



Questions & Answers from the April 29, 2009 Discussion

*Responses from the ICS team to questions
asked at the discussion.*

Voice Messaging

Discussion: NEC Unified Messaging 8500 version 3.0 (or older) is not compatible with Exchange 2007. The Department of Administration chose to transition to Cisco Unity Connections. With Unity connections the voice messages are stored in the voice messaging system and not in Exchange (Integrated Messaging Environment). Where the messages are stored needs to be a consideration as to whether space is taken up in users' Exchange mailboxes. If voice messages are stored in Exchange should Exchange become unavailable voice messages as well as email messages become unavailable. If the voice messages are stored on the voice messaging system they remain available if Email is not; you have the option of the traditional method of calling your voice mailbox to retrieve messages.

Q: Will you change the implementation in the future or include fax capabilities?

A: An Enterprise voice messaging has not yet been a topic of discussion of the ICS Technical sub-committee. When design and architecture needs arise, then the Technical sub-committee is convened to discuss the options and determine the best design. This sub-committee includes representatives from multiple state agencies.

Q: How is voice mail accessible if the LAN goes down?

A: Voicemail messages stored in the ICS Email server would NOT be accessible in the event of a LAN outage. If the message store is maintained on the voicemail server then dial-in access to voicemail would still be available in the event of a LAN outage.

Network Address Translation (NAT)

Discussion: NAT needs to be moved to the Enterprise Internet facing firewalls due to issues that NAT causes with Active Directory and Exchange in particular Kerberos, DC to DC replication, and Exchange server with the client. Basically the static (un-natted) address registered from the source is expected to be the same address that is presented at the destination and if it is not then communication is denied. This is a security design to prevent a man-in-the-middle attack.

Questions and Answers from the April 29th 2009 Discussion

Q: In a mixed NAT/PAT environment will addressing need to be changed?

A: The static addresses will not remain the same. This question is in reference to an agency with a mixed NAT environment (PAT and static NAT) and what would happen with the static NATs. We can do the static NAT, but that the external addresses it would be translated to would have to change to be within a range that exists on the external interface of the firewall.

Q: How does NAT affect VPN connectivity?

A: The VPN user will still communicate to the inside address. There may need to be a change to the inside IP Address the VPN client communicates to, nothing else should need to change. However, as there are alternatives into VPN solution design each agency's solution must be reviewed to determine what if any changes will be needed.

Messaging

Q: How big is a mailbox allowed to be in order to be migrated over?

A: 200Mb

Q: Will you allow PST files in the new environment?

A: Archiving will be the responsibility of the agency so it is up to the agency to decide whether they implement PSTs or some other method of archiving. PSTs would be stored within the agency's environment and not with the ICS system. An enterprise archiving solution may be looked at in the future.

Q: Who manages DNS?

A: ICS System Administrators will manage DNS. However, a local DNS can be placed at each agency. One or more secondary DNS servers will be allowed to run at each agency as need allows.

Q: What about DHCP servers who manages them?

A: Agencies will have the responsibility of their own DHCP servers.

Q: Can an agency's Organizational Unit (OU) be hidden?

A: It is possible but highly complex and not recommended as it can cause problems with the entire forest if not configured correctly. Several Microsoft MVP Engineers have indicated they would not attempt it and to stay away from it as it will cause any number of problems and make troubleshooting impossible.

Questions and Answers from the April 29th 2009 Discussion

Q: Can an agency create new forests?

A: Agencies are free to create forests for testing or whatever other purposes. ICS will not be incorporating additional forests into the infrastructure..

Q: For DNS secondary zones, does it download the entire state DNS?

A: Yes, the first time, which is quite large. Subsequent changes will come as updates to the existing DNS information and does not require a full download each time.

Q: Will agencies be given a designated IP range to prevent DHCP issues?

A: No

Q: Will passwords for Backup Exec be handled by ICS?

A: Yes

Q: Can VMware ESX servers be added into Active Directory (AD)?

A: ESX cannot be added as a manageable or member object in AD. Guest Windows servers on the ESX host can just as with their physical counterparts. It is possible to have Linux servers authenticate user access to them through Active Directory. This is all up to the agency's needs or requirements.

Q: Will NAS backend storage work in AD?

A: Yes, if it utilizes AD.

Q: Can password change requirements be stricter than the ICS domain default of 90-days?

A: Not at this time. AD Forest Functional Level 2008 includes the ability to have differing password policies applied as opposed to the one domain-wide policy in effect now. However, ICS is currently at AD Forest Functional Level 2003 and the policies are not available. ICS cannot transition to Forest Functional Level 2008 until after all agencies are migrated.

Q: Will AD and Exchange changes be pushed down at anytime ICS Administrators decide to do so?

A: Changes will happen, but not without a Change Management process and a Change Advisory Board making decisions. Agencies will have an opportunity to review the proposed changes and make

Questions and Answers from the April 29th 2009 Discussion

comment. ICS is in the process of implementing a Change Management process.

Q: How many user passwords will be remembered?

A: 24

Q: Will OU administrators have control of their Group Policies?

A: Yes, agency OU administrators will have complete control of their Group Policies. It is recommended that agencies begin developing their policies with Group Policy Preference Extensions (GPPE). A Vista workstation or Server 2008 is required in order to use this capability. GPPE management is not available in XP- and Server 2003-based management computers. There are three policies that are required at the domain level; complex passwords, a 20-minute screen save lock, and a "clear last logged on account" policy whereby the username last logged on to the computer is not shown at the logon prompt. What this means to the users is that they will be required to type both their usernames and passwords on initial logon. The screen lock logon prompt will have their usernames showing, however. Other than these, agencies establish their own policies.

Q: Can agencies maintain their Certificate Authority (CA)?

A: ICS will configure and maintain an offline root CA and agencies are free to install a subordinate CA. Agencies are also welcome to maintain their own independent PKI although it is important to realize that implementing this setup, by definition, cannot be integrated with their users' ICS accounts so that users will not be able to perform two-factor authentication and so on.

Q: For non-Blackberry PDAs, how many IOPs are used?

A: Unknown at this time, still researching.

Q: Does the agency password policy have to match the ICS policy before migration?

A: Yes

Q: Do user names need to change?

A: No, as long as the name is unique within the ICS domain. If a username already exists within the domain then the next user coming on board with that same username must change.

Questions and Answers from the April 29th 2009 Discussion

Q: If an agency has utilized an AD field to store phone numbers will they transition over?

A: Yes, if a schema extension is not required.

Q: If an agency utilizes Journaling, will they be able to continue utilizing it?

A: Yes, Journaling is a built-in feature with Exchange. Journaling will be implemented on the ICS Exchange servers and on the storage group in which an agency's mailboxes reside. Per store, it is possible to turn on Journaling and as each agency will have their own Storage Group, this choice is theirs. The ICS technical team will need to understand exactly what hooks and thus permissions the software suite which will be performing archiving (or whatever else) will require beforehand.