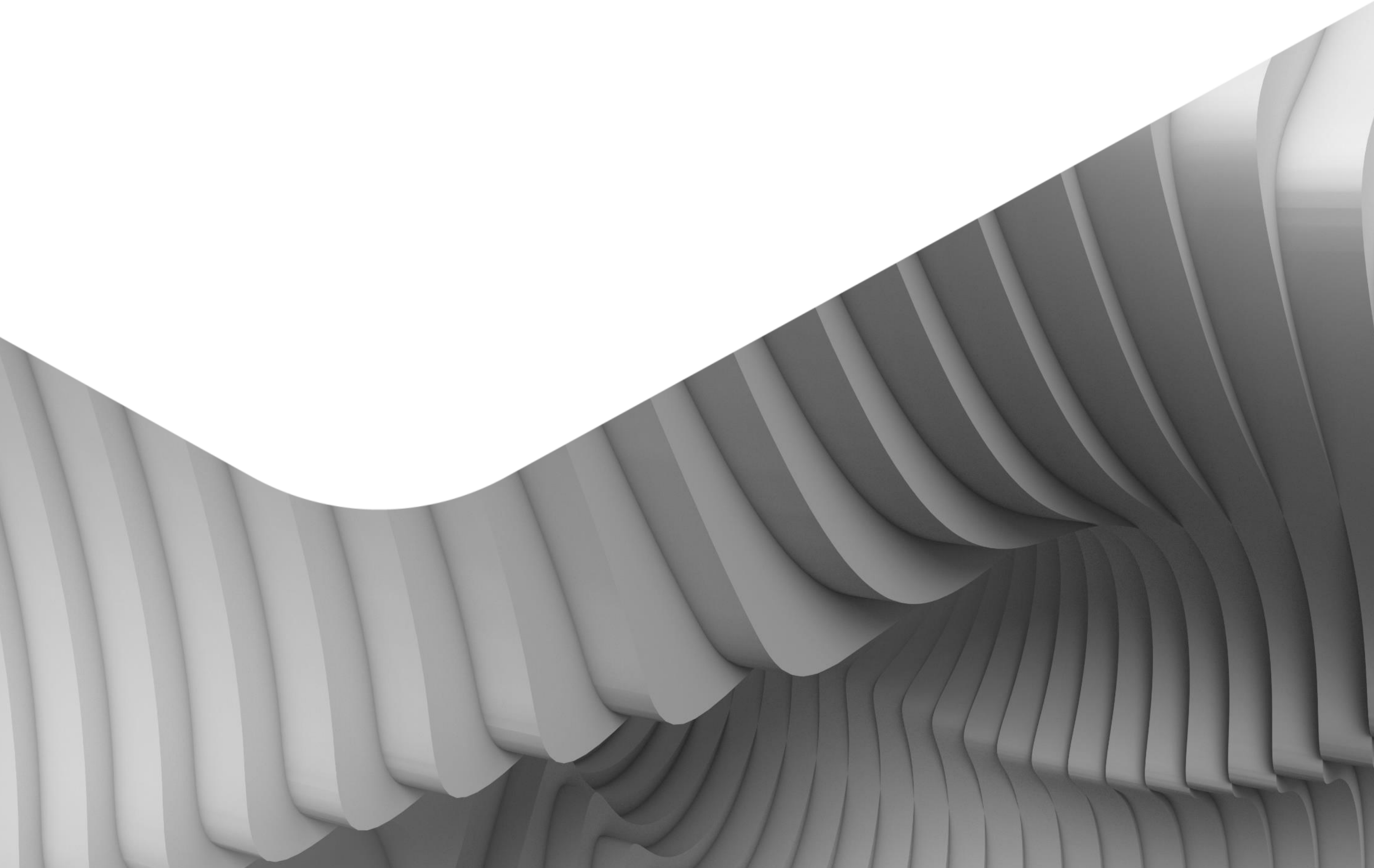
Kemp Zero Trust Access Gateway

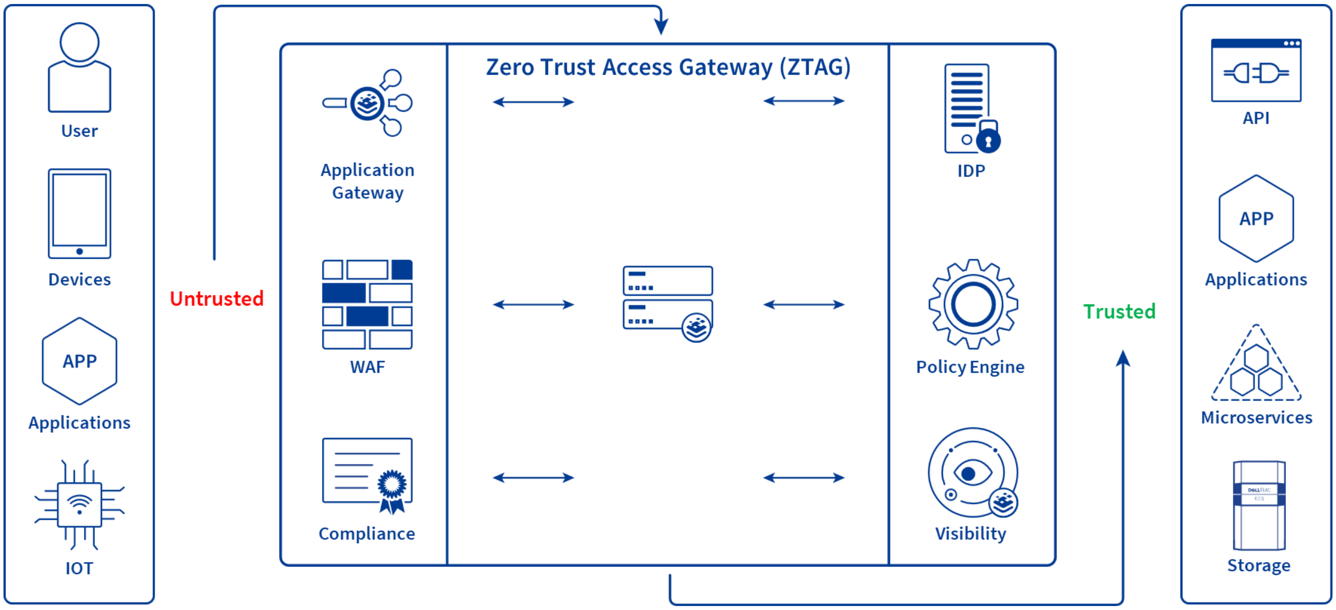
Reference Guide



Contents

Overview

With the increase of threats and other malicious activities targeted at organizations today, the need for a layered security model providing least privileged access has never been more essential. As most modern applications provide a level protection, there are often some gaps that limit the ability to address specific security needs. The Kemp load balancer is set in a privileged position and with its native capabilities is empowered to apply security in ways other solutions fall short. The Kemp Zero Trust Access Gateway (ZTAG) delivers a simple, flexible, and secure approach for providing the necessary access for users and applications to access backend systems while greatly reducing the exposure to today's threats.



The Kemp Zero Trust Access Gateway delivers secure publishing of workloads using the following attributes:

- **Authentication –** Leveraging organization's existing identity provider (iDP), Zero Trust Access Gateway can authenticate users to determine the proper credentials are provided prior to allowing access to the applications being published. Using the Kemp Edge Security Pack, several authentication methods including Multi-Factor Authentication (MFA) can be leveraged to pre-authenticate users prior to allowing access to the published application.
- **Group Membership –** Building off the authentication delivered as part of Zero Trust Access Gateway, group membership assignment can be required as part of access policies. This approach can allow or deny access to an application dependent on group membership or enforce additional authentication methods (i.e., Multi-Factor Authentication).
- **Location** – Since the load balancer can identify the source address of who or what is accessing the back-end systems, granular access control policies can be applied along with other characteristics to permit or deny access to portions of an application and/or require additional authentication methods based on location.

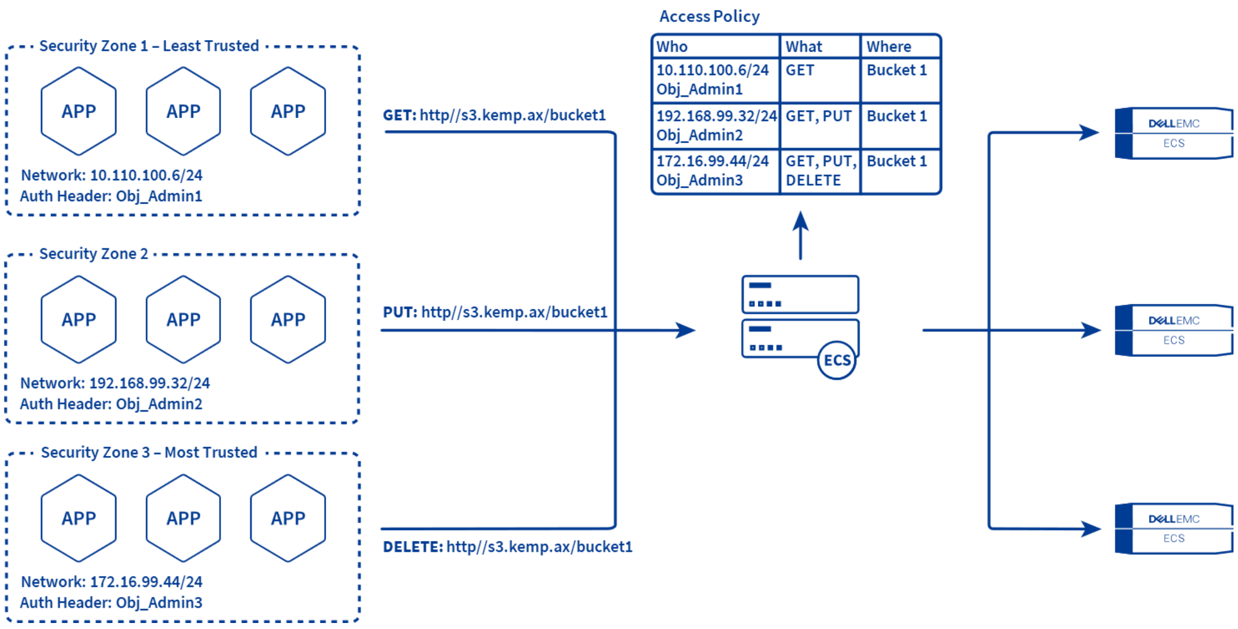
- **HTTP Header** – Publishing workloads at layer 7 provides full visibility of application traffic which can be leveraged to identify intent and apply necessary security policies to ensure least privileged access.
- **Path/ S3 Bucket** – Business critical workloads including web application and object storage solutions require permissions to be applied based on what portion of the application or storage that is being accessed.

How it works

The Kemp Zero Trust Access Gateway provides administrators with a policy builder to implement granular least privileged access to resources published through the load balancer. A configuration file is used to clearly define the application as well as the access policy rules. This configuration file is called by a script that allows the administrator to choose different options during each run dependent on the use case being addressed. Example XML configuration files are provided to assist with the configuration of policies for each use case.

Supported Use Cases

The following are the supported use cases for Zero Trust Access Gateway while additional variations are being constantly developed and released.



Access Policy

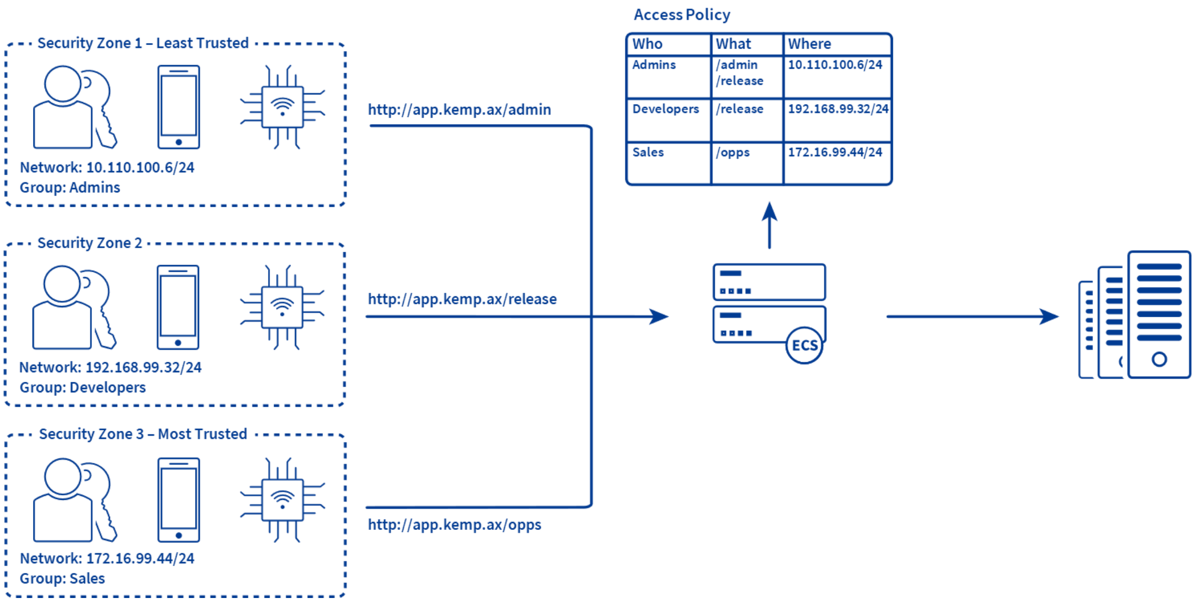
Who	What	Where
10.110.100.6/24 Obj_Admin1	GET	Bucket 1
192.168.99.32/24 Obj_Admin2	GET, PUT	Bucket 1
172.16.99.44/24 Obj_Admin3	GET, PUT, DELETE	Bucket 1

Source IP/Method/Path – This security policy although developed for object storage solutions is not limited to this workload. This approach applies security looking at three specific characteristics of the traffic being captured: Who, What, and Where. The traffic must match all three attributes to be permitted access to the published system. This configuration will ensure applications or users in a less secure zone do not have the necessary access to possibly write any malicious data into the share storage system that may compromise the applications in the highest security zone. Those same applications in the less secure zone may have the ability to write and delete data from other buckets if those buckets were not accessible to highly secure systems.

> Who – The source IP Address of the requestor. Since the primary workload is object storage this IP address may be that of a user or an application access the storage. These source IP addresses would be directly associated with security zones.
> What – The HTTP Method being passed to the published system. This would most commonly be a GET, PUT, or DELETE.
> Where – This is the path of the object being requested or written. In object storage terminology this would commonly be the name of an S3 bucket.

Authentication Header/Method/SourceIP– This security policy is also focused on the Object Storage workload but can be leveraged with other solutions that utilize HTTP methods and the Authorization Header. The traffic once again must match all three attributes to be permitted access to the published system. If the quantity of buckets being secured becomes more difficult to manage, the ability to leverage user accounts to secure the storage is an alternate solution. The accounts that are used to authenticate to today's storage solutions are passed within the HTTP header. This Authentication Header can be used to set policies to permit or deny specific access to the storage or other back-end system. This identifying header can be combined with the source IP address of the application or user to deliver the granular security.

> Who – The Authentication Header within the HTTP traffic. Many object storage vendors leverage the Authentication header to pass credentials for accessing the storage solution.
> What – The HTTP Method being passed to the published system. This would most commonly be a GET, PUT, or DELETE.
> Where – This is Source IP address from where the traffic originated from. This may be in the form of a single IP address or an entire network subnet.



Access Policy

Who	What	Where
Admins	/admin /release	10.110.100.6/24
Developers	/release	192.168.99.32/24
Sales	/opps	172.16.99.44/24

SteeringGroup/Path/SourceIP– This security policy is designed for any application that allows for pre-authentication to occur on the Kemp Load Balancer. Kemp Edge Security Pack is a security feature that provides the ability to pre-authenticate users on the load balancer prior to sending connections to the back-end systems. In addition to verifying a user's identity, Edge Security Pack to permit or restrict access based on group memberships in Active Directory. This functionality combined with identifying the source IP address of the requestor can enforce granular controls to different portions or paths of an application.

> Who – Steering Group. This is a Kemp specific attribute that looks at the Active Directory group a user is a member of and directs (steers) them to a specific element of the published application.
> What – The path within the published application the user is trying to access.
> Where – This is Source IP address from where the traffic originated from. This may be in the form of a single IP address or an entire network subnet.

Trusted/ Untrusted Zone– This security policy leverages Kemp Edge Security Pack allowing for pre-authentication to occur on the Kemp Load Balancer. This approach applies security looking at two specific characteristics of the traffic being captured: Who and Where. Should the traffic match the attributes for a Trusted zone, the user is presented with a simple form to authenticate to the application, but should the traffic be identified as Untrusted, the user will be required to provide multi-factor authentication to gain access. Active Directory Group memberships identified using Kemp Edge Security Pack are also leveraged to ensure that only specific users either from known or un-known network can access the published application.

> Who – Permitted Group. This is a Kemp specific attribute that looks at the Active Directory group a user is a member of and permits or denies access dependent on their group membership.
> Where – This is Source IP address from where the traffic originated from. This may be in the form of a single IP address or an entire network subnet.

Pre-Requisites

The Zero Trust Access Gateway does not require the user to have in-depth knowledge with Kemp products or PowerShell but some familiarity for each is recommended.

The components that make up the Kemp Zero Trust Access Gateway:

- Kemp LoadMaster or ECS Connection Manager
- Kemp Load Balancer PowerShell Module
- Zero Trust Policy Builder PowerShell Script
- Zero Trust Policy Builder Configuration File (XML)

Kemp PowerShell Module

1. **Download the Kemp PowerShell Module**

   The latest Kemp PowerShell Module can be found on the Support Website.

https://support.kemptechnologies.com/hc/en-us/categories/200141477-Downloads

The module contains the following files within the Kemp.LoadBalancer.Powershell folder:

- Kemp.LoadBalancer.Powershell.psd1
- Kemp.LoadBalancer.Powershell.psm1
- deprecated.psm1
- Kemp.LoadBalancer.Powershell-Help.xml

2. **Import the Kemp PowerShell Module** –

Copy the **Kemp.LoadBalancer.Powershell** folder to the relevant folder.

Install the module in a folder that is available in PSModulePath ($Env:PSModulePath).

If PSModulePath does not contain the module folder value, add the module path to the in PSModulePath environment variable. The module path can be for the current user only or for all users. Recommended values are:

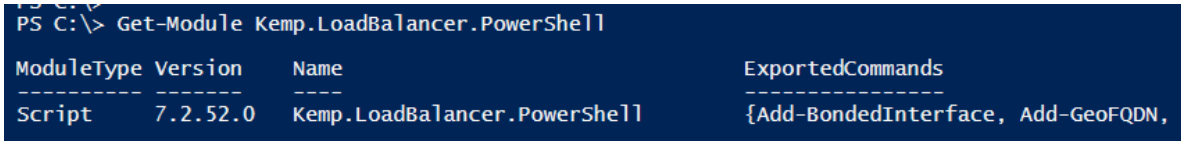
- $home\Documents\WindowsPowerShell\Modules for the current User
- $Env:ProgramFiles\WindowsPowerShell\Modules for All Users

For example, install the Kemp PowerShell module for the current user only:

```
# Save the current value of PSModulePath
$mpath = [Environment]::GetEnvironmentVariable("PSModulePath")
# Add the new path to the $mpath variable
$mpath += ";$home\Documents\WindowsPowerShell\Modules\Kemp.LoadBalancer.Powershell"
# Add the paths in $mpath to the PSModulePath value.
[Environment]::SetEnvironmentVariable("PSModulePath", $mpath)
```

Import the module to start using it:

```
Import-Module Kemp.LoadBalancer.Powershell
Get-Module Kemp.LoadBalancer.Powershell
```



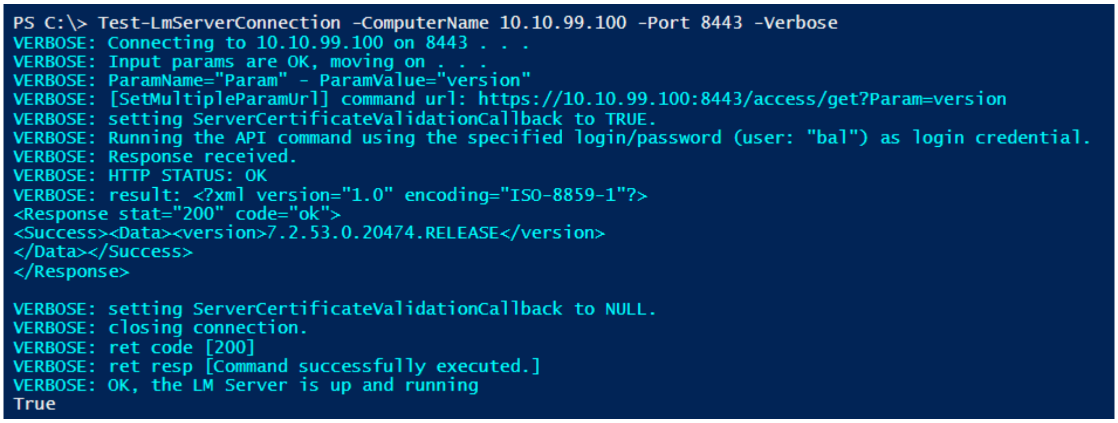
```
PS C:\> Get-Module Kemp.LoadBalancer.PowerShell

ModuleType Version    Name                              ExportedCommands
---------- -------    ----                              ----------------
Script     7.2.52.0   Kemp.LoadBalancer.PowerShell      {Add-BondedInterface, Add-GeoFQDN,
```

For the PowerShell commands to work, the API interface must be enabled on the LoadMaster. To enable it using the Web User Interface (WUI), go to **Certificates & Security** > **Remote Access** and select **Enable API Interface**

You can test the connection to the load balancer by using the **Test-LmServerConnection** command, for example:

Test-LmServerConnection -ComputerName 10.10.99.100 -Port 8443 -Verbose



```
PS C:\> Test-LmServerConnection -ComputerName 10.10.99.100 -Port 8443 -Verbose
VERBOSE: Connecting to 10.10.99.100 on 8443 . . .
VERBOSE: Input params are OK, moving on . . .
VERBOSE: ParamName="Param" - ParamValue="version"
VERBOSE: [SetMultipleParamUrl] command url: https://10.10.99.100:8443/access/get?Param=version
VERBOSE: setting ServerCertificateValidationCallback to TRUE.
VERBOSE: Running the API command using the specified login/password (user: "bal") as login credential.
VERBOSE: Response received.
VERBOSE: HTTP STATUS: OK
VERBOSE: result: <?xml version="1.0" encoding="ISO-8859-1"?>
<Response stat="200" code="ok">
<Success><Data><version>7.2.53.0.20474.RELEASE</version>
</Data></Success>
</Response>

VERBOSE: setting ServerCertificateValidationCallback to NULL.
VERBOSE: closing connection.
VERBOSE: ret code [200]
VERBOSE: ret resp [Command successfully executed.]
VERBOSE: OK, the LM Server is up and running
True
```

Kemp Zero Trust Access Gateway Package

The latest Kemp ZTAG Package can be found on the Support Website.

https://support.kemptechnologies.com/hc/en-us/categories/200141477-Downloads

Unzip the ZTAG Package.

The package contains the following files:

- ZTAG-Policy-Builder.ps1
- Config_AuthHeader.xml
- Config_SourceIP.xml
- Config_SteeringGroup.xml
- Config_Trusted_Zones.xml

Policy Configuration Files

The Zero Trust Policy Builder currently supports four (4) different use cases. Each is defined within a sample configuration XML file. These configuration files determine the state of the environment which is being secured.

Config_AuthHeader.xml supports the Authentication Header/Method/SourceIP use case
Config_SourceIP.xml support the Source IP/Method/Path use case
Config_SteeringGroup.xml supports the SteeringGroup/Path/SourceIP use case
Config_Trusted_Zones.xml supports the Trusted/ Untrusted Zone use case

> It is recommended that Notepad++ or some other XML aware application is used when working with the ZTAG configuration files.

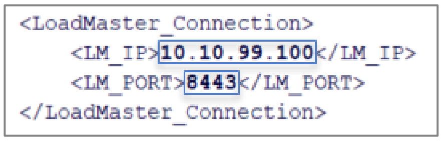
Open the desired sample configuration file. The XML files contain similar sections for the configuration of the Virtual Service that will be used to publish and secure the application/workload. Policy specific sections will be unique based on the use case.

SourceIP/Method/Path Use Case

Open the Config_SourceIP.xml file in Notepad++ or preferred application.

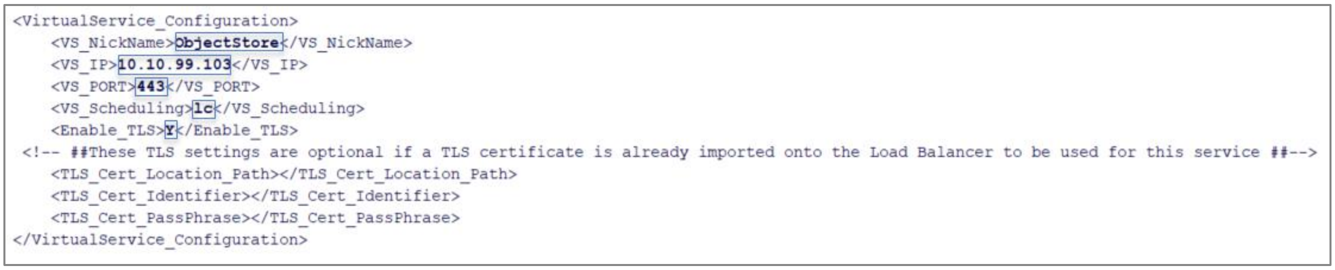
The ZTAG configuration sections for this use case are:

- LoadMaster_Connection
- VirtualService_Configration
- RealServer_Configuration
- RealServer_List
- Identify_Networks
- Zero_Trust_Access_Gateway_Policies
- Backup_Options
- Logging_Options



```
<LoadMaster_Connection>
    <LM_IP>10.10.99.100</LM_IP>
    <LM_PORT>8443</LM_PORT>
</LoadMaster_Connection>
```

1. Modify the LoadMaster connection settings for the LoadMaster or ECS Connection Manager:
    - The LoadMaster or ECS Connection Manager IP Address
    - The LoadMaster or ECS Connection Manager TCP Port



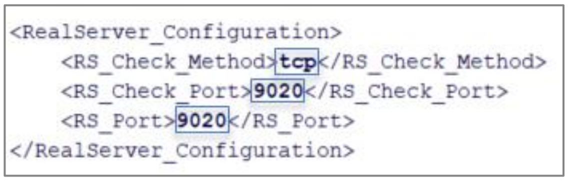
```
<VirtualService_Configuration>
    <VS_NickName>ObjectStore</VS_NickName>
    <VS_IP>10.10.99.103</VS_IP>
    <VS_PORT>443</VS_PORT>
    <VS_Scheduling>lc</VS_Scheduling>
    <Enable_TLS>Y</Enable_TLS>
 <!-- ##These TLS settings are optional if a TLS certificate is already imported onto the Load Balancer to be used for this service ##-->
    <TLS_Cert_Location_Path></TLS_Cert_Location_Path>
    <TLS_Cert_Identifier></TLS_Cert_Identifier>
    <TLS_Cert_PassPhrase></TLS_Cert_PassPhrase>
</VirtualService_Configuration>
```

2. Modify the Virtual Service configuration with settings based on workload requirements.
    - A Nickname (friendly name) to identify the workload being published
    - A Virtual IP Address to publish the workload
    - A Scheduling Method on how the distribution of the traffic to back-end systems should occur.
        - rr = round robin
        - wrr = weighted round robin

    - lc = least connection
    - wlc = weighted least connection
    - fixed = fixed weighting
    - adaptive = resource based (adaptive)
    - sh = source IP hash
    - dl = weighted response time
    - sdn-adaptive = resource based (SDN adaptive)
    - uhash = URL hash
- Select whether SSL/TLS Acceleration should be enabled on the Virtual Service.
    - Y
    - N

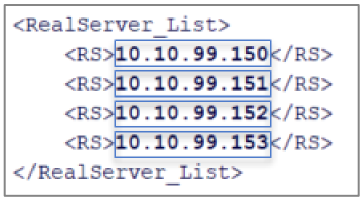
Optional – If a certificate is present on the LoadMaster/ ECS Connection Manager a prompt will be provided to select which certificate should be used in the configuration. A certificate can be uploaded and applied by entering the following parameters

- Path/ location to the certificate file (PFX)
- A friendly name or identifier for the certificate
- The passphrase for importing the certificate



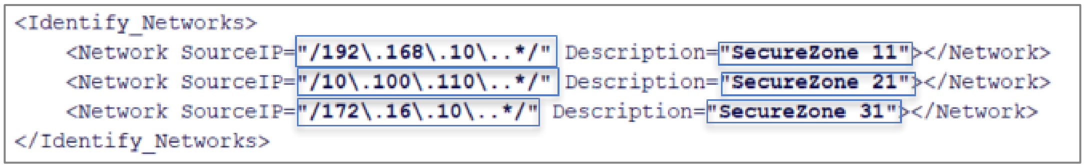
```
<RealServer_Configuration>
    <RS_Check_Method>tcp</RS_Check_Method>
    <RS_Check_Port>9020</RS_Check_Port>
    <RS_Port>9020</RS_Port>
</RealServer_Configuration>
```

3. Modify the Real Server configuration with settings based on workload requirements.
   Real Server Check Method
    - https
    - http
    - tcp



```
<RealServer_List>
    <RS>10.10.99.150</RS>
    <RS>10.10.99.151</RS>
    <RS>10.10.99.152</RS>
    <RS>10.10.99.153</RS>
</RealServer_List>
```

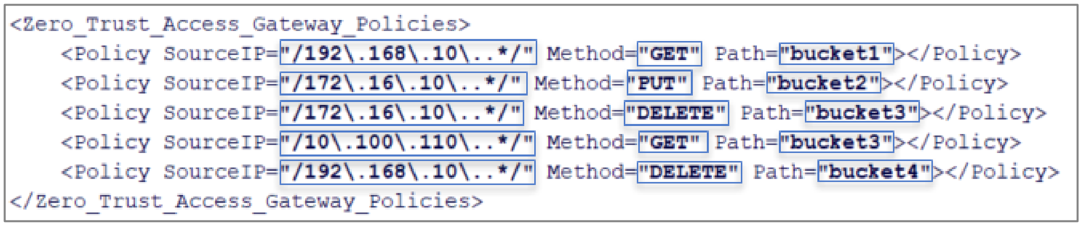
4. Modify the Real Server list with IP Address or FQDN of the back-end systems being published. Lines can be removed or added based on the number of Real Servers in the environment.



```
<Identify_Networks>
    <Network SourceIP="/192\.168\.10\..*/" Description="SecureZone 11"></Network>
    <Network SourceIP="/10\.100\.110\..*/" Description="SecureZone 21"></Network>
    <Network SourceIP="/172\.16\.10\..*/" Description="SecureZone 31"></Network>
</Identify_Networks>
```

5. The SourceIP/Method/Path use case identifies where the traffic originates from based on IP Address. This section defines the networks and description for each within an environment.

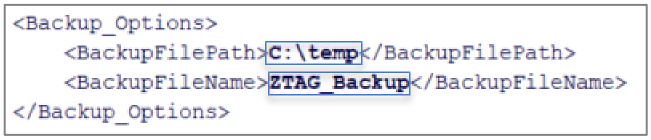
- Source IP Address using Regular Expression (RegEx) to identify the networks in the environment.
- Description (friendly name) of the networks in the environment.



```
<Zero_Trust_Access_Gateway_Policies>
    <Policy SourceIP="/192\.168\.10\..*/" Method="GET" Path="bucket1"></Policy>
    <Policy SourceIP="/172\.16\.10\..*/" Method="PUT" Path="bucket2"></Policy>
    <Policy SourceIP="/172\.16\.10\..*/" Method="DELETE" Path="bucket3"></Policy>
    <Policy SourceIP="/10\.100\.110\..*/" Method="GET" Path="bucket3"></Policy>
    <Policy SourceIP="/192\.168\.10\..*/" Method="DELETE" Path="bucket4"></Policy>
</Zero_Trust_Access_Gateway_Policies>
```

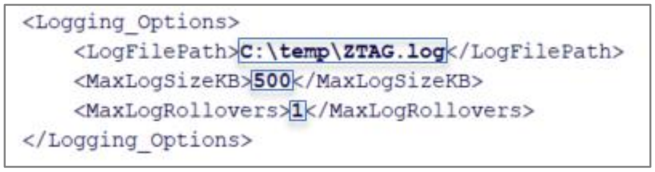
6. The policy section is where the security settings are configured. Lines can be added or removed depending on the number of rules that should be applied in the policy.
    - Source IP Address to apply the security policy to.
    - The method that should be permitted for the defined path/ bucket.
        - GET
        - PUT
        - DELETE
        - POST
    - The path or bucket to apply the security policy to.

Any Source IP Addresses that are applied here **must** be identified in the Identify_Network section above.



```
<Backup_Options>
    <BackupFilePath>C:\temp</BackupFilePath>
    <BackupFileName>ZTAG_Backup</BackupFileName>
</Backup_Options>
```

7. Optional - During each run of the Zero Trust Policy Builder, the option to take a backup before any changes are applied is presented. These options are used to define the name and where the backup should be stored. A date and time stamp will also be included in the backup file name.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Backup file name – Used to identify the backup being taken



```
<Logging_Options>
    <LogFilePath>C:\temp\ZTAG.log</LogFilePath>
    <MaxLogSizeKB>500</MaxLogSizeKB>
    <MaxLogRollovers>1</MaxLogRollovers>
</Logging_Options>
```

8. Logging is generated for each run of the Zero Trust Policy Builder. These settings will provide the location for the log files and how much of the disk can be utilized to store files.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Max Log Size – The maximum size of each of the log files.

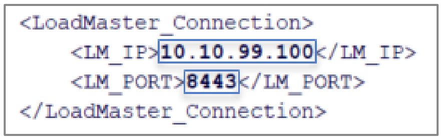
Max Log Rollovers – The maximum number of log file rollovers to allow. Setting of 2 rollover files and 500KB maximum size will allow for 1000KB of storage to be used on the system running the Zero Trust Policy Builder.

AuthHeader/Method/SourceIP Use Case

Open the Config_AuthHeader.xml file in Notepad++ or preferred application.

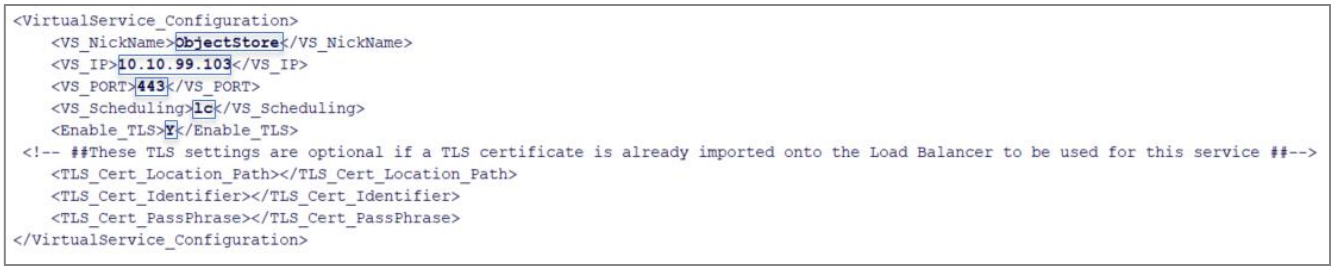
The ZTAG configuration sections for this use case are:

- LoadMaster_Connection
- VirtualService_Configration
- RealServer_Configuration
- RealServer_List
- Identify_Users
- Zero_Trust_Access_Gateway_Policies
- Backup_Options
- Logging_Options



```
<LoadMaster_Connection>
    <LM_IP>10.10.99.100</LM_IP>
    <LM_PORT>8443</LM_PORT>
</LoadMaster_Connection>
```

1. Modify the LoadMaster connection settings for the LoadMaster or ECS Connection Manager:
   - The LoadMaster or ECS Connection Manager IP Address
   - The LoadMaster or ECS Connection Manager TCP Port



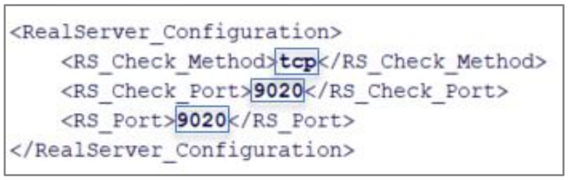
```
<VirtualService_Configuration>
    <VS_NickName>ObjectStore</VS_NickName>
    <VS_IP>10.10.99.103</VS_IP>
    <VS_PORT>443</VS_PORT>
    <VS_Scheduling>lc</VS_Scheduling>
    <Enable_TLS>Y</Enable_TLS>
 <!-- ##These TLS settings are optional if a TLS certificate is already imported onto the Load Balancer to be used for this service ##-->
    <TLS_Cert_Location_Path></TLS_Cert_Location_Path>
    <TLS_Cert_Identifier></TLS_Cert_Identifier>
    <TLS_Cert_PassPhrase></TLS_Cert_PassPhrase>
</VirtualService_Configuration>
```

2. Modify the Virtual Service configuration with settings based on workload requirements.
   - A Nickname (friendly name) to identify the workload being published
   - A Virtual IP Address to publish the workload
   - A Scheduling Method on how the distribution of the traffic to back-end systems should occur.
     - rr = round robin
     - wrr = weighted round robin
     - lc = least connection
     - wlc = weighted least connection
     - fixed = fixed weighting

    - adaptive = resource based (adaptive)
    - sh = source IP hash
    - dl = weighted response time
    - sdn-adaptive = resource based (SDN adaptive)
    - uhash = URL hash
- Select whether SSL/TLS Acceleration should be enabled on the Virtual Service.
    - Y
    - N

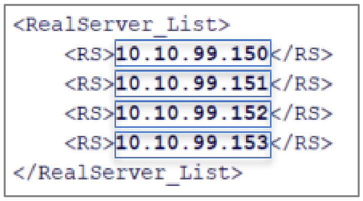
Optional – If a certificate is present on the LoadMaster/ ECS Connection Manager a prompt will be provided to select which certificate should be used in the configuration. A certificate can be uploaded and applied by using entering the following parameters

- Path/ location to the certificate file (PFX)
- A friendly name or identifier for the certificate
- The passphrase for importing the certificate



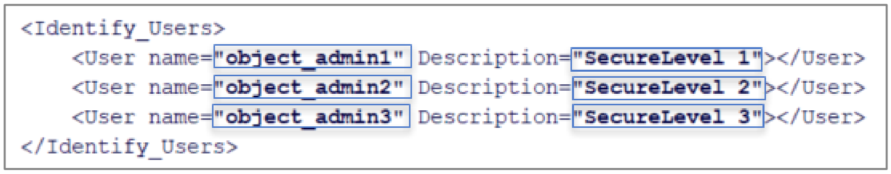
```
<RealServer_Configuration>
    <RS_Check_Method>tcp</RS_Check_Method>
    <RS_Check_Port>9020</RS_Check_Port>
    <RS_Port>9020</RS_Port>
</RealServer_Configuration>
```

3. Modify the Real Server configuration with settings based on workload requirements.
   Real Server Check Method
    - https
    - http
    - tcp



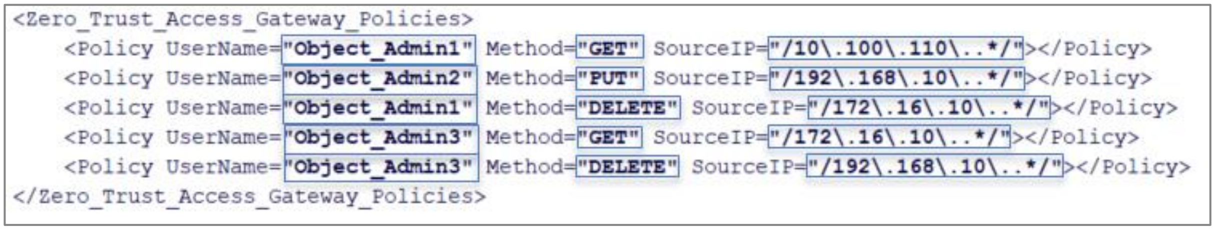
```
<RealServer_List>
    <RS>10.10.99.150</RS>
    <RS>10.10.99.151</RS>
    <RS>10.10.99.152</RS>
    <RS>10.10.99.153</RS>
</RealServer_List>
```

4. Modify the Real Server list with IP Address or FQDN of the back-end systems being published. Lines can be removed or added based on the number of Real Servers in the environment.



```
<Identify_Users>
    <User name="object_admin1" Description="SecureLevel 1"></User>
    <User name="object_admin2" Description="SecureLevel 2"></User>
    <User name="object_admin3" Description="SecureLevel 3"></User>
</Identify_Users>
```

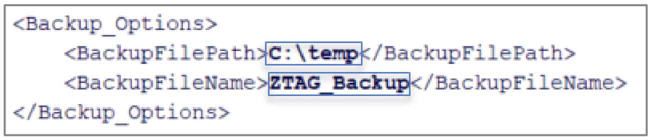
5. The AuthHeader/Method/SourceIP use case identifies who is accessing the workload with the user account that appears in the Authentication Header. This section defines the user accounts or Object IDs and description for each within an environment.
    - Username to identify the account or object ID in the environment.
    - Description (friendly name) of the user account in the environment.



```
<Zero_Trust_Access_Gateway_Policies>
    <Policy UserName="Object_Admin1" Method="GET" SourceIP="/10\.100\.110\..*/"></Policy>
    <Policy UserName="Object_Admin2" Method="PUT" SourceIP="/192\.168\.10\..*/"></Policy>
    <Policy UserName="Object_Admin1" Method="DELETE" SourceIP="/172\.16\.10\..*/"></Policy>
    <Policy UserName="Object_Admin3" Method="GET" SourceIP="/172\.16\.10\..*/"></Policy>
    <Policy UserName="Object_Admin3" Method="DELETE" SourceIP="/192\.168\.10\..*/"></Policy>
</Zero_Trust_Access_Gateway_Policies>
```

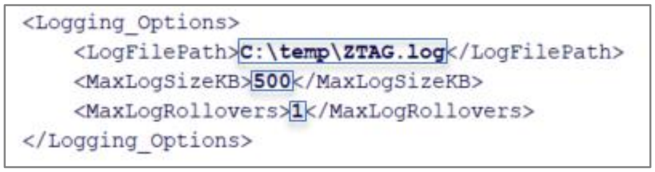
6. The policy section is where the security settings are configured. Lines can be added or removed depending on the number of rules that should be applied in the policy.
    - Username to apply the security policy to.
    - The method that should be permitted for the defined path/ bucket.
        - GET
        - PUT
        - DELETE
        - POST
    - The source IP Address as to where the traffic originates from.

Any Usernames that are applied here **must** be identified in the Identify_Users section above.



```
<Backup_Options>
    <BackupFilePath>C:\temp</BackupFilePath>
    <BackupFileName>ZTAG_Backup</BackupFileName>
</Backup_Options>
```

7. Optional - During each run of the Zero Trust Policy Builder, the option to take a backup before any changes are applied is presented. These options are used to define the name and where the backup should be stored. A date and time stamp will also be included in the backup file name.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Backup file name – Used to identify the backup being taken



```
<Logging_Options>
    <LogFilePath>C:\temp\ZTAG.log</LogFilePath>
    <MaxLogSizeKB>500</MaxLogSizeKB>
    <MaxLogRollovers>1</MaxLogRollovers>
</Logging_Options>
```

8. Logging is generated for each run of the Zero Trust Policy Builder. These settings will provide the location for the log files and how much of the disk can be utilized to store files.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Max Log Size – The maximum size of each of the log files.

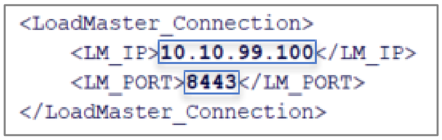
    Max Log Rollovers – The maximum number of log file rollovers to allow. Setting of 2 rollover files and 500KB maximum size will allow for 1000KB of storage to be used on the system running the Zero Trust Policy Builder.

SteeringGroup/ SourceIP/Path Use Case

Open the Config_SteeringGroup.xml file in Notepad++ or preferred application.

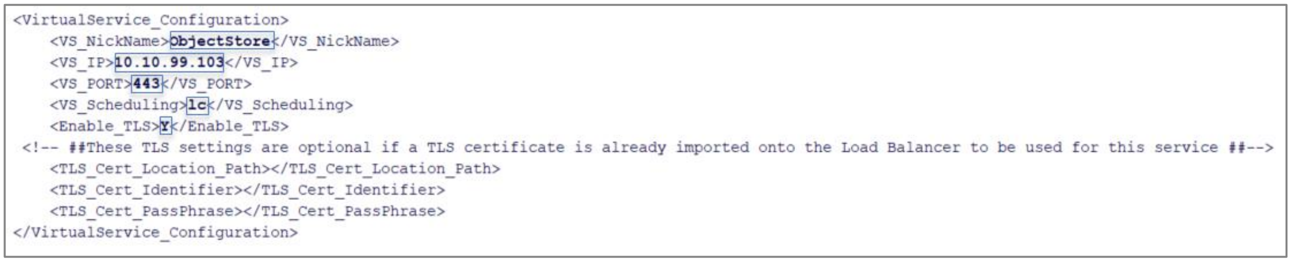
The ZTAG configuration sections for this use case are:

- LoadMaster_Connection
- VirtualService_Configration
- RealServer_Configuration
- RealServer_List
- Identify_Groups
- Zero_Trust_Access_Gateway_Policies
- Backup_Options
- Logging_Options



```
<LoadMaster_Connection>
    <LM_IP>10.10.99.100</LM_IP>
    <LM_PORT>8443</LM_PORT>
</LoadMaster_Connection>
```

1. Modify the LoadMaster connection settings for the LoadMaster or ECS Connection Manager:
   - The LoadMaster or ECS Connection Manager IP Address
   - The LoadMaster or ECS Connection Manager TCP Port



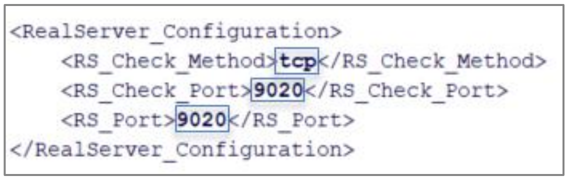
```
<VirtualService_Configuration>
    <VS_NickName>ObjectStore</VS_NickName>
    <VS_IP>10.10.99.103</VS_IP>
    <VS_PORT>443</VS_PORT>
    <VS_Scheduling>lc</VS_Scheduling>
    <Enable_TLS>Y</Enable_TLS>
 <!-- ##These TLS settings are optional if a TLS certificate is already imported onto the Load Balancer to be used for this service ##-->
    <TLS_Cert_Location_Path></TLS_Cert_Location_Path>
    <TLS_Cert_Identifier></TLS_Cert_Identifier>
    <TLS_Cert_PassPhrase></TLS_Cert_PassPhrase>
</VirtualService_Configuration>
```

2. Modify the Virtual Service configuration with settings based on workload requirements.
   - A Nickname (friendly name) to identify the workload being published
   - A Virtual IP Address to publish the workload
   - A Scheduling Method on how the distribution of the traffic to back-end systems should occur.
     - rr = round robin
     - wrr = weighted round robin
     - lc = least connection
     - wlc = weighted least connection
     - fixed = fixed weighting
     - adaptive = resource based (adaptive)
     - sh = source IP hash
     - dl = weighted response time
     - sdn-adaptive = resource based (SDN adaptive)
     - uhash = URL hash

- Select whether SSL/TLS Acceleration should be enabled on the Virtual Service.
  - Y
  - N

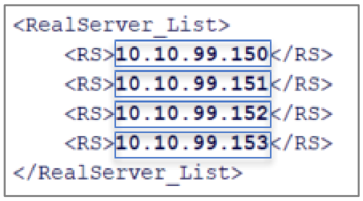
Optional – If a certificate is present on the LoadMaster/ ECS Connection Manager a prompt will be provided to select which certificate should be used in the configuration. A certificate can be uploaded and applied by using entering the following parameters

- Path/ location to the certificate file (PFX)
- A friendly name or identifier for the certificate
- The passphrase for importing the certificate



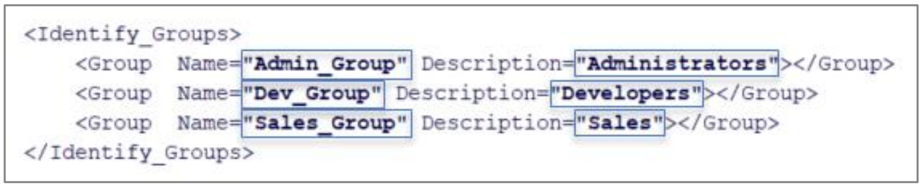
```
<RealServer_Configuration>
    <RS_Check_Method>tcp</RS_Check_Method>
    <RS_Check_Port>9020</RS_Check_Port>
    <RS_Port>9020</RS_Port>
</RealServer_Configuration>
```

3. Modify the Real Server configuration with settings based on workload requirements.
   Real Server Check Method
   - https
   - http
   - tcp



```
<RealServer_List>
    <RS>10.10.99.150</RS>
    <RS>10.10.99.151</RS>
    <RS>10.10.99.152</RS>
    <RS>10.10.99.153</RS>
</RealServer_List>
```

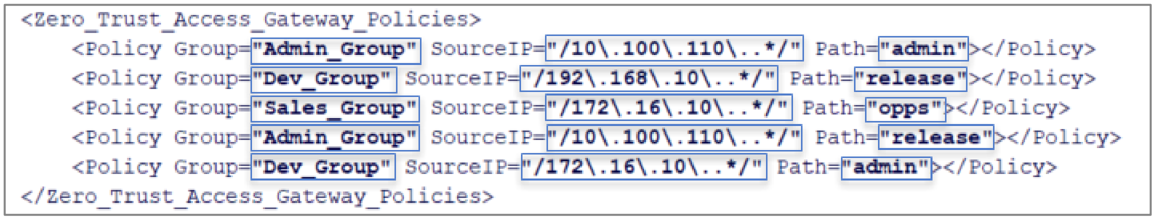
4. Modify the Real Server list with IP Address or FQDN of the back-end systems being published. Lines can be removed or added based on the number of Real Servers in the environment.



```
<Identify_Groups>
    <Group  Name="Admin_Group" Description="Administrators"></Group>
    <Group  Name="Dev_Group" Description="Developers"></Group>
    <Group  Name="Sales_Group" Description="Sales"></Group>
</Identify_Groups>
```

5. The SteeringGroup/SourceIP/Path use case identifies who is accessing the workload with the Active Directory Group they are a member of. This section defines the Active Directory Groups and description for each within an environment.
   - Active Directory Group Names used to secure the environment.
   - Description (friendly name) of the AD Groups in the environment.

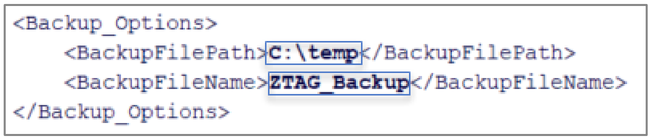
If using the Steering Group Use Case, the Edge Security Pack Single Sign On domain must be configured prior to running the ZTAG Policy Builder



```
<Zero_Trust_Access_Gateway_Policies>
    <Policy Group="Admin_Group" SourceIP="/10\.100\.110\..*/" Path="admin"></Policy>
    <Policy Group="Dev_Group" SourceIP="/192\.168\.10\..*/" Path="release"></Policy>
    <Policy Group="Sales_Group" SourceIP="/172\.16\.10\..*/" Path="opps"></Policy>
    <Policy Group="Admin_Group" SourceIP="/10\.100\.110\..*/" Path="release"></Policy>
    <Policy Group="Dev_Group" SourceIP="/172\.16\.10\..*/" Path="admin"></Policy>
</Zero_Trust_Access_Gateway_Policies>
```

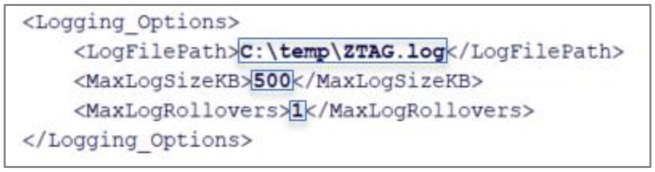
6. The policy section is where the security settings are configured. Lines can be added or removed depending on the number of rules that should be applied in the policy.
    - Username to apply the security policy to.
    - The source IP Address as to where the traffic originates from.
    - The path of the application that the AD group should have access to.

Any Groups that are applied here **must** be identified in the Identify_Groups section above.



```
<Backup_Options>
    <BackupFilePath>C:\temp</BackupFilePath>
    <BackupFileName>ZTAG_Backup</BackupFileName>
</Backup_Options>
```

7. Optional - During each run of the Zero Trust Policy Builder, the option to take a backup before any changes are applied is presented. These options are used to define the name and where the backup should be stored. A date and time stamp will also be included in the backup file name.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Backup file name – Used to identify the backup being taken



```
<Logging_Options>
    <LogFilePath>C:\temp\ZTAG.log</LogFilePath>
    <MaxLogSizeKB>500</MaxLogSizeKB>
    <MaxLogRollovers>1</MaxLogRollovers>
</Logging_Options>
```

8. Logging is generated for each run of the Zero Trust Policy Builder. These settings will provide the location for the log files and how much of the disk can be utilized to store files.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Max Log Size – The maximum size of each of the log files.

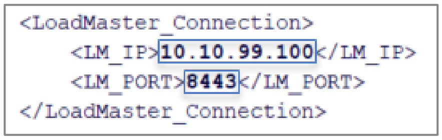
    Max Log Rollovers – The maximum number of log file rollovers to allow. Setting of 2 rollover files and 500KB maximum size will allow for 1000KB of storage to be used on the system running the Zero Trust Policy Builder.

Trusted/Untrusted Zone Use Case

Open the Config_Trusted_Zones.xml file in Notepad++ or preferred application.

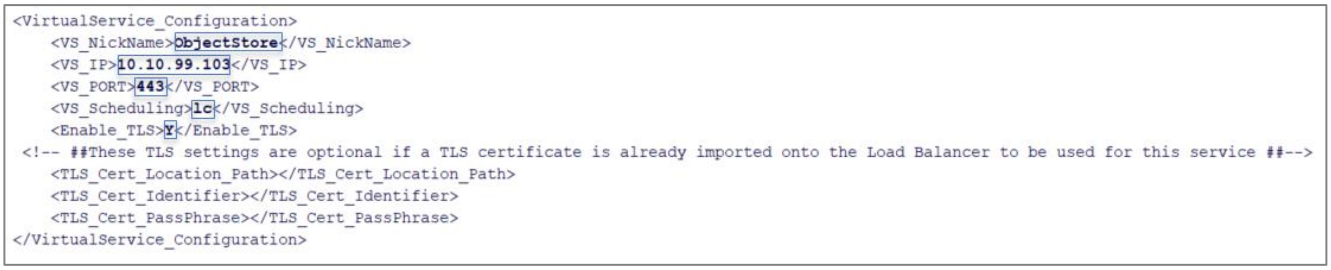
The ZTAG configuration sections for this use case are:

- LoadMaster_Connection
- VirtualService_Configration
- RealServer_Configuration
- RealServer_List
- Zero_Trust_Access_Gateway_Trusted_Zones
- PermitedGroups_Trusted_Zone
- PermitedGroups_UnTrusted_Zone
- Backup_Options
- Logging_Options



```
<LoadMaster_Connection>
    <LM_IP>10.10.99.100</LM_IP>
    <LM_PORT>8443</LM_PORT>
</LoadMaster_Connection>
```

1. Modify the LoadMaster connection settings for the LoadMaster or ECS Connection Manager:
    - The LoadMaster or ECS Connection Manager IP Address
    - The LoadMaster or ECS Connection Manager TCP Port

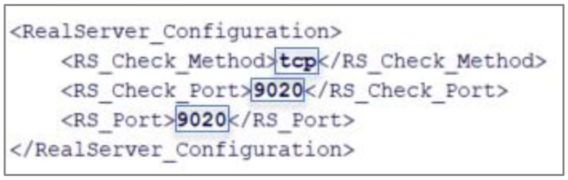


```
<VirtualService_Configuration>
    <VS_NickName>ObjectStore</VS_NickName>
    <VS_IP>10.10.99.103</VS_IP>
    <VS_PORT>443</VS_PORT>
    <VS_Scheduling>lc</VS_Scheduling>
    <Enable_TLS>Y</Enable_TLS>
 <!-- ##These TLS settings are optional if a TLS certificate is already imported onto the Load Balancer to be used for this service ##-->
    <TLS_Cert_Location_Path></TLS_Cert_Location_Path>
    <TLS_Cert_Identifier></TLS_Cert_Identifier>
    <TLS_Cert_PassPhrase></TLS_Cert_PassPhrase>
</VirtualService_Configuration>
```

2. Modify the Virtual Service configuration with settings based on workload requirements.
    - A Nickname (friendly name) to identify the workload being published
    - A Virtual IP Address to publish the workload
    - A Scheduling Method on how the distribution of the traffic to back-end systems should occur.
        - rr = round robin
        - wrr = weighted round robin
        - lc = least connection
        - wlc = weighted least connection
        - fixed = fixed weighting
        - adaptive = resource based (adaptive)
        - sh = source IP hash
        - dl = weighted response time
        - sdn-adaptive = resource based (SDN adaptive)
        - uhash = URL hash
    - Select whether SSL/TLS Acceleration should be enabled on the Virtual Service.
        - Y
        - N

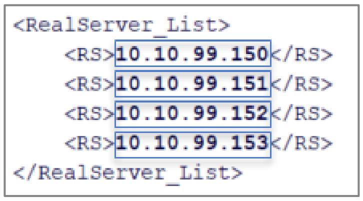
Optional – If a certificate is present on the LoadMaster/ ECS Connection Manager a prompt will be provided to select which certificate should be used in the configuration. A certificate can be uploaded and applied by using entering the following parameters

- Path/ location to the certificate file (PFX)
- A friendly name or identifier for the certificate
- The passphrase for importing the certificate



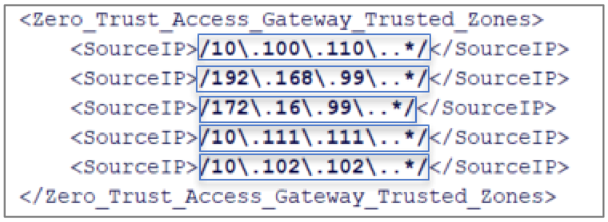
```
<RealServer_Configuration>
    <RS_Check_Method>tcp</RS_Check_Method>
    <RS_Check_Port>9020</RS_Check_Port>
    <RS_Port>9020</RS_Port>
</RealServer_Configuration>
```

3. Modify the Real Server configuration with settings based on workload requirements.
   Real Server Check Method
   - https
   - http
   - tcp



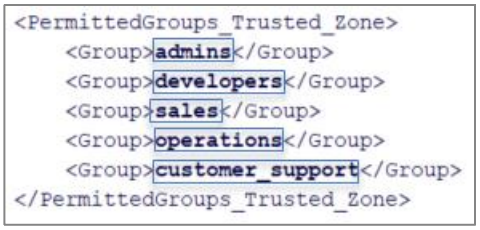
```
<RealServer_List>
    <RS>10.10.99.150</RS>
    <RS>10.10.99.151</RS>
    <RS>10.10.99.152</RS>
    <RS>10.10.99.153</RS>
</RealServer_List>
```

4. Modify the Real Server list with IP Address or FQDN of the back-end systems being published. Lines can be removed or added based on the number of Real Servers in the environment.



```
<Zero_Trust_Access_Gateway_Trusted_Zones>
    <SourceIP>/10\.100\.110\..*/</SourceIP>
    <SourceIP>/192\.168\.99\..*/</SourceIP>
    <SourceIP>/172\.16\.99\..*/</SourceIP>
    <SourceIP>/10\.111\.111\..*/</SourceIP>
    <SourceIP>/10\.102\.102\..*/</SourceIP>
</Zero_Trust_Access_Gateway_Trusted_Zones>
```

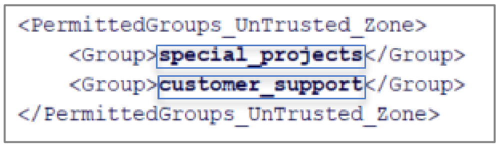
5. The Trusted Zone section identifies the known networks in the environment. These are the networks where Multi Factor Authentication will not be required.
   - The Source IP will be the network address using Regular Expression (RegEx) that clients will be connecting from. Lines can be added or removed depending on the number of known networks in the environment.



```
<PermittedGroups_Trusted_Zone>
    <Group>admins</Group>
    <Group>developers</Group>
    <Group>sales</Group>
    <Group>operations</Group>
    <Group>customer_support</Group>
</PermittedGroups_Trusted_Zone>
```

6. The Permitted Groups Trusted Zone section is where the Active Directory groups are defined. Members of these groups should be granted access to the application if they are connecting to the application from a network that is listed in the Trusted Zones section above. Lines can be added or removed depending on the number of groups that need access to the application.
    - Group – Active Directory group name

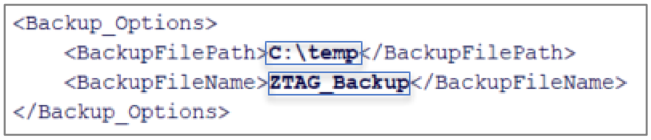
If using the Trusted/ Un-Trusted Use Case, the Edge Security Pack Single Sign On domain for the trusted zone must be configured prior to running the ZTAG Policy Builder



```
<PermittedGroups_UnTrusted_Zone>
    <Group>special_projects</Group>
    <Group>customer_support</Group>
</PermittedGroups_UnTrusted_Zone>
```

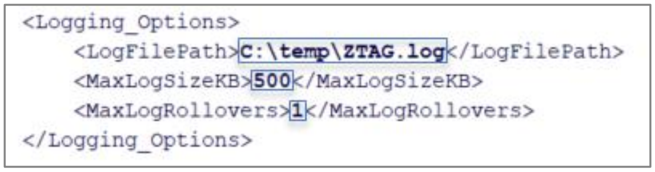
7. The Permitted Groups UnTrusted Zone section is where the Active Directory groups are defined. Members of these groups should be granted access to the application if they are connecting to the application from a network that is NOT listed in the Trusted Zone section above. If the same group should have access regardless of network they are connected to, the group names should be listed in both sections. Lines can be added or removed depending on the number of groups that need access to the application.
    - Group – Active Directory group name

If using the Trusted/ Un-Trusted Use Case, the Edge Security Pack Single Sign On domain for the un-trusted zone must be configured prior to running the ZTAG Policy Builder



```
<Backup_Options>
    <BackupFilePath>C:\temp</BackupFilePath>
    <BackupFileName>ZTAG_Backup</BackupFileName>
</Backup_Options>
```

9. Optional - During each run of the Zero Trust Policy Builder, the option to take a backup before any changes are applied is presented. These options are used to define the name and where the backup should be stored. A date and time stamp will also be included in the backup file name.
    - File Path – Ensure the proper permissions are applied to the folder.
    - Backup file name – Used to identify the backup being taken



```
<Logging_Options>
    <LogFilePath>C:\temp\ZTAG.log</LogFilePath>
    <MaxLogSizeKB>500</MaxLogSizeKB>
    <MaxLogRollovers>1</MaxLogRollovers>
</Logging_Options>
```

8. Logging is generated for each run of the Zero Trust Policy Builder. These settings will provide the location for the log files and how much of the disk can be utilized to store files.
    - File Path – Ensure the proper permissions are applied to the folder.

- Max Log Size – The maximum size of each of the log files.

Max Log Rollovers – The maximum number of log file rollovers to allow. Setting of 2 rollover files and 500KB maximum size will allow for 1000KB of storage to be used on the system running the Zero Trust Policy Builder.

Zero Trust Policy Builder script

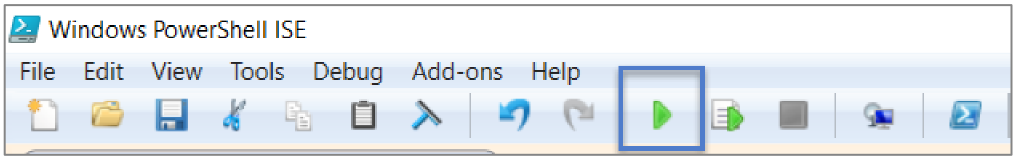
There are two approaches for running the Zero Trust Policy Builder PowerShell script. The PowerShell console and the PowerShell Integrated Scripting Environment (ISE). The interaction with the Zero Trust Policy Builder will be different between these two approaches but the results will be identical. This document will focus on using PowerShell ISE since it provides more user-friendly prompts than the PowerShell Console.

Although some prompts that are presented are common across the different use cases, there are some unique for each.

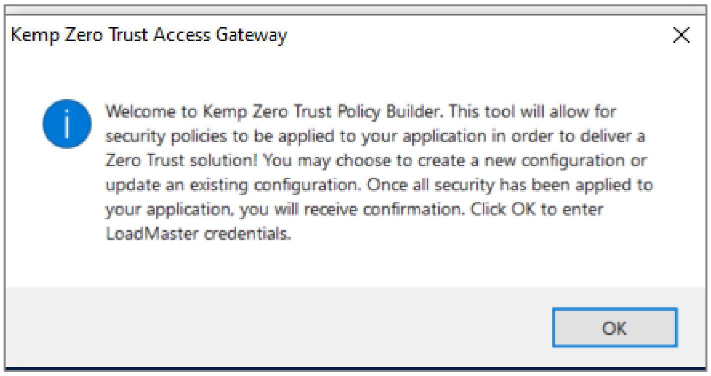
The Zero Trust Policy Builder is a fixed script that should not be modified under any circumstances.

Deploy a new workload

1. Open the ZTAG-Policy-Builder.ps1 script using PowerShell ISE.

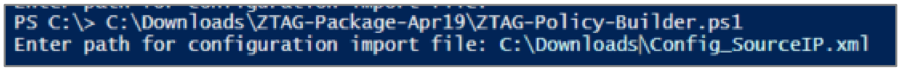


2. Click the Green Arrow to run the ZTAG Policy Builder script.



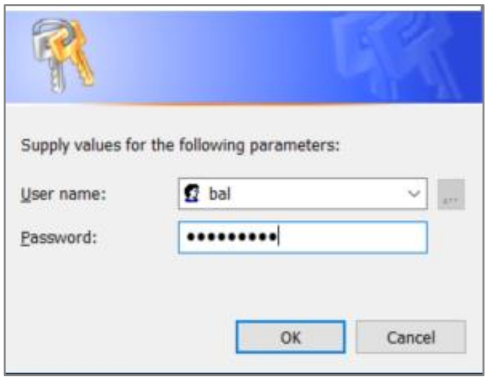
Welcome to Kemp Zero Trust Policy Builder. This tool will allow for security policies to be applied to your application in order to deliver a Zero Trust solution! You may choose to create a new configuration or update an existing configuration. Once all security has been applied to your application, you will receive confirmation. Click OK to enter LoadMaster credentials.

3. Click OK on the Welcome Message.



```
PS C:\> C:\Downloads\ZTAG-Package-Apr19\ZTAG-Policy-Builder.ps1
Enter path for configuration import file: C:\Downloads\Config_SourceIP.xml
```

4. Enter the path to the configuration file that should be used and **Enter**

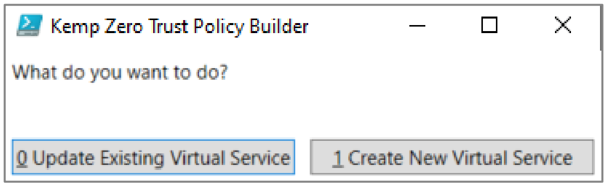


Supply values for the following parameters:

User name: bal

Password: ••••••••••

5. Enter the credentials to authenticate to the LoadMaster or ECS Connection Manager.

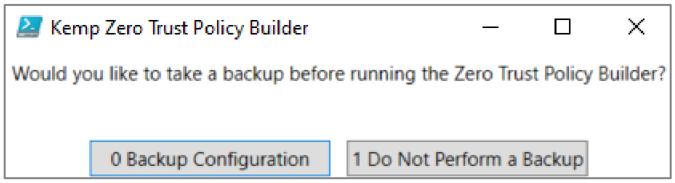


Kemp Zero Trust Policy Builder

What do you want to do?

0 Update Existing Virtual Service
1 Create New Virtual Service

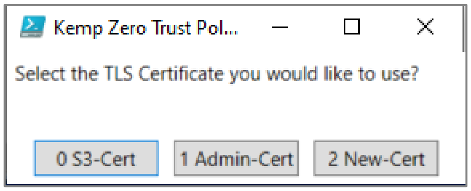
6. Select **Create New Virtual Service**



Kemp Zero Trust Policy Builder

Would you like to take a backup before running the Zero Trust Policy Builder?

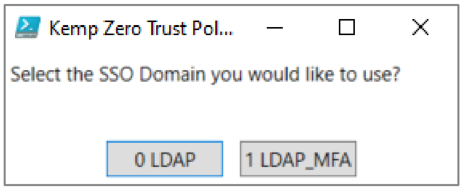
7. Choose whether to perform a backup prior to making any updates on the LoadMaster/ ECS Connection Manager.



Kemp Zero Trust Pol...

Select the TLS Certificate you would like to use?

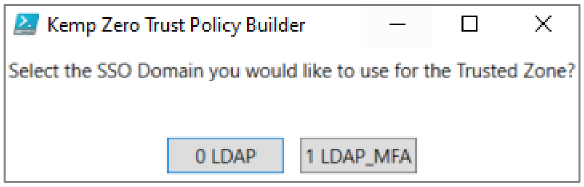
8. If enable TLS was set to “Y” in the configuration file and no parameters were provided to add a new certificate, a prompt to select an existing certificate is provided.



Kemp Zero Trust Pol...

Select the SSO Domain you would like to use?

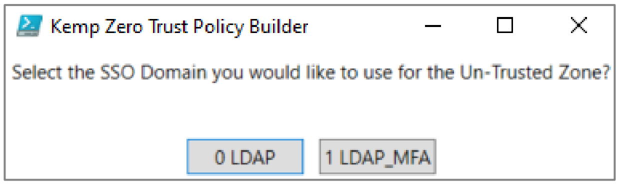
9. **(Steering Group Use Case Only)** – A prompt is presented to select an existing SSO domain to use to pre-authenticate users.



Kemp Zero Trust Policy Builder

Select the SSO Domain you would like to use for the Trusted Zone?

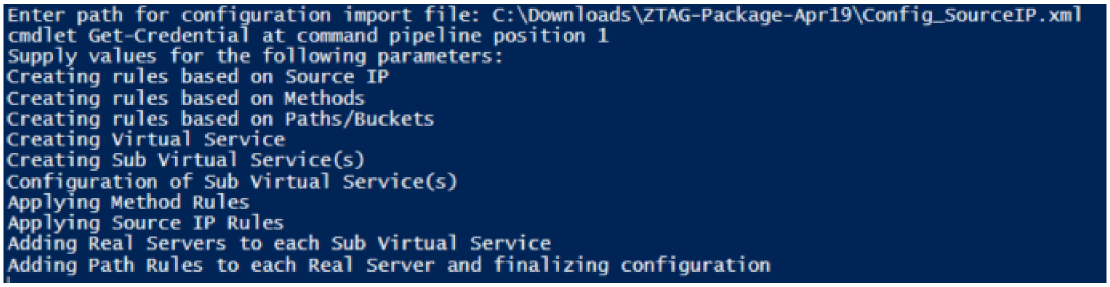
10. **(Trusted/UnTrusted Zone Use Case Only)** – Select the SSO domain to use for known networks within the environment.



Kemp Zero Trust Policy Builder

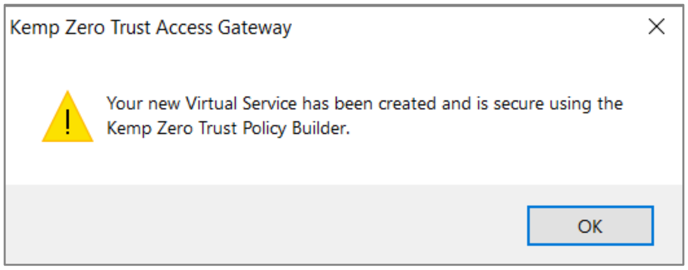
Select the SSO Domain you would like to use for the Un-Trusted Zone?

11. **(Trusted/UnTrusted Zone Use Case Only)** – Select the SSO domain to use for all other networks that do not exist in the environment.



```
Enter path for configuration import file: C:\Downloads\ZTAG-Package-Apr19\Config_SourceIP.xml
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Creating rules based on Source IP
Creating rules based on Methods
Creating rules based on Paths/Buckets
Creating Virtual Service
Creating Sub Virtual Service(s)
Configuration of Sub Virtual Service(s)
Applying Method Rules
Applying Source IP Rules
Adding Real Servers to each Sub Virtual Service
Adding Path Rules to each Real Server and finalizing configuration
```

12. The script steps will be presented as the configuration takes place.



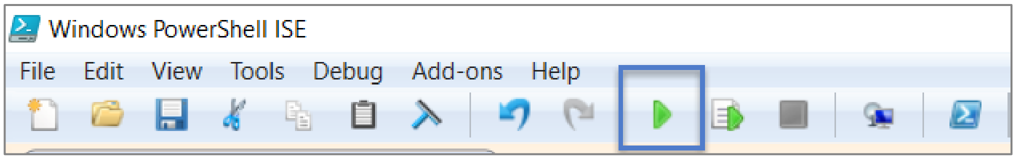
Kemp Zero Trust Access Gateway

Your new Virtual Service has been created and is secure using the Kemp Zero Trust Policy Builder.

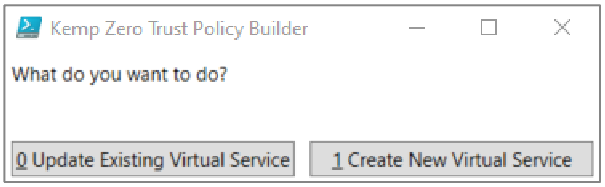
13. A confirmation that the script ran successfully will be presented at completion.

Update an existing workload

The steps to update an existing workload are similar to the steps above other than a few additional prompts.



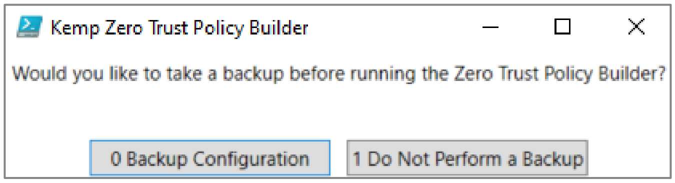
1. Run the script and accept the welcome message


Kemp Zero Trust Policy Builder

What do you want to do?

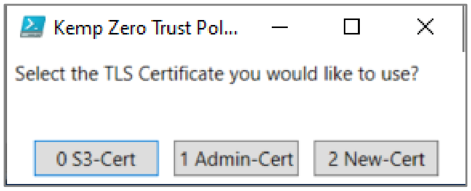
0 Update Existing Virtual Service
1 Create New Virtual Service

2. Select **Update Existing Virtual Service**


Kemp Zero Trust Policy Builder

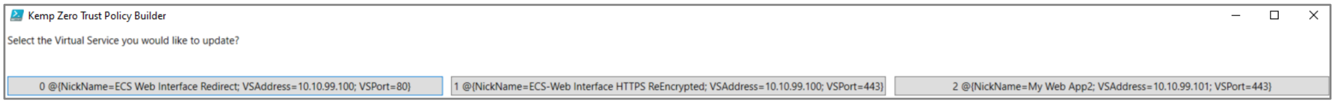
Would you like to take a backup before running the Zero Trust Policy Builder?

3. Choose whether to perform a backup prior to making any updates on the LoadMaster/ ECS Connection Manager.


Kemp Zero Trust Pol...

Select the TLS Certificate you would like to use?

4. If enable TLS was set to “Y” in the configuration file and no parameters were provided to add a new certificate, a prompt to select an existing certificate is provided.


Kemp Zero Trust Policy Builder

Select the Virtual Service you would like to update?

0 @{NickName=ECS Web Interface Redirect; VSAddress=10.10.99.100; VSPort=80}

1 @{NickName=ECS-Web Interface HTTPS ReEncrypted; VSAddress=10.10.99.100; VSPort=443}

2 @{NickName=My Web App2; VSAddress=10.10.99.101; VSPort=443}

5. Select the Virtual Service you would like updated with the changes applied to the configuration file.
6. The remaining prompts will be identical to the steps outlined above.

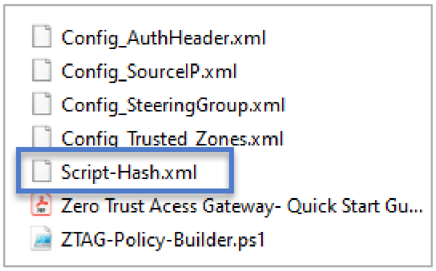
Logging and Troubleshooting

The Zero Trust Policy Builder is developed with several layers of validation prior to running and applying the configuration files. In most cases, the script will display details of a misconfiguration or unsupported policy file and prevent any changes to the load balancer. In the rare instances that a policy is applied and does not depict the desired results, logging is made available to determine the cause.

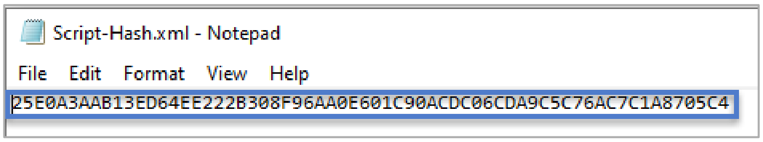
Script Hash

The Zero Trust Policy Builder script is built on PowerShell and should not be modified in anyway. To ensure no changes have been made to the PowerShell script inadvertently, a Hash is provided to verify its uniformity.

1. The expected Hash is delivered as part to the Zero Trust Access Gateway (ZTAG) package. Open the file with the name **Script-Hash.xml** with Notepad or other application that can read XML.

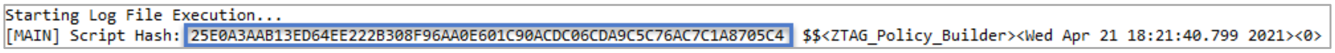


Config_AuthHeader.xml
Config_SourceIP.xml
Config_SteeringGroup.xml
Config_Trusted_Zones.xml
Script-Hash.xml
Zero Trust Acess Gateway- Quick Start Gu...
ZTAG-Policy-Builder.ps1



```
25E0A3AAB13ED64EE222B308F96AA0E601C90ACDC06CDA9C5C76AC7C1A8705C4
```

2. Open the current log file in the specified path and find the line that reads Script-Hash. (There may be several lines depending on the number of times the script was run). The Script-Hash entry in the log must match the hash that is provided in the Script-Hash.xml file.



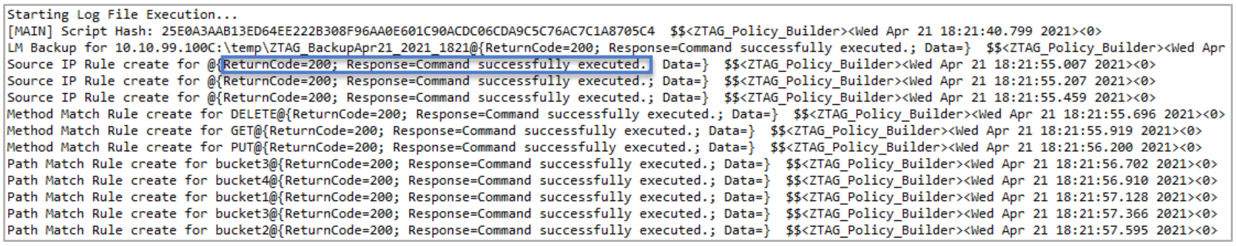
```
Starting Log File Execution...
[MAIN] Script Hash: 25E0A3AAB13ED64EE222B308F96AA0E601C90ACDC06CDA9C5C76AC7C1A8705C4  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:40.799 2021><0>
```

Extended Logging

To help identify any possible errors that may occur during the run of the Zero Trust Policy Builder, extended logging is made available. The log files are written to the path that is specified in the Configuration File (XML).

1. Open the log file and scroll down to the bottom.

2. Each Zero Trust Policy Builder run is separated, and each run starts with **Starting Log File Execution.**
3. Examine the log file for any entry that does NOT equal
   ReturnCode=200; Response=Command successfully executed
4. If a line is found that does not match the response above, there is a description of the action that attempted to take place which can be used for troubleshooting the issue.



```
Starting Log File Execution...
[MAIN] Script Hash: 25E0A3AAB13ED64EE222B308F96AA0E601C90ACDC06CDA9C5C76AC7C1A8705C4  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:40.799 2021><0>
LM Backup for 10.10.99.100C:\temp\ZTAG_BackupApr21_2021_1821@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr
Source IP Rule create for @{ReturnCode=200; Response=Command successfully executed.  Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:55.007 2021><0>
Source IP Rule create for @{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:55.207 2021><0>
Source IP Rule create for @{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:55.459 2021><0>
Method Match Rule create for DELETE@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:55.696 2021><0>
Method Match Rule create for GET@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:55.919 2021><0>
Method Match Rule create for PUT@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:56.200 2021><0>
Path Match Rule create for bucket3@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:56.702 2021><0>
Path Match Rule create for bucket4@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:56.910 2021><0>
Path Match Rule create for bucket1@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:57.128 2021><0>
Path Match Rule create for bucket3@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:57.366 2021><0>
Path Match Rule create for bucket2@{ReturnCode=200; Response=Command successfully executed.; Data=}  $$<ZTAG_Policy_Builder><Wed Apr 21 18:21:57.595 2021><0>
```

Support & Feedback