

SOPHOS

SMALL BUSINESS EDITION

Sophos Control Center 4.0
Guida all'upgrade



Sommario

1	Informazioni sulla guida.....	3
2	Novità in Sophos Control Center 4.0.....	4
3	Requisiti di sistema.....	5
4	Preparazione all'upgrade.....	6
5	Upgrade di Sophos Control Center.....	8
6	Verifica della protezione dei computer.....	9
7	Impostazione del firewall.....	10
8	Impostazione del controllo applicazioni.....	11
9	Impostazione del controllo dispositivi.....	13
10	Supporto tecnico.....	16
11	Copyright.....	17

1 Informazioni sulla guida

Questa guida all'upgrade di Sophos Control Center 4.0 descrive come:

- Eseguire l'upgrade di Sophos Control Center versioni 2.0 e 2.5 a Sophos Control Center versione 4.0.
- Eseguire l'upgrade di Sophos Anti-Virus e Sophos Client Firewall (se la licenza comprende il firewall) a Sophos Endpoint Security and Control.

Se si esegue una versione precedente di Sophos PureMessage e la licenza include un upgrade all'ultima versione di Sophos PureMessage, per istruzioni su come eseguire l'upgrade, consultare la *guida all'upgrade di Sophos PureMessage*.

- Impostare le nuove funzioni di sicurezza.

È possibile reperire informazioni dettagliate su tutte le altre opzioni di configurazione di Sophos Control Center, non incluse in questa guida, nella *guida in linea di Sophos Control Center*.

La documentazione di Sophos è pubblicata in <http://www.sophos.it/support/docs/>.

2 Novità in Sophos Control Center 4.0

La nuova versione di Sophos Control Center ha le seguenti funzioni principali:

Supporto per il software di sicurezza del computer più recente

La nuova versione di Sophos Control Center consente di utilizzare Sophos Endpoint Security and Control per computer, che fornisce la versione più recente dei software antivirus e firewall per Windows 2000 e successivo.

Pannello di controllo

L'interfaccia di Sophos Control Center fornisce ora un pannello di controllo che consente di avere una panoramica immediata dello stato di sicurezza della rete. È possibile configurare i valori di soglia in modo tale che il pannello di controllo avverta ed invii messaggi di allarme ogni qual volta tali valori vengano raggiunti. Per informazioni su come configurare il pannello di controllo, consultare la guida in linea di Sophos Control Center.

Application control

Sophos Control Center consente di rilevare e bloccare le applicazioni il cui utilizzo è considerato inadatto all'ambiente lavorativo. Per ulteriori informazioni sul controllo delle applicazioni, consultare la sezione [Impostazione del controllo applicazioni](#) a pagina 11.

Device control

Il controllo dispositivi consente di impedire agli utenti l'utilizzo nei loro computer di dispositivi hardware esterni non autorizzati, strumenti di memorizzazione rimovibili e tecnologie di connessione wireless. Per ulteriori informazioni sul controllo dei dispositivi, consultare la sezione [Impostazione del controllo dispositivi](#) a pagina 13.

Lancio di Sophos PureMessage e Sophos per Microsoft SharePoint

Se la console di Sophos PureMessage o di Sophos per Microsoft SharePoint è installata nello stesso computer di Sophos Control Center, è possibile lanciarli dalla console di Sophos Control Center.

3 Requisiti di sistema

Per informazioni sui requisiti di sistema, consultare la pagina relativa ai requisiti di sistema del sito web di Sophos <http://www.sophos.it/products/all-sysreqs.html>.

È inoltre necessario avere accesso a Internet per poter scaricare il software dal sito web di Sophos.

Sophos Control Center ed i componenti del server richiedono anche di:

- Avere accesso da e a gli altri computer in rete.
- Utilizzare un sistema operativo per server (quali Windows 2000 Server con Service Pack 4 o successivo, Windows Server 2003, oppure Windows Small Business Server 2003). In caso contrario, viene compromesso il rendimento di Sophos Control Center.

4 Preparazione all'upgrade

Nota:

- Si consiglia di effettuare il backup della versione esistente di Sophos Control Center prima di passare all'upgrade.
- Dopo aver completato la procedura guidata di installazione di Sophos Control Center, sarà necessario disconnettersi dal computer in cui si è effettuato l'upgrade di Sophos Control Center e poi riaccedere, oppure riavviare il computer.
- Se si sceglie di installare Sophos Client Firewall (se incluso nella licenza), è necessario riavviare tutti i computer in cui è installato il software firewall per attivarlo.

Gli allarmi firewall generati nella versione precedente di Sophos Control Center, non saranno più disponibili una volta eseguito l'upgrade a Sophos Control Center 4.0. Sophos consiglia di risolvere tutti gli allarmi firewall prima di eseguire l'upgrade.

4.1 Prerequisiti

Prima di eseguire l'upgrade di Sophos Control Center e poi del software nei computer in rete da lui gestiti, è necessario soddisfare i seguenti prerequisiti:

- Sono rispettati tutti i requisiti hardware e software elencati nella sezione [Requisiti di sistema](#) a pagina 5.
- Si è effettuato l'accesso come amministratore al computer in cui si intende effettuare l'upgrade di Sophos Control Center.

Preparazione dei computer con sistema operativo Windows

Per i computer con sistema operativo Windows, fare quanto segue:

- Disabilitare la Condivisione file semplice su tutti i computer con sistema operativo Windows XP.

Per maggiori informazioni su come effettuare tale operazione, consultare <http://www.sophos.it/support/knowledgebase/article/12837.html>.

- Rimuovere eventuali firewall di altri produttori, eccetto Windows Firewall, da tutti i computer con sistema operativo Windows 2000/XP nei quali si desidera installare il firewall.

Preparazione dei computer in cui **NON** si desidera installare Sophos Client Firewall

Se in possesso delle workstation Windows XP Service Pack 2 o di computer Windows Server 2003 SP1 in cui **non** si desidera installare Sophos Client Firewall, e questi computer sono in possesso di Windows Firewall attivo, fare quanto riportato di seguito:

- Abilitare Condivisione file e stampanti per reti Microsoft.

Per maggiori informazioni su come effettuare tale operazione, consultare <http://www.sophos.it/support/knowledgebase/article/11738.html>.

- Accertarsi che le porte TCP 8192, 8193 e 8194 siano aperte.

- Aggiungere la seguente eccezione di programma: C:\Programmi\Sophos\Remote Management System\RouterNT.exe

Per maggiori informazioni su come effettuare tale operazione, consultare <http://www.sophos.it/support/knowledgebase/article/11075.html>.

- Riavviare i computer affinché le modifiche abbiano effetto.

5 Upgrade di Sophos Control Center

Per eseguire l'upgrade di Sophos Control Center conservando le impostazioni precedenti, accedere al computer in cui è installata la versione precedente di Sophos Control Center come amministratore o amministratore di dominio, a seconda del caso, e fare quanto descritto di seguito:

1. Chiudere tutte le applicazioni Sophos eventualmente aperte.
2. Visitare la pagina relativa al download dei prodotti Sophos <http://www.sophos.it/support/updates/> e digitare il nome utente e la password forniti da Sophos.

Seguire i link per scaricare il programma di installazione di Sophos Control Center ed eseguirlo.

3. Nella pagina **Benvenuti**, cliccare su **Avanti**.

La procedura guidata di installazione di Sophos Control Center accompagna durante l'installazione. Accettare le opzioni predefinite.

4. Portato a termine l'upgrade, cliccare **Fine** per uscire automaticamente. Se invece si desidera uscire più tardi, deselezionare la casella **Disconnetti ora** prima di cliccare su **Fine**.

Talvolta è necessario riavviare Windows invece di uscire semplicemente. In questo caso, la casella non è visualizzata e un successivo messaggio chiede se si desidera riavviare Windows subito o più tardi.

5. All'accesso successivo, entrare con lo stesso account utente.

Dopo avere completato l'installazione di Sophos Control Center, i computer verranno aggiornati automaticamente, non appena portato a termine il download della nuova versione del software per computer.

Nota: nei computer Windows 95, 98 NT e Mac OS X sarà necessario eseguire manualmente l'upgrade di Sophos Anti-Virus. Per ulteriori informazioni sulla protezione manuale dei computer, consultare la guida in linea di Sophos Control Center.

6 Verifica della protezione dei computer

È possibile verificare, tramite il Pannello di controllo, che i computer in rete siano protetti dalle minacce.

Il Pannello di controllo fornisce una visione d'insieme dello stato della protezione della rete. È possibile configurare i valori di soglia in modo tale che il pannello di controllo avverta ed invii messaggi di allarme ogni qual volta tali valori vengano raggiunti.

Per mostrare o nascondere il pannello di controllo, cliccare sul pulsante **Pannello di controllo** nella barra degli strumenti.

Per informazioni su come configurare il pannello di controllo e un elenco completo di icone e del relativo stato da visualizzare, consultare la guida in linea di Sophos Control Center.

7 Impostazione del firewall

Quando si installa Sophos Client Firewall per la prima volta, è configurato per consentire tutto il traffico. È possibile configurarlo per consentire o bloccare solo il traffico desiderato.

Se si imposta il firewall per la prima volta, per informazioni su come configurarlo, consultare la *guida in linea di Sophos Control Center*.

Nota: Sophos Firewall non supporta IPv6. Sophos Client Firewall versione 1 lascia passare i pacchetti IPv6; Sophos Client Firewall versione 1.5 e 2.0 può bloccare o consentire tutti i pacchetti IPv6 a seconda della configurazione.

8 Impostazione del controllo applicazioni

Sophos Control Center consente di rilevare e bloccare le "applicazioni controllate", ovvero applicazioni legittime che non rappresentano una minaccia per la sicurezza, ma il cui utilizzo sul posto di lavoro è ritenuto inappropriato. A tali applicazioni appartengono i client di messaggistica istantanea (IM), i client per il Voice over Internet Protocol (VoIP), i software per imaging digitale, i riproduttori multimediali o i plug-in dei browser.

Nota: questa opzione è valida soltanto per Sophos Endpoint Security and Control per Windows 2000 e successivo.

L'elenco di applicazioni controllate viene fornito e aggiornato regolarmente da Sophos. Non è possibile aggiungere nuove applicazioni all'elenco, ma è possibile inviare a Sophos la richiesta di includere una nuova applicazione legittima che si desidera controllare all'interno della propria rete. Per informazioni, consultare l'articolo della knowledge base 35330 (<http://www.sophos.it/support/knowledgebase/article/35330.html>)

Per informazioni sugli eventi del controllo applicazioni, consultare la guida in linea di Sophos Control Center.

8.1 Impostazione del controllo applicazioni

È possibile configurare Sophos Control Center in modo che ricerchi in accesso le applicazioni che si desidera controllare sulla rete.

1. Nel riquadro di sinistra, sotto **Configurazine**, cliccare su **Configura controllo applicazioni**.

Viene visualizzata la finestra di dialogo **Configura controllo applicazioni**.

2. Nella scheda **Scansione**, impostare le opzioni come segue.

- Per abilitare la scansione in accesso, spuntare la casella **Abilita scansione in accesso**. Se si desidera rilevare le applicazioni, ma non si desidera bloccarle in accesso, selezionare la casella **Rileva ma consenti l'esecuzione**.
- Per abilitare la scansione su richiesta, spuntare la casella **Abilita scansione su richiesta e pianificata**.

Nota: le impostazioni antivirus e HIPS dell'utente determinano quali file vengono esaminati (vale a dire le estensioni e le esclusioni).

3. Cliccare sulla scheda **Autorizzazione** e selezionare l'applicazione che si desidera controllare.

Per informazioni su come selezionare applicazioni, consultare la sezione [Selezione delle applicazioni da controllare](#) a pagina 11.

8.2 Selezione delle applicazioni da controllare

Per impostazione predefinita, tutte le applicazioni sono consentite. Per selezionare le applicazioni che si desidera controllare, procedere come segue.

1. Nel riquadro di sinistra, sotto **Configurazine**, cliccare su **Configura controllo applicazioni**.

2. Nella finestra di dialogo **Configura controllo applicazioni**, cliccare sulla scheda **Autorizzazioni**.

3. Selezionare **Tipo applicazione**, per esempio **Condivisione file**.

L'elenco completo delle applicazioni incluse nel gruppo è visualizzata nell'elenco **Autorizzate**.

- Per bloccare un'applicazione, selezionarla e spostarla nella lista **Applicazioni bloccate** cliccare sul pulsante "Aggiungi".



- Per bloccare qualsiasi nuova applicazione che Sophos aggiungerà a quel tipo in futuro, spostare **Tutte quelle aggiunte da Sophos in futuro** nell'elenco **Applicazioni bloccate**.
- Per bloccare qualsiasi nuova applicazione di quel tipo in futuro, spostarle tutte dalla lista **Autorizzate** a quella **Bloccate**, cliccando sul pulsante "Aggiungi tutte".



Per informazioni su come installare applicazioni controllate, consultare la guida in linea Sophos Control Center.

9 Impostazione del controllo dispositivi

Importante: Sophos Device Control non va installato insieme a un eventuale software di controllo dei dispositivi prodotto da terzi.

Device control consente di impedire agli utenti l'utilizzo nei loro computer di dispositivi hardware esterni non autorizzati, strumenti di memorizzazione rimovibili e tecnologie di connessione wireless. Ciò riduce in modo significativo il rischio di perdite accidentali di dati e limita le possibilità degli utenti di introdurre software dall'esterno dell'ambiente di rete.

I dispositivi di memorizzazione rimovibili, le unità disco ottico e le unità floppy disk possono essere impostate per fornire accesso in sola lettura.

Per impostazione predefinita, il controllo dispositivi è disattivato e tutti i dispositivi sono consentiti.

Se si desidera attivare il controllo dispositivi per la prima volta, Sophos consiglia di:

- Selezionare i tipi di dispositivo da controllare.
- Rilevare i dispositivi senza bloccarli.
- Impostare degli allarmi del controllo dispositivi.
- Rilevare e bloccare i dispositivi o consentire l'accesso in sola lettura ai dispositivi di memorizzazione.

Per informazioni sugli eventi del controllo dispositivi, consultare la guida in linea di Sophos Control Center.

9.1 Tipi di dispositivi controllabili

Device Control consente di bloccare due tipi di dispositivo: *di memorizzazione* e *di rete*.

Memoria

- Dispositivo di memoria rimovibile (per esempio unità flash USB, lettori di schede per PC, unità hard disk esterne)
- Unità disco ottico (unità CD-ROM/DVD/Blu-ray)
- Unità floppy disk.
- Dispositivi di memorizzazione rimovibili sicuri (per es. SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox e IronKey Enterprise Basic Edition USB flash con cifratura dell'hardware)

Utilizzando la categoria dispositivo di memoria rimovibile sicuro, è possibile utilizzare facilmente i dispositivi di memoria rimovibile sicuri supportati, mentre vengono bloccati quelli non sicuri. Un elenco aggiornato dei dispositivi di memoria rimovibile sicuri supportati è disponibile sul sito web di Sophos (www.sophos.it).

Rete

- Modem

- Wireless (interfaccia Wi-Fi, 802.11 standard)
- Interfacce bluetooth
- Infrarossi (Interfaccia infrarossi IrDA)

Device Control blocca interfacce e dispositivi, sia interni che esterni. Per es. il blocco delle interfacce bluetooth porterà al blocco di entrambe:

- L'interfaccia Bluetooth incorporata in computer
- Qualsiasi scheda Bluetooth USB inserita nel computer.

9.2 Impostazione del controllo dispositivi

È possibile configurare Sophos Control Center in modo che esegua la scansione in accesso dei dispositivi che si desidera controllare sulla rete.

1. Nel riquadro di sinistra, sotto **Configurazine**, cliccare su **Configura controllo dispositivi**.
Viene visualizzata la finestra di dialogo **Configura controllo dispositivi**.
2. Nella scheda **Configurazione**, impostare le opzioni come segue.
 - Per abilitare il controllo dispositivi, selezionare la casella di spunta **Abilita la scansione del controllo dispositivi**. Se si desidera rilevare dispositivi ma non bloccarli, selezionare la casella di spunta **Rileva ma non bloccare i dispositivi**.
 - Per impostare il livello di accesso per tutti i tipi di dispositivo, cliccare sulla colonna **Stato** di fianco al tipo di dispositivo e successivamente sul menu a discesa che compare. Selezionare il tipo di accesso che si desidera consentire.

Per impostazione predefinita, i dispositivi hanno accesso completo. Per quanto riguarda i dispositivi di memorizzazione rimovibili, le unità disco ottico e le unità floppy disk, è possibile cambiare il tipo di accesso e selezionare “Bloccato” o “Sola lettura.” Per quanto riguarda i dispositivi di memorizzazione rimovibili sicuri, è possibile cambiare il tipo di accesso e selezionare “Bloccato”.

Per informazioni su come impostare gli allarmi del controllo dispositivi, consultare la guida in linea di Sophos Control Center.

9.3 Esenzione di un dispositivo

È possibile esentare un dispositivo dai criteri del controllo dispositivi.

È possibile esentare un'istanza di dispositivo (“Solo questo dispositivo”) o un modello di dispositivo (“Tutti i dispositivi di questo modello”). Non impostare le esenzioni sia al livello del modello che dell'istanza del dispositivo. Se vengono definite entrambe le esenzioni, il livello dell'istanza del dispositivo avrà priorità.

Per esentare un dispositivo:

1. Nel menu **Visualizza**, cliccare su **Eventi controllo dispositivi**.
Si apre la finestra di dialogo **Controllo dispositivi - Visualizzatore eventi**.

2. Se si desidera visualizzare solo determinati eventi, nel riquadro **Cerca criteri**, impostare i filtri adeguati e cliccare su **Cerca** per visualizzare tali eventi.
3. Selezionare la voce del dispositivo che si desidera esentare e cliccare su **Esporta dispositivo**. Viene visualizzata la finestra di dialogo **Esenta dispositivo**. Sotto **Dettagli dispositivo**, vengono visualizzati tipo, modello e ID del dispositivo.

10 Supporto tecnico

Per ricevere assistenza tecnica relativa a questa versione beta:

1. reperire i dati del proprio indirizzo web di cliente beta (nell'e-mail inviata da Sophos)
2. visitare quell'indirizzo
3. compilare e inviare il modulo.

11 Copyright

Copyright © 2009 Sophos Group. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Plc e Sophos Group. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

Alcuni programmi software sono concessi in licenza (o in sottolicenza) all'utente secondo i termini della GNU General Public License (GPL) o licenze similari per il software libero che, tra gli altri diritti, permettono all'utente di copiare, modificare e redistribuire determinati programmi, o porzioni di programma, e di accedere al codice sorgente. La GPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa e distribuito a un utente in formato binario eseguibile, che il codice sorgente venga messo a disposizione anche degli altri utenti. Per qualsiasi di tale software che sia distribuito insieme a questo prodotto Sophos, è possibile ottenere il codice sorgente tramite ordine postale inviandone richiesta a Sophos.

E-mail: savlinuxgpl@sophos.com

Indirizzo: Sophos Plc, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito.

Copia dei termini della GPL è reperibile all'indirizzo www.gnu.org/copyleft/gpl.html

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it

yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹³ around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>

5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>