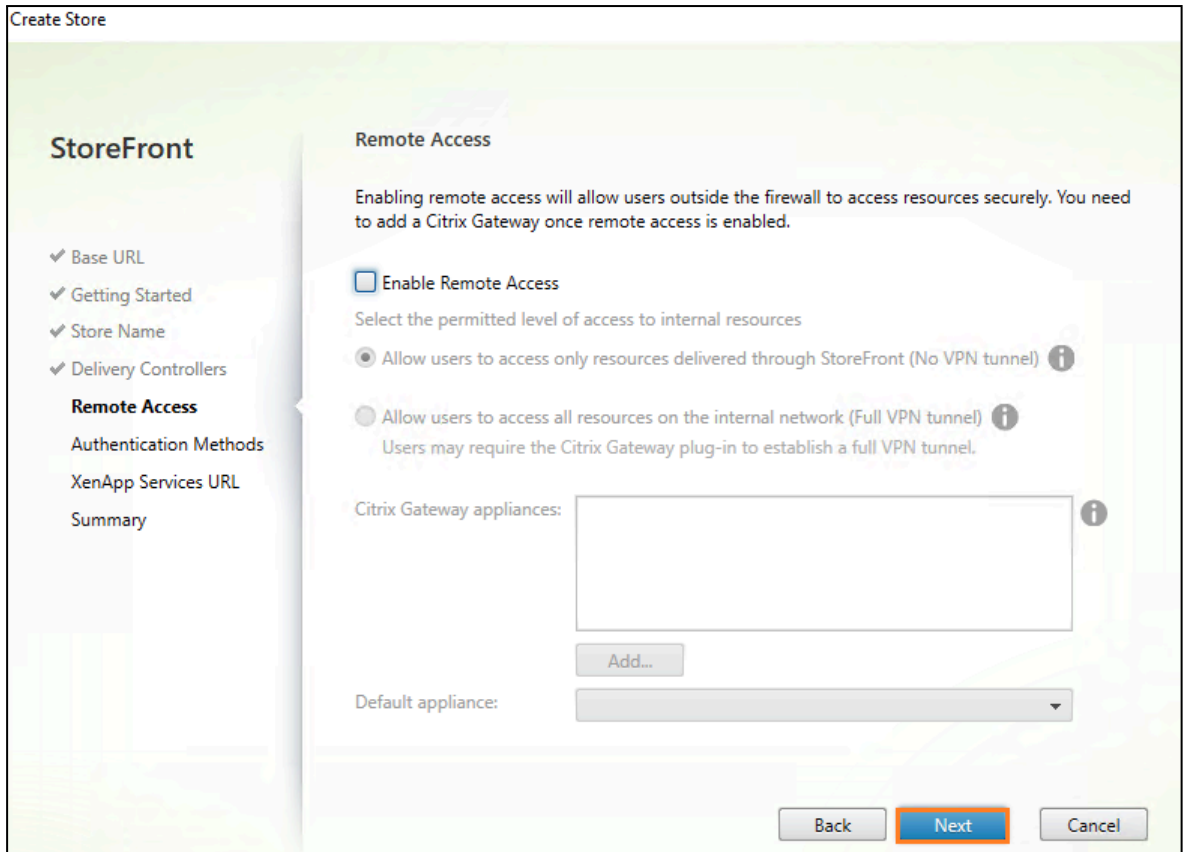
- ✓ Base URL
- ✓ Getting Started
- ✓ Store Name
- Delivery Controllers**
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

**Delivery Controllers**

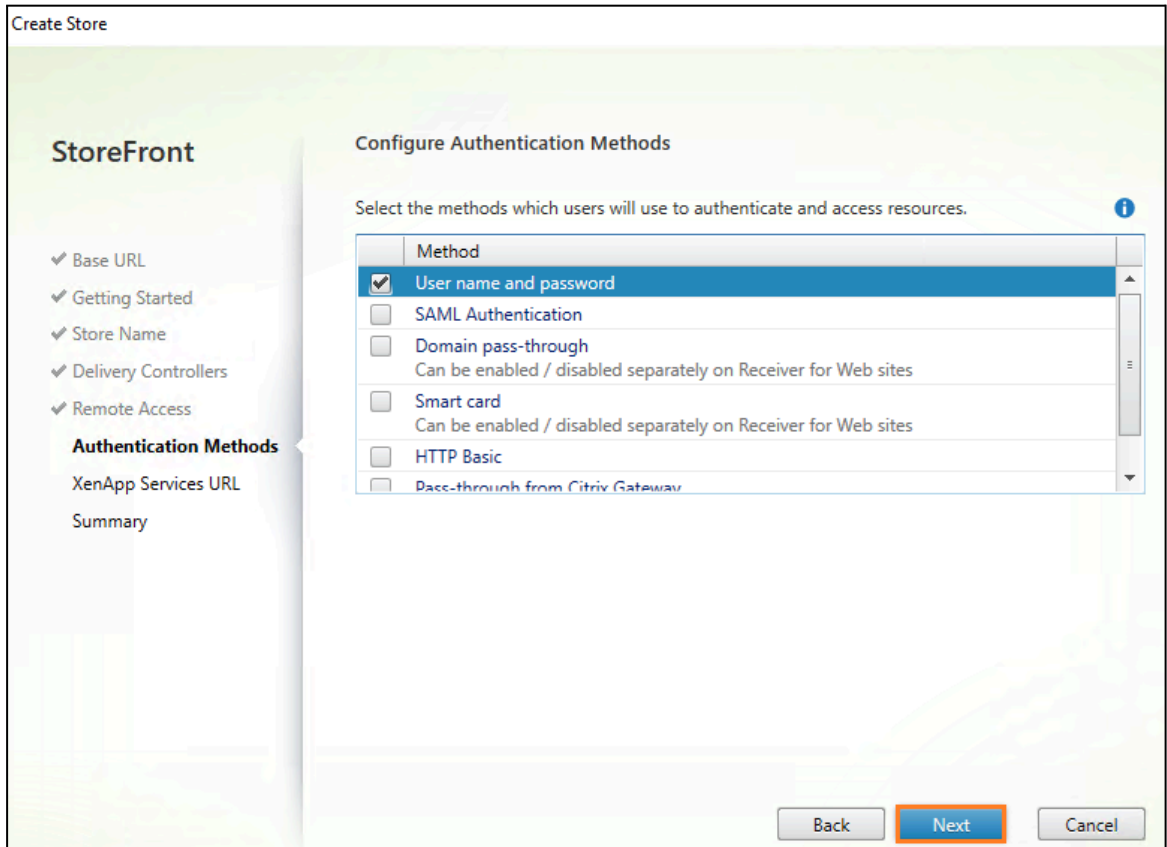
Specify the Citrix Virtual Apps and Desktops delivery controllers or XenApp servers for this store. Citrix recommends grouping delivery controllers based on deployments.

Name	Type	Servers
Controller	Citrix Virtual Apps and Desktops	ddc.YOURDOMAI...

22. Click **Next**.



23. Select **User name and password** and click **Next**.



24. Click **Create**.

Create Store

## StoreFront

- ✓ Base URL
- ✓ Getting Started
- ✓ Store Name
- ✓ Delivery Controllers
- ✓ Remote Access
- ✓ Authentication Methods
- XenApp Services URL**
- Summary


### Configure XenApp Services URL

URL for users who use PNAgent to access applications and desktops.

- Enable XenApp Services URL  
URL: `https://storefront.willian.lab/Citrix/Store/PNAgent/config.xml`
- Make this the default Store for PNAgent  
PNAgent will use this store to deliver resources.

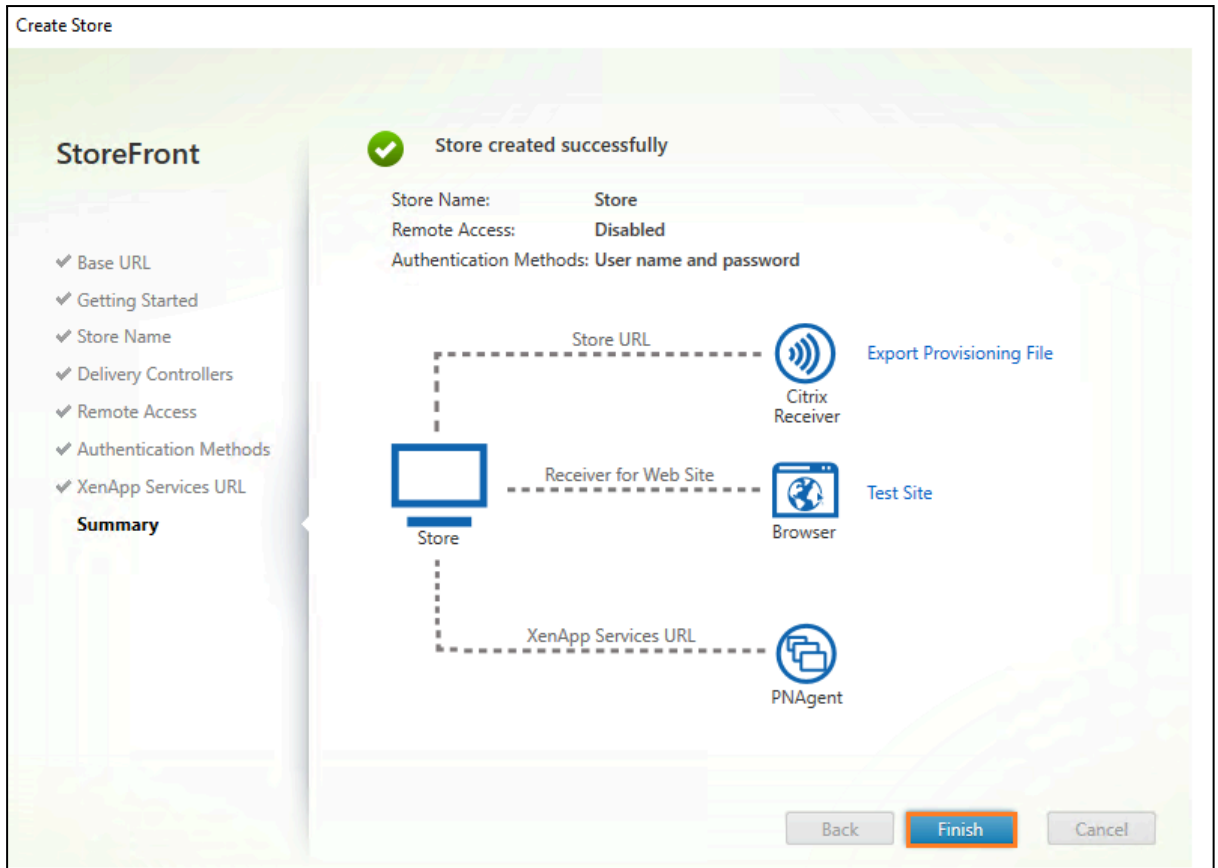
Back Create Cancel

Creating store, please wait...

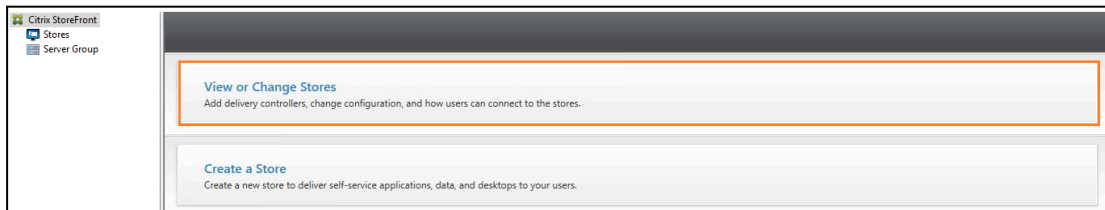


25. Click **Finish**.

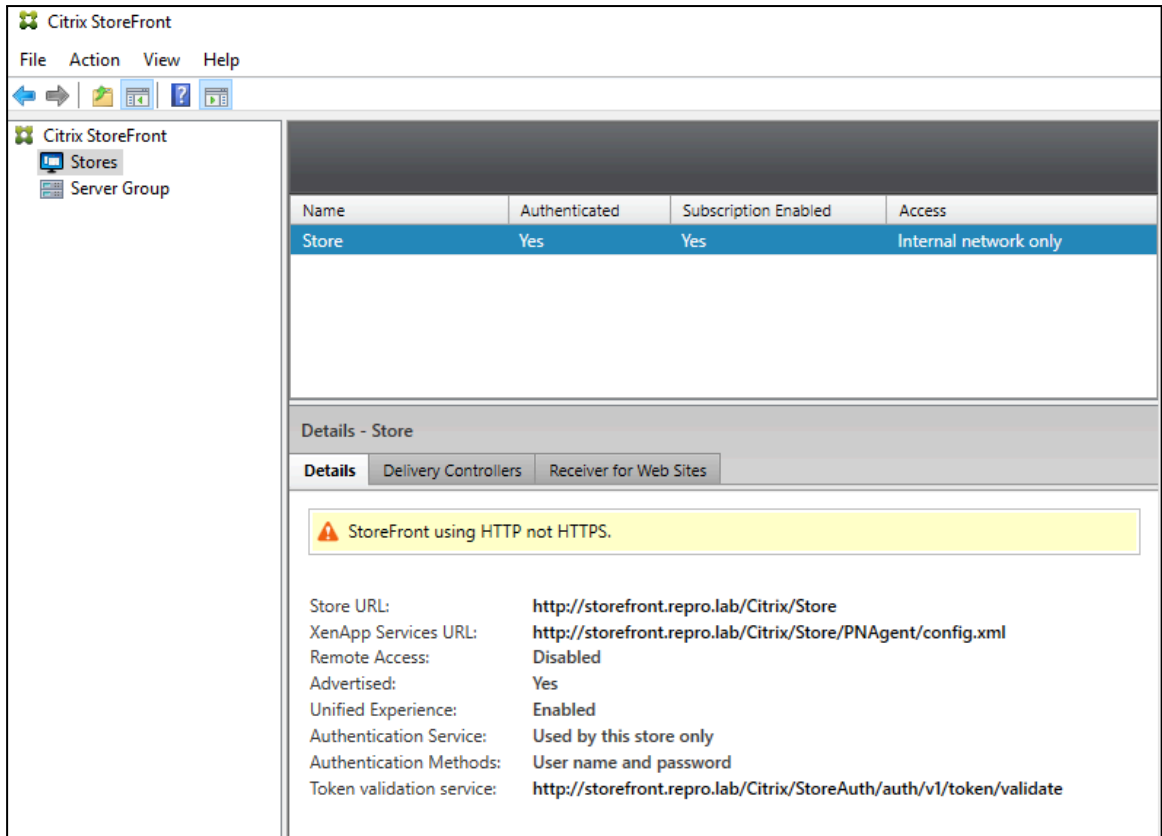




26. Click **View or Change Stores**.



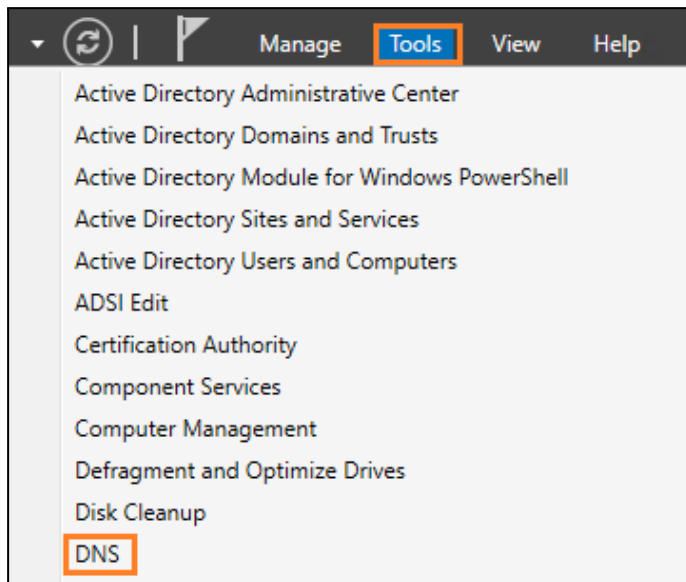
27. Click on **Stores** to see the configured store. It should look like the screenshot below.



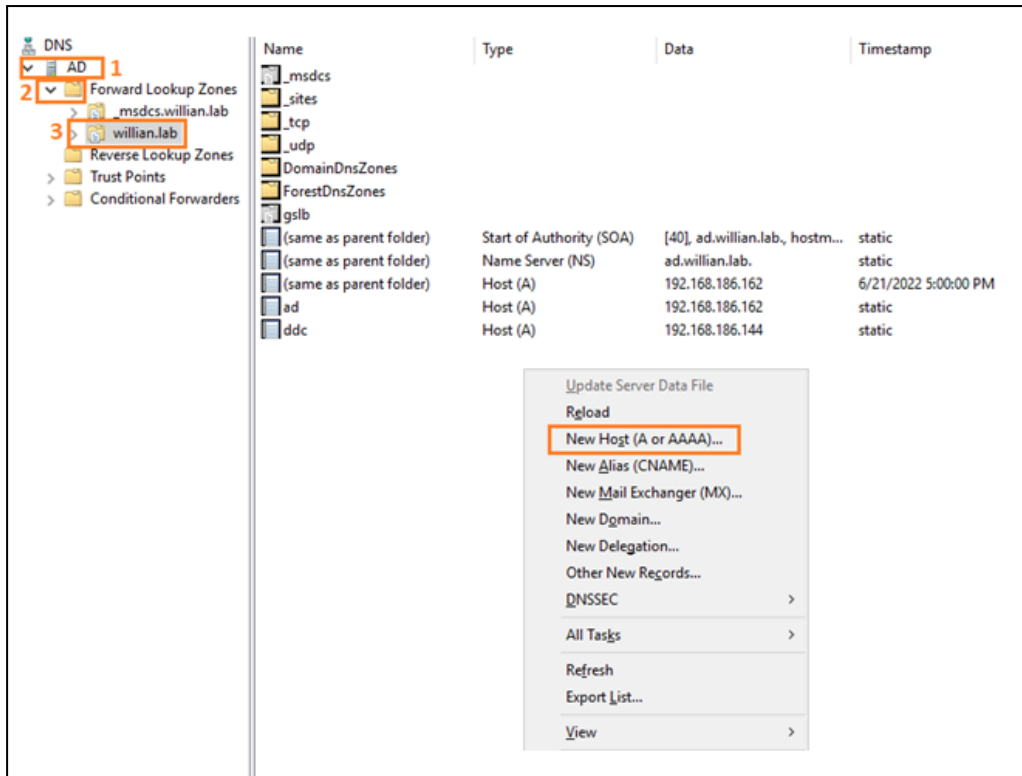
## Configuring DNS entry for Storefront

You need to create a **DNS entry** in your DNS server to be able to resolve to “**storefront.repro.lab**” internally or “your storefront.domain”

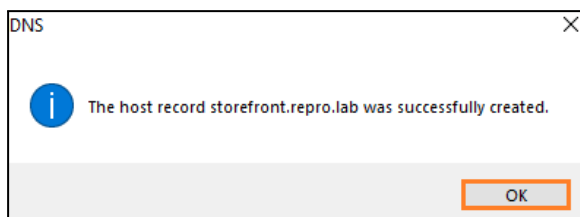
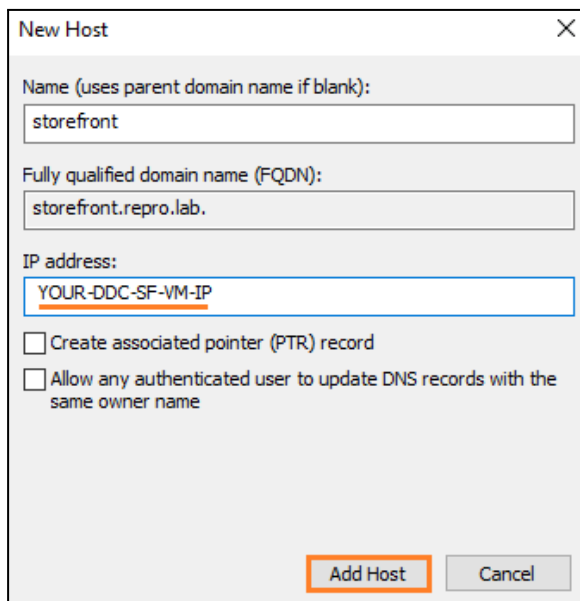
1. Open your internal Windows DNS server. **Tools > DNS**



2. Navigate to your domain: **AD > Forward Lookup Zones > Yourdomain**. Right-click the white space and select **New Host (A or AAAA)...**

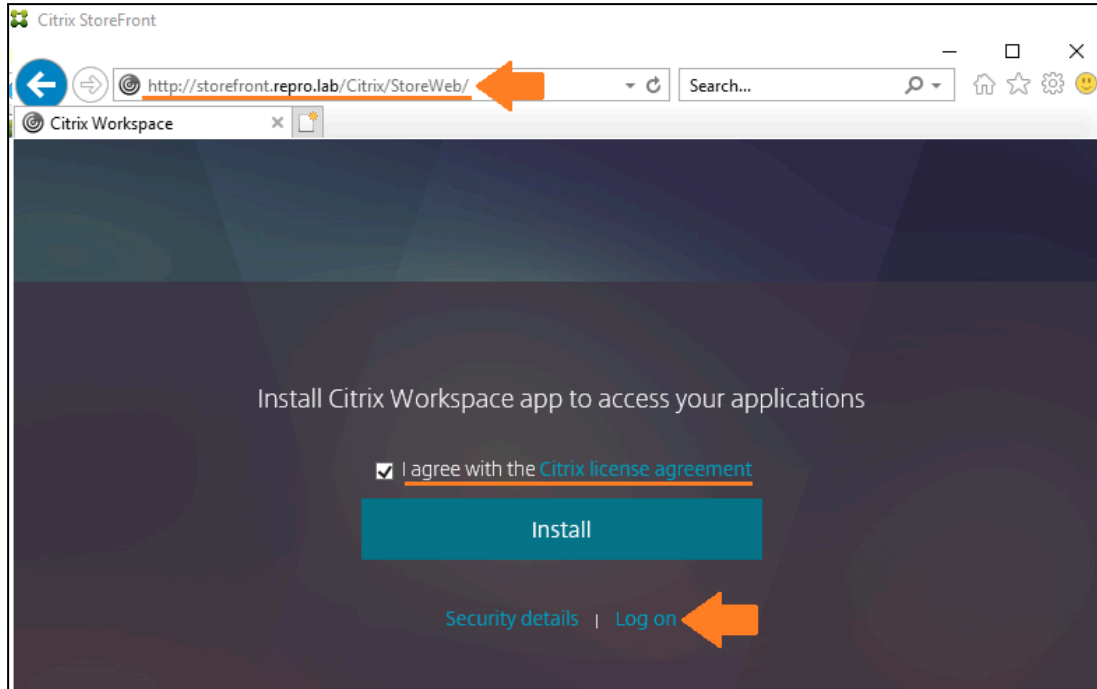


3. Add a host entry for your Storefront. You need to specify your host + DDC-SF VM IP (Storefront and DDC use the same IP)

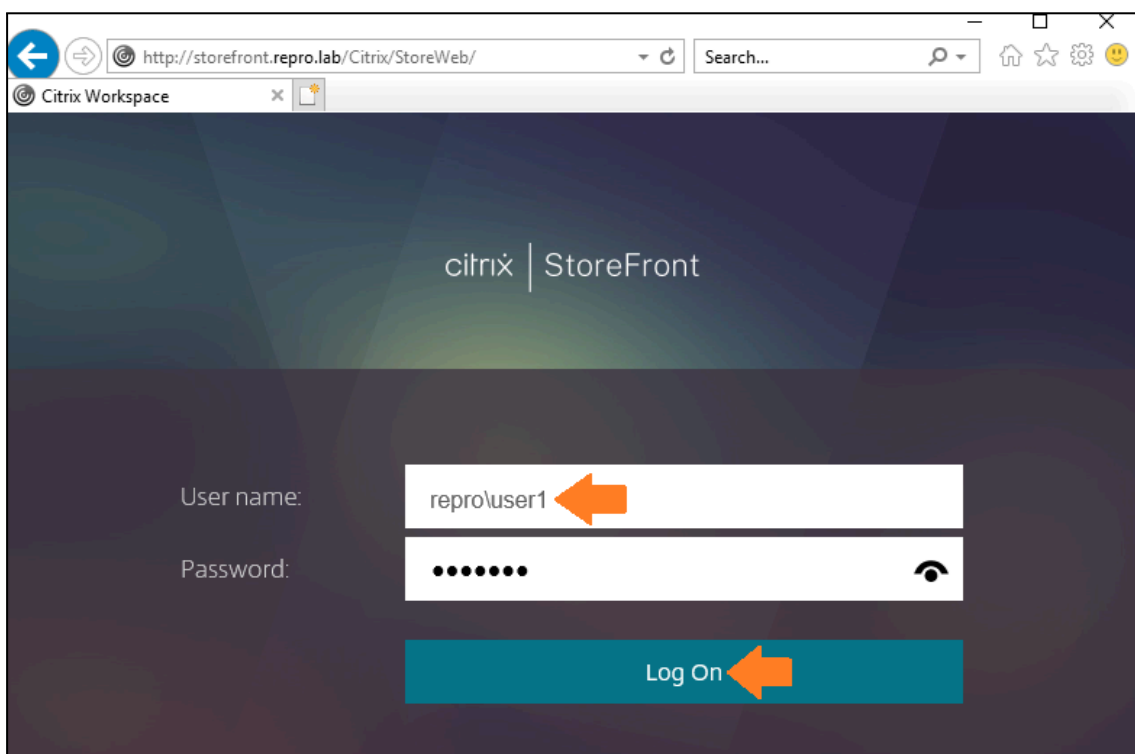


## Testing Internal Launching

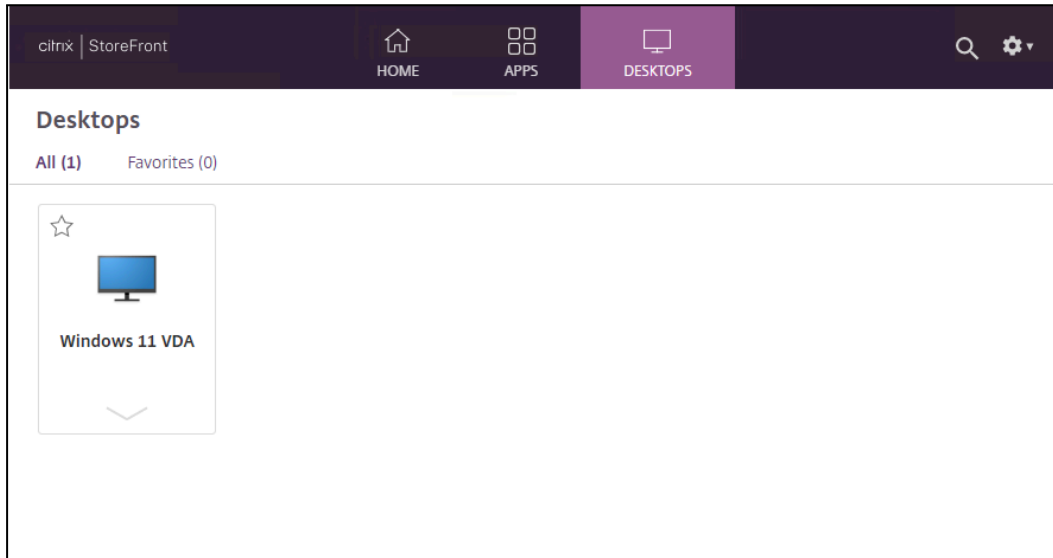
1. From your JumpBox VM or Storefront VM, **open** your browser and type the base URL of your storefront + **WEB** at the end of the URL **http://your-base-url+Web(e.g., <http://storefront.repro.lab/Citrix/StoreWeb>)**.



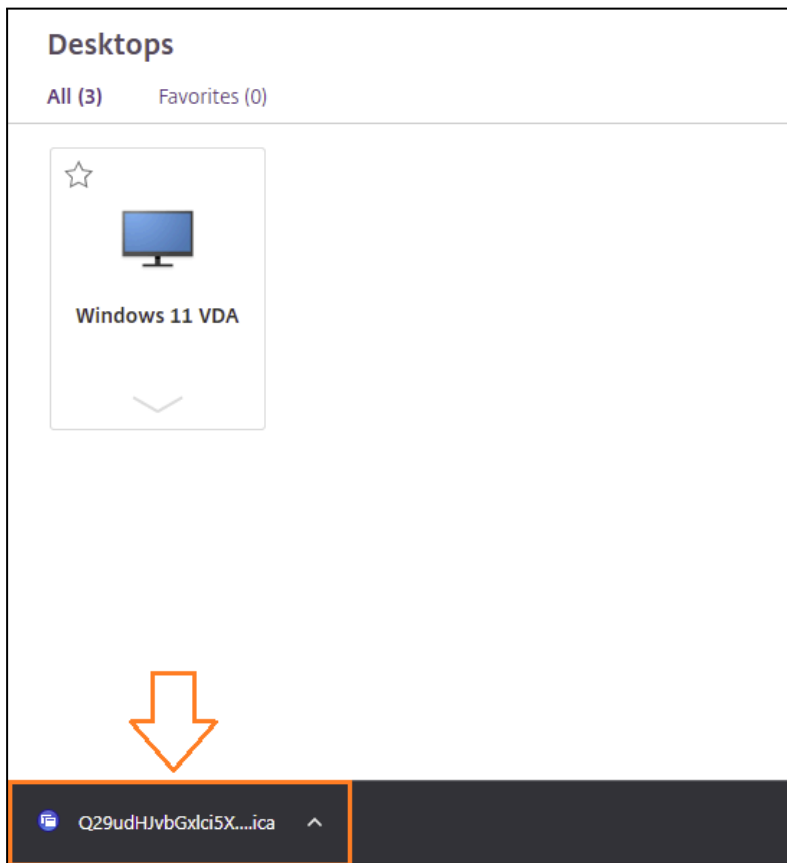
2. Click the **I agree with the Citrix License agreement** check box. If you already have the Citrix Workspace App installed, click **Already installed**, otherwise, click **download** and install the CWA.
3. You now need to enter your LDAP credentials, **Username** and **Password**.

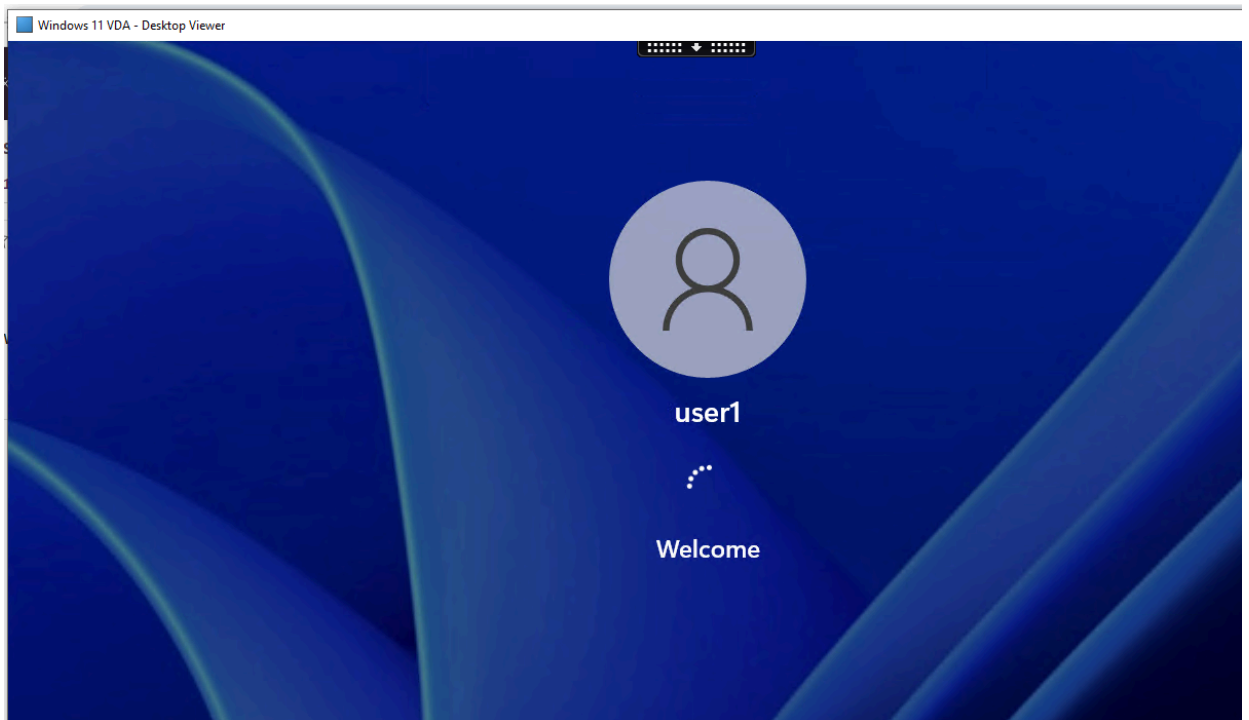


4. Your apps and Desktop are ready.



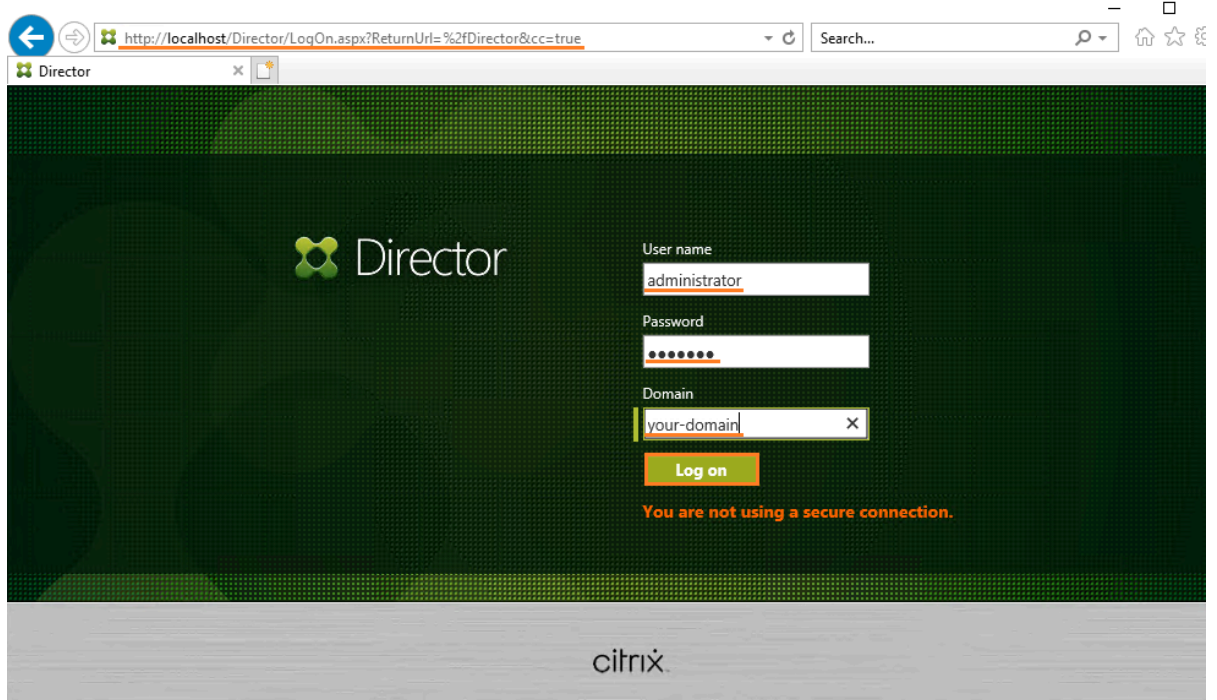
**NOTE:** The ICA file is downloaded whenever you click on the VDA icon. For a successful launch, you must have the Citrix Workspace APP (CWA) installed. If you do not have it installed, either download it when it is prompted during the log-on process or download it from the [Citrix download page](#)





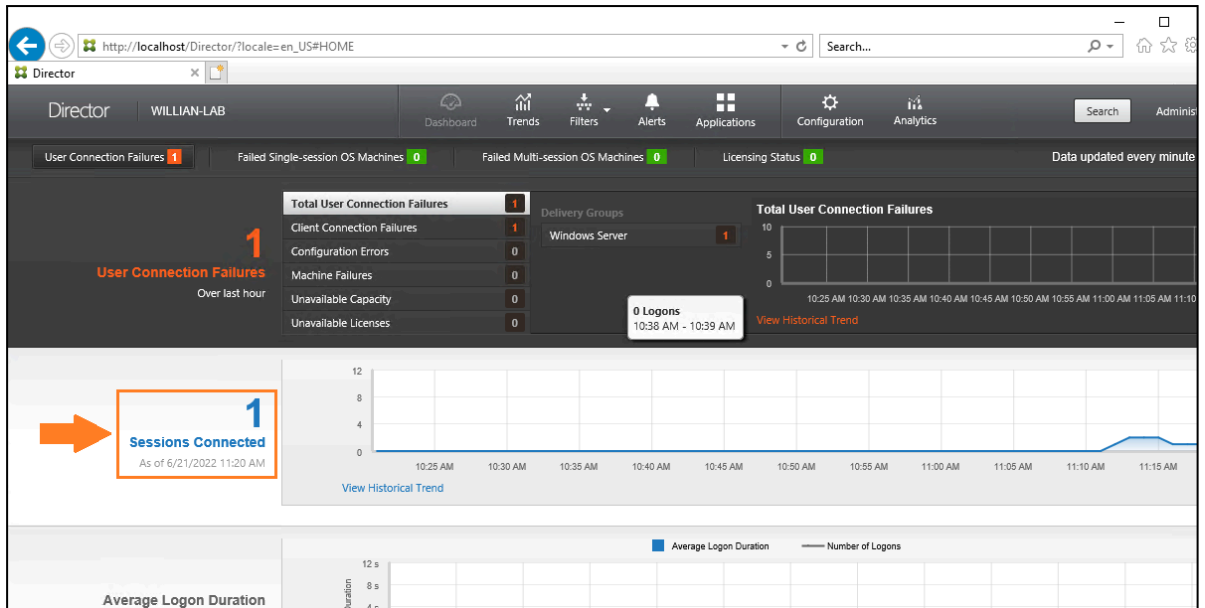
## Monitoring the Sessions with Citrix Director

1. On your DDC Server, open its browser and type `http(s)://localhost/Directory`.
2. Use your administrator user, its password, and your domain (repro.lab) to log on.



There are many things to explore, we will check the basics though, for more, check the [documentation](#).

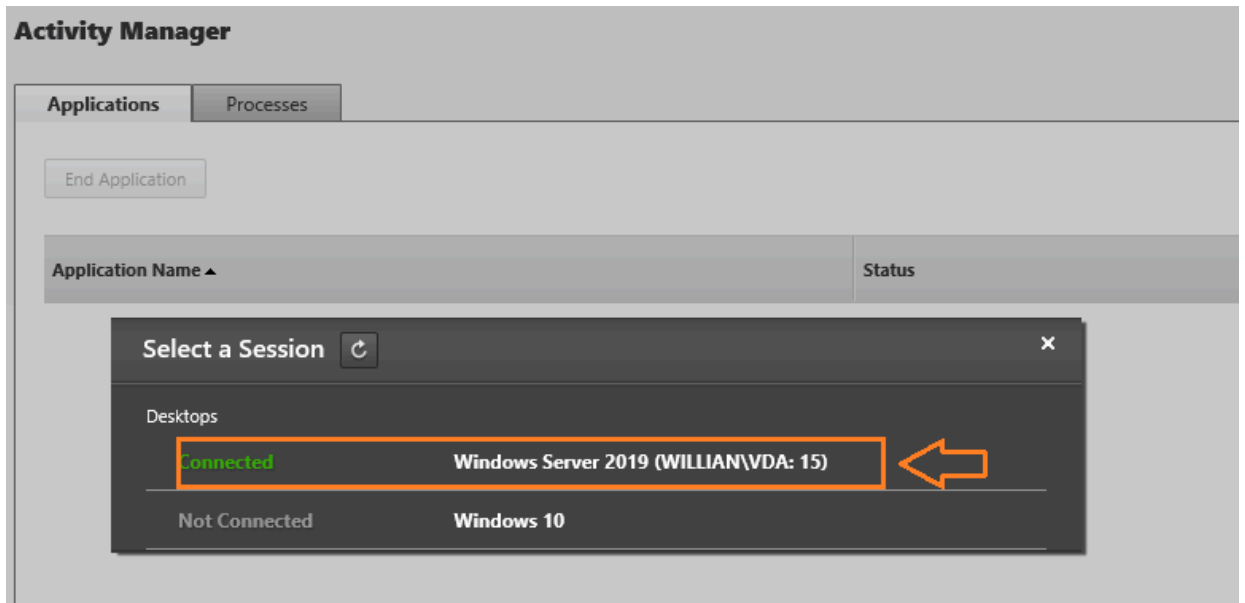
3. Click **Session Connected**.



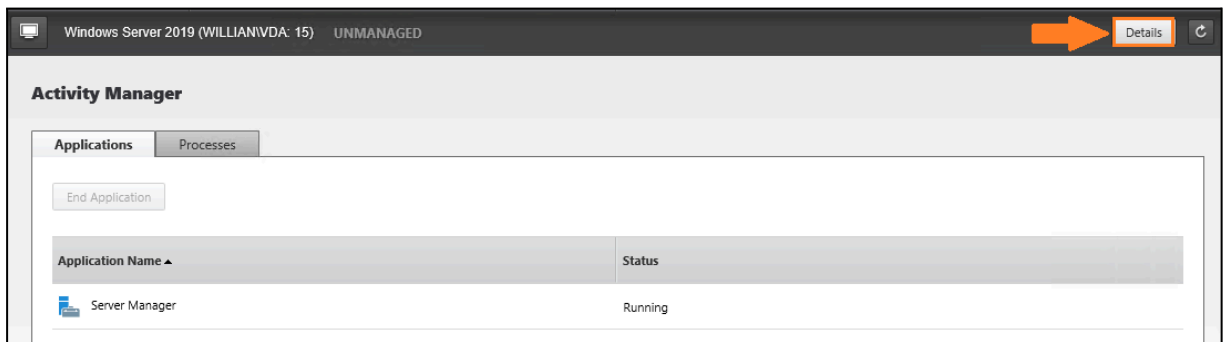
4. Click the user name.

The screenshot shows the 'Filters - All Connected Sessions' page. It includes a 'View:' section with radio buttons for 'Machines', 'Sessions' (selected), 'Connections', and 'Application Instances'. Below is a 'Filter by:' section with dropdowns for 'Session State' (is), 'is', and 'Active'. There are 'Save', 'Save As...', 'Delete', and 'Clear' buttons. The main content is a table titled '1 Session' with columns: Associated User, Session State, Session Start Time, Anonymous, Endpoint Name, Endpoint IP, Citrix Workspace..., Machine Name, and IP Address. The first row shows 'user1' in the 'Associated User' column, which is highlighted with an orange box and an orange arrow pointing to it. Other values in the row include 'Active', '6/21/2022 11:1...', 'No', 'DESKTOP-J10NTI', '10.91.187.34', '22.5.0.18', 'WILLIANVDA', and '192.168.186.156'.

5. Click the session.

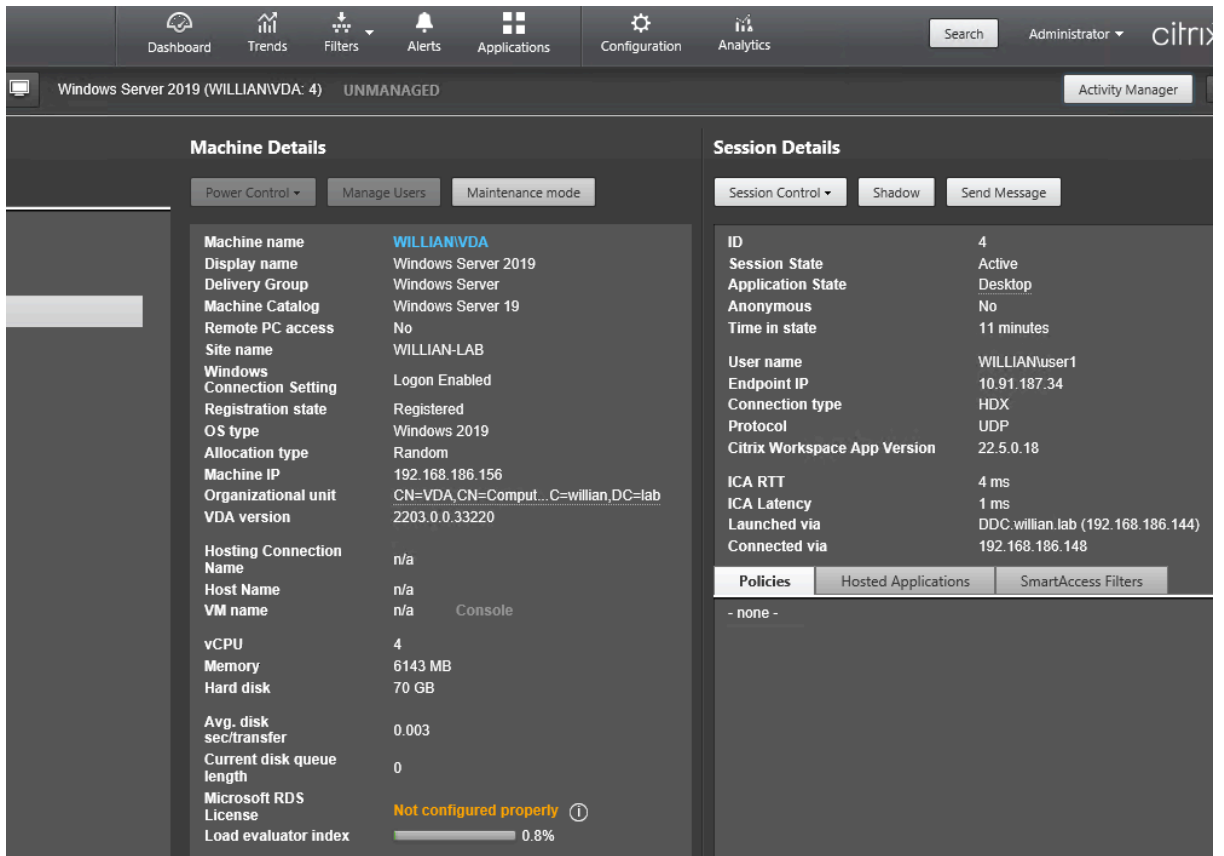


6. Click **Details**.



7. You can see much info such as VDA information, ports, IP, RTT, etc.

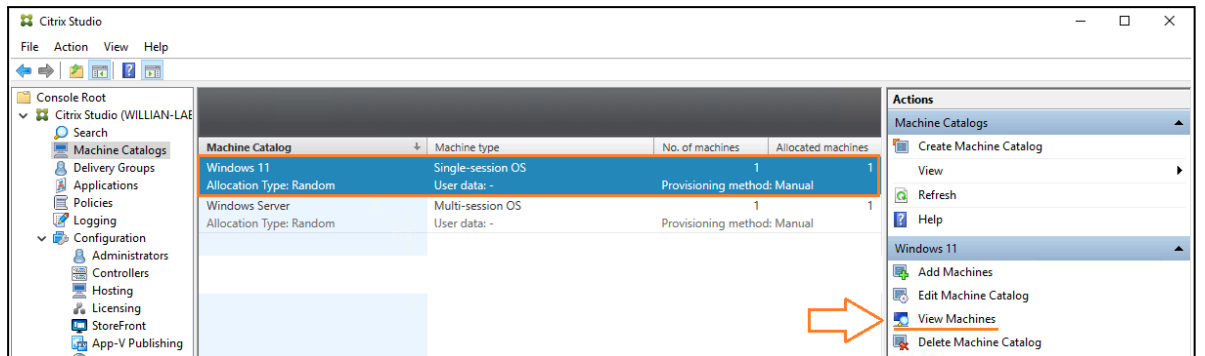




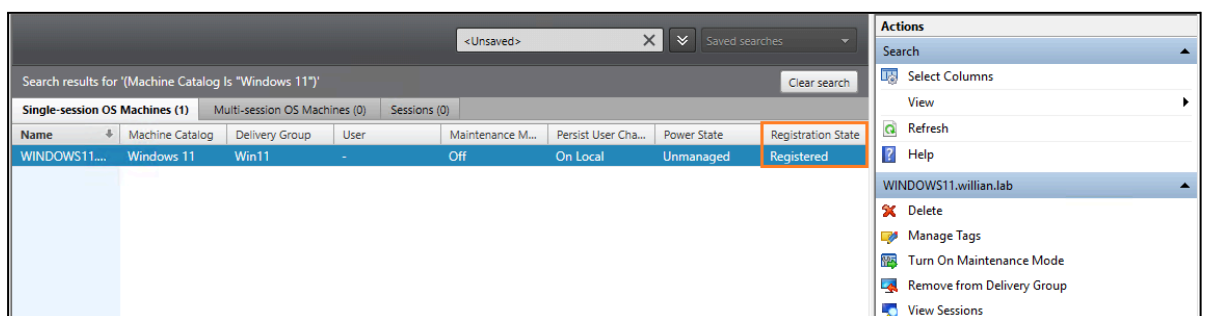
## Verify VDA Machine is Registered with the Delivery Controller

After the reboot completes, verify the Windows 11 VM is properly registered.

1. In Citrix Studio navigate to **Machine Catalogs**, and then select **View Machines**.

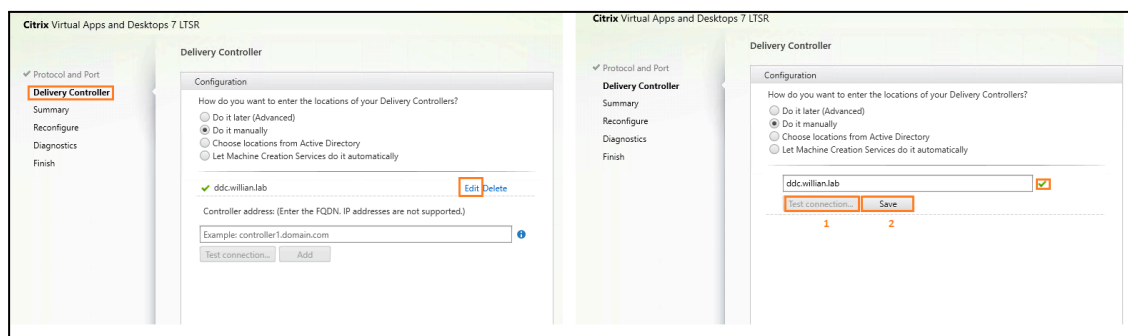
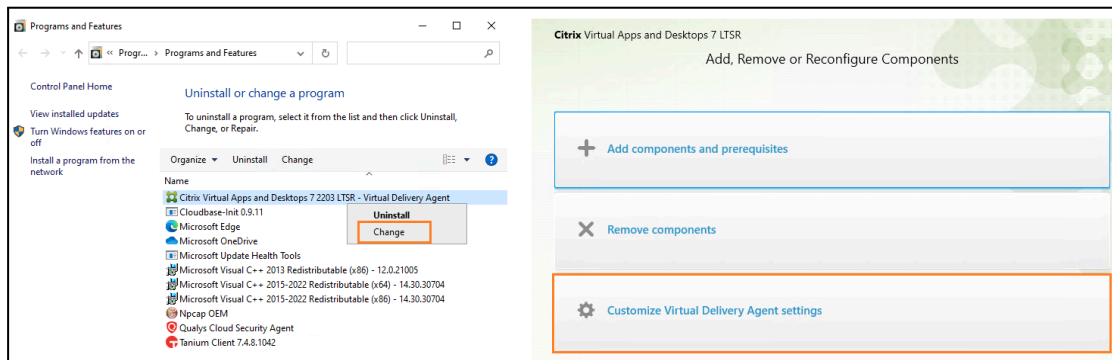


The Registration State should be **Registered**. If it shows **Unregistered**, see [CTX136668](#) for assistance



If you see **Unregistered**, try to reboot your VDA VM and see if this helps. If not, try the below.

2. On **VDA VM**, open the **Control panel > Programs and Features**, click **Change** and **Customize Virtual Delivery Agent settings**.

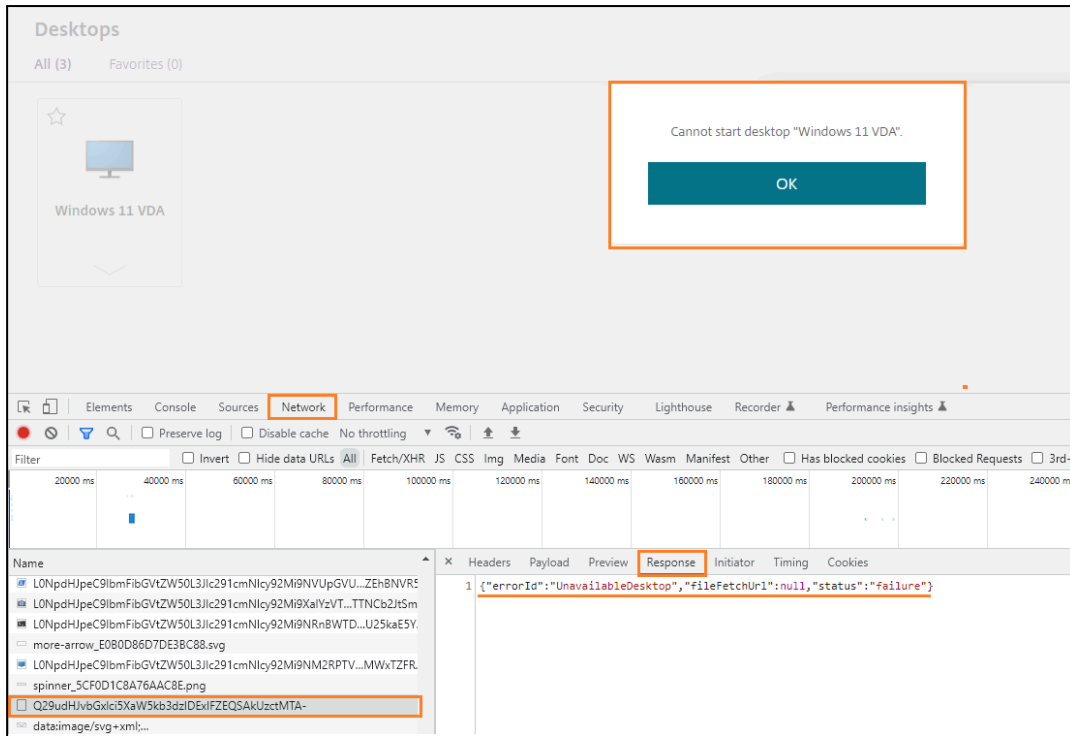


3. Click **Next** and finish the setup. Do not change anything else.
4. Reboot the VDA VM, and after a few minutes, check the registration status.

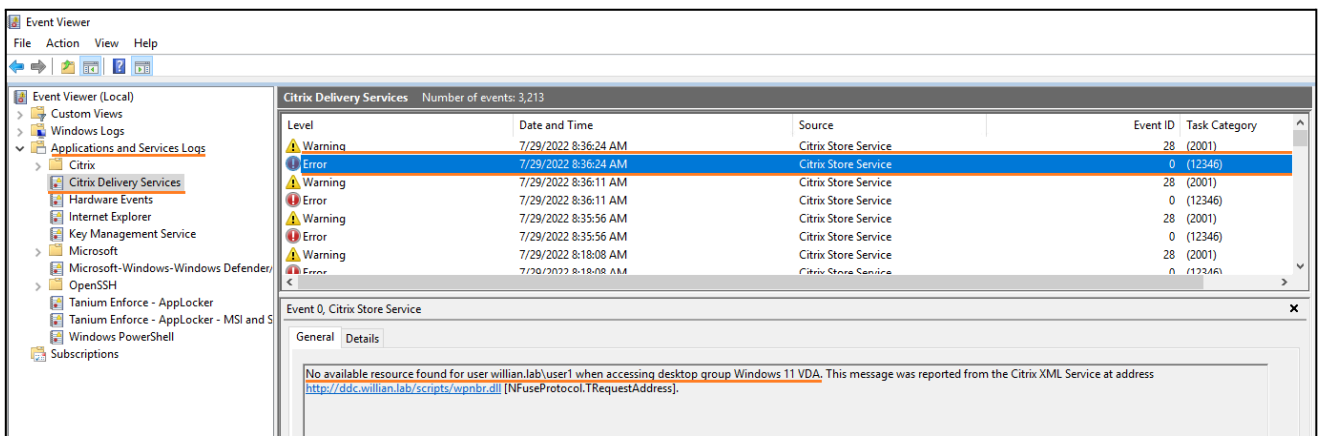
## Unable to Start APP/Desktop

### Error: "Cannot Start app/Desktop"

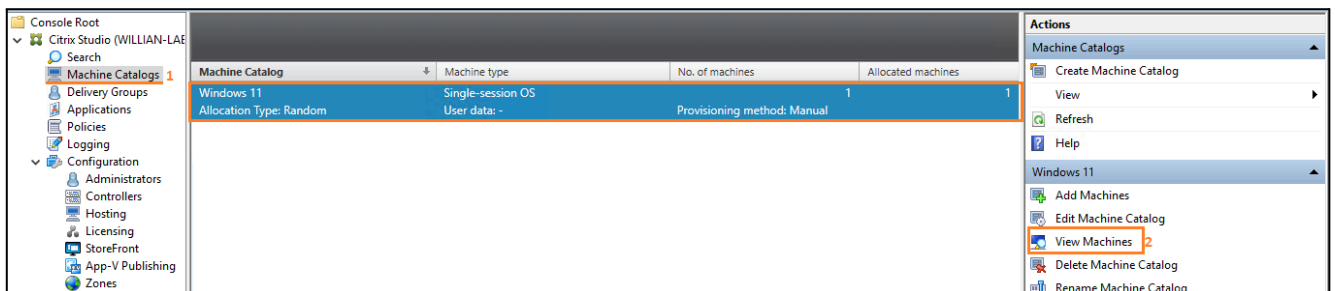
- Make sure you always "log off" from the VDA VM rather than "close" the session, this will avoid issues with a session as it is not multisession.
- Confirm the status of the VDA shows as "Registered" under "Machine Catalog > View Machines".
- Under "Machine Catalog > View Machines" if you see the "log off" option, it means there is a session ongoing, please click "log off" and wait a minute until the session is disconnected as the below screenshots.
- Check the Event Viewer logs "Applications and Services Logs > Citrix Delivery Services" on the DDC-SF VM and seek errors.
- Use the development tools to confirm what is the real response from the controller as the below example, in which the "Unavailable Desktop" error is seen.
- Reboot the VDA VM is also an alternative.



Check the Storefront event viewer logs (Start > Event Viewer > Applications and Services Logs > Citrix Delivery Services) and seek errors. The example below reinforces the error above, no available VDA in the delivery group.



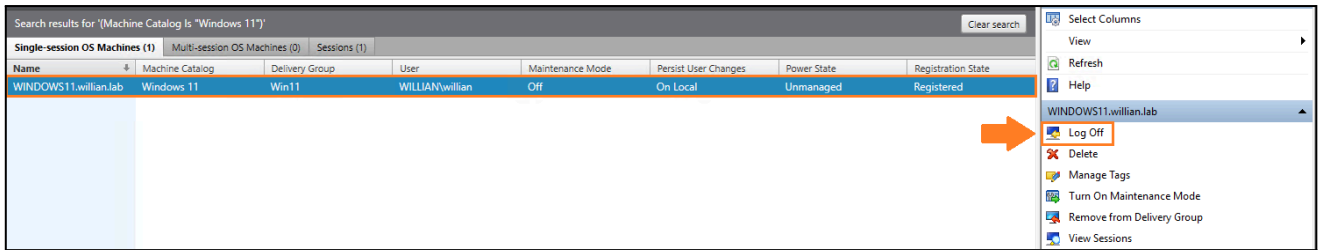
Go to **Machine Catalogs** and click **View Machines**.



Click over the VDA and you will probably see a "log off" icon on the right side. Just click "log Off" and wait a minute. Refresh the page and confirm you do not see the "log off" icon anymore. Log on again to the Storefront and try to launch the Desktop.

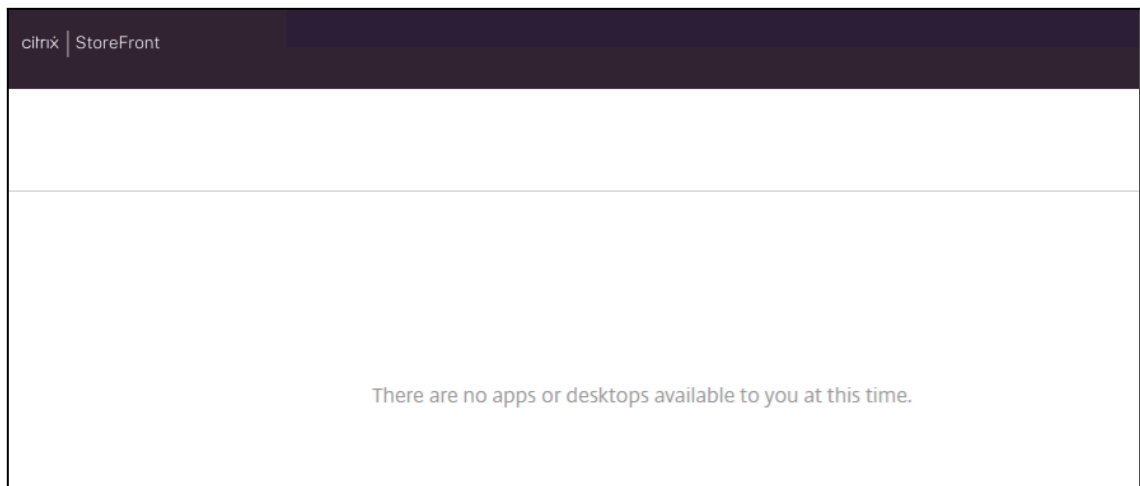
Search results for "(Machine Catalog is "Windows 11")							
Name	Machine Catalog	Delivery Group	User	Maintenance Mode	Persist User Changes	Power State	Registration State
WINDOWS11.willian.lab	Windows 11	Win11	WILLIAN\willian	Off	On Local	Unmanaged	Registered

Select Columns  
 View  
 Refresh  
 Help  
 WINDOWS11.willian.lab  
 Log Off  
 Delete  
 Manage Tags  
 Turn On Maintenance Mode  
 Remove from Delivery Group  
 View Sessions



## There are no apps or Desktops available to you at this time Error

- Confirm your delivery controller Address (FQDN) is correctly added under the Storefront setting "Store Name > > Manage Delivery Controllers, right side option).
- Make sure you can resolve the name properly (ping the address entered)
- Alternatively, you can change the DDC FQDN to DDC IP as a test
- Ensure you did not restrict access under the Delivery group to a specific group/user



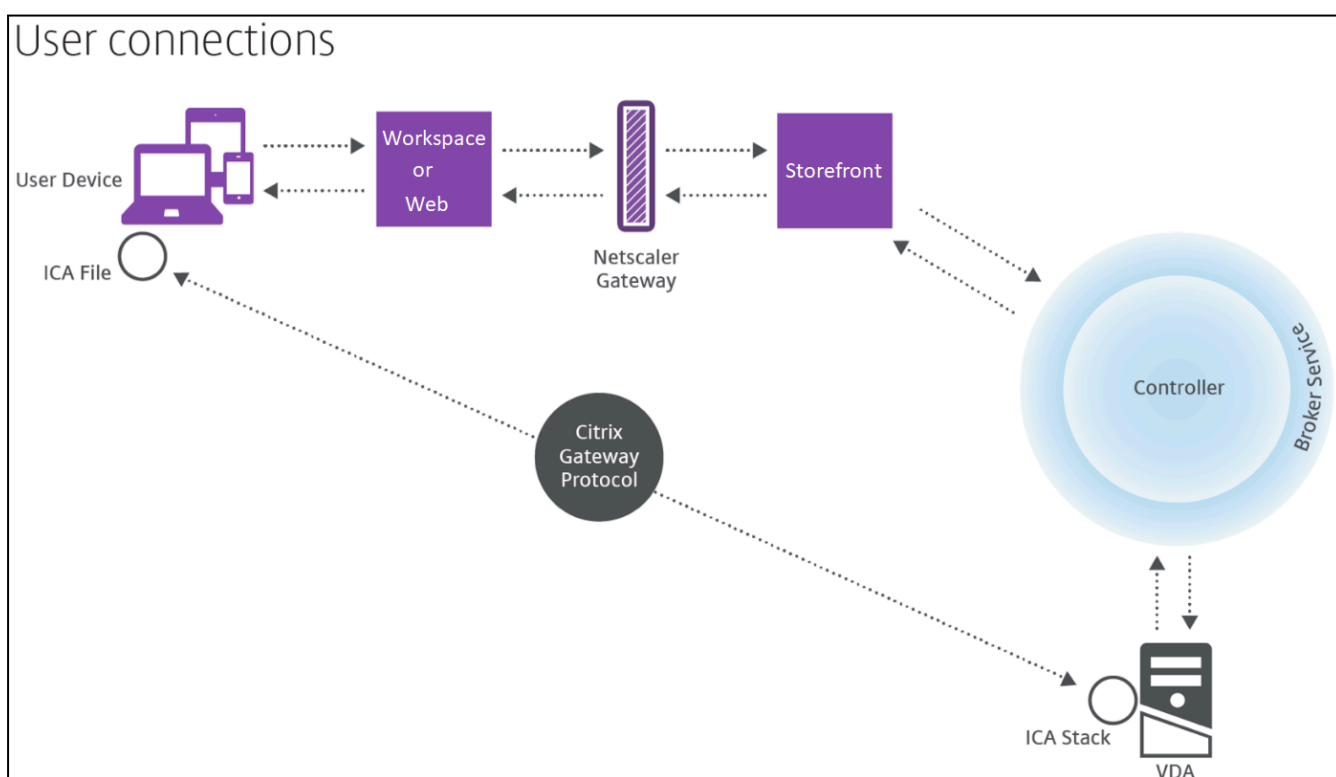
# Integrating NetScaler Gateway with CVAD on-prem

**NOTE 1:** Please ensure that your CVAD environment is up and running before proceeding to the next steps.

NetScaler Gateway is a secure access solution that provides remote access to Citrix Virtual Apps and Desktops.

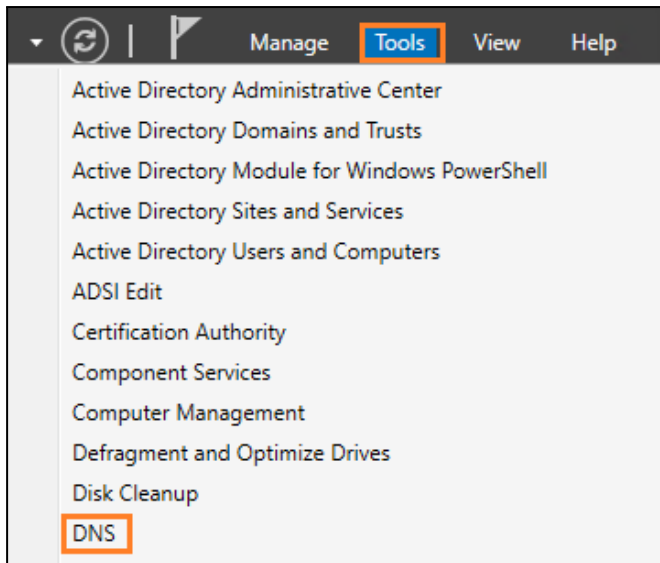
It acts as a secure gateway, authenticating users and providing a secure channel for communication between the client devices and the Citrix infrastructure. ICA (Independent Computing Architecture) is the protocol used by Citrix for communication between the client device and the Citrix Virtual Apps and Desktops servers.

**NOTE 2:** The ICA connection only happens when the end-user opens the external ICA file using the Citrix Workspace app (CWA) installed on their device. The Citrix Workspace app establishes a connection with the Citrix Virtual Apps and Desktops server through the NetScaler Gateway using the information from the ICA file. The below image illustrates the flow.

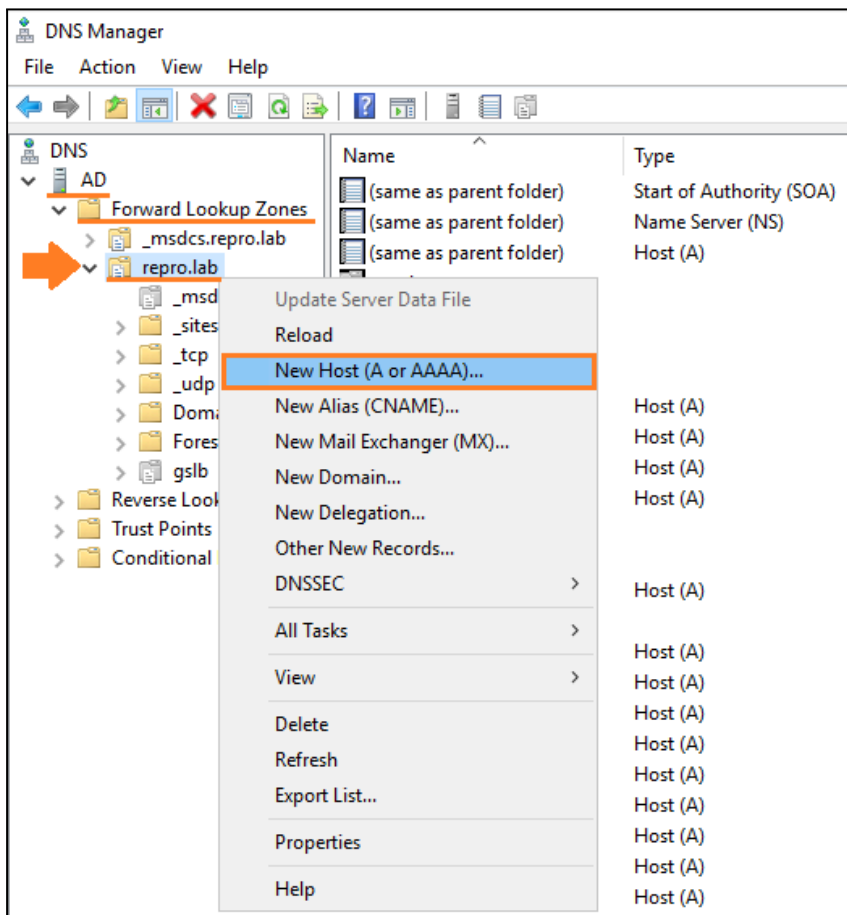


## DNS Configuration for STA and Gateway

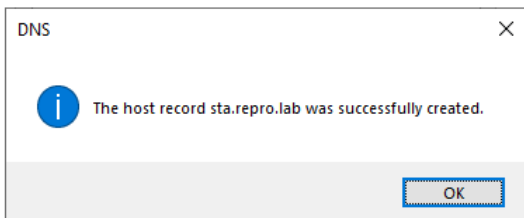
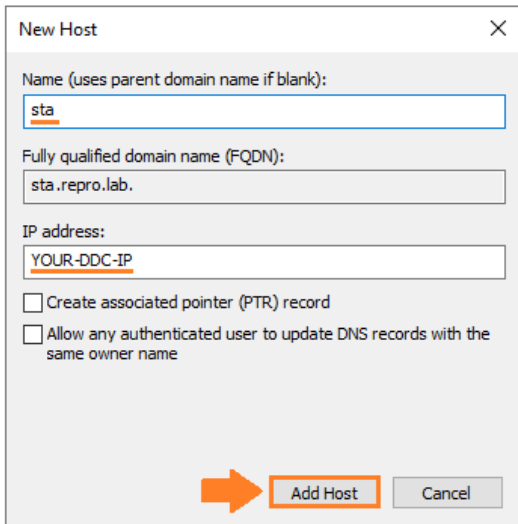
1. Access your internal Windows Server DNS VM and Open the Server Manager. Navigate to **Tools > DNS**.



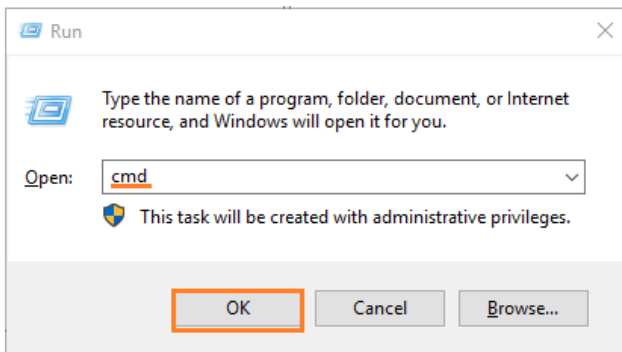
2. Navigate to your domain. **AD > Forward Lookup Zones > repro.lab**. Right-click **repro.lab** and select **New Host (A or AAAA)...**



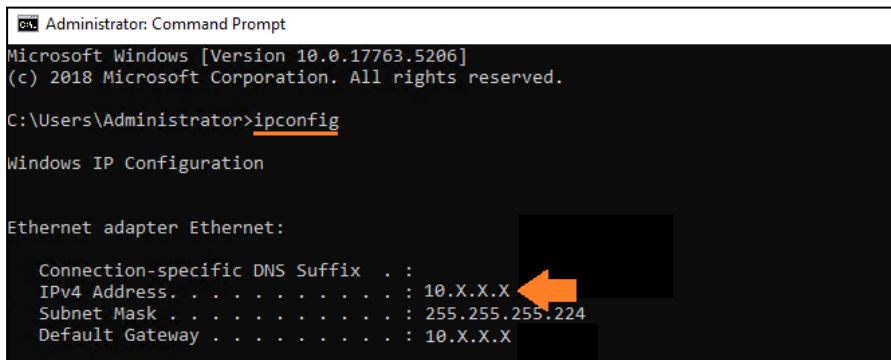
3. Add a host entry for your **STA Server**. As STA is a DDC component (in-built), you need to specify your **host + DDC IP**. We will use **"sta.repro.lab"** to refer to the STA server.



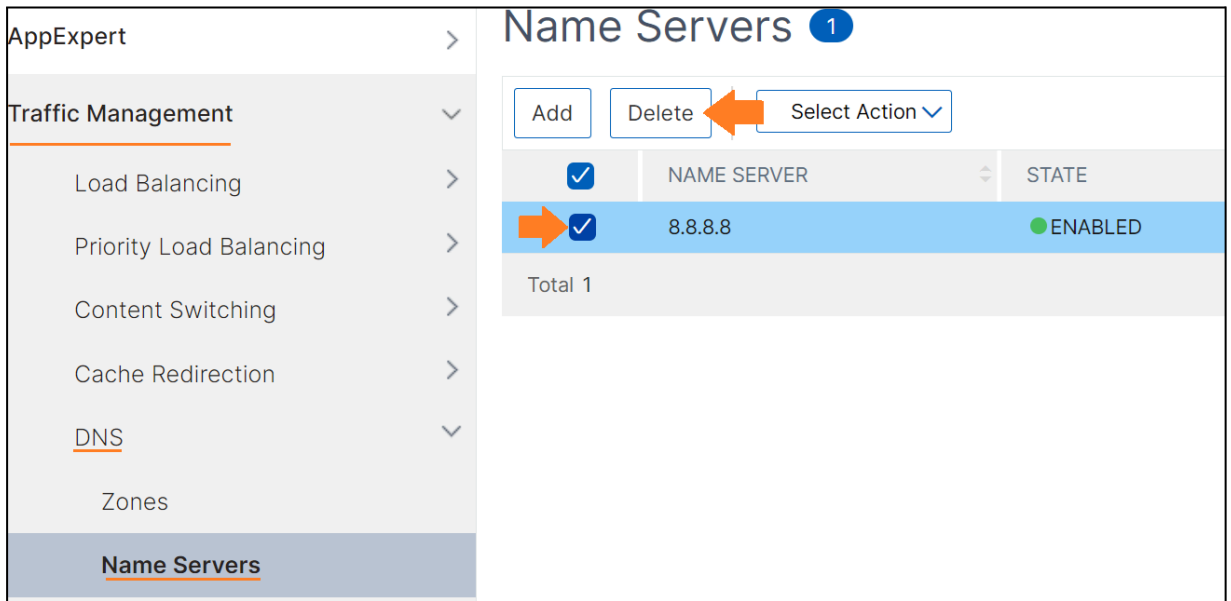
4. Take your **Windows AD-DNS Server's IP** and **add** it to the NetScaler ADC01 and ADC03 as a **DNS Server client (LDNS)**. Without this, the NetScaler will not be able to resolve internal domain names.



5. Enter **ipconfig** and **copy** YOUR OWN IP Address.

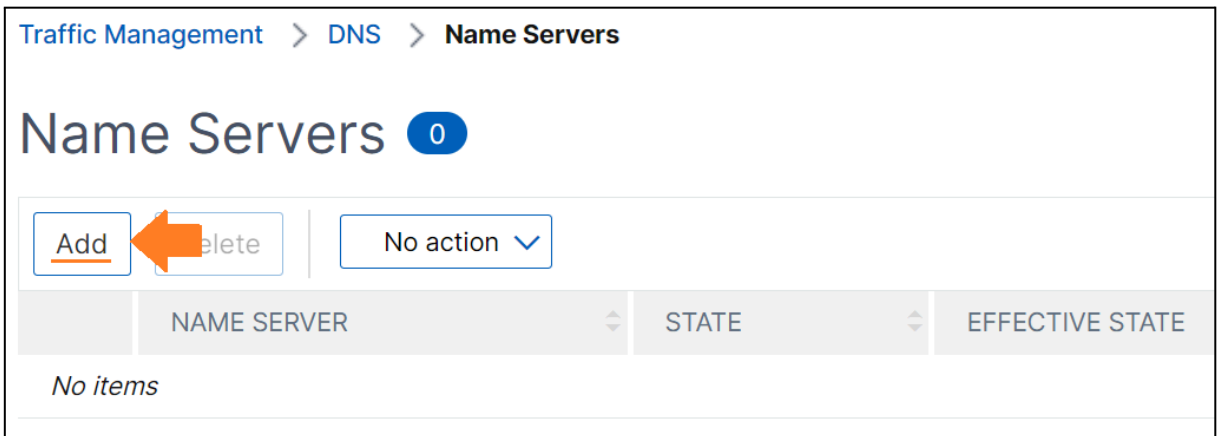


6. From your NetScaler, navigate to **Traffic Management > DNS > Name Servers**, select all your DNS Server IPs and click Delete. Click **YES** to confirm.



The screenshot shows the NetScaler interface for managing Name Servers. On the left, a navigation menu includes 'AppExpert', 'Traffic Management', 'Load Balancing', 'Priority Load Balancing', 'Content Switching', 'Cache Redirection', 'DNS', and 'Name Servers'. The 'Name Servers' section is active. The main content area is titled 'Name Servers 1'. It features an 'Add' button, a 'Delete' button with an orange arrow pointing to it, and a 'Select Action' dropdown. Below this is a table with columns 'NAME SERVER' and 'STATE'. One row is highlighted in blue, containing the IP '8.8.8.8' and the state 'ENABLED'. A 'Total 1' summary is shown at the bottom of the table.

7. Refresh the page and click **Add** to add your own DNS server.



The screenshot shows the NetScaler interface for managing Name Servers after refreshing. The breadcrumb navigation is 'Traffic Management > DNS > Name Servers'. The main content area is titled 'Name Servers 0'. It features an 'Add' button with an orange arrow pointing to it, a 'Delete' button, and a 'No action' dropdown. Below this is a table with columns 'NAME SERVER', 'STATE', and 'EFFECTIVE STATE'. The table is empty, displaying 'No items'.

8. Add your **AD-DNS IP** copied before and select protocol **UDP\_TCP**. Click **Create**.

**NOTE:** Having TCP as a DNS option is beneficial, especially when dealing with substantial DNS responses. For more information, check out this [CTX article](#).



← Create Name Server

IP Address     DNS Virtual Server

IP Address

10 . X . X . X ⓘ

Local

Protocol\*

UDP\_TCP ⓘ

DNS Profile

Enable Name Server

9. Your DNS service should be marked as UP. **Save** the configuration.

Traffic Management > DNS > Name Servers

Name Servers 2

<input type="checkbox"/>	NAME SERVER	STATE	EFFECTIVE STATE	IS LOCAL?	PROTOCOL
<input type="checkbox"/>	10.110.X.X	● ENABLED	● UP	✗	UDP
<input type="checkbox"/>	10.110.X.X	● ENABLED	● UP	✗	TCP

Total 2 250 Per Page

10. Confirm your NetScaler can reach both hostnames you have created. **Open** your NetScaler **ADC01** using the **mRemoteNG** tool.

11. Use the command **"drill"** in the shell to confirm the NetScaler can resolve to **storefront.repro.lab** and **sta.repro.lab**. Alternatively, you can use ping.

**NOTE:** Before the NetScaler version **13.1**, the command **"dig"** was used instead (Freebsd change).

```

root@netscaler01# drill storefront.repro.lab
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 12266
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; storefront.repro.lab.      IN      A

;; ANSWER SECTION:
storefront.repro.lab.      3600   IN      A      10.X.X.X
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
  
```

12. Confirm your NetScaler can resolve **sta.repro.lab** as well.

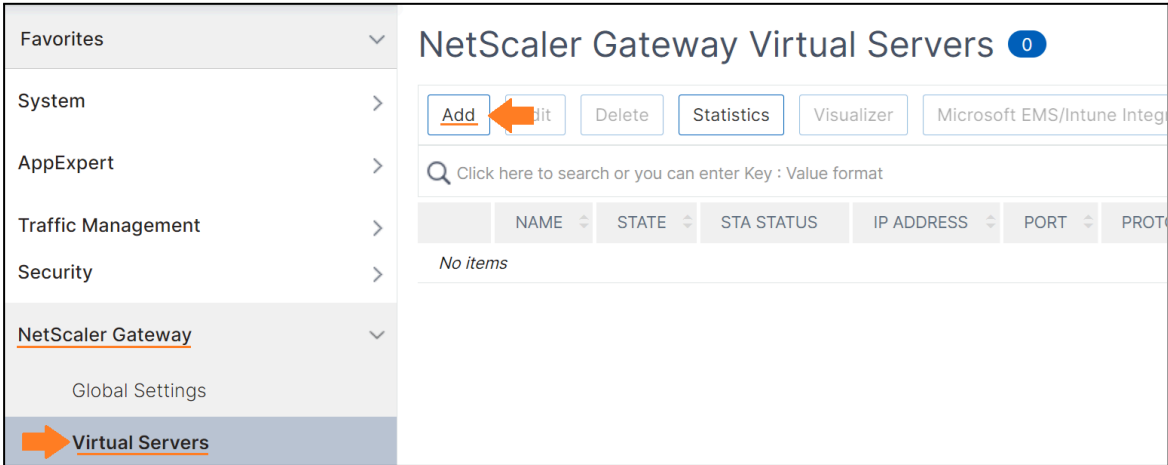
```
root@netscaler01# drill sta.repro.lab
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 12266
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; storefront.repro.lab.          IN      A
;; ANSWER SECTION:
storefront.repro.lab.  3600   IN      A      10.X.X.X
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
```

DNS configuration is done.

## Gateway Vserver Configuration

**NOTE:** For a better understanding, we will create all the Gateway configurations manually.

1. On the NetScaler ADC01 GUI, navigate to **NetScaler Gateway > Virtual Servers** and click **Add**.



2. Enter **external\_gateway\_cvad** in the **Name** input field, and set a new free IP address. Click **OK**.

### VPN Virtual Server

**Basic Settings**

Name\*  
 ⓘ

Protocol\*

IP Address Type\*

IPAddress\*  
 ⓘ

Port\*

▶ More

3. If you have not enabled the SSLVPN feature yet, you will see the below pop-up. Click **Yes**.

? Confirm ×

Feature 'SSLVPN' is disabled.  
Do you wish to enable it?

4. Click **No Server Certificate** and bind the **Wildcard SSL certificate** we have created before.

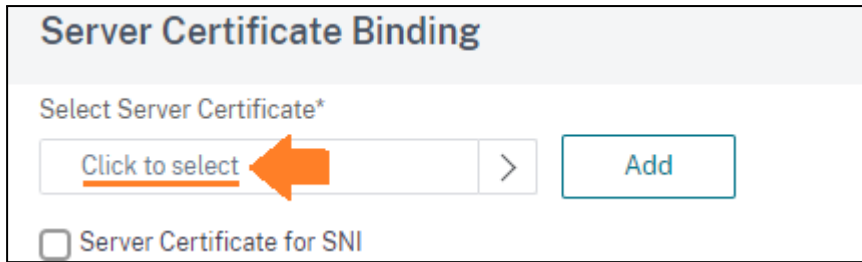
**Certificate**

**No Server Certificate** <input type="button" value="> >

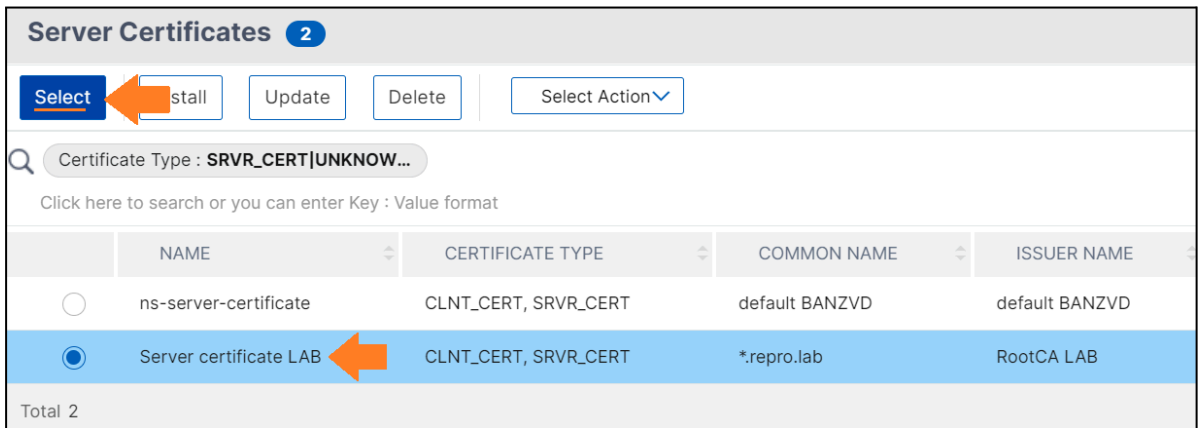
**No CA Certificate** >

**No BundleCertificate** >

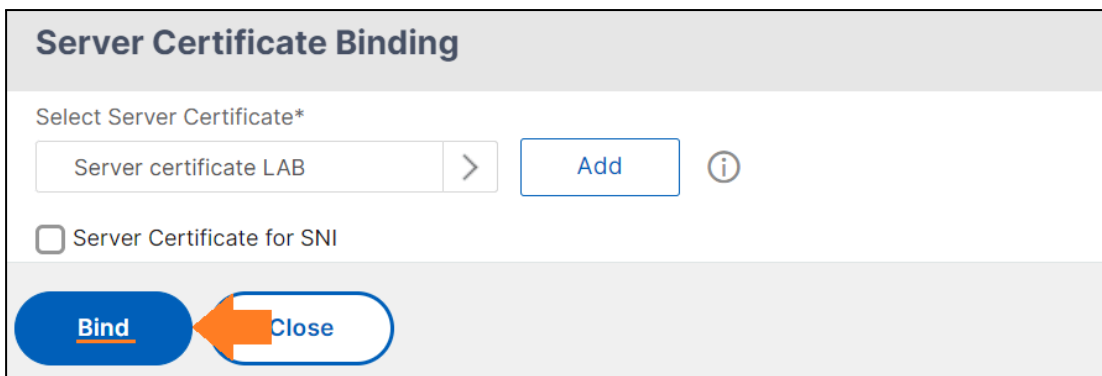
5. Click **Click to Select**.



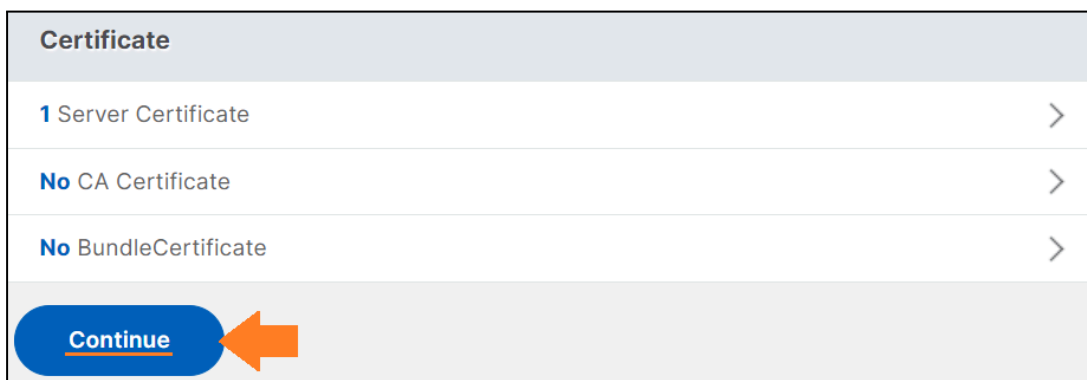
6. Select the **Server Certificate LAB** radio button and click **Select**.



7. Click **Bind**.



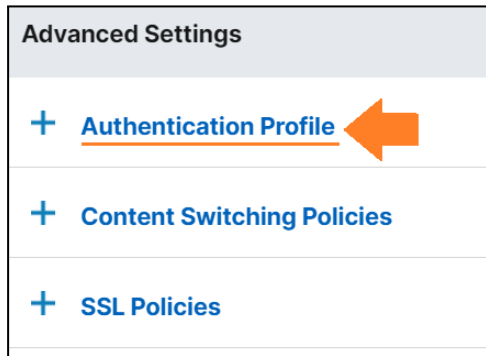
8. Click **Continue**.



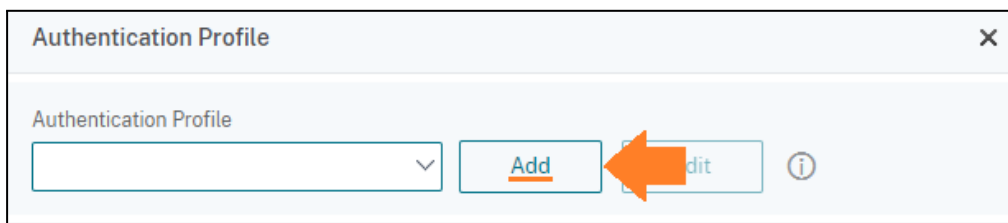
9. Click **Done**.

## Configuring Advanced Authentication

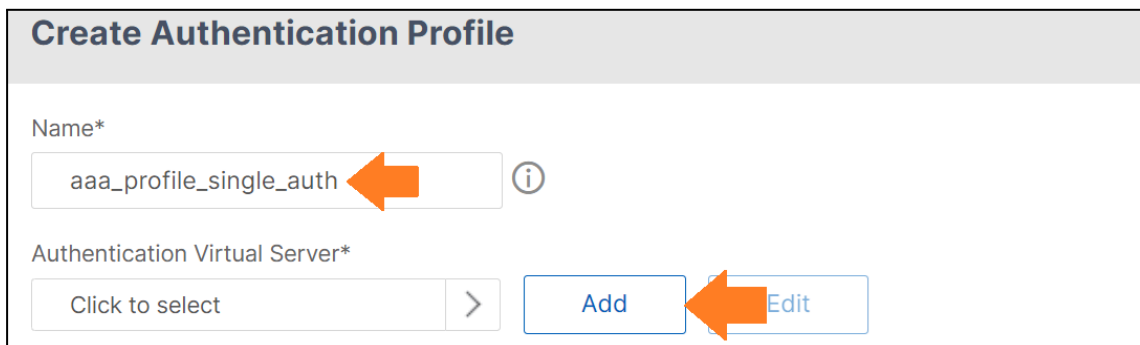
1. Click **Authentication Profile** to add your LDAP server to the Gateway.



2. **11.** Click **Add**.



3. Enter **aaa\_profile\_single\_auth** in the **Name** input field and click **Add**.



4. Enter **aaa\_vserver\_single\_auth** in the **Name** input field, change the **IP Address Type** to **Non Addressable**, and then click OK.

---

**Note:** As this AAA Vserver will be used for internal communication, there is no need for an IP address.

---

### Authentication Virtual Server

**Basic Settings**

Name\*

IP Address Type\*

Protocol

▶ More

OK
Cancel

5. Click **No Authentication Policy** to add your LDAP.

**NOTE:** The “Nfactor Flow” can be used from version 13.0 onwards to create the authentication flow as outlined in the [documentation](#).

**Basic Settings**

Name <b>aaa_vserver_single_auth</b>	IP Address <b>0.0.0.0</b>
	Port <b>0</b>

**Advanced Authentication Policies**

- No** nFactor Flow
- No** Authentication Policy
- No** SAML IDP Policy
- No** OAuth IDP Policy
- No** Smart Access Policy

6. Click **Add** to add the LDAP policy.

7. Enter **ldap\_advanced\_policy** in the **Name** input field, select **LDAP** on the **Action Type** drop-down list, and click **Add** to add an action.

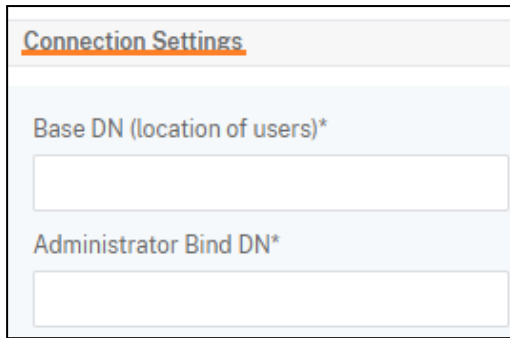
8. Enter the name **LDAP**, select **"Server IP"**, and under **"security type"** select **SSL**.

---

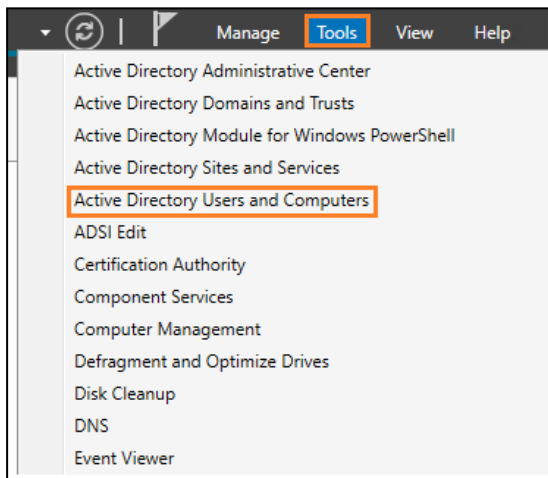
**NOTE: PLAINTEXT** also works, but for security reasons, it is recommended to use SSL. Also, security type as SSL, allows password change (LDAP passwords) through the NetScaler Gateway.

---

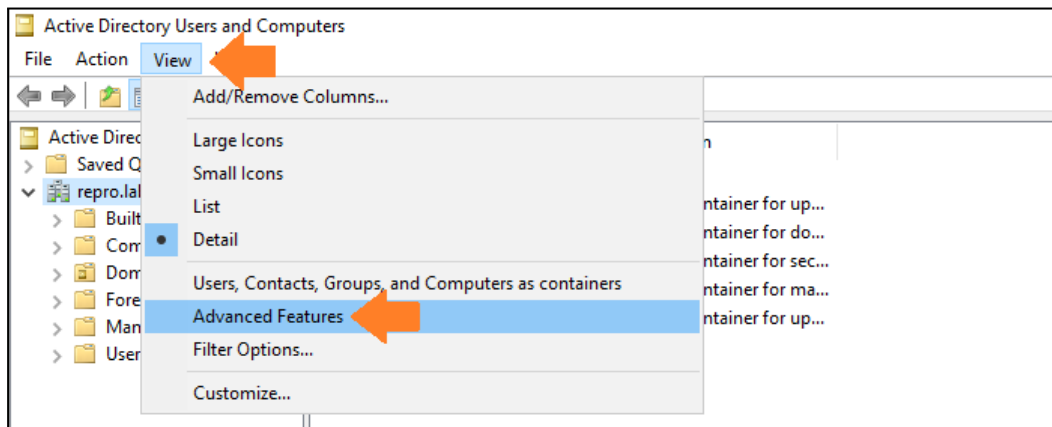
9. Under **Connection Settings**, you will need to specify your **LDAP Base DN** and **Administrator Bind DN** which you can get from your **LDAP Server** as the next steps.



10. In your **Windows Server LDAP (Active Directory) VM**, open the **Server Manager**, and navigate to **Tools > Active Directory Users and Computers**.

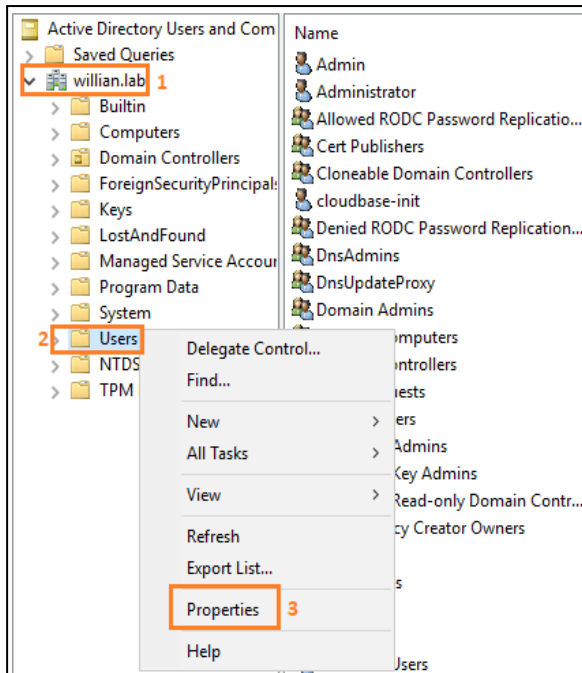


11. Click **View** and enable **Advanced Features**.

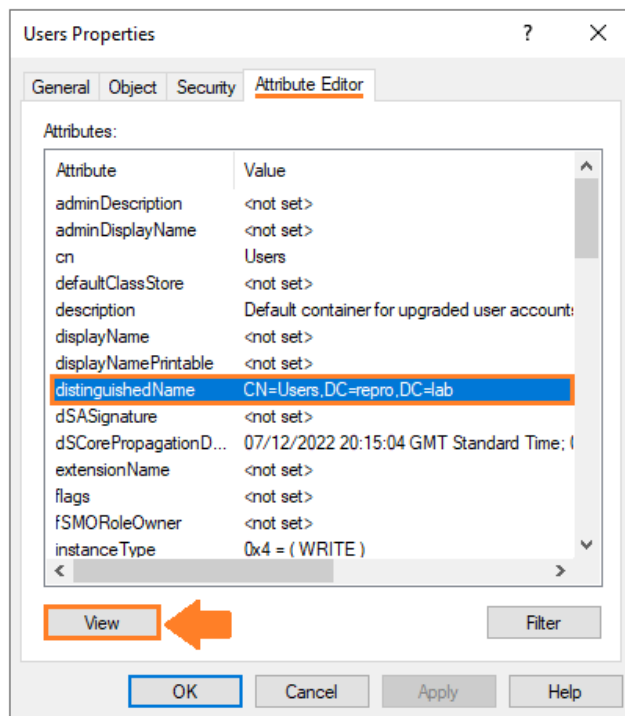


12. Under your domain, right-click **Users** and then click **Properties**.

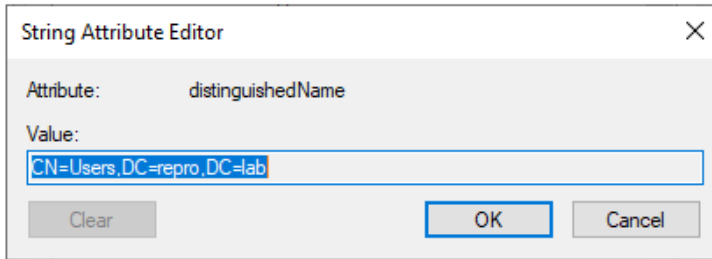




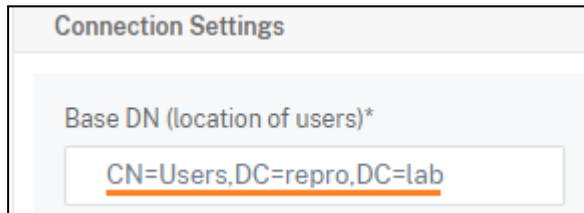
13. Click the **Attribute Editor** tab, select **distinguishedName**, and click **View**.



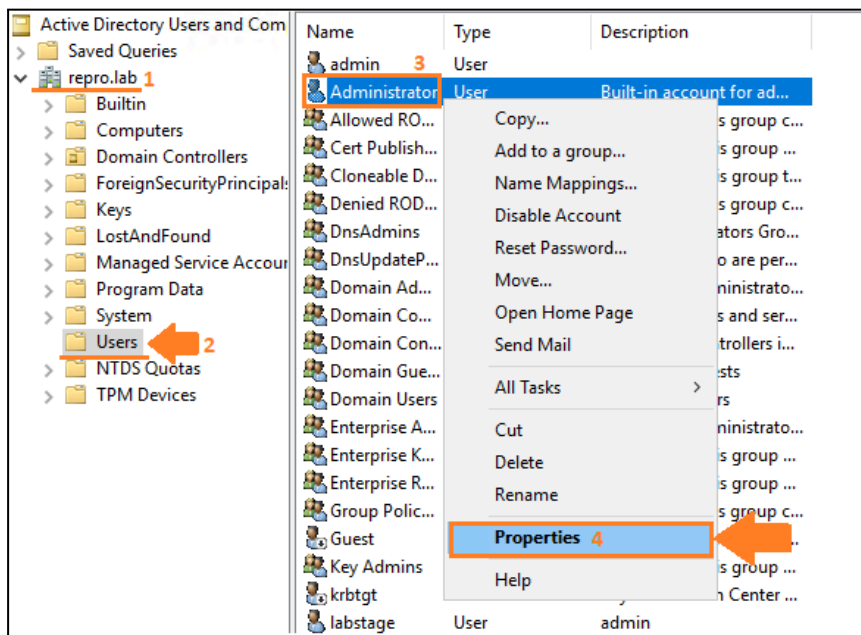
14. Copy the **value**.



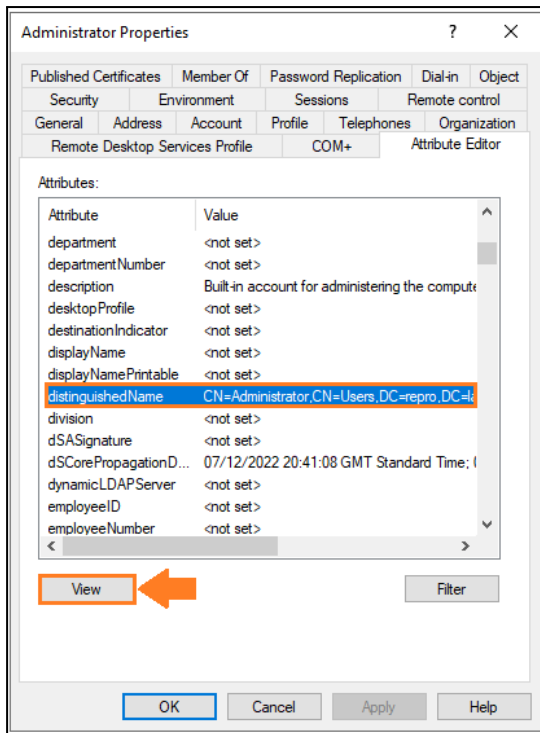
- Go back to the **NetScaler** and paste the above value into the **Base DN (location of users)\*** input field.



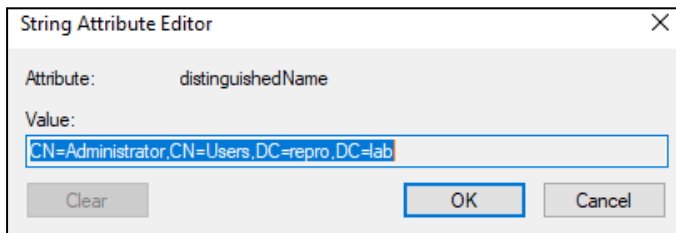
- Return to your **LDAP (Active Directory) VM** to get the Administrator Bind DN\*. Click **Users**, right-click your **administrator/Admin** user, and then click **Properties**.



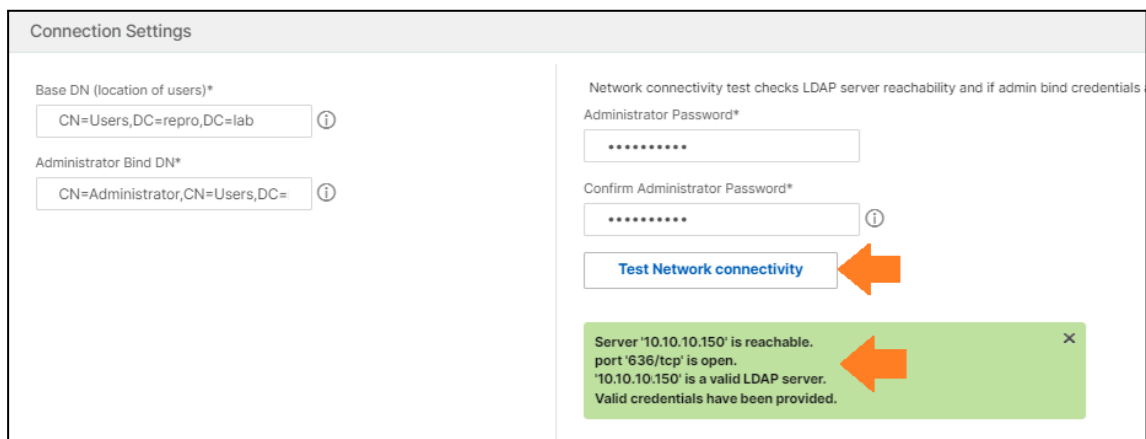
- Click the **Attribute Editor** tab, scroll down to locate **distinguishedName** and click to select it, and then click **View**.



18. Copy the value.



19. Go back to the **NetScaler ADC01**, paste the value under **Administrator Bind DN\***, insert your administrator/admin password, and click **Test Network Connectivity**. If everything goes well, you should see a green message informing the LDAP is reachable and the credential provided is correct.



20. Click the **Server Logon Name attribute** drop-down button and select **sAMAccountName**.

21. Click the **Group Attribute** drop-down button and select **memberOf**.

22. Click the **Sub Attribute Name** drop-down button, and select **cn**.
23. Click the **SSO Name Attribute** drop-down button and select **cn**.
24. Click **Create**.

**NOTE:** `admin-user@domain` is also acceptable for **Administrator Bind DN\*** as in the example below.

The screenshot shows the 'Other Settings' configuration page. On the left side, there are several dropdown menus: 'Server Logon Name Attribute' (set to sAMAccountName), 'Group Attribute' (set to memberOf), 'Sub Attribute Name' (set to cn), and 'SSO Name Attribute' (set to cn). Below these are text input fields for 'Email' (mail), 'Alternate Email', and 'Cloud Attributes\*' (DISABLED). On the right side, there are checkboxes for 'User Required' (checked), 'Allow Password Change' (checked), and 'Referrals' (unchecked). Below these are a 'Maximum Referral Level' dropdown (set to 1), a 'Referral DNS Lookup' dropdown (set to A-REC), and a 'Validate LDAP Server Certificate' checkbox (unchecked). There are also text input fields for 'Default Authentication Group', 'LDAP Host Name', 'OTP Secret', 'Push Service', and 'KB Attribute'. At the bottom left, there is a blue 'Create' button with an orange arrow pointing to it.

**NOTE:** `sAMAccountName` will allow you to use the user's logon name to login rather than **UPN** (email format).

25. Enter the text **true** under the **Expression** section and click Create.

The screenshot shows the 'Create Authentication Policy' page. The 'Name\*' field contains 'ldap\_advanced\_policy'. The 'Action Type\*' dropdown is set to 'LDAP'. The 'Action\*' dropdown is also set to 'LDAP'. The 'Expression\*' field contains the text 'true'. There are 'Add' and 'Edit' buttons next to the 'Action\*' dropdown. At the bottom left, there is a blue 'Create' button with an orange arrow pointing to it.

26. Click **Bind**.

**Policy Binding**

Select Policy\*

ldap\_advanced\_policy > [Add](#) [Edit](#)

► More

**Binding Details**

Priority\*

100

Goto Expression\*

NEXT

Select Next Factor

Click to select > [Add](#) [Edit](#)

[Bind](#) [Close](#)

27. The advanced authentication policy is configured. Click **Continue**.

**Authentication Virtual Server**

**Basic Settings**

Name	aaa_vserver_single_auth	IP Address	0.0.0.0
		Port	0

**Advanced Authentication Policies**

No nFactor Flow

1 Authentication Policy

No SAML IDP Policy

No OAuth IDP Policy

No Smart Access Policy

[Continue](#) [Cancel](#)

28. Click **Done**.

**Advanced Authentication Policies**

No nFactor Flow

1 Authentication Policy

No SAML IDP Policy

No OAuth IDP Policy

No Smart Access Policy

[Done](#)

29. Click **Create**.

**Create Authentication Profile**

Name\*  
 ⓘ

Authentication Virtual Server\*  
 >

30. Click **OK**.

**Authentication Profile**

Authentication Profile  
 ▾   ⓘ

31. Click **Done**.

## STA and Session Policies

- Under **“Advanced settings”** on the right side, click **“Published Applications”** to add your STA server (DDC IP).

**Advanced Settings**

- + Content Switching Policies
- + SSL Policies
- + Intranet IP Addresses
- + Intranet Applications
- + Published Applications

- Click **No STA Server**.

Published Applications ×

- No Next HOP Server >
- No STA Server
- No Url >

3. Enter the **STA fqdn** you created in the first steps of this guide and click **Bind**. Alternatively, you can use your **STA server IP/DDC IP**, it works too. If using **repro.lab**, your STA FQDN is **sta.repro.lab**.

**STA Server Binding**

Secure Ticket Authority Server\*

Secure Ticket Authority Server Address Type  
IPv4 ⓘ

**Bind** Close

40. Your STA is bound. **Click** again over it, and confirm it shows **UP**.

**Published Applications** ×

No Next HOP Server >

**1 STA Server** >

No Url >

4. Click **Close**.

**VPN Virtual Server STA Server Binding**

Add Binding Unbind Refresh

Click here to search or you can en

<input type="checkbox"/>	SECURE TICKET AUTHORITY SERVER	SECURE TICKET AUTHORITY SERVER ADDRESS TYPE	STATE	AUTH ID
<input type="checkbox"/>	http://sta.repro.lab	IPv4	● UP	STA380059977

**Close**

5. Click the **+** in the **Policies** section to add session policies for WEB and Citrix Workspace App (CWA).

**Policies** + ×

Request Policies

4 Cache Policies >

Response Policies

2 Cache Policies >

6. Select Session and click **Continue**.

### Choose Type

**Policies**

Choose Policy\*

Choose Type\*

7. Click **Add**.

**Policies**

Choose Policy Session	Choose Type Request
--------------------------	------------------------

**Policy Binding**

Select Policy\*

8. Enter **session\_policy\_workspace\_app** in the Name input field, and click **Add** to add the CWA profile.

### Create NetScaler Gateway Session Policy

Name\*

Profile\*  
   ⓘ

9. Enter **session\_profile\_workspace\_app** in the **Name** input field and click the **Client Experience** tab.



Choose Type > Create NetScaler Gateway Session Policy > Create NetScaler Gateway Session Profile

### Create NetScaler Gateway Session Profile

Name\*  
 ⓘ

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

<b>Network Configuration</b>	<b>Client Experience</b> ←	Priority	Published Applications	Remote Desktop	PCoIP
------------------------------	----------------------------	----------	------------------------	----------------	-------

Override Global

DNS Virtual Server  
  Override Global

WINS Server IP  
  Override Global

Kill Connections\*  
  Override Global

Advanced Settings

**Create** **Close**

**NOTE:** While we are utilizing **Advanced Authentication**, the SSO option under “Client Experience” will not be affected.

**10. Set:**

- Split Tunnel: **OFF**
- Clientless Access: **ON**
- Plugin-in-type: **Java**

Display Home Page

Home Page  
  Override Global ⓘ

URL for Web-Based Email  
  Override Global

Split Tunnel\*  
  Override Global ←

Session Time-out (mins)  
  Override Global

Client Idle Time-out (mins)  
  Override Global

Clientless Access\*  
  Override Global ←

Clientless Access URL Encoding\*  
  Override Global

Clientless Access Persistent Cookie\*  
  Override Global

Advanced Clientless VPN Mode\*  
  Override Global

Plug-in Type\*  
  Override Global ←

11. Change the default authorization **Action** to **ALLOW** in the **Security** tab .

**Create NetScaler Gateway Session Profile**

Name\*  
 ⓘ

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

Network Configuration | Client Experience | **Security** ← | Published Applications | Remote Desktop | PCoIP

Override Global

Default Authorization Action\*  
  Override Global ←

Secure Browse\*  
  Override Global

Smartgroup  
  Override Global

12. Set the following in the **Published Applications** tab and then click **OK**.

ICA Proxy: **ON**

Web Interface Address: **FQDN of your StoreFront server (or lbvip) – (http://storefront.repro.lab)**

Single Sign-on Domain: **Your domain/NetBIOS**

Account Services Address: **Enter your account services address (base URL Storefront)**

(e.g. <http://storefront.repro.lab> )

**NOTE:** CWA relies on the **service account** to select a Store. The CWA will contact the **Storefront**, download the **Provisioning File**, and will rely on the settings for Store selection.

13. Add the below expression for CWA (**Citrix Workspace App**) and click **Create**. This policy will be evaluated to TRUE if the NetScaler gets hit from a client using the CWA.  
**HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")**

**Create NetScaler Gateway Session Policy**

Name\*  
 ⓘ

Profile\*

Advanced Policy  Classic Policy

Expression\* [Expression Editor](#)

Select Select Select

HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")

[Evaluate](#)

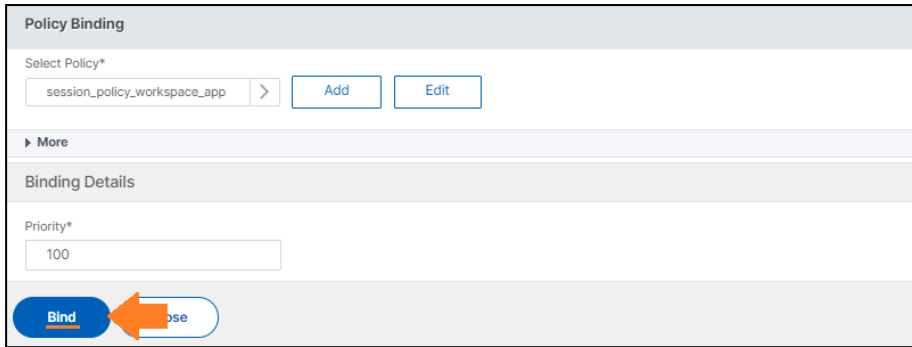
**NOTE:** When conducting a network trace and examining the **HTTP headers**, it becomes evident that a **CLIENT** connected via **Citrix Workspace App (CWA)** is identified by the "**CitrixReceiver...**" tag in the "**User-Agent**". This information is crucial for NetScaler to match the CLIENT to the **CWA Session Policy**, as the policy on NetScaler specifies "User-Agent contains CitrixReceiver".

No.	Time	TCP Delta	Length	Source
6291	2023-08-25 07:44:43.407	0.000000957	1017	10.91.69.154

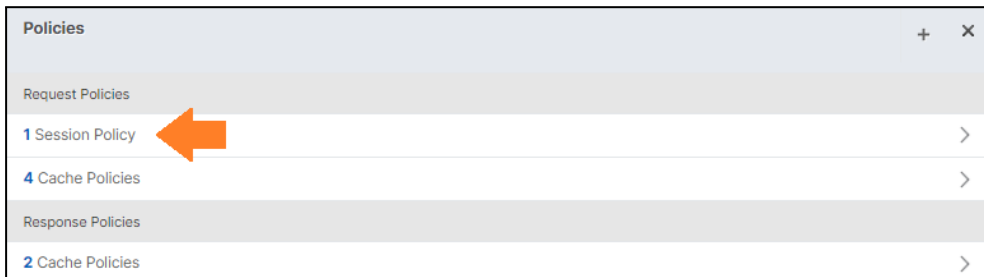
```

> Frame 6291: 1017 bytes on wire (8136 bits), 1017 bytes captured (8136 bits)
> NetScaler Packet Trace
> Ethernet II, Src: c0:42:d0:89:32:36, Dst: 02:00:15:b6:00:0a
> Internet Protocol Version 4, Src: 10.91.69.154 (10.91.69.154), Dst: 10.91.68.209
> Transmission Control Protocol, Src Port: 61367, Dst Port: 443, Seq: 3447, Ack: 21
> Transport Layer Security
v Hypertext Transfer Protocol
  > POST /Citrix/LBSFWeb/CitrixAuth/Login HTTP/1.1\r\n
    Cache-Control: no-cache\r\n
    Connection: Keep-Alive\r\n
    User-Agent: CitrixReceiver/23.7.1.6 Windows/10.0 SelfService/23.7.1.6 (Release)
  
```

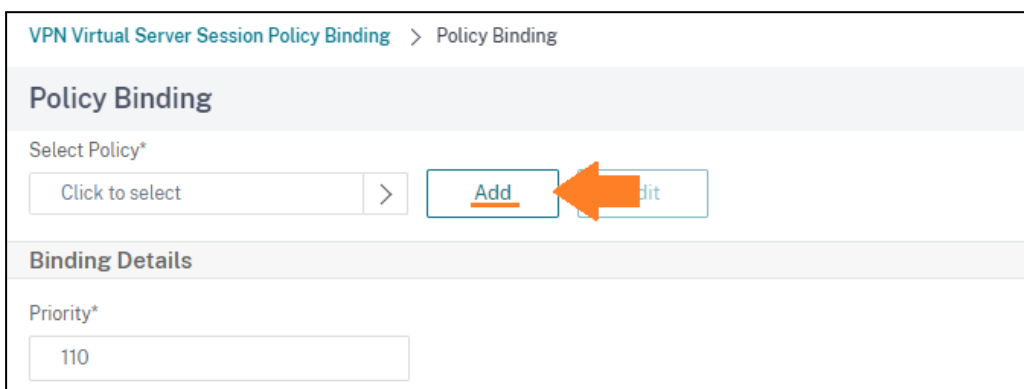
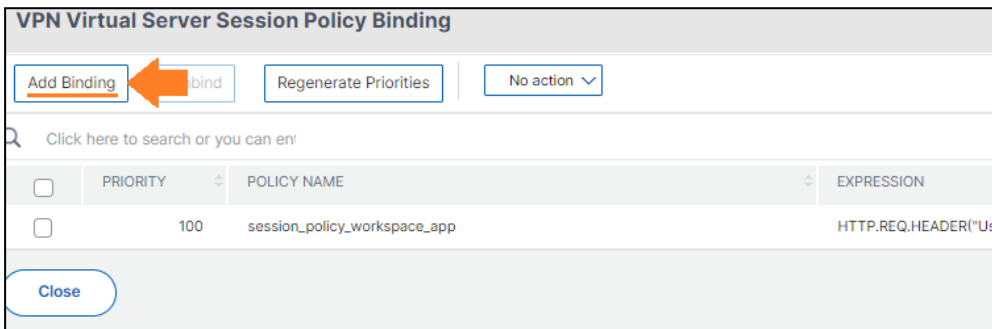
14. Click **Bind**.



15. Click **1 Session Policy** to add the WEB session policy.



16. Click **Add Binding**.



17. Enter **Session\_policy\_Web** in the **Name** input field and click **Add**.

**Create NetScaler Gateway Session Policy**

Name\*  
 ⓘ

Profile\*

Advanced Policy  Classic Policy

18. Enter **session\_profile\_Web** in the **Name** input field and click the **Client Experience** tab.

**Create NetScaler Gateway Session Profile**

Name\*  
 ⓘ

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

**Network Configuration** | Client Experience | Published Applications | Remote Desktop | PCoIP

Override Global

DNS Virtual Server  
  Override Global

WINS Server IP  
  Override Global

Kill Connections\*  
  Override Global

Advanced Settings

19. **Set:**

Split Tunnel: **OFF**

Clientless Access: **ON**

Plugin-in-type: **Windows/MAC OS X**

Network Configuration	Client Experience	Security	Published Applications	Remote Desktop	PCoIP
Accounting Policy					
<input type="text"/>					
Override Global					
<input type="checkbox"/> Display Home Page					
Home Page					
<input type="text"/>					
Override Global					
URL for Web-Based Email					
<input type="text"/>					
Override Global					
Split Tunnel*					
<input type="text" value="OFF"/>					
<input checked="" type="checkbox"/> Override Global					
Session Time-out (mins)					
<input type="text" value="30"/>					
Override Global					
Client Idle Time-out (mins)					
<input type="text"/>					
Override Global					
Clientless Access*					
<input type="text" value="On"/>					
<input checked="" type="checkbox"/> Override Global					
Clientless Access URL Encoding*					
<input type="text" value="Obscure"/>					
Override Global					
Clientless Access Persistent Cookie*					
<input type="text" value="DENY"/>					
Override Global					
Advanced Clientless VPN Mode*					
<input type="text" value="DISABLED"/>					
Override Global					
Plug-in Type*					
<input type="text" value="Windows/MAC OS X"/>					
<input checked="" type="checkbox"/> Override Global					

**NOTE:** While we are utilizing **Advanced Authentication**, the SSO option under “Client Experience” will not be affected.

20. Change the **Default Authorization Action** in the Security tab to **ALLOW**.

Create NetScaler Gateway Session Profile					
Name*					
<input type="text" value="session_profile_Web"/>					
<small>Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.</small>					
Network Configuration	Client Experience	Security	Published Applications	Remote Desktop	PCoIP
Override Global					
Default Authorization Action*					
<input type="text" value="ALLOW"/>					
<input checked="" type="checkbox"/> Override Global					
Secure Browse*					
<input type="text" value="ENABLED"/>					
Override Global					
Smartgroup					
<input type="text"/>					
Override Global					
<input type="checkbox"/> <b>Advanced Settings</b>					

21. Set the following in the **Published Applications** tab and then click **OK**.

22. Set:

ICA Proxy: **ON**

Web Interface Address: **FQDN of your StoreFront server (or lbvip) followed by the path to Store (e.g <http://storefront.repro.lab/Citrix/StoreWeb>**

Single Sign-on Domain: **Your domain/NetBIOS**

Network Configuration Client Experience Security **Published Applications** Remote Desktop PCoIP

ICA Proxy\*  
ON  Override Global ⓘ

Web Interface Address  
http://storefront.repro.lab/Cit  Override Global ⓘ

Web Interface Address Type\*  
IPV4

Web Interface Portal Mode  
 Override Global

Single Sign-on Domain  
repro.lab  Override Global ⓘ

Citrix Receiver Home Page  
 Override Global

Account Services Address  
 Override Global

Create Close

**NOTE:** Workspace for WEB **does not** rely on the setting “**Account Service**” to select a store for the end-users as CWA does, it relies on the **Store path** that is set under Web Interface Address though.

23. Add the below expression for Web browsers and click **Create**. This policy will be evaluated to TRUE if the NetScaler gets hit by a client using Chrome, IE, Edge, Firefox, Safari, etc.  
**HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT**

Create NetScaler Gateway Session Policy

Name\*  
session\_policy\_web ⓘ

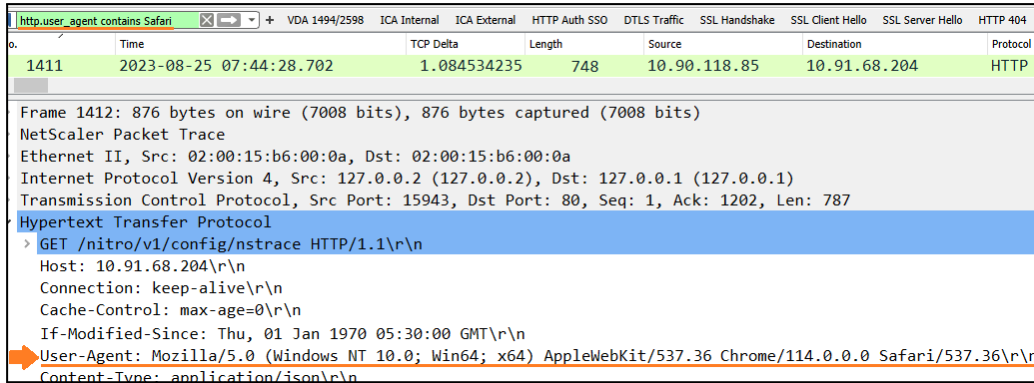
Profile\*  
session\_profile\_Web Add Edit ⓘ

Advanced Policy  Classic Policy

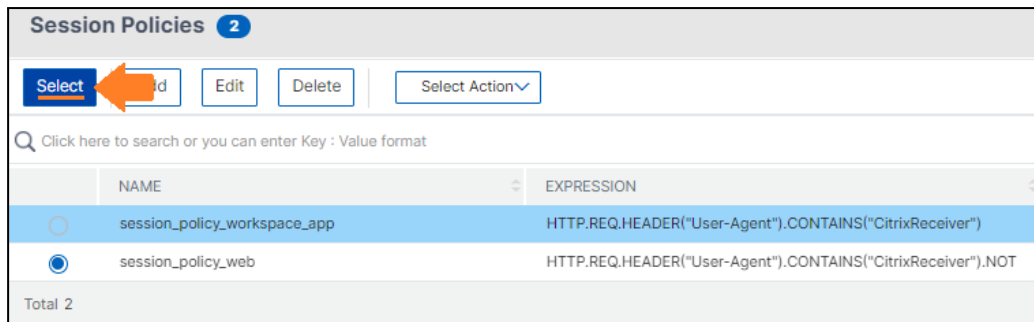
Expression \* [Expression Editor](#)  
Select Select Select ⓘ  
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT ⓘ  
[Evaluate](#)

Create Close

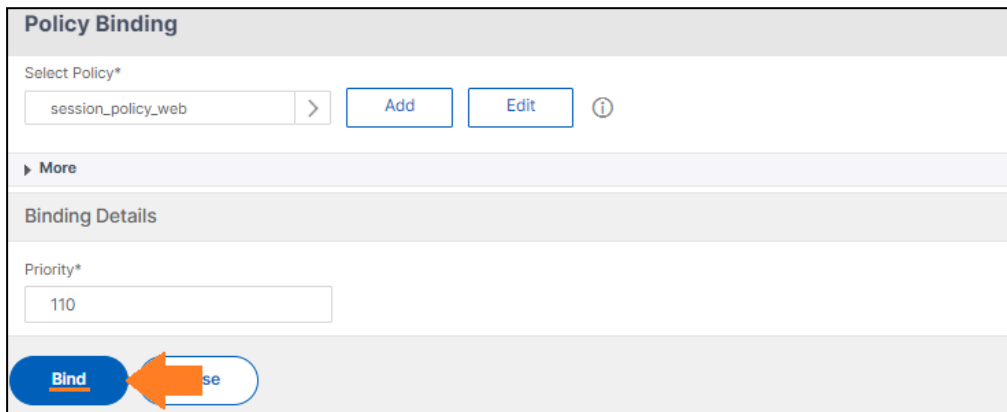
**NOTE:** This policy will be evaluated to **TRUE** if the NetScaler gets hit by a client using Chrome, IE, Edge, Firefox, Safari, etc. The **HTTP Header** from the **CLIENT** will **NOT** contain **CitrixReceiver** as the expression set, thus the policy will be evaluated.



24. Click **Bind**.

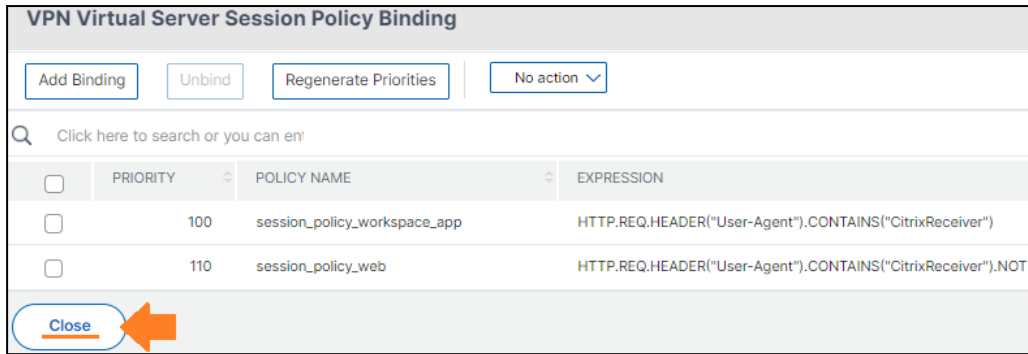


25. Click **Bind**.

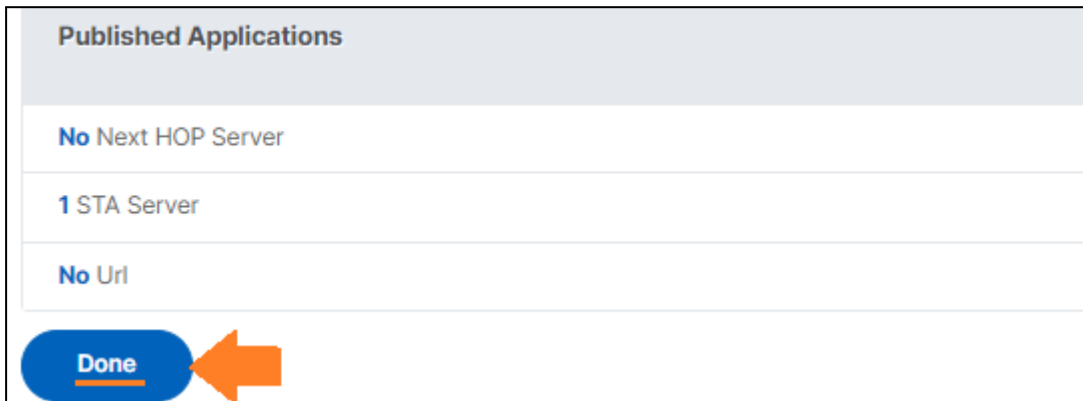


26. You should have 2 session policies bound. Click **Close**.

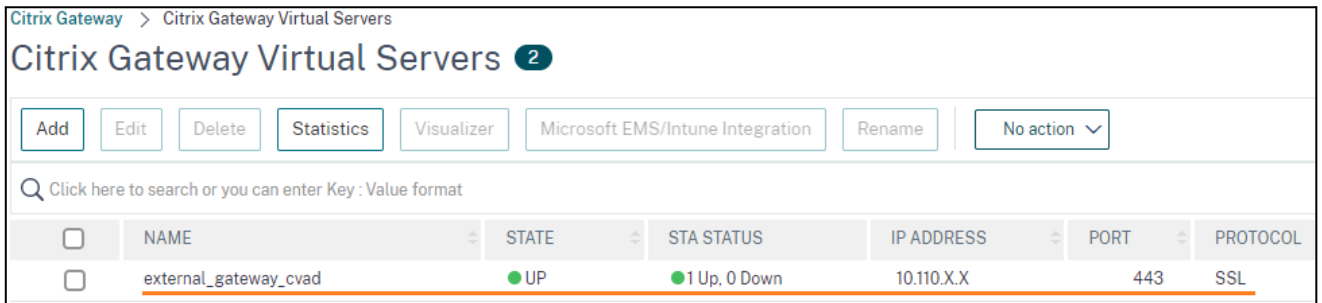




27. Click **Done**.

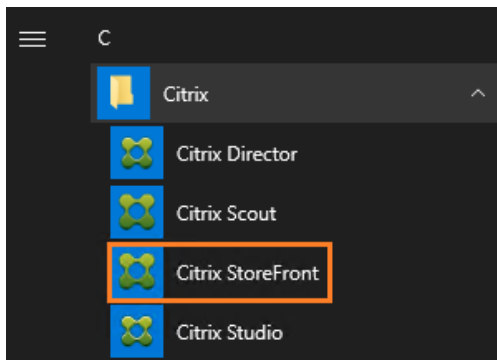


28. Your Gateway Vserver is configured and ready. Save the configuration.

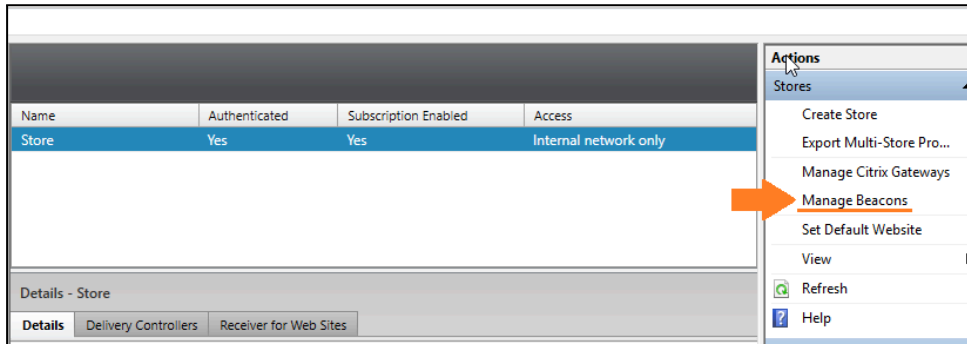


## Storefront Configuration for Gateway

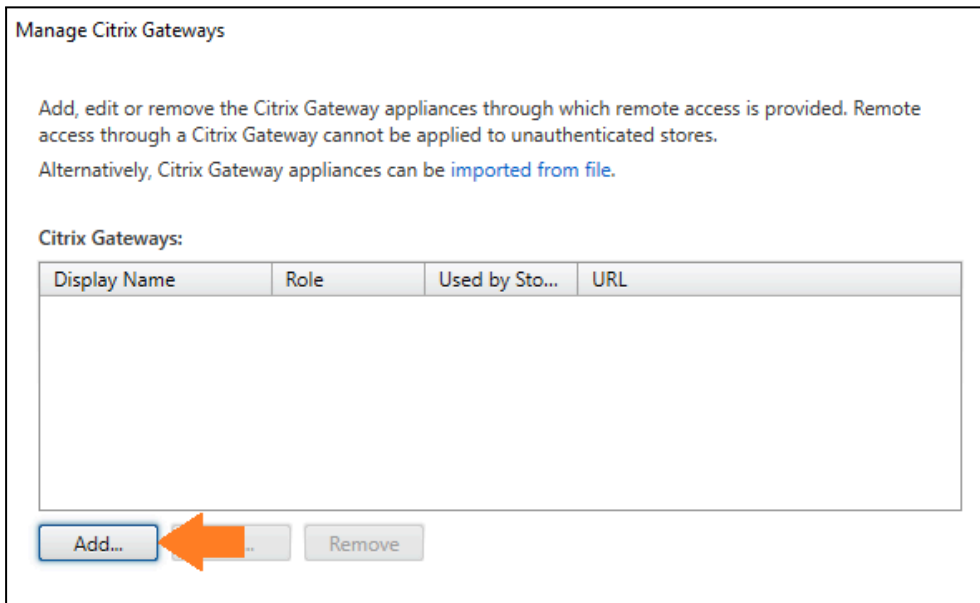
1. Open your Citrix Storefront console from your Windows Server DDC-SF.



2. Select your store and then click **Manage Citrix Gateway**.



3. Click **Add**.

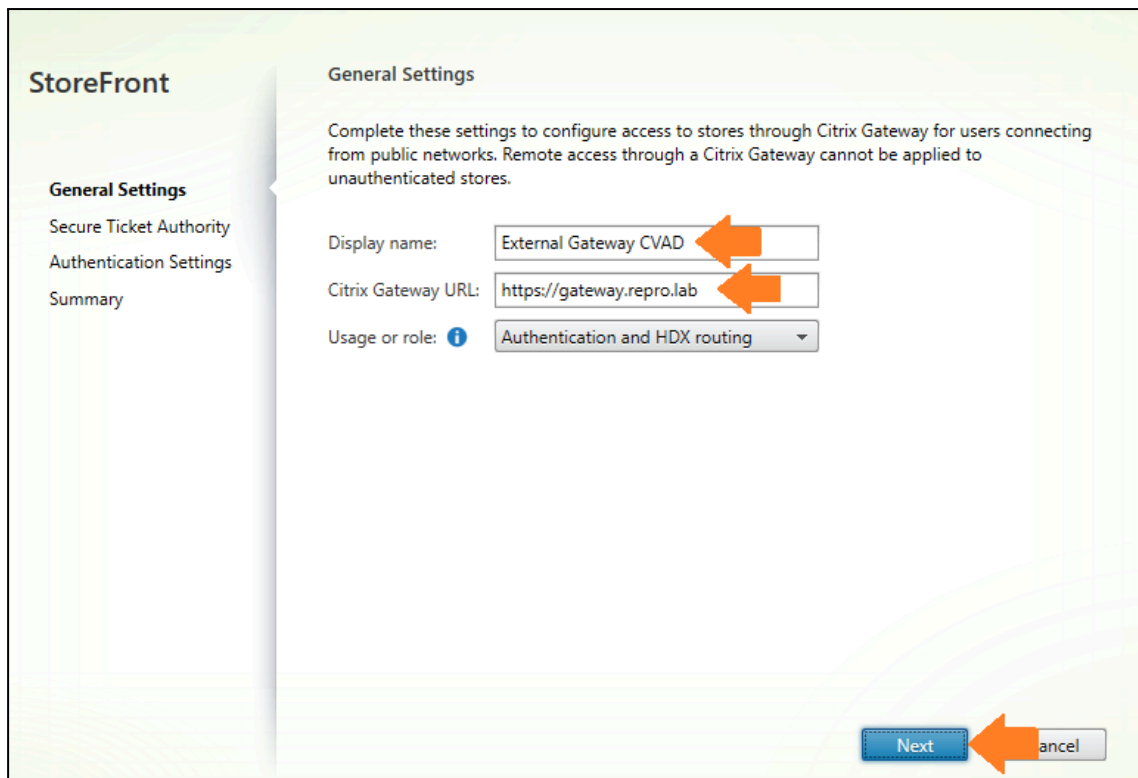


4. Enter **External Gateway CVAD** in the **Display name** input field.
5. Add the NetScaler Gateway URL **gateway.repro.lab** in the **Citrix Gateway URL** input field, which must be used on the browser to access the CVAD, and click **Next**.

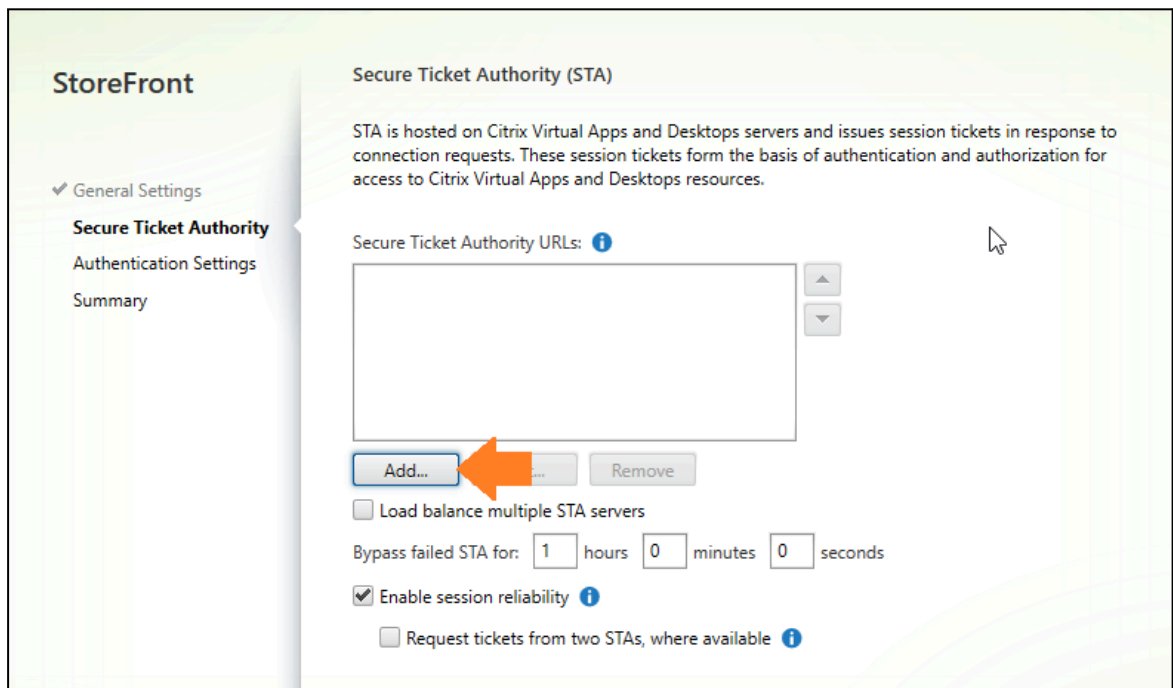
---

**NOTE:** Any misconfiguration may disrupt the integration. It is essential to consistently access CVAD via the Gateway using the identical Gateway URL configured.

---



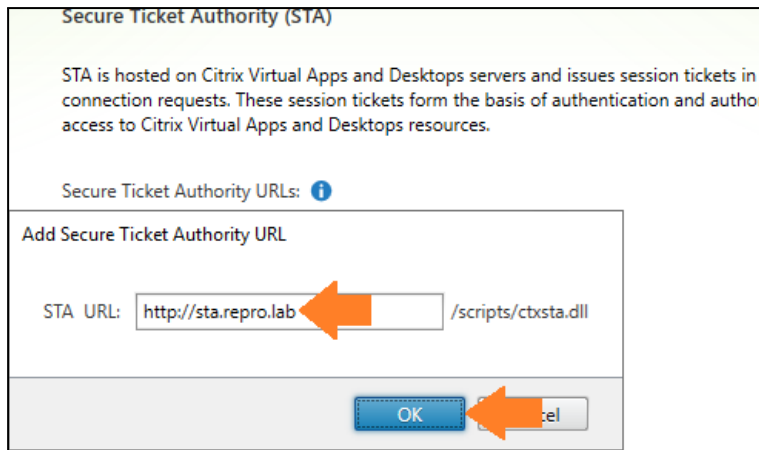
6. Click Add to add your **STA(s)** server(s).



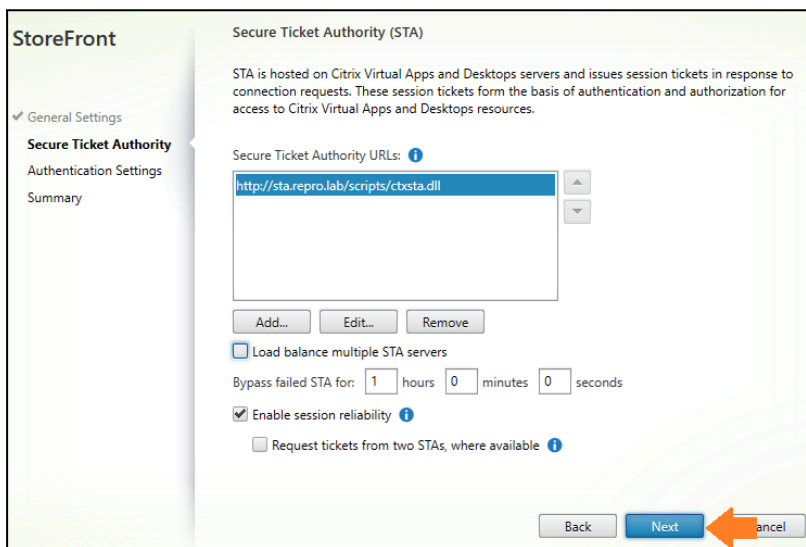
7. Add your **STA** as the below example and click **OK**. You can alternatively, use the STA Server IP (DDC IP). If using "**repro.lab**", you can set "**http://sta.repro.lab**".

**NOTE:** It is crucial to add all the STAs on the NetScaler that have been added to the SF. For instance, if **two** STA servers are added on the Storefront with "load balance multiple STA servers" enabled, and only **one**

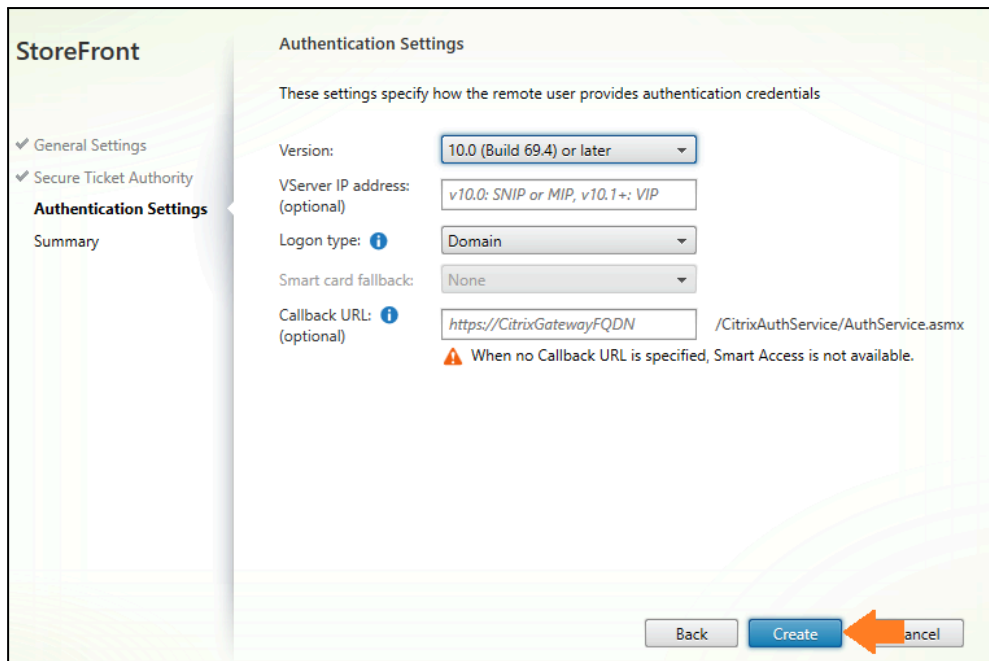
STA is added on the NetScaler, a launch failure may occur whenever the external ICA file contains the STA server not added on the NetScaler.



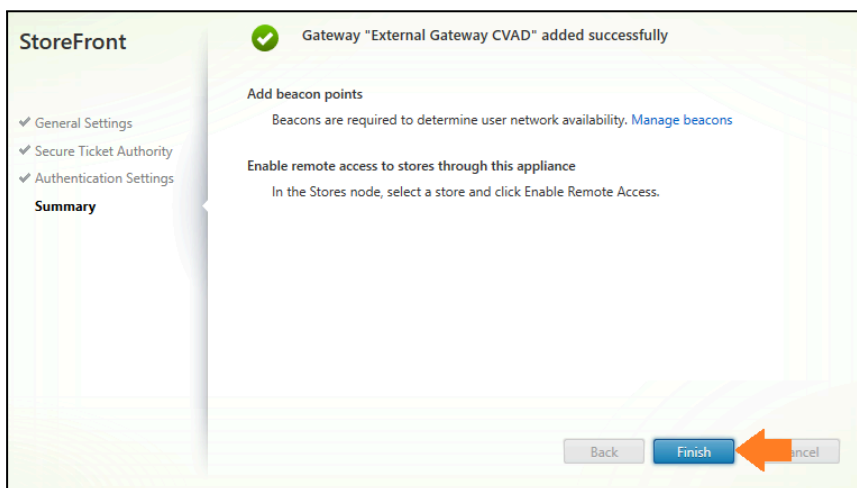
8. Click **Next**.



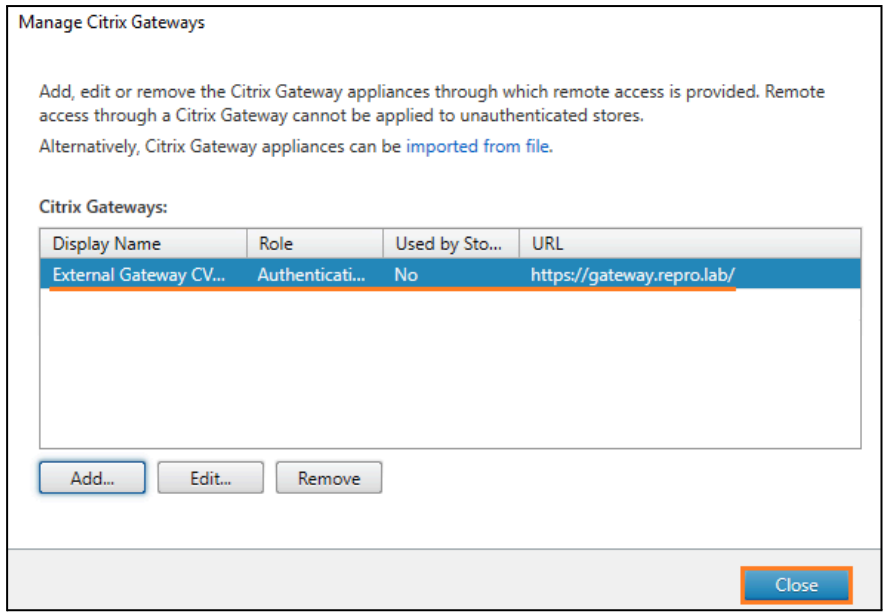
9. Click **Create**.



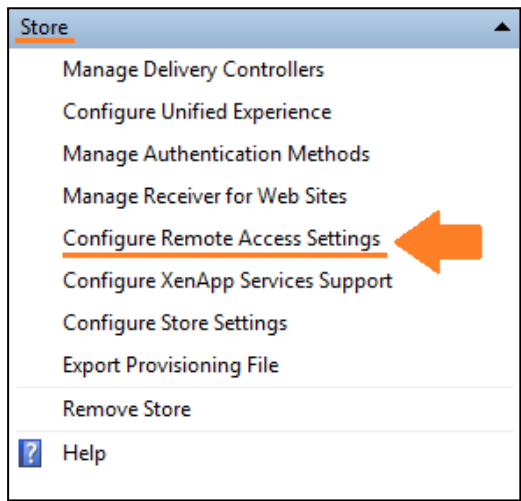
10. The external configuration is done. Click **Finish**.



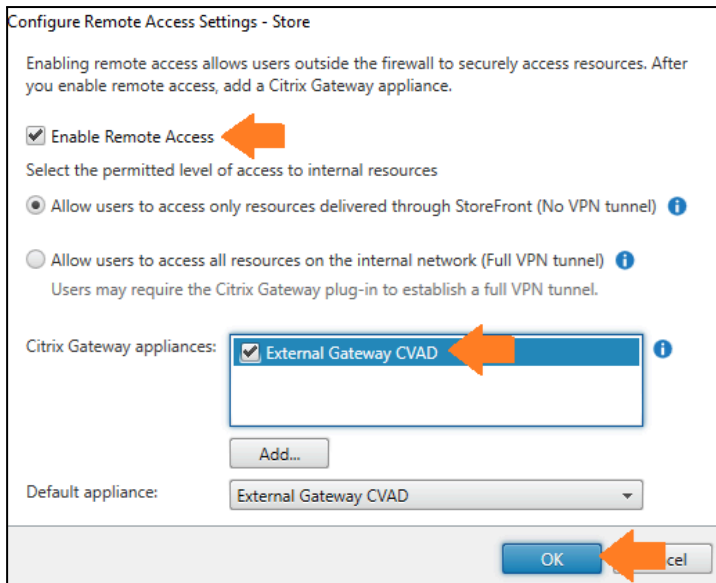
11. Click **Close**.



12. Click **Configure Remote Access Settings** under Store.

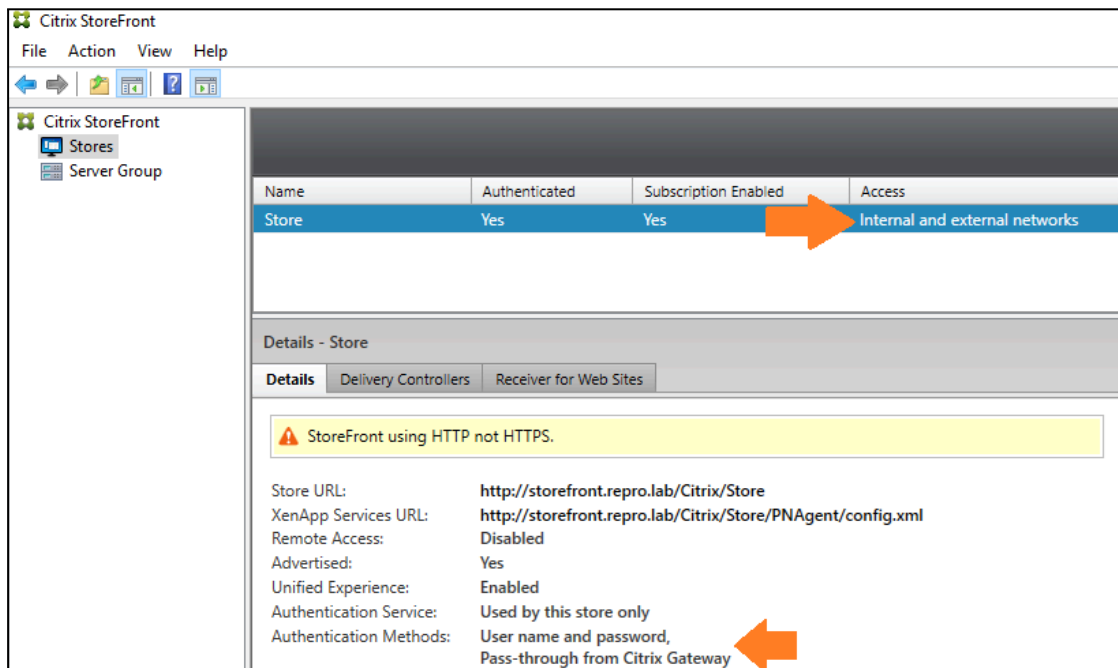


13. Enable the Gateway you just configured.



**NOTE:** In cases where multiple Gateways are configured on the Storefront, it is essential to ensure that the "default Appliance" aligns with the FQDN used by CWA for connection. For example, if CWA connects using "lab.com" but the default appliance gateway configuration is set to "repro.com," the CWA connection will fail.

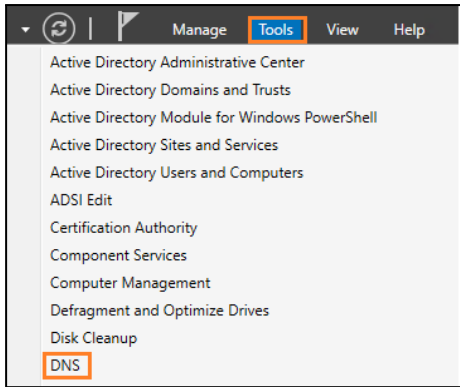
14. Storefront Gateway configuration is done.



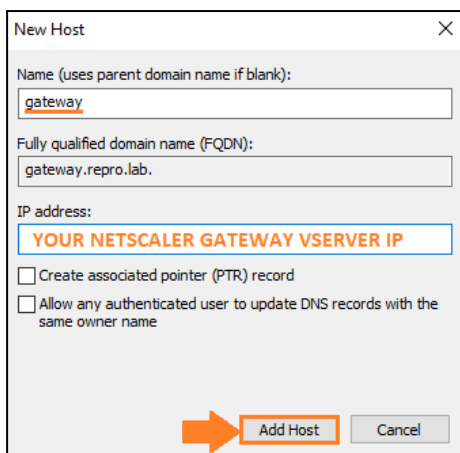
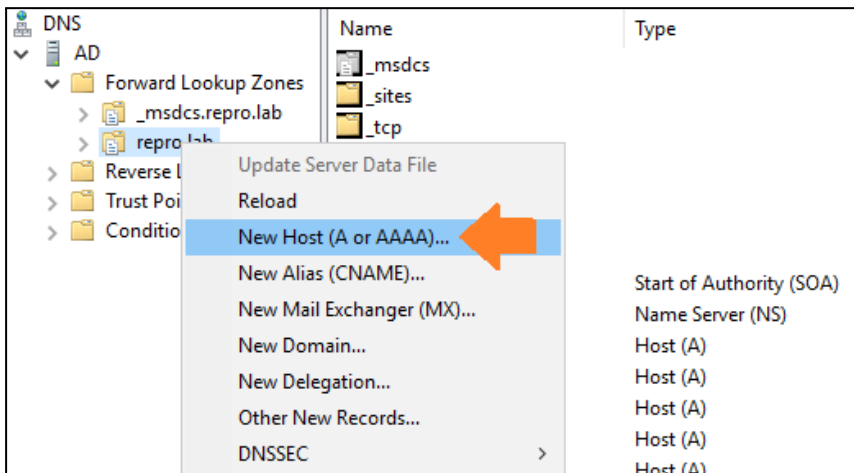
## Testing Authentication, Enumeration, Launch, and Session Via Web Browser

**NOTE:** Your Windows 10 Client VM must have the **internal Root CA** for the Certificate you have configured on your NetScaler Gateway Vserver. When you enter the URL **https://gateway.repro.lab** you **should not** see any SSL warning/errors.

1. From your **Windows Server AD**, open your internal Windows DNS server. **Tools > DNS**.



2. Navigate to **AD > Forward Lookup Zones > repro.lab**.
3. Right-click **repro.lab** and then select **New Host (A or AAAA)....**
4. Add a host entry for your **Gateway**. You need to specify your **host + NetScaler Gateway Vserver**. In your case, we will use **gateway.repro.lab** to refer to the NetScaler Gateway setup.



5. From your **Windows 10 Jumbox VM**, ensure you can resolve the Gateway URL properly.
6. Open your browser and type <https://gateway.repro.lab>.

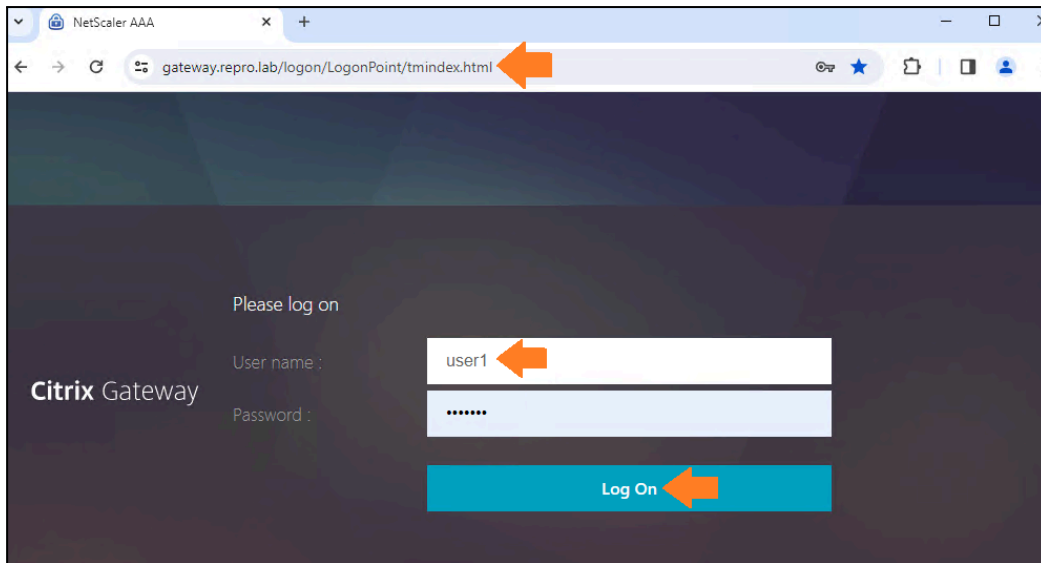
---

**NOTE:** Please do not try with the Gateway IP, FQDN is a must to avoid SSO issues.

---

7. Enter your LDAP credentials (username and password).



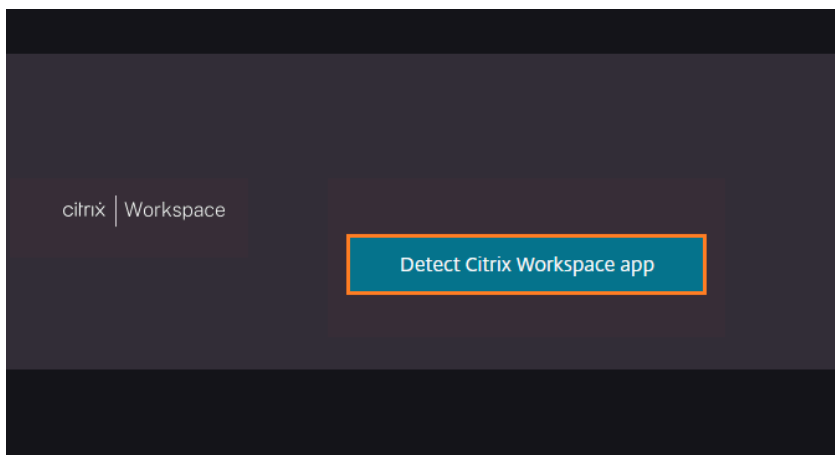


**NOTE:** If you encounter a "Cannot complete your request" error at this stage, please refer to these [troubleshooting steps](#). Many issues observed during this phase are typically attributed to misconfigurations in the **Session profile**, where the NetScaler struggles to resolve the Storefront address.

You can monitor the LDAP authentication in real-time through the NetScaler using the **"/tmp/aaad.debug"** tool as below. For more: [CTX114999](#).

```
> shell
root@netscaler01# cat /tmp/aaad.debug
Fri Jan 26 09:13:09 2024
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[828]: main 0-0: timer
ng...
Fri Jan 26 09:13:10 2024
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[1181]: process_kernel
0-8: partition id is 0
Fri Jan 26 09:13:10 2024
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[1037]: is_valid_auth
req 0-8: received authenticate request: with member details userlen [6],
drlen [13], server_addrlen [0]
Fri Jan 26 09:13:10 2024
```

8. Click **Detect Citrix Workspace app**.



You can monitor real-time the policy hits through the NetScaler at the time you are logging on. As you can see below, there are some cache policy hits (policies that are bound globally by

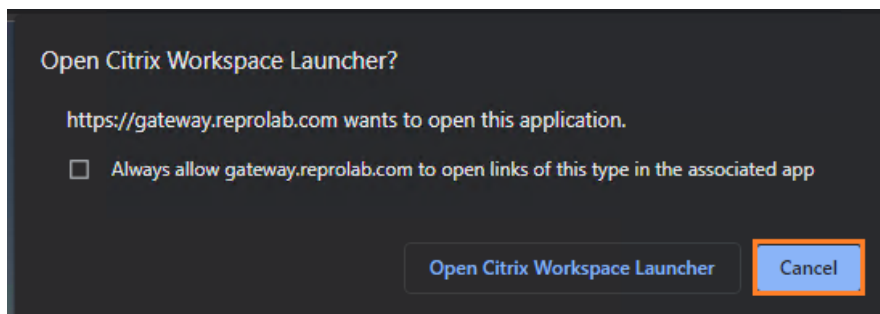
default) + the LDAP policy followed by the Session policy Web.

**command:** nsconmsg -d current -g pcp\_hits

```
root@netscaler01# nsconmsg -d current -g pcp_hits
Displaying performance information
NetScaler V20 Performance Data
NetScaler NS14.1: Build 12.30.nc, Date: Nov 22 2023, 10:23:35 (64-bit)

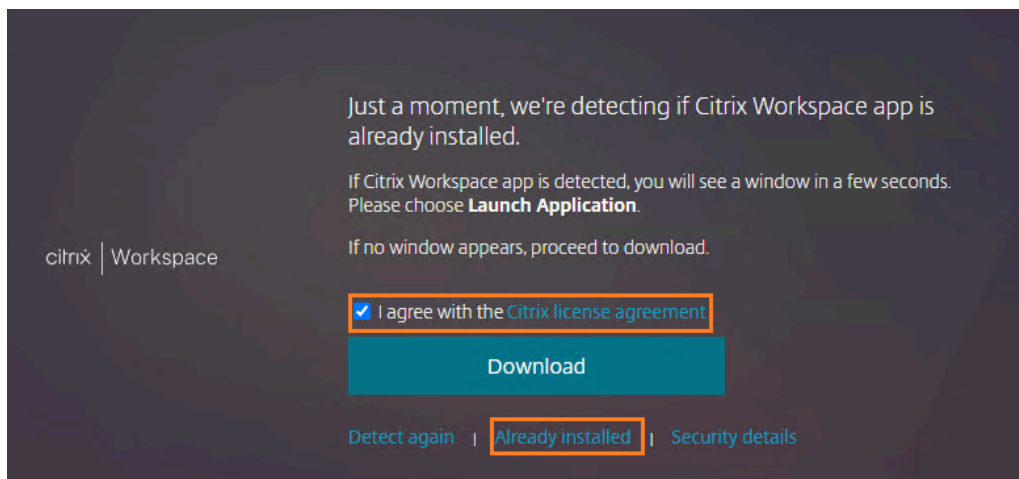
reltime: milliseconds between two records Fri Jan 26 09:16:34 2024
Index  rtime totalcount-val  delta  rate/sec  symbol-name&device-no
  0     7011          307    12      1  pcp_hits rewrite(policy_remove_server_header)
  1      0           121    12      1  pcp_hits cache(_mayNoCacheReq)
  2      0           105     7      0  pcp_hits cache(_noCacheRest)
  3      0           103     1      0  pcp_hits authn(ldap_advanced_policy)
  4      0            12     1      0  pcp_hits vpnsession(session_policy_web)
```

9. Click **Cancel**.

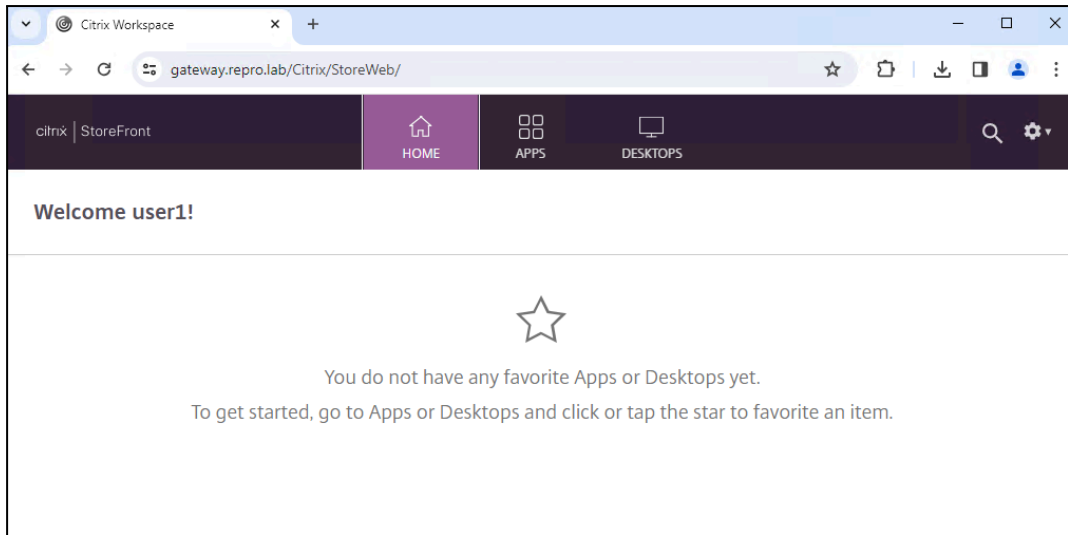


10. Click the **I agree with the Citrix License agreement** check box to select it.

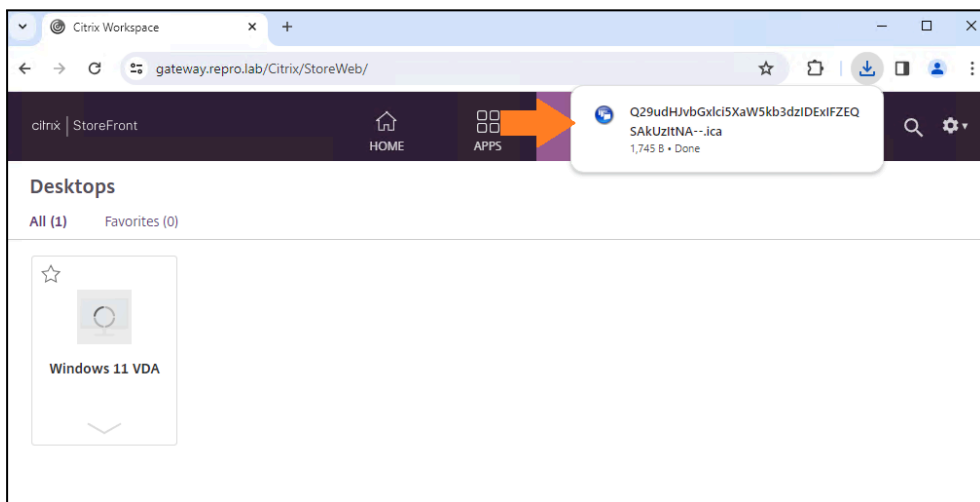
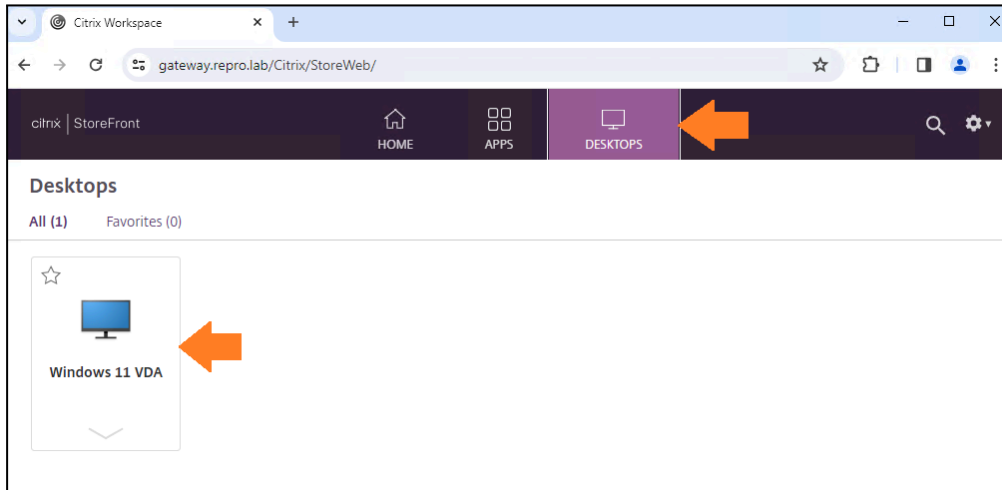
11. If you already have the Citrix Workspace App installed, click **Already installed**, otherwise, click **download** and **install** the **CWA**.



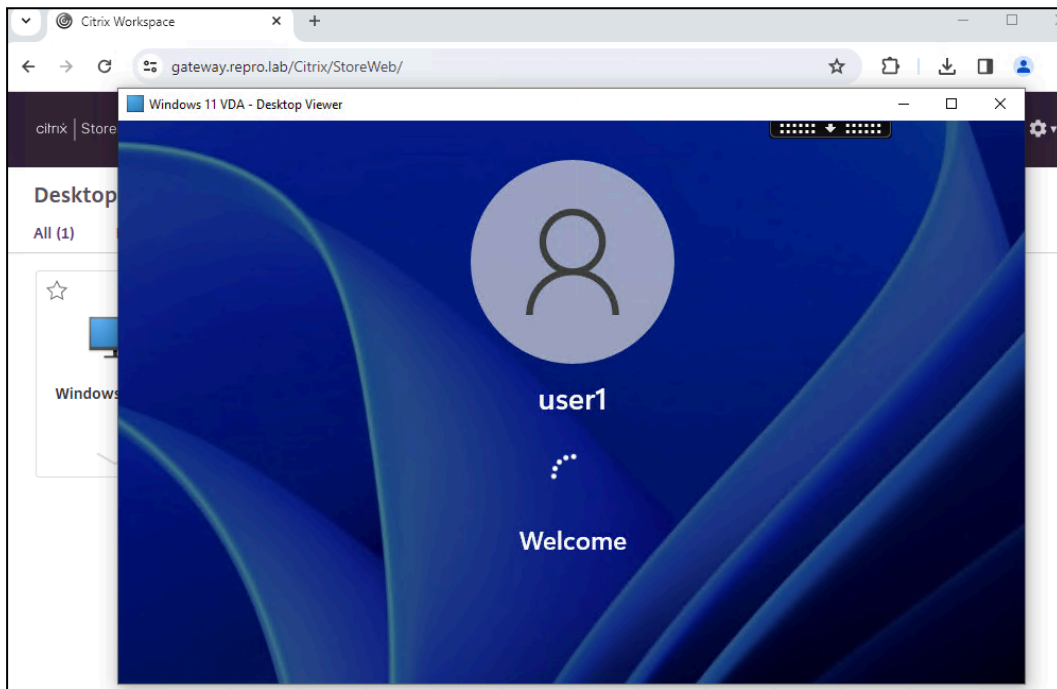
12. The Storefront home page should appear as below. **Resource enumeration** passed.



13. Click the **Desktops** tab and click your Windows VDA to launch it.
14. As soon as the ICA file is downloaded, click launch. **Resource Launch** passed.

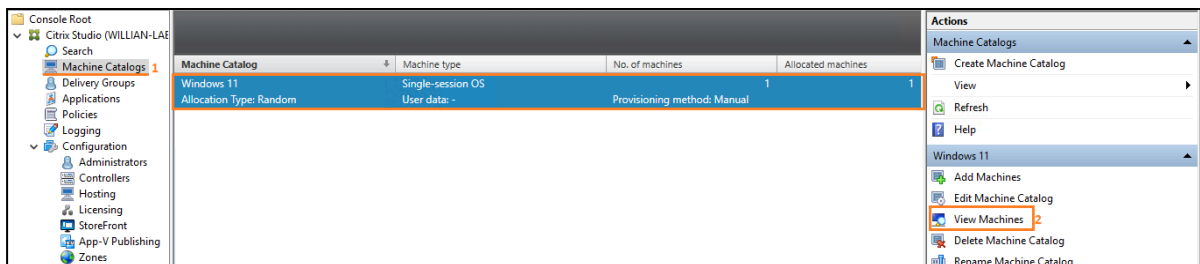


VDA is connecting.

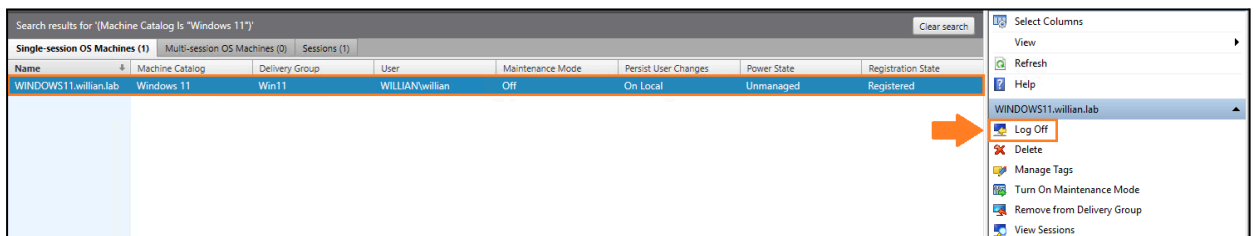


**NOTE:** If you see the error **“Cannot start the desktop”**, please log off the VDA Win 11 from the DDC as the next two images.

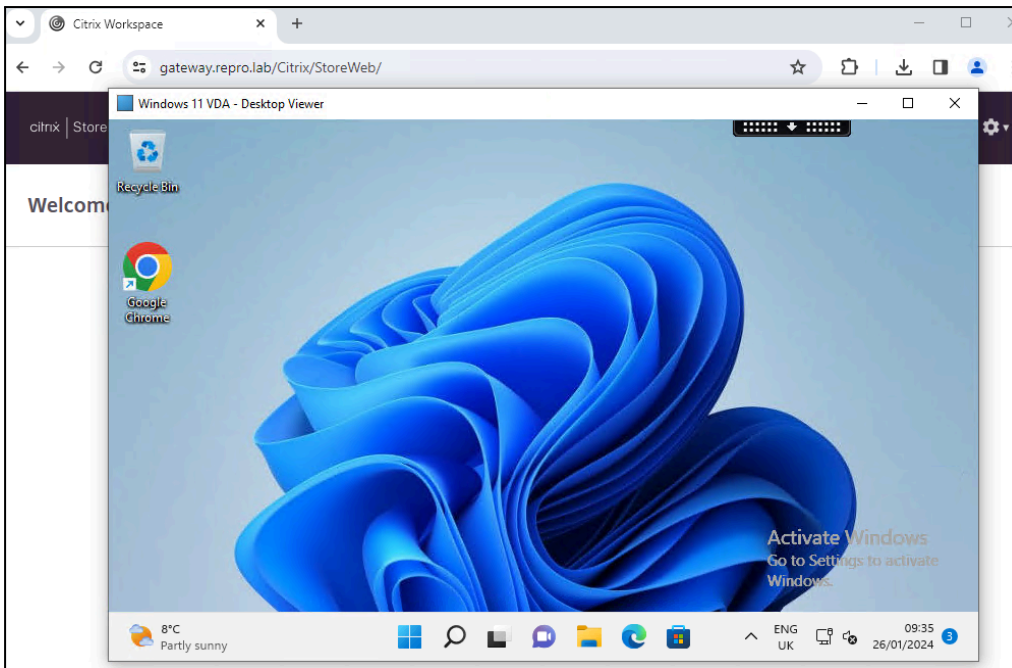
On **DDC-SF VM**, go to **“Machine Catalogs”** and click **“View Machines”**.



Click over the VDA and you will probably see a **“log off”** icon on the right side. **Just click “log Off”** and wait a minute. Refresh the page and confirm you do not see the “log off” icon anymore. Try to launch the VDA now.



**Session Initialization** passed.

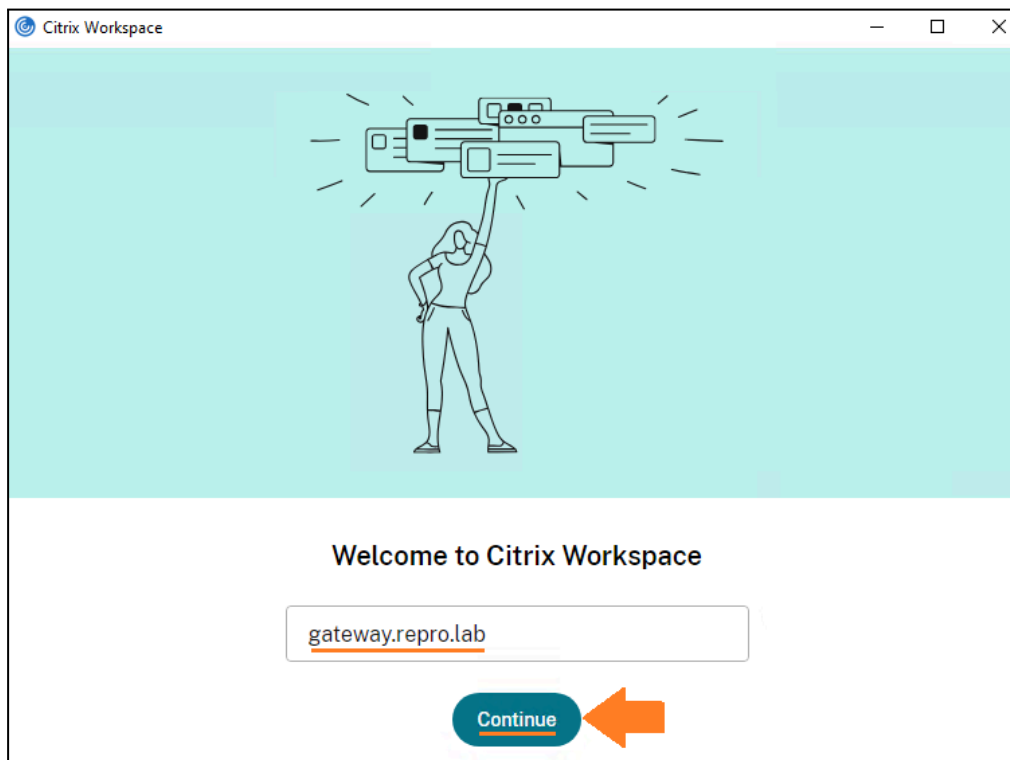


For the entire communication Workflow explained via Wireshark, check the [CTX227054](#)

## Testing Authentication, Enumeration, Launch, and Session Via CWA

**NOTE:** Your launch session might fail through CWA if your Storefront is set to use HTTP. If you wish to configure HTTPS, please follow this CTX Article.

1. Open the CWA, type your Gateway URL gateway.repro.lab, and click Continue.

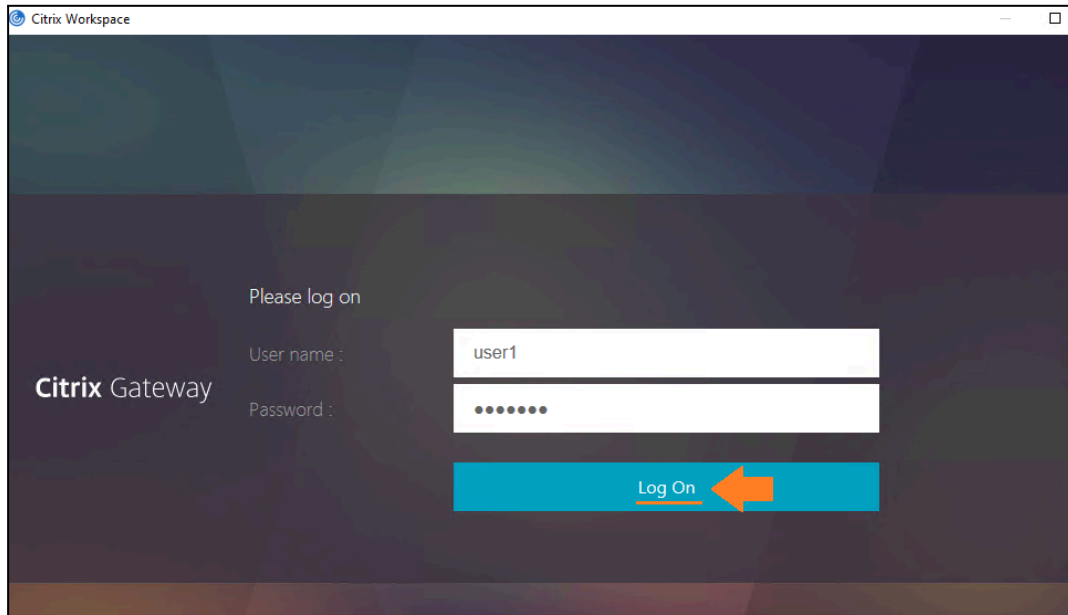


---

**NOTE:** During this test, ensure that the client machine **cannot** reach the **internal Storefront Base URL** (beacon). If the client machine has access to it, Citrix Workspace App (CWA) will **bypass** the NetScaler after authentication and attempt a direct connection to the Storefront to establish the ICA connection.

---

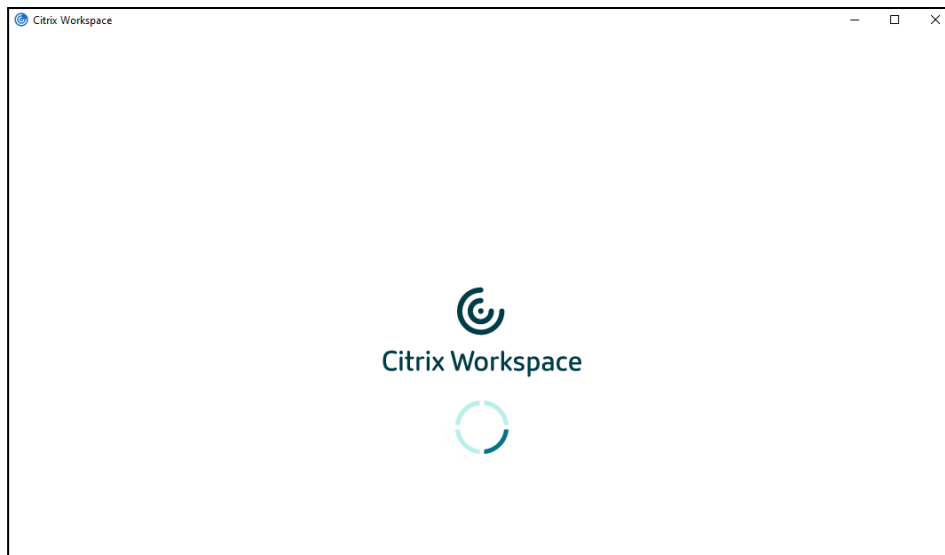
2. If you see a **Security Alert**, click **Yes**.
3. The **Webview** authentication page of the NetScaler Gateway will show. Insert your **LDAP credentials**.



---

**NOTE:** This **WebView** only appears when using **ADVANCED authentication**. If you see a standard pop-up for credentials, it indicates that you are either over **CLASSIC authentication** or Storefront authentication itself.

---



You can also monitor the policies hit through the NetScaler. Now you will see the session policy for CWA is the one getting hits.

**command:** `nscnmsg -d current -g pcp_hits`

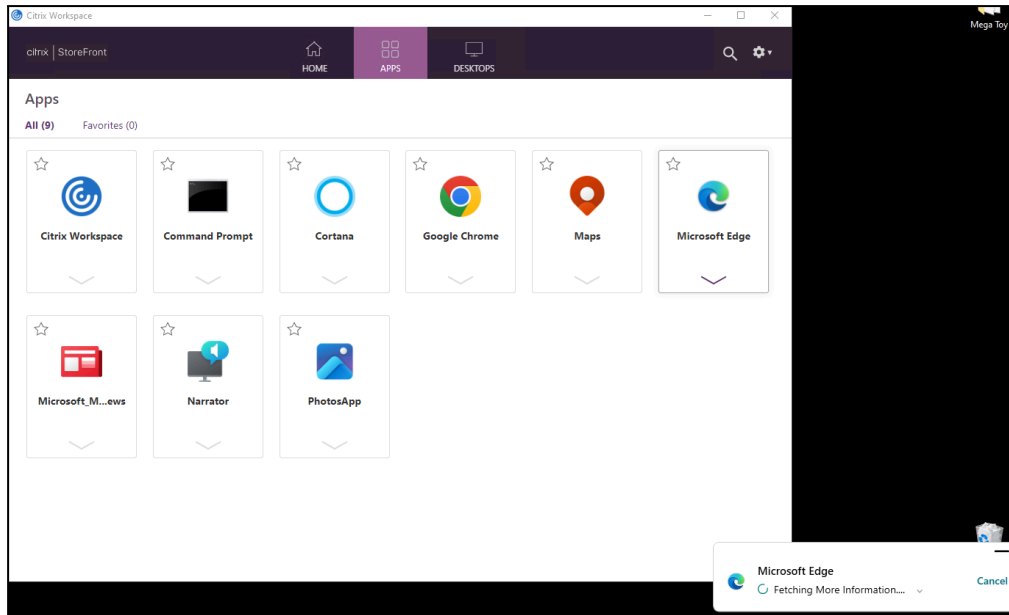
```

root@netscaler01# nsconmsg -d current -g pcp_hits
Displaying performance information
NetScaler V20 Performance Data
NetScaler NS14.1: Build 12.30.nc, Date: Nov 22 2023, 10:23:35 (64-bit)

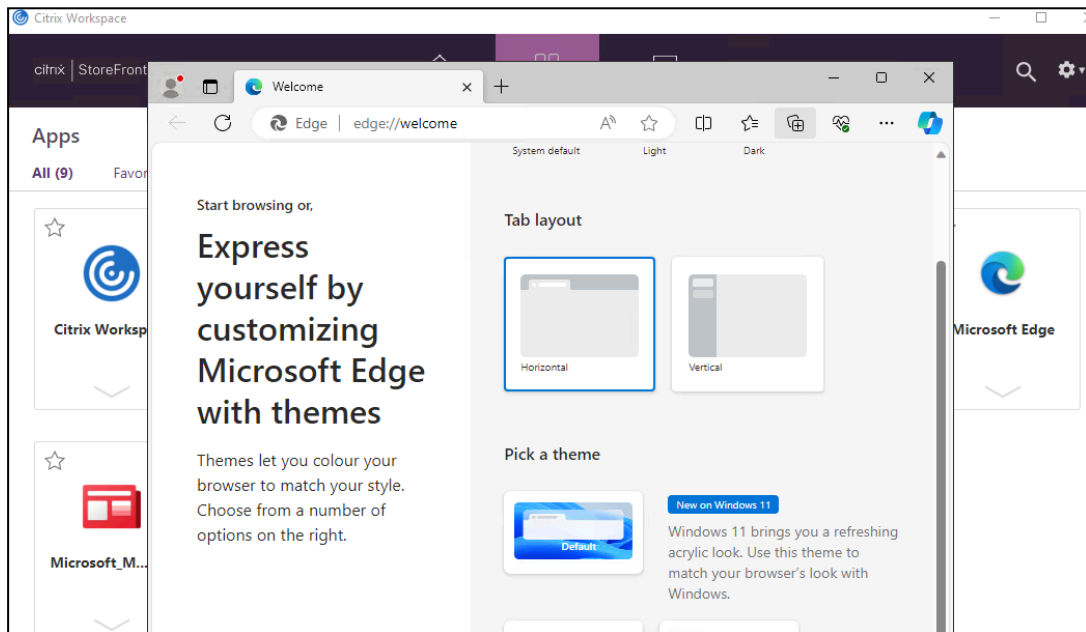
reltime: milliseconds between two records Fri Jan 26 09:36:33 2024
Index  rtime totalcount-val delta rate/sec symbol-name&device-no
0      7011      307      26      1 pcp_hits rewrite(policy_remove_server_header)
1      0         121      24      1 pcp_hits cache(_mayNoCacheReq)
2      0         105      5       0 pcp_hits cache(_noCacheRest)
3      0         103      2       0 pcp_hits authn(ldap_advanced_policy)
4      0          12      2       0 pcp_hits vpnsession(session_policy_workspace_app)

```

4. Click “Apps” or “Desktop” and click to launch.



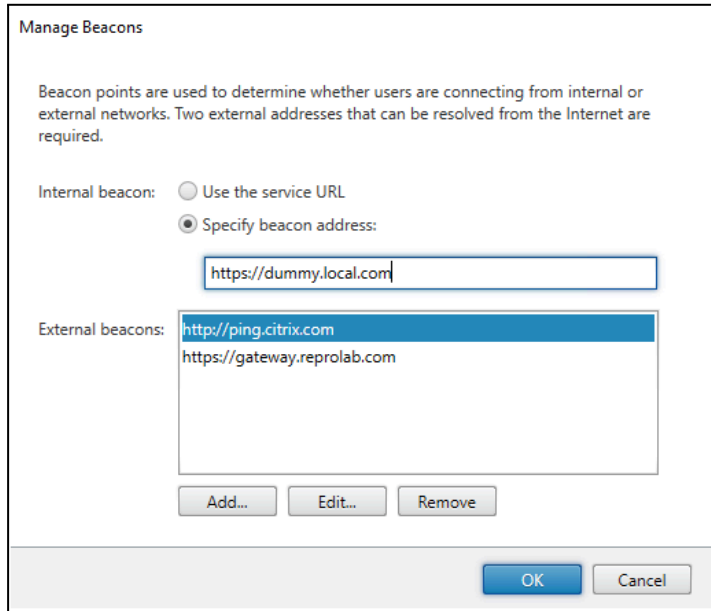
The application has been launched successfully.



**NOTE:** If you are prompted to authenticate twice using CWA, it means your Storefront is being reached directly, which is not expected (when NetScaler Gateway is in place). For example, if the internal beacon point (FQDN) is accessible, this indicates that the user is connected to the local network. However, if the

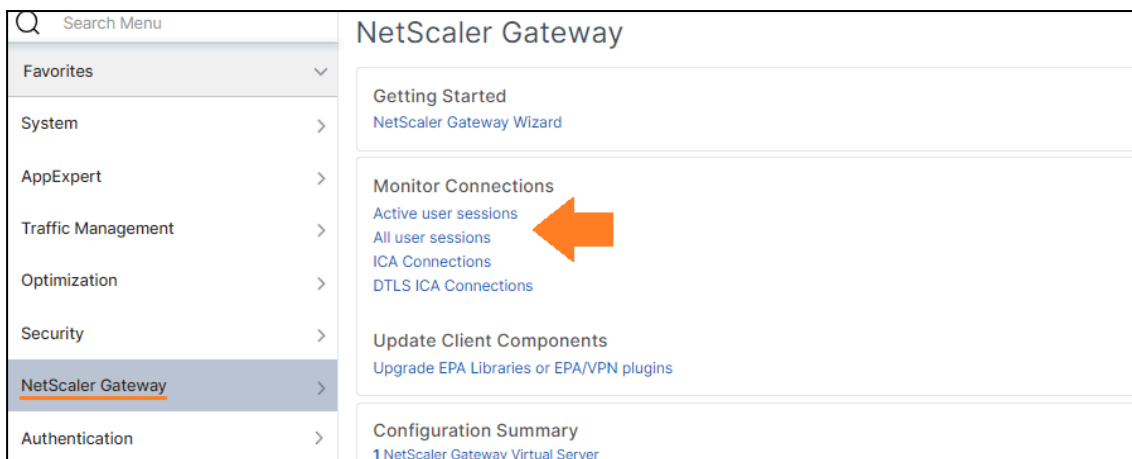
Citrix Workspace app cannot contact the internal beacon point and receives responses from **both the external beacon points**, this means that the user has an Internet connection but is outside the corporate network. Therefore, the user must connect through the NetScaler Gateway.

You can play with beacons to ensure the local VM will not be able to reach the internal base URL. To play with the internal beacon, under **Manager Beacons on your Storefront Server**, add a **dummy URL for "Internal beacon"** (example: dummy.local.com). **Reset** your CWA and test it again.



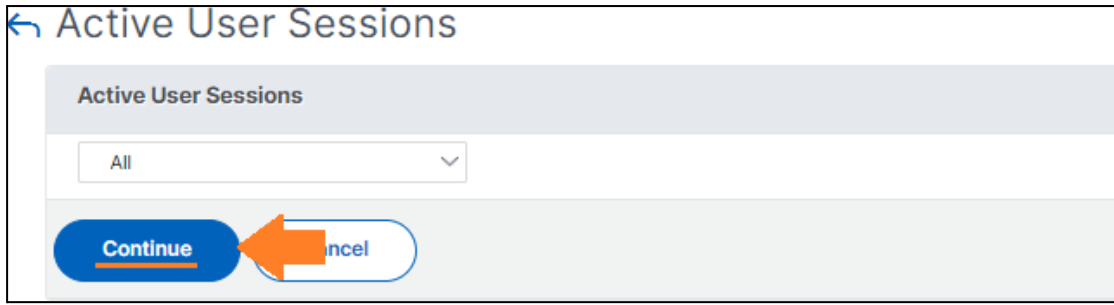
## Monitoring ICA sessions Via NetScaler GUI

1. Navigate to **NetScaler Gateway**.
2. Under **Monitor Connections**, click **Active user sessions** to see all the Sessions and ICA connections towards the VDA.

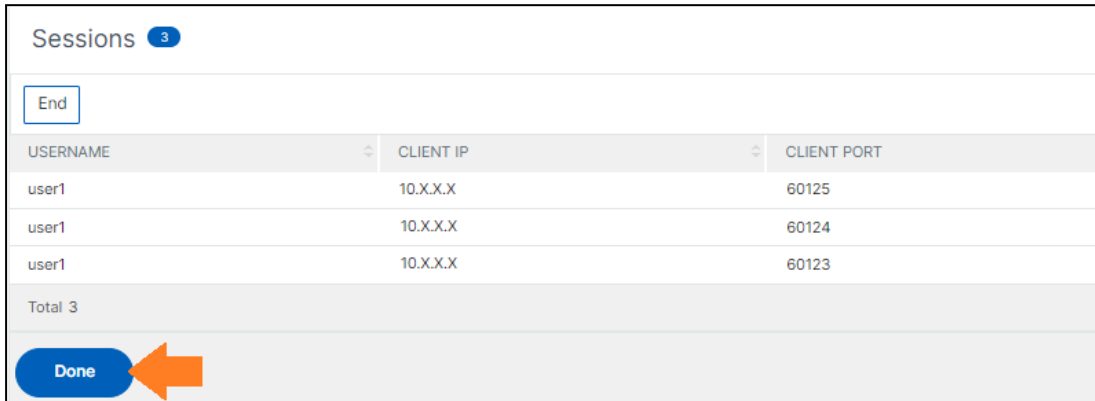


3. Click **Continue**.

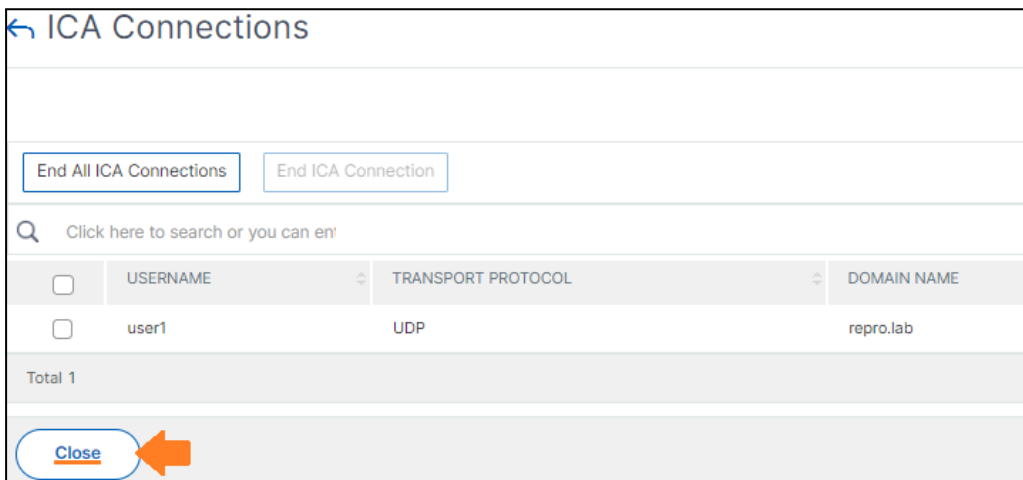




You can see the username, client IP + Port, and Gateway Vserver IP + port info.

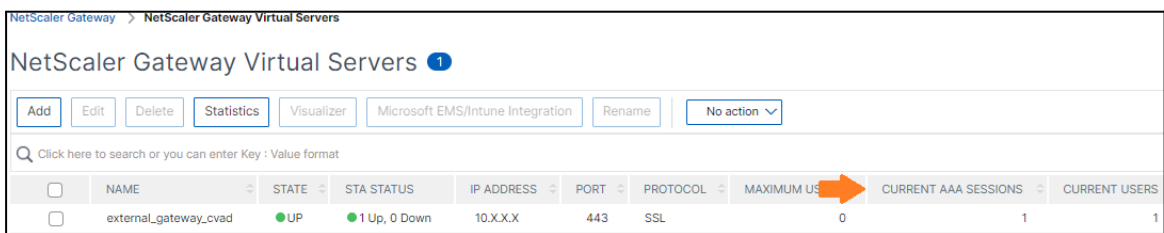


4. Click **ICA connections** to see the client and VDA information.



**NOTE:** It shows **Transport Protocol** as **UDP** because the **DTLS** option is set to **ON**. If you set it to **OFF**, you will see **TCP**.

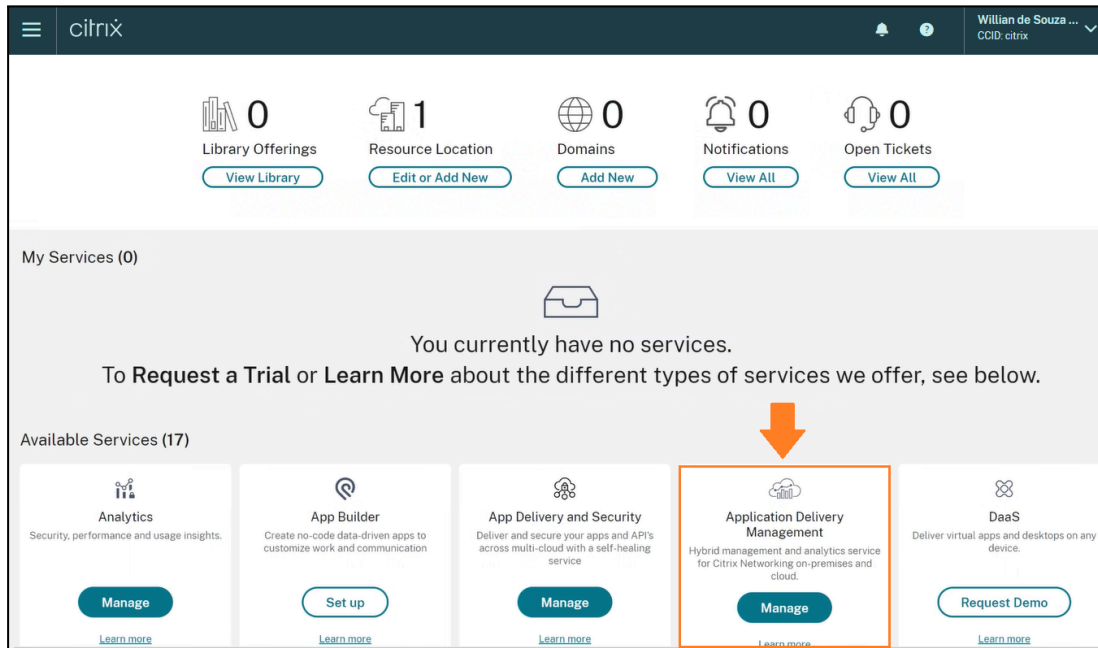
5. Navigate to **Citrix Gateway > Virtual Servers** to see the overall number of AAA sessions and current users.



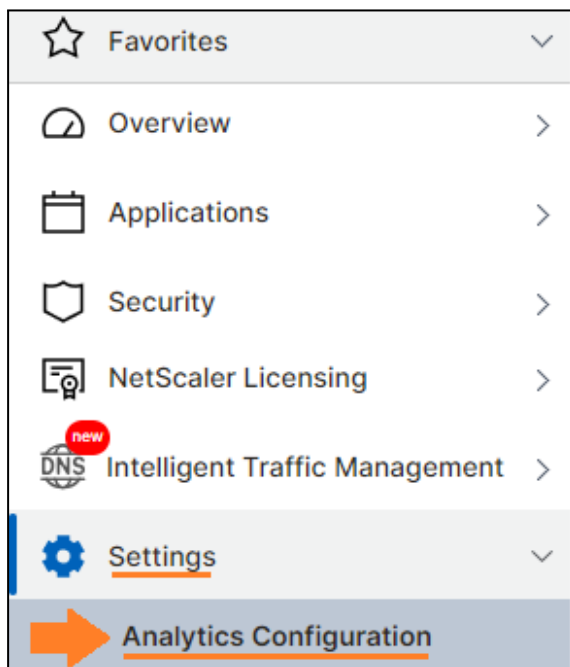
6. You can also kill the ICA/AAA sessions using CLI:  
kill icaconnection -all >> Kill ICA session  
kill aaa session -all >> Kill AAA session

# NetScaler Console HDX integration with NetScaler Gateway

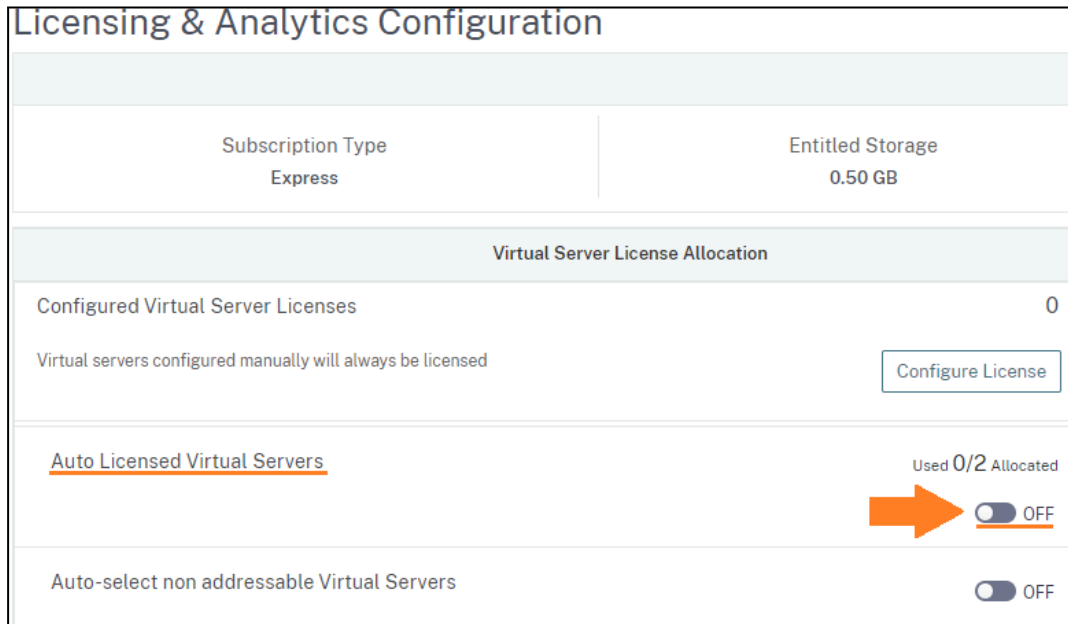
1. Navigate to <https://cloud.citrix.com/> and sign in with your credentials.
2. Select **Manage** on the **Application delivery management** widget.



3. From the menu on the left, navigate to **Settings** > **Licensing & Analytics Configuration**.

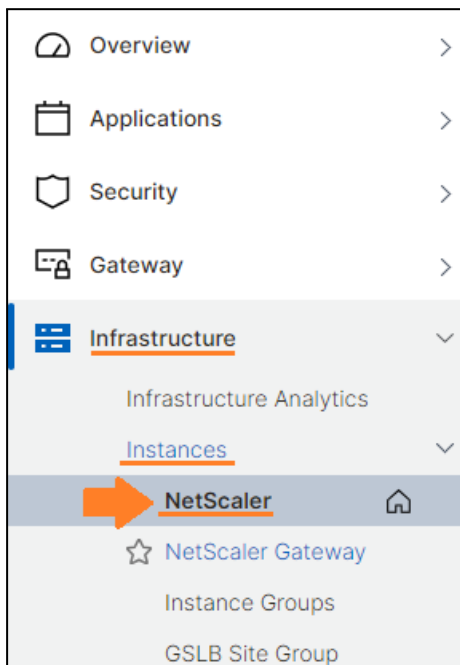


- Under the **Virtual Server License Allocation** section, toggle the **Auto Licensed Virtual Servers** ON/OFF button.

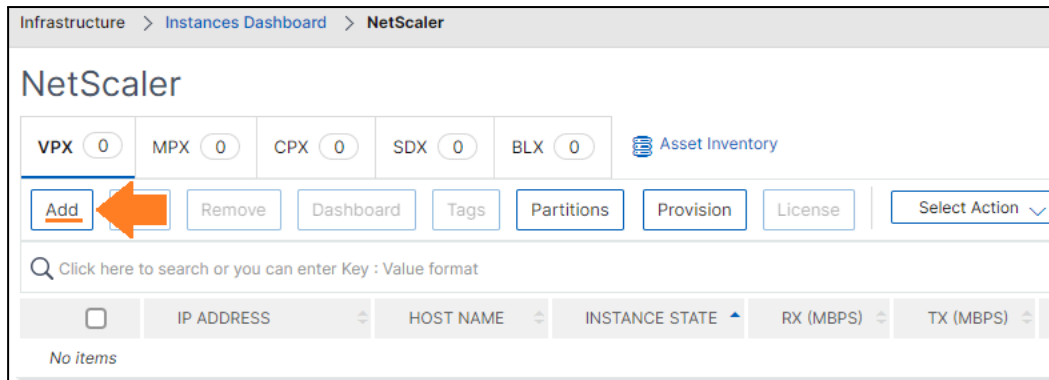


**NOTE:** For build **13.1-12.x or later**, you can manage **up to two** discovered applications or virtual servers and view analytics. Beyond the two discovered applications or the two virtual servers, the customer must buy and apply for an **Advanced license**. Disabling the **Auto Licensed Virtual Servers** will allow you which 2 Virtual servers from your NetScaler are going to be configured for management and analytics instead of leaving that to be automatically selected.

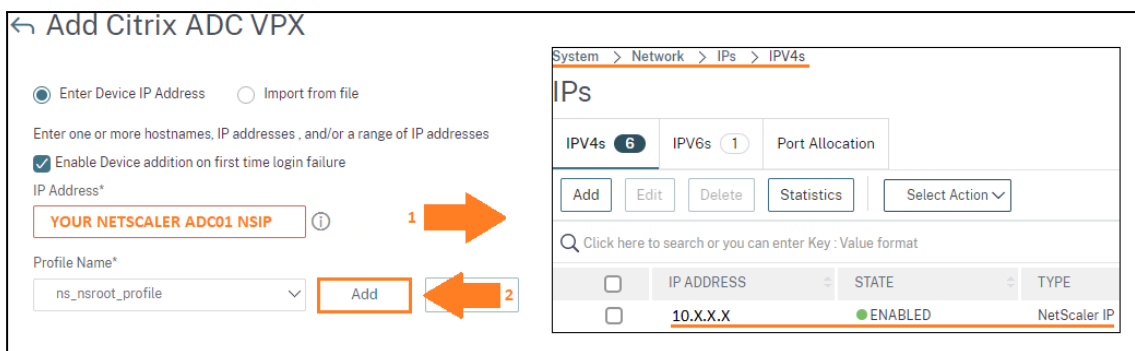
- Navigate to **Infrastructure > Instances > NetScaler**.



- Click **Add** to add your pair of NetScaler VPXs.



7. Enter your **NetScaler ADC01 NSIP** and click **Add** to add a new nsroot profile. This is needed because the ADM needs to have your nsroot/admin password. The default profile contains nsroot/nsroot credentials.



8. Enter the profile name "**new\_profile\_netscaler**", and enter "**nsroot**" as username and your **nsroot password**. Change the SNMP version to "**v2**" and add "**public**" as a community. Click **Create**.

---

**NOTE:** We will not cover SNMP messages.

---

### Create NetScaler Profile

Profile Name\*

Username\*

Password\*

SSH Port

HTTP Port

HTTPS Port

Use global settings for NetScaler communication

▼ SNMP

Version  
 v2  v3

SNMP v3 is more secure and recommended

Community\*

▼ Timeout Settings

Maximum waiting time to reboot NetScaler.

Timeout (in Seconds)

9. Under **Agent**, select **Click to select**.

**NOTE:** Your site will be populated automatically, if you wish, you can **“Edit”** it and change its name to **“Location site”** for example.

← Add NetScaler VPX

Enter Device IP Address     Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

Enable Device addition on first time login failure

IP Address\*

10.X.X.X ⓘ


Profile Name\*

new\_profile\_netscaler [Add] [Edit]

Site\*


Europe Site [Add] [Edit]

Agent\*

Click to select >  Please select value.

10. Select your **ADM agent** and click **"Select"**.

Agents 1

[Select]  [Details] [Delete] [Reboot] [Rediscover] [Attach Site]

Click here to search or you can enter Key : Value format

	IP ADDRESS	HOST NAME	VERSION	STATE
<input checked="" type="radio"/>	10.x.x.x <sup>LSA</sup>	adm-agent.repro.lab	13.1-43.28	Up

11. Confirm all the fields are filled in and click **"OK"**.

**NOTE:** If your agent is not listed, go back to the previous page, and switch the **"SITE"** to the other option available. Then, attempt to find your agent again.

Enter Device IP Address     Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

Enable Device addition on first time login failure

IP Address\*

10.X.X.X ⓘ

Profile Name\*

new\_profile\_netscaler [Add] [Edit]

Site\*


Europe Site [Add] [Edit]

Agent\*

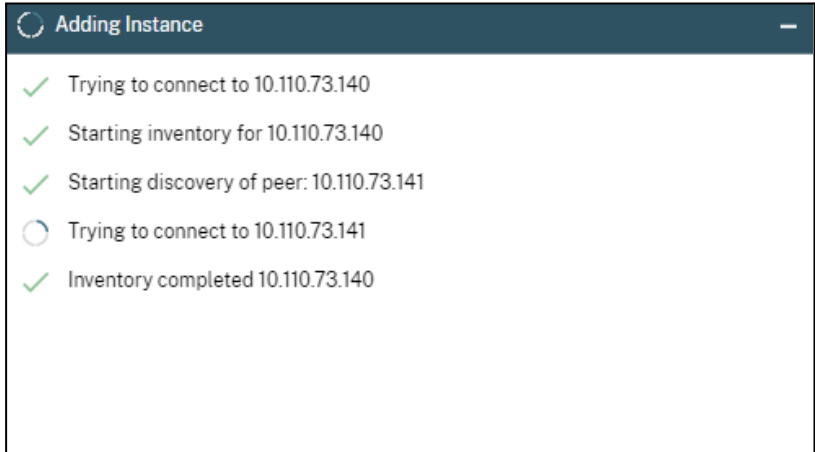
ADM-AGENT >

Tags

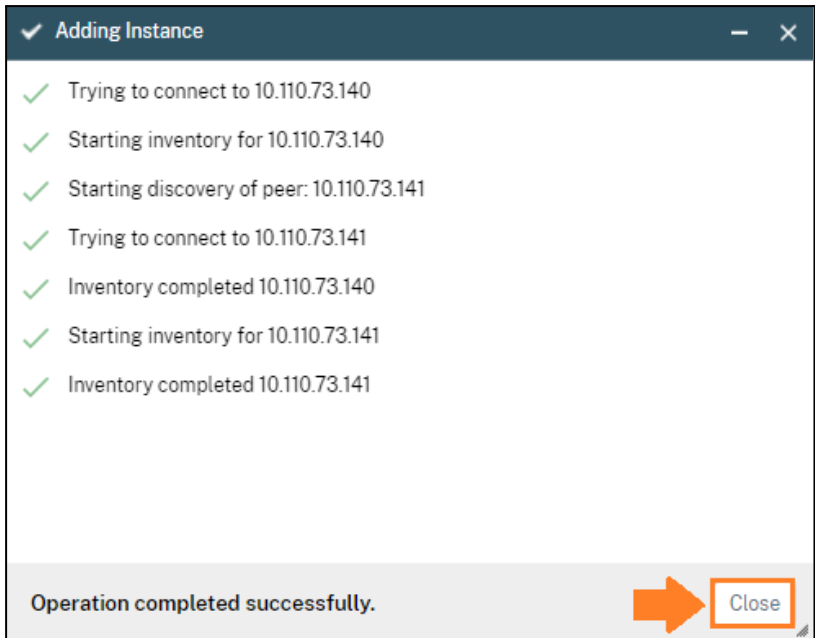
Key Value +

[OK]  [Close]

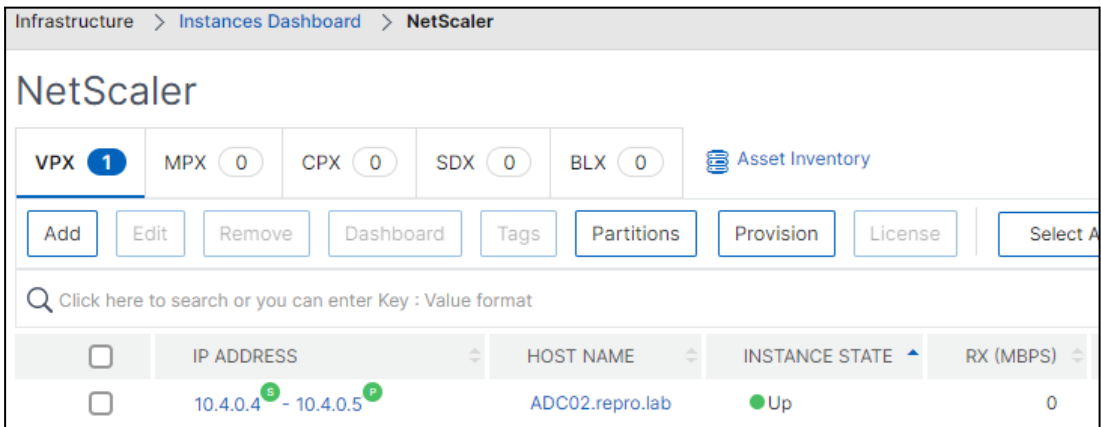
12. As you added your **ADC01** Primary, the NetScaler Console service will start the inventory and discover the **ADC02** Secondary as well. Wait for a few seconds.



13. Click **Close**.

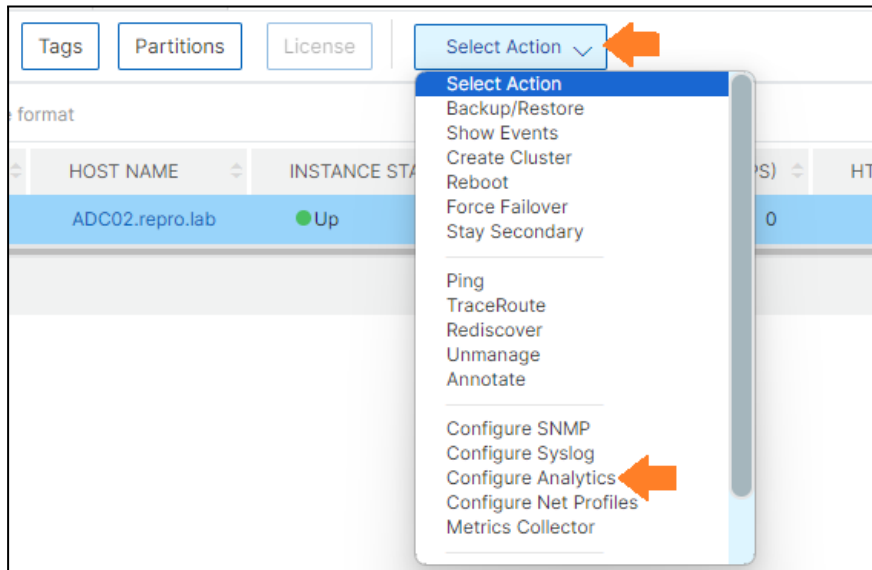


14. Your NetScaler VPXs **ADC01** and **ADC02** are added.

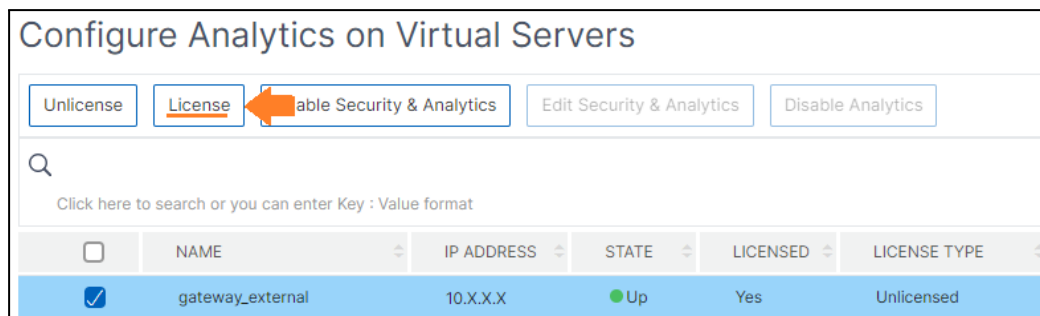




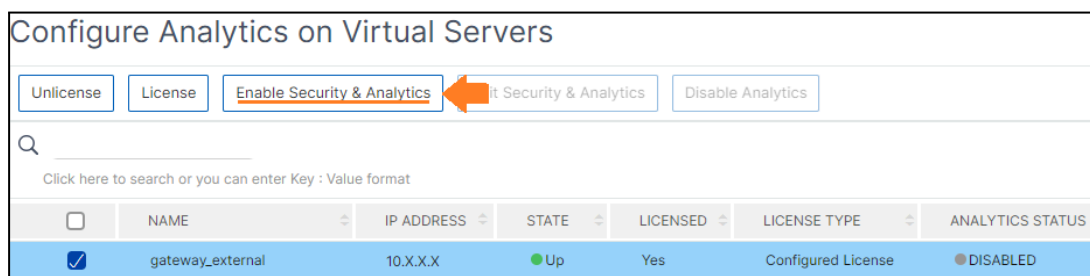
15. To enable the **Analytics** on your NetScaler Gateway, select your pair of the NetScaler and click **Select Action** and **Configure Analytics**.



16. Select your NetScaler gateway VIP **external\_gateway\_cvad** and click **License**.

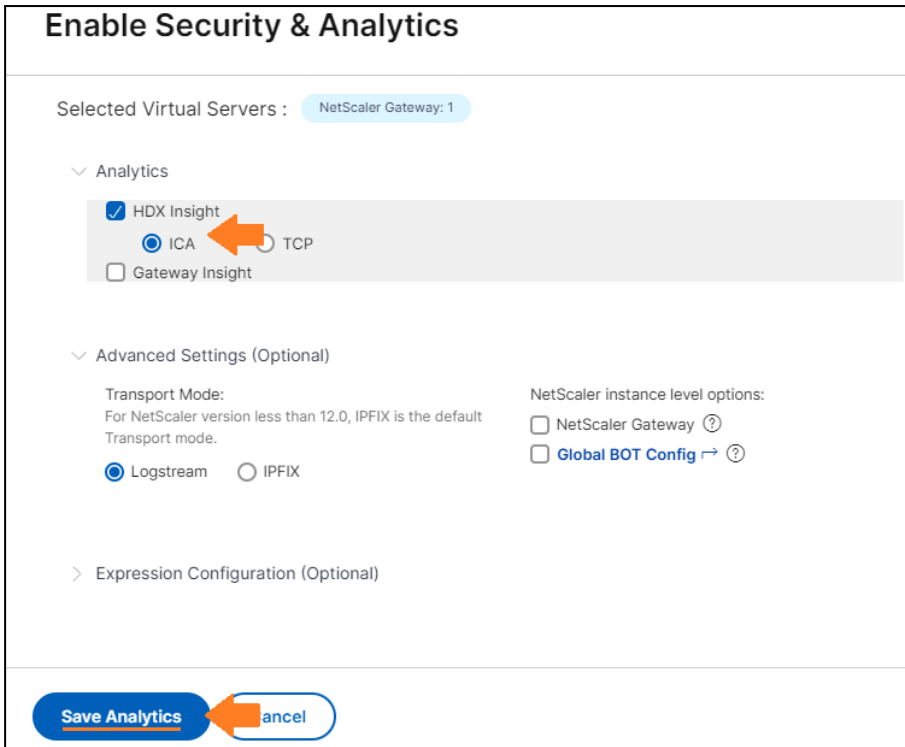


17. Select again your Gateway VIP **external\_gateway\_cvad** and click **Enable Security & Analytics**.

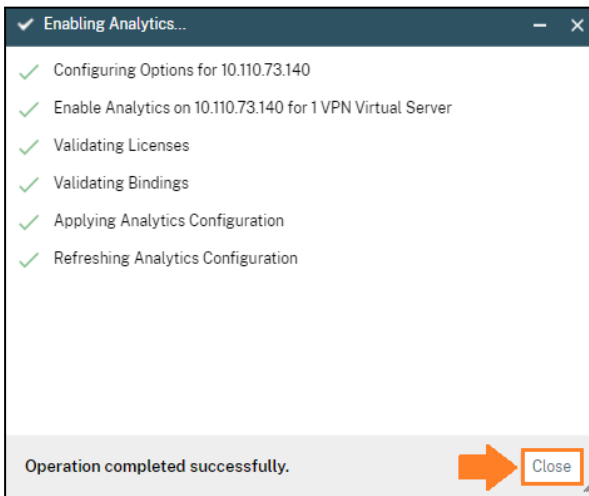


18. Enable **HDX Insight** and ICA. For transport mode, select **Logstream**.

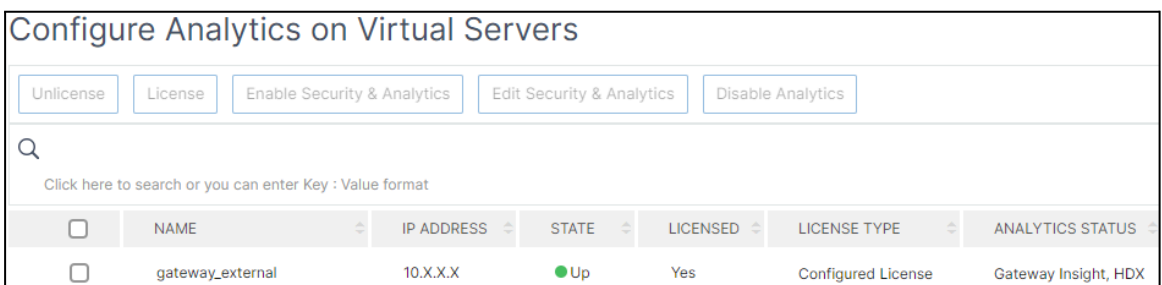
**NOTE: Logstream** is a Citrix-owned protocol that is used as one of the transport modes to efficiently transfer the analytics log data from NetScaler instances to ADM.



19. Click **Close** once the operation is **completed**.

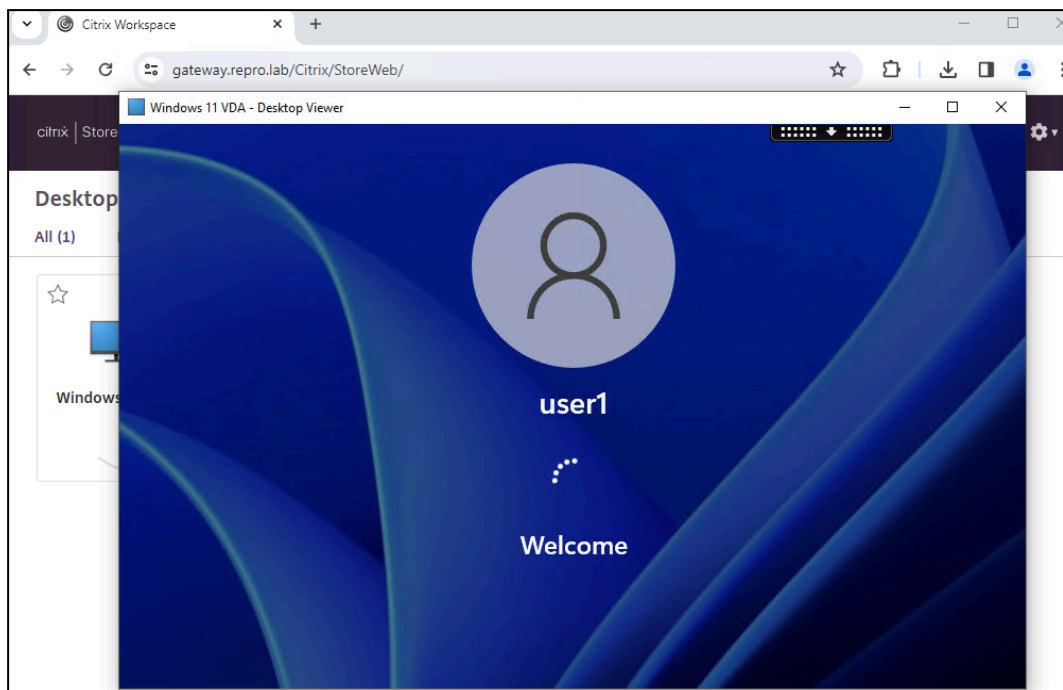
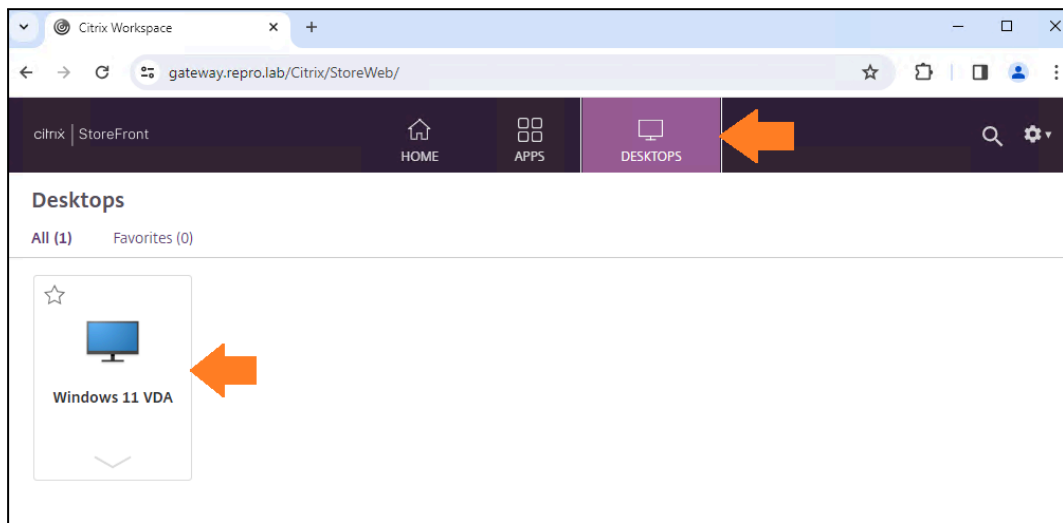


20. The NetScaler Gateway is configured on the ADM.

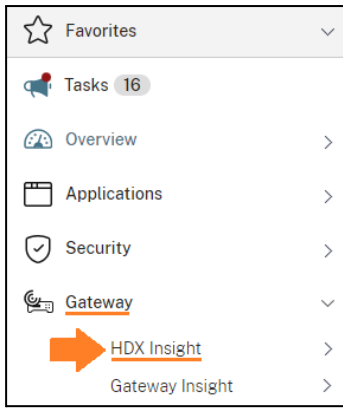


## Generating HDX Traffic and Testing

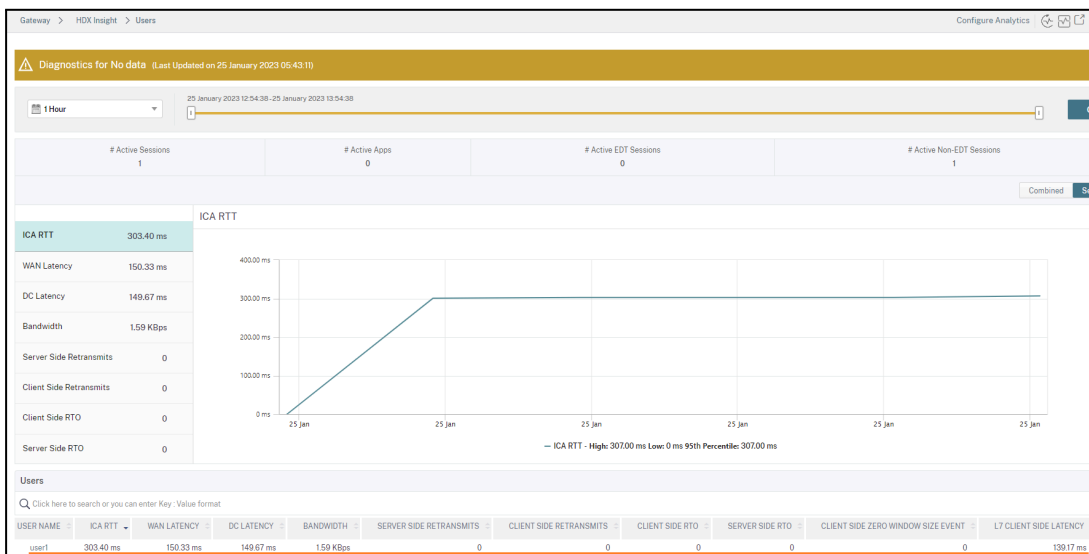
1. Log on to your NetScaler Gateway and launch your VDA Desktop.



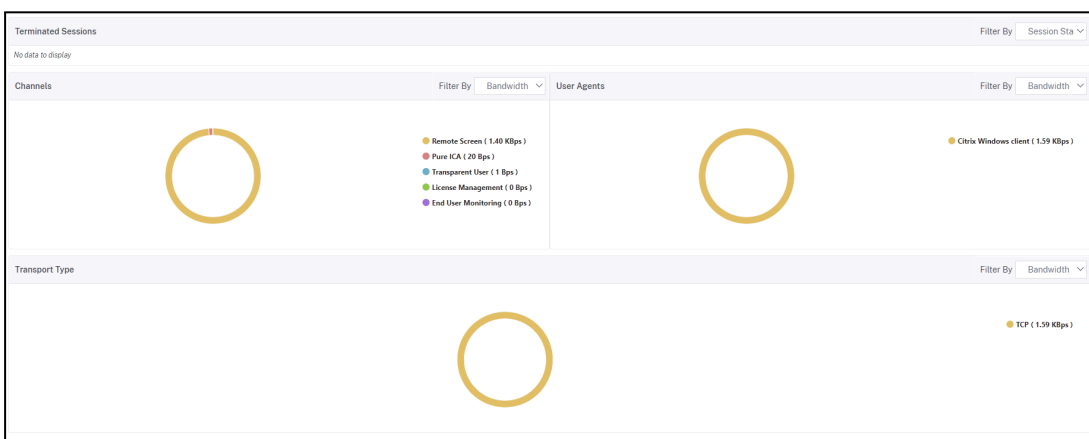
2. Return to the ADM Service and navigate to **Gateway > HDX Insight**.



- In a few times, you will start seeing some data from your VDA session. Refresh the page if you do not see any data.



- You will see the name of the username connected and some network information.



# NetScaler and NetScaler Gateway Troubleshooting

## Cannot Complete your Request Error

---

### Notes:

The "**Cannot complete your request**" error is, unfortunately, a generic message. To identify the actual cause of the error, it is recommended to refer to the logs in the **Storefront/DDC Event Viewer**.

For simplified troubleshooting, if you utilize **multiple** Storefront servers, it is advisable to either **disable** the second/third Storefront on the LB service group/service or modify the "**web interface address**" field with the **Storefront IP**. This approach allows focusing troubleshooting efforts on the active Storefront in the service group or the one configured in the "web interface address".

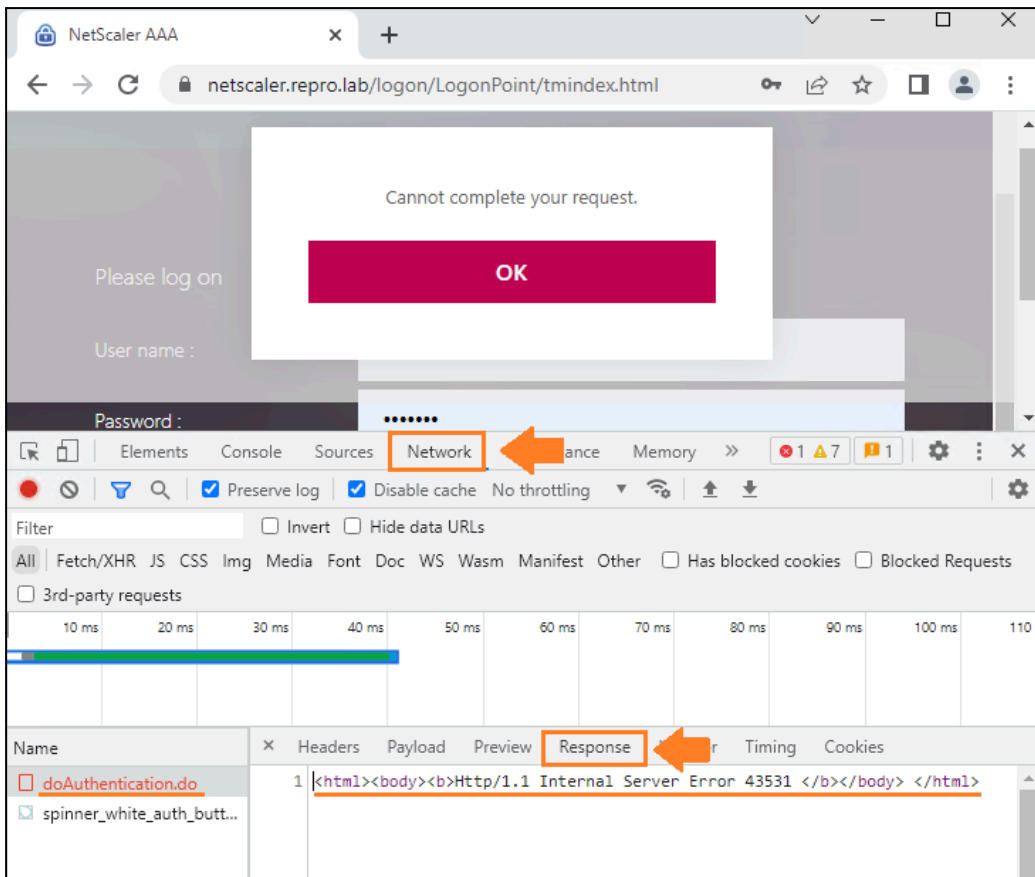
---

1. Start from this [CTX262124](#) article. It contains almost all the necessary steps required to fix this error.
2. Check the **Session profile > Published Applications** tab and ensure the **NetScaler** can properly **resolve the Storefront Address**, either **FQDN (if FQDN)** or **IP Address** as step number 1 in [CTX286594](#).
3. **Missing or misconfigured SSO domain** under the **Session profile > Published Applications** tab when LDAP auth is in place. For **SAML/OAUTH**, it is not required as SAML/OATH uses **UPN**. For more, check out [CTX219618](#)
4. LDAP attributes are misconfigured on the NetScaler. For more, check out the [CTX212422](#)
5. Check the Session Policies and ensure they are in the advanced expressions format (HTTP.REQ..) as [CTX291268](#)
6. SSL certificate missing or Invalid on the NetScaler or Storefront. Check [CTX235844](#) and [CTX224709](#)
7. Create a **dummy service** with the **Storefront IP** and **port** with **TCP monitor**. Confirm it shows UP. It will help confirm there is no communication issue.
8. You can always check the **policy hits** and ensure the **Session Policy** is getting hits accordingly.  
**CLI Commands:**  
> shell  
# nsconmsg -d current -g pcp\_hits  
.. and then reproduce the issue. Watch the logs
9. For troubleshooting related to **DTLS**, check out this [CTX article](#). To check if **DTLS** connection is established, check out this [CTX article](#). If you suspect the issue of launching applications externally is related to **DTLS**, you can disable it under the NetScaler Gateway VIP.

VPN Virtual Server			
Basic Settings			
Name	gateway_external	Maximum Users	0
Protocol	SSL	Max Login Attempts	-
Port	443	ICA Only	false
State	● UP	Enable Authentication	true
RDP Server Profile	-	IPset	-
PCoIP VServer Profile	-	Windows EPA Plugin Upgrade	-
Down State Flush	false	ICA Proxy Session Migration	false
DTLS	true	Enable Device Certificate	false
AppFlow Logging	true		

10. Callback URL misconfigured on the Storefront, "Manage Citrix Gateways" tab. A callback URL is only necessary if you are using Smart Access or any password-less authentication such as SAML, OAUTH, etc. If you are not using any of them, the field needs to be left blank.

**NOTE: "Cannot complete your request" error on the Gateway logon page itself will not log any errors in the Storefront Event Viewer as it is not being reached yet. If you face this error and there are no logs in the SF server, this may indicate an issue on the NetScaler, either Storefront is not reachable or Storefront LB VIP is misconfigured.**



For more: [CTX286594](#) [CTX207162](#) [CTX238964](#) [CTX134940](#)

## Cannot Start App/Desktop Error

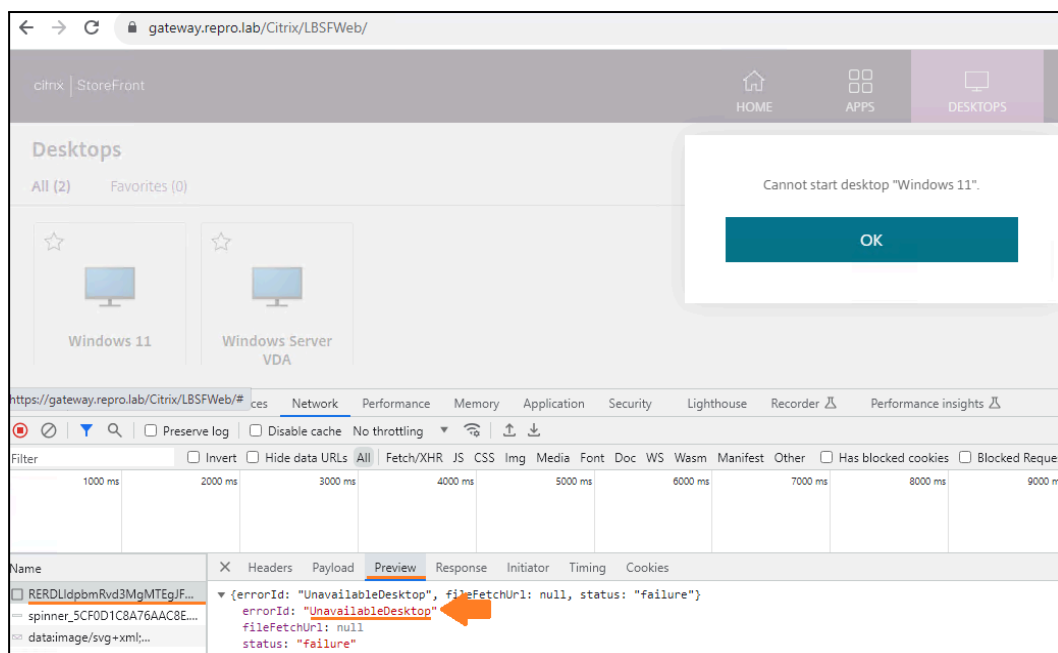
**NOTE: "Cannot Start App/Desktop Error" error is also a generic error. To find out the real cause of the error, always rely on the Storefront/DDC event viewer logs.**

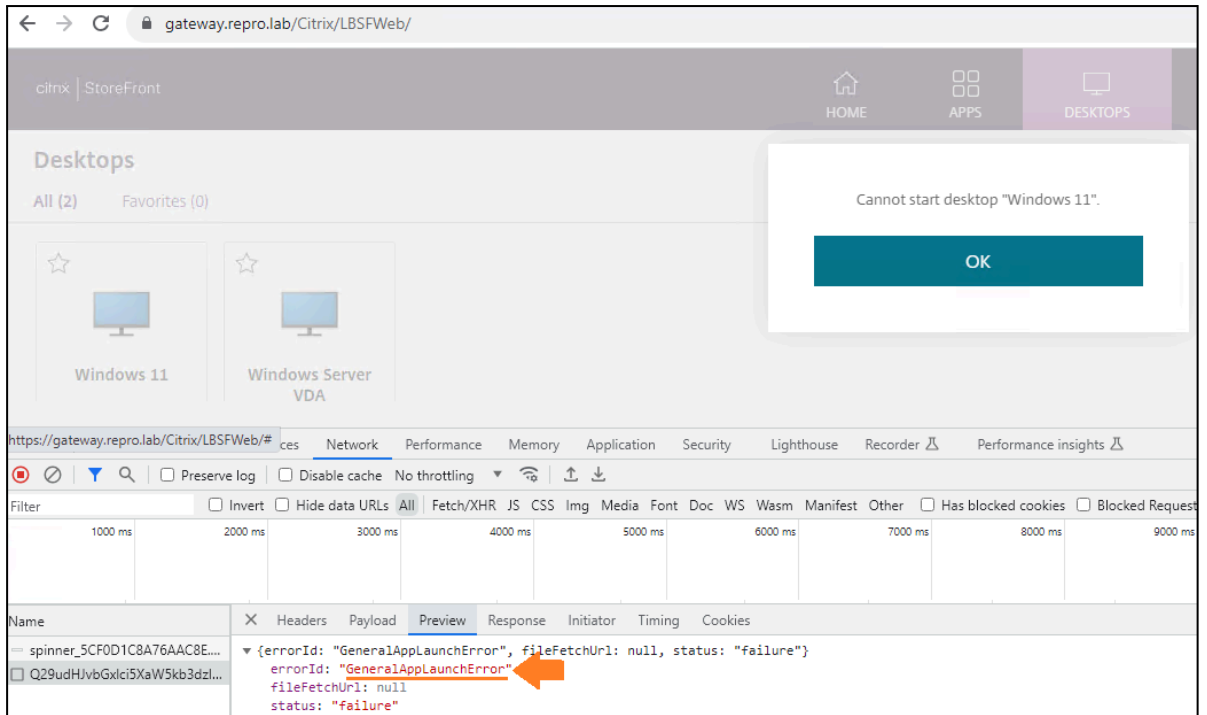
1. Ensure when connecting directly to the StoreFront server, you do not see this error.
2. Check the Storefront/DDC **Event Viewer**.
3. Confirm there are **available VDA VMs** in the **DDC Delivery Group**.
4. StoreFront server is unable to properly resolve the **STA server addresses** set under **Storefront > Citrix Gateway**.
5. If you use **Citrix FAS**, check if the FAS server is able to issue the user's certificate.
6. On the **Storefront/Gateway page**, use the development tools to confirm what is the real response from the controller. In the example below, an **"Unavailable Desktop"** error is seen.

VDA unregistered and no more sessions available are the most common issues for the error **Unavailable Desktop** seen on the browser's developer tools.

STA Address unreachable from Storefront Server is one of the common issues for the error **GeneralApplication Error** seen on the browser's developer tools.

Below you can see both examples.

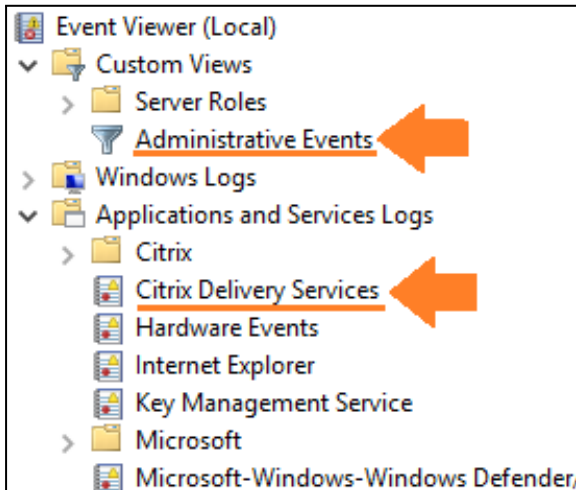




**NOTE:** For SSO failing from NSG to Storefront, confirm the **Gateway FQDN** configured on SF matches with the Gateway URL the customer is reaching the Gateway on the browser. If accessing with Gateway IP, it will fail too.



## Storefront Event Viewer

**Event viewer logs** will indicate the reason for the failures. Navigate to **Event Viewer > Administrative Events** or **Citrix Delivery Services** tab. For all the examples below, the resolutions are provided in the above steps.





**Citrix Delivery Services** Number of events: 1,661

Level	Date and Time	Source
Warning 	9/8/2023 10:03:12 AM	Citrix Store Service
Error 	9/8/2023 10:03:12 AM	Citrix Store Service




Event 0, Citrix Store Service

General Details

No available resource found for user repro.lab\willian when accessing desktop group Windows 11. This message was reported from the Citrix XML Service [NFuseProtocol.TRequestAddress].

**Administrative Events** Number of events: 3,682

Number of events: 3,682

Level	Date and Time	Source	Event ID	Task
Warning 	9/8/2023 10:12:27 AM	Citrix Store Service	28	(200
Error 	9/8/2023 10:12:27 AM	Citrix Store Service	1003	(123
Error 	9/8/2023 10:12:27 AM	Citrix Store Service	0	(123



Event 0, Citrix Store Service

General Details

The server name 1sta.repro.lab cannot be resolved. The specified Secure Ticket Authority could not be contacted and has been temporarily removed from the list of active services.

**Administrative Events** Number of events: 3,684

Number of events: 3,684

Level	Date and Time	Source
Error 	9/8/2023 10:46:12 AM	Citrix Receiver for Web
Error 	9/8/2023 10:46:12 AM	Citrix Authentication Service




Event 7, Citrix Authentication Service

General Details

CitrixAGBasic single sign-on failed because the credentials failed verification with reason: Failed.  
 The credentials supplied were;  
 user: willian  
 domain: repro.labew

**Administrative Events** Number of events: 3,687

Number of events: 3,687

Level	Date and Time	Source
Error 	9/8/2023 10:49:04 AM	Citrix Receiver for Web
Error 	9/8/2023 10:49:04 AM	Citrix Authentication Service
Error 	9/8/2023 10:49:04 AM	Citrix Authentication Service

Event 8, Citrix Authentication Service

General Details

None of the AG callback services responded



3. There are a few important things that need to be checked.
  - a. **Address** – This will show the **STA server** configured on the **Storefront** under the **Citrix Gateway settings**. The same **STA server** shown in the **ICA file must** be on the NetScaler added as an STA and it **must be UP**.
  - b. **SSLProxyHost** – The NetScaler Gateway FQDN. **CWA** (ICA connection) will start towards this address. Make sure this address is reachable from the Client (DNS).

```

Q29udHJvbGxlcj5XaW5kb3dzlDExIFZEQSAkUzItNA-- - Notepad
File Edit Format View Help
[[Encoding]
InputEncoding=UTF8

[ApplicationServers]
Windows 11 VDA $S2-4=

[Windows 11 VDA $S2-4]
Address=;40;STA380059977;6D6CAD992A7CD1DFF7C899ECE885C1
AutoLogonAllowed=ON
BrowserProtocol=HTTPonTCP
CGPSecurityTicket=0n
ClearPassword=657854394EBF40
ClientAudio=0n
ConnectionBar=1
DesiredColor=8
DesiredHRES=4294967295
DesiredVRES=4294967295
FontSmoothingType=0
HDXoverUDP=Preferred
HTTPBrowserAddress=!
InitialProgram=#Windows 11 VDA $S2-4
Launcher=WI
LogonTicket=657854394EBF400AE13C910C90E889
ProxvTimeout=30000
SessionsharingKey=-wv3CRYs2iUh68Wm1rdI3dyW0oTM
SFRAAllowed=Off
SSLCiphers=all
SSLEnable=0n
SSLProxyHost=gateway.repro.lab:443
startSCD=1706261277156
  
```

---

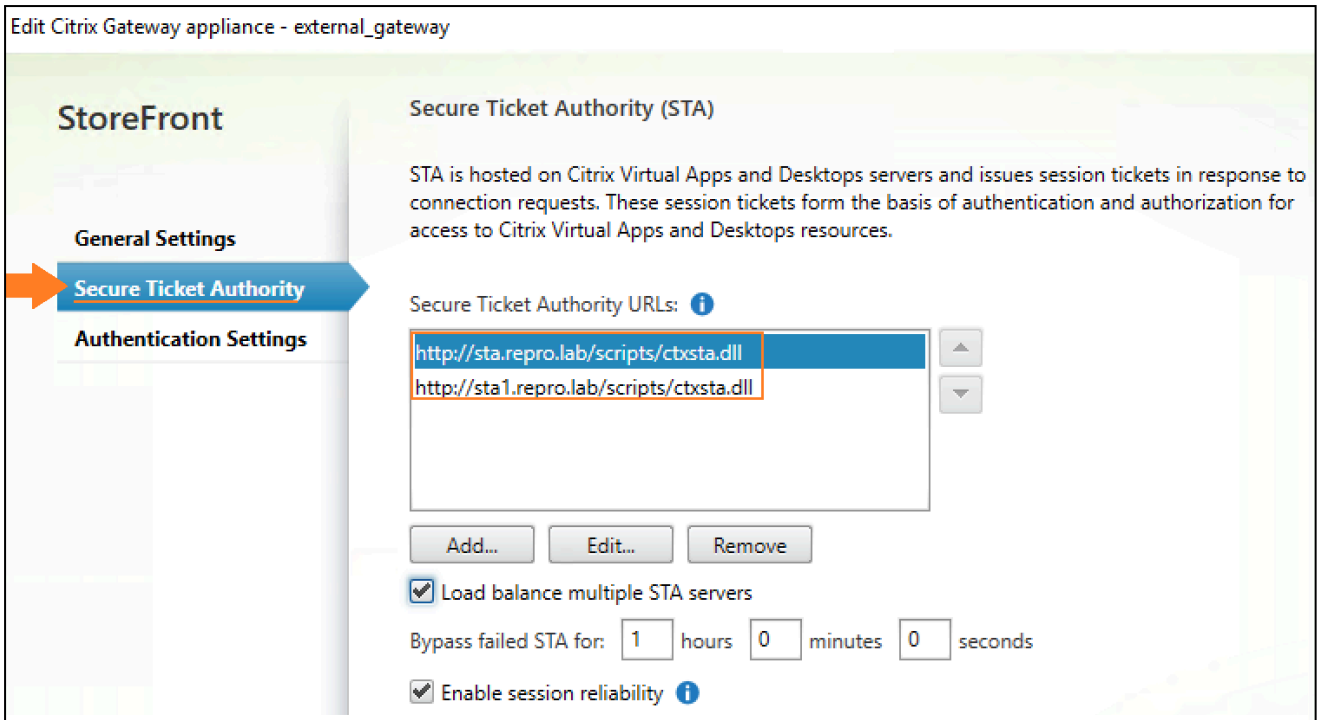
**NOTE:** The **tickets** in each ICA file **expires after about 90 seconds**. After the ticket in an ICA file is used or expires, the user needs another ICA file (re-launch the application/desktop).

---

## Checking STA Server Status – External Launch Failure

External launch through the NetScaler will fail if the **STA(s)** server is **DOWN**. If more than **1 STA** server is in place, **all of them should be UP** as well, otherwise, intermittent launches will happen.

On the **Storefront Server** under the **Citrix Gateway Settings > Security Ticket Authority**, check the STA servers added and confirm their FQDNs/IPs.



On Netscaler, under the **Gateway Virtual Server > Published Applications**, check the STA servers added. The list of STA servers on the NetScaler must be equal to the StoreFront one. If one or more STAs on the NetScaler are either **DOWN** or missed, the session launch will fail/intermittently fail. The **STA AUTH ID** shown in the **EXTERNAL ICA FILE**, must match the **STA AUTH ID** shown on the NetScaler (as shown in the next topic).

VPN Virtual Server STA Server Binding				
<input type="button" value="Add Binding"/> <input type="button" value="Unbind"/> <input type="button" value="Refresh"/>				
<input type="text" value="Click here to search or you can enter"/>				
	SECURE TICKET AUTHORITY SERVER	SECURE TICKET AUTHORITY SERVER ADDRESS TYPE	STATE	AUTH ID
<input type="checkbox"/>	http://sta1.repro.lab	IPV4	DOWN	NA
<input type="checkbox"/>	http://sta.repro.lab	IPV4	UP	STA759059232

**NOTE:** Check out this [CTX](#) for basic troubleshooting.

## LDAP/Radius Authentication Issue

If you cannot authenticate to the NetScaler Gateway portal (LDAP or RADIUS), you can monitor the authentication in real-time through the NetScaler CLI using the `"/tmp/aad.debug"` tool as below or for offline analysis, you can check `/var/nsvpn.log` files. For more check out [CTX114999](#).



**CLI command:**

> shell

# cat /tmp/aaad.debug

...and then reproduce the authentication issue. Watch the logs

```

$ shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

root@ad3# cat /tmp/aaad.debug
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/ldap_common.c[978]: continue_ldap_init 1-86: Connecting to: 192.168.186.162:636
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/ldap_common.c[984]: continue_ldap_init 1-86: User user1 Connecting to: 192.168.186.162:636
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[6106]: register_timer 1-86: setting timer 209
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[6183]: unregister_timer 1-86: releasing timer 209
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/ldap_drv.c[2238]: receive_ldap_user_bind_event 1-86: Bind OK.
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[6183]: unregister_timer 1-86: releasing timer 212
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/ldap_drv.c[2332]: receive_ldap_user_bind_event 1-86: User authentication (Bind event) for user user1 succeeded
Mon Jun 27 08:33:28 2022
/usr/home/build/adc/usr.src/netscaler/aaad/naaad.c[4250]: send_accept 1-86: sending accept to kernel for : user1

```

Some error codes and the cause of the issue. For more, check out [CTX138663](#)

aaad.debug Module Error Codes	Cause
4001	Invalid Credentials
4002	Not Permitted
4003	System Timeout
4004	System Error
4005	Socket Error
4006	Bad User
4007	Bad Password

You can monitor real-time the policy hits through the NetScaler at the time you are logging on. As you can see below, there are some cache policy hits (policies that are bound globally by default) + the LDAP policy followed by the Session policy Web. This is useful to confirm the correct policies/orders are getting hits as desired.

### CLI commands

```
> shell
```

```
# nsconmsg -d current -g pcp_hits
```

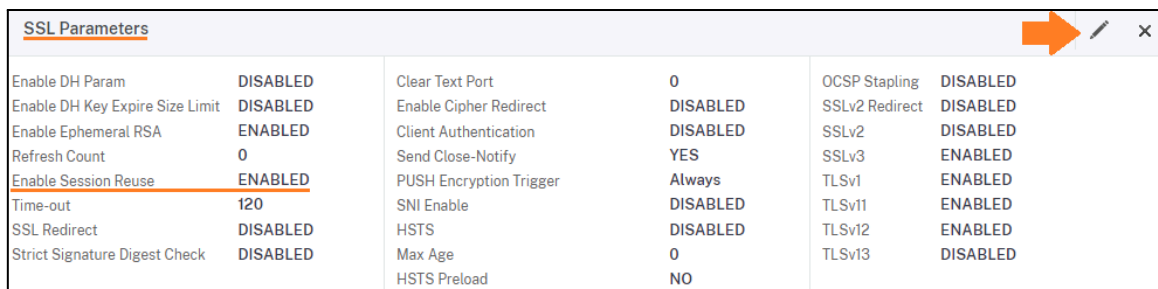
## Taking VPX Network Trace on GUI (Wireshark)

The NetScaler operating system provides a utility called “ns trace” to get a dump of the packets that are received and sent out by an appliance, and you can use these files to troubleshoot any network issue. The Wireshark app needs to be used to read these files. For more information, please check out the [eDocs](#).

Before taking a network trace, it is recommended to disable the **SSL session reuse** parameter under the SSL Virtual Server/Profile you are troubleshooting to ensure you will capture a **full SSL handshake** in the trace. When it is enabled, you can eventually capture a partial handshake instead. In some cases, it is necessary to disable **ECC curves** as well, however, you must not disable it if the related SSL ciphers are used (SSL certificate using ECDSA key). Also, if **DH Param/Key** is enabled, the traffic **will not** be decrypted. If troubleshooting authentication issues, you can follow this [CTX article](#).

Ensure you enable the option after the trace collection. **Do not** disable an SSL session reuse when the persistence method is “**SSLSESSION**”, as it breaks the persistence for existing connections. For more info, refer to this [CTX](#).

1. Edit the SSL virtual server (either NetScaler Gateway VIP or LB SSL VIP) and navigate to **SSL Parameters**.



SSL Parameters					
Enable DH Param	DISABLED	Clear Text Port	0	OCSF Stapling	DISABLED
Enable DH Key Expire Size Limit	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Client Authentication	DISABLED	SSLv2	DISABLED
Refresh Count	0	Send Close-Notify	YES	SSLv3	ENABLED
<b>Enable Session Reuse</b>	<b>ENABLED</b>	PUSH Encryption Trigger	Always	TLSv1	ENABLED
Time-out	120	SNI Enable	DISABLED	TLSv11	ENABLED
SSL Redirect	DISABLED	HSTS	DISABLED	TLSv12	ENABLED
Strict Signature Digest Check	DISABLED	Max Age	0	TLSv13	DISABLED
		HSTS Preload	NO		

2. Uncheck the option **Enable Session Reuse**, click **OK**, and **Done**.

SSL Parameters

Enable DH Param ⓘ  
 Enable DH Key Expire Size Limit  
 Enable Ephemeral RSA  
 Refresh Count  
  
 Enable Session Reuse ⓘ  
 Enable Cipher Redirect  
 SSLv2 Redirect  
 Client Authentication

OCSP Stapling  
 SSL Redirect  
 SNI Enable  
 Send Close-Notify  
 Clear Text Port  
  
 PUSH Encryption Trigger  
  
 Strict Signature Digest Check  
 HSTS  
 Max Age

Protocol

SSLv2     SSLv3     TLSv1     TLSv11     TLSv12

**NOTE:** If an SSL Profile is in place, the same procedure above needs to be done inside the SSL profile.

3. Navigate to the **System > Diagnostics** page, and under **Technical Support Tools**, click **Start new trace**.

Favorites

System

Licenses

Settings

**Diagnostics**

High Availability >

NTP Servers

Reports

Reporting Configs

Profiles

Partition Administration >

User Administration >

## Diagnostics

**View Configuration**

[Saved configuration](#)  
[Running configuration](#)  
[GSLB running configuration](#)  
[Saved v/s Running](#)  
[Revision history](#)  
[Pre v/s post upgrade](#)  
[Peer node \(High Availability\)](#)  
[Detect changed/updated password\(s\)](#)


**Technical Support Tools**

[Generate support file](#)  
[Start new trace](#)  
[Stop running trace](#)  
[Get back trace](#)  
[Call Home](#)

4. Update the packet size to **0** in the Packet size field. If you do not change it, you will not record all packets.

## ← Start Trace

Packet Size

Capture trace in .pcap format

Number of trace files

Trace file name

Trace File ID

Duration of data per file (seconds)

File Size

Trace Buffers

---

**NOTE:** “File Size” is set to **1024 (1GB)**, which means that if the trace capture reaches 1GB, a second file will be created. This is not a problem. You can alternatively, set the “File Size” to **0** if you don’t wish for multiple files of 1GB.

---

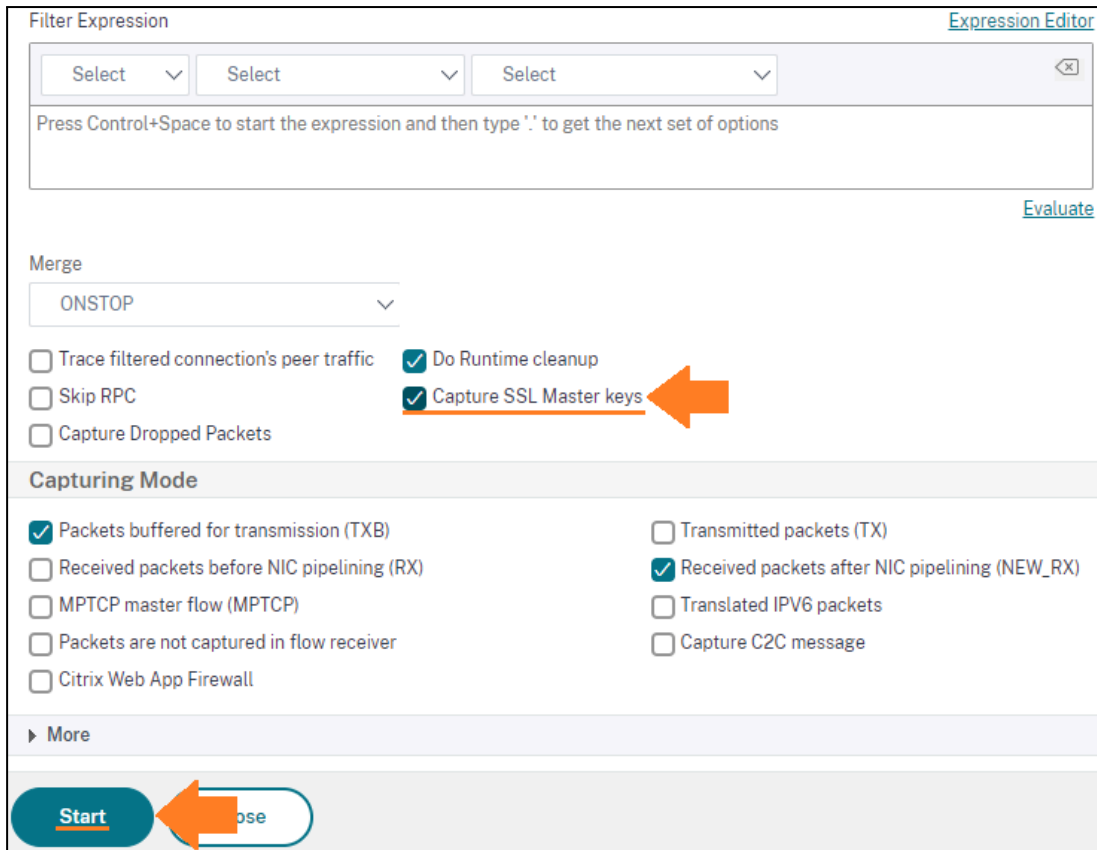
5. Scroll down and enable **Capture SSL Master Keys** if troubleshooting SSL-related issues. It will allow you to decrypt the traffic on the Wireshark. All other settings are optional and not required for this use case. Click **Start**.

---

**NOTE:** If using filters such as Client IP or VIP IP, you must enable the **Trace Filtered connection’s per traffic** option.

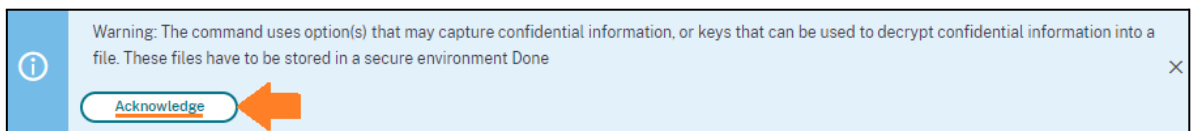
---





**NOTE: SSL Master Keys** are not the customer's private keys themselves, they are **session keys** that will only decrypt this trace/session. This **DOES NOT** work with **FIPS ADCs** as the SSL Session Keys can't be captured from **FIPS HSM**.

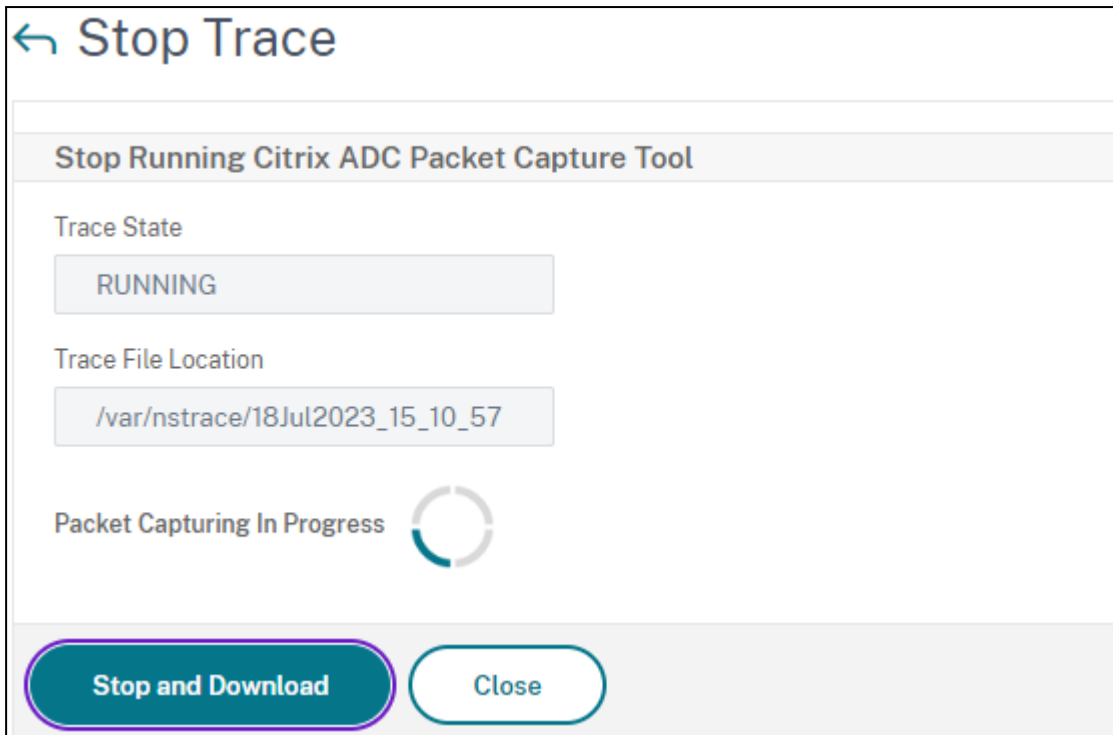
6. Scroll the page UP and click **Acknowledge**.



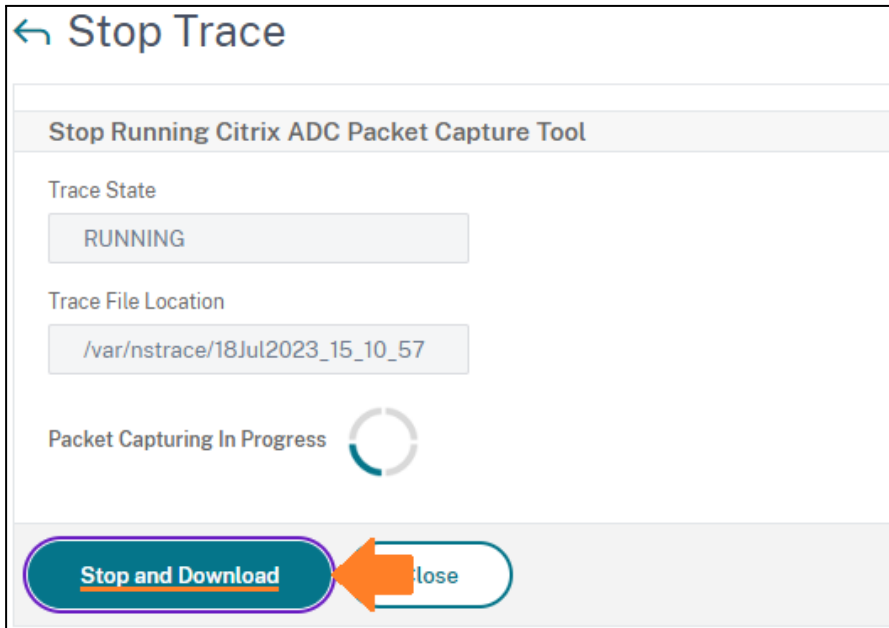
7. Click **OK**.



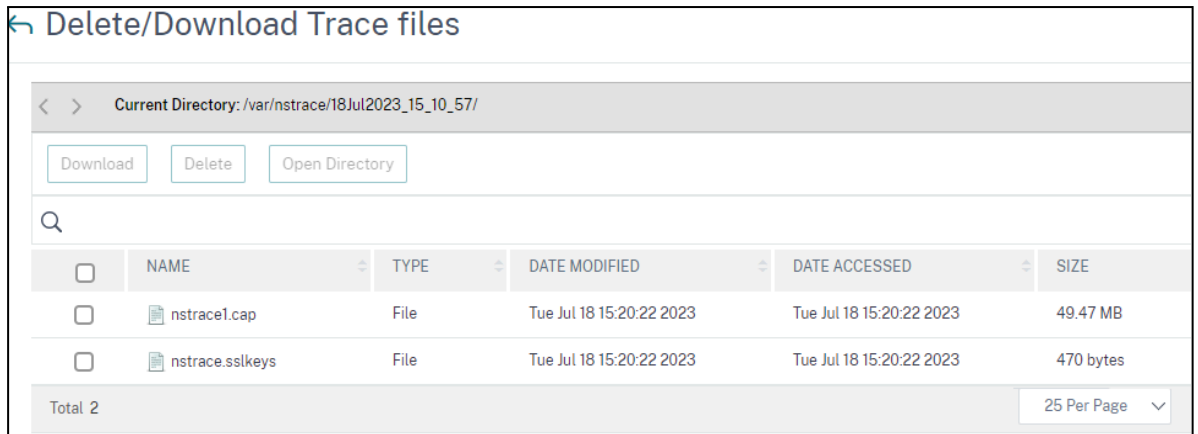
8. Keep the trace running while you reproduce your issue. For better results, open a new browser in the incognito mode and reproduce the issue. Take notes of timestamps related to error messages for example and any username inserted during the tests.



9. Now that you have reproduced the issue, you can stop and download the trace + SSL session Key.



10. You will see two files, **.cap** file, and the **.sslkeys** file. **Download** both (one by one).



- Open the downloaded file (.cap) using the Wireshark tool and Import the keys (.sslkeys) to decrypt the traffic (**Edit > Preferences > Protocols > TLS** and select **“(Pre)-Master Secret log filename)**).

---

**NOTE:** Enable again the **SSL Session reuse parameter** under the SSL settings.

---

## Limitations of Using SSL Session Keys

The following are the limitations of using SSL session keys:

- SSL sessions cannot be decrypted if the initial packets of the session are not captured
- SSL sessions cannot be decrypted if the DH param is enabled
- SSL sessions cannot be captured if the Federal Information Processing Standard (FIPS) mode is enabled

## Taking VPX Network Trace by Using the Command Line Interface (CLI)

From CLI, use the command **“start nstrace” + “-size 0”** to start the capture and capture in full. If you wish to capture the SSL master Keys, add the parameter **“-capsslkeys ENABLED”**. To show the current trace, run **“show nstrace”** and to stop, run **“stop nstrace”**. The file will be saved by default at **/var/nstrace/FOLDER-DATE**.

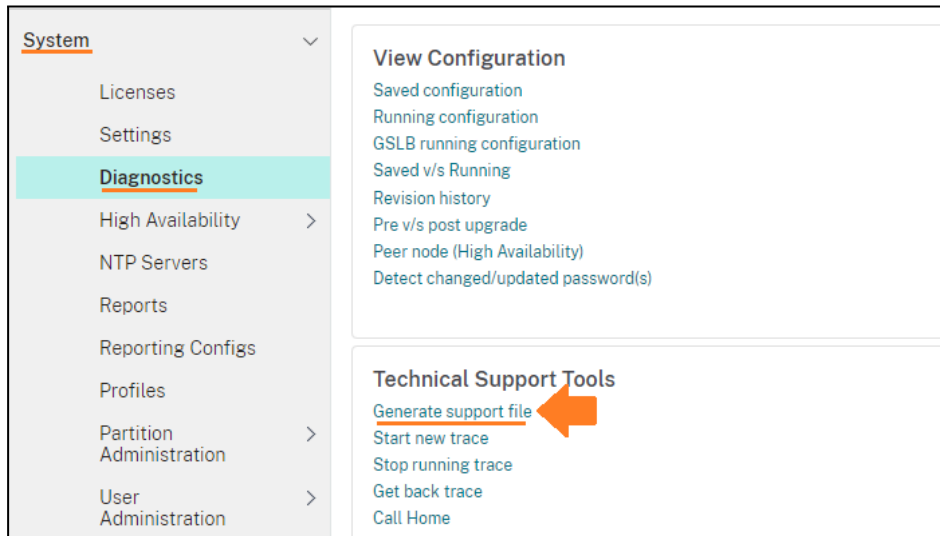
```
> start nstrace -size 0 -capsslkeys ENABLED
> show nstrace
> stop nstrace
```

```
> start nstrace -size 0 -capsslkeys ENABLED
Warning: The command uses option(s) that may capture confidential information, or keys that can be
have to be stored in a secure environment
Done
> show nstrace
State: RUNNING      Scope: LOCAL      TraceLocation: "/var/nstrace/23Aug2023_10_17_58/"
e: 0
Mode: TXB_NEW_RX   Traceformat: NSCAP PerNIC: DISABLED      FileName: 23Aug2023_10_
runtimecleanup: ENABLED
TraceBuffers: 5000 SkipRPC: DISABLED   SkipLocalSSH: DISABLED Capsslkeys: ENABLED
Done
> stop nstrace
Done
```

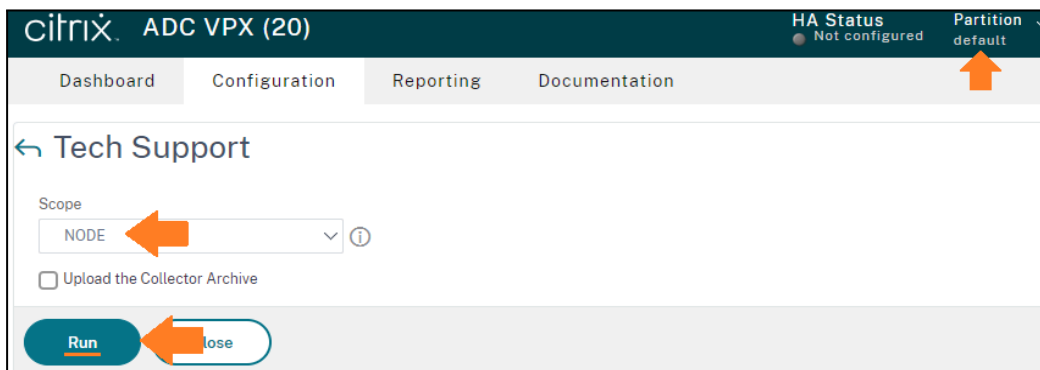
## Taking VPX Logs (Support Bundle)

You can generate a technical support bundle on the appliance to gather netscaler’s configuration/log to be analyzed offline. The NetScaler technical support bundle is a “zipped tar” archive of system configuration data and statistics. For more, check the [eDocs](#).

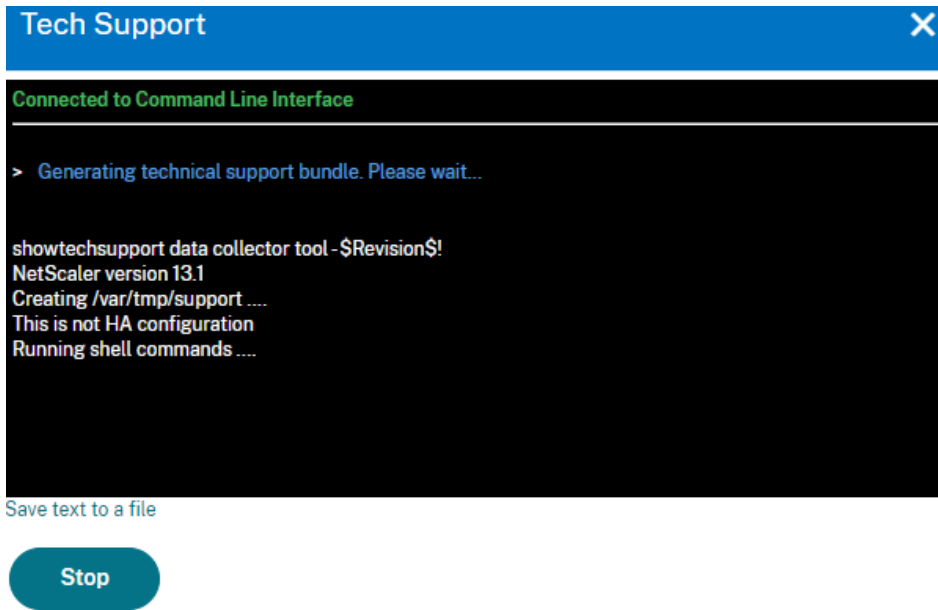
1. Navigate to **System > Diagnostic**. In the Technical Support Tools section, click **Generate Support File**.



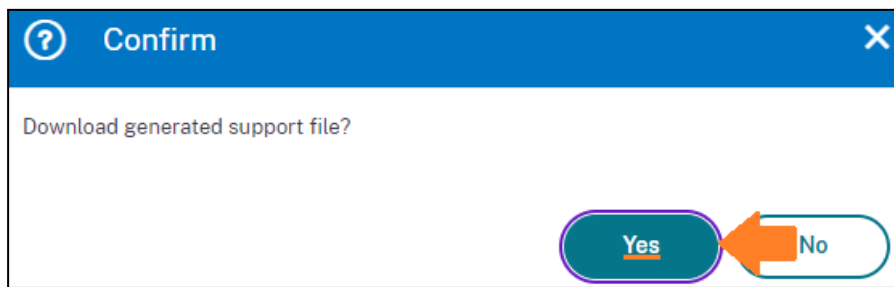
2. NetScaler can run over **Partitions** but most of the NetScaler admins do not use it. Just double-check it is on the default partition in the top-right corner. If so, just keep it as **NODE** under Scope and click **Run**. If not, just select the partition name under Scope.



3. Wait a moment.



4. The Technical Support bundle is generated. Click **Yes** to download the support bundle to your local desktop.



## Taking VPX Logs by Using the Command Line (CLI)

From the CLI, use the command “**show techsupport**” to start the logs capture. The file will be saved by default at **/var/tmp/FOLDER-DATE**.

> show techsupport

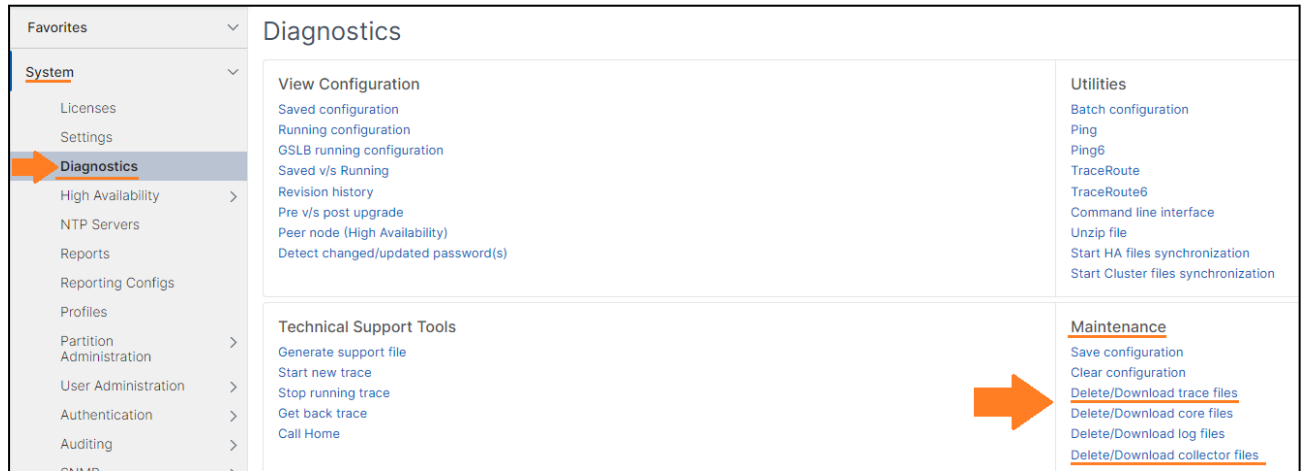
```
> show techsupport
showtechsupport data collector tool - $Revision$!
NetScaler version 13.1
The NS IP of this box is 10.91.68.204
This is not HA configuration
cp: Environment is not a directory
cp: Environment is not a directory
cp: Environment is not a directory
Running shell commands ...
Creating archive ...
/var/tmp/support/support.tgz ---- points to --> /var/tmp/support/collector_P_10.91.68.2

===== IMPORTANT =====
This NetScaler is part of GSLB. Please run this command on other site nodes as well.
This will help in troubleshooting any GSLB related issues.
=====
showtechsupport script took 1 minute(s) and 37 second(s) to execute.
Done
```

## Download Trace Files and Support Bundles Generated by CLI

**NOTE:** You can either download the logs/trace by using **WinSCP** for example or download straight from the **NetScaler GUI**.

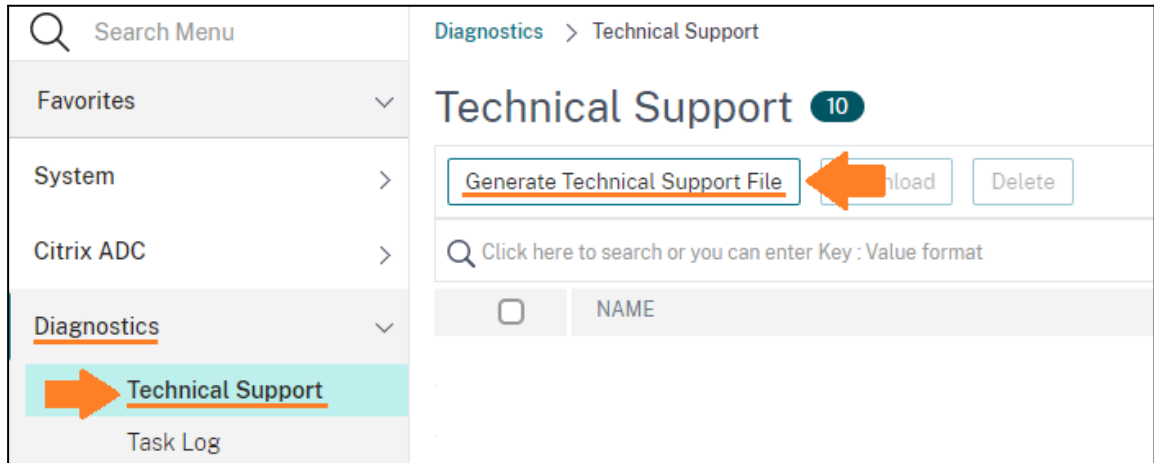
Navigate to **System > Diagnostics** and under **Maintenance** select what you wish to download



You can alternatively, download nslog files (**delete/download log files**) or core/crash files (**delete/download core files**).

## Taking SDX/SVM Logs (Support Bundle)

1. Navigate to **Diagnostics > Technical Support** and click **Generate Technical Support File**.



2. You will need to select which collection of logs you wish to take. In most scenarios, you will need SVM logs + VPX Instance logs, however, depending on the issue you are troubleshooting, you will also need the Hypervisor logs and in this case, you will need to have Hypervisor logs, SVM logs and VPX Instance logs. If you are unsure which collection of logs to take, you could take all of them. You will see the following options:

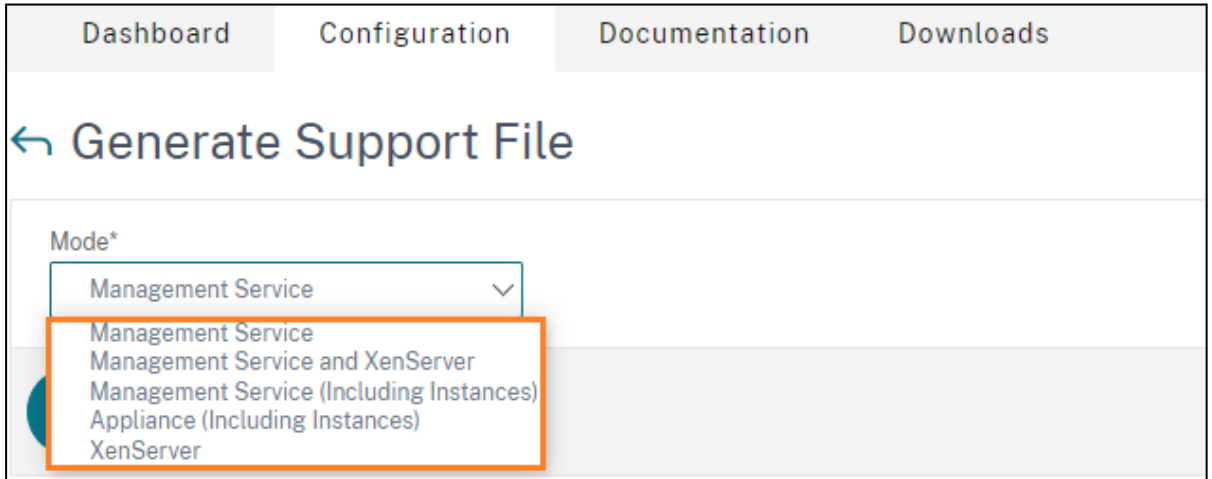
**Management Service** - Contains only the SVM logs (will not contain Hypervisor logs nor VPX instance logs).

**Management Service and XenServer** - Contains the SVM logs and the Hypervisor logs.

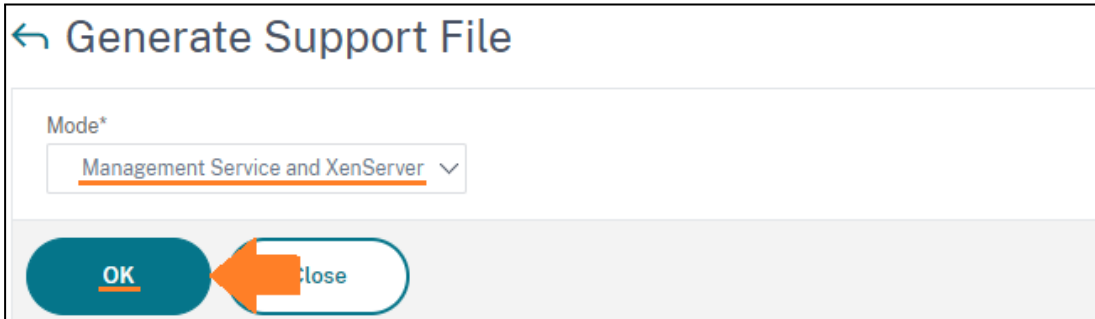
**Management Service (Including Instances)** - Contains the SVM logs and the selected VPX Instance logs. You will need to select which VPX instance you wish the logs from. Click **“Add”** to select the desired Instance.

**Appliance (Including Instances)** - Contains the SVM logs, Hypervisor logs, and the selected VPX Instance logs. You will need to select which VPX instance you wish the logs from. Click **“Add”** to select the desired Instance.

**XenServer** - Contains the Hypervisor logs only.



3. As soon as you select which collection of logs you need, just click OK and your support bundle will be generated.



**NOTE:** There is a tab called **“Task Log”** under Diagnostic which shows all the tasks completed via SVM GUI.



**cloud**<sup>TM</sup>  
**SOFTWARE GROUP**