

Virginia Tech Active Directory Child Domain Usage Requirements

Information for Department Heads

Virginia Tech provides an Active Directory implementation called the “VT AD” domain. It is also known as the “HOKIES” domain. The VT AD domain provides centralized directory services along with related features and functions. Decentralized management of a subsidiary domain—called a “child domain”—is a reasonable option for departments or units that have sufficient resources to manage their own subsidiary domain and desire the flexibility that such management can provide. With the relationship with the VT AD domain, these child domains build on that trusted relationship to be able to trust other child domains as well.

Child domains provide both the flexibility of local management along with the benefits of central management of common features such as the Domain Name Service, the user and contact information, and related other services.

Running a child domain requires sufficient resources in staffing—both time and expertise, as well as certain hardware requirements. Department heads must be aware of these requirements and see to their support in order to continue the child domain. These requirements include:

- Computing hardware that is technically sufficient to manage the child domain;
- Physical security for that hardware;
- System administrator expertise and dedicated time to ensure the ongoing security of the software; and
- Sufficient staffing and back-up staffing to ensure the on-going operations of the child domain, with an individual who is a full-time salaried Virginia Tech employee overseeing the administration of the child domain (“administrator”).
- Further, department heads must see that the technical contact of the child domain is identified to Information Technology.

More detailed specifications may be found in the AD Child Domain Usage Requirements section

The department head also acts as the back-up contact person if the primary contact and the individual designated as the administrator of the system are both unavailable.

Finally, department heads are expected to provide the resources for corrective actions to preserve the security and integrity of the child domain and any impacts that it may have on the overall Active Directory. If the requisite resources are not provided, the child domain may be removed from the Active Directory structure and lose the advantages of both the centralized management services and of the trust relationship with other child domains as well as the VT AD.

The Microsoft Implementation Group will assist with evaluation of whether the child domain structure is the solution that best meets the needs of your department, or whether other solutions (Centralized Services or University Services) may better meet your needs.

AD Child Domain Usage Requirements

Background

Microsoft Active Directory is a decentralized and distributed set of applications, systems and services. Virginia Tech has an Active Directory implementation called the “VT AD”, otherwise known as “HOKIES” and/or “w2k.vt.edu”. The VT AD provides centralized directory services, authorization and authentication, group management, user and workstation management, dynamic DNS, and many other powerful and beneficial features and functions. The VT AD follows an inverted forest topology; there is a root domain (a domain is a security boundary for computers and users), and child domains below this root. Child domains are afforded the maximum amount of flexibility within this forest structure. Child domains build a trust relationship with their peers (other child domains) and the root. With this trust relationship come important responsibilities to insure the continued security, stability and scalability of the VT AD. These benefits and responsibilities are denoted below and require official signatures from administrative and Department Head contacts.

Benefits of participation:

1. Central management of DNS (Domain name service). The VT AD Enterprise Administrators (EA) will maintain this infrastructure service for your child domain.
2. Central management of user and contact objects. The VT AD Root administrators work with IMS, the Middleware group, and IT Security Office (ITSO) to provide secure and up-to-date HOKIES accounts for Faculty and Staff.
3. Central management of web based applications for supplemental AD management. The VT AD Root administrators design, develop, and release web based applications to help child domain administrators manage systems and services in an intuitive and efficient manner.
4. Supplemental system support. The VT AD Root administrators have 24x7 responsibilities for the maintenance of the root AD. They are available during business hours to help child domain troubleshoot system or service issues.
5. Peer to peer support. The VT AD Root administrators maintain a private listserv (w2k-admin) to which all child domain administrators are automatically subscribed. Security, hints, and tips are freely exchanged via this mechanism.

Responsibilities of participation:

If these responsibilities fail to be met, at any time, a set of procedures activate in order to expedite corrective action. These potential actions include (in the severest case) forced demotion of the child domain and deletion of all child domain local users, groups, policies, etc. (See “Resolution procedures for Active directory usage requirement issues”)

System requirements

1. A child domain must have at least two systems running as domain controllers (DCs) in a 24x7 capacity.
2. The child domain controllers must meet or exceed Microsoft’s minimum computer hardware requirements.
(<http://www.microsoft.com/windows2000/server/evaluation/sysreqs/default.asp>)

3. No 3rd party or Microsoft add-on software is allowed on child domain controllers. This includes IIS, Certificate Services, Indexing Service, Windows Media Services, DNS, DHCP, WINS, file and print services, or antivirus software. (Exceptions made with written agreement of EAs)
4. The domain controllers must be in a daily online backup program and their recoverability fully tested.
5. Child domain administrators will maintain their DCs in compliance with the official Microsoft support lifecycle. They will commit the necessary hardware and software to migrate production systems to the next supported Operating System before the extended support retirement date. (<http://support.microsoft.com/default.aspx?pr=lifecycle>)

Security requirements

1. The child domain must allow and not attempt to block domain or site group policies applied to the root or directly to the child by EAs.
2. Only administrator logins will be allowed on the child domain controllers.
3. The domain controllers will be housed in a secure physical location (with auditable access) and with uninterruptible power.
4. Success and failure event auditing will be enabled for the domain controllers and two weeks of event/audit logs will be kept and made accessible to the EAs for security/debugging purposes.
5. Child domain administrators will install all service packs, hotfixes, security roll-ups and IPSEC rule sets in coordination with the EAs. Installation is first vetted in MIG's development and test environments by the EAs. Once testing is successfully completed, installation approval email will be sent to the w2k_admin listserv and notice given as to the criticality (based on MS ranking) of the installation and the timeframe within which installation must occur (typically 10 business days). After the conclusion of this timeframe the EAs will remotely audit the child DCs to verify compliance. The EAs respect the privacy and sovereignty of child domains, therefore these audits will focus on the minimum required information necessary to verify compliance.

Network requirements

1. The child domain controllers will use static, valid Internet-routable accessible IP addresses.
2. The child domain controllers will not firewall or IPSEC traffic to/from other child domain controllers or the root domain controllers.
3. All Windows systems that are members of the child domain will follow the proscribed DNS naming scheme of; [hostname].[child domain].w2k.vt.edu. Hostname will be the same as the machine's NetBIOS name and may not contain underscore characters.
4. All Windows systems that are members of the child domain will use the VT AD root DNS servers as their primary and secondary DNS server addresses.
5. Creation of child-of-child domains is not allowed.

Staffing requirements

1. A technical contact is the first and primary point of contact when interaction with the child domain is required. The technical contact will be the administrator of the child domain systems and directly responsible for uptime, security, backups, and technical compliance with usage requirements.

2. An administrative contact is required to sign this usage document. It cannot be the same person as the technical contact. The administrative contact will be the secondary contact if the technical contact cannot be reached in a timely manner. The administrative contact will maintain the contact information for this document. If technical contact staff changes, the administrative contact is required to contact IMS to update this document within ten business days. The administrative contact must be a full time, salaried employee of Virginia Tech.
3. A Department Head is required to sign this usage document. The Department Head is the tertiary contact when both the technical and administrative contacts cannot be located in a timely manner or if a contact's actions are deemed unsatisfactory to meeting the requirement conditions. The Department Head is ultimately responsible for any security, stability or scalability concerns their child domain causes to their own child domain and any invalid interaction with the VT AD forest.
4. The technical and administrative contacts will be added to a private VT listserv (w2k-admin) for VT AD child domain administrators. This listserv is used to relay important information in a timely manner and communicate effectively with peers. The contacts are required to monitor this listserv with their primary email account.
5. While we encourage peer support mechanism (discussions with EAs, techsupport listserv, w2k_admin listserv, google, etc), it may be necessary to contact professional support services. The child domain contacts acknowledge this need and their department will expend the necessary funds to identify and repair any problems with their DCs within the required timeframe. (MIG suggests familiarizing yourself with the support options offered by MS PSS, see <http://support.microsoft.com/default.aspx?scid=fh;en-us;prodoffer11a&sd=GN>)

Acknowledgement is given by the signers that a needs assessment has been completed contrasting the costs/benefits of maintaining a fully deployed child domain within the VT AD versus joining a centrally managed child domain such as Central Services, or University Services. The signers understand the requirements for continued membership and accept all responsibility for maintaining their child domain in accordance with these conditions.

Technical Contact:

Print: _____

Email: _____

Phone: _____

Administrative Contact:

Print: _____

Sign: _____

Email: _____

Phone: _____

Department Head Contact:

Print: _____

Sign: _____

Email: _____

Phone: _____

-----EA enter information below-----

Date/Time: _____

Child domain controller 1: _____

Child domain name: _____

Child domain controller 2: _____

Notes:

Important information

[Technical contacts (EA)]

For hardware, software, and security questions

General questions email: w2k@vt.edu See also <http://www.w2k.vt.edu> for more info

Primary:	Marc DeBonis	Secondary:	Steve Warrick
Phone:	231-2728	Phone:	231-2634
Email:	marcd@vt.edu	Email:	swarrick@vt.edu

Address: Microsoft Implementation Group
1700 Pratt Drive
Mail Code 0214
Blacksburg, VA 24060

[Account management contacts (IMS)]

For AD object (users, contacts, OUs) questions

General questions email: IMSStaff-DL@exchange.vt.edu

Primary:	Rhonda Randel	Secondary:	Doug Atwater
Phone:	(540) 231-4245	Phone:	(540) 231-1866
Email:	randelr@vt.edu	Email:	datwater@vt.edu

Address: IT Security/IMS
1700 Pratt Drive
Mail Code 0214
Blacksburg, VA 24060

[Policy management contacts (ITSO)]

For usage requirements and enforcement questions

Primary:	Wayne Donald	Phone:	(540) 231-7694
Email:	wdonald@vt.edu		

Address: Info Tech Security Office
1300 Torgersen Hall
Mail Code 0284
Blacksburg, VA 24061

[Listservs]

Public:	techsupport@listserv.vt.edu	Private:	w2k_admin@listserv.vt.edu
---------	--	----------	--

[Active Directory DDNS addresses]

Primary:	grok.w2k.vt.edu	Secondary:	freeman.w2k.vt.edu
	198.82.162.237		198.82.145.6

Resolution procedures for Active Directory Usage Requirements Issues

If the responsibilities outlined in the document “VT Active Directory child domain usage requirements” are not successfully met, the Enterprise Administrators (EAs) will initiate a remediation process as defined below.

1. Identify the issue; rate the criticality, the required resolution process, and the timeframe within which to address this issue.
2. Notify in writing the technical and administrative contact of the child domain with the issue, providing all documentation from step 1.
 - a. Identify if issue solution requires contacting 3rd party pay for services, such as Microsoft Premier Support Services (PSS). The child domain department’s commitment to expend funds for problem resolution is stipulated in the Usage Requirements document.
3. Verify contacts have received issue resolution request.
4. Allot the required time to resolve the issue.
5. Audit child domain to independently verify the issue has been resolved to both parties satisfaction.
6. If successful, provide in writing to the technical and administrative contacts that the issue has been successfully resolved. End.
7. If unsuccessful, contact the technical and administrative contacts and determine any valid mitigating circumstances concerning the issue.
8. If circumstances warrant, extend timeframe. Go to step 4.
9. If circumstances do not warrant extending the timeframe, notify technical, administrative, and department head contacts. Providing all documentation from step 1 and step 7, give deadline for required resolution and consequences of further unsuccessful audits.
10. Allot time for final resolution of issue.
11. Audit child domain to independently verify the issue has been resolved to both parties satisfaction.
12. If successful, provide in writing to the technical, administrative, and department head contacts that the issue has been successfully resolved. End.
13. If unsuccessful, proceed with identified course of action (IPSEC child DCs, demote child domain, etc). Notify technical, administrative, and department head contacts of action taken. End.

Issue risk rating/Timeframe

Critical risk

- Ex. Exploit that threatens the VT AD forest and children is out and available.
 - Ex. Failure of child domain controller causing DoS to other domains in forest
- Timeframe: ASAP within 1-3 days

High risk

- Ex. Exploit is known but not available, but will be available shortly.
 - Ex. Damage to interior door of machine room allows unauthorized access.
- Timeframe: Within 1 week's time

Medium risk

- Ex. No known exploit is available, but MS has identified risk.
- Timeframe: Within 2 week's time

Low risk

- Ex. VT AD not directly impacted, but MS suggests the fix
- Timeframe: Within 3 week's time