

Using LSI Logic TAS with IBM/Rational ClearCase

ClearCase Releases 3.2 or later support LSI Logic Syntax's TotalNET Advanced Server (TAS) on UNIX as an SMB server-based alternative to client-based NFS solutions. ClearCase supports TAS 5.4.1, 6.0, 6.1, 7.0 and 7.1.

Using TAS to provide mixed environment file access for ClearCase is supported only on Solaris 2.6 or later or on HP-UX 11.0 or later or on IBM AIX 4.3.X. A VOB or view server must be on a Solaris or HP-UX or AIX computer if TAS is to provide access from Windows NT clients. If a VOB or view server is on a UNIX platform not yet supported for TAS, use an NFS client product as described in ClearCase UNIX/Windows NT Interoperation.

See the Rational ClearCase Web page (<http://clearcase.rational.com>) for the latest information regarding platform and version support for ClearCase and TAS. Also, ClearCase and MultiSite Release Notes (Windows Edition) contains information about SMB server products with regard to particular ClearCase releases.

If you are using an SMB server product, you must install and configure that product on each UNIX VOB and view server host that you wish to access from a Windows NT client.

1 Upgrading from a Previous Version of TAS

If you are upgrading from one version of TAS to another, follow the instructions in TotalNET Advanced Server Release Notes.

Disabling Opportunistic Locks on ClearCase Volumes

Once you have upgraded to the new version of TAS using the Syntax instructions, ensure that opportunistic locks are disabled for each TAS volume that contains ClearCase storage. (The Support opportunistic locks check box in the volume definition should be cleared.) See Administering Volumes in the General Administrative Tasks chapter of TotalNET Advanced Server Administration Manual for details.

Upgrading TAS Does Not Require Redoing the Configuration Steps

Aside from the exceptions noted in this section, the Syntax upgrade procedures preserve the previous configuration, including existing TAS volumes and file services supporting ClearCase. (To create new TAS volumes or file services, see Creating a Volume or Configuring the File Service for ClearCase-specific details.)

The remainder of this section describes how to perform an initial TAS installation, including how to configure TAS and ClearCase to support mixed environment file access. If you are upgrading a TAS environment that was previously configured to support ClearCase, you can ignore these instructions.

2 Installing TAS

Follow the instructions in the appropriate platform-specific installation section of TotalNET Advanced Server Release Notes to install TAS on each VOB and view server requiring access from Windows NT.

3 Accessing TNAS

You can configure and administer TAS using the TotalNET Administration Suite (TNAS) Web interface. See the TAS, TNAS, and TotalAdmin chapter in TotalNET Advanced Server Administration Manual for details.

To access the TNAS Web interface:

1. Type a URL of this format in a Web browser: *http://computer:port#*

where computer represents the TAS server

port# represents the TNAS port number (the default is 7777)

The TotalNET Advanced Server (TNAS) page appears.

2. Click TotalNET Administration Suite (TNAS); a TNAS logon program appears.
3. Log on as root, using the root password for the TAS server. The TNAS interface now appears in your browser.
4. Click TAS Configuration and Administration in the sphere frame (that is, the frame at the upper right of the interface). The TAS configuration and administration menu now appears in the menu frame (that is, the frame at the lower left of the interface).

4 Performing Initial Setup of TAS

Once you have installed TAS on a server, you must perform an initial setup on that TAS installation. See the Initial Setup Steps chapter in TotalNET Advanced Server Administration Manual for details.

Click Initial Setup in the menu frame of the TNAS Web interface, and follow the instructions in the Syntax documentation, subject to the ClearCase-specific changes noted in these sections.

General TAS Settings

Accept the defaults for Admin user, Admin group, and so on in the General TAS Settings pane.

Enabling and Configuring the CIFS Realm

In the Select Realms to Configure pane, enable the CIFS realm, and click Next; the CIFS Realm Configuration pane appears.

NOTE: ClearCase does not require that the NetWare and AppleTalk realms be enabled.

Configure the CIFS realm as follows:

Server name -- Type the name of the VOB or view server, if it is not already the default.

Workgroup -- Type the name of the Windows NT domain to which your ClearCase clients belong.

Transport List -- Select the protocols appropriate for your site.

Device for NetBEUI -- Accept the default.

WINS Server -- If you are using proxy server authentication mode for CIFS file services (see Configuring the File Service), you might have to specify the IP address(es) of the WINS server(s) for the network on which the authentication proxy server resides.

See the Updating Realm Configuration section under Services for the CIFS Realm in the Configuring Services chapter of TotalNET Advanced Server Administration Manual for details about configuring the CIFS realm.

5 Configuring TAS to Support ClearCase

After initial setup, configure the TAS server to support ClearCase, using the TNAS Web interface.

Creating a TAS Username Map for clearcase_albd

Create a TAS username map from the Windows NT ClearCase service user account to a UNIX user account whose primary group ID (GID) can access all VOBs and views that will be accessed by TAS file services.

NOTE: By convention, the name of the ClearCase service account is clearcase_albd. However, a community can choose the user account name to be whatever it wants, so long as all ClearCase computers in the community have defined the ClearCase service account to be the chosen user account name.

To create the TAS username map:

1. Click TAS System in the menu frame; the TAS System Configuration and Administration pane appears.
2. Click Username Maps; the Username Maps pane appears. Make these changes to support ClearCase: In the text box, type the name of a UNIX domain user account whose principal group has the appropriate privileges for VOB/view storage access and click Create.

See ClearCase Administrator's Manual (UNIX Edition) for details about group- and user-level access to ClearCase data.

In List of client accounts, type clearcase_albd.

NOTE: If the Windows NT ClearCase service user account is configured to be a user name other than clearcase_albd, type that user name instead.

Click Submit at the bottom of the form; then click OK in the confirmation message.

See Addendum: ClearCase Service Account and ClearCase Group for details about the ClearCase service account. See Administering Username Maps in the General Administrative Tasks chapter of TotalNET Advanced Server Administration Manual for details about creating user name mappings in TAS.

Creating a Volume

Create a TAS volume that exports the directory where the VOB and/or view storage are physically located. Clients use the volume name to represent the path to the physical VOB or view storage location.

NOTE: We recommend that you test the TAS installation and configuration using non-ClearCase files before attempting to use TAS to access VOBs and views. See Testing the TAS Configuration for details.

The procedure required to support ClearCase is summarized below:

1. Click TAS System in the menu frame; then click Volumes in the TAS System Configuration and Administration pane.

2. Type a name (for example, ccstore) in the text box.

Ensure that the volume name is of a form that is acceptable for all realms that will access it. For example, some realms do not accept names longer than 12 characters.

NOTE: The text box contains a symbolic name for the volume, not the pathname to the volume storage. However, it is a good idea to specify TAS volume names that correlate to the VOB and view storage paths. (For example, a TAS volume named ccstore may be associated with /ccstore on the UNIX computer.) If these names do not correlate, examine the volume properties to determine which pathnames are associated with which volumes.

3. Click Create; a New Volume Definition pane appears. Make these changes to support ClearCase:
Pathname -- Type the pathname to the virtual root of the storage area. This pathname is the root of the VOB or view storage areas for the VOB or view server. In other words, all VOB or view storage areas must be located below this pathname (but they need not be direct subdirectories of this pathname).

For example, if you type /ccstore, legal VOB and view storage names for this volume are /ccstore/vobstore, /ccstore/home/vobstore, and /ccstore/home/project/viewstore.

Volume umask -- Type 002.

Filename Case -- Select preserve.

Support opportunistic locks -- Clear the check box.

Click Submit at the bottom of the form; then click OK in the confirmation pane.

See the Administering Volumes section in TotalNET Advanced Server Administration Manual for details about creating and administering volumes.

Configuring the File Service

To configure the TAS file service to support ClearCase:

1. Access the file service:

- a. Click CIFS Realm in the menu frame.

- b. Click Manage CIFS File Services; a list of the file services appears.

- c. Click the file service that corresponds to your TAS server; then click Administer. A menu of file service operations appears.

2. Click Configuration; an update file service form appears. Make these changes to support ClearCase:
Volume references -- Select the TAS volumes this file service references and exports.

Browse master -- Select off.

Umask -- Type 002.

Freespace report method -- Select root.

Windows 95 logon server -- Ensure this check box is cleared.

Windows NT logon server -- Ensure this check box is cleared.

NOTE: You cannot use the NT Logon Server feature if the TAS volumes are to include ClearCase storage.

Click Submit at the bottom of the form; then click OK in the confirmation pane to return to the menu of file service operations.

3. Click Authentication and Service Mode Options; the Authentication Mode form appears. Select either the Local authentication or Authentication proxy servers check box and click Submit. An authentication mode configuration pane appropriate for the mode selected appears.

NOTE: You cannot use Share mode authentication if the TAS volumes are to include ClearCase storage.

See your system administrator for assistance in determining the authentication mode for your site. See Configuring Security under Services for the CIFS Realm in TotalNET Advanced Server Administration Manual for details about file server authentication.

a. If you select Authentication proxy servers, configure the authentication mode pane as follows:
Authentication proxy servers -- Type the name of the proxy server in this text box.

NOTE: You may need to specify in the CIFS realm the IP addresses of the WINS servers for the network on which the authentication proxy server resides. (See Enabling and Configuring the CIFS Realm.)

Username map -- Select this check box to ensure that the file service references the clearcase_albd username map specified in Creating a TAS Username Map for clearcase_albd.

b. If you select Local authentication, configure the authentication mode pane as follows:

Password encryption -- Select this check box.

NOTE: If you select Local authentication, you must enter every user that will access TAS file services in a local password encryption database on the server supporting those file services. If your CIFS realm contains multiple servers supporting TAS file services, you must configure a local password encryption database on each server.

Username map -- Select this check box to ensure that the file service references the clearcase_albd username map specified in Creating a TAS Username Map for clearcase_albd.

Click Submit at the bottom of the authentication mode configuration form. Then click OK in the confirmation pane to return to the menu of file service operations.

See the Creating and Modifying File Services section in TotalNET Advanced Server Administration Manual for details about modifying file services.

6 Start Services and Accept Service Connections

To start the TAS file services and accept service connections:

1. Click TAS System in the menu frame and then click TAS System Administration.
2. Click Start Services in the TAS System Administration pane.
Click OK in the Confirmation pane; then click OK to return to the TAS System Administration pane.
3. In the TAS System Administration pane, click Accept Service Connections.
Click OK in the Confirmation pane; then click OK to return to the TAS System Administration pane.

See the Controlling the Server System section in the General Administrative Tasks chapter of TotalNET Advanced Server Administration Manual for details about starting TAS services and accepting service connections.

At this point, TAS is configured to support ClearCase. You can exit the TNAS Web interface.

7 Configuring ClearCase to Support TAS

For all ClearCase Windows NT clients that will access TAS volumes, change the MVFS Performance settings in the ClearCase Control Panel program as follows:

1. Start the ClearCase Control Panel program; the ClearCase Properties dialog box appears.
2. On the MVFS Performance tab, under Mnodes:
Click Override for both Maximum number of mnodes to keep on the free list and Maximum number of mnodes to keep for cleartext free list. Set the value for both to 800.
3. Click OK to apply the changes and close the dialog box.
4. Restart the Windows NT client.

8 Testing the TAS Configuration

This section summarizes how to test a TAS installation and configuration both using non-ClearCase files and using ClearCase VOBs and views.

Testing the TAS Configuration on Non-ClearCase Files

We recommend that you test the TAS installation and configuration using non-ClearCase files and directories before attempting to use TAS to provide file access to VOBs and views, as follows:

1. Create a directory structure on your TAS server (for example, /tasstore/testdir) and a test file in that directory (for example, /tasstore/testdir/testfile).
2. Install and configure TAS as described in this chapter, using tasstore as the volume name and /tasstore as the path name for the volume.
3. From a Windows NT client, create a file in the TAS volume. Then verify that the UNIX user and group settings for that file are correct.
4. Verify that all Windows NT clients can access the TAS volume, including testing permission and access restrictions, until you are confident that TAS is working properly.

Testing the TAS Configuration with ClearCase

To test that ClearCase and TAS are working together properly:

1. On a UNIX VOB or view server, install and configure TAS as described in this chapter, creating volumes containing VOB and/or view storage.
2. Verify that your ClearCase user and group assignments are appropriate. To do so, use the tests described in the section Checking User and Group Assignments in the Administration: Configuring a Mixed Environment for ClearCase chapter of ClearCase UNIX/Windows NT Interoperation.

3. On a Windows NT ClearCase client, use the Region Synchronizer to import views, VOBs, or both from the UNIX TAS server.
4. Ensure that you can use any UNIX views or VOBs that you imported from the TAS server.

9 Addendum: ClearCase Service Account and ClearCase Group

NOTE: This section is intended to expand on the information presented in ClearCase Requirements for Users, Groups, and Domains in the ClearCase and Windows NT Server Domains chapter of ClearCase Administrator's Manual.

Typically, for each ClearCase community (that is, a group of users sharing a set of ClearCase resources), there must be a ClearCase service user account and ClearCase group generic to all workstations accessing the community's resources.

This account and group must be defined in a Windows NT domain (that is, they cannot be local to the machine on which you are running ClearCase Site Preparation). In multi-domain environments, this Windows NT domain must be trusted by all domains containing machines in the ClearCase community.

ClearCase Service Account

ClearCase server processes run as a Windows NT user account. This user account is called the ClearCase service account.

This user must be a member of the ClearCase Group.

By convention, the name of the user account is clearcase_albd. However, a community can choose the user account name to be whatever it wants, so long as all ClearCase hosts in the community have defined the ClearCase service account to be the chosen user account name.

ClearCase Group

The ClearCase group is a Windows NT global group used to enable ClearCase server processes to access all VOB and view storage directories within a community.

NOTE: Windows NT defines the concepts of global group and local group. Be sure that the ClearCase group is created as a global group.

By convention, the name of the ClearCase group is clearcase. However, a community can choose any group name it wants so long as all ClearCase hosts in the community have defined the ClearCase group to be the group name chosen.

WARNING: ClearCase grants the members of the ClearCase group special administrative privileges (for example, the ability to delete ClearCase elements without being the element or VOB owner). Therefore, only ClearCase administrative user accounts and the ClearCase service account ought to be members of this group.

Defining the ClearCase Service Account and ClearCase Group

Typically, the ClearCase administrator defines the default ClearCase service account and ClearCase group for the community by running the ClearCase Site Preparation Wizard.

If the user account and group for the community have already been created by running the ClearCase Site Preparation Wizard previously, those values are used as the default when you rerun the wizard to create a new release area for the current ClearCase release.

If the user account and group do not yet exist (as is the case when you are running ClearCase Site Preparation for the first time), the wizard attempts to create them. In this case, you must have domain Administrator privileges when running ClearCase Site Preparation. If you do not have these privileges, the wizard cannot create the account and group; someone with the appropriate privileges must create the account and group manually before you run ClearCase Site Preparation (see [Creating the Account and Group Manually](#)). Once the account and group exist, you can specify them in the ClearCase Site Preparation Wizard (for security purposes, you must supply and confirm the password for the user account).

The account and group names specified during ClearCase Site Preparation are presented as the defaults when users run the ClearCase Installation wizard.

Creating the Account and Group Manually

The procedure in this section describes how to create a ClearCase service account and a ClearCase global group in a Windows NT domain. You must have domain Administrator privileges to create this user account and group.

To create the account and group:

1. Start the User Manager for Domains utility.
2. Create a new global group called clearcase (or whatever group name the community wants to use). In the Description box, type the following text:

Used exclusively by the ClearCase Service Account and ClearCase administrative users.

3. Create a new user, clearcase_albd (or whatever user name the community wishes to use), and put the group name defined in Step #2 in the new user's group list. Select the Password never expires check box.

In the Description box, type the following text:

Used exclusively by ClearCase servers

NOTE: If you install ClearCase on an NTFS file system, the ClearCase service account must have read/execute permissions for the ccase-home-dir directory tree. After installing ClearCase, log on as the local Administrator, navigate to the ClearCase installation directory in Windows Explorer, right-click the directory, select Properties, click the Security tab, click Permissions, and assign read/execute permissions.