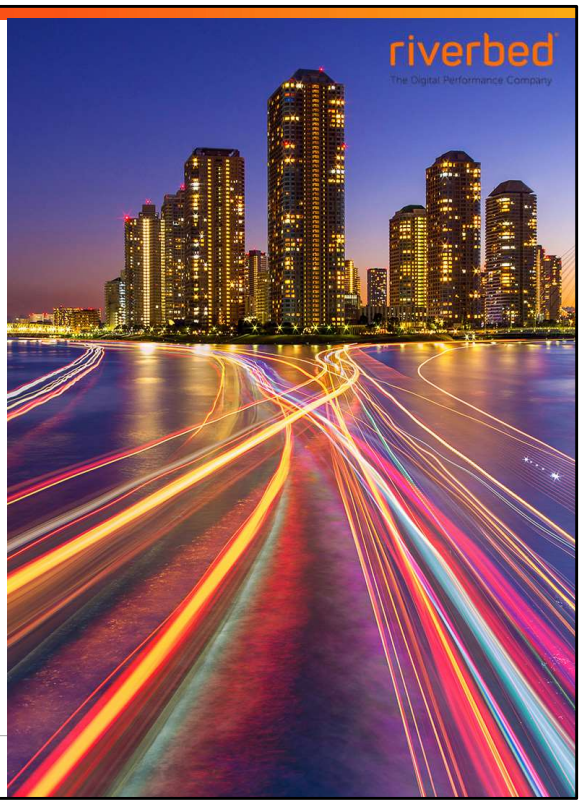
Customize Windows Traffic in an Active Directory Environment

© 2021 Riverbed Technology. All rights reserved.

Learning Objectives

After completing this module, you will be able to:

- Describe Active Directory.
- Integrate SteelHeads with Active Directory.
- Describe NTLM and Kerberos authentication.
- Join a SteelHead to an Active Directory domain.
- Optimize SMB file shares.
- Perform CIFS prepopulation.
- Verify SMB optimization.
- Optimize MS Exchange traffic.



© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Key Points

- Microsoft protocols such as MAPI and SMB are used extensively by the modern business.
- In order for these businesses to work effectively, users need fast email and file sharing, regardless of their location.
- In order to optimize protocols such as encrypted MAPI and SMB-signed connections, the server-side SteelHead needs to be joined to the domain.

© 2020 Riverbed Technology, Inc. All rights reserved.

riverbed 3

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Why is Active Directory Important?

- Active Directory is everywhere.
- Microsoft emails, file shares and authenticated HTTP are essential to the modern business.
- These protocols must perform well to ensure maximum productivity.
- In order to accelerate these protocols, the first step is to add the server-side SteelHead to a Domain.
- In order to understand how to do this it is important to first understand the components of Active Directory and this is what we will cover in this module.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 5

Microsoft introduced Active Directory back in Windows 2000. Since that time, Active Directory has become the backbone of most Windows networks, integrating with nearly everything a user does in a Microsoft environment.

From mapping a share on a corporate network to sending an email via Exchange, Active Directory is everywhere, ensuring that users are authenticated correctly when they login, and also ensuring that they have permissions to perform the actions they need to do.

Now, this is important as sending emails and accessing files are two of the most common actions users perform and both of which are essential in a modern company. It is, therefore, important that these protocols are accelerated to ensure maximum efficiency.

However, due to the overarching importance of Active Directory in nearly all-things Windows, one of the first procedures a SteelHead engineer will have to perform is to add a SteelHead to a Domain.

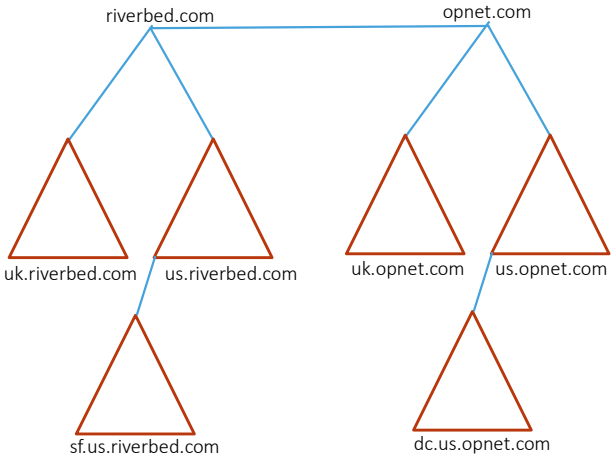
In order to understand the steps and options required we must first look at Active Directory and how it is made up.

© 2021 Riverbed Technology. All rights reserved.

Organizational Structure of Active Directory

Terms – Domain, Tree and Forest

- **Domain** - A collection of objects that share a common database. A user can login to one machine, and then login to another, which is part of the same domain using the same user name and passwords.
- **Tree** - A group of domains that share a contiguous namespace.
- **Forest** - A group of domain trees that do not share a contiguous namespace.



© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 6

Domain: A *Domain* is a collection of objects that share a common database. This means that all of the objects are managed centrally, so a user can login to one machine, and then login to another, which is part of the same domain using the same user name and passwords. For large corporations, this is essential as otherwise these would have to be managed on separate machines, which would be totally un-scalable.

Tree: A *Tree* is a group of domains that share a contiguous namespace. In other words, a tree consists of a parent domain plus a number of child domains whose name reflects that of the parent.

Forest: A *Forest* consists of a group of domain trees that do not share a contiguous namespace. For example, you could have two trees with parents, one with the name *riverbed.com* and another with the name *opnet.com.* Like a Tree there is a two-way transitive trust between the domains within the forest.

The diagram contains two trees, which are part of the same Active Directory forest.

© 2021 Riverbed Technology. All rights reserved.

Key Components of Active Directory

Key Functional Concepts

- **Domain Controllers** - Authenticate all users logging on to the domain in which they are located
- **Schema** - A set of rules that define the classes of objects plus their attributes that can be created
- **Schema Master** - Holds the only copy of the Schema
- **Global Catalog** - A central information database holding data that describes objects throughout the entire Active Directory forest namespace
- **Global Catalog Server** - Locates objects and authenticates users by their user principle name (UPN), e.g., *d.smythe@riverbed.com*
- **PDC Emulator** - Handles operations for legacy client logons
- **Read Only Domain Controller (RODC)** - Non-writeable domain controllers, typically installed in remote offices, holding a limited number of passwords

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 7

Domain Controller (DC): Domain Controllers authenticate all users logging on to the domain in which they are located. They also serve as centers from which you can administer Active Directory. A domain controller stores a complete copy of the schema plus all objects contained in the domain.

Schema: The *schema* is a set of rules which define the classes of objects plus their attributes which can be created in Active Directory. For example, a user object can possess attributes such as password, group membership, etc.

Global Catalog: The *global catalog* is a central information database, holding data which describes objects throughout the entire Active Directory forest namespace. The global catalog is built up by replicating information between all domain controllers in the forest.

Global Catalog Server: By default the first domain controller in a new domain. Its role is to locate objects and authenticate users by their user principle name (UPN), e.g. dave@riverbed.com, and to provide universal group membership information.

PDC emulator: The PDC emulator's job is to handle operations for legacy client logons and directory maintenance, including object and password changes. Importantly, it acts as a time synchronization master, synchronizing the time for the other domain controllers within the domain. One domain controller in every domain holds this role.

Schema Master: Holds the only writable copy of the Active Directory schema.

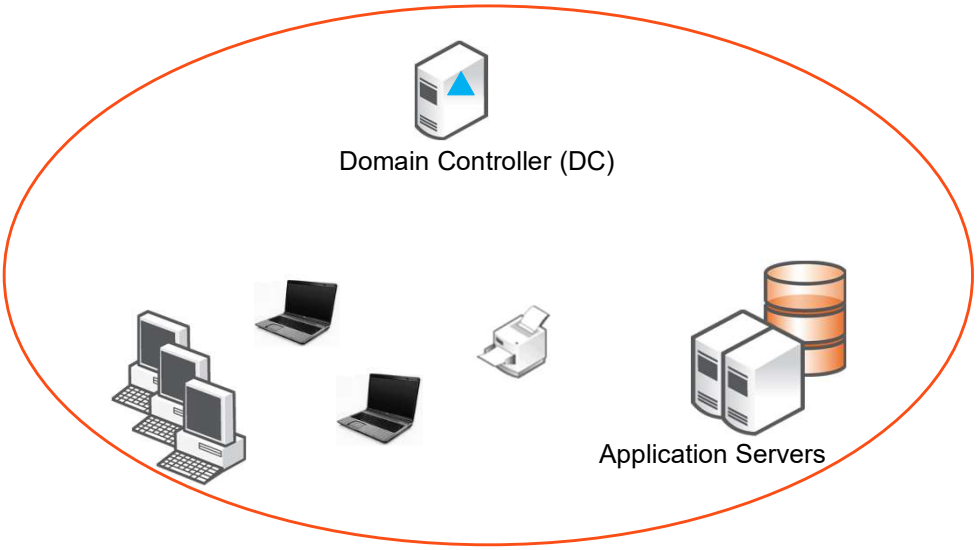
Read-Only Domain Controller (RODC): These are non-writeable domain controllers, typically installed in remote offices where there is a worry about security. Changes that users attempt when connected to an RODC are not made directly. Instead, a writable DC is contacted, and the change is made there once the credentials have been checked. If appropriate, this change is then replicated back across to the RODC. Importantly, RODCs hold very few passwords.

© 2021 Riverbed Technology. All rights reserved.

Domain Relationships

Single Domain

- Only a single domain controller is required.
- All resources that have joined the same domain are subject to the domain permissions and authentications.



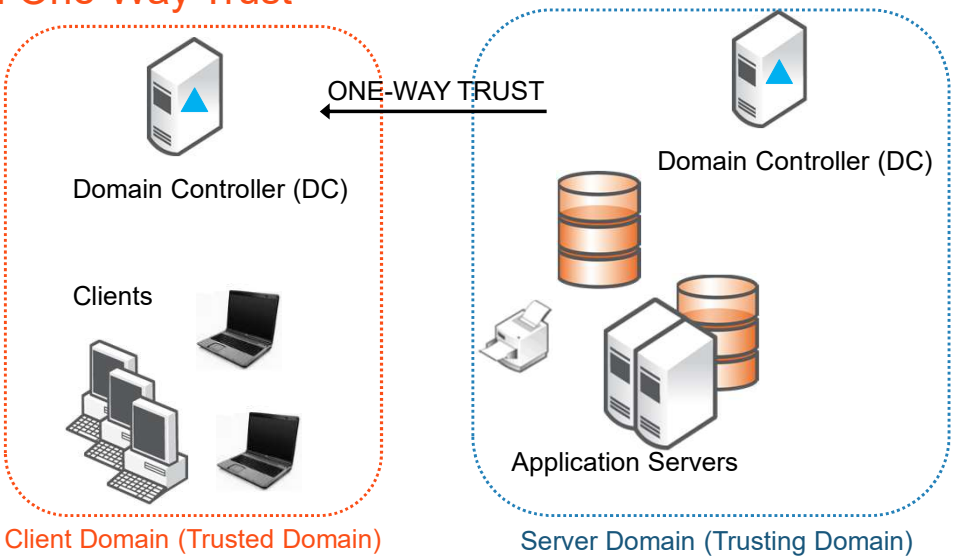
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Domain Relationships

Two Domains and One-Way Trust

- The trust relationship between the domains allows clients and servers to access each other.
- Resources in the client domain are allowed to access resources in the server domain, but not the other way around.



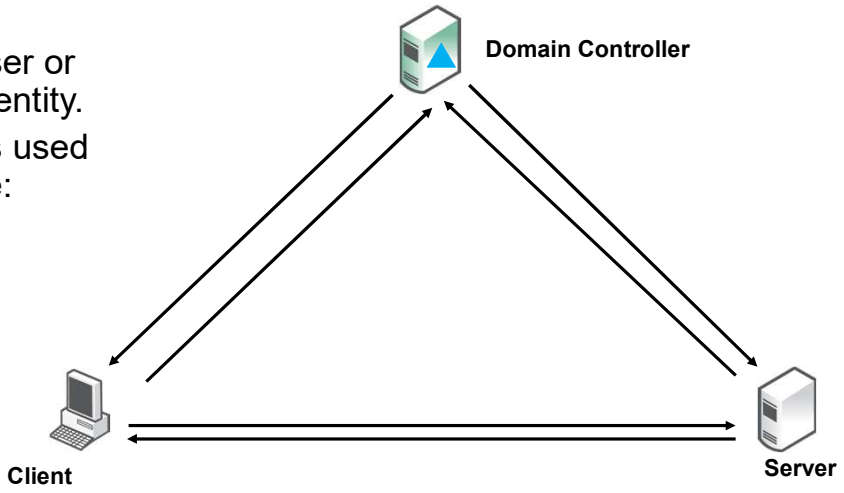
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Key Components of Active Directory

Authentication

- Authentication is the process whereby a user or device proves their identity.
- The two key protocols used in Active Directory are:
  - NTLM
  - Kerberos



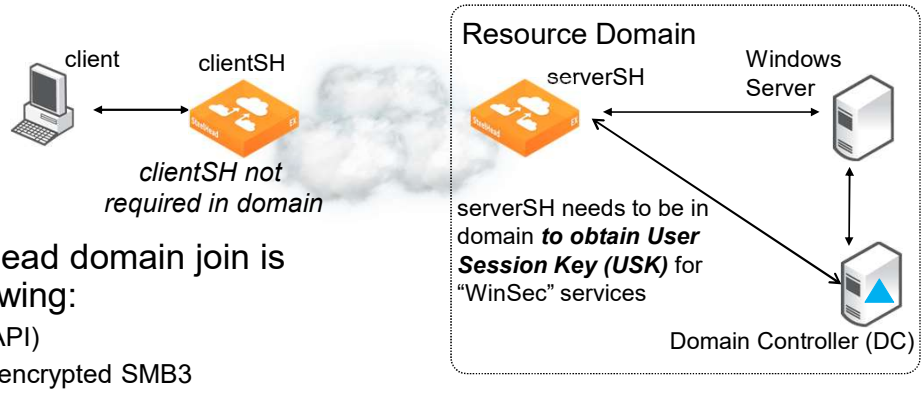
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

What Does AD Have to do With SteelHeads?

Server-Side SteelHead Needs to Join the Domain



- A server-side SteelHead domain join is required for the following:
  - Encrypted Exchange (MAPI)
  - Signed SMB and signed/encrypted SMB3
- Should the serverSH *not* get the USK…
  - For signed SMB, optimization will be SDR/LZ only.
  - For encrypted MAPI/SMB3, the connection will be passed-through.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 12

The important thing here is that both encrypted MAPI and signed/encrypted SMB use tokens, which the server-side SteelHead needs in order to re-sign or decrypt the traffic. However, in order to obtain such a token it needs to be able to authenticate and act *as* the client.

© 2021 Riverbed Technology. All rights reserved.

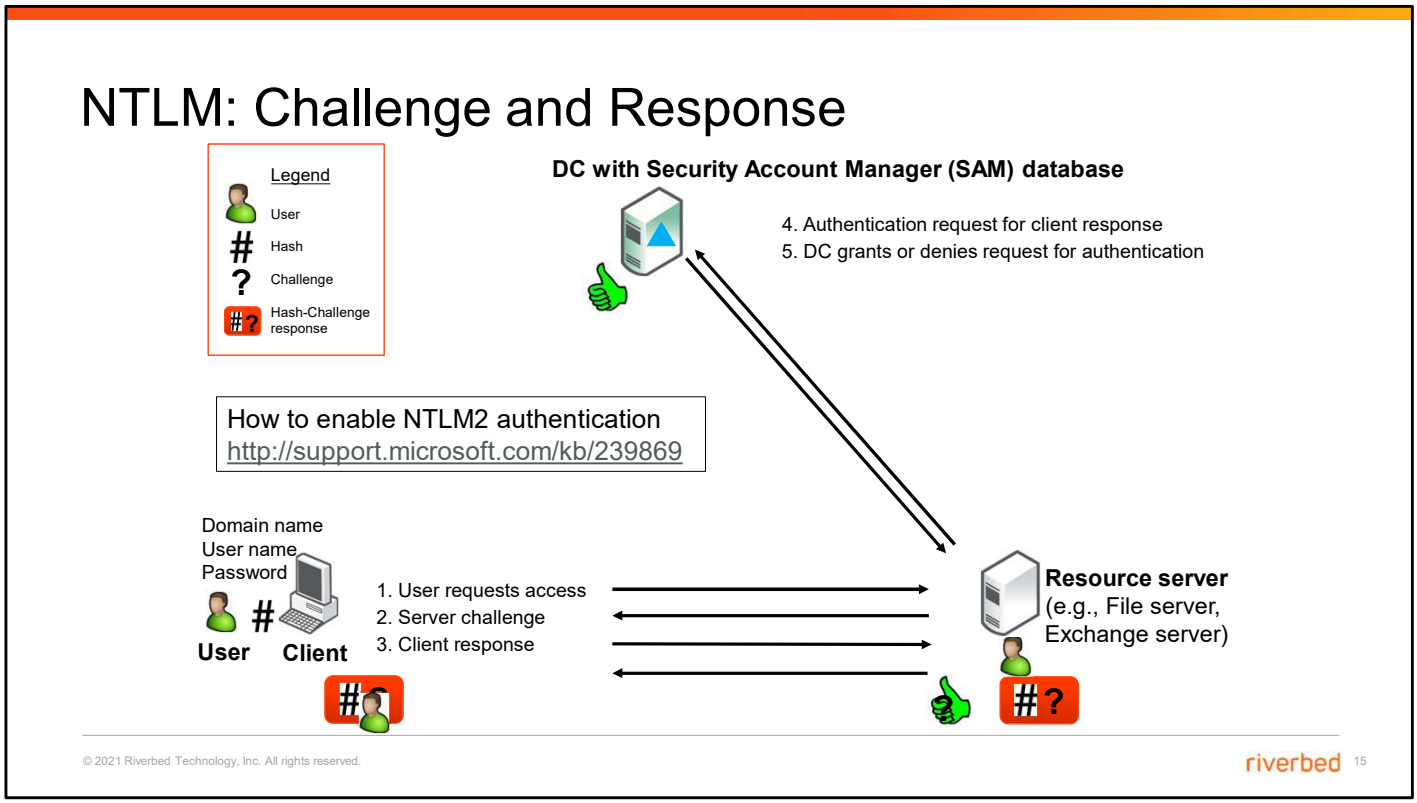
Which Protocols Require a Domain Join?

- All of the following protocols require a domain join:
  - Signed SMB
  - Signed SMB2
  - Signed/Encrypted SMB3
  - Encrypted MAPI
  - Encrypted Outlook-Anywhere
  - SharePoint
  - Microsoft Web Servers requiring “per request” Kerberos authentication
- The exact configuration depends on the authentication method being used.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.



A user accesses a client computer and provides a domain name, user name, and password. The client computes a cryptographic *hash* of the password and discards the actual password.

1. The client sends the user name to the server (in *plaintext*).

2. The server generates a 16-byte random number, called a *challenge* or *nonce,* and sends it to the client.

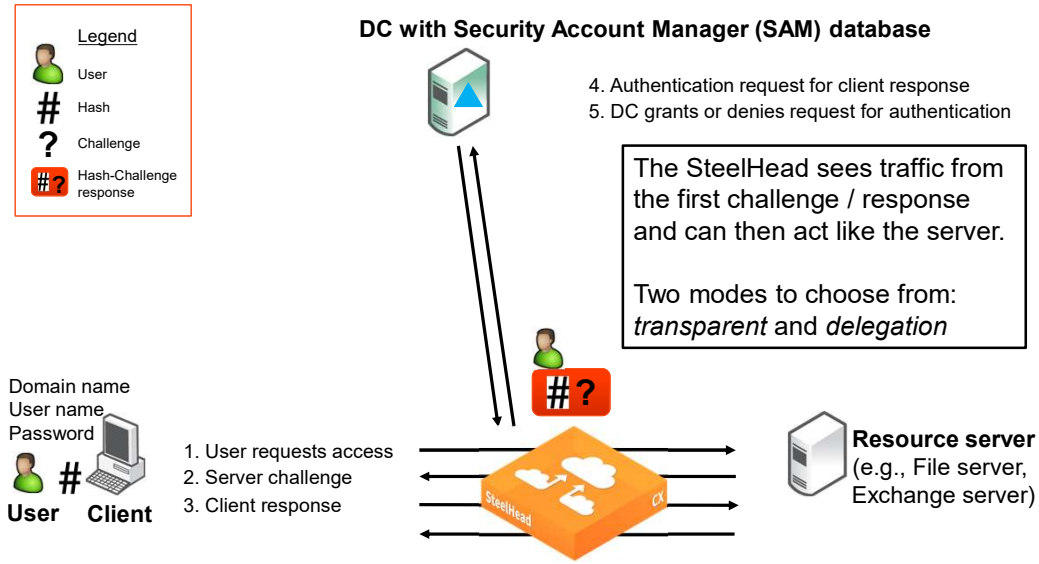
3. The client encrypts this challenge with the hash of the user's password and returns the result to the server. This is called the *response*.

4. The server sends the following three items to the domain controller: User name, Challenge sent to the client, Response received from the client.

5. The domain controller retrieves the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge. The domain controller compares the encrypted challenge it computed to the response computed by the client (in step 3). If they are identical, authentication is successful.

© 2021 Riverbed Technology. All rights reserved.

NTLM: Operation with Server-Side SteelHead



© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 16

When there is a server-side SteelHead in the network that is configured to perform pass-through authentication, it is ideally placed to see the “handshake” between the client and server.

As a result, it has all the pieces of the jig-saw puzzle to send them to the domain controller (in the same sort of way that the server does).

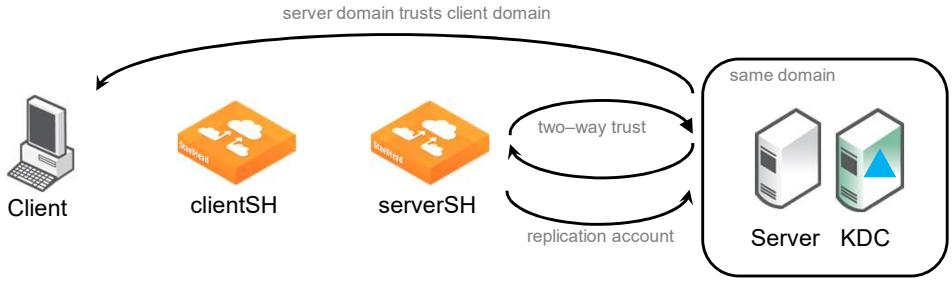
The SteelHead can then use the same token as the client and server thereby ensuring that any signing (for SMB traffic) is preserved, and any encrypted MAPI can be decrypted/re-encrypted.

For the original Delegation mode, we access the DC with elevated privileges in order to get user information. It was the Microsoft recommended way to interact with their environments.

© 2021 Riverbed Technology. All rights reserved.

Kerberos: Overview

- Kerberos came out of MIT and was developed with industry.
- SteelHead acts like a DC to obtain credentials via a replication user account.
- Kerberos is strict:
  - Hashes of passwords are never sent across the network.
  - All machines authenticate against a Key Distribution Center (KDC).
  - A client asks the KDC for permission to talk to a resource.
  - Domain trust requirements are a little complicated.



© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 17

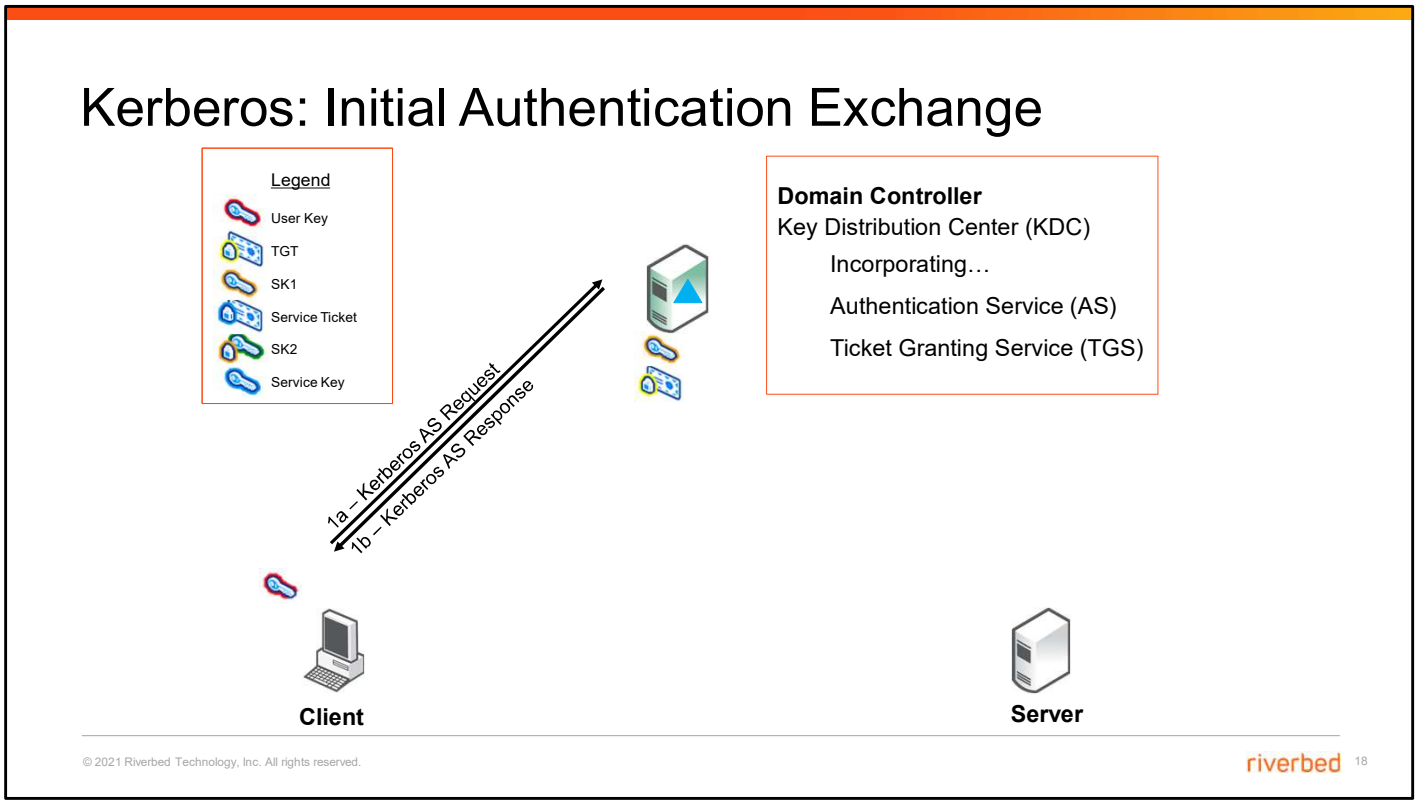
For end-to-end Kerberos authentication, a replication user account in the domain of the server has to be configured at the serverSH.

The serverSH can be in any domain that has a two-way trust to the domain of the server. The client can be in any domain that is trusted (incoming trust) from the domain of the server. The client DNS should have been configured correctly so that it can contact the KDC of the server's domain. If the client is not configured correctly it will not be able to get the Kerberos ticket and will use NTLM authentication.

The basic Kerberos process is as follows:

- When a user logs on, their user name and password is verified by Authentication Service on the Key Distribution Center (KDC)
- The KDC will consult AD, and if the login is valid, it will grant the user a *Ticket Granting Ticket* (TGT) plus the first of two session keys. Think of the TGT as a passport, identifying the user.
- Next, the client presents the TGT to the Ticket Granting Service on the KDC, asking for the credentials of the server that it want to connect to. The response is a Service Ticket that has two parts, a client part (encrypted with the client key), and a server part (encrypted with the server key). Within each is a ticket plus a temporary session key plus the clients identity. Think of the Service Ticket as a VISA.
- Finally, the client creates a new authenticator, encrypted with the session key and transmits it, along with the server part of the Service Ticket, to the server. The client and server now both have copies of the session key, so they can now communicate.
- Now, with the SteelHead added to the domain, it can use a replication user account to request a copy of the server’s machine account credentials including the service key.

© 2021 Riverbed Technology. All rights reserved.



This is an example of authentication in a simple environment with a client user, Domain Controller with KDC, and a resource, or application server.

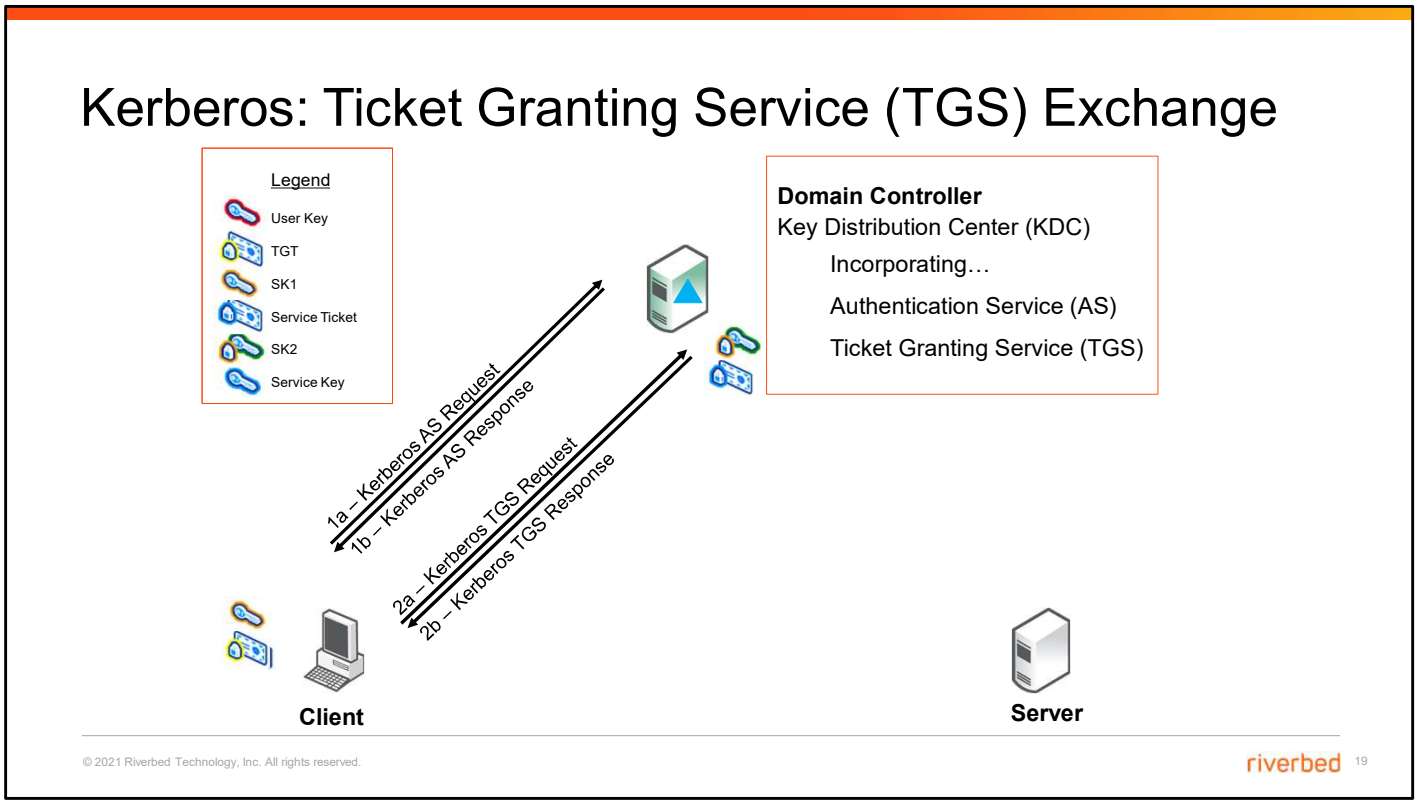
When initially logging on to a Microsoft Windows network, users must request access by providing a login name and password in order to be verified by the Authentication Service (AS) portion of a Key Distribution Center (KDC) within their domain. This is the first step of the AS exchange.

The KDC has access to Active Directory user account information. Once successfully authenticated, the Authentication Server grants the user a Ticket to Get Tickets (TGT) that is valid for the local domain. The TGT (sometimes referred to as the “AS reply”) has a default lifetime of 10 hours and may be renewed throughout the user's log-on session without requiring the user to re-enter his or her password. The AS reply includes two components: the TGT itself, which is encrypted with a key that only the TGS can decrypt, and the first of two session keys encrypted with the user's password hash. This initial session key (sometimes abbreviated to SK1), is used as part of any future communications with the KDC.

The TGT is cached on the client user machine in volatile memory space and is used to request sessions with services throughout the network. You could think of it like a stamp in your passport. It effectively says that you have passed the access controls to enter the country, and you can use it to prove to other security personnel that you have entered the country legally.

Note: The abbreviation TGT is sometimes referred to as Ticket Granting Ticket as well as Ticket to Get Tickets. The two terms are referring to the same thing and can be used interchangeably.

© 2021 Riverbed Technology. All rights reserved.

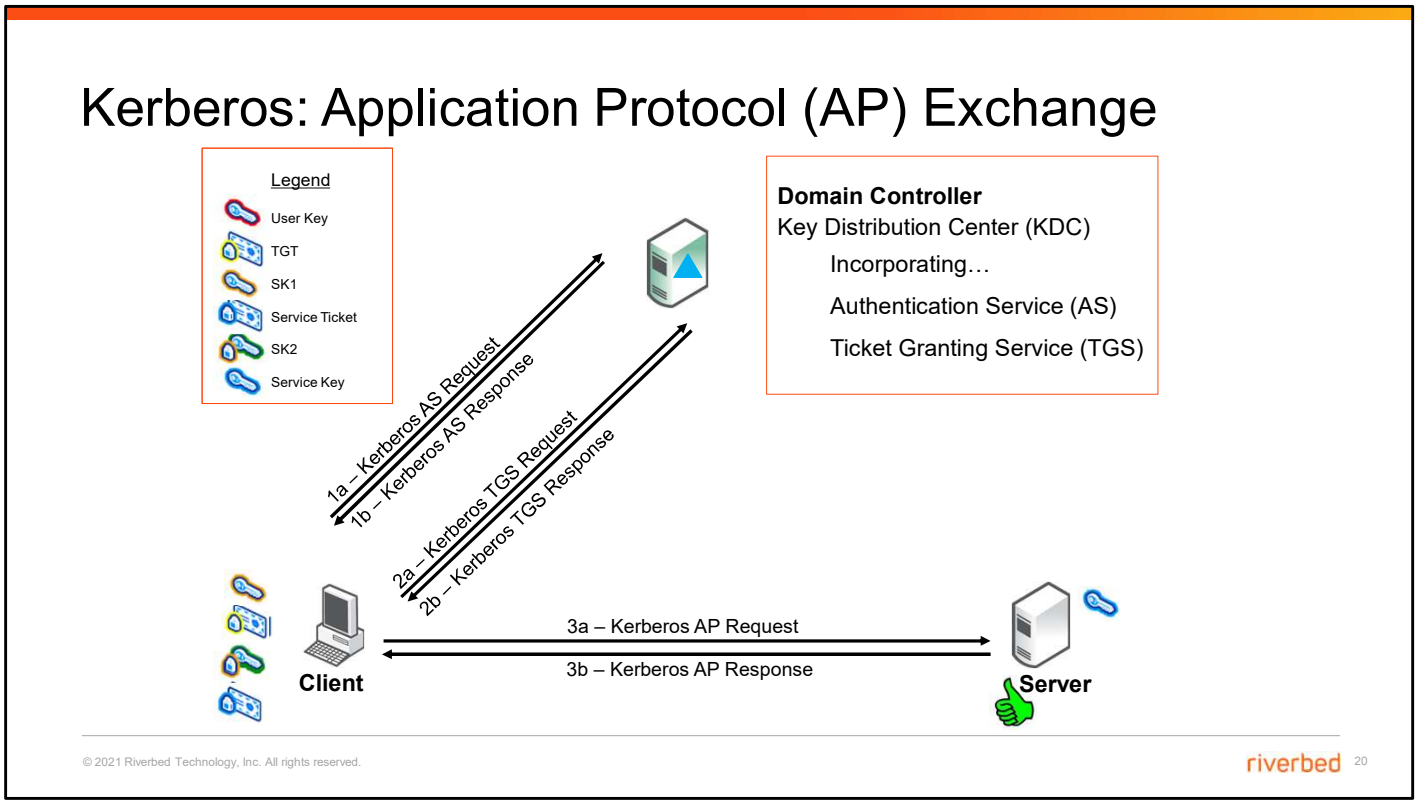


The next exchange is the **TGS Exchange**.

Using the TGT obtained from the AS exchange, the client sends a request to the Ticket Granting Service on the KDC for "credentials" of the server that it wants to open a connection to.

The TGS responds with the credentials in the form of a Service Ticket that also has two components. One component is encrypted in the server's key (which the client cannot read) the other is encrypted with the client’s key, which the client can read. The credentials themselves consist of a "ticket" for the server and a temporary encryption key. This encryption key is the second of the two session keys (SK2) issued during the sequence of exchanges. This particular session key is only valid for communicating with the desired server and lasts for the lifetime of the session with the server. A second or subsequent session with the server will need a new key (SK2) to be requested from the TGS.

© 2021 Riverbed Technology. All rights reserved.



The final exchange is the Application Protocol (AP) exchange between the client and the server itself.

The client creates yet another authenticator, this time encrypted using SK2, and transmits it with the service ticket (which contains the client's identity and a copy of the session key (SK2), all encrypted with the server's key) to the server.

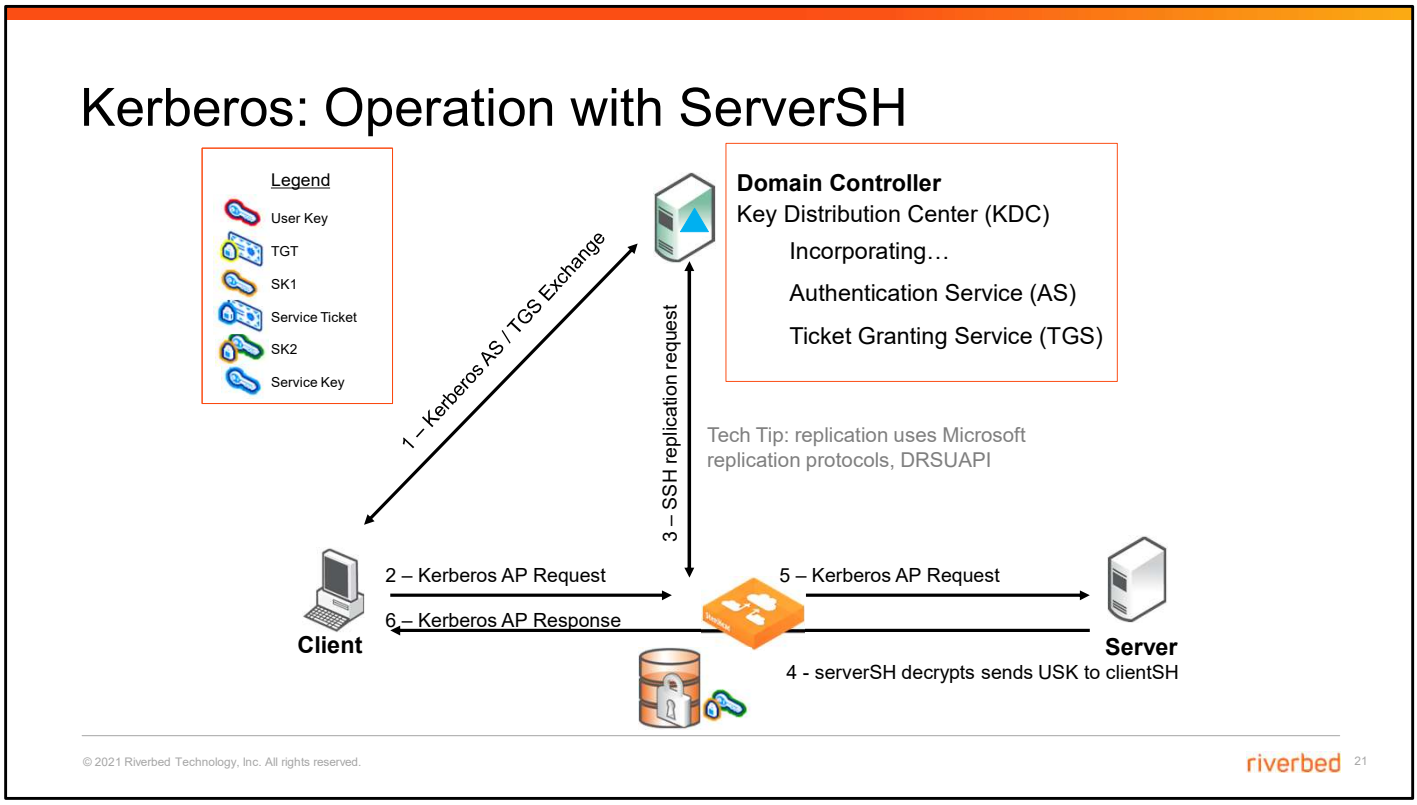
The session key, SK2, is now in the hands of both the client and server. It is used by the server to authenticate the client, and if mutual authentication is requested by the client, the key may be used by the client to authenticate the server. Mutual authentication is not always configured by the Windows Admin, but it is possible and therefore it’s important to know it can occur.

Note: This final (AP) exchange is quite often completed using whatever application protocol (AP) is required between the client and server. For example, SMB and SMB2 for file sharing, MAPI for email, or HTTP for SharePoint.

Now the client and server have a session set up so that they can communicate with each other (email, file transfer, etc.).

Don’t forget, as soon as the session ends, a new session can only be started once the client has performed another TGS Exchange and AP Exchange - steps 2 and 3 on this diagram. The duration of a session varies according to the type of application. For example, file transfers from a file server, the session could last until the shared folder has been unmapped, which could be a number of hours, but for some SharePoint implementations each HTTP transfer could be a separate session requiring its own authentication.

© 2021 Riverbed Technology. All rights reserved.



Let's go back to our previous diagram, but this time we'll add a server-side SteelHead. We leave out the client-side SteelHead to avoid confusion. Obviously, it would be part of the optimized connections, but in terms of authentication, it plays no significant part.

It's just the server-side SteelHead we need to concentrate on. Also removed are a few of the arrows and so forth because we're really interested in the stage where the client-user has already acquired a service ticket and SK2 from the TGS exchange so that it can open up a session with a resource server.

So let's assume that the client-user has already performed the AS exchange and this is followed by the TGS exchange. It now has the service ticket and session key (SK2) so it can go ahead and contact the server it wants to set up a connection with. Now, normally this would be a case of using the service ticket and session key to connect to the server as part of the AP exchange and wait for the "thumbs-up" from the server that all is well. In this case, we now have a SteelHead on the server side (don't forget, we have one on the client side too, but it is just not visible in the diagram).

The client knows nothing different and begins the AP exchange, sending the ticket and key as part of its request towards the server. The server-side SteelHead intercepts the request and by looking inside the request can see which server the client wants to talk to. The server-side SteelHead has already joined the domain and is part of the Windows AD, so it can use the replication user account to send a request to the domain controller for a copy of the server's machine account credentials including the service key.

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Join a SteelHead to a Domain – Pre-requisites

Pre-requisites for a Successful Domain Join

- **DNS** - Ensure that the SteelHead has the root and all child domains specified as search suffixes as well as a valid DNS server. The join is done via the SteelHead's *Primary* IP address, which should also be configured in DNS.
- **NTP** - Both NTLM and Kerberos are time sensitive. For Kerberos, the SteelHead clock must be within 30 seconds of the DC's clock.
- You will need an account of sufficient privileges so that the SteelHead can be joined as a RODC. Normally a domain admin account, but not necessarily as long as it has permission to join a computer to the domain.
- Know your AD structure! This is the hardest part in many ways. If you have a multi-domain forest it is recommended joining the SteelHead to the root domain.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 23

In order to do this you must ensure that you have prepared the following:

- **DNS** - Ensure that the SteelHead has the root and all child domains specified as search suffixes as well as a valid DNS server (obviously). The join is all done using the SteelHead's Primary IP address so that should also be configured in DNS.
- **NTP** - Both NTLM and Kerberos are time sensitive. For Kerberos, the SteelHead's clock must be within 30 seconds of the DC's clock (5 minutes for NTLM) so make sure you have this configured.
- Make sure you have an account of sufficient privileges so that the SteelHead can be joined as a RODC. This will usually be a domain admin account, but does not necessarily need to be one as long as it has permissions to be able to join a computer to the domain.
- Know your AD structure! This is the hardest part in many ways. If you have a multi-domain forest it is recommended joining the SteelHead to the root domain.

© 2021 Riverbed Technology. All rights reserved.

Join a SteelHead to a Domain – Join Options

- There are three join type options:
  - Workstation
  - Active Directory Integrated (Windows 2003 or later)
  - Active Directory Integrated (Windows 2008 or later)
- Unless you are using a very old version of Windows you should always choose *Active Directory Integrated (Windows 2008 or later)*
  - This joins the SteelHead to the domain as a RODC, which is essential for NTLM Transparent Mode.
  - If you are absolutely certain that only Kerberos authentication will be used, and NTLM has been *completely* disabled, you can opt for *Workstation.*

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 24

Note that Active Directory Integrated (Windows 2003 or later) does not work across multiple domains.

In environments where NTLM and Kerberos authentication co-exist, there may be servers which accept only Kerberos-authenticated users. In these cases, simply adding the server-side SteelHead appliance(s) to the correct domain, yet not completing the SteelHead Kerberos integration, would allow full optimization to NTLM servers, but no latency optimization – and therefore slower connectivity – to the Kerberos-authenticated servers.

SteelHeads support joining domains that are operating in native or mixed modes for the following domain functional levels:

- Windows 2000
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

© 2021 Riverbed Technology. All rights reserved.

Join a SteelHead to the Domain – “Server-Side”

Which SteelHead?

- The manual says *Server-Side SteelHead* but what does this mean?
  - This is the SteelHead that makes the actual request to the server.
- But what if we have local branch file servers?
  - This is not uncommon, so in reality all SteelHead appliances could be joined to the Domain where necessary.
  - Remember, *server-side* and *client-side* are relative concepts.
  - Having an SCC makes this much easier.

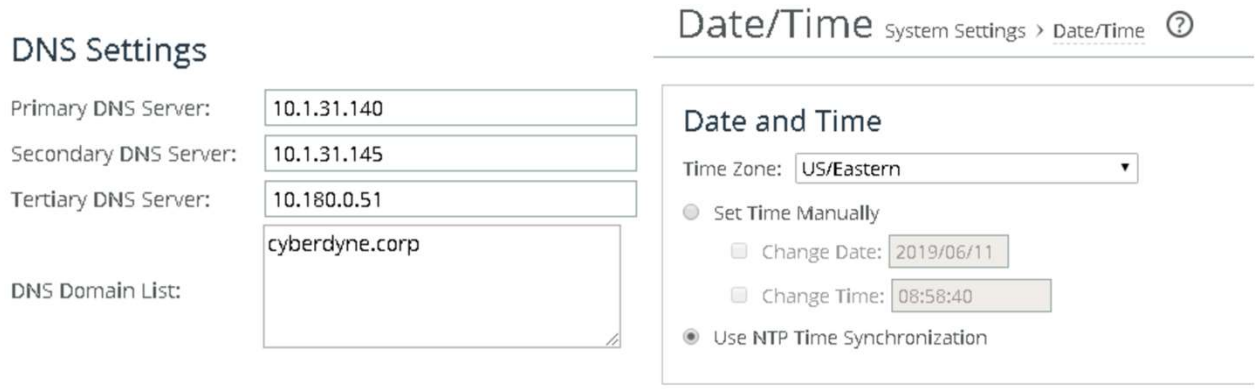
© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 25

© 2021 Riverbed Technology. All rights reserved.

SteelHead (SH) Domain Join – Configue NTP & DNS

1. Configure DNS and NTP on Datacenter SteelHead.



© 2021 Riverbed Technology, Inc. All rights reserved.

There should probably be a step 0 here: Have a large mug of coffee by your side before you start! This is going to take some time and all of the steps need to be followed. This often fails on the first attempt due to a mistake in an early step (usually this one) but don't worry, as once you have configured this, configuring both encrypted MAPI and signed/encrypted SMB should be pretty straightforward.

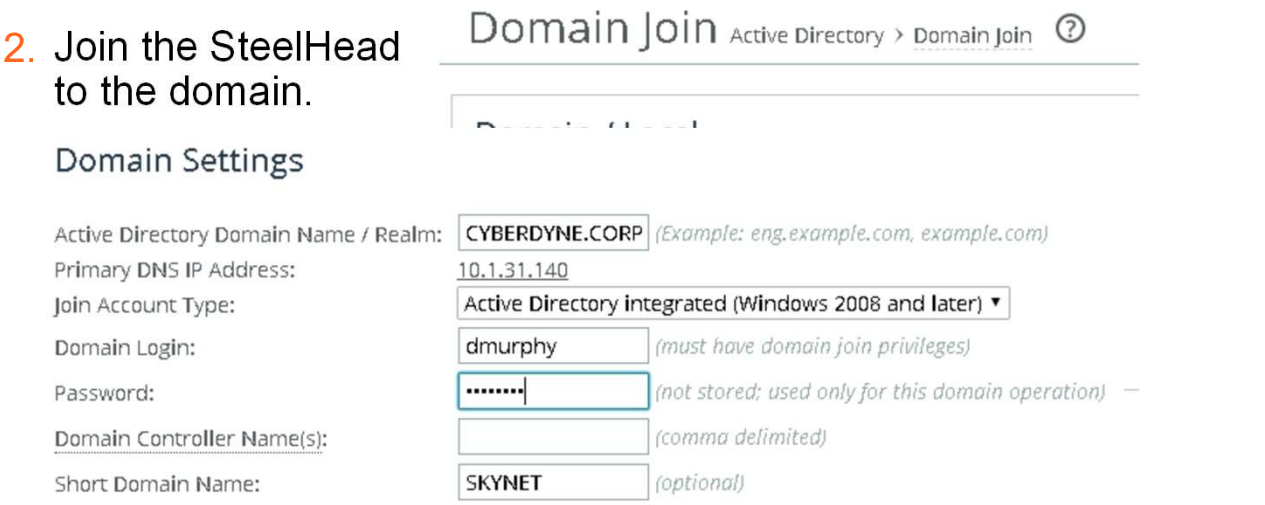
For NTP, you should configure the SteelHead to use the same NTP server as all the other servers in the domain.

Note that you can test the DNS settings using the *Test DNS* tool at the bottom of the *Host Settings* page.

© 2021 Riverbed Technology. All rights reserved.

SteelHead (SH) Domain Join – Domain Settings

2. Join the SteelHead to the domain.



© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 27

Note that this will be located at a different location in the GUI, depending on the version of RiOS.

For 8.x this is found under *Configure* > *Networking* > *Windows Domain.*
For 9.x this is under *Optimization* > *Active Directory* > *Domain Join.*

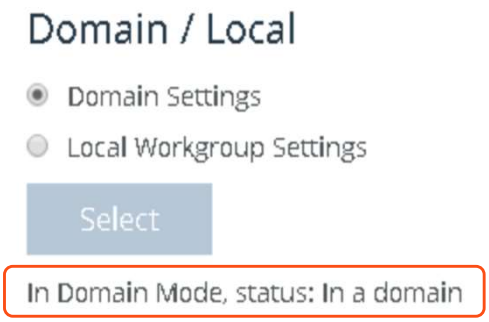
In either case, though, the page is the same. Ensure that the account you use here has sufficient privileges.

Fill in the details (you will have to fill in the NETBIOS name if it is different from the FQDN name) and click *Join.* There will probably be a minute or two between clicking *Join* and the SteelHead actually joining. If it takes longer than that refreshing the page sometimes helps.

© 2021 Riverbed Technology. All rights reserved.

SteelHead (SH) Domain Join – Successful Join

- Once joined the status should change to **In a domain**.



© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

SteelHead (SH) Domain Join – DC Load Balancing

Domain Controller Load Balancing

- Can configure load balancing with up to six domain controllers (by default) using this command:
  - **`protocol domain-auth configure load-balancing`**
- Domain controllers are discovered via DNS
- Can alternatively specify a static list of domain controllers

Domain Controller Name(s):		*(comma delimited)*
Short Domain Name:	SKYNET	*(optional)*

- To verify use this command:
  - **`show protocol domain-auth load-balancing`**

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 29

You can configure the server-side SteelHead to communicate simultaneously with multiple domain controllers in the same domain. This enables the server-side SteelHead to:

- Sustain higher quantities of authentication requests.
- Tolerate the loss of a domain controller much more efficiently.
- Reduce the load it places on an individual domain controller.

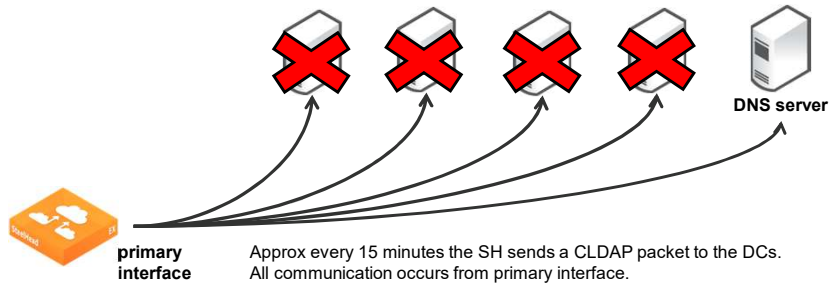
You can balance traffic across a maximum of eight domain controllers. Use the **show protocol domain-auth load-balancing** command to display the current status.

© 2021 Riverbed Technology. All rights reserved.

SteelHead (SH) Domain Join – DC Health Check

Troubleshooting: DC Health Check

- The SH communicates with all listed domain controllers.
  - each DC is then known to be “good” or “bad”
- A new user session will attempt to use the first listed good DC.
- If all the DC’s in the list are not good, SH still works …
- A DNS request automatically updates the SH with a list of available DC’s.



© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 30

"CLDAP“, connectionless LDAP (LDAP over UDP), is used to communicate between the SH and DCs in the domain controller list.

You might need a “*” at the end of the DC list in order to use the DNS request.

We say in the slide that the primary port is used to communicate with the DCs. This is not strictly true. The primary port has been QA’d and is the only supported port to use for out-of-band Active Directory traffic. However, field reports suggest that Aux and in-path-mgmt may also work – though they are as yet “not officially supported”.

© 2021 Riverbed Technology. All rights reserved.

Join a Domain Without the Administrator Account

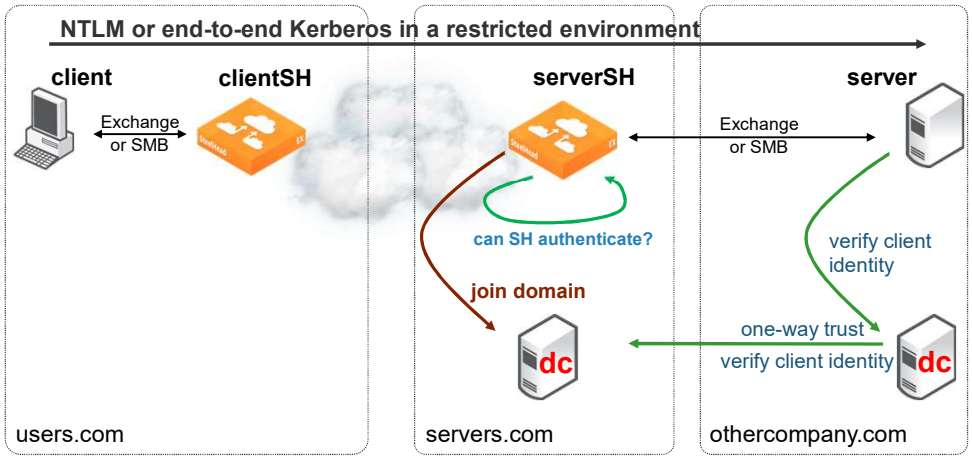
- As a customer you may have security concerns.
  - *"No! The SH team cannot have the Administrator password."*
- You may have a point …
  - At domain join, auth code alters permissions letting SH account access the USK.
- Work-around:
  - Windows admin must set permission for the machine account.
  - A less-privileged user can join SteelHead to the domain.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Join a Domain: “oneway-trust” Command

- For a ServerSH to optimize to a domain other than its own, CLI config is required.




```
(config) # protocol domain-auth oneway-trust dns-name <fqdn> netbios-name <netbios>
```

© 2021 Riverbed Technology, Inc. All rights reserved.

In some Windows domains there are only one-way trusts between domains. This is usually due to a combination of security and management requirements configured by the Windows admin. In this situation it is useful to know that Delegation Mode is not supported (covered later) and the server-side SteelHead needs to be configured to use Transparent mode. Kerberos authentication is supported in RiOS 8.5 and later through this command:

```
protocol domain-auth restricted-krb enable
```

The server-side SteelHead must join a Domain that has a one-way trust to the resource domain where the servers are located.

© 2021 Riverbed Technology. All rights reserved.

Join a Domain: One-Way Trust Considerations

- One-way trusts are complicated – use the cli command and avoid details!
- Outlook Anywhere assumes one-way trusts for:
  - office365.com and outlook.com

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 33

Trust is “given”. A domain gives trust to a user so that the trust is going out from the domain to the user. It’s a detail and doesn’t need to be remembered, but when talking to the experts knowing this terminology can avoid confusion.

Note that “one-way” trust in Kerberos has been renamed / rebranded by Product Management to “Kerberos in a restricted environment”. This was brought about because Office365 supports two-way trusts, but still requires some work by the SH to make things work.

© 2021 Riverbed Technology. All rights reserved.

Authentication Modes on SteelHead

- Kerberos Constrained Delegation
  - “Delegation Mode” needs a delegate user account
  - Part Kerberos and part NTLM
  - http://technet.microsoft.com/en-us/library/cc995228.aspx
- Transparent Mode
  - Windows calls it “pass-through Authentication”
  - Widely used for backward compatibility and end-to-end Kerberos fallback
  - http://technet.microsoft.com/en-us/library/cc722778.aspx
- End-to-end Kerberos
  - “Kerberos Authentication Support” needs a replication user account for server domain
  - http://msdn.microsoft.com/en-gb/library/windows/desktop/aa378747%28v=vs.85%29.aspx

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 34

End-to-end Kerberos authentication is the default choice for Windows 7 onwards and Windows Server 2008 onwards. But for backwards compatibility, it is quite often the case that clients and servers automatically negotiate to use either NTLM or Kerberos. For this reason, it is usually a good idea to configure for end-to-end Kerberos mode and also have the server-side SteelHead appliance join the domain and integrate with Windows AD. Prior to RiOS 7, Delegation Mode was used, but in more recent releases the combination of Active Directory Integrated Mode and End-to-end Kerberos Mode have deprecated the older Delegation Mode.

© 2021 Riverbed Technology. All rights reserved.

Authentication Modes – Diagrammed

- Transparent Mode
  - Recommended mode and fallback for end-to-end Kerberos

NTLM NTLM

- End-to-end Kerberos
  - Configure *replication* account on Domain Controller and SteelHead

Kerberos Kerberos

- Kerberos constrained delegation (deprecated)
  - Configure *delegation* account on Domain Controller and SteelHead

NTLM Kerberos

© 2021 Riverbed Technology, Inc. All rights reserved.

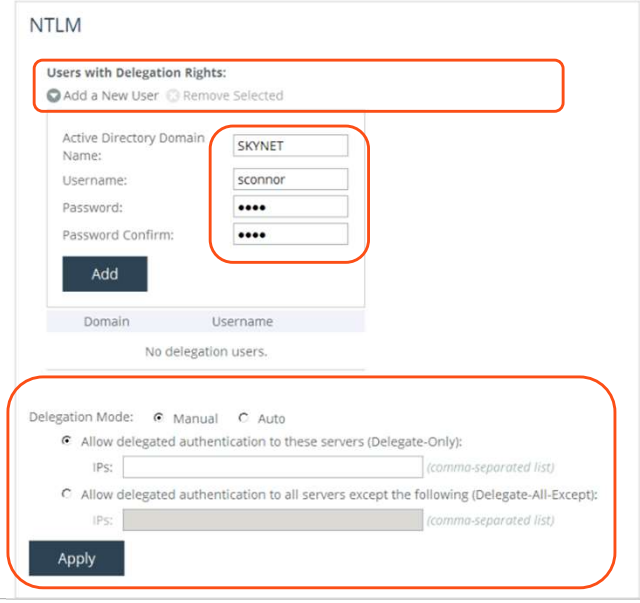
riverbed 35

Some modes of operation guarantee NTLM even if you believe “Kerberos only” is configured, for example mapping a network drive via IP address.

There is a way for the Windows admin to disable fallback to NTLM, but it must be explicitly set up and is a different procedure from enabling Kerberos as the default. It is worth being a little skeptical even if the customer is convinced NTLM cannot be happening.

© 2021 Riverbed Technology. All rights reserved.

NTLM: Configure Delegation Mode



- Windows Admin must create special user
- Manual mode:
  list servers on DC
  list servers on SH
- Auto mode:
  SH updates DC list
  SH updates own list

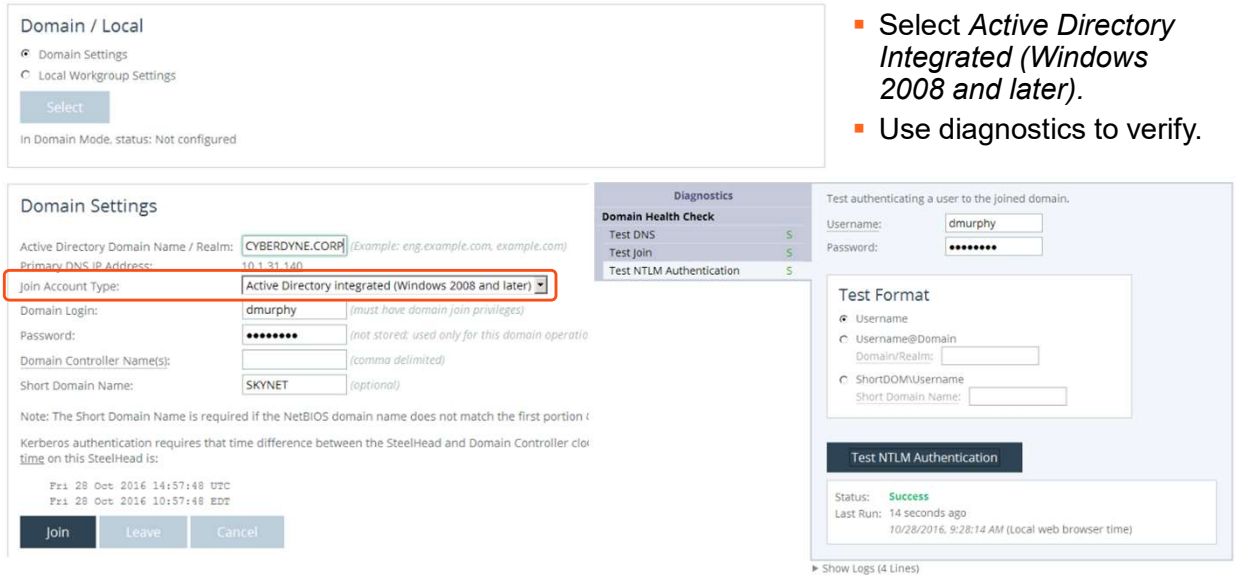
© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 36

This requires a lot of work in Active Directory and has since been deprecated. NTLM Transparent Mode is now the recommended NTLM mode.

© 2021 Riverbed Technology. All rights reserved.

NTLM: Configure Transparent Mode



- Select *Active Directory Integrated (Windows 2008 and later).*
- Use diagnostics to verify.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 37

© 2021 Riverbed Technology. All rights reserved.

What is a Replication User Account?

- A pre-requisite for optimizing end-to-end Kerberos authenticated connections
- A 'normal' account that has been assigned privileges to perform AD replication
- Configure first in Active Directory server, then add credentials to the server-side SteelHead(s)
  - Once configured, the account allows SteelHeads to obtain relevant session keys
- Kerberos in multi-Child domains which may require a Replication User in each child domain; see Knowledge Base article S24599

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 38

A replication user account is a normal account that has been assigned the limited privileges needed to perform AD replication. This task is performed on the Domain Controller using the "Delegation of Control Wizard" (right-click the Domain under ADUC) and adding the permissions for *Replicating Directory Changes* and *Replicating Directory Changes All.* This must be done in Active Directory prior to configuring on the SteelHead. Note that this must be done for every child-domain for which you have a server (Exchange or signed-SMB) that you will need to optimize with.

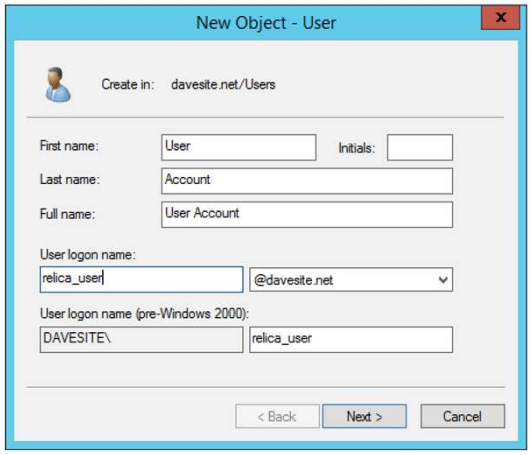
Once the replication user has been added in AD it must be added under the server-side SteelHead's *Kerberos* settings, along with the domains that it is replicating for. This account can then replicate active directory information, enabling the server-side Steelhead to obtain the relevant keys required to optimize encrypted MAPI and signed and/or encrypted SMB2/3 traffic using end-to-end Kerberos authentication.

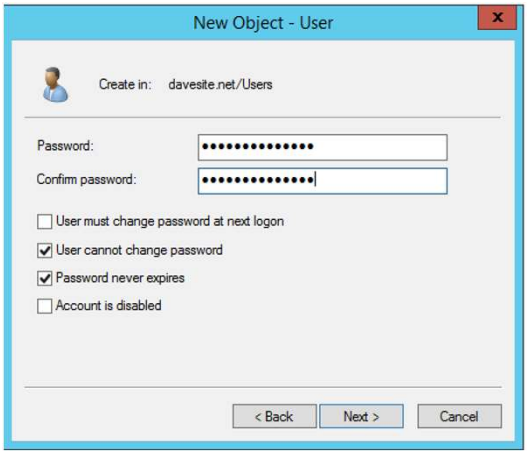
© 2021 Riverbed Technology. All rights reserved.

Replication User Account – User Account Creation

On Domain Controller – Create Standard User

1. In ADUC, create a standard user account.





© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 39

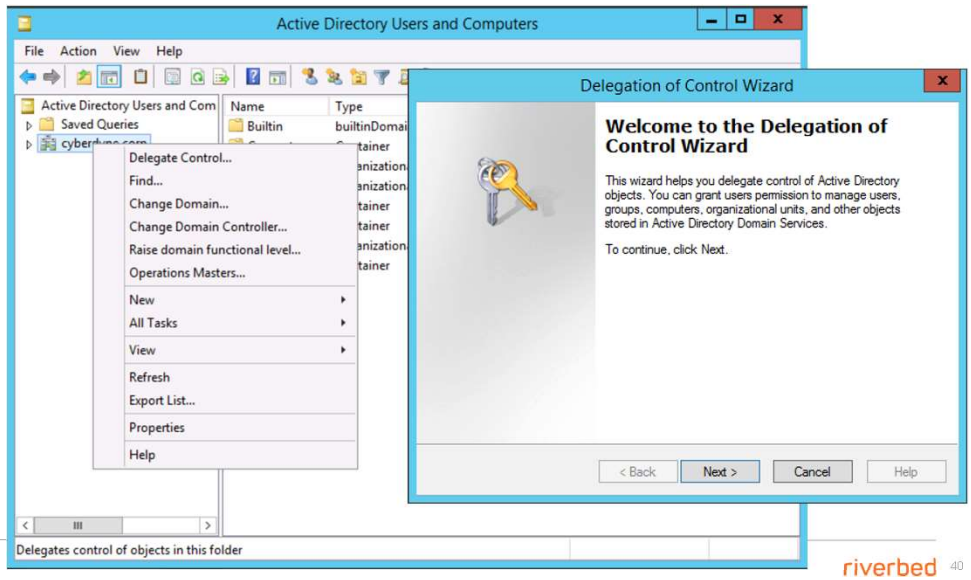
First, create a user in AD and make sure that the password is both secure and does not expire.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Delegation (1/6)

On Domain Controller – Delegation Walk-through

2. Right-click the domain with the WinSec server and select **Delegate Control** for each domain you need to optimize with.



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 40

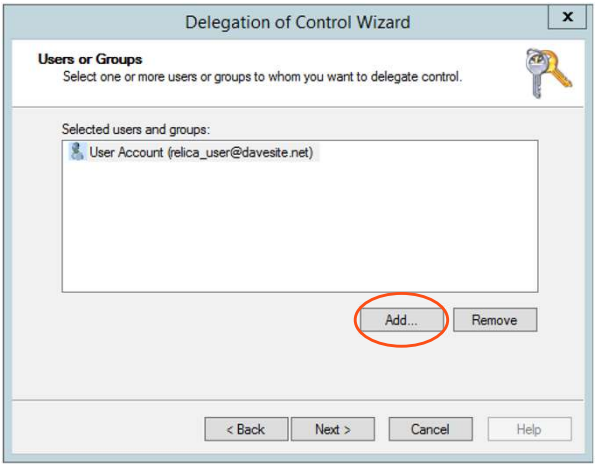
Then, for every domain with a server that you need to optimize with, you must first right-click, as shown, and select *Delegate Control*.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Delegation (2/6)

On Domain Controller – Delegation Walk-through

3. Select the user.



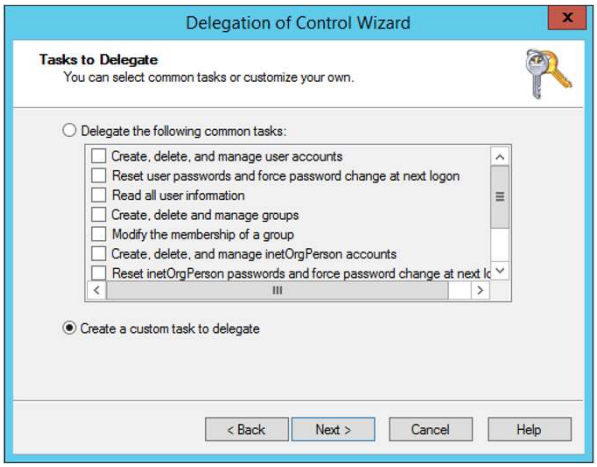
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Delegation (3/6)

On Domain Controller – Delegation Walk-through

4. Select **Create a custom task to delegate**.



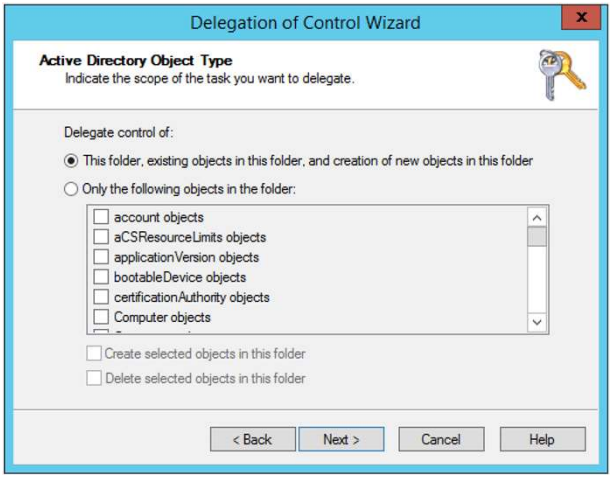
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Delegation (4/6)

On Domain Controller – Delegation Walk-through

5. Choose **This folder, existing objects in this folder, and creation of new objects in this folder**.



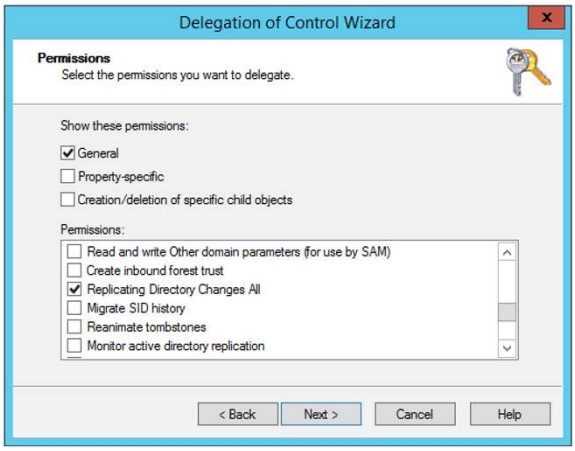
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Delegation (5/6)

On Domain Controller – Delegation Walk-through

6. Select **General** and scroll down to select both:
   - **Replicating Directory Changes**
   - **Replicating Directory Changes All**



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 44

Note that if you do not see the options in the *Permissions* box it could be that you selected a container below the root of the domain when you selected Delegate Control. You will not see the replication options if you do not select the root.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Delegation (6/6)

On Domain Controller – Delegation Walk-through

7. Review your settings and, if correct, click **Finish**.

© 2021 Riverbed Technology, Inc. All rights reserved.

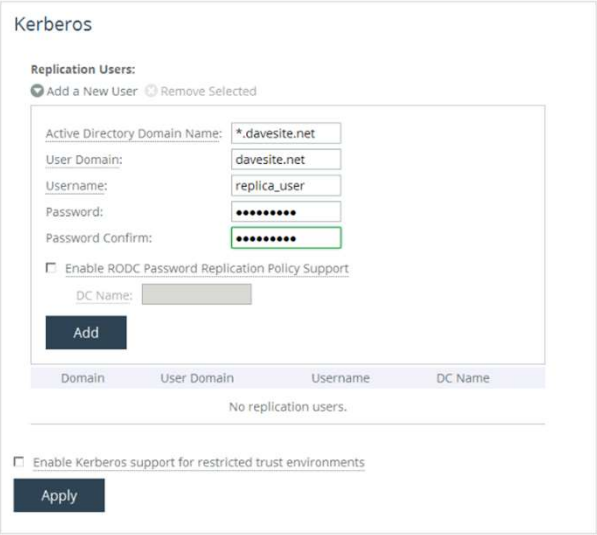
riverbed 45

Importantly, you need to do this for every child-domain for which you have a server (Exchange or signed-SMB) that you will need to optimize with.

© 2021 Riverbed Technology. All rights reserved.

Replication User Account – Add to Server-Side SH

8. Add the configured replication user to the server-side SteelHead. Note the wildcard - in this example the replication user is replicating for the following child domains:
   - ford.davesite.net
   - arthur.davesite.net
   - zaphod.davesite.net



© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 46

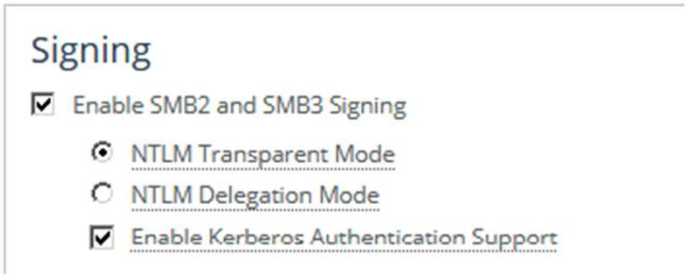
We are using the wildcard to specify all sub-domains that we have configured in the earlier step for the replication user. This is important or it won't work!

We can enable one-way trust support as well, for Kerberos named *Enable Kerberos support for restricted trust environments.*

© 2021 Riverbed Technology. All rights reserved.

Enable SteelHead Optimization Features

- The account is all setup now and can be used for Kerberos Authentication Support. Select the Enable option to configure optimization.



- Then click **Apply** to enable.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Kerberos vs NTLM

Kerberos has many advantages

- More secure: No password stored locally or sent over the net
- Best performance: improved performance over NTLM authentication
- Delegation support: Servers can impersonate clients and use the client's security context to access another resource
- Simpler trust management: Avoids the need to have p2p trust relationships on multiple domains environment
- Supports MFA (Multi Factor Authentication)

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Domain Easy Config

- This can all be made a lot simpler using the *Easy/Auto Config* tools.

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 49

The above can all be made a lot simpler using the *Easy/Auto Config* tools, which can even setup the replication user for you – it just needs creating and the SteelHead will assign the correct privileges.

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins and Auth – Test DNS

- If you have domain join problems run the **Test DNS** test.

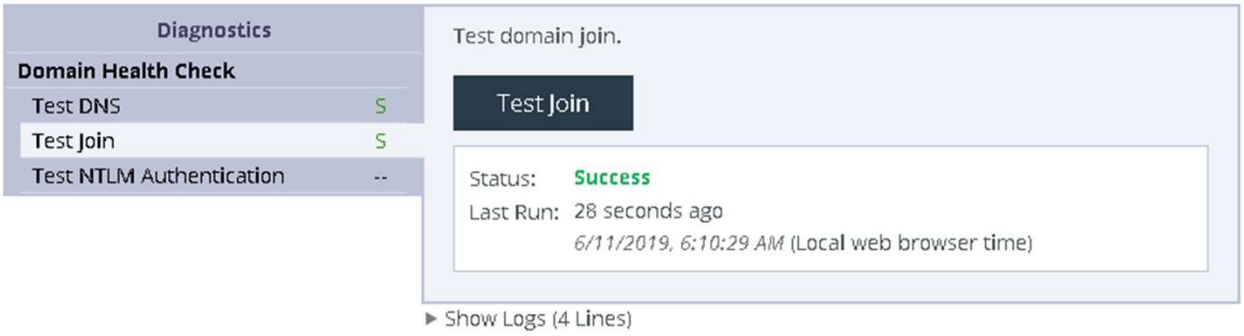
© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 50

If you have issues at this point then navigate to the lower part of the screen and try running some of the built-in diagnostics. Common problems are incorrect Short Domain Name (NETBIOS name) and incorrect domain controllers. Usually you do not need to specify these, though the DC should really be within 8ms of the SteelHead so sometimes you need to put the domain controller name in to force the SteelHead to use a local domain controller.

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins and Auth – Test Join

- If you still have problems then run the **Test Join** test at the bottom of the page.

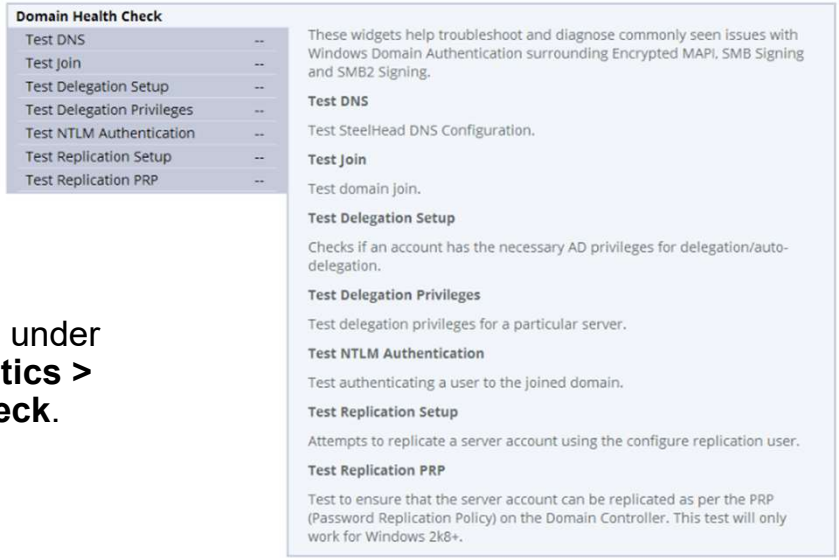


© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 51

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins and Auth – Useful Tools

- There are also a range of tools available on the SteelHead for all aspects related to AD.
- These can be found under **Reports > Diagnostics > Domain Health Check**.



© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins Via CLI – DNS Settings

- **protocol domain-auth test dns**
- **show protocol domain-auth test dns**

```
n130-sh1 (config) # protocol domain-auth test dns join-domain  cyberdyne.corp
Test DNS Status: STARTED.
Check result using: 'show protocol domain-auth test dns'
n130-sh1 (config) # show protocol domain-auth test dns

Action                          Status           Last Run
--------------------------------------------------------------------------------

Test DNS                        SUCCESS          Tue Jun 11 09:39:09 2019 EDT
--------------------------------------------------------------------------------


RESULT: Testing DNS Configuration
 Join Domain: cyberdyne.corp
DNS Test Passed
```

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins Via CLI – Verify Join

Confirm SteelHead Correctly Joined to the Domain

- **protocol domain-auth test join**
- **show protocol domain-auth test join**

```
n130-sh1 (config) # protocol domain-auth test join
Test Join Status: STARTED.
Check result using: 'show protocol domain-auth test join'
n130-sh1 (config) # show protocol domain-auth test join

Action                          Status          Last Run
--------------------------------------------------------------------------------

Test Join                       SUCCESS         Tue Jun 11 09:45:16 2019 EDT
--------------------------------------------------------------------------------


RESULT: Test Join result:

Testing if SH is joined to a domain
Join to domain CYBERDYNE.CORP is OK
Domain Join Test Succeeded
```

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins Via CLI – Test Auth

Ensure SteelHead can Authenticate Client Connections

- **protocol domain-auth test authentication**
- **show protocol domain-auth test authentication**

```
n130-sh1 (config) # protocol domain-auth test authentication username dmurphy password ZeroCool
Test Authentication Status: STARTED.
Check result using: 'show protocol domain-auth test authentication'
n130-sh1 (config) # show protocol domain-auth test authentication

Action                          Status          Last Run
--------------------------------------------------------------------------------

Test Authentication             SUCCESS         Tue Jun 11 09:50:27 2019 EDT
--------------------------------------------------------------------------------


RESULT: Test authentication result:

Testing authentication of dmurphy on the joined Domain Controller
challenge/response password authentication succeeded
Authentication Test Succeeded
```

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Troubleshoot Domain Joins Via CLI – Domain Settings

Verify Domain Settings

- **`show domain settings`**

```
n130-sh1 # show domain settings
Log level                        : 0
Max log size (KB)                : 25000
Password refresh interval (Day)  : 0
Disable IPv6 Lookups             : yes
Use default domain               : yes
Ignore trusted domains           : no
Max winbind children allowed     : 0
Enable tdb mmap                  : yes
Domain controller list           :
Kerberos settings                : yes
Smb2 for domain-ops              : yes
n130-sh1 #
```

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

HOL1121

Active Directory

In this lab, you will:

- Integrate SteelHead in an Active Directory Domain

Duration: **20 minutes**

eLab system: link and access details provided in your course confirmation email

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 57

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

The Importance of SMB

- Server Message Block (SMB) protocol now the default for sharing files between servers and users
- Fast on the LAN, not so good on the WAN
- Users need fast, secure access to shared files
- Just a few seconds of waiting for files to load can add up to a lot of wasted time in a large office

$$T = \$^2$$

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 59

Outside of Unix environments Windows file sharing protocols have become almost the default standard for sharing files between servers and users. Veteran IT professionals would remember spending hours configuring NFS and Novell, but for well over a decade now, Microsoft has totally eclipsed them with its *Server Message Block* (SMB) protocol.

The files may not be being served by an actual Windows machine. For large environments, there is a good chance it will be some form of fileserver such as NetApp FAS. The key point here is that, for a large enterprise, SMB is as critical to transferring files around as the Tube is to travelling around London.

From a user's point of view they need to be able to access their central files quickly while confident that Windows locking mechanisms ensure consistency, with other users barred from editing the file when they have it open.

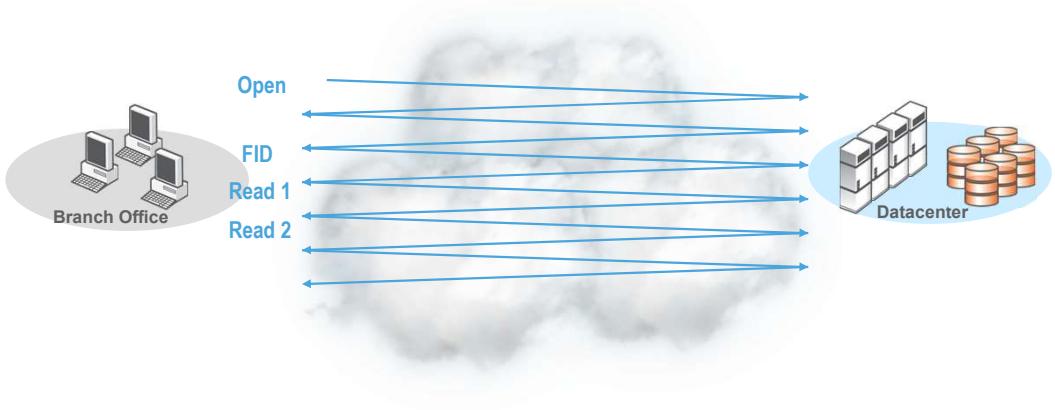
From the business perspective these files need to be located centrally, facilitating collaboration while at the same time enabling simple backup and restore. Speed is important from the business perspective too. If a user opens 100 files a day and we can reduce the transfer time from 3 minutes to a few seconds we have saved them nearly 300 minutes or five hours! And this is just for one user – with a branch of 100 users we have saved 500 hours or 20 days' worth of productivity – it does not take much to prove the value.

© 2021 Riverbed Technology. All rights reserved.

The Nature of SMB

Why Does SMB Performance Suffer Over the WAN?

- SMB is ‘chatty’
- Multiple turns involved in listing folder contents and opening files



© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 60

SMB is very fast on a LAN and is even used in Hyper-V environments for storing virtual machine files. Unfortunately, SMB is quite ‘chatty’ which, while fine on a sub-microsecond LAN, is awful on a WAN with a latency many orders of magnitude greater than that.

As you can see, opening a file using SMB creates many application ‘turns’, each of which costs time, which adds up very quickly on high-latency links. The aim is to configure the SteelHead so that it can optimize these connections and restrict the turns to the low-latency LAN and keep them off the WAN. Remember that Riverbed’s own protocol in the inner-channel is proprietary and designed to be efficient across WANs and, therefore, has far fewer turns than the protocol being optimized.

Before we look into how to optimize SMB we first need to have a look at the protocol itself.

© 2021 Riverbed Technology. All rights reserved.

Overview of SMB Protocol

Steps to Access a File on a Server

- For a client to access a file on an SMB server the following steps occur on the client:
  1. Paste the full filename to determine the server name.
  2. Establish a TCP connection to the server.
  3. Negotiate what type of SMB dialect and option is used with the server.
  4. Transfer credentials and authenticate access to the server.
  5. Open the file for operations by sending the filename and desired access to the server.
  6. Perform read, write, or other operations on the file, typically in a serial fashion.
  7. Close the file for operation.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 61

After a connection to the server is established, client systems tend to leave the connection open for some amount of time, even when there are no open files by the client.

This has an impact on CIFS optimization because RiOS can optimize CIFS connections only when it detects the beginning of the CIFS connection.

This is due to the negotiation of SMB options and SMB dialect that allow RiOS to understand what client and server operating systems are in use, which revision of the CIFS protocol is in use, and other options relevant to optimizing the connection.

© 2021 Riverbed Technology. All rights reserved.

SMB Dialects – Overview

- CIFS – Refers to original flavor of SMB, pre Windows Vista/2008
- A quick timeline of signing and encryption:
  - *SMB signing*: Windows NT 4.0 Service Pack 3
  - SMB2 Windows Vista 2006
  - SMB2.1, introduced with Windows 7 and Server 2008 R2
  - SMB3 has encryption and multichannel
    - RiOS DOES support SMB3 encryption
    - RiOS does NOT support SMB3 multichannel
  - SMB3.0.2, introduced in Windows 8.1/Server 2012 R2, has minor improvements, including the ability to turn off SMB1
  - SMB3.1.1, introduced with Windows 10/Server 2016, has more improvements, mainly pre-authentication integrity, encryption enhancements and support for cluster rolling upgrades to Scale-Out File Servers.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

SMB Dialects – Default Negotiation Table

Which Protocol will be Negotiated?

OS	Windows Server 2003	Windows Server 2008	Windows Server 2008R2	Windows Server 2012	Windows Server 2012R2	Windows Server 2016
Windows XP	SMB1.0	SMB1.0	SMB1.0	SMB1.0	SMB1.0	SMB1.0
Windows Vista	SMB1.0	SMB2.0	SMB2.0	SMB2.0	SMB2.0	SMB2.0
Windows 7	SMB1.0	SMB2.0	SMB2.1	SMB2.1	SMB2.1	SMB2.1
Windows 8	SMB1.0	SMB2.0	SMB2.1	SMB3.0	SMB3.0	SMB3.0
Windows 8.1	SMB1.0	SMB2.0	SMB2.1	SMB3.0	SMB3.0.2	SMB3.0.2
Windows 10	SMB1.0	SMB2.0	SMB2.1	SMB3.0	SMB3.0.2	SMB3.1.1

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 63

© 2021 Riverbed Technology. All rights reserved.

SMB/RiOS Dependencies

- From a RiOS perspective, the versions needed to support recent versions (i.e. 3.x) of SMB are:
  - SMB3.0.0 latency optimization and SDR is supported in RiOS 8.5+
  - SMB3.0.2 latency optimization and SDR is supported in RiOS 9.0+
  - SMB3.1.1 latency optimization and SDR is supported in RiOS 9.2+
- This is important as SDR needs to be able to see the raw, unencrypted data, so the SteelHead needs to understand the protocol in order to integrate and decrypt/re-encrypt.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

File Locking and Oplocks – Overview

Ensure Safe Concurrent Access

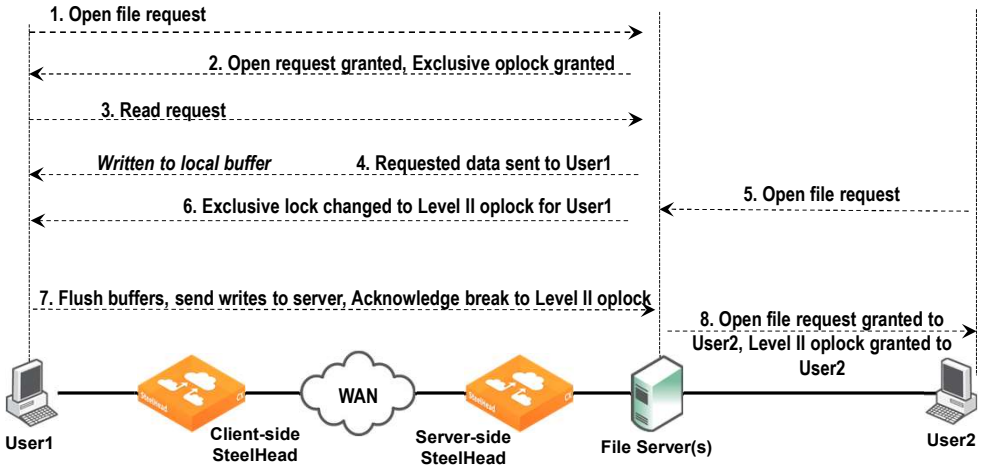
- If a file is shared, consistency needs to be ensured to prevent multiple clients writing simultaneously.
- Oplocks allows a client to be notified by the server when it is:
  - The only client accessing the file, or
  - Accessing the file with other clients that are only reading, not writing
- When a client is granted an oplock it can perform certain actions on the file locally without notifying the server.
- If additional clients request access to the file, remote operations must be synchronised with the server before granting access.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Optimization and Oplocks

SteelHead Only Optimizes Traffic When Oplocks Are Granted



© 2021 Riverbed Technology, Inc. All rights reserved.

Opportunistic Lock – Also known as oplock. A lock requested by a client on a file that resides on a remote server. To prevent any compromise to data integrity, the SteelHead appliance only optimizes data where exclusive access is available (in other words, when locks are granted).

When an oplock is not available, the SteelHead appliance does not perform application-level latency optimizations but still performs Scalable Data Referencing and compression on the data as well as TCP optimizations.

Therefore, even without the benefits of latency optimization, SteelHead appliances still increase WAN performance, but not as effectively as when application optimizations are available.

Types of oplocks that a client may hold:
- Level II oplock
- Exclusive oplock
- Batch oplock

Oplock levels are reduced when conflicting opens are made to a file.

The SteelHead maintains safety and file integrity, thus it reduces optimization to bandwidth-only when a client has shared access to a file instead of exclusive access, in order to ensure file correctness.

© 2021 Riverbed Technology. All rights reserved.

File Locking and Oplocks – Oplock Types

- Batch
  - Generally used by command line applications that repeatedly open many of the same files
  - Allows clients to perform file opens completely without notifying the server
- Exclusive
  - Granted to a client if the file is not already opened by another client
  - Client has sole (*exclusive)* access to the file, so it is safe to cache changes
- Level II
  - Not requested by a client
  - An exclusive oplock can be downgraded to level II by the server if another client needs to access the file, but has not yet performed a write

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 67

RiOS registers these concurrency controls: file locks, share access controls, and oplocks. The RiOS CIFS module tracks the state of every file opened between the client and server, and it uses this state to determine which types of optimized connections can safely be applied to file requests on the clients.

For example, when a client is granted an exclusive oplock on a file, RiOS can safely perform read-ahead and write-behind of file data because it is the only client accessing the file. Some of the CIFS features in RiOS enable more in-depth recognition of concurrency control, like the overlapping open optimization and the applock optimization feature.

© 2021 Riverbed Technology. All rights reserved.

Safe Reading and Writing

Write-Through and Write-Back

- Two modes of writing to a remote file
- Write-Through
  - Client sends data to server for writing and waits for an acknowledgement before sending more data
  - When finished, closes file on server and waits for acknowledgment
  - Safe, but slow across a WAN
- Write-Back
  - Client does not wait for acknowledgement before writing more data
  - Synchronization is forced by the client closing the file or flushing the cache
  - Used in MS Office applications

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 68

The concurrency controls—file locks, shared-access controls, and oplocks—ensure that clients can coordinate their reads and writes in an orderly fashion. In particular, when a client wants to read from a file, it knows that reading from a local cache is safe (for example, through oplocks), or that its reads and writes are coordinated with other clients (for example, through byte range locks).

When a client wants to write data to a file, there are two modes of writing that are supported in CIFS environments: write-through and write-back. The application using CIFS can decide which of these two modes to use every time it needs to write.

For write-through mode, the process falls into a pattern in which the client sends data to the server for writing, waits for an acknowledgment from the server, sends some more data, waits, and repeats this process, until all the data is written and acknowledged. At this point the client sends a CIFS command to close the file on the server. The acknowledgment from the server that the file is closed signals that all data is safely written to disk. The server releases any lock on the file and makes it available for read/write access to other clients. Although this might be the safest way when writing data, when sending data across the WAN, it is not the most efficient method because the round-trip time across the WAN is typically several magnitudes higher than across the LAN.

Write-back mode is a form of optimization in which the client does not need to wait until the write is acknowledged before proceeding with the next operation. Synchronization is forced by the client flushing its cache or closing the file. Microsoft Word and Excel are good examples of applications that use CIFS in a write-back mode. If for any reason there is a problem when the file is closed, the user is informed and the data is recovered using the automatic save mechanism.

In write-back mode, there are several places where data can linger on its way to the disk: the client machine can gather writes, the server file system can delay pushing to disk, and even the server's physical disk subsystem can cache writes in RAID cards or on memory in the disk itself. RiOS provides another place for this temporary buffering between the client and long-term storage to occur during write-back mode.

RiOS honors the client-specified write-back or write-through mode for each write operation. In general, most clients use write-back mode, because the performance of write-through mode—even on local disks, without the added performance impact of WAN-based usage—is unacceptable to end users. RiOS can deliver fast write performance over the WAN in a way that is analogous to how file servers and network attached storage (NAS) appliances deliver fast write performance.

© 2021 Riverbed Technology. All rights reserved.

Security Signatures and SMB Signing – Overview

- Q: What does SMB Signing do?
- A: Appends a message "hash" *with each message*
  - Hash function takes variable length input and returns fixed length output
  - Hash function uses **User Session Key (USK)**
- Q: Why does SMB Signing do this? A: Consider a message, "M" . . .

Given a message, "M" | **M** = "Earnings report came in – bonuses for all!"

Hash the message | **hash(M)** = "da4258096"

- ***If*** @Host2: hash(ReceivedMessage) == Hash sent with message
  then Host2 knows message was not tampered with
- *Is it obvious why Application Streamlining needs to re-sign SMB to work and what SteelHeads would need to perform SMB Signing?*

© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 69

The CIFS protocol includes a feature to cryptographically sign every CIFS protocol datagram between the client and server. The file data that traverses the network is still sent in the clear, even when this option is used, so this CIFS feature does not protect against network snooping. However, it does protect against man-in-the-middle attacks.

The security signature feature is typically controlled through Windows group policy settings, with a separate client-side and server-side three-way setting that controls whether signing is used or not. This policy setting is then used during the initial CIFS session by the client and server to determine whether or not to sign their CIFS sessions.

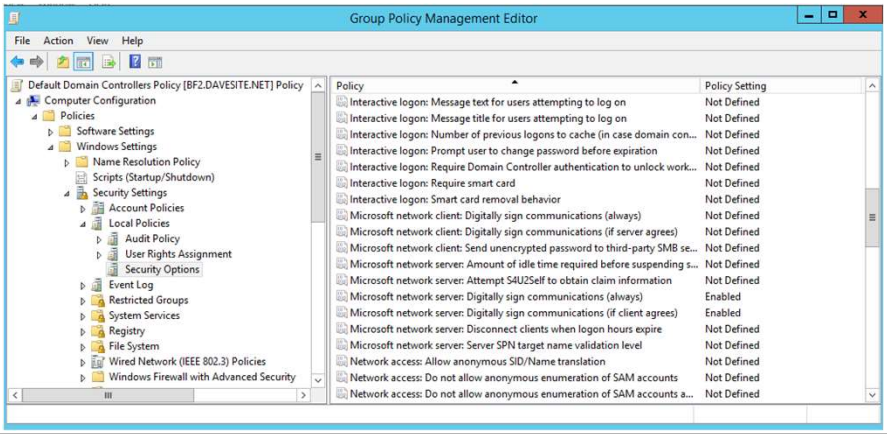
The following table shows the result when a client attempts to connect to a server—either the connection fails due to incompatible settings, or the session can sign the CIFS datagrams.

	Server - Disabled	Server - Enabled	Server - Required
Client - Disabled	Not signed	Not signed	No connections
Client - Enabled	Not signed	Signed	Signed
Client - Required	No connections	Signed	Signed

© 2021 Riverbed Technology. All rights reserved.

SMB Signing - Windows Settings

- Can be configured under Group Policy
- Two settings for both Client and Server connections:
  - Digitally Sign Communications (If Client/Server Agrees) - *Enabled*
  - Digitally Sign Communications (Always) - *Required*



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 70

Note that this is *Required* on Domain Controllers.

© 2021 Riverbed Technology. All rights reserved.

To Sign or Not to Sign?

- Whether a connection is signed or not depends on the settings on both the server and the client.
- For Domain Controllers the default setting is *Required*.

		Server SMB Settings		
		Disabled	**Enabled**	**Required**
Client SMB Settings	**Disabled**	Not-signed	Not-signed	Connection refused
	Enabled	Not-signed	Signed	Signed
	Required	Connection refused	Signed	Signed

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

SMB3 Encryption Overview

- SMB3 encrypts original message and appends a crypto-hash of the message
  - Hash function takes variable length input and returns fixed length output
  - Encryption and hash functions leverage **User Session Key (USK)**
- To visualize this, consider a message, "M" . . .

M = "Earnings report came in – bonuses for all!"

encrypt(M) = **lTzpy7o9+19jacsl0N9FOCEtHfszXNxTwiiyn+H8TlERrW0**

hash(M) = "bi933m0z#6"

Host1

hash(M)	**(encrypt(M)**

Host2

- ***If*** Host2 computes: hash(ReceivedMessage) == hash(M)
  then Host2 knows message was not tampered with

- *Is it obvious why both data & application streamlining need to decrypt SMB to work?*

© 2021 Riverbed Technology, Inc. All rights reserved.

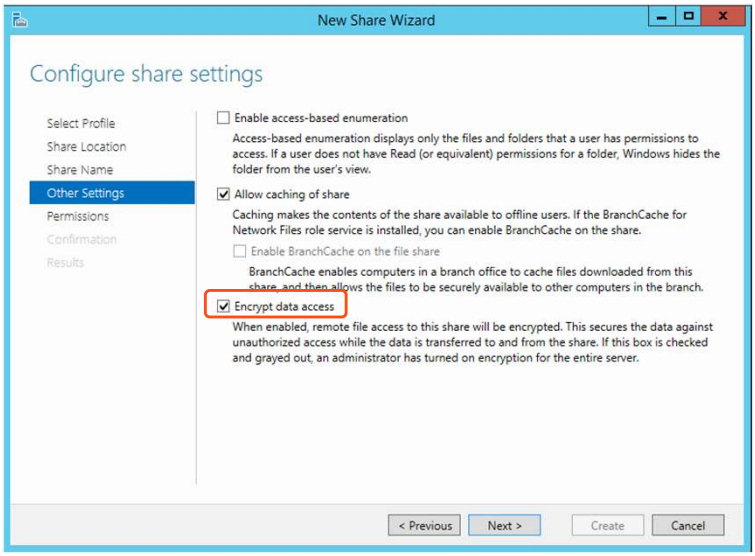
riverbed 72

© 2021 Riverbed Technology. All rights reserved.

Configure SMB3 Encryption in Windows

Use Server Manager

- Can configure either during share creation or later using File and Storage Services



© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Optimize SMB Using Riverbed

SteelHead SMB Optimizations

- Read Ahead
  - Regular and Strided
  - Metadata prefetching and caching
  - Convert multiple requests into one larger request
- Write Behind
  - Convert multiple requests into one larger request
- Dynamic Prediction – use Markov model to predict opens and is considered a read ahead attribute
- Applock (for .doc/.docx & .xls/.xlsx file types) and Print optimization
- Disables automatically (by default, allowing bandwidth reduction and TCP optimizations only) if SMB signing enabled and not configured, or oplock lost
- Traffic on ports 445 and 139 automatically intercepted and optimized

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 74

© 2021 Riverbed Technology. All rights reserved.

Configure CIFS (SMB1) Optimization

- Enabled by default
- Can enable or disable specific features

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 75

Enable Latency Optimization - Enables SMB1 optimized connections for file opens and reads. Latency optimization is the fundamental component of the CIFS module and is required for base-optimized connections for file opens and reads. Although latency optimization incorporates several hundred individual optimized connection types, the most frequent type of file opens is where exclusive opportunistic locks have been granted, and read-ahead operations are initiated on the file data. RiOS optimizes the bandwidth used to transfer the read-ahead data from the server side to the client side.

Disable Write Optimization - Prevents write optimization. If you disable write optimization, the SteelHead still provides optimization for CIFS reads and for other protocols, but you might experience a slight decrease in overall optimization. Most applications operate safely with write optimization because CIFS allows you to explicitly specify write-through on each write operation. However, if you have an application that doesn't support explicit write-through operations, you must disable it in the SteelHead.

Optimize Connections with Security Signatures (that do not require signing) - This feature automatically stops Windows SMB signing. SMB signing prevents the SteelHead from applying full optimization on CIFS connections and significantly reduces the performance gain from a SteelHead deployment. Because many enterprises already take additional security precautions (such as firewalls, internal-only reachable servers, and so on), SMB signing adds minimal additional security at a significant performance cost (even without SteelHeads).

Enable Dynamic Write Throttling - Enables the CIFS dynamic throttling mechanism that replaces the current static buffer scheme. When there's congestion on the server side of the optimized connection, dynamic write throttling provides feedback to the client side, allowing the write buffers to be used more dynamically to smooth out any traffic bursts. We recommend that you enable dynamic write throttling because it prevents clients from buffering too much file-write data. This is the default setting. If you enable CIFS dynamic throttling, it's activated only when there are suboptimal conditions on the server side causing a backlog of write messages; it doesn't have a negative effect under normal network conditions.

Enable Applock Optimization - Enables CIFS latency optimizations to improve read and write performance for Microsoft Word (.doc) and Excel (.xls) documents when multiple users have the file open.

Enable Print Optimization - Improves centralized print traffic performance. For example, when the print server is located in the datacenter and the printer is located in the branch office, enabling this option speeds the transfer of a print job spooled across the WAN to the server and back again to the printer. By default, this setting is disabled.

Enable this control on the client-side SteelHead. Enabling this control requires an optimization service restart.

© 2021 Riverbed Technology. All rights reserved.

Optimize SMB2/3

SMB2 and 3 Support

- SMB2 support
  - RiOS supports latency and bandwidth reduction for native SMB2 clients and servers.
- SMB3 support
  - Enabling SMB3 also enables support for SMB3.1.1 and 3.0.2.
  - SMB3 supports encryption between the client and server.
    - SMB2/3 must be configured to optimize this.
  - To benefit from both latency and bandwidth optimization for SMB3.1.1, SMB2/3 and SMB2 signing must both be enabled and configured.
    - For NTLM-authenticated domains, the server-side SteelHead must be joined to the domain in Active Directory Integrated (Windows 2008 or later) mode.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 76

SMB3.1.1 adds these encryption and security improvements:

- Encryption - The SMB3.1.1 encryption ciphers are negotiated per-connection through the negotiate context. Windows 10 now supports the AES-128-CCM cipher in addition to AES-128-GCM for encryption. SMB3.1.1 can negotiate to AES-128-CCM to support older configurations. Encryption requires that SMB2 signing is enabled on the server-side SteelHead in NTLM-transparent (preferred) or NTLM-delegation mode, and/or end-to-end Kerberos mode. Domain authentication service accounts must be configured for delegation or replication as needed.
- Preauthentication Integrity - Provides integrity checks for negotiate and session setup phases. The client and server maintain a running hash on all of the messages received until there’s a final session setup response. The hash is used as input to the key derivation function (KDF) for deriving the session secret keys.
- Extensible Negotiation - Detects man-in-the-middle attempts to downgrade the SMB2/3 protocol dialect or capabilities that the SMB client and server negotiate. SMB3.1.1 dialect extends negotiate request/response through negotiate context to negotiate complex connection capabilities such as the preauthentication hash algorithms and the encryption algorithm.

© 2021 Riverbed Technology. All rights reserved.

Configure SMB2/3 Optimization

SteelHead Configuration

- SMB2 and SMB3 optimization needs enabling on both the server- and client-side SteelHead (so they can both 'talk' SMB2/3).
- Can also enable optimization for Distribution File System (DFS) file shares.

© 2021 Riverbed Technology, Inc. All rights reserved.

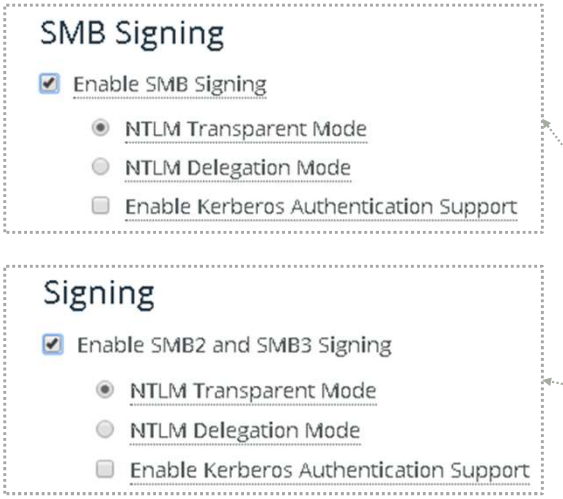
riverbed 77

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

© 2021 Riverbed Technology. All rights reserved.

Configuring SMB2/3 Signing

SteelHead Configuration



- Signing requires AD Integration
  - Just needs enabling on server-side SteelHead
  - Also required in order to optimize SMB3 encrypted connections
  - Separate boxes under configuration pages for
    - CIFS (SMB1)
    - SMB2/3

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Overlapping Open Optimization

Use With Care!

- In order to optimize SMB, the Server-Side SteelHead needs to maintain an exclusive oplock.
- Sometimes this cannot happen for the following reasons:
  - Application making multiple, conflicting opens of the same file
  - Client not asking for oplock
  - Server not granting oplock
- Enabling this feature client-side changes the way the SteelHead deals with oplocks, BUT at the price of denying simultaneous access for unoptimized clients.
- This can give a big performance boost for some drawing packages.

© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 79

When Riverbed first introduced this feature back in RiOS 3.0 it was turned on by default and caused countless support calls.

The problem is that, once a connection is optimized, the server-side SteelHead establishes an exclusive oplock and will not relinquish this until the file is closed. This means that clients accessing this file from locations without a SteelHead, or locally, cannot access the file, not even read-only as this would require the server-side SteelHead dropping to a level II oplock. SteelHead-optimized clients have access as normal because the server-side device talks to the client-side SteelHead and gives it the data it requires. Only if you are sure that there will be no local or unoptimized clients should you enable this.

The Applock feature achieves the same effect for Office documents but without the drawbacks.

© 2021 Riverbed Technology. All rights reserved.

HOL1152

Optimizing SMB-signed File Services

In this lab, you will:

- Optimize SMBv2/v3 in a Windows Domain

Duration: **30 minutes**

eLab system: link and access details provided in your course confirmation email

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 80

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation – Overview

- Normally the SteelHead appliances 'learn' the data dynamically.
- Occasionally this 'learning' approach is insufficient.
  - E.g., one-off transfers of large .jpg or .avi files
- The solution is *CIFS Prepopulation.*
- Prepopulation = SDRing data before the client has asked for it.
- This avoids the penalty of a cold transfer, giving warm performance immediately.
- BUT - *This only works if you know in advance what the client is going to request.*

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 82

Under normal circumstances the SteelHeads learn the pattern of data and gradually populate their data stores with the segments and references that they require.

However, there are times when this *learning* approach is insufficient, e.g. one-off transfers of large compressed or encrypted files.

© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation – Traffic Flow

- Importantly, the client is the client-side SteelHead's Primary Port
- This *must* route via the LAN port of the SteelHead
- Many support tickets raised by not following this golden rule!

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation – Configuration Overview

The basic steps for configuring CIFS prepopulation are very simple:

1. Enable CIFS Prepopulation
2. Add a Prepopulation Share (but make sure you have your credentials ready)
3. Configure the Scheduled Synchronization
4. Add a Policy and Rules (e.g., just pre-pop .jpg files)

These are all performed on the client-side SteelHead.

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation Config (1/4)

Enable CIFS Prepopulation

- Click **Enable CIFS Prepopulation** and then click **Apply**.
- A new table of *Prepopulation Shares* will appear at the bottom of the page.

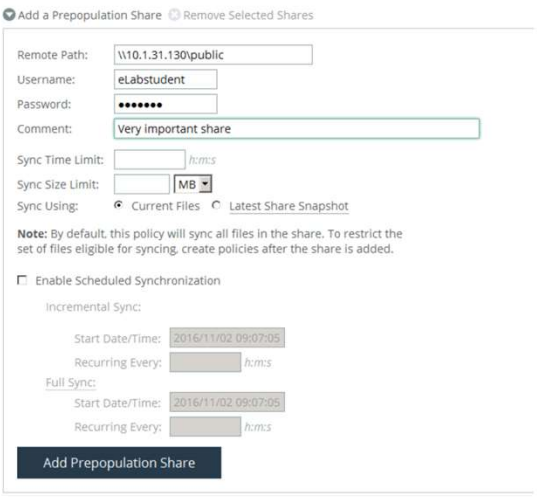
© 2021 Riverbed Technology, Inc. All rights reserved.

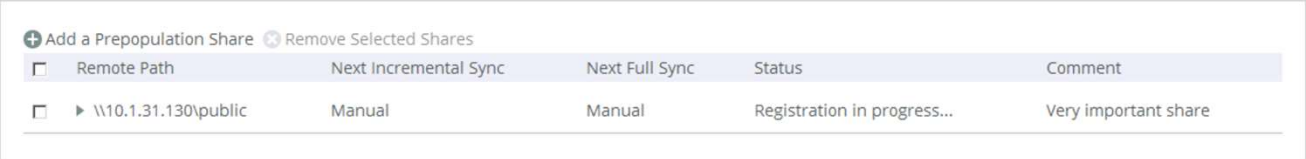
© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation (2/4)

Add a Prepopulation Share

- Click **Add a Prepopulation Share**.
- Fill in the share details.
- Click the **Add Prepopulation Share** button to register the share.
- The share will appear in the list of Prepopulation Shares.





© 2021 Riverbed Technology, Inc. All rights reserved.

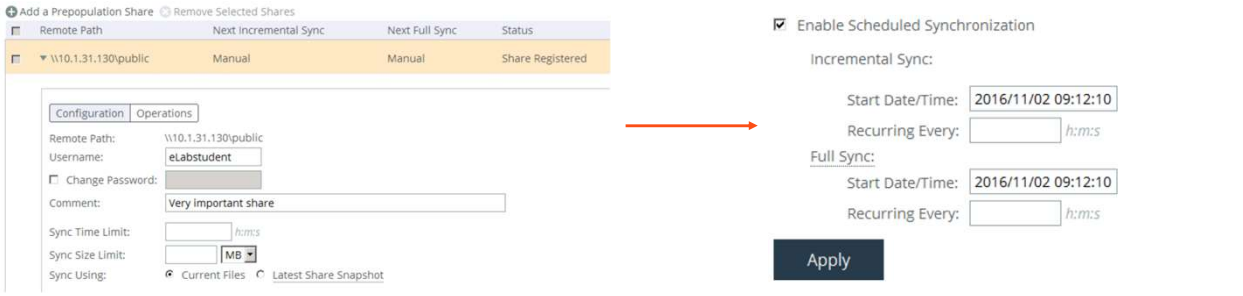
riverbed 86

© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation (3/4)

Configure the Scheduled Synchronization

- Click the arrow next to the share to expand.
- Ensure that the **Configuration** tab is selected.
- Scroll down, select **Enable Scheduled Synchronization** and configure the *sync schedule*. *(note the default start time is immediately…)*
- Click **Apply** to commit settings.



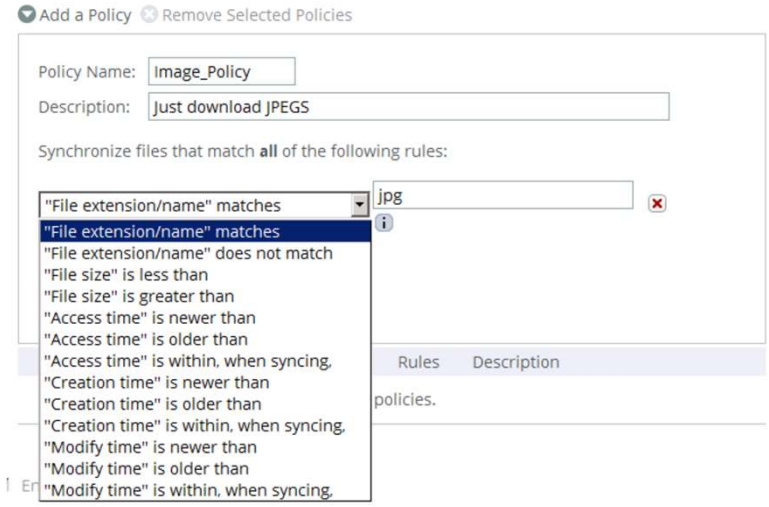
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

CIFS Prepopulation (4/4)

4. Add a Policy and Rules

- Click the arrow next to the share to expand.
- Expand **Add a Policy**.
- Select the condition and the relevant parameter.
- Example use:
  - Create a policy to download all PPTs
  - Create a policy to download all new files
- When finished, click **Add Policy**.



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 88

© 2021 Riverbed Technology. All rights reserved.

Putting it all Together – Real World Use Case

Scenario	A large healthcare company needed to access X-ray images stored on a central server to be used during appointments with patients.
Issue	The bandwidth was insufficient to transfer the files in a satisfactory time. The images were also large and compressed making the data unique every time, so SDR could not help very much.
Solution	The solution was to configure CIFS prepopulation at the local branch office SteelHead. The customer configured this to run every evening, ensuring that the next day's images had been prepopulated overnight, resulting in a warm transfer of the data as soon as the medical professional required them.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 89

We had a customer that needed to examine X-ray images on a central server when they had an appointment with their patients.

Unfortunately the bandwidth was insufficient and as the images were large and compressed, the data was unique every time, so SDR could not help very much.

The solution was to configure CIFS prepopulation at the local branch office SteelHead.

What this does is connect to the share at a certain, pre-defined interval and then pull down the data from a central share, SDRing the data before it is actually required.

The customer in question configured this to run every evening, ensuring that the next day's images had been prepopulated overnight, resulting in a warm transfer of the data as soon as the medical professional required them.

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Verify Optimization – Current Connections Report

- The connection should show up as *SMB30-SIGNED* under the *Current Connections Report*.
- The user account used to connect should also be listed.

CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time	Application	User Identity
		10.1.21.110:51664	10.1.31.140:445	10	8	23%	2019/06/12 07:41:29	SMB30-SIGNED	dmurphy@cyberdyne.corp

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 91

© 2021 Riverbed Technology. All rights reserved.

Verify Optimization – Current Connections Details

Current Connections Report – Details

- Expanding the connection should yield further information.

Connection type:	RiOS + SCPS
Connection age:	44 seconds
Application:	SMB30-SIGNED
User Name:	dmurphy
User Domain:	cyberdyne.corp
Transport:	TRANSPORT_ID_NONE
Notes:	In-path SDR optimized LZ compressed Client side SCPS initiate: WAN side

Refresh Data
Send Keep-Alive
Reset Connection

Log for this SteelHead

Source 10.1.21.110:51664

SH 10.1.120.21:7801
SteelHead VCX 9.8.0 **(YOU ARE HERE)**
10.1.120.21:11085

Transparency mode: Correct Addressing
Congestion control: New Reno

SH 10.1.130.31:7800
SteelHead VCX 9.8.0

Destination 10.1.31.140:445

	LAN side	WAN side
Bytes	10,748	8,551
Packets	52	112
Retransmitted	0	0
Fast retransmitted	0	0
Timeouts	0	0
Congestion window	6	10

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 92

© 2021 Riverbed Technology. All rights reserved.

File System Protocol Errors

CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time	Application
		10.1.21.110:50883	10.1.31.140:445	4	7	0%	2016/06/08 13:38:05	SMB2-SIGNED
		10.1.21.110:61143	10.1.31.140:445	4	5	0%	2016/06/08 13:38:16	SMB2
		10.1.21.110:63548	10.1.31.140:445	92	77	16%	2016/06/08 13:42:00	SMB2

- Protocol error (red triangle icon) means no latency optimization and maybe no SDR.
  - Use the available tools to help figure it out

Connection type:	RiOS + SCPS
Connection age:	49 seconds
Application:	SMB21
Application error:	SMB2_DISABLED
Transport:	TRANSPORT_ID_NONE
Notes:	In-path
	SDR optimized
	LZ compressed
	Client side
	SCPS initiate: WAN side

- Check the logs too (example from a different connection…)

```
Jun 28 12:24:45 chief-sh222 sport[12719]: [smbmux_sfe.NOTICE] 81 {10.12.11.85:51269
10.12.5.33:445} SMB2 parser not being created: connection blacklisted for SMB2.
```

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 93

In this slide, we see information from two different connections; one shown via the GUI, the other via CLI.

First, the GUI at the top of the page shows the ‘collapsed’ connection information. Note the protocol error. That’s OK, it’s our job to figure out what’s going on.

We click the magnify glass and get the screen in the middle. The message says that signing is in use. That should not be a problem, and recall SMB2 is off by default. In this case, SMB2 signing optimization had not been enabled.

The CLI shows a syslog connection detail saying “CONNECTION_BLACKLISTED” and the log line shows the same thing.

Use the connection details and logs to very quickly understand the issue. You are encouraged to introduce errors in a lab environment and look at the resulting error messages.

© 2021 Riverbed Technology. All rights reserved.

Troubleshooting and Protocol Blacklists

- If SMB2/3 signing and/or SMB2/SMB3 optimization have not been configured:
  - Signed SMB2/SMB3 connections will get no latency optimization
  - Unencrypted SMB2/3 connections will still get SDR/LZ optimization
  - SMB3 encrypted connections will be passed through
- Blacklists avoid repeated problems due to configuration issues.
  - CIFS / SMB2 = 20 minutes
  - *Remember to check blacklists during debugging!*
- Check all blacklists on both SteelHeads via CLI:
  - For SMB1
    ```
    # show protocol cifs smb signing blacklist
    # no protocol cifs smb signing blacklist
    ```
  - For SMB2 & SMB3
    ```
    # show protocol smb2 signing blacklist
    # no protocol smb2 signing blacklist
    ```

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 94

The first time you do this you will probably encounter the red triangle of doom in *Current Connections.* Firstly, *don't panic,* as there are a number of commands to help you solve these problems.

The two most useful commands are:
 # show protocol smb2 signing blacklist

and

 # no protocol smb2 signing blacklist

© 2021 Riverbed Technology. All rights reserved.

Putting it all Together – Real World Use Case

Scenario	An large, international coach making company had offices worldwide. They used a CAD application that accessed a central share in their UK from offices throughout the world. Editing and sharing files using SMB was an essential part of their business.
Issue	Due to the nature of how the CAD application opened and re-wrote many small files, they had to install local servers in many of their remote sites because opening a single CAD file without this, from Hong Kong to London, took over an hour! This was due to the round trip time multiplied by the dozens of files needed for a single drawing.
Solution	Riverbed ran a Proof of Concept, and even the cold transfer reduced the file opening time from over an hour to less than 5 minutes. A warm, or slightly modified file took just a few seconds. This enabled them to finally consolidate their infrastructure and store all files centrally.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 95

© 2021 Riverbed Technology. All rights reserved.

HOL1153

CIFS Prepopulation

In this lab, you will:

- Pre-populate CIFS File Share at Branch Office

Duration: **30 minutes**

eLab system: link and access details provided in your course confirmation email

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 96

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

The Importance of Email to the Modern Business

- A fast, secure email system is essential to the modern business for the following reasons:
  - Immediacy
  - Global reach
  - Record keeping
  - Targeted marketing
  - Reduced costs
  - Efficiency

- None of these business benefits will happen if emails are too slow due to poor WAN performance.
- Riverbed can optimize mail traffic, improving user experience and realizing the benefits listed above.

© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 98

Long gone are the days when snail mail was sufficient. In the connected enterprise fast access to emails is essential. Email brings the following benefits:

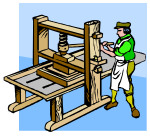
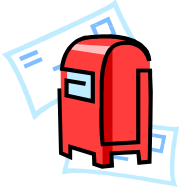
- **Immediacy** - Rather than having to wait a day or more for conventional mail to be delivered and then responded to, email communication is almost instantaneous. This leads to streamlined business processes, enabling decisions and authorizations to be communicated in hours, even minutes. The result is improved productivity as more can be accomplished in less time.
- **Global reach** - For a large, global business, email reduces global barriers, allowing workers worldwide to communicate across time zones. As a case in point, this module was written in the UK and the PPT will was emailed to the rest of the team in the US when finished. They then reviewed and gave feedback within hours. Imagine trying to do the same thing with conventional mail!
- **Record keeping** - Emails remain in a user's inbox unless they are intentionally deleted. This allows users to search through emails very quickly to extract important documents – far easier than searching through physical documentation. Also, modern software exists to securely archive email and store for years in the event of legal disputes.
- **Targeted marketing** - Businesses can send marketing and sales emails in a quick, automated fashion, to specifics groups of customers, perhaps notifying them of product updates or discounts.
- **Reduced costs** - Sending large documents by post can be expensive. With email, you can send many documents to many recipients with zero printing or delivery costs. Sure, there will be a cost for maintaining a mail server but this is relatively low.
- **Efficiency** - Good use of email can reduce the reliance on face-to-face meetings and phone conversations, speeding up and transforming business processes.

© 2021 Riverbed Technology. All rights reserved.

Evolution of Microsoft Exchange Protocols

MAPI/Encrypted MAPI

- The 'classic' MS Exchange mail protocol used up to Exchange 2010
- An abbreviation of *Messaging Application Programming Interface*
- Not so much a protocol as an access method using a set of C libraries over the RPC protocol. Should be called *MAPI/RPC*.
- The client connects to port 135 and is then re-mapped to a dynamic port.
- Encrypted MAPI (eMAPI) has been the default since 2007.
- Riverbed has supported encrypted MAPI since RiOS 5.

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 99

When Riverbed first started optimizing Exchange traffic the current version of Exchange was Exchange 2003. This used the classic MAPI protocol. This stands for *Messaging Application Programming Interface* and is not, strictly speaking, a protocol in its own right but an access method using a set of C libraries.

The main transport method used was Microsoft's *Remote Procedure Calls,* or RPC, leading to the term MAPI/RPC.

The client would connect to the server using port 135 and then be re-mapped to a dynamic higher-level port.

There is also the option to encrypt MAPI (eMAPI) communications, which Riverbed brought in support for in RiOS 5.

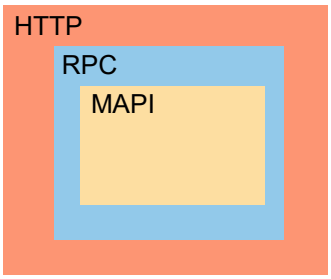
This is an important feature/configuration as modern versions of Outlook/Exchange tend to encrypt MAPI by default.

© 2021 Riverbed Technology. All rights reserved.

Evolution of Microsoft Exchange Protocols

Outlook Anywhere (RPC/HTTP)

- Introduced with Exchange 2007
  - Was actually in Exchange 2003 but called RPC over HTTP
- Key advantage over MAPI/RPC is the server is now connected over a known port
- Much better from the point of view of firewall configurations
- It uses an RPC Proxy, enabling Outlook clients to connect over the internet
- Remote users can connect to their Exchange server without a VPN
- Usually transported over HTTPS
- MAPI can additionally be encrypted



MAPI is double-wrapped

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 100

Exchange 2007 brought about a change by introducing *Outlook Anywhere.*

This had actually been around in Exchange 2003 but used the more technical term RPC over HTTP.

This had a big advantage over MAPI/RPC as the server could now be connected to over a known, rather than dynamic port, which is much better from the point of view of firewall configurations.

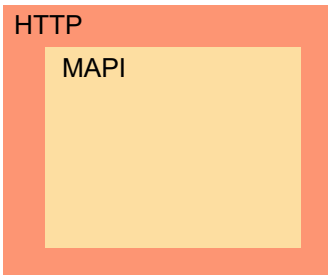
It also uses an RPC Proxy which enables Outlook clients to connect over the internet. The RPC proxy is located on the RPC server's network (typically a DMZ) and can accept requests from the internet, enabling remote users to connect to their Exchange server without a VPN.

© 2021 Riverbed Technology. All rights reserved.

Evolution of Microsoft Exchange Protocols

MAPI/HTTP

- New transport protocol
- Introduced with Exchange 2013 SP1 and Outlook 2013 SP1
- Long-term replacement for RPC/HTTP
- MAPI/RPC has been removed from Exchange 2013
- RPC encapsulation within HTTP has now been removed
  - MAPI now encapsulated directly within HTTP
- Will require fewer concurrent TCP connections
  - Great for Admission Control on the SteelHead
- Improves network resiliency and performance



MAPI is single-wrapped

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 101

MAPI over HTTP is a new transport protocol used to connect Outlook and Exchange.

MAPI/HTTP was first delivered with Exchange 2013 SP1 and Outlook 2013 SP1.

It is the long term replacement for RPC over HTTP and is now the main method for Outlook clients connecting to an Exchange server, **with MAPI/RPC now removed from Exchange 2013**.

The following excellent TechNet blog explains the connectivity and the reasons for moving to it:
https://blogs.technet.microsoft.com/exchange/2014/05/09/outlook-connectivity-with-mapi-over-http/

© 2021 Riverbed Technology. All rights reserved.

Other Exchange Communication Methods

Outlook Web App

Regular HTTP traffic. No special client requests. Everything done on Server.

- **OWA: Outlook Web App** is a web browser mail interface
  - Formerly “Outlook Web Access” and “Exchange Web Connect”
- **No RiOS specific mail optimizations**
  - Benefit from SSL + HTTP for attachments

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Other Exchange Communication Methods

Exchange Web Services

Client sends requests via HTTP. Server returns data. Client uses data in custom app.

- Exchange Web Services - EWS
  - Used by MAC clients to access Exchange
  - Used by Lync on all platforms to obtain free / busy data
- No RiOS specific mail optimizations
  - Will see benefit from SSL + HTTP for attachments

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

How Riverbed can Help – MAPI over HTTP

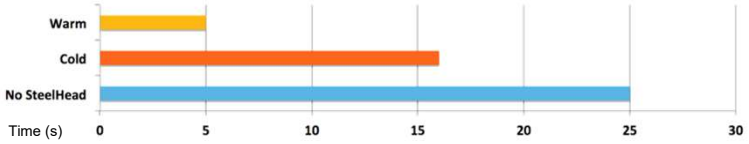
Don't Let Upgrading Slow You Down

For the latest email, SteelHead speeds communication and saves bandwidth.

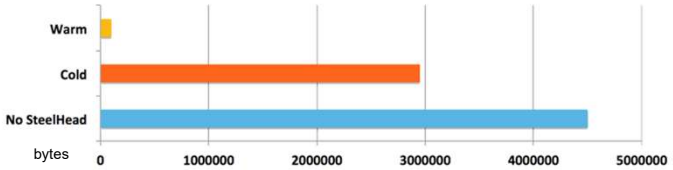
Exchange

Office 365

Up to 5X Faster



Up to 98% Data Reduction



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 104

With Exchange 2013 SP1 and later versions, OA utilizes the MAPI over HTTP protocol - in effect it is actually MAPI over HTTPS, which stands for secure and encrypted.

To show the effectiveness of SteelHead, a 'send file attachment' operation was performed using Outlook 2013 SP1 and Exchange 2013 on premise with MAPI over HTTP enabled over a 5Mbps link and 100ms latency.

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – MAPI Optimizations

- MAPI optimization does not require a separate license and is enabled by default.
- RiOS MAPI optimizations enabled by default include:
  - Read ahead on emails and attachments
  - Write behind on emails and attachments
  - Folder Synchronization
  - Prepopulation
- Optimizations that need to be configured:
  - Encrypted MAPI
  - Outlook Anywhere
  - MAPI/HTTP

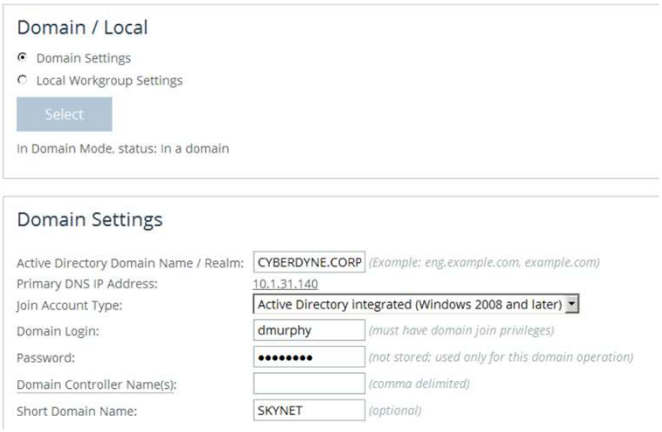
© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 105

© 2021 Riverbed Technology. All rights reserved.

Encrypted MAPI Optimization – Domain Join

- Step-By-Step Procedure:
  1. Join Server-Side SteelHead to the same domain as the Exchange Server.
     - This has been covered in detail in another module.



© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 106

To enable the SteelHead to optimize encrypted MAPI traffic between the Outlook client and the Exchange server:

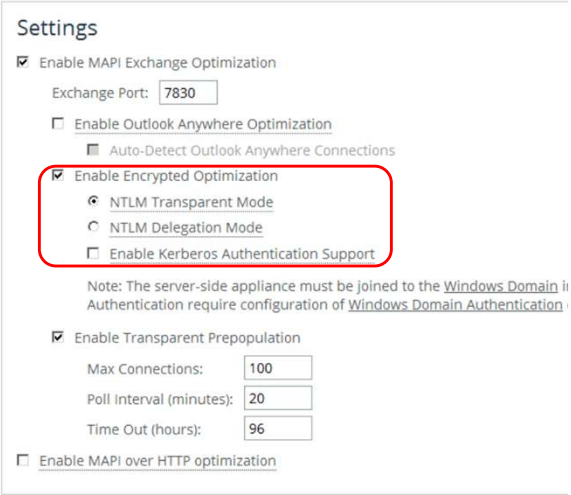
1. Join the server-side SteelHead to the same Windows domain that the Exchange server belongs to and operates as a member server. The server-side SteelHead must be able to ping the domain controller by name. You can use an adjacent domain (through Cross-Domain support) if the SteelHead is running RiOS 6.1 or later.
2. Enable the Encrypted Optimization option on client-side and server-side SteelHeads involved in optimizing MAPI encrypted traffic. Alternatively, use the **protocol mapi encrypted enable** command.
3. Use transparent mode for all client types. Delegation mode is a legacy feature and should be migrated to transparent mode, unless you have a specific need for Kerberos Constrained Delegation.
4. Restart the service on all SteelHeads that have the Encrypted Optimization option enabled.
5. Under *Current Connections,* verify that the SteelHead is optimizing the encrypted MAPI traffic.

© 2021 Riverbed Technology. All rights reserved.

Encrypted MAPI Optimization – MAPI Settings

2. Enable encrypted MAPI optimization on all SteelHead appliances participating in the optimization.
3. Use Transparent Mode for all client types (Delegation Mode has been deprecated). If using Kerberos ensure that you have also configured a replication user.
4. Restart the optimization service.

```
protocol mapi encrypted enable
```



© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Encrypted MAPI Optimization (Opt) – Validation

5. Under *Current Connections* verify that the SteelHead is optimizing the encrypted MAPI traffic. Note the SteelHead MAPI port of 7830.

▸	»	10.0.1.16:50273	10.33.248.40:7830	14,019	481	96%	2014/10/24 11:34:15	MAPI
▸	»	10.0.1.16:50274	10.33.248.40:7830	3,982	225	94%	2014/10/24 11:34:15	MAPI

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 108

It is worth mentioning that MAPI admission control preemptively closes the MAPI session to reduce the connection count in order to bring the SteelHead out of admission control.

MAPI sessions are closed in the following order:
- MAPI prepopulation connections
- MAPI sessions with the largest number of connections
- MAPI sessions with the most idle connections
- The oldest MAPI session
- MAPI sessions exceeding the memory threshold

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – RPC/HTTP Overview

Configure Outlook Anywhere Optimization (RPC/HTTP)

- Step-By-Step Procedure:
  1. Enable SSL on both the client- and server-side SteelHeads (see later module for details).
  2. Install the certificate and key from the Outlook Anywhere IIS HTTP server on the server-side SteelHead.
  3. Create an in-path rule on the client-side SteelHead to identify Outlook Anywhere traffic:
     - If IIS HTTP server is only used for RPC Proxy, use Latency Optimization Policy: Outlook Anywhere and disable auto-detect under MAPI settings.
     - If IIS HTTP server is also handling web sites, use Latency Optimization Policy: Normal and enable auto-detect under MAPI settings.

© 2021 Riverbed Technology, Inc. All rights reserved.
riverbed 109

To configure Outlook Anywhere optimization complete the following steps:

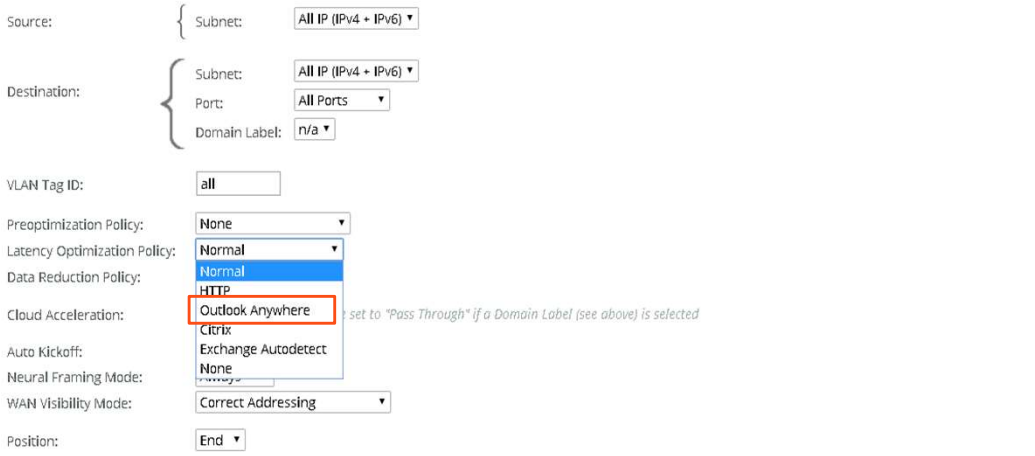
1. Enable SSL on both the client- and server-side SteelHeads (see later module for details).
2. Install the certificate and key from the Outlook Anywhere server on the server-side SteelHead.
3. As part of the configuration, on the client-side SteelHead, ensure that port 443 is removed from the secure port label OR, if the RPC proxy is dedicated to use with Outlook Anywhere, create an in-path rule to the RPC Proxy (IIS) server with a pre-optimization policy of SSL and a latency optimization policy of Outlook Anywhere.
4. On the client-side and server-side SteelHead, choose *Optimization* > *Protocols: MAPI*.
5. Select *Enable Outlook Anywhere Optimization*.
6. Select *Auto-Detect Outlook Anywhere Connections* (important if the RPC proxy also hosts other web services).
7. Click *Apply*.
8. Verify that you see a Current Connection with the application type *MAPI-OA.*

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – RPC/HTTP In-Path Rule

Configure Outlook Anywhere Optimization (RPC/HTTP)

- Create the in-path rule:



© 2021 Riverbed Technology, Inc. All rights reserved.

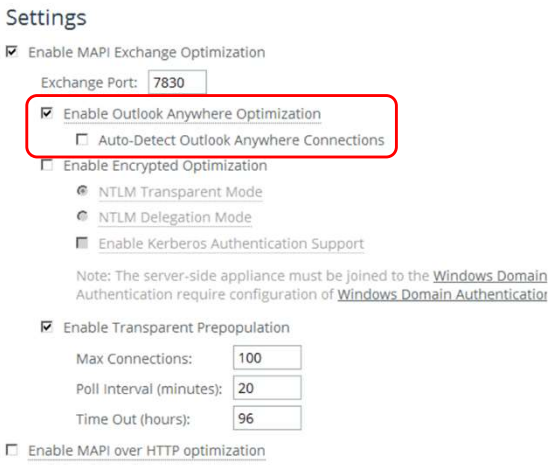
riverbed 110

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – RPC/HTTP Settings

Configure Outlook Anywhere Optimization (RPC/HTTP)

4. On both SteelHead appliances, select **Enable Outlook Anywhere Optimization**.
5. If the IIS proxy also hosts other web services, select **Auto-Detect Outlook Anywhere Connections**.
6. Click **Apply**.



© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – RPC/HTTP Verification

Configure Outlook Anywhere Optimization (RPC/HTTP)

8. Verify that you see Current Connections with the application type *MAPI-OA* or *eMAPI-OA*.

10.0.1.16c49848	10.33.248.40:443	22,615	7,664	66%	2014/11/10 12:20:10	eMAPI-OA
10.0.1.16c49849	10.33.248.40:443	202	22	89%	2014/11/10 12:20:11	eMAPI-OA
10.0.1.16c49851	10.33.248.40:443	198	116	41%	2014/11/10 12:20:30	eMAPI-OA
10.0.1.16c49852	10.33.248.40:443	15,799	363	97%	2014/11/10 12:20:31	eMAPI-OA

Note that to optimize encrypted MAPI you will also have to follow the steps under ***Configure Encrypted MAPI Optimization****.*

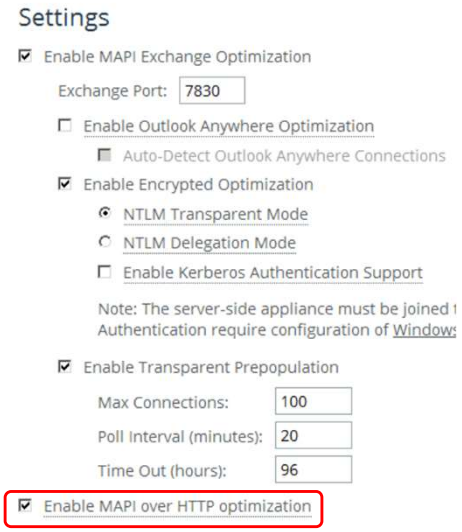
© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – MAPI/HTTP Setting

Configure MAPI/HTTP Optimization

- MAPI/HTTP optimization was introduced in RiOS 9.1 but for bandwidth only.
- RiOS 9.2 added latency optimization.
- Step-By-Step Procedure:
  1. Enable SSL on both the client- and server-side SteelHead appliances (see the SSL module for the details on this).
  2. Install the server (IIS) certificate on the server-side SteelHead.
  3. Under MAPI settings, select **Enable MAPI over HTTP optimization**.



© 2021 Riverbed Technology, Inc. All rights reserved. riverbed 113

If you are using Exchange 2013 SP1 then this is relevant. Microsoft removed MAPI/RPC in this version so you will be either using RCP/HTTP or MAPI/HTTP. For the latter you will need RiOS 9.1 or, ideally 9.2, which has full latency support, on all SteelHeads participating in the optimization

To use MAPI/HTTP you must enable MAPI over HTTP on all Client Access Servers (CAS) across the Exchange deployment.

With Exchange Server 2016, MAPI over HTTP is enabled by default at the organization level. Even with MAPI over HTTP enabled, the Exchange server can still use RPC over HTTP (Outlook Anywhere) for any Outlook clients that are not MAPI over HTTP capable.

The steps to configure MAPI/HTTP are fairly similar to configuring RPC/HTTP and are as follows:

1. Enable SSL on both the client- and server-side SteelHead appliances (see the SSL module for the details on this).
2. Install the server (IIS) certificate on the server-side SteelHead.
3. Under MAPI settings, enable *MAPI over HTTP optimization.*
4. Change the default in-path rule to have a latency policy of *Exchange Autodetect,* or create a specific one with the *Exchange Autodetect* latency policy, a destination port of 443 and a pre-optimization policy of SSL.
5. Verify under *Current Connections* that the *Application Type* is *MAPI-HTTP.*

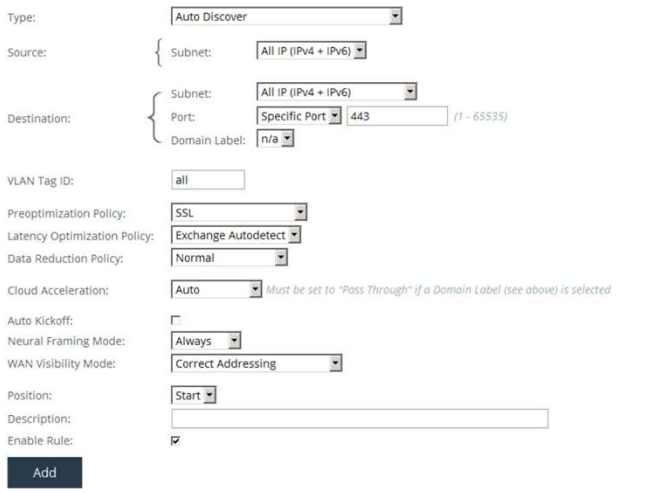
© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – MAPI/HTTP In-Path Rule

Configure MAPI/HTTP Optimization (Continued)

4. Create a new default in-path rule with a latency policy of *Exchange Autodetect* and destination port of *443*.

   This should only be applied to HTTP(S) traffic and will automatically detect the MAPI transport protocol (MAPI/HTTP, OutlookAnywhere, HTTP).



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 114

© 2021 Riverbed Technology. All rights reserved.

Optimize Exchange Traffic – MAPI/HTTP Verification

Configure MAPI/HTTP Optimization (Continued)

5. Verify under Current Connections that the Application Type is *MAPI-HTTP*.

CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time	Application
		10.5.156.61:52575	10.5.156.36:443	23	20	10%	2015/03/27 09:06:03	MAPI-HTTP
		10.5.156.61:52576	10.5.156.36:443	26	26	1%	2015/03/27 09:06:04	MAPI-HTTP
		10.5.156.61:52705	10.5.156.36:443	1,669	1,471	11%	2015/03/27 09:09:48	MAPI-HTTP
		10.5.156.61:52714	10.5.156.36:443	1,759	1,514	13%	2015/03/27 09:10:01	MAPI-HTTP
		10.5.156.61:52716	10.5.156.36:443	46	32	30%	2015/03/27 09:10:02	MAPI-HTTP
		10.5.156.61:52721	10.5.156.36:443	20	16	18%	2015/03/27 09:10:10	MAPI-HTTP
		10.5.156.61:52735	10.5.156.36:443	2	1	53%	2015/03/27 09:10:40	HTTP

Note that to optimize encrypted MAPI you will also have to follow the steps under ***Configure Encrypted MAPI Optimization****.*

© 2021 Riverbed Technology, Inc. All rights reserved.

© 2021 Riverbed Technology. All rights reserved.

MAPI over HTTP Admission Control – Overview

- A MAPI session is comprised of a collection of multiple TCP connections from an Outlook client to the Exchange server.
- MAPI differs from other protocols because the TCP connections of a session are not independent of other TCP connections from the same session.
- All TCP connections between the client and server must be either optimized or unoptimized. If you optimize only some of the connections, the session fails.
- You must optimize all client MAPI connections by the same pair of client-side and server-side SteelHeads, or have them all set to pass through. If the connections are not optimized by the same pair of SteelHeads the session fails.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 116

When you use an Exchange server and the clients are using Microsoft Outlook, Outlook initiates and maintains multiple TCP connections with the Exchange server. A MAPI session is the collection of multiple TCP connections from an Outlook client.

When Microsoft Outlook connections are optimized, the SteelHead remaps contexts to prevent inadvertent mixing of optimized and non-optimized traffic. MAPI differs from other protocols because the TCP connections of a session are not independent of other TCP connections from the same session.

Because of how Exchange servers interact with MAPI sessions, you must optimize all client MAPI connections by the same pair of client-side and server-side SteelHeads, or have them all set to pass through. If you optimize only some of the connections, the session fails. If the connections are not optimized by the same pair of SteelHeads the session fails.

© 2021 Riverbed Technology. All rights reserved.

MAPI over HTTP Admission Control – Configuration

- Can enable MAPI over HTTP Admission Control so that MAPI over HTTP optimization gracefully degrades as SH reaches capacity
- When triggered, new MAPI over HTTP connections are bypassed
- MAPI over HTTP Admission Control is disabled by default and can be enabled using the following command:
  - `amnesiac (config) # admission control mapi enable`
- Enable on both the client- and server-side SteelHeads

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 117

This command enables the SteelHead appliances to process MAPI over HTTP traffic when SteelHeads enter admission control status. These memory enhancements allow MAPI over HTTP optimization to degrade gracefully as the SteelHead nears capacity. MAPI over HTTP optimization is maintained for as many users as possible without pushing the SteelHead over capacity.

MAPI over HTTP admission control is disabled by default.

This command only affects the SteelHead where the command is executed. We recommend enabling MAPI admission control on both the client- and server-side SteelHeads.

© 2021 Riverbed Technology. All rights reserved.

HOL1156

Optimizing MS Exchange Traffic

In this lab, you will:

- Optimize Mail Traffic with Microsoft Exchange

Duration: **45 minutes**

eLab system: link and access details provided in your course confirmation email

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 118

© 2021 Riverbed Technology. All rights reserved.

Module Review

You should now be able to:

- Describe Active Directory.
- Integrate SteelHeads with Active Directory.
- Describe NTLM and Kerberos authentication.
- Join a SteelHead to an Active Directory domain.
- Optimize SMB file shares.
- Perform CIFS prepopulation.
- Verify SMB optimization.
- Optimize MS Exchange traffic.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed
The Digital Performance Company

© 2021 Riverbed Technology. All rights reserved.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 120

This slide intentionally left blank

© 2021 Riverbed Technology. All rights reserved.